DİJİTAL ÇAĞDA BİLİŞSEL VE TOPLUMSAL DAYANIKLILIK

YENİ MEDYA OKURYAZARLIĞI

EMRE ERDOĞAN & PINAR UYAN-SEMERCİ

Dijital Çağda Bilişsel ve Toplumsal Dayanıklılık

Yeni Medya Okuryazarlığı

Emre Erdoğan

Pınar Uyan-Semerci

EMRE ERDOĞAN, PINAR UYAN-SEMERCİ

DİJİTAL ÇAĞDA BİLİŞSEL VE TOPLUMSAL DAYANIKLILIK

YENİ MEDYA OKURYAZARLIĞI

CREATING SOCIETAL COGNITIVE RESILIENCE AGAINST INFORMATION DISORDERS

resaid JEAN MONNET CENTRE OF EXCELLENCE

Bu yayın, İstanbul Bilgi Üniversitesi bünyesinde yürütülen ve Avrupa Birliği Jean Monnet Mükemmeliyet Merkezleri Programı tarafından desteklenen RESAID (Bilgi Düzensizliklerine Karşı Bilişsel Toplumsal Dirençlilik Yaratmak) kapsamında hazırlanmıştır. Ancak ifade edilen görüş ve düşünceler sadece yazar(lar)a aittir ve Avrupa Birliği veya Avrupa Eğitim ve Kültür Yürütme Ajansı'nın (EACEA) görüşlerini yansıtmak zorunda değildir. Avrupa Birliği ve EACEA bunlardan sorumlu tutulamaz.

ISBN: 978-605-399-669-9
E-ISBN: 978-605-399-670-5

İSTANBUL, MART 2026

TASARIM GÖKÇE UYSAL-GÜNDOĞDU
YAYINA HAZIRLAYAN GÖKÇE UYSAL-GÜNDOĞDU
KAPAK GÖRSELİ LALE DURUİZ
BASKI VE CİLT Vizyon Basımevi Kağıtçılık Matbaacılık ve Yayıncılık San. Tic. Ltd. Şti.
Beylikdüzü O.S.B. Mah. Orkide Cad. No:1/Z Beylikdüzü İstanbul
Telefon: 0212 671 61 51 / Faks: 0212 671 61 50 • Sertifika No: 52098

İstanbul Bilgi University Library Cataloging-in-Publication Data
İstanbul Bilgi Üniversitesi Kütüphanesi Kataloglama Bölümü Tarafından Kataloglanmıştır.

Names: Erdoğan, Emre, author. | Uyan-Semerci, Pınar, author.
Title: Dijital çağda bilişsel ve toplumsal dayanıklılık : yeni medya okuryazarlığı / Emre Erdoğan, Pınar Uyan-Semerci.
Description: Bilgi Düzensizliklerine Karşı Bilişsel Toplumsal Dirençlilik Yaratmak (RESAID), 2026. | Includes bibliographical references.
Identifiers: ISBN: 9786053996699 (paperback) | 9786053996705 (ebook)
Subjects: LCSH: Media literacy. | Mass media --Social aspects. | Mass media --Moral and ethical aspects. | Truthfulness and falsehood. | Misinformation --Psychological aspects. | Disinformation --Case studies. | Fake news. | Facts (Philosophy) | Persuasion (Psychology) | Attitude change. | Polarization (Social sciences) | Mass media --Technological innovations. | Artificial intelligence --Social aspects. | Gamification.
Classification: LCC: P96.M4 E73 2026

EMRE ERDOĞAN

PINAR UYAN-SEMERCİ

DİJİTAL ÇAĞDA BİLİŞSEL VE TOPLUMSAL DAYANIKLILIK

YENİ MEDYA OKURYAZARLIĞI

Kitap ve ders videolarına erişmek için resaid.bilgi.org.tr adresini veya karekodu kullanabilirsiniz.

İÇİNDEKİLER

Yazarlar

EMRE ERDOĞAN

Prof. Dr. Emre Erdoğan, İstanbul Bilgi Üniversitesi Uluslararası İlişkiler Bölümü öğretim üyesidir. Siyaset bilimci olan Erdoğan, siyasal katılım, dış politika, kamuoyu, çocuk ve gençlerin iyi olma hali, metodoloji ve istatistik alanlarında araştırmalar yapmakta ve dersler vermektedir. Türkiye'de sosyal sermaye, gençlik, ötekileştirme, kutuplaşma, bilgi düzensizlikleri ve popülizm konularında çalışmalarını sürdürmektedir. Çok sayıda ulusal ve uluslararası araştırma projesinde yürütücü ve araştırmacı olarak yer alan Erdoğan, Reflektif Sosyal Bilimler Dergisi'nin kuruluşundan itibaren editörlüğünü üstlenmiştir.

PINAR UYAN-SEMERCİ

Prof. Dr. Pınar Uyan Semerci, İstanbul Bilgi Üniversitesi Uluslararası İlişkiler Bölümü, Siyaset Bilimi ve Kamu Yönetimi Programı'nda öğretim üyesidir. Akademik çalışma alanları siyaset felsefesi, karşılaştırmalı siyaset, sosyal politika ve sosyal bilimlerde metodoloji olan Uyan-Semerci, adalet, haklar, vatandaşlık, insani gelişim, yapabilirlik yaklaşımı, yoksulluk, göç, kolektif kimlik oluşumları, ötekileştirme, kutuplaşma, bilgi düzensizlikleri, çocuk işçiliği ve çocuğun iyi olma hali konularında birçok ulusal ve uluslararası araştırma projesi yürütmüş, makale ve kitap yayını yapmıştır.

Başlarken

İnternetin hayatımıza girişiyle bilgiye daha kolay ulaşmanın dünyayı daha iyi bir yer yapacağı kanısı oluşmuştu. Ancak zamanla gördük ki bilgiye erişmek kolaylaşırken, doğru bilgiye ulaşmak ve gerçeği yalandan ayırmak giderek zorlaştı. Nobel ödüllü iktisatçı Herbert Simon'ın yıllar önce dikkat çektiği "bilgi zenginliğinin dikkat yoksulluğu yaratması" paradoksu, artık günlük hayatımızın kaçınılmaz bir parçası haline geldi.

İstanbul Bilgi Üniversitesi Göç Çalışmaları Uygulama ve Araştırma Merkezi bünyesinde yürüttüğümüz araştırmalarda, toplumdaki ötekileştirme, kutuplaşma ve ayrımcılık pratiklerine odaklanırken, medyanın bu süreçlerdeki belirleyici etkisini yakından gözlemleme fırsatı bulduk. Çalışmalarımız hem sosyal medya hem de geleneksel medyanın, toplumun farklı kesimlerinin birbirinden kopuk "gerçeklikler" içinde yaşamasına yol açtığını ve bu durumun bireysel tutum ile davranışları nasıl şekillendirdiğini ortaya koydu. Özellikle tüm dünyayı etkileyen pandemi dönemiyle birlikte infodemi ve genel anlamda bilgi düzensizlikleri, yoğun olarak emek verdiğimiz, günlük hayatımızı ve iyi olma halimizi derinden etkileyen acil bir çalışma alanımıza dönüştü. Bu süreçte TÜBİTAK desteğiyle yürüttüğümüz, bireylerin COVID-19 salgınındaki yanlış bilgilere karşı tutumlarını inceleyen araştırma projesi, sorunu bilimsel bir çerçevede derinlemesine analiz etmemiz için bize çok güçlü bir temel sundu.

Bugün, bu birikimimizi Avrupa Birliği Jean Monnet Mükemmeliyet Merkezleri Programı tarafından desteklenen ve İstanbul Bilgi Üniversitesi bünyesinde yürüttüğümüz RESAID (Bilgi Düzensizliklerine Karşı Toplumsal

Bilişsel Dirençlilik Yaratmak) çatısı altında kapsamlı bir ders kitabına dönüştürmeye çalıştık. Yıllara yayılan akademik araştırma, eğitim ve saha deneyimimizin somut bir ürünü olan bu kitabı hazırlarken temel bir hedefimiz vardı: İçinde yaşadığımız ve her gün devasa miktarda veriye maruz kaldığımız dijital dünyada, sizlere, yeni medya okuryazarlığı ile bilişsel ve toplumsal dirençlilik için farklı disiplinlerdeki ilgili yazından yararlanarak kapsamlı ancak olabildiğince anlaşılır, pratik önerileri de içeren bir kitap sunmak.

Temel amacımız; bilgi düzensizliklerinin çoklu krizler çağında bireyleri, kurumları ve demokratik süreçleri nasıl etkilediğini görünür kılmak ve bu etkilere karşı hak temelli, çok aktörlü bir müdahale modeli inşa etmektir. Urie Bronfenbrenner'in "Biyoekolojik Modeli"ni temel alarak kurguladığımız RESAID ile, sorunu sadece yalan haberlerin çürütülmesi olarak değil, bireyin ve toplumun dirençliliğinin güçlendirilmesi olarak ele aldık. Bu doğrultuda çevrim içi açık dersler (MOOC) de hazırladık. Konuların daha kolay anlaşılmasını sağlamak için kitabın her bölümünün girişine ilgili derslerimizi izleme önerisi olarak ekledik. Bu derslerin yanı sıra katılımcıların farkındalıklarını arttırmak için, süreçleri ve taktikleri farklı şapkalarla deneyimleyerek öğrenebilecekleri "InfoChief", "Catch and Match", "Fanus" ve "Sparkline" isimli dijital oyunlar geliştirdik.

2025 yılında konunun uzmanlarını ve ilgili akademisyenleri bir araya getiren akademik bir konferans düzenledik. Bu konferansta sunulan bildiriler hakikat-sonrası çağın felsefi tartışmalarından yapay zekâ destekli haber üretimine, 2023 seçimlerindeki siyasal infodemiden göçmen karşıtı yankı odalarına ve influencer ekonomisine kadar dijital dünyanın güncel meselelerini çok boyutlu çerçevede ele alan ve on iki makaleden oluşan bir kitaba dönüştü. Medya, sivil toplum, bürokrasi ve güvenlik sektörü temsilcileriyle bir araya geldiğimiz çalıştaylar organize ederek, bu alandaki profesyonellerin

doğru bilgiyi yayan değişim elçilerine dönüşmesini hedefledik. Ayrıca, İstanbul'da katılımcılarımızla bilgi düzensizlikleri ve mücadele yöntemleri üzerine birlikte çalıştığımız dört günlük RESAID Bahar Okulu'nda bir araya geldik. Sorunu karar alıcıların gündemine taşımak için küresel paydaşlara ulaşmayı hedefleyen Brüksel merkezli bir çalıştay planladık. Buna ek olarak, bilgi düzensizliklerinin yaratabileceği riskleri farklı boyutlarıyla analiz eden ve çözüm önerileri sunan İngilizce ve Türkçe politika belgeleri üreterek kanun yapıcılara yol gösterici somut kaynaklar sunmaya çalıştık. Sayfaları çevirdikçe proje kapsamında ürettiğimiz çevrim içi açık derse, dijital oyunlara, bildiri kitabına ve politika belgelerine sık sık referans verdiğimizi göreceksiniz.

RESAID ekosisteminin temel bir parçası olan bu kitabı planlarken hedef kitlemizi lise son sınıflar ve üniversite öğrencileri olarak belirledik. Gençlerin zihinsel ve akademik gelişimlerine katkı sunacak, temel bir kaynak olarak kullanabilecekleri bir ders kitabı tasarlamak istedik. Kitabın dilini ve yapısını kurgularken sadece akademik bir çerçevede kalmamaya özen gösterdik. İnternet kullanan, sosyal medyada vakit geçiren ve haber okuyan, yaşı veya mesleği ne olursa olsun herkesin kullanımına açık bir kaynak olarak tasarladık. Çünkü biliyoruz ki dijital dünyada doğruyu bulmak, hepimizi çok yakından ilgilendiren ortak bir ihtiyaç.

Kitabın birinci bölümünde, sorunun adını doğru koyarak işe başlamak istedik. Günlük hayatta sıkça kullandığımız "yalan haber" (*fake news*) kavramının aslında ne kadar yetersiz kaldığını; bu terimin bazen siyasetçiler veya güçlü figürler tarafından, kendilerini eleştiren gerçek haberleri itibarsızlaştırmak için kullanılmaya başladığını anlattık. Bu yüzden, meseleyi daha kapsayıcı bir çerçeveden ele alarak "bilgi düzensizlikleri" şemsiye kavramını kullanmayı tercih ettik. Bu bölümde okuyucuya bilgi düzensizliklerinin üç temel türünü tanıttık. Sorunun sadece basit bir teknoloji veya iletişim kazası

olmadığını vurgulamaya çalıştık. Amartya Sen'in "yapabilirlik yaklaşımı"nı ele alarak, yanlış bilginin insanların doğru karar verme, sağlıklı yaşama ve siyasi süreçlere katılma özgürlüklerini nasıl kısıtladığını, bunun aslında temel bir insan hakları ve güvenlik meselesi olduğunu okuyucuya sunmayı hedefledik.

İkinci bölümde ise insan zihnine ve psikolojisine odaklanarak, "Yanlış bilgilere neden bu kadar hızlı inanabiliyoruz?" sorusuna yanıt aradık. İnsan beyninin milyonlarca yıl önceki koşullarda hayatını kurtaran "hızlı karar verme" refleksinin bugünün karmaşık dijital dünyasında bizi nasıl savunmasız bıraktığını anlattık. Bu noktada Daniel Kahneman'ın sistem 1 ve sistem 2 modelini inceledik. Ayrıca bu bölümde "bilişsel önyargılarımızı" ele aldık. Sadece kendi görüşümüzü destekleyen bilgileri aradığımız "doğrulama yanlılığı"nı; bir konuyu az bilenlerin neden uzmanlardan daha özgüvenli konuştuğunu açıklayan "Dunning-Kruger etkisi"ni; yalanların sürekli tekrarlandığında zihnimizde nasıl doğruymuş gibi algılandığını gösteren "yanıltıcı doğruluk etkisi"ni inceledik. Bölümün sonunda ise sosyal medya platformlarının bizi ekranda daha uzun süre tutmak için dopamin döngülerimizi nasıl kullandığını, "sonsuz kaydırma" gibi tasarımlarla zihnimizi nasıl yorduğunu ve dikkat ekonomisinin çalışma mantığını ele aldık.

Üçüncü bölümde, meselenin toplumsal boyutunu tartıştık. İnternetin başlangıçta herkesi bir araya getirecek bir "küresel köy" olacağı hayal edilirken, nasıl bizi birbirinden kopuk dijital adalara böldüğü sorusuna yanıt aradık. "Yankı odaları" ve "filtre balonları" kavramlarını açıkladık. İnsanların toplumdan dışlanma korkusuyla fikirlerini söylemekten çekindiği "suskunluk sarmalı"nı ve benzer düşünen insanların bir araya geldiğinde fikirlerinin nasıl daha da radikalleştiğini açıklayan "grup kutuplaşması" yasasını ele aldık. Ayrıca bu bölümde siyasi ve toplumsal kutuplaşmanın geldiği noktayı değerlendirdik; okuyucunun toplumsal ayrışmanın kökenlerini daha net görmesini

hedefledik. Kutuplaşmanın artık sadece fikir ayrılığı olmadığını, karşı tarafı "düşman" olarak gören "duygusal kutuplaşma"ya dönüştüğünü anlattık.

Dördüncü bölümde ise teoriden pratiğe geçerek, karşımıza çıkan bilgilerin doğruluğundan nasıl emin olabileceğimizi adım adım aktarmaya çalıştık. Geleneksel "dikey okuma" yerine, profesyonel doğrulayıcıların tercihi olan "yanal okuma" tekniğini ve bu süreci sistemleştiren SIFT (Dur, Araştır, Bul, İzini Sür) metodolojisini detaylandırdık. Görsel ve video doğrulama araçlarından tersine arama yöntemlerine; deepfake ile cheapfake ayrımından yapay zekâ tespiti süreçlerine kadar birçok tekniği ele aldık. Ayrıca, silinen içeriklere ulaşmak için Wayback Machine'in kullanımı ve bot hesapları tespit etme stratejileriyle okuyucularımıza dijital dünyada nasıl iz sürebileceklerini anlatmak istedik.

Beşinci bölümde küresel bir güvenlik perspektifinden konuyu ele aldık. Karşımızdaki sorunun birkaç trolün yaydığı yalanlarla sınırlı olmadığını; devletlerin, istihbarat servislerinin ve organize ağların yürüttüğü büyük operasyonların da var olduğunu anlattık. Bu çerçevede FIMI (Yabancı Bilgi Manipülasyonu ve Müdahalesi) kavramını açıkladık. Bu bölümde, dışarıdan gelen kasıtlı ve zararlı bir bilginin, sanki yerel ve masum bir düşünceymiş gibi aracı aktörler kullanılarak nasıl temize çıkarıldığını, yani "bilgi aklama" süreçlerinin teknik işleyişini adım adım detaylandırmayı planladık. Yapay zekânın bu ekosistemdeki rolünü ele alırken, botların sadece metin üretmekle kalmayıp, güvenlik duvarlarını aşmak için bilerek yazım hataları yapan "gerçek bir insan" taklidi dahi yapabildiğini gösterdik. Son olarak, savaş alanının artık fiziksel topraklar veya bilgisayar ağları değil, doğrudan insan beyni olduğu gerçeğinden hareketle "bilişsel harp" ve zihnimizi hedef alan "nöro-savaş" kavramlarını tartıştık.

Altıncı bölümü, tüm bu karanlık tabloya karşı bireysel ve toplumsal

olarak nasıl bir savunma inşa edebileceğimizi anlatmak için kurguladık. Yanlış bilgi yayıldıktan sonra onu yalanlamanın (çürütme) her zaman işe yaramamasından hareketle, tıbbi aşılama mantığından ilham alan "psikolojik aşılama" ve "ön-çürütme" (p*rebunking*) stratejilerini merkeze aldık. İnsanlara henüz bir yalanla karşılaşmadan önce manipülasyon taktiklerinin nasıl çalıştığını küçük ve zararsız dozlarla göstererek onların zihinsel bağışıklık kazanmalarının önemini aktardık. İletişimi koparan "geri tepme etkisinden" kaçınmak için, yanlış bilgiyi tekrarlamayan "hakikat sandviçi" modelini ve karşı tarafı yargılamayan "empatik iletişim" stratejilerini pratik yöntemler olarak okuyucuya sunduk.

Yedinci ve son bölümde, sorunun sadece bireysel çabalarla aşılamayacak kadar büyük olduğunu, ancak sistemsel ve çok aktörlü bir yönetişimle mümkün olduğunu vurguladık. Şirketlerin kendi düzenlemelerinin yetersizliğini göstererek; devlet, teknoloji şirketleri ve sivil toplumun sorumluluk paylaştığı "eş-düzenleme" modelini sunduk. Avrupa Birliği'nin pazar gücünü kullanarak Dijital Hizmetler Yasası (DSA) ve Yapay Zekâ Yasası (*AI Act*) gibi düzenlemelerle küresel standartları belirleyen "Brüksel etkisi"ni detaylandırdık. Bölümü tamamlarken devletin düzenleyici rolü, platformların şeffaflık sorumluluğu, sivil toplumun denetleyici gücü ve biz bireylerin eleştirel tüketim alışkanlıklarını içeren "çok paydaşlı yönetişim modeli"ni ele aldık.

Bölümlere başlarken eklediğimiz tartışma soruları ile okuyucuyu konuya hazırlamayı amaçladık. Konuların daha iyi anlaşılması ve öğrenme sürecini pekiştirmek için kavram, görsel, izle, dinle, örnek ve dene kutularıyla okuyucunun öğrenme sürecine etkin katılımını hedefledik. Görsellerin tamamını yapay zekâ araçlarını kullanarak oluşturduk. Teknolojinin imkânlarını kullanarak, uzun ve teorik anlatımları görselleştirip daha anlaşılır bir yapıya kavuşturmayı hedefledik. Kısacası teknolojiyi sadece bir anlatım konusu olarak

değil, karmaşık süreçleri basitleştiren ve bilgiyi erişilebilir kılan bir araç olarak kullandık. Ek Kaynaklar kısmında ise, konunun daha da derinine inmek, akademik makalelere veya detaylı raporlara ulaşmak isteyen meraklı okuyucularımız için bir ek kaynak listesi önerdik. Her bölümün içindeki alt başlıklara, anlattığımız temel kavramları öğrenmeyi kolaylaştırmak ve bilgilerin kalıcı olmasını sağlamak için kısa testler ekledik.

Sonuç olarak, içinde olduğumuz dijital dünyada doğru bilgiye erişimi, günümüzde diğer tüm haklarımızın hayata geçebilmesi için temel bir insan hakkı olarak görüyoruz. Dijital dünyadaki bilgi düzensizliklerini yalnızca teknik bir iletişim sorunu değil; doğru bilgiye erişimimizi, özgür irademizi ve demokratik süreçlere katılımımızı doğrudan tehdit eden bir insan hakları meselesi olarak değerlendiriyoruz. Dezenformasyon ve manipülasyon teknikleri, toplumu kutuplaştırarak ortak bir gerçeklik zemini üzerinde buluşmamızı engelliyor. Ancak inanıyoruz ki bu gidişat bireylerden sivil topluma, devletlerden uluslararası kurumlara kadar tüm aktörlerin sorumluluk almasıyla dönüştürülebilir. Bu kitabın kutuplaşmanın yerini dayanışmaya bıraktığı, eleştirel düşüncenin hepimize rehberlik ettiği, daha şeffaf ve güvenli bir bilgi ekosistemi inşa etmeye katkı sunmasını umuyoruz.

İstanbul, 9 Mart 2026

Bölüm 1

Bilgi Ekosisteminde Temel Kavramlar

🎯 TARTIŞMA SORULARI

1. Bilgi düzensizlikleri nedir? Türleri nelerdir?
2. Mezenformasyon, dezenformasyon ve malenformasyon arasındaki farklar nelerdir?
3. Yapay zekâ çağında bilgi düzensizliklerine karşı dirençlilik geliştirmek için hangi beceriler gereklidir?
4. Bilgi düzensizlikleri temel hak ve özgürlüklerimizi ihlal edebilir mi?
5. Yapabilirlik yaklaşımı nedir? Bilgi düzensizlikleri yapabilirlikler açısından nasıl kısıtlar getirir?

Giriş

Bu bölüm, Herbert Simon'un 1970'lerde öngördüğü bilgi zenginliğinin dikkat yoksulluğu yarattığı argümanından yola çıkarak, modern çağın en büyük çelişkisi olan bilgi karmaşasını incelemektedir. Bilgiye ulaşmanın saniyeler sürdüğü ancak doğruyu bulmanın giderek zorlaştığı günümüzde, popüler "*fake news*" kavramının neden yetersiz kaldığı ve siyasetçiler tarafından eleştirileri bastırmak için nasıl bir araca dönüştürüldüğü tartışılacaktır. Yaklaşımımız sorunu sadece yanlış bir sosyal medya paylaşımı veya teknik bir iletişim kazası olarak görmenin ötesine geçmektedir. Bu bölümde bilgi düzensizlikleri bireyin özgür iradesini kısıtlayan bir insan hakları sorunu, bir insani güvenlik meselesi ve yapabilirlikleri kısıtlayan önemli bir sorun olarak ele alınmaktadır.

İZLE

RESAID tarafından hazırlanan açık erişim derslerin *Bilgi Düzensizliklerinin Temelleri* başlıklı bölümünü izleyerek temel kavramlar hakkında hazırlık yapabilirsiniz.

Giriş
https://youtu.be/GyppRFSO6_U
Yanlış Bilgi ve Bilgi Ekosistemi
https://youtu.be/B0hHxhw4OGw
Bilgi Düzensizliklerinin Etkileri
https://youtu.be/b96wE4W7kiA
Kriz Dönemlerindeki Etkisi
https://youtu.be/FBPrt8pL5Zc
Toplumsal Dirençliliğin Temelleri
https://youtu.be/NvnrcDU3hoM

21. Yüzyılın Bilgi Paradoksu

İnsanlık tarihinin büyük bir bölümünde bilgi sınırlıydı; üretmek zordu, aktarmak zaman alırdı ve çoğu zaman yalnızca belirli çevrelerin erişimine açıktı. Bugün ise bambaşka bir dönemin içindeyiz. 21. yüzyılın ilk çeyreğinde, her an üzerimize yağan devasa bir veri akışıyla, adeta kontrol edilmesi güç bir bilgi bolluğu ile karşı karşıyayız. Dijital teknolojilerin gelişmesiyle birlikte bilgiye erişim kanalları çoğaldı, işlem gücü hızla arttı ve bilgi artık neredeyse sınırsız hale geldi. İnternet, sosyal medya ve dijital platformlar sayesinde artık bilgiye erişim birkaç saniyelik bir mesele. Ancak bu dönüşüm, beklenmedik bir paradoksu da beraberinde getirdi: Bilgiye bu kadar kolay ulaşıyorken, doğru bilgiye ulaşmak neden bu kadar zor?

Bu çağın temel sorununu en net biçimde ortaya koyan tespitlerden biri, Nobel ödüllü iktisatçı Herbert Simon'a aittir. Simon, daha 1970'li yıllarda dikkat çekici bir öngörüde bulunur: *"Bilgi zenginliği, dikkat yoksulluğu yaratır."* Simon'a göre bir kaynak ne kadar bol hale gelirse gelsin, onu işleyebilecek insan dikkati ve zihinsel kapasite aynı hızla artmaz. Aksine, bilgi çoğaldıkça dikkat daha da kıymetli ve sınırlı bir hale gelir.[1]

Bu yapısal kriz, çağdaş felsefe, sosyoloji ve iletişim çalışmaları literatüründe sıklıkla "epistemik kaos" olarak adlandırılan bir süreci tetiklemiştir. Epistemoloji, yani bilginin doğası, kaynağı ve kapsamı ile ilgilenen felsefe dalı, bugün belki de tarihindeki en zor sorularla yüz yüzedir. Artık temel mesele, yalnızca "bilmek" (bilgiye erişmek) değil; aksine, her gün maruz kaldığımız sayısız ve çoğu zaman birbiriyle çelişen içerik arasından doğru olanı ayırt edebilmektir. Gerçek bilgi ile söylenti, anlamlı veri ile dikkat dağıtan gürültü iç içe geçmiştir. Bu karmaşa içinde bireyin en önemli ihtiyacı, gördüğüne ve

[1] Simon, H. A. (1971). Designing organizations for an information-rich world. M. Greenberger (Der.), *Computers, communications, and the public interest* içinde (ss. 37–72). The Johns Hopkins Press.

duyduğuna mesafe koyabilme becerisidir. Bu ayırt etme becerisi, basit bir teknik yeterlilikten çok daha fazlasını ifade eder. Bireyin kendi aklıyla düşünebilmesi, karar alabilmesi ve yönlendirilmeye karşı direnç gösterebilmesi için temel bir koşuldur. Başka bir deyişle, bilişsel otonomi, bilgi bolluğu çağında kendiliğinden var olmaz; ancak sorgulayan ve eleştiren bir bakışla mümkün hale gelir.

Bu epistemik kriz, modern söylemi şekillendiren ve hakikatle ilişkimizi tanımlayan bir dizi yeni kavramı beraberinde getirmiştir. Bu kavramlardan ilki, hakikat ötesi (*post-truth*) kavramıdır. Bu kavram, 2016 yılında Oxford Sözlüğü tarafından yılın kelimesi seçilerek yaygın biçimde kullanılmaya başlanmıştır. Bu kavram, gerçeklerin ve kanıta dayalı bilgilerin insanların düşüncelerini etkileme gücünün azaldığı bir durumu tanımlar. Bunun yerine duygular, kişisel inançlar ve önyargılar karar alma süreçlerinde daha belirleyici hale gelir. Bu ortamda yalan, artık her zaman ahlaki bir sorun olarak görülmez. Siyasi ya da ticari bir amaca hizmet ettiği sürece, işe yarayan bir araç olarak kabul edilebilir. Böylece asıl önemli olan, artık gerçeğin ne olduğu değil; insanların gerçeği nasıl algıladığı ve bu algının nasıl yönlendirildiğidir.

Bu algı yönetimini besleyen dinamiklerden biri ise FOMO (***F**ear **o**f **M**issing **O**ut*) başka bir deyişle "gelişmeleri kaçırma korkusu" dur. Dijital platformlar, bireye sürekli olarak bir şeyleri kaçırdığı hissini yaşatır. Son dakika haberleri, viral içerikler, trend olan paylaşımlar… Hepsi kullanıcıyı çevrim içi tutmak ve dikkatini platformda sabitlemek üzere tasarlanmıştır. FOMO, bireyin bilgiyi anlamak için değil, geri kalmamak için tüketmesine yol açar. Böylece bilgi, düşünmeye alan açan bir araç olmaktan çıkar; sürekli yetişilmesi gereken bir akışa dönüşür.

Özellikle Z kuşağı arasında yaygınlaşan ve dijital kültürü eleştirel bir biçimde tanımlamak için kullanılan argo bir ifade olan beyin çürümesi (*brain rot*) kavramı, dijital ortamlarda çok hızlı tüketilen; çoğu zaman yüzeysel,

manipülatif ve bilişsel değeri düşük içeriklerin zihinsel etkilerini anlatır. TikTok ya da Instagram Reels'ın bitmeyen kaydırma döngüsü (*doomscrolling*) gibi pratikler, bireyin dikkat süresini kısaltır ve derinlemesine düşünme becerisini zayıflatır. "Beyin çürümesi" sorunun yalnızca içeriklerin kalitesiyle sınırlı olmadığını da gösterir. Dijital medyanın hız, tekrar ve süreklilik üzerine kurulu yapısı, eleştirel düşünmeyi ve karmaşık problemler üzerine odaklanmayı giderek zorlaştırır. Sürekli yeni uyarana maruz kalan birey, anlık haz ve dopamin ödüllerine alıştıkça, uzun süreli dikkat gerektiren ve anlamlı bilgi işleme süreçlerinden uzaklaşma riskiyle karşı karşıya kalır.

Bu kavramlar yalnızca günümüz sorunlarını adlandırmakla kalmaz; aynı zamanda bilginin ne olduğu, nasıl dolaşıma girdiği ve nasıl algılandığı konusunda tarihte eşi benzeri görülmemiş bir değişim yaşandığını da gösterir. Epistemik kaos ortamında ise dijital okuryazarlık ve eleştirel düşünme becerileri, bireyin kendini koruyabilmesi için vazgeçilmez hale gelir. Bugün bu beceriler, yalnızca kişisel değil, aynı zamanda toplumsal düzeyde de sağlıklı düşünmenin en önemli dayanaklarından biridir.

Hakikatle kurduğumuz ilişki ve manipülasyon sorunu dijital çağa özgü değildir; araçlar değişse de temel dinamikler tarih boyunca benzer kalmıştır. Antik Çağ'da Eflatun'un mağarasındaki insanlar nasıl hakikati duvara yansıyan gölgeler üzerinden dolaylı deneyimlediyse, bugün de bizler ekranlar aracılığıyla gerçeğin kendisini değil, bize sunulan kurgulanmış versiyonlarını izlemekteyiz. Bu "aracılı" deneyim, 19. yüzyılda matbaanın ticarileşmesiyle ekonomik bir modele dönüşmüştür. 1835'te New York Sun gazetesinin tiraj artırmak için kurguladığı Büyük Ay Aldatmacası (*Great Moon Hoax*) bugünkü tık tuzağı (*clickbait*) mantığının tarihsel kökenidir. Tarih boyunca olduğu gibi bugün de dikkat, doğruluğun önünde gelen en kıt kaynaktır. Benzer bir mekanizma Soğuk Savaş döneminde siyasi bir silaha dönüşmüş; KGB'nin "Operation Denver" operasyonuyla AIDS'in ABD tarafından üretildiği yalanını

yayması, internetin olmadığı bir dünyada dahi yanlış bilginin devlet eliyle küresel ölçekte nasıl siyasallaştırılabileceğini kanıtlamıştır. Yanlış bilgi yeni değildir. Yeni olan, onun daha hızlı yayılması, daha görünmez hale gelmesi ve gündelik hayatın merkezine yerleşmiş olmasıdır.

Bu kitap, Avrupa Birliği tarafından desteklenen RESAID projesinin derinlemesine araştırmalarına ve elde edilen somut çıktılara dayanarak hazırlandı. Amacımız, günümüzde giderek daha görünür hale gelen bilgi düzensizliklerini, yanlış bilgi, dezenformasyon ve kasıtlı manipülasyon dahil, anlaşılır ve bütünlüklü bir çerçevede ele almaktır. Bu çalışmada bilgi düzensizliklerini yalnızca bir iletişim sorunu ya da teknolojinin kaçınılmaz bir sonucu olarak görmüyoruz. Aksine, bu olgunun bireylerin düşünme biçimlerinden toplumsal ilişkilerimize kadar uzanan derin ve gerçek etkileri olduğunu kabul ediyoruz. Yanlış bilginin yalnızca ne bildiğimizi değil, nasıl karar verdiğimizi ve dünyayı nasıl yorumladığımızı da şekillendirdiğini savunuyoruz. Bu nedenle kitap, bilgi düzensizliklerinin sadece bilgi ekosistemini değil; aynı zamanda insan onurunu, güvenliğini ve özgürlüğünü nasıl tehdit ettiğini görünür kılmayı amaçlar.

Bilgi düzensizlikleri, bireylerin doğru, güvenilir ve yeterli bilgiye erişim hakkının zedelenmesi demektir. Oysa bu hak, insanların bilinçli kararlar alabilmesi, kendi yaşamları üzerinde söz sahibi olabilmesi ve kamusal hayata eşit biçimde katılabilmesi için vazgeçilmezdir. Yanlış ya da kasıtlı olarak çarpıtılmış bilgiyle karşı karşıya kalan bireyler, yalnızca yanıltılmaz; aynı zamanda bilinçli seçim yapma imkânından da mahrum bırakılır. Bu durumun etkileri yalnızca bireysel düzeyle sınırlı değildir. Bilgi düzensizlikleri, demokratik süreçleri doğrudan zayıflatır; seçimlerden sağlık kararlarına, kamusal tartışmalardan toplumsal güvene kadar pek çok alanda ciddi tahribat yaratır. Doğru bilgiye erişemeyen bireylerin siyasi tercihler yapması, sağlıkla ilgili doğru kararlar alması ya da kamusal tartışmalara katılması giderek zorlaşır.

Böylece bilgi düzensizliği, demokrasinin işleyişini bozan ve temel hakların kullanımını engelleyen yapısal bir soruna dönüşür.

Bilgi düzensizlikleri, yalnızca devletleri ya da siyasal sistemleri ilgilendiren yüksek bir mesele değil; bireylerin günlük yaşamlarını, sağlıklarını ve güvenliklerini doğrudan etkileyen ciddi bir insan güvenliği sorunudur. Özellikle pandemi, doğal afet, iklim krizi, savaş ve göç gibi kriz dönemlerinde yayılan yanlış ve manipüle edilmiş bilgiler insanların hayati kararlar almasını doğrudan etkiler. Aşı karşıtlığına yol açan sağlık dezenformasyonu, bireylerin etkisiz ya da tehlikeli tedavi yöntemlerine yönelmesine neden olabilir. Afet anlarında yayılan asılsız söylentiler, güvenli alanlardan kaçışa, yardım çalışmalarının aksamasına ve panik ortamının derinleşmesine yol açabilir. Benzer biçimde, göç ve güvenlik konularında dolaşıma giren manipülatif içerikler, toplumsal gerilimi artırarak şiddet riskini besleyebilir.

Nobel ödüllü ekonomist Amartya Sen'in "yapabilirlikler yaklaşımı" (*capability approach*), bilgi düzensizliklerinin birey üzerindeki etkisini anlamak için güçlü bir çerçeve sunar.[2] Bu yaklaşıma göre insani gelişim, yalnızca sahip olunan kaynaklarla değil; bireylerin değer verdikleri şeyleri yapabilme ve olabilme özgürlüğüyle de ölçülür. Başka bir deyişle, önemli olan insanların neye sahip olduğu değil, bu imkânları kullanarak nasıl bir yaşam sürebildikleridir. Bilgi düzensizlikleri tam da bu noktada devreye girer. Sürekli yanlış, eksik ya da manipüle edilmiş bilgiye maruz kalan bireyler, özgür ve bilinçli kararlar almakta zorlanır. Ne hakkında rıza gösterdiklerini, hangi seçeneklerin gerçekten mümkün olduğunu ya da kendi çıkarlarına neyin hizmet ettiğini ayırt edemezler. Bu durum, bireyin potansiyelini gerçekleştirme, yaşam tercihleri yapma ve kendi hayatı üzerinde söz sahibi olma kapasitesini ciddi

[2] Sen, A. (1979). *Equality of what?* (C. 1); Sen, A. (1993). Capability of well-being. A. Sen ve M. Nussbaum (Der.), *The quality of life* içinde (s. 30–53). Oxford University Press. https://doi.org/10.1093/0198287976.003.0003

biçimde sınırlar. Bu nedenle bilgi düzensizlikleri bireysel özgürlükleri aşındıran ve toplumsal adaleti zedeleyen derin bir yapısal sorundur. Doğru bilgiye erişimin olmadığı bir ortamda, insanların "yapabilme" ve "olabilme" imkânları da giderek daralır.

Bilgi Düzensizliği Ne Anlama Gelir?

"Yalan, sahte haber" (*fake news*) terimi, ilk ortaya çıktığı dönemde medyanın güvenilirliğine dair meşru endişeleri yansıtsa da akademik, gazetecilik ve politika yapıcı çevrelerce iki temel ve kritik nedenle terk edilmiştir. İlk kullanımda odak, geleneksel "haber" formatındaki yanlış bilgilere yönelikti. Ancak günümüzde yanlış bilginin yayılma biçimleri sadece metin tabanlı makalelerle sınırlı kalmamıştır. İnternet mim'leri, bağlamından koparılmış ses kayıtları, *deepfake* ve *cheapfake* videolar gibi görsel ve işitsel manipülasyonlar, yanlış bilginin temel taşıyıcıları haline gelmiştir. Bu genişleyen alanı dar bir "haber" terimiyle tanımlamak, sorunun boyutunu ve çeşitliliğini göz ardı etmek anlamına gelmektedir.

Bu terim, özellikle siyasetçiler ve güçlü figürler tarafından, kendilerini eleştiren ve kamu yararını gözeten *doğru* ve *araştırmacı* gazetecilik ürünlerini ve eleştirel haberleri itibarsızlaştırmak için bir araç olarak kullanılmaya başlanmıştır. "Bu yalan haberdir" retoriği, kamuoyunun bilgi kaynağına olan güvenini sarsarak meşru denetim mekanizmalarını devre dışı bırakma amacı taşımaktadır. Bu saptırılmış kullanım, terimin nesnel analiz için uygunluğunu kaybetmesine neden olmuştur. Bu nedenlerle, sorunu daha kapsayıcı, nötr ve analitik bir çerçevede incelemek üzere "bilgi düzensizlikleri" (*information disorders*) şemsiye kavramına geçilmiştir.

Bilgi düzensizlikleri kavramı, yayılan içeriği iki ana eksende değerlendirir: Bilginin nesnel gerçeklikle uyumu, doğru mu? Yanlış mı? İkinci eksen ise şudur: Bilgiyi üreten veya yayan kişinin bu eylemi kasıtlı olarak siyasi,

finansal, kişisel zarar vermek amacıyla, hizmet etmek üzere yapıp yapmadığı. Bir başka deyişle "Kasıt var mı? Hata mı?" sorusuna verilen yanıt. Bu iki eksenin kesişimi, bilgi düzensizliğinin üç ana halini ortaya çıkarmaktadır. Bilgi düzensizlikleri, yanlış veya yanıltıcı bilginin niteliği ile bu bilginin yayılmasındaki niyet temelinde üç kategoriye ayrılır: Mezenformasyon, dezenformasyon ve malenformasyon.[3]

Mezenformasyon (Misinformation): Hataya Dayalı Yanlış Bilgi

Yanlış bilginin, kasıt olmaksızın, tamamen bir hataya veya yanlış anlamaya dayalı olarak üretilmesi, yeniden paylaşılması veya yayılmasıdır. Mezenformasyon yayan kişi, içeriğin yanlış olduğunu bilmez; aksine, içeriğin doğru olduğuna samimiyetle ve iyi niyetle inanır. Paylaşımda zarar verme, manipülasyon veya hile yapma kastı yoktur. Çoğunlukla panik, aşırı duygusallık veya altruistik dürtülerle, örneğin, "bir uyarı yapayım da başkası zarar görmesin" düşüncesiyle, hızlıca yayılır. 6 Şubat Depremleri gibi büyük afetler sırasında bir barajın patladığı iddiasının, sadece insanları uyarma ve olası can kaybını önleme iyi niyetiyle sosyal medyada hızla yayılması böylesi bir paylaşımdır. Niyet iyi olsa dahi, yayılan yanlış bilgi panik ve kaos yaratarak riske yol açar.

Dezenformasyon (Disinformation): Kasıtlı Manipülasyon

Yanlış bilginin, bilerek, isteyerek ve kanıtlanabilir bir zarar verme veya manipülasyon amacıyla üretilmesi, organize edilmesi ve yayılmasıdır. Bu, bir hatanın değil, belirli bir siyasi, finansal veya jeopolitik hedefi olan organize bir

[3] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe Publishing. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c; Wardle, C. (2020). *Understanding information disorders*. First Draft. https://firstdraftnews.org/long-form-article/understanding-information-disorder.

stratejinin ürünüdür. Hedef kitleyi aldatmak, siyasi süreçleri etkilemek, finansal piyasaları manipüle etmek veya bir kişiyi/kurumu itibarsızlaştırmak esastır. En etkili dezenformasyon kampanyaları, tamamen saf yalanlar üzerine kurulmaz. Aksine, içine %10-20 oranında "gerçek" kırıntıları, doğru bir fotoğraf, gerçek bir olay, doğru bir alıntı serpiştirilerek genel güvenilirlik duygusu sağlanır. Bu, genellikle gerçeğin bağlamından koparılması (*context manipulation*) yoluyla yapılır. Avrupa Birliği (AB) ve NATO raporlarına konu olan "Doppelgänger Operasyonu"; saygın uluslararası gazetelerin ve hükümet sitelerinin web sitelerinin birebir klonlanıp (*doppelgänger*) içlerine sahte haberler yerleştirilmesi ve bu sahte haberlerin bot hesaplar aracılığıyla yayılması bunlardan biridir.

Malenformasyon (Malinformation): Gerçeğin Silahlaşması

Bilgi düzensizlikleri literatüründe "gerçeğin silahlaştırılması" olarak tanımlanan malenformasyon (*malinformation*) gerçek bir e-posta, doğru bir adres veya yaşanmış bir olay gibi teknik olarak doğru olan verilerin bağlamından koparılarak, özel hayatın gizliliğini ihlal edecek veya muhatabına zarar verecek şekilde dolaşıma sokulmasıdır. Dezenformasyondan farklı olarak burada bilgi yalan değildir; ancak kullanım niyeti kötücül olup bilgi bir saldırı aracına dönüştürülmüştür. Genellikle itibar suikastları, kişisel intikamlar ve zorbalık kampanyalarında karşımıza çıkan bu türün en çarpıcı örnekleri arasında; özel ilişkilere ait görüntülerin rıza dışı yayılması ve siyasi figürleri itibarsızlaştırmak amacıyla geçmişe ait özel yazışmaların sızdırıldığı "gizli iletişim ifşaları" yer alır. Bu vakalarda materyal doğru olsa da eylemin arkasındaki temel motivasyon zarar vermektir.

Yeni Nesil Tehditler: FIMI ve Yapay Zekâ

FIMI (***F****oreign* ***I****nformation* ***M****anipulation and* ***I****nterference*-Yabancı Bilgi Manipülasyonu ve Müdahalesi), dezenformasyon ve bilgi düzensizliğine geleneksel "yanlış bilgi" odağından farklı olarak, doğrudan "ulusal güvenlik" ve sistemsel istikrar perspektifinden yaklaşan kapsamlı bir çerçevedir. FIMI, bir bilgi operasyonunun kaynağına ve kullanılan taktiklere odaklanarak, bilgi alanının yabancı aktörler tarafından bir savaş alanı olarak kullanılması durumunu inceler. FIMI'yi geleneksel dezenformasyondan ayıran temel iki farktan söz edebiliriz. Bunlardan biri aktör odaklılıktır. FIMI operasyonları, kesinlikle dış aktörler tarafından yürütülür. Bunlar, doğrudan yabancı devletler olabileceği gibi, bu devletlerin kontrolü veya desteği altındaki vekil gruplar, devlet destekli medya kuruluşları, siber ordular veya organize trol fabrikaları da olabilir. Amaç, hedef ülkenin iç dinamiklerini yabancı bir çıkar doğrultusunda etkilemektir. İkinci temel fark olan davranış odaklılıkta ise içeriğin mutlaka yalan olması gerekmez; operasyonun gücü, içeriğin niteliğinden ziyade hedef kitleye sunuluş biçimindeki manipülasyondan kaynaklanır. Bu süreçte odak nokta, "koordineli sahte davranış" gibi taktiklerdir; insanları taklit eden botlar ve troller aracılığıyla mesajların yayılım hızı yapay olarak artırılırken, koordineli ağlar belirli anlatıları kasıtlı olarak trendlere sokar. Sonuç olarak, tamamen doğru içerikler bile bu manipülatif yöntemlerle yapay bir görünürlük kazandırılarak toplumsal kutuplaşmayı derinleştirmek veya bir konuyu olduğundan çok daha önemli göstermek amacıyla araçsallaştırılabilir.

Üretken Yapay Zekâ (*Generative AI*) ve Dezenformasyonun Endüstrileşmesi

Bilgi manipülasyonu alanı, üretken yapay zekâ (*generative AI*) teknolojilerinin hızlı gelişimiyle radikal bir dönüşüm geçirmiştir. Bu durum, dezenformasyon operasyonlarının endüstrileşmesi anlamına gelmektedir. Yapay zekâ (YZ-*Artificial Intelligence-AI*) araçları (ChatGPT, Midjourney vb.) sayesinde, sahte içerik (metin, görsel, video-deepfake) üretme maliyeti sıfıra yaklaşmış, operasyonların hızı ve ölçeği ise katlanarak artmıştır. Özellikle video ve ses manipülasyonları (*deepfake*), sıradan bir kullanıcı için gerçeğinden ayırt edilemez hale gelmiştir. Bu, siyasi liderlerin sahte açıklamaları veya sahte kanıtlar üretmek için kullanılabilir. Üretken YZ, hedef kitlelerin diline, kültürüne ve hassasiyetlerine tam olarak uyan, kusursuz dilbilgisine sahip, yerelleştirilmiş manipülatif metinleri saniyeler içinde üretebilir. Bu, birebir kişiselleştirilmiş dezenformasyon kampanyalarının önünü açmaktadır.

🔍 **KAVRAM:** YAPAY ZEKA

Neyi açıklar?: İnsan zekasını gerektiren algılama, öğrenme, problem çözme ve karar verme gibi karmaşık görevleri gerçekleştirebilen akıllı sistemler ve makineleri ifade eder.

Neden önemli?: İnsan kapasitesini aşan veri işleme gücüyle, "bilmek" kavramını depolamaktan çıkarıp ve bilgiyi hızla erişme ve işleme yeteneğine dönüştürerek karar alma süreçlerini optimize eder.

Geleneksel botlar basit komutlarla çalışırken, yeni nesil YZ destekli botlar (*generative agents*) artık daha karmaşık ve insana yakın diyaloglar kurabilir, uzun vadeli sanal kimlikler oluşturabilir ve "koordineli sahte davranış" (*Coordinated Inauthentic Behavior*- CIB) operasyonlarının tespit edilmesini zorlaştıracak şekilde daha organik etkileşimler sergileyebilir. Yapay zekâ, dezenformasyonun maliyetini sıfıra indirmiştir. Bir yapay zekâ modeli saniyede binlerce farklı ve ikna edici yalan haber üreterek, bilgi düzensizliği üretimini "endüstrileşme" aşamasına taşımıştır. Bu gelişmeler, FIMI ile mücadelenin

sadece içerik denetiminden öte, teknolojik savunma, dijital okuryazarlık ve ulusal siber güvenlik stratejilerinin ayrılmaz bir parçası haline gelmesini zorunlu kılmaktadır.

Bilgi Ekosisteminin Anatomisi: Analiz Modelleri

Harvard Shorenstein Merkezi'nin dezenformasyon olaylarını bir "suç mahalli" titizliğiyle incelemek için geliştirdiği üçlü analiz modeli, sürecin ilk ve en kritik aşamasını "aktör" (*agent*) olarak tanımlar. Bu aşama, dezenformasyonun kaynağını ve onu harekete geçiren güdüleri, yani "kim ve neden?" sorularını merkeze alır. Analiz sürecinde, dezenformasyonu üreten, finanse eden veya yayan aktörler belirlenirken geniş bir yelpaze taranır: Ulusal çıkarlar veya jeopolitik hedefler doğrultusunda hareket eden istihbarat servisleri ve siber ordular gibi devlet aktörleri; borsa manipülasyonu veya haksız rekabet yoluyla ekonomik kazanç peşinde koşan finansal aktörler ve seçimleri etkilemek ya da toplumsal kutuplaşmayı derinleştirmek isteyen siyasi partiler veya aktivist gruplar gibi politik aktörler mercek altına alınır. Bu aktörlerin kimliğinin ötesinde, onları bu eyleme iten temel motivasyonun; parasal kazanç, siyasi nüfuz, ideolojik yayılma veya sadece kamuoyunu karıştırarak kriz anlarını manipüle etme isteğinin tespit edilmesi, dezenformasyonun yapısını çözmek için hayati önem taşır.

KAVRAM:
ÜRETKEN YAPAY ZEKA

Neyi açıklar?: Mevcut veriyi sadece sınıflandıran (bu kuş mu, köpek mi gibi) geleneksel modellerin aksine, öğrendiğin paternlerden yola çıkarak metin, görsel, ses veya kod gibi yeni içerikler yaratan teknolojidir.

Neden önemli?: Veriyi okumaktan üretme çağına geçişi temsil eder; içerik üretim süreçlerinde üretken yapay zekanın kullanılması bilgi düzensizlikleri açısından önemli bir kırılmayı beraberinde getirir.

Harvard Shorenstein Merkezi'nin analiz modelinin ikinci ayağı olan "mesaj" (*message*), dezenformasyonun yapısal özelliklerini, formatını ve alıcı üzerindeki psikolojik etkisini mercek altına alır. Bu

aşamada ilk dikkat çeken unsur "görsel üstünlük etkisi"dir; insan beyninin görselleri metne göre çok daha hızlı işlemesi ve akılda tutması nedeniyle, dezenformasyon genellikle bağlamından koparılmış veya sahte olarak üretilmiş çarpıcı görsel materyaller üzerinden kurgulanır. Ancak içeriğin asıl vurucu gücü, rasyonel düşünceden ziyade "duygusal kodlama"ya dayanmasında yatar. Mesajın yayılım hızını artıran bu stratejide; belirsizlik yaratarak paniği tetikleyen korku, haksızlık algısı üzerinden kutuplaşmayı körükleyen öfke ve hedef kitleyi "kirli" göstererek sosyal dışlanmayı meşrulaştıran tiksinme gibi güçlü duygular kullanılır. Sürecin inandırıcılığı ise Stephen Colbert'in literatüre kazandırdığı "hakikatimsi" (*truthiness*) kavramıyla pekişir; mesaj nesnel gerçeklere dayanmasa bile, alıcının mevcut önyargılarını ve inançlarını doğruladığı sürece kişiye sezgisel olarak "doğruymuş gibi" gelir ve kanıt aranmaksızın kabul görür.

Harvard Shorenstein Merkezi'nin[4] analiz modelinin son ve en kritik unsuru olan "yorumlayıcı" (*interpreter*), mesajı alan kişiyi ve mesajın algılanma biçimini merkeze alır; zira bir mesajın anlamı yayıldığı bağlamdan bağımsız düşünülemez. Bu süreçte mesajın anlamı, yayıcıdan ziyade alıcının zihninde ve duygusal durumunda şekillenir. Öyle ki alıcının stres, yalnızlık, bilgi arayışı veya güvensizlik gibi psikolojik durumları, inanç eşiğini düşürerek dezenformasyona karşı savunmasızlığını belirler. Bireysel psikolojinin ötesinde, alıcının içinde bulunduğu toplumsal, kültürel ve siyasi çevre de mesajı yorumlayan bir filtre işlevi görür. Bir mesaj, alıcının siyasi eğilimleri ve dini görüşleri gibi mevcut inanç sistemlerine ne kadar uyuyorsa o kadar doğru kabul edilirken; kutuplaşmış veya öfkeli toplumsal ruh haline hitap ettiği ölçüde de

[4] Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Shorenstein Center on Media, Politics and Public Policy. https://shorensteincenter.org/resource/information-disorder-framework-for-research-and-policymaking/

hızla benimsenip yayılır. Tüm bu süreci pekiştiren "eko odaları" ve "filtre baloncukları" ise, sosyal medya ağları ve kapalı gruplar aracılığıyla alıcının yalnızca kendi görüşlerini onaylayan bilgileri görmesini sağlayarak dezenformasyonun sorgulanmadan kabul edilmesini kolaylaştırır.

RESAID Modeli: Hak Temelli ve Çok Katmanlı Dirençlilik Modeli

RESAID projesi günümüzün en önemli toplumsal sorunlarından biri olan bilgi düzensizliklerini anlamlandırmak ve bu duruma karşı bireysel ve toplumsal direnci artırmak amacıyla geliştirilmiş bir çerçevedir. Projenin temel dayanağı, ünlü gelişim psikoloğu Urie Bronfenbrenner'in Biyoloekolojik Modeli'dir.[5] Bronfenbrenner'in modeli, bireyin gelişimini izole bir olay olarak değil, etkileşimli çevresel sistemler bütünü içinde ele alır. RESAID, bu sistemi bilgi düzensizliklerinin yayılımı ve birey üzerindeki etkisi bağlamına uyarlar. Bu uyarlama, bilgi düzensizliklerinin yalnızca içerikle ilgili bir sorun olmaktan ziyade, bireyin içinde bulunduğu sosyal, kültürel ve teknolojik çevreden köken alan karmaşık bir ekolojik sorun olduğunu gösterir. Birey, bu iç içe geçmiş sistemlerin merkezinde yer alır ve her bir sistem, bilgiye erişimini, yorumlama biçimini ve yanlış bilgiye karşı kırılganlığını farklı şekillerde etkiler.

Bireyin en yakın ve doğrudan etkileşimde bulunduğu çevre olan mikrosistem; bilgi düzensizlikleri bağlamında kişisel güvenin ve duygusal bağların en yoğun yaşandığı alandır. Aile üyeleri, yakın arkadaşlar, iş arkadaşları ve WhatsApp veya Telegram gibi kapalı grupların oluşturduğu bu yapıda, bilgi kaynağa duyulan samimiyet nedeniyle genellikle eleştirel bir süzgeçten

[5] Bronfenbrenner, U. (2005). *Making human beings human: Bioecological perspectives on human development*. Sage; Bronfenbrenner, U., & Morris, P. A. (2006). The bioecological model of human development. R. M. Lerner & W. Damon (Der.), *Handbook of child psychology: Theoretical models of human development* içinde (Cilt 1). Wiley. https://doi.org/10.1002/9780470147658.chpsy0114

geçirilmeden kabul edilme eğilimindedir. Bilimsel otoritelerin yerini "güvendiğim bir dostum gönderdi" veya "dayımın oğlu söyledi" gibi referansların aldığı bu ortam, işleyen "güven transferi" mekanizması sayesinde dezenformasyonun hem en hızlı hem de duygusal etkisi en yüksek şekilde yayıldığı zemini yaratır. Bu alanda yayılan yanlış bilgiler genellikle bireyin dünya görüşü ve kimliğiyle örtüştüğü için, bunlara direnç göstermek dış kaynaklı bilgilere kıyasla çok daha zordur.

Bireyin farklı mikrosistemleri arasındaki etkileşim ve bağlantı noktalarını ifade eden mezosistem, farklı kaynaklardan gelen çelişkili bilgilerin bireyde bilişsel çelişki (*cognitive dissonance*) yarattığı kritik bir alandır. Okuldaki eleştirel düşünce eğitimi ile evdeki geleneksel inançlar veya işyeri ile sosyal çevre arasındaki zıt bilgi akışları bu sistemin temel bileşenlerini oluşturur. Bilgi düzensizlikleri bağlamında mezosistem, bireyin doğrulama (*fact-checking*) becerileri ile duygusal bağlılıkları arasında yaşanan bir mücadele sahasıdır. Örneğin, okulda bilimsel yöntem ve sorgulamayı öğrenen bir bireyin, evde ailedeki yetişkinlerden veya güvenilir bir arkadaşından duyduğu komplo teorileriyle karşılaşması tipik bir mezosistem çatışmasıdır. Bu noktada birey, bilimsel/eğitimsel otorite ile duygusal/ailevi otorite arasında bir seçim yapmak zorunda kalır; bu kritik karar süreci ise çoğunlukla bireyin "ait olma ihtiyacı" ve kimlik motivasyonları tarafından şekillendirilir.

Ekzosistem bireyin doğrudan içinde bulunmadığı ancak gelişimini ve bilgiye maruz kalışını dolaylı olarak etkileyen teknolojik altyapı ve pazar dinamiklerini kapsayan dış çevresel faktörlerdir. Sosyal medya şirketlerinin algoritmaları, içerik denetleme politikaları, medya sahiplik yapıları ve reklam odaklı "dikkat ekonomisi" bu sistemin temel bileşenlerini oluşturur. Bu yapıda algoritmalar bireyle doğrudan etkileşime girmese de hangi bilginin, doğru veya yanlış, ona ulaşacağını belirleyen ana faktördür. Sistemin temel amacı kullanıcıyı platformda tutmak olduğu için genellikle duygusal,

kutuplaştırıcı ve dezenformasyon içeren içerikler, daha doğru ancak "yavan" içeriklere kıyasla daha fazla görünürlük kazanır. Bu durum, bireylerin "filtre balonları" (*filter bubbles*) ve "yankı odaları" (*echo chambers*) içine hapsolmasına yol açarak yanlış bilgiye maruz kalma olasılığını artırır ve farklı görüşlere karşı toleransı zayıflatır.

Bireyin çevresel katmanlarının en geniş halkasını oluşturan makrosistem toplumun temel kültürel değerlerini, ideolojik yapılarını, yasal çerçevelerini ve tarihsel travmalarını kapsayan genel atmosferdir. Toplumsal kutuplaşma seviyesi, otoriteye bakış açısı ve medya okuryazarlığı politikaları gibi bileşenlerin belirleyici olduğu bu katmanda, bilgi düzensizlikleri genellikle "güdülenmiş muhakeme" (*motivated reasoning*) mekanizmasıyla derinleşir. Bu bilişsel önyargı nedeniyle bireyler, nesnel gerçeği aramak yerine kendi siyasi veya kültürel kimliklerini destekleyen bilgileri kabul etme eğilimi gösterirler. Kutuplaşmanın yüksek olduğu makrosistemlerde kitleler, hakikatin kendisine değil, kendi gruplarının kurguladığı "gerçeğe" inanmaya motive edilirken; şeffaf olmayan siyaset ve medyaya güvensizlik gibi yapısal sorunlar, dezenformasyonun mevcut toplumsal fay hatlarını kullanarak hızla yayılmasına zemin hazırlar.

Geleneksel güvenlik anlayışı genellikle devletlerin sınırlarını ve egemenliğini korumaya odaklanırken, insani güvenlik kavramı odağı bireye kaydırarak, kişinin günlük hayatındaki emniyetini ve esenliğini temel alır. Bu yaklaşım, sadece fiziksel şiddet tehditlerini değil, aynı zamanda bireyin yaşam kalitesini ve potansiyelini tehdit eden tüm unsurları güvenlik kapsamına dahil eder.

Bilgi düzensizlikleri bu modern güvenlik anlayışı için ciddi bir tehdit oluşturmaktadır. Örneğin, aşı karşıtı yalanlar ve komplo teorileri halk sağlığını tehlikeye atarak bireyin sağlık güvenliğini doğrudan tehdit eder. Benzer şekilde, seçimler öncesinde veya sırasında yayılan manipüle edilmiş veya

asılsız siyasi bilgiler, demokratik süreçlere olan güveni aşındırarak ve bireylerin bilinçli oy kullanma hakkını sekteye uğratarak siyasi güvenliğini riske atar. Bu durum, bireyin temel yaşam alanlarında güvensizlik ve belirsizlik yaratır.

Bilgi düzensizliğinin birey üzerindeki etkilerini anlamlandırmada, Nobel ödüllü iktisatçı ve filozof Amartya Sen'in geliştirdiği yapabilirlik yaklaşımı (*capability approach*) kritik bir çerçeve sunar.[6] Sen'e göre, bir toplumun veya bireyin refah düzeyi, sadece sahip olduğu ekonomik kaynaklarla değil, bireyin fiilen sahip olduğu gerçek özgürlüklerle, "yapabilirlikleriyle" (*capabilities*) ölçülür. Yapabilirlikler, bireyin değerli bulduğu işlevleri (*functionings*) yerine getirme özgürlüğünü ifade eder; örneğin, sağlıklı olma, eğitim alma, siyasi sürece katılma veya bilinçli tercihler yapabilme gibi.

🔍 **KAVRAM:** FİLTRE BALONU

Neyi açıklar?: Sosyal medyada sürekli benzer görüşleri, aynı tür haberleri ve "zaten katıldığın" içerikleri mi görüyorsunuz? Filtre balonu, bireylerin sahip oldukları ideolojilerine ve arama geçmişlerine dayanarak benzer fikirde oldukları içeriklerle karşılaşmasını sağlayarak, onlardan olmayan içeriklerden izole olmasını sağlayan durumdur.

Neden önemli?: Filtre balonu, kişinin dünyayı tek bir pencereden görmesine yol açar. Bu da kutuplaşmayı, doğrulama yanlılığını ve dezenformasyona açıklığı artırır.

Bilgi düzensizliği, tam olarak bu yapabilirlikleri hedef alır. Manipülatif içeriklere maruz kalan bireyin, gerçek ile yalanı ayırt etme ve bu bilgi zemininde özgür ve bilinçli karar verme kapasitesi sakatlanır. Bireyin kendi hayatıyla ilgili rasyonel ve özerk tercihler yapma gücü zayıflar. Dolayısıyla, bilgi düzensizliğiyle mücadele, salt bir bilgi doğrulama çabası olmanın ötesinde, bireyin temel rasyonel özgürlüklerinin korunması ve yeniden tesisi için

[6] Sen, A. (1980). Equality of what? S. M. McMurrin (Der.), *The Tanner lectures on human values* içinde (Cilt 1, ss. 195–220). University of Utah Press; Sen, A. (1993). Capability and well-being. M. Nussbaum & A. Sen (Der.), *The quality of life* içinde (ss. 30–53). Oxford University Press. https://doi.org/10.1093/0198287976.003.0003

yürütülen bir özgürlük mücadelesi olarak görülmelidir. Bu mücadele, bireyin tam potansiyelini gerçekleştirmesi için gerekli olan bilişsel özerkliği ve yapabilirlikleri savunur.

Sonuç: Dijital Bağışıklık

Yapılan analizler, bilgi düzensizliği meselesinin teknik bir sorundan çok daha öte, derin insani ve etik boyutları olan bir güvenlik ve özgürlük krizi olduğunu ortaya koymaktadır. Klasik güvenlik tanımlarını aşan bu durum, bireyin sağlık güvenliği ve siyasi güvenliği gibi temel insani güvenlik alanlarını doğrudan hedef alarak güvenlik kavramının genişlemesine neden olmaktadır. Amartya Sen'in yapabilirlik yaklaşımı açısından bakıldığında ise yanlış bilgi, bireyin yapabilirliklerini ve özgür iradesini baltalayarak refahın temelini sarsan doğrudan bir özgürlük tehdidine dönüşür. Bu çok boyutlu tehdide karşı koyabilmek için bireylerin yalnızca teknik araçlarla değil, aynı zamanda eleştirel düşünme, şüphecilik ve doğrulama becerileriyle donatılması elzemdir. Bu gereklilik, eğitim sistemleri ve sivil toplumun öncelikli görevi olarak, bireyleri manipülasyona karşı dirençli kılacak bir "dijital bağışıklık" sisteminin inşa edilmesini zorunlu kılar.

Yukarıdaki kapsamlı analizler ve çıkarımlar, bilgi düzensizlikleri meselesinin, geleneksel güvenlik ve siyaset bilimi paradigmalarının ötesine geçen, çok katmanlı ve köklü bir sorun olduğunu açıkça göstermektedir. Bu mesele, salt teknolojik veya algoritmik bir sapma olarak ele alınmaktan ziyade, derin insani, etik, sosyo-ekonomik ve siyasal boyutları olan bir kriz olarak nitelendirilmelidir. Bu krizin yol açtığı kritik çıkarımlar, yeni bir güvenlik ve özgürlük anlayışının temelini atmaktadır.

Bilgi düzensizlikleri; devletler arası çatışmalar veya siber saldırılar gibi klasik güvenlik tehditleri bağlamının yanı sıra, doğrudan bireyin ve toplumun

esenliğini hedef alan bir tehdit olarak konumlanmaktadır. Bu tehdit, özellikle iki kritik alanda yoğunlaşmaktadır: Bunlardan biri sağlık güvenliği ve refahı alanındaki tehdittir. Yanlış veya manipülatif sağlık bilgileri, aşı tereddüdünden kanıtlanmamış tedavi yöntemlerine yönelmeye kadar bir dizi riski tetikleyerek halk sağlığı çabalarını baltalamaktadır. Bireylerin bilimsel kanıtlara dayalı kararlar alma yeteneği aşındırılmakta, bu durum salgın yönetimi gibi kritik süreçlerde toplumsal riskleri katlamaktadır. Bu bağlamda bilgi düzensizlikleri, modern bir biyolojik güvenlik tehdidi olarak da okunabilir.

İkinci alan ise siyasi güvenlik ve demokratik süreçlerdir. Kasıtlı dezenformasyon kampanyaları, seçim süreçlerinin meşruiyetini hedef almakta, toplumsal kutuplaşmayı derinleştirmekte ve kurumlara olan güveni sistematik olarak aşındırmaktadır. Yanlış bilgi, bireylerin rasyonel ve bilgilendirilmiş siyasi tercihler yapmasını engelleyerek, demokrasinin temel taşı olan katılımcı vatandaşlığı zehirlemektedir. Bu, bir ulus-devletin iç bütünlüğüne ve siyasi istikrarına yönelik doğrudan bir tehdittir.

Yapabilirlik yaklaşımı çerçevesinden bakıldığında bilgi düzensizlikleri sadece ifade özgürlüğünü değil, özgürlüğün daha derin bir katmanını, bireyin tam potansiyeline ulaşma ve kendi hayatı hakkında anlamlı tercihler yapma yeteneğini, baltalamaktadır. Yanlış bilgi, bireyin gerçeği doğru bir şekilde algılama ve bu algıya dayanarak bilinçli kararlar alma yeteneğini felce uğratır. Eğer birey, aldığı bilgilerin güvenilirliği konusunda sürekli şüphe içindeyse veya kasıtlı olarak yanıltılıyorsa, Sen'in tanımladığı yapabilirlikler (örneğin, sağlıklı olma, siyasi süreçlere etkin katılma, eğitim alma yapabilirliği) ciddi ölçüde kısıtlanır. Bu durum, bireyin otonomisini ve özgür iradesini dolaylı yoldan gasp etmek anlamına gelir. Bireyin refahının temel dayanağı olan "eyleme geçme özgürlüğü" (*freedom to act*) ortadan kalkar. Sürekli bir bilgi kirliliği ortamında yaşamak, bireyin gerçeği bilme hakkını ihlal eder ve

manipülasyona açık hale gelmesine yol açar. Bu, etik bir boyut taşıyarak, bireyin rasyonel bir varlık olarak sahip olduğu onuru zedelemektedir.

Bu karmaşık ve yaygın tehdit karşısında verilecek yanıt, sadece platform düzenlemeleri veya içerik kaldırma gibi teknik çözümlerle sınırlı kalamaz. Kalıcı ve sürdürülebilir bir çözüm, toplumun bizzat kendisinin bilgi manipülasyonuna karşı içsel bir direnç geliştirmesini gerektirmektedir. Bu direnç, bir tür dijital bağışıklık sistemi olarak kavramsallaştırılabilir. Tıpkı biyolojik bir bağışıklık sisteminin zararlı patojenlere karşı vücudu koruması gibi, dijital bağışıklık da bireyleri bilgi manipülatörlerinin taktiklerine karşı korur. Bu pasif bir savunma değil, aktif bir bilişsel süreçtir. Bu bağışıklığın temel bileşenlerinden biri eleştirel düşünme becerisidir. Bireyin bir bilginin kaynağını, amacını ve arkasındaki çıkarı sorgulama yeteneğini ifade eder. İkincisi şüphecilik ve doğrulama alışkanlığıdır. Özellikle duygusal tepki uyandıran veya şaşırtıcı içeriklere karşı anında inanmak yerine, bilgi kaynaklarını çapraz doğrulama (*cross-referencing*) becerisini kapsar. Son olarak ise medya okuryazarlığı ve dijital vatandaşlık eğitiminden bahsedilebilir. Bireylerin algoritmaların işleyişini, trol çiftliklerinin ve bot hesapların taktiklerini anlamasını sağlamayı kapsar.

Bu bağışıklık sisteminin inşası, sadece bireylerin kişisel çabası olamaz. Hem örgün eğitim sistemlerinin müfredatına entegre edilmeli hem de sivil toplum kuruluşları, medya kuruluşları ve teknoloji platformları tarafından sürekli desteklenmelidir. Bu, çağımızda etik bir zorunluluk ve toplumsal bir önceliktir. Bilgi düzensizliklerine karşı mücadele, 21. yüzyılın en temel insani kalkınma ve güvenlik mücadelesidir.

TEMEL ÇIKARIMLAR

Bu bölümde günümüz bilgi ekosisteminin paradoksu olan "bilgi bolluğu ve dikkat kıtlığı" ilişkisinden yola çıkılarak bilgi düzensizliklerinin anatomisi, işleyiş mekanizmaları ve birey üzerindeki güvenlik/özgürlük tehditleri ele alınmıştır.

Temel Kavramlar ve Mekanizmalar

Bilgi Düzensizlikleri: Wardle ve Derakhshan, "yalan haber" teriminin yetersiz kalması ve siyasallaşması nedeniyle, bilgi ekosistemindeki sorunları "doğruluk" ve "zarar verme niyeti" eksenlerinde inceleyen "bilgi düzensizlikleri" kavramını geliştirmiştir. Bu model, düzensizliklerini niyet ve olgusal duruma göre mezenformasyon, dezenformasyon ve malenformasyon olarak üç temel kategoriye ayırır.

Mezenformasyon (*Misinformation*): Kasıt olmadan, hataya dayalı yayılan yanlış bilgi (Örn: Depremde iyi niyetle yayılan yanlış ihbarlar).

Dezenformasyon (*Disinformation*): Zarar verme veya manipülasyon kastıyla, bilinçli üretilen yanlış bilgi (Örn: Seçim manipülasyonu).

Malenformasyon (*Malinformation*): Doğru bilginin (gerçek belge, görüntü) bağlamından koparılarak zarar verme amacıyla kullanılması (Örn. Gizli bilgilerin ifşası).

Biyoekolojik Model: Bronfenbrenner'in teorisine dayanan ve RESAID projesiyle bilgi düzensizliklerine uyarlanan model, bireyi birbirini etkileyen iç içe geçmiş çevresel sistemlerin (aile, okul, teknoloji, kültür) merkezinde konumlandırır. Model, kişinin yanlış bilgiye karşı direncini veya kırılganlığını izole bir durum olarak değil, bu sosyal ve teknolojik katmanların karmaşık etkileşiminin bir sonucu olarak açıklar.

1.1. KENDİNİZİ TEST EDİN

Soru 1: Bir gazetecinin özel hayatına dair gerçek fotoğrafların, onu susturmak amacıyla bağlamından koparılarak sosyal medyada yayılması hangi kategoriye girer?

A) Dezenformasyon

B) Mezenformasyon

C) Malenformasyon

D) Parodi

Soru 2: Büyük bir doğal afet sırasında, sosyal medyada dolaşıma giren ve aslında 10 yıl önceki başka bir olaya ait olan bir fotoğrafın, kullanıcılar tarafından güncel olduğu sanılarak ve insanları uyarmak amacıyla iyi niyetle paylaşılması hangi bilgi düzensizliği türüne girer?

A) Dezenformasyon

B) FIMI

C) Mezenformasyon

D) Malenformasyon

Soru 3: Harvard modeline göre, bir dezenformasyonun başarısı ve etkisi en çok neye bağlıdır?

A) Mesajı yayan aktörün harcadığı paraya

B) Aktör, mesaj ve yorumlayıcı arasındaki karmaşık etkileşime

C) Mesajın görsel kalitesinin yüksekliğine

D) Kullanılan teknolojik altyapının hızına

1.1. MERAKLISINA EK KAYNAKLAR

Balkan, E., & Ülgen, S. (2023). Yanlış bilgilendirme, malinformasyon ve *dezenformasyon üzerine bir rehber*. EDAM (Ekonomi ve Dış Politika Araştırmalar Merkezi).

Erdoğan, E., Uyan-Semerci, P., Eyolcu Kafalı, B., & Çaytaş, Ş. (2022). İnfodemi ve Bilgi Düzensizlikleri Kavramlar, Nedenler ve Çözümler. İstanbul Bilgi Üniversitesi Yayınları.

Hameleers, M., Powell, T. E., Van Der Meer, T. G., & Bos, L. (2020). A picture paints a thousand lies? The effects of visual modalities in disinformation. *New Media & Society*, *22*(10), 1895–1912.

Koçer, S. (2022). Bir insan ve toplum problemi olarak yanlış bilgi. *Reflektif Journal of Social Sciences*, *3*(2), 333–339. https://doi.org/10.47613/reflektif.2022.73

Koçer, S. (2025). *Hakikat sonrası çağda enformasyon düzensizliği, güven ve yılmazlık: Antropolojik bir bakış açısı* (Politika Belgesi No 3). RESAID.

Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

United Nations Development Programme. (2025). *Human development report 2025*.

Bölüm 2

Yanlış Bilginin Psikolojisi

🎯 TARTIŞMA SORULARI

1. İnsan zihni dijital dünyada neden kolay yanılır?
2. Yanlış bir bilgiye inanmayı bırakmak neden zordur?
3. Yankı odaları farklı görüşleri görmemizi nasıl sınırlar?
4. Sosyal medya platformları dikkatimizi nasıl kullanır?
5. Algoritmalar neden öfke ve korku içeren içerikleri öne çıkarır?

Giriş

Bu bölüm, yanlış bilginin neden ve nasıl bu kadar etkili olabildiğini anlamak için insan zihninin işleyişine odaklanmaktadır. İlk olarak, zihnin neden kolay yanıldığını ele alarak beynin hızlı karar alma eğilimlerini, duyguların düşünme süreçlerindeki rolünü ve bizi yanılgılara açık hâle getiren bilişsel kısa yolları inceler. Ardından, yanlış olduğu fark edilse bile bazı inançlardan neden vazgeçmekte zorlandığımızı tartışır; doğrulama yanlılığı, aidiyet duygusu ve sezgisel düşünmenin bu dirençteki payını ortaya koyar. Son olarak bölüm, dijital platformların bu zihinsel eğilimleri nasıl sistemli biçimde kullandığını ele alır; yankı odaları, dikkat ekonomisi ve algoritmaların yanlış bilginin yayılımını ve kalıcılığını nasıl güçlendirdiğini analiz eder. Bu bağlamda bu bölümün amacı, okurun neden yanıldığını fark etmesinin yanı sıra, dijital çağda yanlış bilgiye karşı dirençlilik geliştirebilmesi için gerekli temel kavrayışı edinmesine katkı sunmaktır.

🎬 İZLE

RESAID tarafından hazırlanan açık erişim dersler yanlış bilgilere neden inandığımızı ve bu bilgilerin nasıl bir etkileşime yol açtığını açıklar. Aşağıda yer alan videoları izlemeniz konuyu daha kolay anlamanıza yardımcı olacaktır.

Giriş
🔗 https://youtu.be/VNe0kg-UP9E
Yanlış Bilgiye İnanmanın Psikolojik Nedenleri
🔗 https://youtu.be/hsX7B4kAqo4
Komplo Teorileri ve Toplumsal Etkileri
🔗 https://youtu.be/en98AXpZD34
Sosyal ve Bilişsel Faktörler
🔗 https://youtu.be/IKHcsBEozp8

Neden Kolay Yanılırız?

Siber güvenlik uzmanları bir sistemi korumaya çalışırken işe yüzeyden başlamaz. Güvenlik duvarları ya da antivirüs programları ilk bakışta işe yarar gibi görünse de deneyimli bir saldırgan için bunlar kolayca aşılabilecek engellerdir. Asıl önemli olan, savunmayı en temelden kurmaktır: Sistemin nasıl çalıştığını, verinin nasıl aktığını ve işletim sisteminin çekirdeğinde hangi doğal zayıflıkların bulunabileceğini anlamak. Yazılım dünyasında, sistemin kendi yapısından kaynaklanan ve çoğu zaman fark edilmeden var olan bu tür açıklar sıfır gün (*zero-day)* güvenlik açığı olarak adlandırılır. Bu açıklar, sonradan eklenen bir hatadan değil; bizzat sistemin tasarımından doğar. Üstelik çoğu zaman, yıkıcı sonuçlar ortaya çıkana kadar kimse bu açığın varlığının farkına bile varmaz. Benzer bir durum, dezenformasyon ve manipülasyonla mücadele ederken de karşımıza çıkar. Eğer zihnimizi yanlış bilgiye, algı yönetimine ve bilişsel saldırılara karşı korumak istiyorsak önce kendi işletim sistemimizi anlamamız gerekir. Özetle; insan beyninin nasıl çalıştığını, hangi biyolojik ve evrimsel eğilimlerle karar verdiğini ve nerelerde doğal olarak savunmasız olduğunu anlamak ilk adımdır.

Modern insanlık, özellikle Aydınlanma Çağı'ndan ve 20. yüzyılın başlarındaki iktisadi teorilerden bu yana, kendisini büyük bir gururla rasyonel, mantıklı, tamamen veri odaklı ve faydacı bir aktör (*homo economicus*) olarak tanımlamayı benimsemiştir. Toplumsal söylemimizde; kararlarımızı soğukkanlı analizlerle aldığımıza, karşımıza çıkan bir haberi okurken onu eleştirel bir gerçeklik süzgecinden geçirdiğimize ve inançlarımızı sadece somut kanıtlara dayandırdığımıza inanmak isteriz. Eğer yeterince akıllı ve bilgiliysek, dezenformasyon bizi etkilemez gibi hissederiz. Yanlış bilgi sorununun başkalarının sorunu olduğuna inanmak isteriz. Ancak, son kırk yılda bilişsel bilim, nörobilim, davranışsal iktisat ve evrimsel psikoloji alanında yapılan devrim

niteliğindeki çalışmalar, bu rasyonel insan mitini temelden sarsmış, hatta tamamen yerle bir etmiştir. Daniel Kahneman, Amos Tversky ve Richard Thaler gibi öncülerin çalışmaları; beynimizin karar verirken çoğu zaman hızlı ve pratik yollar kullandığını, bu kısayolların çoğu zaman işe yarasa da yanlış ve yanıltıcı sonuçlara ulaşmamıza da neden olabildiğini ortaya koymuştur.

Bilimin ortaya koyduğu kabul etmesi zor ama aynı zamanda özgürleştirici bir gerçek var: İnsan beyni, 21. yüzyılın yoğun ve karmaşık bilgi akışını sürekli analiz etmek, sosyal medyadaki bilgi kirliliğini ayıklamak ya da algoritmaların oluşturduğu yankı odalarından çıkmak için her zaman yeterli değildir. Beynimiz, yaklaşık 3,5 milyon yıllık biyolojik bir geçmişin izlerini taşır. Modern dünyanın karmaşık sorunları ortaya çıkmadan çok önce, mağara yaşamı gibi zorlu koşullarda hayatta kalmaya odaklı bir şekilde işlemeye alışmıştır. Bu dönemde önemli olan, uzun uzun düşünmek değil; tehlikeyi hızlı fark etmek ve hızlı tepki vermektir. Bu nedenle beynin temel öncelikleri oldukça nettir: Hayatta kalmak, riskten kaçınmak ve mümkün olduğunca az enerji harcamak. Beyin, özellikle kritik anlarda, ayrıntılı analizler yerine hızlı ve pratik kararları tercih eder. Bu yaklaşım, geçmişte yaşamı sürdürmek için gerekliydi ve bugün de beynin bilgiyle kurduğu ilişkiyi büyük ölçüde şekillendirir. Bu açıdan bakıldığında, gerçeği aramak çoğu zaman soyut ve zahmetli bir uğraştır; hayatta kalmak ise acil ve somut bir ihtiyaçtır. Bu iki eğilim karşı karşıya geldiğinde, beynimiz genellikle güvenli olanı tercih eder. Örneğin, bir inanç bizi bir topluluğun parçası yapıyor ve kendimizi güvende hissetmemizi sağlıyorsa, bu inancın yanlış olduğunu gösteren mantıklı kanıtları çok da umursamayabiliriz. Çünkü dışlanmak ya da yalnız kalmak, beyin için ciddi bir risk olarak algılanır. Bu nedenle insanlar bazen açık kanıtlara rağmen inançlarını savunur. Bu durum her zaman mantıksızlıkla ilgili değildir; çoğu zaman beynin daha az enerji harcayan ve riski azaltan yolu seçmesiyle ilgilidir.

🎧 DİNLE

Adam Grant: *"... Ve bir noktadan sonra, fikirleri kimliklerinin bir parçası hâline geliyor. Bilim insanlarının bile bununla zorlandığını biliyorum… Peki, fikirlerinin kimliğinin bir parçasına dönüşmesini nasıl engelliyorsun?"*

Daniel Kahneman: *"Bence… Bu kulağa kötü gelebilir ama ben fikirlerin kıt olduğunu hiç düşünmedim. Eğer o fikir iyi değilse, onun yerine daha iyisi gelir. Bu yüzden bir fikri bırakmak, birçok insanda bir tür panik yaratabiliyor: 'O fikrim yoksa elimde ne kalır? O fikrim yoksa ben kimim?' Bu nedenle fikirlerle daha az özdeşleşmek, çok sayıda fikre sahip olmakla da bağlantılı: çoğunun iyi olmadığını görüp iyi olan birkaçını seçmeye çalışmakla."*

🔗 Podcast'in tamamını dinlemek için:
https://www.ted.com/talks/taken_for_granted_daniel_kahneman_doesn_t_trust_your_intuition

Dezenformasyon yayan aktörler, profesyonel troller, propaganda ağları, kötü niyetli siyasi gruplar ve dolandırıcılar; günümüzün en tehlikeli "zihin korsanları"dır. Bu kişiler, insan zihninin bazı alışkanlıklarını ve duygusal hassasiyetlerini çok iyi tanır ve bunları bilinçli biçimde kullanır. Bu zihin korsanlarının en büyük avantajı, karmaşık teknolojiler üretmek zorunda olmamalarıdır. Onlar, gelişmiş yazılımlar ya da teknik sistemler yerine, çok daha basit bir noktaya, insan zihninin "fabrika ayarları" diyebileceğimiz, hepimizin paylaştığı temel düşünme reflekslerine ve duygusal tepkilere odaklanır. Bu nedenle dezenformasyon, siber saldırılardan farklı bir şekilde işler. Hedef bilgisayar sistemleri değil, doğrudan insan zihnidir. Zihin korsanları, beynin uzun zamandır kullandığı alışkanlıkları devreye sokar ve bu sayede mesajlarını çok hızlı ve etkili biçimde yayabilir. Yanlış bilgi ve manipülasyon, özellikle duyguları harekete geçirdiğinde güç kazanır. Korku, öfke, aidiyet ihtiyacı ya da onaylanma isteği gibi duygular devreye girdiğinde, insanlar edindikleri bilgiyi

sorgulamak yerine bu bilgiye istinaden tepki vermeye yönelir. İşte bu nedenle dezenformasyon ikna edicidir.

Yanlış bilgi ve manipülasyon, çoğu zaman insanın en temel korkularına seslenerek etkili olur. Bu korkular günlük hayatta farkında olmadan kararlarımızı şekillendirir ve doğru ile yanlışı ayırmamızı zorlaştırır. Bu korkulardan ilki kaybetme kaygısıdır. İnsan zihni, olası bir kazançtan çok, sahip olduğu bir şeyi kaybetme tehdidine daha güçlü tepki verir. Ekonomik güvence, kimlik, statü ya da kişisel güvenlik gibi alanlarda yaratılan "elinizden alıyorlar" söylemi, bu korkuyu harekete geçirerek manipülatif mesajları daha ikna edici hale getirir. Bir diğer önemli etken, dışlanma ve yalnız kalma korkusudur. Bir gruba ait olmak insanlara güven ve anlam hissi sağlar; bu aidiyet tehdit edildiğinde, bireyler yanlış bilgiyi sorgulamak yerine grubun sunduğu anlatıyı kabul etmeye daha yatkın hale gelir. Özellikle "biz" ve "onlar" ayrımı üzerinden kurulan dil, bu eğilimi güçlendirir. Son olarak, belirsizlikten kaçınma ihtiyacı yanlış bilginin cazibesini artırır. Zihin, belirsizliği sevmez. Karmaşık ve net olmayan durumlar rahatsızlık yaratır. Karmaşık gerçeklerle yüzleşmek yerine komplo teorileri ya da aşırı basitleştirilmiş açıklamalar hızlı ve kesin cevaplar sunar. Bu nedenle de çekici görünür. Bu bağlamda yanlış bilgiye inanmak; çoğu zaman zihnin belirsizlik ve tehdit karşısında geliştirdiği koruyucu ve uyum sağlayıcı stratejilerden biri olarak ortaya çıkar.

Yanlış bilgi ve manipülasyon yalnızca korkulara değil, insanların kendileriyle ilgili beklentilerine ve ihtiyaçlarına da hitap eder. Ait olma, onaylanma ve kendini değerli hissetme arzusu, bu sürecin en temel itici güçleri arasındadır. İnsanlar genellikle zaten inandıkları düşünceleri destekleyen bilgilere yönelir; kendi görüşlerini doğrulayan içerikler güven verir ve zihinsel bir rahatsızlık yaratmaz. Doğrulama yanlılığı (*confirmation bias*) olarak bilinen bu eğilim, manipülatif içeriklerin etkisini artırır. Bu tür içerikler, kişinin zaten inanmak istediği şeyi sanki kanıtlıyormuş gibi sunarak sorgulama ihtiyacını

devre dışı bırakır. Bunun yanı sıra, kendini özel hissetme ihtiyacı da yanlış bilginin cazibesini güçlendirir. Özellikle komplo teorileri, bireyi "gerçeği" bilen azınlığın bir parçası haline getirerek güçlü bir aidiyet ve üstünlük duygusu sunar. Bu anlatılar, kişiyi herkesin kandırıldığı bir dünyada gerçeğin farkında olan nadir kişilerden biri konumuna yerleştirir ve kendini diğerlerinden daha bilgili ve ayrıcalıklı hissetmesini sağlar.

Beyin, her bilgiyi tek tek ve ayrıntılı biçimde incelemez. Zihinsel yükü azaltmak için bilişsel kısa yollar (*heuristics*) kullanır. Bu kısayollar çoğu zaman işimizi kolaylaştırırlar, ancak yanlış bilgiye de açık hâle getirebilirler. Manipülatif içerikler bu durumu bilinçli olarak kullanır. Bir bilginin doğru olup olmadığını sorgulatmak yerine, bizde uyandırdığı duyguya odaklanmamızı sağlar. Örneğin korku, öfke ya da heyecan uyandıran içerikler daha inandırıcı görünebilir. Benzer şekilde, bir bilginin çok paylaşılmış olması da doğru olduğu izlenimini yaratır. "Herkes paylaşıyorsa doğrudur" düşüncesi, eleştirel düşünmenin geri planda kalmasına yol açar.

> 🔍 **KAVRAM:** KOMPLO TEORİSİ
>
> **Neyi açıklar?:** "Bunu bize söylemiyorlar", "Asıl gerçek gizleniyor" gibi ifadeler tanıdık geliyor mu? Komplo teorileri, toplumsal ve siyasal olayların nedenlerini; her şeye hâkim aktör/aktörlerin gizli planları ve kasıtlı komploları üzerinden açıklayan anlatılardır.
> **Neden önemli?:** Komplo teorileri, zihnin belirsizlikten kaçma arzusunu tatmin ederek eleştirel düşünmeyi felç eder ve karmaşık gerçekleri basit gizli planlara indirger. Kanıtların yerini sarsılmaz inançların aldığı bu ortamda, toplumsal güven çürür ve demokrasiyi tehdit eden derin bir gerçeklik bölünmesi ortaya çıkar.

Zihnimiz Neden Acelecidir?

Beynimiz, evrimsel olarak küçük, yüz yüze iletişim ağlarına ve bilgi kıtlığına göre optimize edilmiş "Taş Devri yazılımıyla" çalışır. Ancak biz, bu eski yazılımı modern, aşırı bağlantılı, sürekli bilgi akışı altında olan devasa bir dijital bilgi ekosisteminde kullanmaktayız. Bu uyumsuzluk, devasa bir güvenlik açığı yaratır. Beyin, bu yeni ortamdaki manipülasyon hızına, hacmine ve

duygusal yoğunluğuna karşı savunmasızdır. Eleştirel düşünme, kaynak kontrolü gibi mantıklı şüphecilik mekanizmalarını devreye sokmak, duygusal temelli ve hızla yayılan bilgilere inanmaktan daha fazla enerji gerektirir. Çoğu zaman, beyin "enerji tasarrufu modu"na geçer ve duygusal tepkiyi temel almayı seçer. Dijital zihin savaşından korunmanın ve zihinsel güvenliği sağlamanın ilk ve en önemli adımı, biyolojik mirasımızı oluşturan evrimsel zayıflıkları, bilişsel eğilimleri ve duygusal tetikleyicileri derinlemesine kavramaktır. Zihinsel güvenlik duvarımız, dış tehditlere ek olarak, içeriden kaynaklanan bu "fabrika ayarı kusurlarına" karşı da mutlaka korunmalıdır.

Günümüzde yaygın olarak görülen kaygı, kronik stres, dikkat dağınıklığı ve bilgi kirliliğine karşı savunmasızlık yalnızca bireysel sorunlar değildir. Bilim insanları bu durumu, "evrimsel uyumsuzluk" adı verilen bir teoriyle açıklar. Bu teoriye göre sorun şudur: İnsan beyni çok yavaş değişen biyolojik bir geçmişe sahiptir; ancak yaşadığımız sosyal ve teknolojik dünya çok hızlı dönüşmüştür. Özellikle son yüzyılda teknoloji, iletişim ve bilgi üretimi olağanüstü bir hız kazanmıştır. Beyin ise bu hıza aynı ölçüde uyum sağlayamamıştır. İnsan zihni, binlerce yıl önce küçük gruplar hâlinde, yüz yüze ilişkilerin olduğu ve bilginin sınırlı olduğu koşullarda işlemeye alışmıştır. Bu koşullarda hızlı karar vermek, tehlikeyi çabuk fark etmek ve duygulara göre hareket etmek hayatta kalmak için avantajlıydı. Bugün ise bambaşka bir ortamdayız. Milyarlarca insanın aynı anda etkileşimde bulunduğu, algoritmaların yön verdiği ve sürekli değişen bir dijital dünyada yaşıyoruz. Beynin alışık olduğu çalışma koşulları ile içinde bulunduğu bilgi ortamı arasında ciddi bir uyumsuzluk vardır. Bu uyumsuzluk, tıpkı eski bir sistemin çok karmaşık bir programı çalıştırmaya zorlanması gibi, çeşitli sorunlara yol açar. Günümüzde yaşanan pek çok psikolojik zorluk ve bilgi kirliliğine karşı kırılganlık, beynin alışık olduğu işleyiş ile modern yaşamın talepleri arasındaki bu gerilimin bir sonucudur.

Doğada hayatta kalmaya çalışan atalarımız için bilgi, günümüzdeki gibi entelektüel bir lüks ya da akademik bir merak konusu değildi. "Bu yılan zehirli mi?", "Şu bulutlar fırtına mı getiriyor?" veya "Karşı kabile dost mu, düşman mı?" gibi soruların cevabı, anlık bir ölüm-kalım meselesiydi. Doğru bilgi hayatta kalmayı sağlarken, yanlış bilgi hızla gen havuzundan silinmeye yol açardı. Ancak her zaman doğru bilgiyi tespit etmek kolay değildi. Bu durumda ilginç bir soru ortaya çıktı: Yanılmak kaçınılmazsa, hangi yönde yanılmak daha güvenliydi?

Bunu basit bir örnekle düşünelim. Doğada yürüdüğünüzü ve çalılıklardan belirsiz bir hışırtı sesi geldiğini hayal edin. Önünüzde iki temel tepki seçeneği vardır. İlkinde, zihniniz bu sesi potansiyel bir tehdit olarak yorumlar: "Bu bir aslan, bir yılan ya da kötü niyetli bir kişi olabilir." Bu varsayımla hemen kaçarsınız ya da kendinizi savunmaya geçersiniz. Eğer gerçekten bir aslan varsa, bu hızlı tepki hayatınızı kurtarır. Eğer ses yalnızca rüzgârdan geliyorsa, boşuna korkmuş olursunuz; biraz yorulur, enerji harcar ve belki de utanç yaşarsınız. Ancak sonuçta hayattasınızdır. Bu, yanlış alarm vermek pahasına güvenliği önceleyen, maliyeti görece düşük bir hatadır.

İkinci tepkide ise zihin daha şüpheci davranır. "Dur, hemen panik yapmayayım; belki de bu sadece rüzgârdır" diyerek sesin ne olduğunu anlamaya çalışırsınız. Eğer gerçekten rüzgârsa, doğru karar vermiş olursunuz ve enerjinizi boşa harcamazsınız. Ancak ses bir aslandan geliyorsa siz durumu analiz etmeye çalışırken saldırıya uğrayabilirsiniz. Bu da en yüksek maliyetli hataya yol açar. İnsan zihni, evrimsel olarak bu iki seçenek arasında çoğu zaman ilkini, yanlış da olsa alarm vererek, hayatta kalmayı tercih edecek şekilde gelişmiştir. Doğal seçilim, bu iki hata türünden birini uzun süre boyunca sistematik biçimde daha avantajlı kıldı. Milyonlarca yıl boyunca, en ufak bir belirsizlikte bile hızlı ve abartılı tepki verenler, daha "paranoyak" olanlar, daha fazla hayatta kaldı. Çalılıktaki belirsiz bir şekli hızla yılana benzeten,

her gölgede bir tehdit gören, "Ya varsa?" deyip kaçmayı seçenler çoğu zaman yaşamayı başardı. Buna karşılık, şüpheci davranıp "Dur, önce kanıt göreyim" diyen atalarımız bazen çok geç kaldı. Bu geç kalma sonucunda da kimi zaman yılanların zehrine maruz kaldı, kimi zaman da aslanlara yem oldu. Bu yüzden biz, istatistiksel olarak, hayatta kalma ihtimali en yüksek olan o hızlı tepki veren ve tehdide inanma eğilimi güçlü ataların mirasını taşıyoruz. Beynimizde kalıcı bir eğilim var. "Hata yönetimi teorisi" adı verilen bu teoriye göre, zihnin, belirsizlik karşısında genellikle bedeli en düşük hatayı seçiyor. Örneğin "Kabileye zehirli bir avcı yaklaşıyor" ya da "O mantar zehirli" gibi tehdit içeren bir bilgiyi sorgulamadan doğru kabul etmenin bedeli çoğu zaman sadece biraz boş yere paniklemektir. Ama bu bilgiyi umursamamanın, yanılmanın bedeli ise ölüm olabilir. İşte bu nedenle beyin, tehlike sinyallerinde çoğu zaman "önce inan, sonra sorgula", hatta bazen "hiç sorgulama" mantığıyla çalışır.

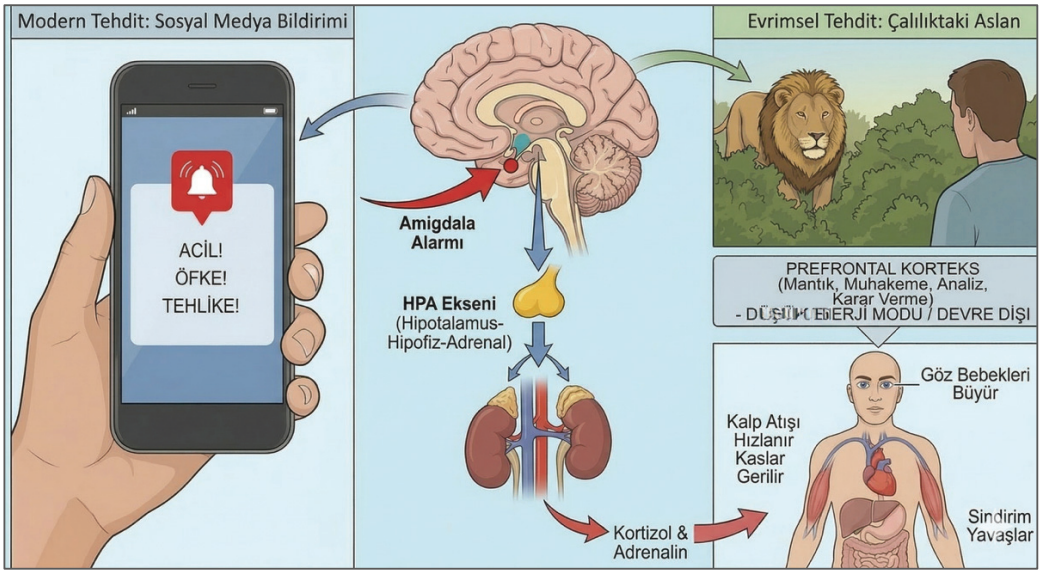
KAVRAM: ÖFKE TUZAĞI

Neyi açıklar?: Öfke tuzağı (*rage bait*), kullanıcıyı bilgilendirmekten ziyade öfkelendirmeyi, kışkırtmayı ve duygusal tepki üretmeyi hedefleyen içerikleri ifade eder. Abartılı başlıklar, kutuplaştırıcı söylemler ve kasıtlı çarpıtmalar, etkileşim ekonomisinin en verimli araçları arasındadır.

Neden önemli?: Öfke, dijital platformlarda en hızlı yayılan duygulardan biri olduğu için, hakikat çoğu zaman geri planda kalır.

Artık doğa koşullarında yaşamıyoruz. Ancak beynimizin en eski ve duygusal kısmı olan limbik sistem, özellikle de amigdala, bunun farkında değil. Evrimsel geçmişimizde çalılıklardan gelen bir hışırtı hayati bir tehlike anlamına geliyordu. Bugün ise bu tehlike sinyalinin yerini, cebimizde taşıdığımız telefonlardan gelen bildirim sesi, titreşim ya da bir sosyal medya uyarısı almış durumda. Bir zamanlar tehdit; aslan, yılan, düşman bir savaşçı ya da sel gibi somut ve fiziksel tehlikelerdi. Bugün ise tehdit olarak algılanan şeyler çoğu zaman dijital: "Son dakika: Büyük deprem bekleniyor" başlığı, "Hesabınız ele geçirildi" uyarısı, "Aşılar tehlikeli" diyen bir video ya da sert bir siyasal

kutuplaşma içeriği bu tehdit örneklerinden.



Şekil 2.1.1 *Sosyal medya bildirimlerinin "savaş ya da kaç" mekanizması üzerindeki etkisi*

Sorun şu ki, beynimiz bu iki tehdit türü arasında biyolojik bir ayrım yapamaz. Korku, öfke ya da "acil tehlike" duygusu uyandıran bir bildirim gördüğümüzde, vücudumuz hâlâ çalılıktaki bir aslanla karşılaşmışız gibi tepki verir. Bu tepki otomatik ve çok hızlıdır. Önce amigdala devreye girer ve alarm verir. Ardından HPA ekseni olarak bilinen stres sistemi çalışmaya başlar. Kana adrenalin ve kortizol salgılanır. Kalp atışı hızlanır, kaslar gerilir, göz bebekleri büyür, sindirim yavaşlar. Vücut, kendini "savaş ya da kaç" durumuna hazırlar. Bu sürecin en kritik sonucu ise şudur: Mantık, muhakeme, analiz ve sağlıklı karar vermeden sorumlu olan prefrontal korteks (PFK) geçici olarak geri plana itilir. Çünkü acil bir tehdit anında beynin önceliği düşünmek değil, hayatta kalmaktır. Kortizol ve adrenalin, PFK'nın çalışmasını yavaşlatır; hatta kısa süreliğine devre dışı bırakır. Tam da bu nedenle, dijital ortamda karşılaştığımız korku ve panik yüklü içerikler, düşünmeden tepki vermemizi kolaylaştırır. Bunun nedeni basittir: Aslandan kaçarken

düşünmeye değil, hızlı tepki vermeye ihtiyaç vardır. O an matematik çözmez, felsefe yapmaz, bir bilginin kaynağını kontrol etmezsiniz. Vücut bu acil durumda enerjiyi düşünmeden değil, kaslardan ve reflekslerden yana kullanır.

Dijital ortamda yanlış bilgilerin, yalan haberlerin ve kutuplaştırıcı içeriklerin hızla yayılmasının temelinde de bu mekanizma vardır. Bu içerikler mantığa değil, doğrudan korkuya ve öfkeye seslenir. Limbik sistem adeta şunu duyar: "Tehlike var! Düşünme, hemen tepki ver!" Paylaşmak, bağırmak, taraf tutmak bu yüzden bu kadar kolaydır. Modern teknoloji, ilkel hayatta kalma refleksimizi sürekli sahte tehlike sinyalleriyle tetikleyerek bizi bilgi kirliliğine karşı savunmasız bırakır.

🎬 İZLE

"Gerçekten umuyorum ki insanlar filmi izlesin ve geçmişe bakıp şöyle desinler: 'Eğer gerçeği görmek için bu gözlükleri takıyor olsaydım- ki bunlar öfke gözlükleridir; bir başka deyişle bana tıklayacağım şeyleri göster, bu da beni kızdıracak şeyleri göster demektir- ve bunu tekrar, tekrar ve tekrar yapsaydım [dünya nasıl görünürdü]?"

Tristan Harris *The Social Dilemma* belgeselini anlatırken değindiği bu metaforu, sosyal medya algoritmalarının çalışma prensibini açıklamak için kullanıyor. Algoritmalar etkileşim istedikleri için, insan doğasında en hızlı tepkiyi veren duygu olan öfkeyi tetikleyen içerikleri önümüze getirir. Bu durum, tıpkı takılan bir gözlük gibi dünyayı olduğundan daha kötü, daha sinir bozucu ve daha düşmanca görmemize neden olur.

🔗 Belgeseli izlemek için:
https://www.netflix.com/tr/title/81254224

Neden Sorgulamak Yerine İnanırız?

Neden her haberi tek tek doğrulamıyoruz? Neden içeriğini okumadan, yalnızca başlığın yarattığı etkiyle paylaş tuşuna basıyoruz? "Google'lamak" veya kaynak kontrolü yapmak bu kadar kolayken, neden çürütülebilir bir dedikoduya veya komplo teorisine inanmayı seçiyoruz? Bu gerçekten modern insanın tembelliği midir? Kısa ve bilimsel cevap: Hayır. Bu durum sadece tembellikle açıklanamaz. Asıl neden, insan beyninin doğası gereği enerji tasarrufu yapacak şekilde çalışmasıdır. Beyin, biyolojik olarak tutumlu davranır; mümkün olan her durumda daha az enerji harcamayı seçer. Bu da milyonlarca yıllık evrimin şekillendirdiği, hayatta kalmaya yönelik bir stratejidir.

İnsan beyni ne kadar gelişmiş ve etkileyici olursa olsun, aynı zamanda vücudun en kıymetli organıdır. Bir yetişkinin beyninin ağırlığı, vücut ağırlığının yalnızca yaklaşık %2'sini oluşturur. Buna rağmen beyin, vücut dinlenme hâlindeyken bile kullanılan enerjinin yaklaşık %20'sini tek başına tüketir. Yeni doğan bebeklerde ise bu oran, beynin hızla gelişmesi nedeniyle %60'a kadar çıkar. Bu tablo, beyin için harcanan enerjinin vücut açısından ne kadar büyük bir yük olduğunu açıkça gösterir.[7] Bu yüksek enerji ihtiyacı, beynin sürekli tasarruf yapacak şekilde çalışmasını zorunlu kılar. Özellikle bazı zihinsel faaliyetler beyin için oldukça maliyetlidir: dikkatle odaklanmak, bilgiyi derinlemesine analiz etmek, eleştirel okumak ve farklı kaynakları karşılaştırmak gibi. Bu tür işlemler sırasında beynin enerji tüketimi anlık olarak artar. Bu nedenle beyin, hayati bir zorunluluk olmadıkça, bu tür zahmetli düşünme süreçlerinden kaçınma eğilimindedir. Psikolojide bu durum "bilişsel cimrilik" (*cognitive miser*) kavramıyla açıklanır. Susan T. Fiske ve Shelley E. Taylor'a göre model, insanların bilgi işleme kapasitelerinin sınırlı olduğu temel fikrine

[7] Aiello, L. C., & Wheeler, P. (1995). The expensive-tissue hypothesis: the brain and the digestive system in human and primate evolution. *Current Anthropology,* 36(2), 199-221.

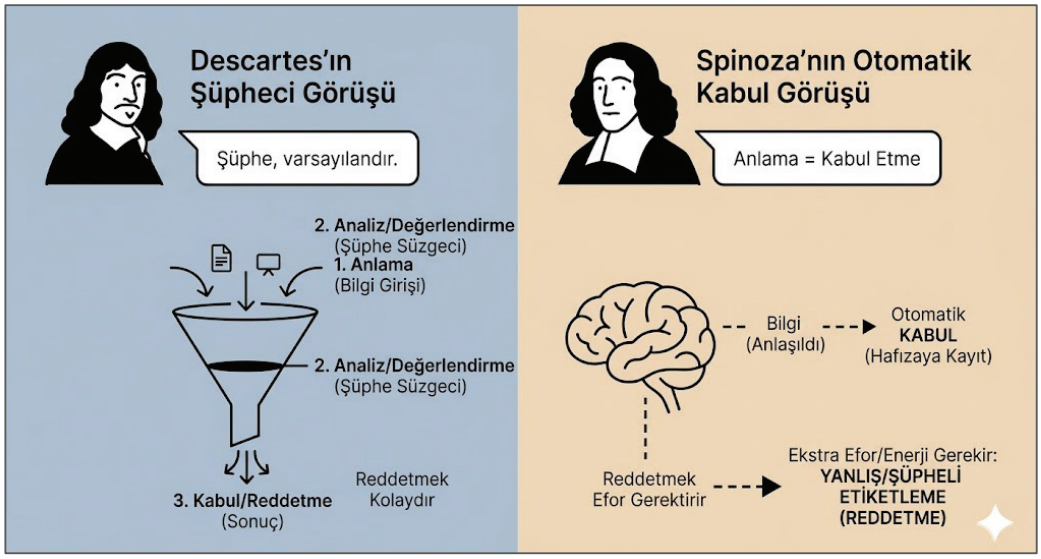
dayanmaktadır. Bu modele göre, insan zihni genellikle en hızlı ve en az enerji gerektiren yolu seçer. Detaylı düşünmek yerine, sezgisel kısa yolları kullanır. Bu zihinsel kestirmeler gündelik hayatın çoğunda işimizi kolaylaştırır; ancak yanlış ve yanıltıcı bilgiler karşısında bizi savunmasız bırakır.

Dezenformasyonun bu kadar cazip olmasının nedeni de tam olarak budur. Yanlış bir bilgiye inanmak neredeyse hiçbir zihinsel çaba gerektirmez. Oysa bir bilgiyi doğrulamak; arama yapmak, farklı kaynaklara bakmak ve güvenilirliği sorgulamak anlamına gelir. Bu da beyin için yüksek maliyetli bir süreçtir. Özellikle yorgun, stresli ya da uykusuz olduğumuzda, beyin otomatik olarak en düşük maliyetli seçeneğe yönelir: Hemen inanmak ve paylaşmak. Sosyal medyanın sürekli bildirimler, sonsuz kaydırma ve dikkat dağıtıcı içeriklerle dolu yapısı ise beynimizi sürekli yorgun tutarak, yanlış bilgiye karşı direncimizi daha da zayıflatır.

Bir bilginin zihnimizde nasıl anlaşıldığı ve inanca dönüştüğü sorusu 17. yüzyıldan beri filozofların ve günümüzde nörobilimcilerin temel tartışma konularından biri olmuştur. Bu konuda iki temel yaklaşım vardır ve bu yaklaşımlar birbirine tamamen zıttır. İlk yaklaşım, ünlü Fransız düşünür René Descartes'a dayanır. Bu görüşe göre zihin, karşılaştığı bilgiye önce şüpheyle yaklaşır. Bilgi önce algılanır, sonra dikkatle incelenir ve ancak bu değerlendirmeden sonra doğru ya da yanlış olduğuna karar verilir. İnanmak, bilinçli ve kontrollü bir sürecin sonucudur. Bu modele göre şüphe etmek doğaldır, inanmak ise sonradan gelir. Hollandalı filozof Baruch Spinoza ise tamamen karşıt bir tez öne sürer. Ona göre insan zihni, bir bilgiyi anladığı anda onu otomatik olarak doğru kabul eder. Bilgiyi reddetmek ya da şüphe duymak ise ikinci bir adımdır ve ekstra zihinsel çaba gerektirir. İnanmak varsayılandır; reddetmek ise sonradan ve isteyerek yapılan bir düzeltmedir.

Yüzyıllar boyunca felsefi düşünce, René Descartes'ın bilginin doğası ve inanç oluşumu hakkındaki rasyonel modelini daha mantıklı ve kabul edilebilir

bulmuştur. Bu kartezyen model, bir fikri veya bilgiyi kabul etmeden önce kapsamlı bir değerlendirme ve mantıksal doğrulama sürecinden geçirilmesi gerektiğini savunur. Anlama ve inanma süreçlerinin birbirinden ayrı ve sıralı olduğunu öne sürer. Ancak, modern bilişsel psikoloji ve nörobilim alanındaki ilerlemeler, özellikle de sosyal biliş alanında çığır açan çalışmalarıyla tanınan Daniel Gilbert ve meslektaşlarının 1990'lardaki kapsamlı deneyleri, bu yerleşik kartezyen görüşe meydan okumuş ve Baruch Spinoza'nın yüzyıllar önce ileri sürdüğü alternatif bir modelin haklı olduğunu güçlü bir şekilde kanıtlamıştır.



Şekil 2.1.2 *Descartes ve Spinoza'nın bilginin doğasına ilişkin görüşleri*

Spinoza, bilginin edinimi ve inanç oluşumu sürecinin Descartes'ın öne sürdüğünden çok daha entegre ve otomatik olduğunu savunmuştur. Spinoza'ya göre, beynimiz bir bilgiyi *anladığı* anda, o bilgiyi otomatik olarak doğru kabul etme eğilimindedir. Anlama eylemi, beraberinde geçici veya varsayılan bir inanma eylemini de getirir. Bu inancı daha sonra, bilinçli ve çaba gerektiren bir süreçle inanmama veya yanlışlama yoluyla reddetmemiz gerekir. Gilbert'ın deneyleri, bu Spinozacı modelin insan zihninin gerçeğe daha yakın

bir temsili olduğunu göstermiştir: Anlama anında, otomatik olarak inanma gerçekleşir; inanmamak ise sonradan devreye giren ve ek bilişsel yük gerektiren bir düzeltme sürecidir. Bu bulgu, insan zihninin işleyişini anlamada Descartes'ın şüpheye dayalı modelinden ziyade, Spinoza'nın yaklaşımının daha açıklayıcı olduğunu ortaya koymaktadır.

Araştırmalar, beynimizin varsayılan yöneliminin inanmak olduğunu göstermektedir. İnanma süreci hızlı, otomatik ve neredeyse zahmetsizdir; çok az enerji harcar. Buna karşılık şüphe etmek, sorgulamak ya da bir bilgiyi reddetmek bilinçli bir çaba gerektirir, zaman alır ve daha fazla zihinsel enerji tüketir. Yeni bir bilgiyle karşılaştığımızda, örneğin "Günde bir kaşık tarçın tip 2 diyabeti %100 iyileştirir" iddiasında olduğu gibi, beynimiz bu bilgiyi çok kısa bir sürede, adeta bir dosyayı kaydeder gibi, geçici olarak doğru kabul eder. Ancak yeterli zamanımız, zihinsel enerjimiz ve ön bilgimiz varsa ikinci bir adım devreye girer. Bu aşamada durur, düşünür ve "Bu bilimsel olarak mantıklı mı?" diyerek ilk kabulü bilinçli bir çabayla geri çekebiliriz.

Günlük hayatta ise çoğu zaman bu ikinci aşama gerçekleşmez. Yorgun olduğumuzda, dikkatimizi dağıtan başka içeriklerle karşılaştığımızda ya da zaman baskısı altındayken ilk ve otomatik kabul kalıcı hâle gelir. Çünkü bilgiyi sorgulayıp reddetmeye yetecek zihinsel kaynaklar devreye girmemiştir. Bu nedenle dezenformasyonun etkisi insanların düşünmeyi bırakmasından değil; beynimizin enerji tasarrufu yapacak şekilde çalışmasından kaynaklanır. Doğrulamak bilinçli bir tercihtir ve emek ister. İnanmak ise varsayılan, hızlı ve enerji dostu yoldur.

Nobel ödüllü psikolog Daniel Kahneman, 2011 yılında yayınladığı ve modern bilişsel bilimler tarihinin temel taşlarından biri olarak kabul edilen eseri *"Hızlı ve Yavaş Düşünme"* (*Thinking, Fast and Slow*)[8] kitabında, insan

[8] Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.

zihninin nasıl çalıştığını açıklamak için basit ama güçlü bir model sunar. Kahneman'a göre zihnimiz tek parça değildir. Aksine, birbirinden çok farklı özelliklere sahip iki ayrı düşünme sistemi aynı anda çalışır: Sistem 1 ve sistem 2. Günlük kararlarımızdan karmaşık muhakemelere kadar pek çok zihinsel süreç bu iki sistemin etkileşimiyle şekillenir.

Sistem 1, zihnimizin hızlı, otomatik ve duygusal kısmıdır. Bir otopilot gibi çalışır; sürekli aktiftir ve kapatılamaz. Çoğu zaman farkında bile olmadan bizi yönlendirir. Bu sistem sezgilerle hareket eder. Düşünmek için çaba harcamaz; hızlı, içgüdüsel ve duygusaldır. Sistem 1, beynin "tehlike algılayan" eski kısmına dayanır. Amacı analiz yapmak değil, hayatta kalmak için mümkün olan en hızlı tepkiyi vermektir. Sistem 1; ani bir sese irkilmekten basit hesapları yapmaya, yüz ifadelerinden duyguları anlamaktan alışkanlıkla araba kullanmaya kadar pek çok gündelik işi üstlenir. Cümleleri otomatik olarak tamamlamamız ya da tanıdık bir durumu düşünmeden anlamamız da bu sistem sayesinde olur. Ancak sistem 1'in bir bedeli vardır: Kolay ikna olur, sabırsızdır ve karmaşık analizden hoşlanmaz. Olayları basitleştirir, eksik bilgileri hızla doldurur ve tutarlı bir hikâye kurmaya çalışır; doğru olup olmadığıyla fazla ilgilenmez. Bu yüzden de hızlıca neden-sonuç ilişkileri kurar ve güçlü duygular üretir. Dijital çağda, özellikle sosyal medyada, direksiyon çoğu zaman sistem 1'dedir. Akışta hızla ilerlerken bir içeriğe anında öfke, korku ya da sevinçle tepki veren; düşünmeden beğenen, paylaşan ya da sert tepki gösteren sistem odur. Sistem 1 için önemli olan bilginin doğruluğu değil, uyandırdığı duygunun gücüdür.

Sistem 2, zihnimizin düşünen, hesaplayan ve dikkat gerektiren kısmıdır. Bir pilot gibi çalışır; sürekli devrede değildir, ancak ihtiyaç olduğunda bilinçli bir çabayla kontrolü ele alır. Bu sistem yavaştır ama mantıklıdır. Adım adım düşünür, kanıt arar ve rasyonel kararlar vermeye çalışır. Kökeni, beynin en gelişmiş bölgesi olan prefrontal kortekstir. Bu bölge planlama,

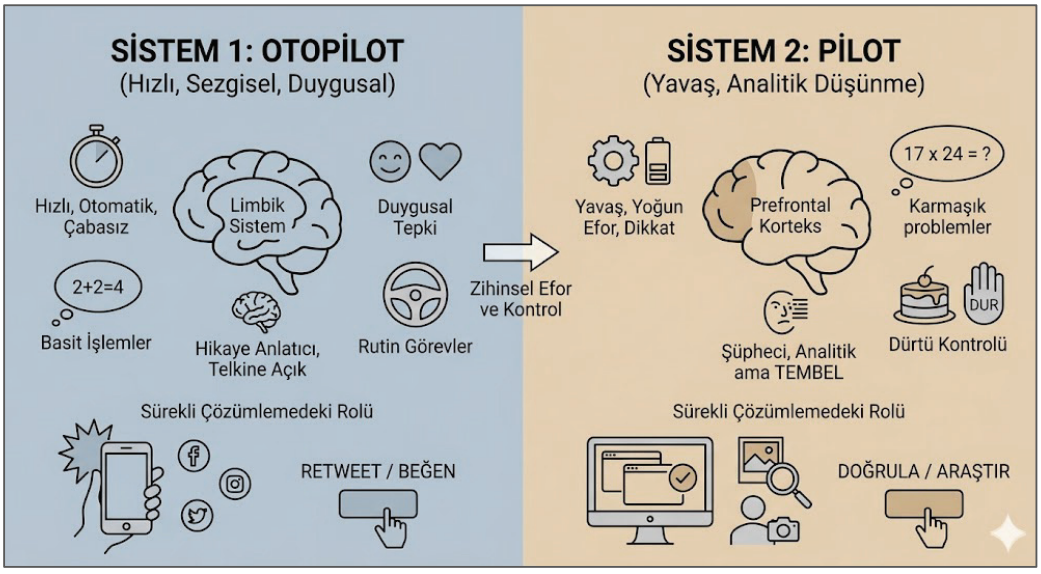
dürtüleri kontrol etme ve soyut düşünme gibi karmaşık zihinsel işlevlerden sorumludur. Sistem 2, karmaşık problemleri çözmek, dikkat gerektiren işlere odaklanmak ve durup düşünmeyi gerektiren kararları vermek için devreye girer. Bir matematik sorusunu çözmek, bir iddianın mantıklı olup olmadığını tartmak ya da anlık bir isteğe karşı koymak, örneğin diyetteyken pastayı reddetmek bu sistemin işidir. Ancak sistem 2'nin önemli bir zayıflığı vardır: Çok enerji tüketir. Bu yüzden tembeldir ve yalnızca mecbur kaldığında tam kapasite çalışır. Çoğu zaman, sistem 1'in hızlıca vardığı sonuçları sadece yüzeysel biçimde kontrol eder; adeta bir noter gibi onaylar. Bilgi düzensizlikleriyle mücadelede asıl sorumluluk sistem 2'ye düşer. Bir haberin doğruluğunu kontrol etmek, farklı kaynaklara bakmak ya da bir görselin manipüle edilip edilmediğini araştırmak bu sistemin işidir. Ancak bu süreçler zihinsel yorgunluk yaratır. Duygular yoğunlaştığında ya da dikkat dağıldığında, sistem 2 kolayca geri çekilir ve kontrol yeniden sistem 1'e geçer.

İZLE

Sistem 1 ve Sistem 2: Beyninizdeki Gizli Savaş
https://www.youtube.com/watch?v=BwKcz1fFXPQ

Dezenformasyonun, propagandanın ve viral içeriklerin başarısı, insan zihninin nasıl çalıştığını iyi bilmeye dayanır. Bu içerikler, Daniel Kahneman'ın tanımladığı iki düşünme sistemi arasındaki farktan yararlanır: hızlı ve duygusal sistem 1 ile yavaş ve mantıklı sistem 2. Temel strateji basittir: Sistem 1'i duygularla harekete geçirmek, sistem 2'yi ise devre dışı bırakmak. Manipülatif içerikler, düşünmeyi değil tepki vermeyi hedefler. Amaç; analiz yapan zihni atlayarak, otomatik ve içgüdüsel tepkileri yöneten sistemi kontrol altına almaktır. Çarpıcı bir başlık, sarsıcı bir görsel ya da kısa bir video güçlü bir duygu yarattığında, dikkat hızla sistem 1'e kayar. Korku, öfke ya da heyecan

arttıkça, durup düşünme ve sorgulama ihtimali azalır. Böylece içerik, doğruluğu kontrol edilmeden kabul edilir ve hızla yayılır. Kısacası manipülasyonun gücü mantıktan değil, duyguyu doğru anda ve doğru dozda tetiklemesinden gelir. Bu da zihinsel bir kısa yol yaratarak, eleştirel düşüncenin devreye girmesini engeller.



Şekil 2.1.3 *Sistem 1 ve sistem 2 arasındaki farklar*

Manipülasyon araçları, insan zihninin hızlı ve otomatik çalışan sistem 1'ini devreye sokmak için en güçlü duygusal tetikleyicilere odaklanır. Bu tetikleyicilerin başında öfke gelir. Haksızlık, mağduriyet ya da bir "düşman" anlatısı üzerinden beslenen öfke, insanları durup düşünmeden tepki vermeye iter. Bu duygu yoğunlaştığında zihin ayrıntıları sorgulamaz; içerik hızla paylaşılır, tepki bir eyleme dönüşür ve yanlış bilgi kolayca yayılır. Korku da benzer biçimde güçlü bir etkiye sahiptir. Güvenlik, sağlık, ekonomi ya da gelecek hakkında bir tehdit hissi yaratıldığında, eleştirel düşünme geri plana itilir; insanlar hızlıca kendilerini güvende hissettirecek açıklamalara ve çözümlere yönelir. Bu durum, rahatlatıcı ya da "kurtarıcı" gibi sunulan yanlış bilgilere

inanmayı kolaylaştırır. Mizah ve alay ise zihnin savunma mekanizmalarını daha sessiz bir şekilde aşar. "Sadece şaka" hissi, içeriğin ciddiyetle sorgulanmasını engellerken, alaycı dil karşıt görüşleri küçümseyerek tartışmayı mantık zemininden koparır. Son olarak haz ve cinsellik çağrışımları, insanın en temel dürtülerine hitap ederek dikkati hızla çeker ve zihni otomatik moda sokar. Bu tür içerikler, anlık haz arayışını tetiklediği için bireyin odağı rasyonel analizden uzaklaşır; içeriğin amacı ve doğruluğu geçici olarak sorgulanmaz.

Manipülatif içeriklerin asıl amacı, bireyi düşünen ve sorgulayan bir yurttaş olmaktan çıkarıp, duygularıyla hareket eden ve anlık tepki veren bir hâle getirmektir. Bu noktada eleştirel düşünce geri çekilir; kontrol, hızlı ve duygusal çalışan sistem 1'e geçer. İşte manipülasyonun en kolay ve etkili olduğu zemin tam da burasıdır. Bu yüzden dijital çağda en önemli savunma adımı, tepki vermeden önce durabilmektir. Bir içerik sizde öfke, korku ya da aşırı heyecan yarattığında, ilk yapılması gereken bu duyguyu fark etmektir. Bu kısa farkındalık anı, düşünmeye alan açar ve yavaş düşünen sistem 2'yi devreye sokar. Bu duraklama sırasında basit ama kritik sorular sormak gerekir: "Bu içerik beni neden bu kadar etkiledi?", "Hangi duyguma hitap ediyor?", "Bunun doğru olması ne kadar mantıklı?", "Buna inanmak için elimde ne var?". Bu küçük yavaşlama, manipülasyona karşı en güçlü savunmadır ve dijital okuryazarlığın temelini oluşturur.

Kahneman'ın *Hızlı ve Yavaş Düşünme* kitabında anlattığı sistem 1 ve sistem 2 modeli, yalnızca teorik bir açıklama değildir; beynin yapısında da somut bir karşılığı vardır. Bu model, duygularla çalışan beyin bölgeleri ile mantık ve kontrolü yöneten bölgeler arasındaki sürekli etkileşimi ifade eder. Bir yanda hızlı tepki veren duygusal tepki merkezi, diğer yanda düşünmeyi ve karar vermeyi yöneten mantıksal yönetim merkezi bulunur. Bu iki yapı arasındaki gerilim, özellikle yanlış bilgi ve manipülasyonun neden bu kadar etkili

olabildiğini anlamak açısından kilit önemdedir.

👉 DENE

Şu soruyu hızla, durup düşünmeden, aklınıza gelen ilk cevapla yanıtlayın: *Bir beyzbol sopası ve bir topun toplam fiyatı 1,10 dolardır. Sopa, toptan 1,00 dolar daha pahalıdır. Top kaç dolardır?*
Çoğu insanın verdiği cevap: "10 sent". Hatta bu cevap, Harvard, MIT ve Princeton gibi üniversitelerdeki öğrenciler arasında bile oldukça yaygındır. TÜBİTAK tarafından desteklenen 120K639 No'lu "'İnfodemi' ile Etkin Mücadele için Bireylerin Yanlış Bilgi Karşısındaki Tutumlarının ve Bu Tutumların Belirleyicilerinin Araştırılması: Covid-19 Örneği" projesinde de bu sorunun benzeri, 18 yaş üstü nüfusu temsil eden 1629 kişilik bir Türkiye örneklemine sorulmuş, yalnızca %8,1'i soruyu doğru yanıtlamıştır. Çünkü zihnimiz, toplam fiyatı otomatik olarak 1,00 + 0,10 şeklinde ayırır. Bu hızlı ve sezgisel yanıt, sistem 1'in tipik bir ürünüdür. Araştırma sonuçlarına ulaşmak için:
🔗https://www.infodemiylemucadele.org/ana-sayfa/ara%C5%9Ft%C4%B1rman%C4%B1n-bulgular%C4%B1

❗ **Şimdi dur ve düşün (Sistem 2 devrede)**
Eğer top 10 sent olsaydı sopa 1,10 dolar olurdu. Toplam fiyat 1,20 dolar ederdi. Bu cevap yanlıştır.
✅ **Doğru Cevap: 5 sent: Sopa:** 1,05 dolar, Top: 0,05 dolar, Toplam: 1,10 dolar ✔
Bu basit deney, en zeki insanların bile ilk tepkilerinin yanıltıcı olabileceğini ve doğru sonuca ulaşmak için sistem 2'yi bilinçli olarak devreye sokmak, zihinsel bir *fren* yapmak gerektiğini açıkça gösterir.

Amigdala, beynin derinliklerinde yer alan, küçük ama etkisi büyük bir yapıdır. Evrimsel olarak beynin en eski bölümlerinden biri olan amigdala, karşılaştığımız durumların tehlikeli olup olmadığına hızla karar vermekle görevlidir. Günümüzde tehditler değişmiş olsa da bu yapı hâlâ aynı hayatta kalma mekanizmalarını işletir. Amigdalanın temel işi; korku, öfke, saldırganlık ve benzeri güçlü duyguları harekete geçirmektir. Bu yönüyle beynin alarm sistemi gibi çalışır. Bir durum riskli görünüyorsa, hemen uyarı verir. Bu

yapının en ayırt edici özelliği hızıdır. Gördüğümüz, duyduğumuz ya da okuduğumuz bilgiler, mantıklı düşünmeden sorumlu olan prefrontal kortekse ulaşmadan milisaniyeler önce amigdalada işlenir. Bu "kısa yol" sayesinde, potansiyel bir tehlike karşısında durup düşünmeden hemen tepki verebiliriz. Yolda hızla yaklaşan bir arabanın sesini duyduğumuzda refleksle geri çekilmemiz buna iyi bir örnektir.

Yanlış bilgi ve manipülasyon da tam olarak bu mekanizmayı hedef alır. Yabancı Bilgi Manipülasyonu ve Müdahalesi (*Foreign Information Manipulation and Interference-FIMI*) kapsamında yayılan "Ülke elden gidiyor!", "Ekonomik felaket yaklaşıyor!" ya da "Sana haksızlık yapılıyor!" gibi duygusu yüksek mesajlar, doğrudan amigdalayı uyarır. Bu mesajlar, çok kısa sürede beyinde "tehlike var" alarmını çalıştırır ve kontrolü hızlı ve duygusal tepkiler veren sistem 1'e bırakır.

KAVRAM: FIMI

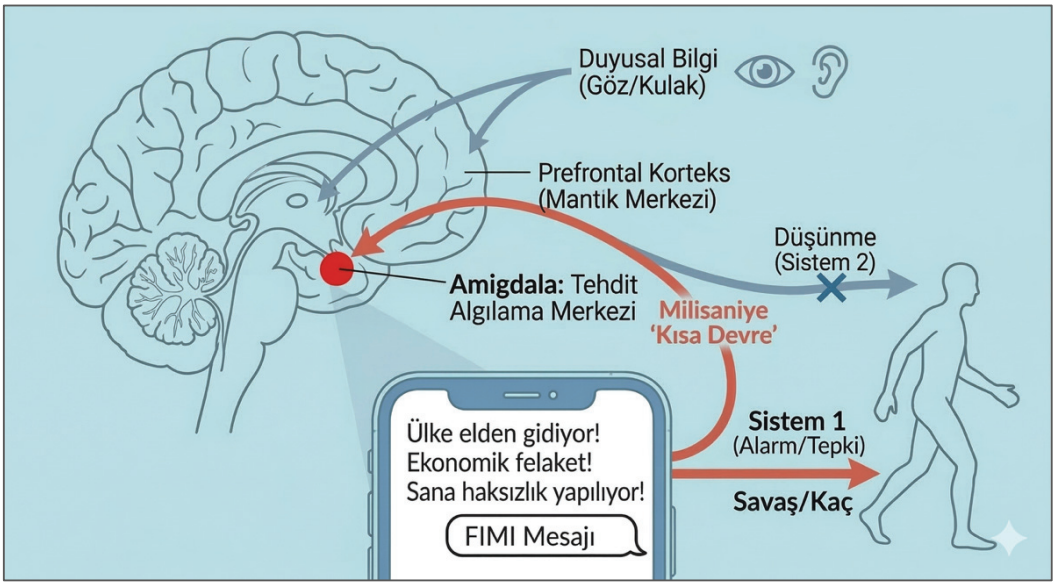
Neyi açıklar?: Yabancı Bilgi Manipülasyonu ve Müdahalesi (*Foreign Information Manipulation and Interference-FIMI*), çoğunlukla yasadışı olmayan yollarla, bir toplumun ya da ülkenin değerlerini, demokratik süreçlerini ve karar alma mekanizmalarını etkilemeyi veya zayıflatmayı amaçlayan bilgi temelli müdahaleleri tanımlar.

Neden önemli?: Amaç ikna etmekten çok, kafa karışıklığı yaratmak, güvensizlik üretmek ve toplumsal ayrışmayı derinleştirmektir.

Prefrontal korteks, alnımızın hemen arkasında yer alan ve beynin evrimsel olarak en son gelişmiş bölümüdür. Mantıklı düşünme ve kendimizi kontrol edebilme becerilerimizin merkezidir; bizi diğer canlılardan ayıran temel zihinsel işlevler burada yürütülür. Bu bölge; planlama, problem çözme, eleştirel düşünme, ahlaki değerlendirme ve özellikle dürtü kontrolünden sorumludur. Daniel Kahneman'ın tanımladığı sistem 2 tam olarak burada çalışır. Ancak prefrontal korteks yavaş çalışır ve çok enerji harcar. Bu yüzden beyin, çoğu zaman daha hızlı ve zahmetsiz olan duygusal tepkilere yönelir. PFK'nın en önemli görevi, amigdaladan gelen aşırı tepkileri düzenlemek ve sakinleştirmektir. Olan biteni

bağlam içinde değerlendirir ve şunu hatırlatır: *"Sakin ol, bu sadece bir haber; gerçek bir tehlike yok."*

Normalde beyin şöyle çalışır: Amigdala bir tehlike sinyali verir, prefrontal korteks bu sinyali değerlendirir ve uygun tepkiye karar verir. Ancak korku, öfke ya da aşırı heyecan çok yükseldiğinde bu denge bozulur. Amigdala kontrolü ele geçirir. Bu duruma "amigdalanın haczi", amigdalanın ele geçirmesi (*amygdala hijack*) denir. Psikolog Daniel Goleman'ın adlandırdığı bu durum, duyguların düşünmenin önüne geçmesi anlamına gelir.[9] Goleman, amigdalayı beynin "psikolojik nöbetçisi" olarak tanımlar.



Şekil 2.1.4 *Amigdala haczi ve sistem 1 tepkisi*

Bu nöbetçi hiç uyumaz ve sürekli şu ilkel soruyu sorar: "Bu nefret ettiğim bir şey mi? Bu beni incitir mi? Bundan korkmalı mıyım?" Eğer cevap "Evet" ise, amigdala anında alarm düğmesine basar. Normalde gözümüzden veya kulağımızdan gelen bir bilgi, önce beynin düşünen parçasına,

[9] Goleman, D. (1995). *Emotional intelligence bantam books.* New York.

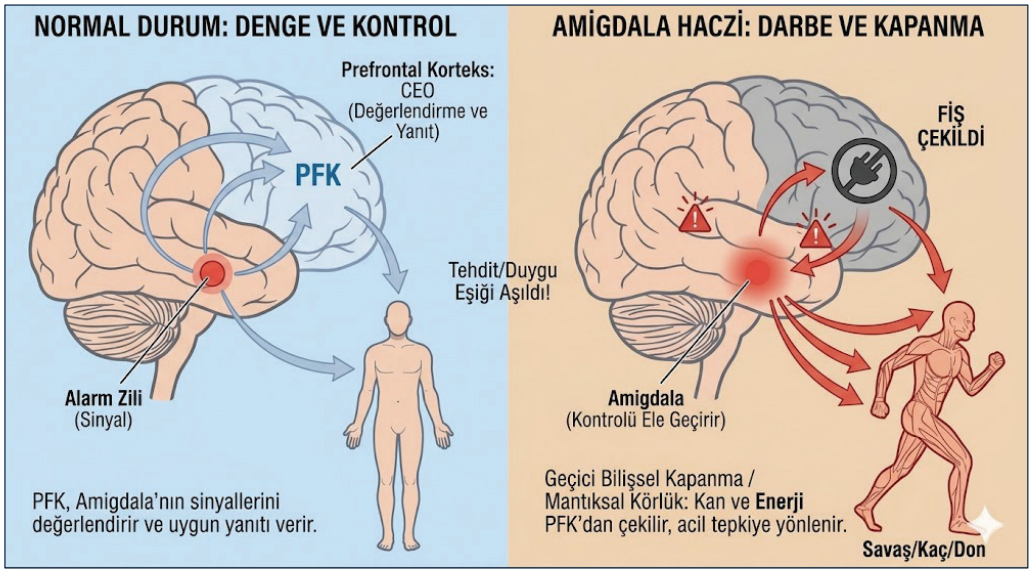
neokortekse gider, orada analiz edilir ve sonra tepki verilir. Ancak Goleman, beynimizde bir "sinirsel arka sokak" (*neural back alley*) olduğunu belirtir. Bu, çok hızlı çalışan bir kestirme yoldur. Tehdit anında bilgi, düşünen beyne uğramadan doğrudan bu kestirme yoldan amigdalaya gider. Amigdala, düşünen beyin henüz ne olduğunu bile anlamadan kontrolü ele geçirir; duygusal merkez, rasyonel merkezi devre dışı bırakıp yönetimi ele alır.

Dezenformasyon, FIMI veya manipülatif içerikler, basitçe bir yalan yaymaktan ibaret değildir. Aynı zamanda beynin duygusal tepkilerini hedef alan bir etki yaratmayı amaçlar. Temel hedef, amigdalayı harekete geçirerek mantıklı düşünmeden sorumlu olan prefrontal korteksi devre dışı bırakmaktır. Bu durumda kişi, bilginin kaynağını ya da doğruluğunu sorgulamaz. Korku, öfke veya panikle düşünmeden tepki verir; içeriği hızla paylaşır ya da aceleci kararlar alır. Bu yüzden dijital çağda bilgi okuryazarlığı, sadece bir düşünme becerisi değil, duyguların düşünmenin önüne geçmesini engelleyen bir savunma aracıdır.

İnsan beyni, iki yönlü bir işleve sahip olacak biçimde evrimleşmiştir. Sadece yiyecek bulma ve tehlikeden kaçınma gibi bireyin hayatta kalmasına yönelik süreçleri düzenlemekle kalmaz; aynı zamanda insanın bir grubun içinde uyumlu ve sürdürülebilir biçimde var olmasını da mümkün kılar. Primatların ve erken insan topluluklarının tarihinde, yalnız kalmak neredeyse kesin bir ölüm anlamına gelir.

Antropolog ve evrimsel psikolog Robin Dunbar'ın araştırmaları, bu sosyal zorunluluğun nörolojik bir yansımasını ortaya koymuştur. Dunbar'a göre, insan beyninin problem çözme, dil ve bilinçli düşünmeyle ilişkilendirilen en dış katmanı neokorteks kapasitesi, ortalama 150 kişilik bir sosyal grubu idare edebilecek şekilde sınırlandırılmıştır. Bu sayı, "Dunbar Sayısı" olarak bilinir. Dunbar Sayısı, bir kişinin gerçekten tanıdığı, güvendiği ve karşılıklı ilişki sürdürebildiği insan sayısını ifade eder. Tesadüf değildir; erken insan

topluluklarının ve avcı-toplayıcı kabilelerin büyüklüğü de yaklaşık bu kadardı. Bu sınır, grubun birlikte hareket etmesi, kaynakları paylaşması ve kendini savunması için hayatiydi.



Şekil 2.1.5 *Prefrontal korteksin devre dışı kalması ve amigdala haczi*

Avcı-toplayıcı çağda, 150 kişilik hayati kabilenizden dışlanmak, medeni dünyanın güvenli ağından kopmak, tek başına tehlikelerle dolu doğada kalmak demekti. Bu durum, çoğu zaman kesin bir ölüm anlamına geliyordu. Bu güçlü evrimsel baskı, insan beyninde derin bir iz bıraktı. Zamanla bilişsel mekanizmalarımız, katı gerçekler, sosyal uyumu, bir gruba ait olmayı önceleyecek şekilde şekillendi.

Grubun benimsediği ve hayatta kalmaya yaradığına inanılan bir yanlışa katılmak (örneğin "Kutsal ağaca dokunursak yağmur yağar, dokunmazsak kuraklık olur"), grubun dışında kalıp doğru ama işe yaramayan bir bilgiyi savunmaktan (örneğin "Bulut yok yağmur yağmayacak, ağacın bununla ilgisi yok") evrimsel olarak çok daha güvenliydi. Haklı olup yalnız kalmak yerine, yanlış bir inancı grupla birlikte paylaşarak hayatta kalmak, doğal seçilim açı-

sından daha avantajlıydı.

Günümüzde fiziksel kabilelerin yerini, dijital ve sanal kabileler aldı. Sosyal medyada binlerce kişilik gruplar, yankı odaları ve politik fanuslar içinde yaşıyoruz. İnsan beyninin eski uyarı sistemi bu ortamlarda da çalışmaya devam eder. Bir kişi, takipçilerinin ya da ait olduğu grubun benimsediği bir yalanı sorgulamayı hâlâ sosyal bir risk olarak algılar. Beyin bunu, kabileden dışlanmanın dijital bir karşılığı gibi yorumlar. Grubun paylaştığı ve aidiyeti güçlendiren bir yanlışı, doğruluk adına açıkça eleştirirseniz, "hain", "öteki" ya da "düşman" ilan edilmekten korkarsınız. Kısaca, dijital kabilenizden dışlanma tehdidi hissedersiniz. Bu korku, çoğu zaman doğruyu söyleme isteğini bastırır. Yanlış ya da duygusal olarak yüklü bir bilgiyi beğenmek veya paylaşmak, çoğu zaman gerçeği onaylamak anlamına gelmez. Daha çok, gruba verilen bir sadakat mesajıdır: "Ben sizdenim, sizinle aynı taraftayım." Bu davranışta, gerçeği arama isteğinden çok, gruba ait olma ihtiyacı öne çıkar.

📌 **ÖRNEK DENEY:** Asch'in Uyum Deneyi (1951)

Sosyal psikolog Solomon Asch, insanların grup baskısı karşısında gerçeği nasıl görmezden gelebildiğini gösteren ünlü bir deney yaptı. Deneyde katılımcılara açıkça farklı uzunlukta çubuklar gösterildi ve en uzun olanı seçmeleri istendi. Ancak odadaki diğer kişiler (deneyin parçası olan oyuncular) bilerek yanlış cevap verdiğinde, gerçek katılımcıların %75'i, kendi gözleriyle gördükleri doğruyu söylemek yerine grubun yanlış cevabına uydu.

Sonuç: İnsan, sosyal bir varlıktır. Yalnız kalmaktansa, yanılmayı tercih edebilir. Bugün dijital dünyada trend listeleri, beğeni sayıları ve paylaşım miktarları, bu grup baskısının modern karşılığıdır. Bir içerik milyonlarca kez beğenildiğinde, beyin otomatik olarak şunu düşünür: "Bu kadar kişi yanılıyor olamaz!"

Yanlış Bir Bilgiye İnanmakta Neden Israr Ederiz?

Bir önceki bölümde, insan beyninin enerji tasarrufu yapmak üzere evrimleşmiş bir yapı olduğunu gördük. Beyin, sınırlı enerjisini verimli kullanabilmek için çoğu zaman sezgisel kısa yollara başvurur. Bu kısa yollar, ayrıntılı düşünmek yerine deneyime ve örüntülere dayanır; hızlıdır ve çoğu durumda işe yarar. Atalarımız için bu hayatiydi: Tehlike anında hızlı karar vermek, kusursuz ama geç bir karardan daha değerliydi. Bu yönüyle kısa yollar, evrimsel bir başarıdır. Ancak modern dünyada koşullar değişti. Bugün karşı karşıya olduğumuz sorunlar artık ani fiziksel tehditler değil; yoğun bilgi akışı, karmaşık veri setleri ve sürekli maruz kaldığımız dijital içeriklerdir. Zihin bu yeni ortamda da aynı hız odaklı stratejileri kullanmaya devam eder. Sonuç olarak, karar verirken ve bilgi değerlendirirken aynı tür yanılgıları tekrar tekrar üretiriz. Bu bölüm, işte bu tekrar eden zihinsel yanılgıların neden ortaya çıktığını ve neden çoğumuzun kendini "ortalamanın üstünde" gördüğünü anlamaya odaklanmaktadır.

TEMEL ÇIKARIMLAR

Bu bölüm, modern dijital dünyada sıkça yanılmamızın sebebinin beynimizin binlerce yıllık evrimsel mirası olduğunu açıklar. Beynimiz, bilgi kıtlığının olduğu ve tehlikelerin aslan, yılan gibi somut olduğu taş devri koşulları için evrimleşmiştir. Ancak bugün, bu "eski donanımı" aşırı bilgi yüklemesi ve dijital uyaranlarla dolu modern bir dünyada kullanmaya çalışıyoruz. Bu durum, bilim insanlarının "evrimsel uyumsuzluk" dediği bir güvenlik açığı yaratır.

Temel Kavramlar ve Mekanizmalar

Sistem 1 ve Sistem 2: Nobel ödüllü Daniel Kahneman'a göre zihnimiz iki modda çalışır: Sistem 1, otopilot, hızlı, duygusal ve otomatiktir. Sistem 2, pilot modeli ise yavaş, mantıklı ve efor gerektirir. Enerji tasarrufu yapmak isteyen beynimiz, sosyal medyada gezinirken genellikle eleştirel sistem 2'yi kapatıp, duygusal sistem 1'i kullanır.

İnanmak Varsayılandır: Spinoza'nın öngördüğü ve modern bilimin doğruladığı üzere; beyin bir bilgiyi anladığı anda otomatik olarak "doğru" kabul eder. Onu reddetmek veya sorgulamak sonradan gelen, çaba gerektiren bir iştir. Yorgunken yalanlara daha çabuk inanmamızın sebebi budur.

Amigdala Haczi: Korku veya öfke içeren bir bildirim gördüğümüzde, beynin alarm merkezi amigdala yönetimi ele alır ve mantıklı düşünen bölgeyi prefrontal korteks devre dışı bırakır. Bu mekanizma bizi aslandan kaçarken kurtarır; ancak dijital dünyada düşünmeden "paylaş" butonuna basmamıza neden olur.

2.1. KENDİNİZİ TEST EDİN

Soru 1: Daniel Kahneman'ın zihin modeline göre; sosyal medyada gezinirken enerji tasarrufu yapmak amacıyla kullandığımız, hızlı, duygusal ve otomatik çalışan mekanizmaya ne ad verilir?

A) Prefrontal korteks

B) Sistem 2 (Pilot)

C) Sistem 1 (Otopilot)

D) Eleştirel muhakeme

Soru 2: Modern araştırmaların doğruladığı "Spinozacı model"e göre, insan beyni yeni bir bilgiyle karşılaştığında nasıl bir süreç izler?

A) Önce şüphe eder, kanıt arar, ikna olursa inanır.

B) Bilgiyi doğru kabul eder; reddetmek sonradan gelen bir çabadır.

C) Bilgiyi nötr bir veri olarak kaydeder.

D) Sadece daha önce duyduğu bilgilere inanır.

Soru 3: Dijital dünyada "Son dakika!" gibi korku veya öfke uyandıran bir içerik gördüğümüzde, mantıklı düşünme merkezi olan prefrontal korteks baskılayarak savaş ya da kaç tepkisini tetikleyen beyin bölgesi hangisidir?

A) Hipokampus

B) Amigdala

C) Neokorteks

D) Beyincik

2.1. MERAKLISINA EK KAYNAKLAR

Erdoğan, E., Uyan-Semerci, P., Eyolcu-Kafalı, B. ve Çaytaş, Ş. (2022). *İnfodemi ve bilgi düzensizlikleri: Kavramlar, nedenler ve çözümler*. İstanbul Bilgi Üniversitesi Yayınları.

Evans, J. St. B. T., Barston, J. L., & Pollard, P. (1983). On the conflict between logic and belief in syllogistic reasoning. *Memory & Cognition*, 11(3), 295-306.

First Draft. (2020). *Yanlış bilgi psikolojisi I: Neden savunmasızız?* (Teyit.org, Çev.). https://teyit.org/files/yanlis-bilgi-psikolojisi-first-draft.pdf

Gow, J. (2013). *Normalcy bias and disaster preparedness*. Journal of Emergency Management, 11(2), 123-131.

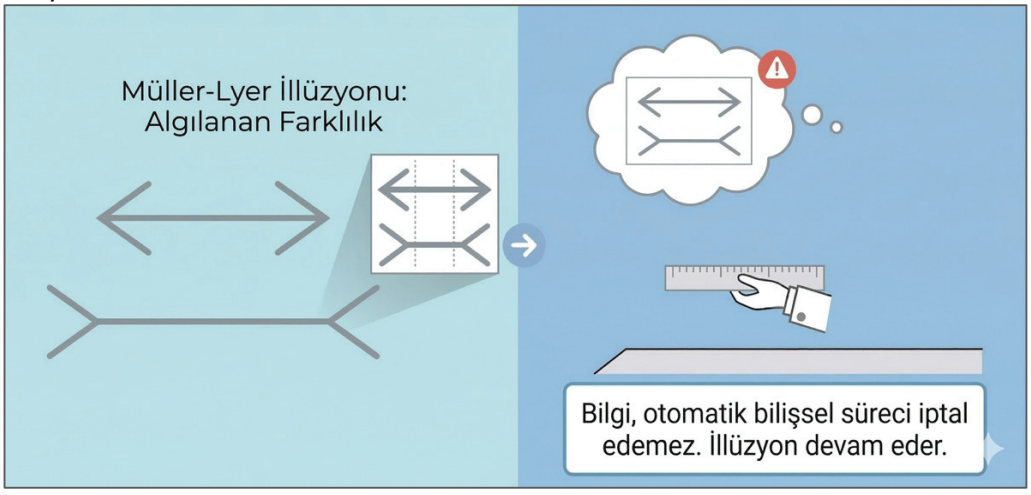
Gürcan, T. (2014). *Asch'in uyum deneyi: Çıkıntı olmamak adına hizaya girmenin psikolojisi*. Evrim Ağacı. https://evrimagaci.org/aschin-uyum-deneyi-cikinti-olmamak-adina-hizaya-girmenin-psikolojisi-2421

Slovic, P., Finucane, M., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, 177(3), 1333–1352.

Bilişsel Önyargı Nedir?

Bilişsel önyargılar, basit hatalardan ya da anlık dikkatsizliklerden farklıdır. Bir hesap hatası yapabilir veya dalgınlıkla yanlış bir karar verebiliriz; bunlar rastgele ve geçicidir. Bilişsel önyargılar ise tesadüf değildir. Zihnimizin çalışma biçimine yerleşmiş, herkeste görülen ve tekrar eden düşünme sapmalarıdır. Bu yüzden kişisel zayıflık değil, insan olmanın ortak bir özelliğidir.

Önyargıların nasıl çalıştığını anlamak için göz yanılmalarına, optik illüzyonlara bakmak yeterlidir. Örneğin Müller-Lyer illüzyonunda, aynı uzunluktaki iki çizgi, üzerlerindeki oklar nedeniyle farklı görünür. Bunun bir yanılsama olduğunu bilseniz bile, çizgiler gözünüze hâlâ farklı uzunlukta görünür. Çünkü beyin, mesafe ve derinliği algılarken otomatik olarak böyle çalışır. Bilişsel önyargılar da aynıdır. Nasıl işlediklerini bilmek onları tamamen ortadan kaldırmaz. Zihin, bilgimizden bağımsız olarak, bu otomatik kalıpları üretmeye devam eder.



Şekil 2.2.1 *Müller-Lyer illüzyonu analojisi: Bilişsel önyargıların kalıcılığı*

Bilişsel önyargılar, dezenformasyon yayan kişi ve gruplar için çok güçlü araçlardır. Kötü niyetli aktörler, troller ya da dolandırıcılar insanların zihnine zorla girmeye çalışmaz. Bunun yerine, önyargıları bir Truva atı gibi

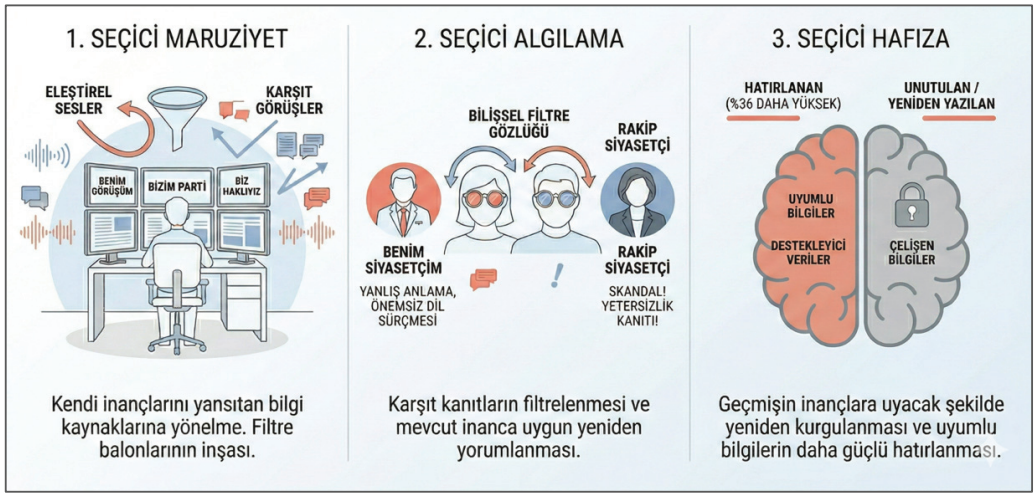
kullanırlar. Özetle, kapıyı dışarıdan kırmaz, kişinin o kapıyı kendi isteğiyle açmasını sağlarlar. Bu aktörler insan psikolojisinin basit bir kuralını iyi bilir: En ikna edici yalan, zaten inanmak istediğimiz yalandır. Bu yüzden dezenformasyon çoğu zaman açık bir kandırma gibi değil, "zaten bildiğini doğrulayan" bir bilgi gibi sunulur. Kişinin duygularına, inançlarına ya da kimliğine hitap eden anlatılar öne çıkarılır. Böylece akılcı sorgulama devre dışı kalır. Bilişsel önyargılar, bu sürecin hem zeminini hazırlar hem de yanlış bilginin hızla yayılmasını tetikler. Bu bölümde, insan zihninin en kritik yedi temel önyargısını analiz edeceğiz. Bu önyargıları tanımak, zihinsel savunma sistemimizi inşa etmenin ilk ve en hayati adımıdır.

Doğrulama Yanlılığı (Confirmation Bias): Tüm Önyargıların Temeli

Doğrulama yanlılığı, insanların kendi inançlarını, düşüncelerini ya da görüşlerini destekleyen bilgilere daha kolay yönelmesi ve bu bilgileri daha çabuk kabul edip hatırlamasıdır. Buna karşılık, inandıklarımızla çelişen bilgiler çoğu zaman görmezden gelinir, önemsizleştirilir ya da reddedilir. Bu nedenle doğrulama yanlılığı, karar verme süreçlerini en güçlü biçimde etkileyen ve en yaygın görülen bilişsel önyargılardan biridir. Bu durum, beynimizin dünyayı tarafsız biçimde kaydetmediğini gösterir. Zihin, dış gerçekliği olduğu gibi aktaran bir kamera gibi çalışmaz. Aksine, neye inanmak istiyorsa onu seçer, rahatsız edici bilgileri dışarıda bırakır ve böylece kendine ait bir "gerçeklik" oluşturur. Bu psikolojik süreç genellikle üç temel aşamada işler ve zamanla inanç sistemimizin giderek daha sağlam ve sorgulanmaz hâle gelmesine hizmet eder. İlk aşama seçici maruz kalmadır (*selective exposure*). Kişi, daha bilgiyle karşılaşma noktasında bile kendi görüşlerini destekleyen kaynaklara yönelir. Örneğin belirli bir siyasi görüşe sahip olan biri, o görüşü onaylayan yayınları takip ederken karşıt sesleri kapatır ya da bilinçli biçimde görmezden gelir. Bu alışkanlık zamanla bireyi, yalnızca kendi inançlarını yansıtan

içeriklerle çevreleyen yankı odaları ve filtre balonları içine hapseder. Sonuçta kişi, farklı bakış açılarıyla temasını giderek kaybeder.

İkinci aşama seçici algılamadır (*selective perception*). Bu aşamada kişi, kendi görüşleriyle çelişen bir bilgiyle karşılaştığında onu olduğu gibi kabul etmek yerine, zihinsel bir filtreden geçirerek yeniden yorumlar. Desteklenen bir siyasetçinin ciddi bir hatası "yanlış anlaşılma" ya da "önemsiz bir dil sürçmesi" olarak açıklanırken, karşıt görüşteki birinin küçük bir hatası hızla "büyük bir skandal" ya da "yetersizlik" olarak etiketlenir. Kanıt ne kadar güçlü olursa olsun, zihin önce mevcut inancı korumayı tercih eder. Böylece bilgi, gerçeği anlamak için değil, inancı savunmak için kullanılır.



Şekil 2.2.2 *Doğrulama yanlılığı döngüsü*

Üçüncü ve son aşama ise seçici hafızadır (*selective memory*). Bu noktada zihin, geçmişte öğrenilen bilgileri ve yaşananları mevcut inançlara uyacak şekilde hatırlar. Kendi görüşümüzü destekleyen bilgiler daha net ve kalıcı biçimde akılda kalırken, çelişen bilgiler hızla silinir. Araştırmalar, insanların kendi inançlarıyla uyumlu bilgileri, karşıt bilgilere kıyasla daha iyi hatırladığını göstermektedir. Böylece zihin yalnızca bugünü değil, geçmişi de

inançlarını doğrulayacak biçimde yeniden kurar; inançlar zamanla hem algımızı hem de hafızamızı şekillendiren güçlü bir çerçeveye dönüşür.

Doğrulama yanlılığı yalnızca siyaset ya da kişisel inançlarla sınırlı değildir; bilimsel çalışmalardan günlük kararlara, işe alımdan yatırım tercihlerine kadar pek çok alanda hatalara yol açar. Bu önyargının farkına varmak, daha eleştirel düşünmenin ve daha objektif kararlar almanın ilk ve en önemli adımıdır. Kutuplaşmış toplumlarda doğrulama yanlılığı, masum bir "fikir ayrılığı" olmaktan çıkar ve kolektif bir gerçeklik bölünmesi yaratır. Bu yalnızca siyasi tercihlerde ayrışmak değildir; aynı toplumda yaşayan insanların, aynı olayları bambaşka anlamlandırması, farklı gerçeklik setleriyle yaşaması demektir. Toplumsal dokuyu zayıflatan temel mekanizmalardan biri budur.

İstanbul Bilgi Üniversitesi bünyesinde faaliyet gösteren TurkuazLab'ın 2020 yılında yayımladığı "Türkiye'de Kutuplaşmanın Boyutları" başlıklı kapsamlı araştırma, bu gerçeklik bölünmesinin Türkiye'de ne denli derin sosyal bölünmelere yol açtığını çarpıcı sosyo-ekonomik verilerle kanıtlamaktadır. Bulgular, kutuplaşmanın yalnızca siyasetle sınırlı kalmadığını; gündelik hayatın ve özel ilişkilerin içine kadar sızdığını göstermektedir. Araştırmadan öne çıkan veriler, siyasi kutuplaşmanın zamanla rasyonel bir fikir ayrılığından çıkıp duygusal bir kopuşa dönüştüğünü ortaya koymaktadır: Türkiye'deki katılımcıların neredeyse dörtte üçü (%74,9), çocuklarının kendi siyasi görüşlerine uzak bir partinin destekçisiyle evlenmesini onaylamamaktadır. Bu oran, kutuplaşmanın artık basit bir fikir ayrılığının ötesine geçtiğini; karşı gruba yönelik derin bir güvensizlik, düşmanlık ve hatta nefret hissine, duygusal kutuplaşmaya dönüştüğünü ortaya koyar. Siyasi kimlik, bu noktada bireylerin özel hayatına kadar girerek, aile kurma gibi en temel ve kişisel kararlarda bile güçlü bir engel hâline gelmiştir. Katılımcıların üçte ikisinden fazlası (%66), kendileriyle farklı siyasi görüşe sahip kişilerle iş yapmayı ya da komşu olmayı istememektedir. Bu durum, toplumda hem mekânsal hem de

ekonomik bir ayrışmanın güçlendiğini göstermektedir. Farklı siyasi gruplar, kendi mahallelerini ve iş çevrelerini oluşturarak birbirleriyle temas ettikleri alanları giderek daraltmaktadır. Temasın azalması ise insanların yalnızca kendi görüşlerini duymasına yol açan yankı odalarını güçlendirmekte ve doğrulama yanlılığını beslemektedir.

Sosyolojik ve demografik veriler, toplum içinde farklı mahalleler, yaşam tarzları ve sosyo-ekonomik gruplar arasındaki temasın giderek azaldığını açıkça göstermektedir. İnsanlar artık kendilerinden farklı olanlarla daha az konuşmakta, daha az yan yana gelmekte ve ortak alanları daha az paylaşmaktadır. Bu fiziksel ve sosyal ayrışma, doğrulama yanlılığının yalnızca bireysel bir düşünme alışkanlığı olmaktan çıkıp toplumsal bir silaha dönüşmesi için uygun bir zemin yaratır. "Öteki" ile konuşmadığınız, birlikte çalışmadığınız, aynı mahallede yaşamadığınız ve en temel sosyal bağları bile kurmadığınız durumlarda, kişinin kendi inançlarını sorgulamasını sağlayacak karşılaşmalar da ortadan kalkar. Böyle bir ortamda doğrulama yanlılığı, rakipsiz hâle gelir. Çünkü zihni sarsacak, alışılmış düşünceyi zorlayacak hiçbir dış etken kalmaz. Bu noktadan sonra doğrulama yanlılığı, toplumsal kutuplaşmayı besleyen üç aşamalı bir döngü halinde işlemeye başlar. İlk aşamada birey, sosyal, fiziksel ve dijital alanlarda giderek daralan bir çevrenin içine çekilir. Medya alışkanlıkları, arkadaş çevresi ve gündelik tercihler, kişinin zaten inandığı görüşleri sürekli olarak doğrulayan bir yankı odası yaratır. Bu ortamda birey yalnızca kendi grubunun sesini duyar, onaylanır ve desteklendiğini hisseder. Zamanla bu yankı odası, dışarıdan gelen

🔍 **KAVRAM:** YANKI ODALARI

Neyi açıklar?: Yankı odaları (*eco-chambers*) kavramı, bireylerin çoğunlukla kendi inanç ve görüşleriyle uyumlu bilgi ve fikirlerle karşılaştığı, farklı bakış açılarının ise dışlandığı iletişim ortamlarını ifade eder.

Neden önemli?: Bu ortamlar, yanlış bilgilerin sorgulanmadan tekrar edilmesini kolaylaştırırken kutuplaşmayı derinleştirir ve eleştirel düşünmeyi zayıflatır.

eleştirilere ve farklı bilgilere karşı bir bilişsel kalkan işlevi görür; kişi hem neye inanacağını hem de neyin "gerçek" olduğunu grubun normlarına göre belirlemeye başlar.

İkinci aşamada, bu kapalı yapı içinde karşıt görüşlerden gelen bilgiler otomatik olarak reddedilir. Farklı bir siyasi görüşten, başka bir toplumsal gruptan ya da "öteki" olarak görülen bir kaynaktan gelen bilgi, içeriğine bakılmaksızın geçersiz sayılır. Bu bilginin bilimsel bir çalışmaya, resmî bir rapora ya da doğrudan bir tanıklığa dayanması sonucu değiştirmez; belirleyici olan bilginin kimden geldiğidir. Bu aşamada bilgi, akılcı bir değerlendirmeden geçmez; duygusal ve ideolojik filtrelerden süzülerek "yalan", "manipülasyon" ya da "gruba yönelik bir saldırı" olarak etiketlenir. Böylece eleştirel düşünme geri plana itilir.

Üçüncü ve son aşamada ise bu döngü, bireyin kendi grubunun anlattığı hikâyeyi tek ve tartışılmaz bir gerçeklik olarak benimsemesiyle tamamlanır. "Gerçeklik" artık farklı bakış açılarını buluşturan ortak bir zemin olmaktan çıkar; grubun değerleri, korkuları ve kabulleri etrafında inşa edilen kapalı bir anlatıya dönüşür. Bu durum, karşıt grupların yaşam deneyimlerini, somut sorunlarını ve meşru taleplerini görünmez kılar. Zamanla empati zayıflar, gruplar arasındaki mesafe derinleşir ve toplumsal kutuplaşma, kalıcı bir gerçeklik uçurumuna dönüşür.

Bu noktada doğrulama yanlılığı, yalnızca bireysel bir düşünme hatası ya da algı yanılgısı olmaktan çıkar. Toplumsal kutuplaşmayı sürekli besleyen, güveni, empatiyi ve ortak gerçeklik duygusunu zayıflatan güçlü ve tehlikeli bir toplumsal mekanizmaya dönüşür. Böylece doğrulama yanlılığı hem toplumsal ayrışmayı besler hem de bireyleri kendi inanç sistemleri içinde giderek daha katı ve dışa kapalı bir zihinsel alana hapseder.

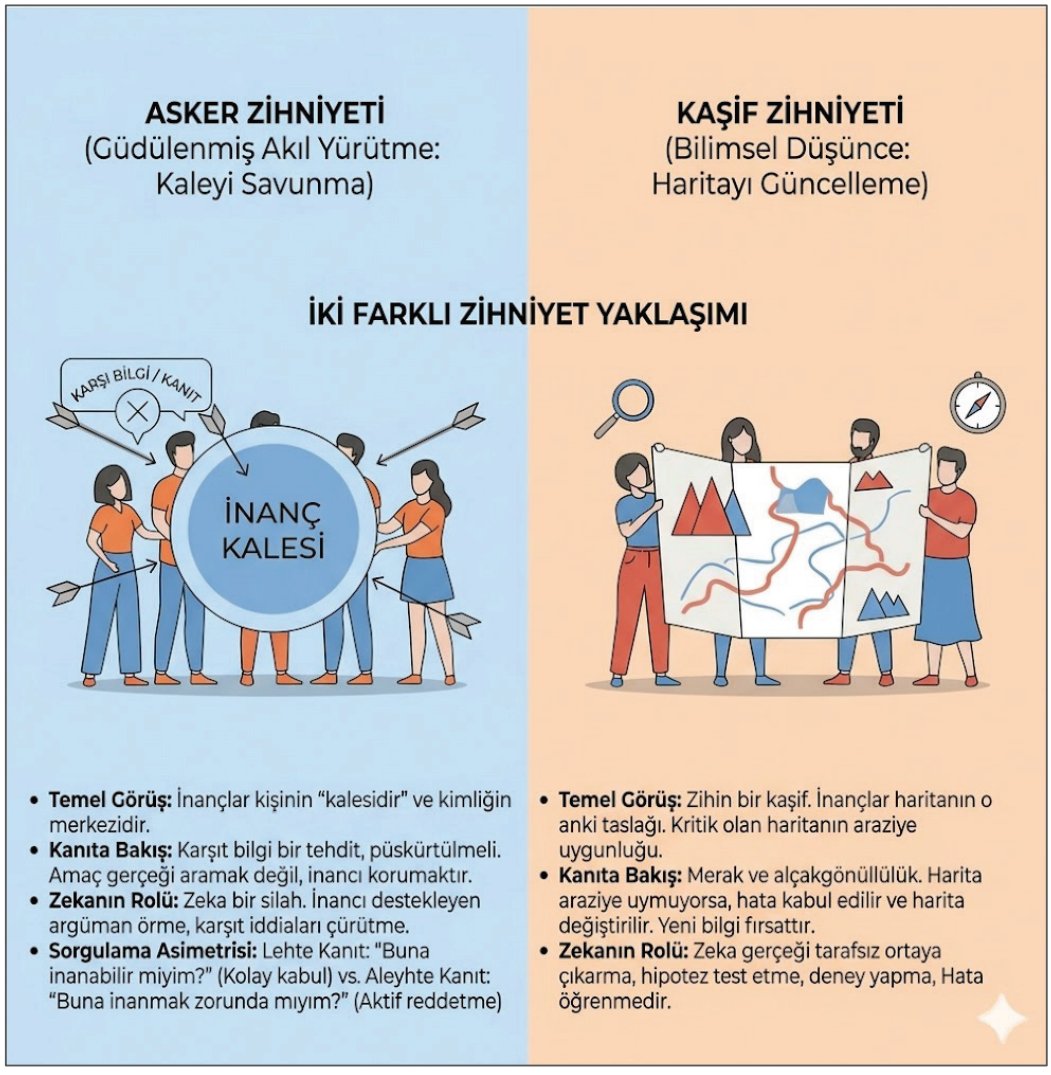
Güdülenmiş Muhakeme

Güdülenmiş muhakeme, doğrulama yanlılığının daha güçlü ve daha aktif bir biçimidir. Bu durumda insanlar sadece duymak istediklerini seçmez; aynı zamanda sahip oldukları inançları korumak için düşünme becerilerini bilinçli biçimde kullanırlar. Siyasi görüşler, kimlikler ya da dünya görüşleri tehdit altındaysa, zekâ ve mantık gerçeği anlamak için değil, bu inançları savunmak için devreye girer. Bu bir düşünce tembelliği değildir. Aksine, zihnin yoğun biçimde çalıştığı bir süreçtir. Ancak amaç gerçeği bulmak değil, zaten inanılan şeyi haklı çıkarmaktır. Beyin bu noktada bir araştırmacı gibi değil, bir savunma avukatı gibi davranır.

Bilişsel bilimci Julia Galef, insan zihninin bilgiyle karşılaştığında iki farklı modda çalışabildiğini söyler. Bu iki zihinsel yaklaşım, yalnızca neye inandığımızı değil, gerçeğe nasıl baktığımızı ve yeni bilgilerle nasıl ilişki kurduğumuzu da belirler. Galef bu yaklaşımları "asker zihniyeti" ve "kâşif zihniyeti" olarak adlandırır.[10] Asker zihniyetinde, inançlar korunması gereken birer kale gibidir ve kişinin kimliğinin merkezinde yer alır. Bu modda zihin, gerçeği anlamaya değil, mevcut inançları savunmaya odaklanır. Karşıt bilgiler bir tehdit olarak algılanır; önemli olan bu tehdidi bertaraf etmektir. Zekâ, gerçeği keşfetmek için değil, inancı savunmak için kullanılır. Kişi, kendi görüşünü destekleyen bilgilerle karşılaştığında "Buna inanabilir miyim?" diye sorarken, ters düşen bilgiler karşısında "Buna inanmak zorunda mıyım?" sorusuna sığınır. Bu nedenle en küçük bir gerekçe bile karşıt bilgiyi reddetmek için yeterli hâle gelir. Kâşif zihniyetinde ise zihin, dünyayı daha iyi anlamaya çalışan bir keşif aracıdır. İnançlar, mutlak doğrular olarak değil, gerektiğinde güncellenebilecek geçici haritalar olarak görülür. Bu yaklaşımda merak ve alçakgönüllülük ön

[10] Galef, J. (2021). *The scout mindset: Why some people see things clearly and others don't*. Penguin.

plandadır; eğer mevcut harita gerçeklikle uyuşmuyorsa, değiştirilmesi doğal kabul edilir. Zekâ savunma yapmak için değil, anlamak için kullanılır; hipotezler test edilir, veriler incelenir. Yanılmak bir tehdit değil, öğrenmenin bir parçasıdır ve yeni bilgiler, inançları güncellemek için bir fırsat olarak görülür.



Şekil 2.2.3 *Bilgiye yaklaşımda iki farklı zihniyet modeli (Julia Galef)*

Sanılanın aksine, zeki olmak bilişsel önyargılardan korunmayı garanti

etmez. Araştırmalar, özellikle matematiksel ve analitik becerileri yüksek kişilerin, kendi siyasi ya da kimlik temelli inançlarıyla çelişen bilgileri "mantıklı" gerekçelerle açıklama ve kendi görüşlerine uydurma konusunda daha becerikli olduğunu gösteriyor. İklim krizi, aşılar ya da silah kontrolü gibi konularda sunulan veriler, bu kişiler tarafından reddedilmez; aksine ustaca yeniden yorumlanır. Bu durum, zekânın gerçeği bulmak için değil, inanılan şeyi savunmak için kullanılması anlamına gelir. Zeki bireyler, yanlış ya da önyargılı düşüncelerini haklı çıkarmak için daha karmaşık, daha ikna edici ve hatta "bilimsel" görünen açıklamalar üretebilir. Böylece zekâ, önyargıların panzehiri olmak yerine, onları daha güçlü ve daha görünmez hâle getiren bir yakıta dönüşür. Bu nedenle güdülenmiş muhakeme, insanı bilgisizliğinden değil, tam tersine bilişsel yeteneklerinden vurur. Kişi, kendi zekâsının kurbanı haline gelebilir.

Yanıltıcı Doğruluk Etkisi

"Bir yalanı yeterince sık tekrarlarsan, gerçek olur." Bu söz, sadece Nazilerin baş propagandacısı Joseph Goebbels'e atfedilen karanlık bir ilke veya George Orwell'in distopik eseri *1984*'ten çarpıcı bir alıntı değildir. Aynı zamanda modern nörobilim ve sosyal psikolojinin defalarca ortaya koyduğu evrensel bir bilişsel gerçeği özetler. İnsan zihni bilgiyi değerlendirirken, çoğu zaman mantıksal sorgulamadan çok tekrarın yarattığı tanıdıklığa dayanır; tekrar edilen bilgi, doğru olup olmadığına bakılmaksızın daha inandırıcı hale gelir.

1977 yılında Lynn Hasher, David Goldstein ve Thomas Toppino tarafından yapılan "yanıltıcı doğruluk etkisi" (*illusory truth effect*) deneyinde, katılımcılara farklı konularda bazıları doğru, bazıları ise açıkça yanlış olan bilgi cümleleri sunuldu.[11] Haftalar boyunca yapılan tekrar testlerinde dikkat çekici

[11] Hasher, L., Goldstein, D., & Toppino, T. (1977). Frequency and the conference of referential validity. *Journal of verbal learning and verbal behavior*, *16*(1), 107-112.

bir sonuç ortaya çıktı: Katılımcılar, başlangıçta yanlış ya da şüpheli buldukları ancak tekrar tekrar karşılaştıkları yanlış bilgileri, daha önce hiç görmedikleri doğru bilgilere kıyasla zamanla daha doğru, daha güvenilir ve daha inandırıcı olarak değerlendirmeye başladı. Bu bulgu, zihnin "tekrar edilen bilgi gerçeğe yakındır" şeklinde işleyen güçlü bir kısa yol kullandığını açıkça gösterir. Tekrarın bu etkisinin temelinde işleme akıcılığı adı verilen basit bir mekanizma var. İnsan beyni enerji tasarrufu yapmayı sever. Daha önce karşılaşılan bir bilgiyi işlerken daha az çaba harcar ve daha hızlı çalışır. Tekrarlanan bilginin zihindeki yolları adeta pürüzsüzleşir. Beyin bu kolaylığı yanlış yorumlar. "Bu bilgiyi hızlı ve zorlanmadan işledim" hissi, zihinde şu sonuca dönüşür: "Demek ki bu bilgi tanıdık, güvenli ve muhtemelen doğru." Böylece tanıdıklık, farkında olmadan doğrulukla eş anlamlı hale gelir.

👉 DENE

Şimdi dürüstçe aşağıdaki durumu düşünün: Çok sevdiğiniz, güvendiğiniz ve oy verdiğiniz bir siyasetçi hakkında, yolsuzluk yaptığını gösteren güçlü ve açık bir kanıt (örneğin, net bir ses kaydı ya da video) ortaya çıkıyor. İlk tepkiniz hangisi olur?

A) "Demek ki yanılmışım. Bu kanıt çok açık, inkâr edilemez."
B) "Bu kesinlikle montaj. Yapay zekâ ile üretilmiş olabilir. Bu, bize karşı kurulan bir komplo."

Eğer cevabınız **B** ise, bu güdülenmiş muhakemenin tipik bir örneğidir. Büyük olasılıkla aynı kanıt, sizin karşı olduğunuz bir siyasetçi için ortaya çıksaydı, bu kez "Zaten belliydi, işte kanıtı" demekte bu kadar zorlanmazdınız. Bu örnek bize şunu gösterir: Zihin, çoğu zaman kanıtın ne kadar güçlü olduğuna göre değil, o kanıtın bizim kimliğimizle ve inançlarımızla nasıl bir ilişki kurduğuna göre çalışır. İnancı tehdit eden bilgi reddedilir; inancı destekleyen bilgi ise sorgulanmadan kabul edilir.

Sosyal medyada yürütülen FIMI operasyonlarının en temel ve sinsi yöntemi, tekrar yoluyla tanıdıklık yaratmaktır. Bu amaçla binlerce sahte hesap (botlar ya da ücretli trol ağları), aynı yalanı eş zamanlı ve defalarca paylaşır.

"Seçimlerde büyük hile var", "X kişisi haindir" ya da "Aşılar kısırlığa neden oluyor" gibi iddiaların sürekli karşımıza çıkmasının nedeni budur. Bu yöntem, psikolojide maruz kalma etkisi olarak bilinen mekanizmayı bilinçli biçimde kullanır. Bu tür operasyonların amacı sizi mantıklı argümanlarla ikna etmek değildir. Çünkü yalanlar çoğu zaman kanıtla savunulamaz ve kolayca çürütülür. Asıl hedef, yanlış bilgiyi sürekli tekrar ederek zihne aşina hale getirmektir. Aynı cümleyi defalarca görmek ve duymak, beynin onu daha kolay işlemesine yol açar. Beyin ise bu kolaylığı, "Bu bilgi tanıdık ve dolayısıyla güvenilir olabilir" şeklinde yorumlar. Zamanla insanlar, bu bilginin ilk kaynağını unutmaya başlar. Buna "kaynak amnezisi" denir. Bilgiyi kimin paylaştığı silinir; ancak içerik ve yarattığı "doğruymuş" hissi zihinde kalır. Böylece yalan, mantıklı bir iddia olmaktan çıkar ve sezgisel bir "doğru"ya dönüşür. Bilişsel bilimde bu sürece "yanıltıcı doğruluk etkisi" denir. Sonuçta yanlış bilgi, akılcı değerlendirmeyi aşarak duygusal ve sezgisel karar sistemine yerleşir. Bu da toplumsal kutuplaşmayı artırır ve demokratik süreçlere duyulan güveni adım adım zayıflatır.

Kolaydaki Bilişsel Kısa Yol

Bilişsel psikologlar Daniel Kahneman ve Amos Tversky'nin tanımladığı "kolaydaki bilişsel kısa yol" (*availability heuristic*), karar verirken sıkça kullandığımız temel zihinsel kısa yollardan biridir[12]. İnsan beyni bir olayın ne kadar sık yaşandığını ya da ne kadar riskli olduğunu hesaplarken, istatistiklere bakmak yerine o olayın hafızada ne kadar kolay ve hızla canlandığına bakar. Aklımıza hızlı gelen, bize daha olasıymış gibi görünür. Örneğin uçak kazaları son derece nadirdir; ancak medyada uzun süre yer alır, dramatik görüntüler ve duygusal hikâyelerle anlatılır. Buna karşılık araba kazaları çok daha sık

[12] Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5*(2), 207-232.

yaşanır ama çoğu zaman haber bile olmaz. Bu zihinsel kısa yol nedeniyle insanlar uçuştan korkar ve uçakla seyahat etmeyi riskli bulur, oysa arabayla günlük seyahat riskini umursamaz. İstatistikler, havalimanına giderken yolda araba kazasında ölme ihtimalinin, uçak içinde ölme ihtimalinden katbekat fazla olduğunu gösterse bile, beynimiz en canlı ve duygusal anıları referans alır.

İletişim bilimci George Gerbner'in geliştirdiği "acımasız dünya sendromu", dijital çağda sosyal medya algoritmalarıyla birleştiğinde çok daha güçlü ve yıkıcı bir etki yaratır. Gerbner, televizyonda sürekli şiddet içeriğine maruz kalan kişilerin, suç oranları gerçekte düşse bile, dünyayı olduğundan daha tehlikeli ve acımasız algıladığını göstermiştir.[13] Sosyal medya bu etkiyi daha da artırır. TikTok, X (Twitter) ve Instagram gibi platformlar, kullanıcıların dikkatini çekmek için öfke, korku ve tehdit içeren içerikleri öne çıkarır. Eğer bir kişinin akışında sürekli sokak kavgaları, suç videoları, ekonomik felaket haberleri ya da polis şiddeti görüntüleri varsa, beyin bu yoğun ve kaotik içerikleri genelleyerek tüm topluma yayar. İstatistiklere bakmadan şu sonuca varır: "Suç oranları patladı, toplum çöktü, ülke yaşanmaz halde, her yer kaos ve güvensizlik." Oysa gerçek durum çok farklı olabilir. Suç oranları düşüyor, ekonomik göstergeler iyileşiyor ya da genel tablo istikrarlı olabilir. Ancak doğrulama yanlılığı, ekranda sık gördüğümüz olayları dünyanın tamamı sanmamıza yol açar. Bu algı, toplumsal güveni zedeler, korkuyu büyütür ve kutuplaşmayı derinleştiren, panik duygusuyla verilen kararların önünü açar.

[13] Gerbner, G., & Gross, L. (1976). Living with television: The violence profile. *Journal of Communication, 26*(2). https://doi.org/10.1111/j.1460-2466.1976.tb01397.x; Gerbner, G. (1998). Cultivation analysis: An overview. *Mass communication and society*, *1*(3-4), 175-194.

Dunning-Kruger Etkisi

1999 yılında Cornell Üniversitesi psikologları Justin Kruger ve David Dunning tarafından bilimsel olarak tanımlanan Dunning-Kruger etkisi,[14] insan zihninin en çarpıcı ve trajik hatalarından birini ortaya koyar: "Bir konuda yetersiz, deneyimsiz veya bilgisiz olan kişiler, sadece o konuda başarısız olmakla kalmaz, aynı zamanda kendi yetersizliklerini fark edecek bilişsel kapasiteden de yoksundurlar."

Gündelik dilde sıkça "cahil cesareti" olarak adlandırılan bu durum, bilgi düzeyi ile özgüven arasında ters bir ilişki olduğunu gösterir. Bir konuyu örneğin aşılar, ekonomi ya da dış politika gibi karmaşık alanlarda yüzeysel biçimde bilen kişiler, çoğu zaman konuyu tamamen çözdüklerini, hatta uzmanlardan daha iyi anladıklarını düşünürler. Bunun temel nedeni, bilginin ne kadar derin, karmaşık ve çok katmanlı olduğunu görememeleridir. Kısacası, "bilmediklerini bilmezler." Buna karşılık, yıllarını aynı alana adamış gerçek uzmanlar genellikle daha temkinli konuşur. "Kesin" ifadeler yerine "olasılıklar", "sınırlılıklar" ve "belirsizlikler" üzerinde dururlar. Ancak bu dikkatli ve ölçülü dil, çoğu zaman dışarıdan bakıldığında kararsızlık ya da özgüven eksikliği gibi algılanabilir. Böylece, en çok bilenler en az emin görünenler olurken; en az bilenler en yüksek özgüveni sergileyenler hâline gelir.

Dijital çağda bilgiye ulaşmak hiç olmadığı kadar kolaylaştı. Ancak bu kolaylık, Dunning–Kruger etkisini daha da güçlendiren yeni bir sorunu beraberinde getirdi: epistemik kibir, bilgiye dair aşırı özgüven. İnternet; özellikle YouTube, TikTok ve bloglar aracılığıyla, karmaşık konular hakkında kısa, basitleştirilmiş ve yüzeysel bilgiler sunar. Bir kişi, yalnızca 10–15 dakikalık "Büyük resmi öğrenin" ya da "Gerçekleri kimse söylemiyor" başlıklı bir video

[14] Kruger, J., & Dunning, D. (1999). Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*, *77*(6), 1121.

izledikten sonra, kendini virolojiye, ekonomiye ya da tarihe yıllarını vermiş bir uzmandan daha bilgili sanabilir. Bu noktada uzmanlara karşı şu tür bir tavır gelişir: "Sen gerçeği bilmiyorsun, sistemin içindesin; ben kendi araştırmamı yaptım." Dezenformasyon tam da bu özgüven üzerine kurulur. Pandemi, iklim krizi, ekonomik kriz ya da savaş gibi karmaşık ve belirsizlik içeren konulara; basit, kesin, duygusal ve suçlayıcı açıklamalar sunar. Bu tür anlatılar, Dunning–Kruger etkisini besler ve güçlendirir. Belirsizliğe tahammülü olmayan zihnimiz, çok katmanlı ve olasılıklar içeren bilimsel açıklamalar yerine, "Her şey gizli güçlerin oyunu" gibi net, iddialı ve özgüvenli yalanlara daha kolay inanır. Çünkü bu tür açıklamalar düşünmeyi değil, rahatlamayı vaat eder.

Devam Eden Etki

Dezenformasyonla mücadelede gazetecilerin ve teyitçilerin en çok zorlandığı durumlardan biri şudur: Bir yalan ortaya atıldıktan sonra, bu yalan çürütülse bile zihindeki etkisi tamamen kaybolmaz. İşte bu duruma "devam eden etki" denir. Araştırmalar, insanların bir bilginin yanlış olduğunu açıkça öğrendikten sonra bile, karar verirken ve olayları değerlendirirken bu yanlış bilgiyi farkında olmadan kullanmaya devam ettiğini gösterir. Yalan bilgi, zihinde silinmeyen bir iz bırakır. Bu yüzden "yalanı düzeltmek", çoğu zaman yalanın yarattığı etkiyi sıfırlamaya yetmez. Bu etkinin bu kadar güçlü olmasının nedeni, yalanın zihinde bir hikâye kurmasıdır. Örneğin "Orman yangınını X örgütü çıkardı" iddiası, olaylara neden–sonuç ilişkisi kazandıran basit ve net bir açıklama sunar. Zihin için bu tür açıklamalar rahatlatıcıdır; çünkü belirsizliği ortadan kaldırır ve dünyayı anlaşılır kılar. Bir teyitçi çıkıp "Hayır, bu doğru değil" dediğinde, bu hikâye bir anda çöker ve zihinde bir boşluk oluşur. İnsan beyni bu tür nedensellik boşluklarını sevmez. Belirsizlik hissi, yanlış olduğunu bildiği ama tutarlı görünen eski hikâyeden bile daha rahatsız edici olabilir.

Eğer yalan çürütülürken yerine doğru, tutarlı ve açıklayıcı yeni bir anlatı konmazsa, zihin bu boşluğu doldurmak için eski hikâyeye geri döner. Kişi, yanlış olduğunu bilse bile, bilişsel rahatlık için o yanlışı kullanmaya devam eder.

Şekil 2.2.4 *Etkili çürütmenin yolu: Sandviç metodu*

Devam eden etki ile mücadelede yalnızca "Bu bilgi yanlış" demek çoğu zaman yeterli olmaz. Yanlış bilgi, zihinlerde yer ettikten sonra iz bırakmaya devam eder. Bu nedenle etkili bir çürütme, sandviç metodu olarak bilinen üç aşamalı bir yaklaşımı izlemelidir. İlk aşamada doğru bilgi en baştan açık, net ve anlaşılır biçimde paylaşılır. Böylece zihin, sağlam bir başlangıç noktası edinir. İkinci aşamada, yanlış bilginin neden ortaya çıktığı, neden ikna edici göründüğü ve hangi açılardan hatalı olduğu açıklanır. Bu adım, yanlış bilginin yarattığı boşluğu doldurarak zihnin parçaları bir araya getirmesini sağlar. Son aşamada ise doğru bilgi yeniden vurgulanır ve anlatı tekrar bu doğru bilgi üzerine sabitlenir. Sandviç metodu, yalnızca yanlışı düzeltmekle kalmaz; aynı zamanda zihnin doğru bilgi etrafında tutarlı ve kalıcı bir anlam çerçevesi oluşturmasına yardımcı olur.

Grup İçi Yanlılık ve Kabilecilik

Şimdiye kadar ele aldığımız bilişsel önyargılar daha çok bireysel düzeyde işleyen zihinsel kısa yollara odaklanıyordu. Ancak bilginin nasıl algılandığını ve kabul edildiğini güçlü biçimde etkileyen, bireysel olmaktan çok sosyal bir mekanizma daha vardır: grup içi kayırma ve grup dışı önyargı. Sosyal psikolojinin öncü isimlerinden Henri Tajfel'in çalışmaları[15], insanların grup aidiyetine ne kadar hızlı ve güçlü biçimde bağlandığını açıkça gösterir. Tajfel'in "minimal gruplar" deneylerinde, insanlar tamamen rastgele ve anlamsız ölçütlerle -örneğin yalnızca "mavi tişörtlüler" ve "kırmızı tişörtlüler" olarak- ayrılsalar bile, bu ayrımın keyfi olduğunu bilmelerine rağmen otomatik ve neredeyse içgüdüsel tepkiler geliştirir. Bu tepkiler iki temel eğilim etrafında şekillenir: Kişi kendi grubundakileri daha yetkin, daha dürüst ve daha güvenilir görme eğilimindeyken, diğer gruba karşı daha şüpheci olur; onları daha az güvenilir ve hatta potansiyel olarak kötü niyetli algılamaya başlar. Bu sosyal mekanizma, yanlış bilginin neden çoğu zaman "bizden geliyorsa" daha kolay kabul edildiğini anlamak için kritik bir anahtar sunar.

Bu eğilimler, insanın evrimsel geçmişinden miras kalmıştır. Atalarımız için hayatta kalmak, ait oldukları kabilenin korunmasına bağlıydı; bu nedenle "biz" ve "onlar" ayrımı, güvenliği sağlayan temel bir mekanizma olarak gelişti. Ancak aynı mekanizma, özellikle siyaset, ideoloji ve dijital topluluklar içinde modern dünyada bilginin ve gerçeğin algılanmasını ciddi biçimde çarpıtabilir. Günümüzde siyasi kutuplaşmanın, katı ideolojilerin ve çevrimiçi fan gruplarının yaygın olduğu bir ortamda bu kabile mantığı tehlikeli bir inanç sistemine dönüşür: "Bizimkiler" genellikle iyi niyetli, dürüst ve ahlaklı kabul edilir; yaptıkları hatalar ya istisna sayılır ya da "daha büyük bir amaç" için

[15] Tajfel, H., Billig, M. G., Bundy, R. P., & Flament, C. (1971). Social categorization and intergroup behaviour. *European journal of social psychology*, *1*(2), 149-178.

mazur görülür. Buna karşılık "onlar", baştan kötü niyetli, gizli planlar peşinde ve manipülatif kişiler olarak algılanır; söyledikleri her şey bu olumsuz çerçeve içinde yorumlanır. Bu bakış açısı, özellikle dezenformasyon ve yalan haberlerle karşılaşıldığında bilginin eleştirel biçimde değerlendirilmesini zorlaştırır. Zihin, doğruluğu sorgulamak yerine grubu savunmaya yönelir; böylece bilişsel süreçler akıl yürütmeden çok duygusal ve sosyal refleksler tarafından yönetilmeye başlar. Sonuçta yanlış bilgi, gerçek olup olmadığına bakılmaksızın "bizden" geldiği için daha kolay kabul edilirken, doğru bilgi "onlardan" geldiğinde reddedilebilir hâle gelir.

Bu çifte standart, dezenformasyonun hızla yayılması için son derece elverişli bir zemin yaratır. Grup üyeleri, kendi gruplarından gelen yanlış bilgileri sorgulamak yerine, onları mantıklı göstermeye çalışır. Böylece "bizim" yalanlarımız artık açık birer yalan olarak görülmez; "haklı davamızın gereği", "stratejik bir hamle" ya da "daha büyük bir gerçeğin parçası" olarak yeniden tanımlanır. Bu noktada bireysel doğruluk arayışı geri plana düşer; onun yerini grup kimliğini ve aidiyeti koruma refleksi alır. Gerçek, ortak bir uzlaşma zemini olmaktan çıkar ve kimliği gösteren bir işarete dönüşür. Bilimsel veriler ve somut olgular bile, kişinin ait olduğu grubun sınırları içinde kabul edilebilir olup olmamasına göre değerlendirilir. Sonuçta, karşılıklı anlayışı ve akılcı tartışmayı imkânsız hale getiren derin bir toplumsal kutuplaşma ortaya çıkar.

Bu bölümde, insan zihninin evrimsel mirasından gelen ve bizi manipülasyona açık hâle getiren bilişsel zayıflıklar, sezgisel önyargılar ele alındı. Bu önyargılar basit bireysel hatalar değildir; binlerce yıl boyunca hayatta kalmamızı sağlayan zihinsel mekanizmaların, günümüzün yoğun ve karmaşık dijital bilgi ortamıyla uyumsuzluğunun bir sonucudur. Özellikle doğrulama yanlılığı, sürü psikolojisi ve duygusal olarak güçlü bilgiyi akılcı değerlendirmelerin önüne koyma eğilimi bu durumu açıkça gösterir. Zihnimiz çoğu zaman eleştirel düşünmek yerine, ait olmayı ve hızlı tepki vermeyi tercih eder.

Asıl soru şudur: Bu biyolojik eğilimler, kâr odaklı sosyal medya platformlarının bilinçli olarak tasarlanmış algoritmalarıyla birleştiğinde ne olur?

Bir sonraki bölümde, "dikkat ekonomisini" daha yakından inceleyeceğiz. Bu bölümde, platformların bizi sürekli bildirimler, beğeniler ve kaydırmalarla bir "ödül döngüsüne" sokarak ekrana bağladığını; her etkileşimin de davranışı pekiştiren bir mekanizma gibi çalıştığını göreceğiz. Daha da önemlisi, bu sistemlerin kullanıcının iyiliğinden çok platformun çıkarına hizmet ettiğini; dezenformasyonu, kutuplaşmayı ve güçlü duygusal tepkileri etkileşimi artıran bir "yakıt" olarak kullanmasını tartışacağız. Kısacası bu tasarım, yalnızca bağımlılığı güçlendirmiyor; aynı zamanda manipülasyonu da kolaylaştırıyor.

TEMEL ÇIKARIMLAR

Bu bölüm, yanlış bilgide ısrar etmemizin sebebinin bir "anlama eksikliği" değil, zihnimizin enerji tasarrufu yapan "fabrika ayarları" olduğunu anlatır. Bilişsel önyargılar herkeste bulunan sistematik düşünme kalıplarıdır. Dezenformasyon zihne zorla girmez; bu önyargıları kullanarak kapıyı bizim içeriden açmamızı sağlar. Çünkü en ikna edici yalan, zaten inanmak istediğimiz yalandır.

Temel Kavramlar ve Mekanizmalar

Doğrulama Yanlılığı: Beynimiz tarafsız bir kayıt cihazı değildir. Sadece mevcut inançlarımızı destekleyen bilgileri seçer, çelişenleri ise filtreler. Bu durum bizi "yankı odaları"na hapseder; kendi görüşümüzü destekleyen yalanları, karşıt görüşteki gerçeklere tercih ederiz.

Güdülenmiş Muhakeme: Zeki olmak yanılmayı engellemez. İnançlarımız tehdit altındaysa, zekâmızı gerçeği arayan bir "bilim insanı" gibi değil, inancımızı savunan bir "avukat" gibi kullanırız. Eğitimli insanlar, inandıkları yanlışa mantıklı kılıflar uydurmakta daha yetenekli olabilirler.

Yanıltıcı Doğruluk Etkisi: Bir yalan sık tekrarlandığında beyin için "tanıdık" hale gelir. Zihin, bu tanıdıklık hissini otomatik olarak "doğruluk" sinyali olarak algılar. Bir iddia ne kadar saçma olsa da çok duymak ona inanmayı kolaylaştırır.

Kolayda Bilişsel Kısa Yollar: Beynimiz riskleri istatistiklere göre değil, hatırlaması en kolay ve en duygusal örneklere göre hesaplar. Sosyal medyada sürekli felaket içeriği görmek, gerçek veriler aksini söylese bile bize dünyanın "kaos içinde" olduğu hissini verir.

Dunning-Kruger Etkisi: Bir konuyu az bilmek, o konunun ne kadar

karmaşık olduğunu görmeyi engeller. Bu yüzden konuya yüzeysel hâkim olanlar, uzmanlardan daha kesin ve özgüvenli konuşabilir. Karmaşık gerçekler yerine basit yalanlar daha çekici gelir.

Devam Eden Etki: Bir yalan çürütülse bile zihindeki etkisi tamamen silinmez. Yalanlar zihinde tutarlı bir hikâye oluşturur. Eğer doğrusu anlatılırken bu hikâyenin yerini dolduracak yeni bir açıklama yapılmazsa, zihin o yanlışı doğruymuş gibi kullanmaya devam eder.

Grup İçi Yanlılık: Evrimsel olarak "haklı olmak"tan çok "bizden olmak" önemlidir. Sosyal dışlanma korkusuyla, grubumuzdan gelen yanlışları savunma, karşı gruptan gelen doğruları reddetme eğilimindeyiz. Gerçek, kimlik ve aidiyet duygusunun gerisinde kalır.

2.2. KENDİNİZİ TEST EDİN

Soru 1: Bir kişi yalnızca kendi siyasi görüşünü destekleyen haber kaynaklarını takip ediyorsa, aşağıdaki bilişsel ön yargılardan hangisinin etkisi altındadır?

A) Dunning–Kruger etkisi

B) Doğrulama yanlılığı

C) Kolayda bilişsel kısa yol

D) Çapa etkisi

Soru 2: "Yanıltıcı doğruluk etkisi"ne göre, bir bilginin doğruymuş gibi algılanmasını en çok hangi unsur artırır?

A) Kaynağın güvenilirliği

B) Mantıksal tutarlılığı

C) Tekrar edilmesi

D) Gizli bilgi izlenimi vermesi

Soru 3: Dunning–Kruger etkisi temel olarak neyi ifade eder?

A) Tevazu ve öz farkındalık

B) Kendi yetersizliğini fark etme

C) Bilgi eksikliği ile gelen aşırı özgüven

D) Yardım isteme eğilimi

2.2. MERAKLISINA EK KAYNAKLAR

Alper, S., & Yılmaz, O. (2025). *Komplo teorilerine neden inanırız?* Doğan Kitap.

Cabas, M. ve Kozanoğlu, C. (Sunucular). (2024, 6 Eylül). Komplo teorileri (Konuk: O. Yılmaz) [Sesli podcast bölümü]. *Nereden başlasam* içinde. Spotify. https://open.spotify.com/episode/4wZ3Em9DMqhP122Hf7kWAr

Fazio, L. K., Brashier, N. M., Payne, B. K., & Marsh, E. J. (2015). Knowledge does not protect against illusory truth. *Journal of Experimental Psychology: General*, 144(5), 993–1002.

Karaosmanoğlu, K. (2021). *Komplo teorileri: Disiplinlerarası bir giriş* (2. Baskı). İletişim Yayınları

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2(2), 175–220.

Kunda, Z. (1990). The case for motivated reasoning. *Psychological Bulletin*, 108(3), 480–498.

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, 13(3), 106–131.

Lewandowsky, S., Stritzke, W. G. K., Freund, A. M., Oberauer, K., & Krueger, J. I. (2013). Misinformation, disinformation, and violent conflict: From Iraq and the "War on Terror" to future threats to peace. *American Psychologist*, 68(7), 487–501.

Pronin, E., Lin, D. Y., & Ross, L. (2002). The bias blind spot: Perceptions of bias in self versus others. *Personality and Social Psychology Bulletin*, 28(3), 369–381.

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Der.), *The Social Psychology of Intergroup Relations* (ss. 33–47). Brooks/Cole.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive Psychology*, 5(2), 207–232.

Dikkat Ekonomisi ve Algoritmalar

Bu Bir İrade Meselesi mi?

Google'un eski çalışanlarından olan, Center for Humane Technology'nin kurucusu Tristan Harris, teknoloji endüstrisinin mantığını tek bir cümleyle özetler: *"Beyin sapına inebilmek için aşağıya doğru bir yarış"* (*Race to the bottom of the brain stem*). Bu ifade, dijital teknolojilerin yalnızca dikkatimizi çekmekle yetinmediğini; en ilkel, en dürtüsel ve en savunmasız yanımıza beyin sapına ve limbik sistemimize doğrudan ulaşmayı hedeflediğini anlatırken, bir yandan da rekabetin hepimizi aşağıya çeken bir yarış olduğunu vurgulamaktadır.

Bu çarpıcı tespit, dijital ekosistemin gerçek iş modelini açıkça ortaya koyar: Facebook, Instagram, TikTok, X (Twitter) ve YouTube gibi dev platformlarda bizler müşteri değil, ham maddeyiz. Bu şirketlerin asıl müşterisi, dikkatimizi ve davranışlarımızı satın alan reklamverenlerdir. Platformların sattığı şey, çoğu zaman sanıldığı gibi yalnızca adımız, yaşımız ya da konumumuz gibi kişisel veriler değildir. Bu bilgiler, sistemin çalışması için kullanılan birer yakıttır. Asıl ürün, gelecekte nasıl davranacağımızın öngörülebilirliğidir. Amaç, bizleri mümkün olduğunca uzun süre ekranda tutmak; bu sırada sürekli veri toplayarak davranış kalıplarınızı giderek daha isabetli biçimde tahmin etmek ve sonunda bu davranışları reklamverenin istediği şekilde yönlendirebilmektir.

Daha önceki bölümlerde ele aldığımız anında tatmin arayışı, korku ve öfkeye hızlı kapılma, biz-onlar ayrımı ve doğrulama yanlılığı gibi biyolojik ve psikolojik eğilimler, platformlar için bir sorun ya da kullanıcı arızası değildir. Tam tersine, bu eğilimler algoritmik tasarımın temel malzemesidir. Çünkü insanı ekranda tutmanın ve etkileşimi artırmanın en kolay yolu, rasyonel ve

yavaş düşünen zihni (sistem 2) geri plana itmek; dürtüsel ve duygusal sistemi (sistem 1) korku, öfke ve merakla sürekli uyarmaktır. Tristan Harris'in "beyin sapına inme yarışı" dediği şey tam da budur: en ilkel, en otomatik tepkilerimize doğrudan dokunmak.

Bu bölümde, sosyal medya algoritmalarının bu zayıf noktaları nasıl sistemli biçimde kullandığını; özellikle dopamin döngüleri üzerinden dikkatimizi nasıl "hacklediğini"; "ücretsiz" görünen hizmetlerin gerçek bedelini nasıl dikkatimiz, ruh sağlığımız ve zihinsel enerjimizle ödediğimizi ele alacağız. Ayrıca bu algoritmik düzenin, bizi dezenformasyona, kutuplaşmaya ve duygusal manipülasyona karşı neden daha savunmasız hâle getirdiğini, mekanizmaları adım adım açarak inceleyeceğiz.

Sonsuz Akış: "Durdurma" İşaretlerini Yok Etmek

Nobel ödüllü ekonomist Herbert Simon'un 1971'de ortaya koyduğu bilgi çağı paradoksu, meseleyi net biçimde özetler: "*Bilgi zenginliği, dikkat yoksulluğu yaratır."* İnsan dikkati sınırlı ve son derece değerli bir kaynaktır; gün içinde yalnızca belli bir süre odaklanabiliriz. Milyarlarca dolarlık teknoloji şirketleri arasındaki rekabet de tam olarak bu sınırlı zihinsel alanı ele geçirme mücadelesidir.

Bu tabloyu bir adım ileri taşıyan Shoshana Zuboff, durumu "gözetim kapitalizmi" (*surveillance capitalism*) kavramıyla açıklar.[16] Zuboff'a göre teknoloji devleri, korkularımızı, sevinçlerimizi, alışkanlıklarımızı, özetle insan deneyimini davranışsal veriye dönüştürür. Bu veriler büyük yapay zekâ sistemlerinde işlenir ve insanların ne yapacağını önceden tahmin etmeyi amaçlayan "tahmin ürünleri" olarak pazarlanır. Bu iş modelini çarpıcı biçimde an-

[16] Zuboff, S. (2019). *The age of capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

latan bir örnek de Reed Hastings'ten gelir. Hastings, Netflix'in en büyük rakiplerinin Amazon ya da Disney değil, uyku olduğunu söyler. Çünkü uyku, ekranla bağın koptuğu tek andır. Nihai hedef, kullanıcıyı mümkün olduğunca uzun süre ekranda tutmak ve dikkati sürekli bir "dikkat madeninde" işlemeye devam etmektedir.

İZLE

Shoshana Zuboff'un *The Age of Surveillance Capitalism* kitabından yola çıkarak hazırlanan *De grote dataroof* dijital çağın yeni ekonomik düzenini anlatmaktadır.

Belgeseli izlemek için:

https://www.youtube.com/watch?v=hIXhnWUmMvw

İnsan zihni, dikkatini ne zaman sürdürüp ne zaman bırakacağına çevreden gelen bazı doğal sinyallerle karar verir. Bu sinyallere "durdurma işaretleri" (*stopping cues*) denir. Durdurma işaretleri, beynimize "Burada bitti, durabilirsin, şimdi düşünme ve değerlendirme zamanı" mesajı verir. Bu sayede zihin hem mola verir hem de otomatik tüketimden çıkar. Eski dünyada**,** zihni koruyan doğal duraklar hayatın parçasıydı. Geleneksel medyada içerik kendiliğinden sona ererdi. Gazetede sayfalar biter, kitapta bölüm tamamlanır, televizyon programında jenerik akardı. Bu net bitişler, kişiyi otomatik izleme ya da tüketme hâlinden çıkarır; kısa bir durup düşünme alanı açardı. Zihin, gördüğünü değerlendirme, anlamlandırma ve dinlenme fırsatı bulurdu. Bu duraklar aynı zamanda farkında olmadan işleyen bir bilişsel savunma mekanizması işlevi görürdü. Yeni dünyada ise dijital platformlar bu doğal durakları bilinçli biçimde ortadan kaldırırken, sonsuz kaydırma, otomatik oynatma ve bir sonraki video önerileriyle içerik akışı aralıksız devam edebilmektedir. Böylece kullanıcı durup düşünmeye değil, akışın içinde kalmaya yönlendirilir; zihin sürekli uyarana maruz kalarak dinlenme ve değerlendirme imkânını

giderek kaybeder. Bu kesintisizlik, fark edilmesi zor ama güçlü bilişsel tuzaklar yaratır.

Bu tasarımların amacı, kullanıcıyı mümkün olduğunca uzun süre platformda tutmaktır. Bunun için zihin, sürekli hızlı ve tepkisel düşünme modunda (sistem 1) kalır. Sürekli akış, zamanla karar yorgunluğu yaratır. Her içerikten sonra "Devam mı? Durayım mı?" sorusunu yanıtlamak yorucudur. Bir noktadan sonra kişi karar vermeyi bırakır ve akışa teslim olur. Eleştirel düşünme devre dışı kalır. Ayrıca "bir sonraki içerik belki daha iyidir" beklentisi, durmayı zorlaştırır ve zihinsel savunma mekanizmalarını zayıflatır. Sonuç olarak, durdurma işaretlerinin yokluğu tesadüf değil; dikkati sürekli içeride tutmak için tasarlanmış bilinçli bir stratejidir.

Tasarımcı Aza Raskin tarafından geliştirilen ve kendisinin sonradan pişmanlık duyduğunu açıkladığı "sonsuz kaydırma" dijital platformların en güçlü bağımlılık araçlarından biridir. Bu tasarım, kullanıcıya "bitti" hissi veren sayfa sonlarını ve durakları tamamen ortadan kaldırır. TikTok, Instagram ve X'te parmağı her aşağı kaydırışta yeni içerik otomatik olarak gelir. Böylece beyin durma sinyali alamaz ve bilinçdışı, otomatik sistem 1 modunda kalır. Davranış bilimci Brian Wansink ve arkadaşlarının gerçekleştirdiği ünlü "dipsiz çorba kasesi" deneyi, bu etkiyi son derece çarpıcı bir biçimde ortaya koyar.[17] Deneyde bazı katılımcılara, alt kısmından fark edilmeden sürekli doldurulan "dipsiz" çorba kaseleri verilirken, diğer katılımcılar normal kaselerden çorba içer. Sonuçlar dikkat çekicidir: Dipsiz kâseden çorba içenler, ne kadar tükettiklerini fark edemedikleri için, normal kâseden içenlere kıyasla yaklaşık %73 daha fazla çorba tüketir. Üstelik bu katılımcılar, daha fazla yemiş olmalarına rağmen, kendilerini daha tok hissettiklerini de söylemezler. Sosyal medya,

[17] Wansink, B., Painter, J. E., & North, J. (2005). Bottomless bowls: Why visual cues of portion size may influence intake. Obesity Research, 13(1), 93-100. https://doi.org/10.1038/oby.2005.12

bu dipsiz kâsenin dijital versiyonudur. Kullanıcı, "sayfa bitti", "içerik tamamlandı" gibi görsel ipuçlarından mahrum kalır. Beyin, "durayım mı?" sorusunu soracak o kısa düşünme anını bulamaz.

İZLE

Aza Raskin: *"Sosyal medya ile icat edilen sonsuz kaydırma, yeni bir tür güçtü. Yeni bir teknolojiydi. Ve bu yeni bir tür sorumlulukla geldi: Temelde birinin dopamin sistemini ve "durdurma işaretlerinin" eksikliğini hackliyorum. Zihinleri uyanıp 'Bunu hala yapmak istiyor muyum?' demiyor. Çünkü kapıya dirseğinizi koyup 'Hey, senin için bir şey daha var, bir şey daha var' demeye devam ediyorsunuz. Bunu hacklediğinizde, 'İnsanların egemenliğini ve seçimlerini koruma sorumluluğumuz var' dememiz gerekirdi."*

Aza Raskin'inin yer aldığı bu videoyu izlemek için:

https://www.youtube.com/watch?v=rQCPqnocCfs

Sonsuz akış, kullanıcıyı kesintisiz ve pasif bir tüketim hâline sokar. Bu hipnotik akış sürerken zihinsel kaynaklar yüzeyselleşir. En tehlikeli sonuçlardan biri de budur: dezenformasyon bu akışa kolayca sızar. Zihin otopilotta (sistem 1) kaldığında; sorgulayan, kaynak kontrolü yapan ve mantık hatalarını yakalayan sistem 2 büyük ölçüde devre dışı kalır. Sonuçta kullanıcı, saatlerce kaydırırken sunulan içeriği sorgulama becerisini giderek kaybeder.

Neden Her Defasında "Son Bir Kez Daha" Bakarız?

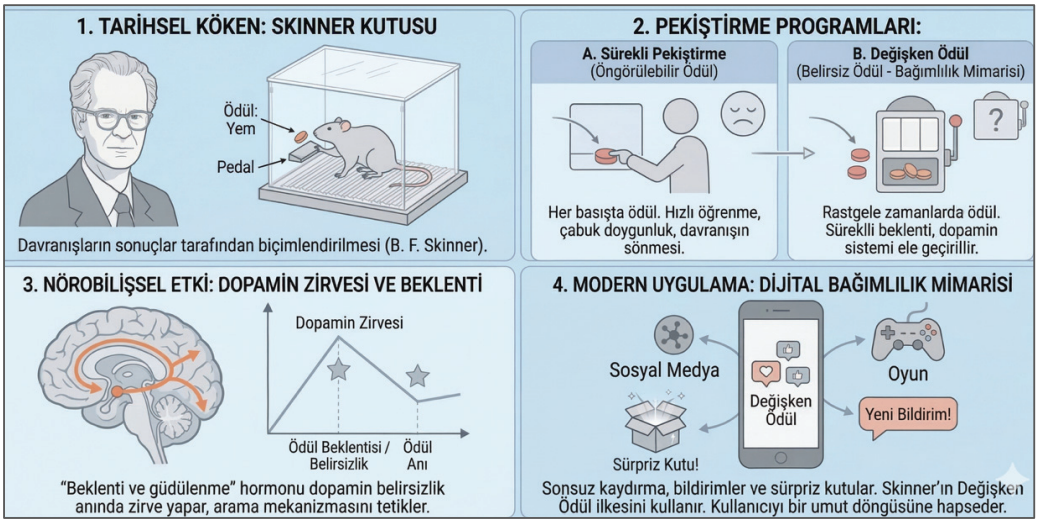
Sosyal medyanın bağımlılık yaratma gücü, beynimizin ödül sistemiyle doğrudan oynamasından kaynaklanır. Bu sistemin merkezinde ise dopamin bulunur. Ancak yaygın inanışın aksine dopamin bir "mutluluk hormonu" değildir. Nörobilimci Robert Sapolsky'nin de vurguladığı gibi dopamin; hazdan çok arzu, motivasyon ve beklentiyle ilgilidir[18]. Bizi mutlu etmez, bizi aramaya ve devam etmeye iter. Başka bir deyişle dopamin, "aldım ve bitti" hissinden çok, "acaba bir şey daha var mı?" sorusunu besler. Sosyal medya tasarımları da tam olarak bu soruya oynar.

Bugün sosyal medya, mobil uygulamalar ve dijital oyunlarda gördüğümüz bağımlılık mimarisi, kökenini 20. yüzyıl davranışçı psikolojisine borçludur. Özellikle B.F. Skinner'ın "edimsel koşullanma" (*operant conditioning*) deneyleri, bu sistemin temelini oluşturur. Skinner, fareler ve güvercinlerle yaptığı gözlemlerde "Skinner Kutusu" adı verilen bir düzenek kullandı ve davranışların ödül türüne göre nasıl şekillendiğini inceledi. Onun keşfi, bugün dijital platformların merkezinde yer alan kritik bir ilkeyi ortaya koydu: Günümüzde "değişken ödül" olarak adlandırılan değişken oranlı pekiştirme (*variable-ratio reinforcement*) ilkesi.[19]

B. F. Skinner, ödüllerin bir davranışı sürdürme gücünü iki temel senaryo üzerinden açıklar. Sürekli pekiştirme durumunda, davranış her seferinde ödüllendirildiği için öğrenme hızlı gerçekleşir; ancak ödülün ne zaman geleceği öngörülebilir olduğundan, zamanla doygunluk oluşur ve davranış giderek zayıflayarak sonunda söner. Öğrenme hızlıdır ama kalıcılığı düşüktür. Buna karşılık değişken ödül düzeninde, ödülün ne zaman ve ne kadar

[18] Sapolsky, R. M. (2017). *Behave: The biology of humans at our best and worst*. Penguin Press.
[19] Skinner, B. F. (2005). *Science and human behavior*. The B.F. Skinner Foundation. (Orijinal eser 1953 yılında yayımlanmıştır).

geleceği bilinmez; bazen hemen gelir, bazen uzun süre hiç gelmez. Tam da bu belirsizlik, davranışı güçlü ve zorlayıcı kılar: Organizma her seferinde "belki bu sefer" beklentisiyle davranışı sürdürür. Bu noktada davranış artık bir ihtiyacı karşılamaktan çıkar; belirsizliğin peşinden koşan bir arayışa dönüşür. Bu arayış, dopamin sistemini güçlü biçimde devreye sokar.



Şekil 2.3.1 *Dijital bağımlılık mimarisinin psikolojik temelleri*

Değişken ödül sistemi, insan davranışını iki temel nörobilişsel mekanizma üzerinden etkiler. İlki, beklenti zirvesi olarak tanımlanan dopamin etkisidir. Dopamin, ödül alındığında değil; ödülün gelip gelmeyeceğinin belirsiz olduğu anda yükselir. "Yeni bir şey var mı?" sorusu, beynin motivasyon merkezini harekete geçirir ve bu beklenti hâli sonsuz kaydırma, sayfayı yenileme ya da bildirimleri kontrol etme gibi davranışlarla sürekli canlı tutulur. İkinci mekanizma ise sönmeye karşı dirençtir. Değişken ödülle öğrenilen davranışlar, ödül tamamen ortadan kalksa bile en geç sönen davranışlar arasındadır. Kişi artık keyif almasa dahi, "belki bir sonraki kontrolde bir şey olur" düşüncesiyle uygulamaya geri dönmeye devam eder. Bu durum, bir platformun cazibesi azalmış olsa bile neden sürekli kontrol edildiğini açıklayan temel

dinamiklerden biridir.

Özetle, rastgele bildirimler, sürpriz içerikler, sonsuz kaydırma gibi modern dijital tasarımlar doğrudan Skinner'ın "değişken ödül" ilkesini temel alır. Bu sistem, kullanıcıyı öngörülemez bir umut döngüsüne hapseder. Etkili bir bilişsel savunma geliştirilmediğinde, davranış zamanla kontrolsüz, zorlayıcı ve otomatik bir hâl alır. Bu noktada mesele irade eksikliği değil; bilinçli olarak tasarlanmış bir nörobilimsel tuzaktır.

Dijital Slot Makineleri: Yenilemek için Aşağı Çekip Bırakmak ve Bildirimler

Günümüz dijital platformları, davranışsal psikolojinin en etkili mekanizmalarından biri olan değişken ödül (belirsiz ödül) ilkesini doğrudan kullanır. Bu ilke, bir davranıştan sonra ödülün gelip gelmeyeceğini ya da ne zaman geleceğini bilmemekten doğan güçlü beklenti ve belirsizlik hissine dayanır. Araştırmalar, belirsiz ödüllerin; düzenli ve öngörülebilir ödüllere kıyasla, bir davranışı sürdürmeyi ve onu tekrar tekrar yapma isteğini çok daha güçlü biçimde tetiklediğini gösterir. Dijital platformlar da bu mekanizmadan yararlanarak kullanıcıların dikkatini ve zamanını mümkün olan en üst düzeyde tutmayı amaçlar.

Kumar endüstrisi, bu psikolojik prensibin en yalın ve en yıkıcı örneğini tek kollu canavar slot makineleri üzerinden sunar. Oyuncunun kolu çekmek ya da düğmeye basmak gibi yaptığı her eylem bir ödülü garanti etmez. Her denemede kazanıp kazanmayacağınızı, kazanırsanız bunun küçük bir geri ödeme mi yoksa büyük bir ikramiye mi olacağını bilemezsiniz. İşte bu öngörülemezlik, beynin ödülle ilişkili kimyasalı olan dopaminin, ödül gerçekleştiğinde değil, beklenti anında yoğun biçimde salgılanmasına yol açar. Bu durum, oyuncunun makineden kopmasını zorlaştırır ve bağımlılık yaratan döngüyü besler.

Sosyal medya platformlarında ekranı aşağı çekip bırakarak yapılan

aşağı çekip bırakmak (*pull-to-refresh*) hareketi de nörolojik olarak bir slot makinesinin kolunu çekmeye çok benzer. Kullanıcı, her yenilemede olası bir "ödül" bekler. Beyin arka planda şu sorularla meşguldür: "Ne gelecek?", "Benim için önemli bir şey mi?", "Yeni bir beğeni, yorum ya da takipçi mi?", "Eski bir arkadaşın paylaşımı mı, yoksa beni şaşırtacak ya da duygulandıracak bir içerik mi?" Ya da belki hiçbir şey. Bu belirsiz sosyal ödül ihtimali, uygulamayı tekrar tekrar açma ve yenileme davranışını tetikler. Kullanıcı, tatmin edici bir içerik bulana kadar bu döngüyü sürdürme eğilimi gösterir.

Gelen bir bildirim sesi ya da titreşimi (*ping* etkisi) Pavlov'un köpeklerinde zil sesinin yarattığı tepkiye benzer bir şartlanma oluşturur. Pavlov'un deneyinde zil, yemeğin geleceğini haber veren bir uyarıcıydı. Dijital dünyada ise bu "ping", beynin ödül merkezine "Bir ödül geliyor olabilir, dikkatini buraya ver" mesajını gönderir. İçerik önemli olmasa bile, kişi telefonu istem dışı ve otomatik bir refleksle kontrol etme eğilimi gösterir. Bu tepki, bilginin kendisinden çok, olası bir sosyal ödülü kaçırma korkusu ve dopamin salınımıyla ilişkilidir.

Sonuç olarak, dijital platformlar beğeniler, haberler, bildirimler gibi rastgele ödüller üzerinden kullanıcı davranışını sistemli biçimde yönlendirir. Amaç, cihazla geçirilen süreyi artırmak ve sürekli bir dikkat bağımlılığı döngüsü oluşturmaktır. Bu mekanizma, günümüz bilişsel bilim ve psikolojik savunma tartışmalarının merkezinde yer alır.

Yanlış ve Kutuplaştırıcı İçerik Neden Daha Çok Yayılıyor?

Dijital teknolojilerin yarattığı sorun yalnızca ekran süresi ya da bildirim bağımlılığı değildir. Yukarıda belirttiğimiz bu derin etkileşimin merkezinde, beynin temel ödül sistemi olan dopamin yer alır. Dezenformasyon ve kutuplaştırıcı içerikler, bu sistemi en güçlü ve en tehlikeli biçimde besleyen unsurlardır. Sosyal medya ve içerik platformları, kullanıcıların platformda daha uzun

süre kalmasını ve daha fazla etkileşim kurmasını hedefleyen algoritmalarla çalışır. Bu algoritmalar, insan psikolojisindeki dopamin tetikleyicilerini bilinçli biçimde kullanır.

Öfke, kızgınlık ve saldırma dürtüsü gibi güçlü duygular, beynin ödül merkezlerini diğer duygulara kıyasla çok daha yoğun biçimde uyarır. Bu tepki, evrimsel olarak tehditlere hızlı yanıt vermeyi sağlamak için gelişmiştir; ancak dijital ortamda bu mekanizma amacından saparak kolayca tetiklenir. Kişi, kendi inançlarını ve dünya görüşünü doğrulayan; karşı tarafı "haksız", "kötü" ya da "akılsız" gösteren bir dezenformasyon veya kutuplaştırıcı içerikle karşılaştığında, bunu anlık bir ödül gibi algılar. Bu durum, doğrulama yanlılığını besler ve "Ben zaten biliyordum, haklıymışım" düşüncesini güçlendirir. Haklı çıkma hissi, beyinde kısa süreli bir dopamin artışı yaratır.

Benzer şekilde, sosyal medyada bir trolle tartışmak, karşıt görüşlü bir içeriğe sert ya da aşağılayıcı bir yorum yazmak da geçici bir haz sağlar. Bu haz, üstünlük kurma ya da karşı tarafa haddini bildirme duygusuyla ilişkilidir. Ancak bu ödül, kişiyi daha fazla çatışmacı içeriğe yönlendirir ve zamanla daha agresif bir dijital tutumun yerleşmesine yol açar. Bu noktada filtre balonu devreye girer. Algoritmalar, kullanıcının en son hangi içeriklerle etkileşime girdiğini tespit eder ve ona benzer, hatta daha uç ve daha öfke yüklü içerikleri göstermeye başlar. Sonuçta öfke, haklılık hissi ve kutuplaşma birbirini besleyen bir döngüye dönüşür.

İnsan beyni, hayatta kalma içgüdüsünün bir parçası olarak yeni, sıra dışı ve beklenmedik bilgilere doğal bir ilgi duyar. Çünkü evrimsel açıdan yeni bir bilgi ya olası bir tehdit ya da önemli bir fırsat anlamına gelmiştir. Bu eğilim, yenilik arayışı önyargısı (*novelty bias*) olarak adlandırılır ve dezenformasyonun yayılmasında kilit bir rol oynar. Yalan haberler ve komplo teorileri, çoğu zaman doğrulanmış bilgilere kıyasla daha çarpıcı, daha dramatik ve gizli bir hava taşır. Gerçeklik genellikle karmaşık ve sıkıcıdır; buna karşılık

yalanlar basit, net ve yüksek dozda heyecan içerir. Bu dramatik etki, dikkat çekmeyi kolaylaştırır.

Komplo anlatılarının bir diğer güçlü yönü, özel bilgiye sahip olma hissi yaratmasıdır. Kişi, başkalarının bilmediği ya da saklandığı iddia edilen bir gerçeğe ulaştığını düşündüğünde, bu durum beyinde dopamin artışına yol açar ve özgüveni besler. Bu haz, söz konusu bilgiyi hızla başkalarıyla paylaşma isteğini güçlendirir. Yalan haberlerin doğru bilgilere göre daha hızlı yayılmasının arkasında da bu mekanizma yatar. Algoritmalar ise bu ilgiyi hızla fark eder. Kullanıcının yeni, şaşırtıcı ve gizemli içeriklere gösterdiği tepkiyi izleyerek, ona giderek daha uç ve daha az doğrulanmış içerikler sunar. Böylece yenilik arayışı, gizem ve dezenformasyon birbirini besleyen sürekli bir döngüye dönüşür.

İnsanlar, sosyal varlıklar olarak, ait oldukları bir gruba kabul edilme ve o gruptan onay alma ihtiyacı duyar. Dijital ortamda bu ihtiyaç, beğeniler, paylaşımlar ve yorumlar üzerinden doğrudan dopamin ile ödüllendirilir. Bir dezenformasyon ya da kutuplaştırıcı görüş, kişinin ait olduğu sosyal çevre, arkadaş grubu ya da siyasi/ideolojik topluluk tarafından onaylandığın-da, bu durum "kabileye ait olma" ve "kabile içinde değerli olma" hissini anın-da güçlendirir. Sosyal onay, beyinde güçlü bir ödül tepkisi yaratır. Ancak bu ödül mekanizması, bilginin doğruluğunu sorgulama eğilimini zayıflatır. Kişi, grubundan beğeni ve onay almak uğruna, farkında olmadan yanlış ya da za-rarlı bilgilerin yayılmasına katkıda bulunabilir. Gruptan dışlanma korkusu, bilgiyi teyit etme isteğinden çoğu zaman daha

KAVRAM: YANKI ODALARI

Neyi açıklar?: Yankı odaları (*echo-chambers*), bireylerin çoğunlukla kendi inanç ve görüşleriyle uyumlu bilgi ve fikirlerle karşılaştığı, farklı bakış açılarının ise dışlandığı iletişim ortamlarını ifade eder.

Neden önemli?: Bu ortamlar, yanlış bilgilerin sorgulanmadan tekrar edilmesini kolaylaştırırken kutuplaşmayı derinleştirir ve eleştirel düşünmeyi zayıflatır.

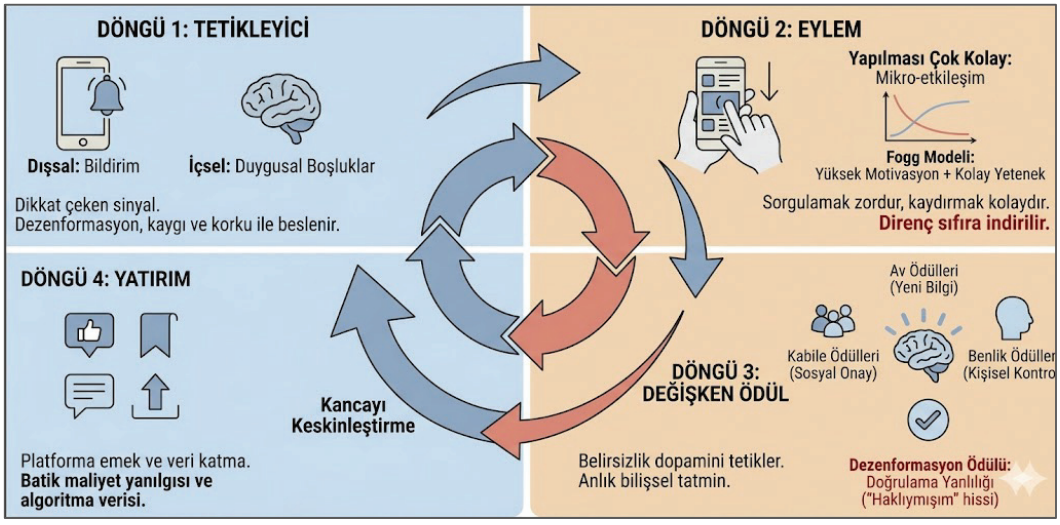
baskın hâle gelir. Bu süreci algo-ritmalar daha da pekiştirir. Benzer düşünen kullanıcılar, dijital "kabileler" için-de bir araya getirilir. Bu kapalı alanlarda paylaşılan her içerik, doğru olsun ya da olmasın, güçlü bir sosyal kanıt gibi algılanır. Sonuçta yanlış bilgiler, grup içinde hızla normalleşir ve savunulur.

Teknoloji etiği ve kullanıcı deneyimi alanında öne çıkan isimlerden Nir Eyal, Hooked: How to Build Habit-Forming Products (2014)[20] adlı çalışmasında, dijital ürünlerin kullanıcıda nasıl kalıcı alışkanlıklar, hatta kimi zaman bağımlılıklar yarattığını açıklayan dört aşamalı bir model sunar. Kanca modeli (*hooked model*) olarak bilinen bu yaklaşım, bugün en başarılı mobil uygulamaların, sosyal medya platformlarının ve oyunların psikolojik mimarisini anlamak için temel bir çerçeve sağlar. Aynı model, dezenformasyonun dijital ortamlarda nasıl hızla yayıldığını ve kullanıcıları tekrar tekrar kendine çektiğini kavramak açısından da yol göstericidir. Dezenformasyonun sosyal platformlarda yayılma biçimi, Eyal'in kanca modelindeki dört aşamayı neredeyse birebir izler.

İlk aşama tetikleyicidir. Bu, kullanıcıyı platforma yönelten ilk işarettir. Telefon bildirimleri gibi dışsal tetikleyiciler dikkati anında çeker. Ancak kalıcı alışkanlıkları asıl besleyenler içsel tetikleyicilerdir. Can sıkıntısı, yalnızlık, kaygı veya belirsizlik gibi duygusal boşluklar, dijital ürünlerin bir kaçış mekanizması olarak kullanılmasına yol açar. Dezenformasyon, özellikle korku ve kaygı üzerinden bu duygusal boşluklara seslenir ve kullanıcıyı içeriğe çeker. İkinci aşama eylemdir. Burada belirleyici olan, eylemin son derece kolay olmasıdır. Uygulamayı açmak ya da ekranda tek parmakla aşağı kaydırmak gibi basit hareketler neredeyse hiç çaba gerektirmez. Bu kolaylık, içeriğin doğruluğunu sorgulamayı geri plana iter. Dezenformasyon da tam bu ortamda hızla tüketilir ve çoğu zaman sorgulanmadan geçip gider. Üçüncü

[20] Eyal, N. ve Hoover, R. (2014). *Hooked: How to build habit-forming products*. Portfolio/Penguin.

aşama değişken olan ödüldür. Eylemin ardından gelen tatmin her seferinde farklıdır. Bu belirsizlik, dopamin salınımını artırır ve kullanıcıyı döngüde tutar. Ödül kimi zaman beğeni ve onay, kimi zaman yeni bir şey öğrenme hissi, kimi zaman da kontrol duygusu olabilir. Dezenformasyon bağlamında ise ödül çoğunlukla şok edici, korkutucu ya da kişinin doğrulama yanlılığını besleyen içeriklerdir. "Haklıymışım" hissi, bu döngüyü güçlü biçimde besler. Son aşama ise yatırımdır. Kullanıcı bu aşamada platforma zaman, dikkat ve veri yatırır. Beğenmek, yorum yapmak ya da içeriği kaydetmek bu yatırımlara örnektir. Bu yatırımlar, bir yandan kullanıcının platformdan kopmasını zorlaştırır; diğer yandan algoritmaların kullanıcıyı daha iyi tanımasını sağlar. Böylece bir sonraki döngüde sunulan tetikleyiciler ve ödüller daha isabetli ve daha güçlü hâle gelir. Kısacası dezenformasyon, bu dört aşamalık döngü içinde kullanıcıyı tekrar tekrar kendine çeken bir alışkanlık mekanizması kurar.



Şekil 2.3.2 *Kanca modelinin işleyişi*

Dijital çağın en çarpıcı çelişkilerinden biri şudur: Bir bilginin ne kadar hızlı yayıldığı, çoğu zaman ne kadar doğru olduğuyla ters orantılıdır. Bu durumu

bilimsel olarak ortaya koyan önemli bir çalışma[21], 2018 yılında MIT araştırmacıları Soroush Vosoughi, Deb Roy ve Sinan Aral tarafından Science dergisinde yayımlanmıştır. Araştırma, 2006–2017 yılları arasında Twitter'da paylaşılan 126 bin haber hikâyesini ve 4,5 milyondan fazla tweeti incelemiş ve modern sosyal bilimlerin en çarpıcı bulgularından birine ulaşmıştır: Yanlış bilgiler, doğru bilgilere kıyasla daha hızlı yayılmakta, daha fazla kişiye ulaşmakta ve sosyal ağlara daha derinlemesine nüfuz etmektedir. Bu tablo yalnızca teknolojiyle açıklanamaz. Yanlış bilginin bu kadar etkili yayılmasının arkasında, insan psikolojisi ile sosyal medya platformlarının etkileşim odaklı ekonomik modeli birlikte rol oynar. Bu üstün yayılma gücü, dört temel mekanizmanın bir araya gelmesiyle ortaya çıkar.

Veriler, yanlış bilgilerin doğru bilgilere göre çok daha hızlı yayıldığını gösterir. Doğru bir haberin yaklaşık bin beş yüz kişiye ulaşması günler sürebilirken, yalan haberler bu sayıya saatler içinde ulaşır ve kısa sürede etkileşim zirvesine çıkar. Bu hız, yanlış bilginin düzeltilmesini çoğu zaman etkisiz hâle getirir. Üstelik yalan haberler sadece daha fazla kişiye ulaşmakla kalmaz; paylaşım zincirlerinde daha çok el değiştirerek sosyal ağların içine daha derinlemesine yerleşir.

KAVRAM: BOT

Neyi açıklar?: Botlar sosyal medyada insan gibi davranacak şekilde programlanmış, otomatik paylaşım yapan ve etkileşim kuran sahte ya da yarı-otomatik hesaplardır.

Neden önemli?: Yanlış bilgileri kısa sürede çok sayıda kişiye ulaştırabilir, bir içeriğin olduğundan daha popüler veya güvenilir görünmesine yol açabilir.

Yanlış bilginin bu kadar hızlı yayılmasının asıl nedeni botlar değil, insanların paylaşma davranışlarıdır. Araştırmalar, botların doğru ve yanlış bilgiyi benzer biçimde yaydığını; buna karşılık yanlış bilgilerin insanlar tarafından çok daha hızlı ve yoğun şekilde paylaşıldığını göstermektedir. Bunun

[21] Vosoughi, S., Roy, D. ve Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559

başlıca iki nedeni vardır: İlki yenilik etkisidir. Yanlış bilgiler çoğu zaman daha şaşırtıcı, beklenmedik ve tuhaf görünür; insan beyni ise sıradan gerçeklerden ziyade yeni olana daha fazla dikkat kesilir. İkincisi ise duygusal yoğunluktur. Yanlış bilgiler genellikle öfke, korku ya da aşırı coşku gibi güçlü duygular uyandırır ve bu duygular, durup düşünmeden yapılan paylaşımları tetikleyerek yanlış bilginin hızla yayılmasına zemin hazırlar. Öfke, korku, kaygı ve coşku gibi yüksek uyarılma yaratan duygular, insanı harekete geçirir. Yanlış bilgiler bu duyguları özellikle hedef alır. Kişi, "Bu haksızlık durdurulmalı" ya da "Herkes bunu bilmeli" düşüncesiyle içeriği hızla paylaşır. Buna karşılık sakinlik ya da memnuniyet gibi duygular, paylaşma davranışını pek tetiklemez.

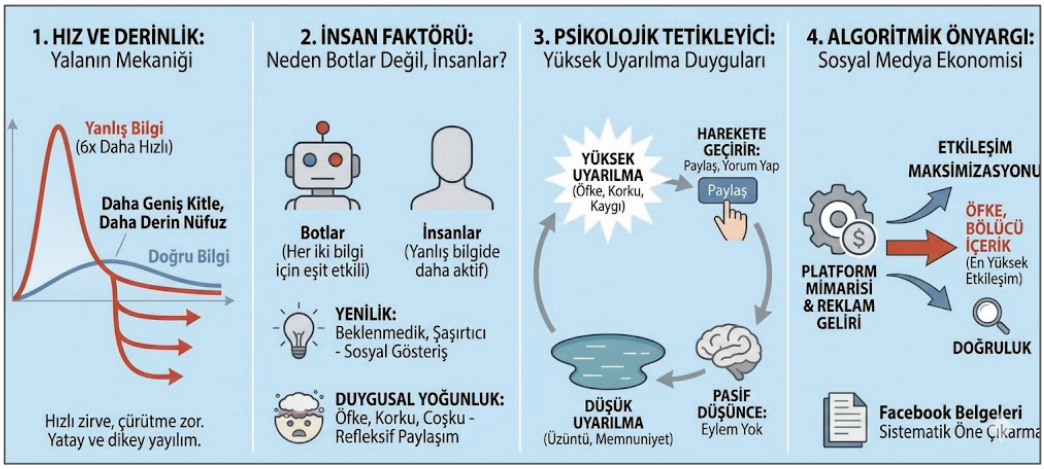
Bu sürecin en kritik halkası, sosyal medya platformlarının kendisidir. Bu platformlar, doğru bilgiyi öne çıkarmak için değil; kullanıcıların daha fazla beğenmesi, yorum yapması ve paylaşması, özetle daha fazla etkileşim üretmesi için tasarlanmıştır. Çünkü etkileşim arttıkça kullanıcılar platformda daha uzun süre kalır ve bu da reklam gelirlerini yükseltir. Yüksek uyarılma yaratan duygular arasında, özellikle öfke (nefrete yakın duygular), en yüksek, en hızlı ve en sürdürülebilir etkileşimi getiren duygudur. Platformlar, reklam gelirlerini artırmak için kullanıcıları uygulamada tutmayı amaçladığından, algoritmalar bilinçli veya bilinçsiz olarak en çok etkileşim getiren içeriği öne çıkarmayı öğrenmiştir.

Bu durumu somut biçimde ortaya koyan en önemli belgeler, Facebook dosyaları olarak bilinen sızıntılardır. [22] Facebook'un eski çalışanı Frances Haugen tarafından kamuoyuna açıklanan ve ilk olarak The Wall Street Journal tarafından 2021 yılında yayımlanan bu belgeler, platformun kendi iç

[22] Feiner, L. (2021, 3 Ekim). *Facebook whistleblower reveals identity, accuses the platform of a 'betrayal of democracy'*. CNBC. https://www.cnbc.com/2021/10/04/facebook-whistleblower-reveals-identity-ahead-of-60-minutes-interview.htm

araştırmalarına rağmen algoritmalarının bölücü, öfke ve nefret içeren içerikleri sistematik olarak öne çıkardığını göstermektedir. Bunun nedeni nettir: Bu tür içerikler, kullanıcı zamanı ve etkileşimi gibi platformun temel ekonomik göstergelerini en üst düzeye çıkarır.

Sonuç olarak, yanlış bilginin bu kadar etkili yayılması insanın yeniliğe ve güçlü duygulara olan doğal eğilimi, öfke ve korkunun paylaşımı tetiklemesi ve algoritmaların etkileşim odaklı ticari mantığı bir araya geldiğinde ortaya çıkan bir kısır döngünün ürünüdür. Bu döngü, sakin ve doğrulanmış bilgilerin geri planda kalmasına, kullanıcıların ise daha az düşünerek ve daha hızlı tepki vererek içerik tüketmesine yol açar.



Şekil 2.3.3 *Yanlış bilginin yayılımı*

Zihin Zamanla Nasıl Yeniden Yazılır?

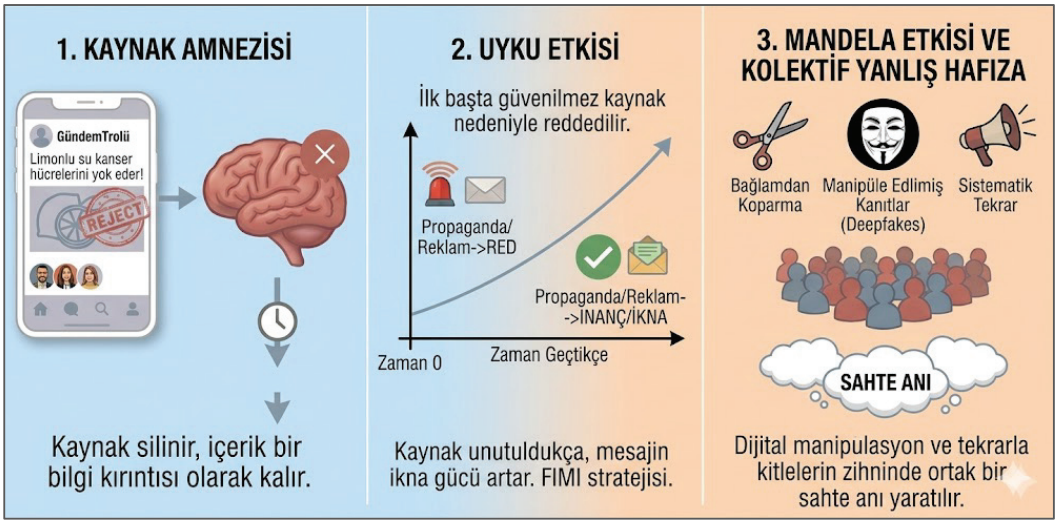
Dijital dezenformasyon ve özellikle FIMI-yabancı devlet kaynaklı bilgi manipülasyonu, doğrudan insan zihninin doğal işleyişini hedef alır. Amaç, karmaşık yalanlar üretmekten çok, yanlış veya çarpıtılmış bilgileri zamanla sorgulanmaz ve tanıdık görünen "gerçekler" hâline getirmektir. Bu süreçte

belirleyici olan şey, bilginin ne kadar mantıklı olduğu değil; insanların zamanla bilginin kaynağını unutması ve hafızanın bu boşluğunun istismar edilmesidir.

İnsan hafızası, bir bilginin içeriğini, o bilginin nereden geldiğinden ayrı tutma eğilimindedir. Buna kaynak amnezisi denir. Beyin, enerji tasarrufu yapmak için genellikle bilginin anlamını korur; ancak kaynağını, bağlamını ve güvenilirliğini zamanla siler. Günlük hayatta sıkça yaşadığımız bir durumdur: Bir şeyi net biçimde hatırlarız ama onu kimden, nerede ya da hangi bağlamda duyduğumuzu hatırlamayız. Dezenformasyon bu mekanizmayı bilinçli biçimde kullanır. Örneğin, güvenilmez bir sosyal medya hesabında "Limonlu su kanseri yok eder" gibi bilimsel dayanağı olmayan bir iddia gördüğünüzü düşünelim. O an bu bilgiyi ciddiye almaz ve geçersiniz. Ancak haftalar ya da aylar sonra, kaynağı tamamen unutulmuş hâlde, "Limonun kanserle ilgili bir faydası vardı galiba" diye hatırlayabilirsiniz. Böylece başlangıçta reddedilen bilgi, kaynağından koparak nötr ve masum bir bilgi kırıntısı gibi zihinde yer eder. Dezenformasyonun zihne sızmasının en yaygın yollarından biri budur.

Uyku etkisi (*sleeper effect*), kaynağı unutmanın daha güçlü bir biçimi olarak, ilk anda güvenilmez bulunan bir mesajın zaman geçtikçe daha ikna edici hâle gelmesini açıklar. Bu süreç genellikle üç aşamada işler. İlk aşamada kişi mesaja maruz kalır, kaynağını güvenilmez bulur ve mesajı reddeder. İkinci aşamada mesajın içeriği hafızada kalmaya devam ederken, "bu bilgi güvenilmez bir kaynaktan gelmişti" şeklindeki uyarı sinyali giderek zayıflar. Son aşamada ise kaynağı büyük ölçüde unutulan mesaj, yeniden değerlendirildiğinde daha makul ve güvenilir görünmeye başlar. Büyük ölçekli dezenformasyon kampanyaları tam da bu gecikmeli etkiyi hedefler: Yalan içerikler, farklı ve çoğu zaman zayıf kaynaklardan tekrar tekrar dolaşıma sokularak tanıdıklık yaratılır ve zaman içinde kaynağın izi silinmeye çalışılır.

Büyük ölçekli dezenformasyon ve manipülasyon operasyonları, mesajın anlık etkisine değil, bu gecikmeli ve birikimli etkiye dayanır. Strateji, yalan ya da çarpıtılmış bilgiyi tek bir güçlü kaynaktan vermek değil; onu çok sayıda, farklı ve çoğu zaman güvenilirliği düşük kaynak üzerinden tekrar tekrar dolaşıma sokmaktır. Bu tekrarlar sayesinde içerik giderek tanıdık hâle gelirken, mesajın nereden geldiği bilgisi silikleşir. Sonuçta kaynağın güvenilmez-



Şekil 2.3.4 *Bellek yanılgıları ve dezenformasyon*

liği önemsizleşir ve bilgi, sıradan ya da tarafsız bir gerçek gibi algılanmaya başlar. Uyku etkisi, dezenformasyonun uzun vadede neden bu kadar etkili olabildiğini açıklayan temel mekanizmalardan biridir. Bazı yalanlar ilk anda değil, zamanla ikna eder.

Mandela etkisi ise çok sayıda insanın hiç yaşanmamış bir olayı ya da bir gerçeğin yanlış bir versiyonunu, son derece net ve kişisel bir anıymış gibi hatırlaması durumudur. Nelson Mandela'nın 1980'lerde hapishanede öldüğü inancı bu durumun örneğidir. Bu durum, hafızanın yalnızca bireysel değil, kolektif düzeyde de kırılgan ve yönlendirilebilir olduğunu gösterir. Dijital ortamda yürütülen organize dezenformasyon ve yabancı devlet manipülasyon

FIMI operasyonları, geçmiş olayları ve söylemleri bilinçli biçimde yeniden dolaşıma sokarak kolektif hafızayı hedef alır. Bu tür operasyonlar çoğunlukla bağlamından koparma, manipüle edilmiş kanıtlar ve sistematik tekrar gibi yöntemler üzerinden işler. Gerçek görüntüler, sözler ya da belgeler yanıltıcı bir bağlamla sunulabilir; deepfake'ler, montajlanmış görseller ve sahte videolar aracılığıyla gerçek çarpıtılabilir; aynı yanlış bilgi çok sayıda farklı hesap ve kaynaktan sürekli olarak paylaşılabilir. Örneğin bir siyasetçinin hiç söylemediği ya da tamamen farklı bir bağlamda dile getirdiği bir söz, binlerce görünüşte bağımsız hesap tarafından tekrar tekrar paylaşıldığında, zamanla gerçekten söylenmiş gibi algılanmaya başlar. Bu sürekli maruz kalma hâli, toplumun geniş kesimlerinde sahte ama güçlü bir kolektif anının oluşmasına yol açar. Bu sürecin en kritik aşamasında, gerçek kanıtlar etkisini yitirir. Olayın orijinal bağlamı, somut belgeler ya da hatta video kayıtları gösterildiğinde bile, bazı kişiler "Ben onu net hatırlıyorum, söyledi" diyerek gerçeği reddeder. Bu noktada hatırlanan şey artık olayın kendisi değil, tekrar yoluyla zihne yerleşmiş olan organize anlatıdır. Bu durum yalnızca toplumsal kutuplaşmayı artırmakla kalmaz; bireyin kendi hafızasına olan güvenini de zedeler. Sonuçta, gerçeklikle bağ zayıflar ve dezenformasyona karşı bilişsel savunma hattı ciddi biçimde aşınır.

Oyunlaştırılmış Komplo Evreni

Günümüzde dezenformasyonun ulaştığı en ileri aşamalardan biri, bilginin oyunlaştırılmasıdır. Artık insanlar yanlış bilgiye yalnızca maruz kalan pasif izleyiciler değil; aksine bu bilgiyi araştıran, çözen, yorumlayan ve yeniden üreten aktif "oyuncular" hâline gelmektedir. Komplo anlatıları bu sayede etkileşimli, sürükleyici ve bağımlılık yaratabilen yapılara dönüşür. Çoğu zaman "alternatif gerçeklik oyunları" (*Alternative Realitty Games*-ARG) mantığıyla işleyen bu anlatılarda katılımcılara gizli ipuçları sunulur, parçalı bilgiler

dağıtılır ve gerçeğe ulaşma görevi verilir. "Kendi araştırmanı kendin yap" (*Do Your Own Research*-DYOR) gibi çağrılar, bireyi hazır bir anlatıya inanmaya değil, onu bizzat keşfetmeye davet eder. Bu süreçte devreye giren psikolojik mekanizmalar, inancı giderek daha dirençli hâle getirir. İnsanlar kendi emekleriyle ulaştıkları sonuçlara, hazır sunulan bilgilere kıyasla daha fazla değer verir; saatlerce ipuçları arayan ve bağlantılar kuran birey için inanç artık dışarıdan gelen bir iddia değil, kendi zekâsının ve çabasının ürünü hâline gelir. Zaman, enerji ve sosyal bedel arttıkça "bu kadar emek verdim, yanılıyor olamam" düşüncesi güçlenir ve kişi inancına daha sıkı bağlanır. Aynı anda doğrulama yanlılığı devreye girer; teoriyi destekleyen en zayıf kaynaklar bile kanıt olarak görülürken, çelişkili bilgiler otomatik biçimde reddedilir ve ana akım medya, akademi ya da resmî kurumlar anlatının parçası olan "büyük komplonun aktörleri" olarak etiketlenir. Böylece kapalı, kendi kendini besleyen bir bilgi evreni oluşur. Oyunlaştırılmış komplo anlatıları güçlü bir aidiyet ve kimlik duygusu da üretir: İpuçlarını "çözebilenler" kendilerini uyanmış, ayrıcalıklı bir grubun parçası olarak görür; bu kimlik özellikle belirsizlik ve güvensizlik dönemlerinde bireylere anlam, amaç ve üstünlük hissi sunar.

İZLE

Q: Into the Storm, HBO tarafından yayımlanan 2021 yapımı altı bölümlük bir belgesel dizisidir. Yönetmenliğini Cullen Hoback'ın üstlendiği yapım, çevrim içi komplo teorisi hareketi QAnon'un kökenlerini, yükselişini ve toplumsal etkisini inceler. Alternatif gerçeklik oyunu (ARG) mantığı, "kendi araştırmanı yap" (DYOR) kültürü, aidiyet/kimlik inşası ve tekrar-dopamin döngüsü gibi mekanizmaları somut örneklerle görünür kılıyor.

🔗 Belgeseli izlemek için:
https://www.hbomax.com/tr/tr/shows/q-into-the-storm/031763fb-40bb-4e47-8a71-123f7a31ac09

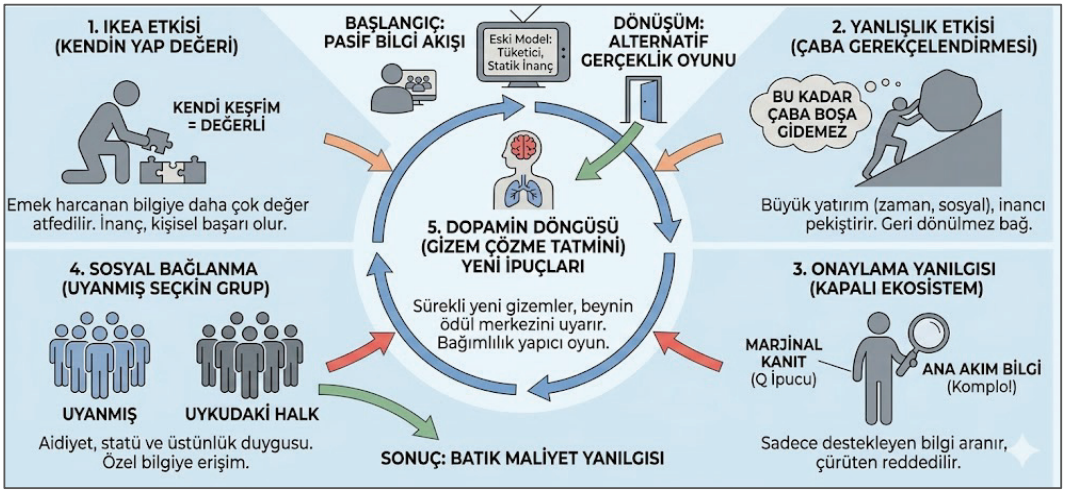
Sürekli yeni ipuçlarının ortaya çıkması ise beynin ödül sistemini uyarır; her yeni bağlantı ve her "keşif" kısa süreli bir tatmin yaratarak komplo teorisini durağan bir inançtan çıkarıp bağımlılık yaratan bir dedektiflik oyununa dönüştürür. Bu oyunlaştırma stratejisinin nihai ve en güçlü sonucu ise batık maliyet yanılgısında ortaya çıkar. Birey, komplo teorisini çözmek için ne kadar çok zaman, duygusal enerji ve sosyal çevre harcarsa, teorinin yanlış olduğunu kabul etmenin psikolojik ve sosyal maliyeti o kadar artar. Oyundan vazgeçmek yalnızca bir fikirden vazgeçmek değil; aynı zamanda büyük bir kişisel yatırımı değersiz ilan etmek, "uyanmış" kimliğini reddetmek ve grubun aidiyetini kaybetmek anlamına gelir. Bu ağır maliyet, kanıtlar ne kadar güçlü olursa olsun, bireyi inanç sistemine sadık kalmaya zorlar. Sonuç olarak oyunlaştırılmış komplo teorileri yalnızca yanlış bilgi üretmez; aynı zamanda son derece dirençli, kendi kendini sürdüren bir inanç ve aidiyet sistemi kurarak dezenformasyonu geçici bir içerik sorunu olmaktan çıkarıp kalıcı bir kültürel ve psikolojik fenomene dönüştürür.

🎧 DİNLE

QAnon and Conspiracy Narratives başlıklı podcast, QAnon ve benzeri komplo anlatılarının psikolojik dinamiklerini ele alır.

🔗 Dinlemek için:

https://www.youtube.com/watch?v=CRE4ImMk0c4



Şekil 2.3.5 *Oyunlaştırılmış dezenformasyon: Pasif izleyiciden aktif oyuncuya*

TEMEL ÇIKARIMLAR

Bu bölüm, dijital platformların ve sosyal medyanın, önceki bölümlerde öğrendiğimiz bilişsel önyargıları nasıl ticari bir modele dönüştürdüğünü anlatır. Tristan Harris'in deyimiyle teknoloji şirketleri, "beyin sapımıza inebilmek için" bir yarış içindedirler; en ilkel, dürtüsel ve savunmasız yanımızı hedeflerler. Bu platformlarda yaşanan sorun bir "irade eksikliği" değil, insan psikolojisinin açıklarını kullanan bilinçli bir tasarımdır. Sosyal medya, dikkatimizi mümkün olduğunca uzun süre ekranda tutmak, dikkat ekonomisi için dopamin sistemimizi ve sosyal korkularımızı "hackler".

Temel Kavramlar ve Mekanizmalar

Dikkat Ekonomisi: Dijital platformlarda "ücretsiz" hizmet yoktur. Biz müşteri değiliz; dikkatimiz ve davranışlarımız reklamverenlere satılan "hammaddedir". Amaç, kullanıcıyı sürekli platformda tutarak gelecekteki davranışlarını tahmin etmek ve yönlendirmektir.

"Durdurma İşaretleri"nin Yokluğu: Eski dünyada gazetelerin sonu, kitapların bölümleri gibi beynimize "dur ve düşün" diyen doğal işaretler vardı. Dijital tasarımcılar sonsuz kaydırma (*infinite scroll*) ve otomatik oynatma ile bu işaretleri yok etmiştir. Beyin durup düşünme fırsatı bulamadığı için, eleştirel sistem 2 devreye giremez ve kişi saatlerce otomatik pilotta, sistem 1'de kalır.

Değişken Ödül: Kumar makinelerinde kullanılan "değişken oranlı pekiştirme" ilkesi sosyal medyaya uyarlanmıştır. Bir bildirimin ne zaman geleceğini veya içeriğin ne olacağını bilmemek, belirsizlik, beynin ödül sistemini, dopamin ile sürekli tetikler. "Acaba yeni bir şey var mı?" sorusu, bizi sürekli sayfayı yenilemeye iter.

Öfke Algoritması: Algoritmalar "doğru" bilgiyi değil; beğeni, yorum, paylaşım gibi etkileşim getiren bilgiyi sever. İnsanları en çok harekete geçiren duygu öfke ve korkudur. Bu yüzden algoritmalar, kutuplaştırıcı ve kışkırtıcı içerikleri bilerek öne çıkarır.

Yenilik Arayışı: Beynimiz evrimsel olarak yeni ve şaşırtıcı olana odaklanır. Yalan haberler genellikle gerçeklerden daha "yeni", daha dramatik ve daha duygusal olduğu için, sosyal medyada doğrulardan çok daha hızlı yayılır.

Uyku Etkisi (Kaynağı Unut, Mesajı Hatırla): Hafızamız, bir bilginin içeriğini kaydederken, o bilginin nereden geldiğini, kaynağını zamanla siler. Güvenilmez bir kaynaktan duyduğumuz bir yalanı başta reddetsek bile, zamanla kaynağı unutup sadece mesajı hatırladığımız için o bilgi bize tanıdık ve "doğru" gelmeye başlar.

Oyunlaştırılmış Komplo: Modern dezenformasyon, insanlara hazır bilgi vermek yerine onlara "Kendi araştırmanı yap" (DYOR) der. İnsanlar,

parçaları birleştirip bir "gerçeğe" ulaştıklarını sandıklarında, kendi emekleriyle buldukları bu sonuca, yanlış bile olsa sıkı sıkıya bağlanırlar. Bu süreç, komplo teorisine inanmayı bir tür dedektiflik oyununa dönüştürür.

2.3. KENDİNİZİ TEST EDİN

Soru 1: B. F. Skinner'ın deneylerine göre, bir davranışı (örneğin butona basmak ya da ekranı kaydırmak) alışkanlık ve bağımlılık hâline getiren en güçlü ödül sistemi hangisidir?

A) Sürekli ödül (Her basışta ödül verilmesi)

B) Değişken ödül (Rastgele zamanlarda, belirsiz ödül)

C) Gecikmeli ödül

D) Hiç ödül verilmemesi

Soru 2: "Uyku etkisi" dezenformasyonun yayılmasında nasıl bir rol oynar?

A) İnsanların yalan bilgileri unutup yalnızca doğru bilgileri hatırlamasını sağlar.

B) Bilginin içeriğini hatırlanıp, geldiği güvenilmez kaynak unutulur.

C) Bilgi kaynaklarının daha şeffaf hâle gelmesini sağlar.

D) Hafızayı güçlendirir.

Soru 3: Sosyal medya algoritmaları temel olarak neyi artırmak üzere tasarlanmıştır?

A) Toplumsal barış ve huzur

B) Doğru bilgi ve eğitimi yaymak

C) Kullanıcı mutluluğu

D) Etkileşim ve platformda geçirilen süre

2.3. MERAKLISINA EK KAYNAKLAR

Fiske, S. T., & Taylor, S. E. (2021). *Social cognition: From brains to culture* (4. Baskı.). SAGE Publications.

Friggeri, A., Adamic, L. A., Eckles, D., & Cheng, J. (2014). Rumor Cascades. *Proceedings of the Eighth International Conference on Weblogs and Social Media*.

McGuire, W. J. (1964). Inducing resistance to persuasion: Some contemporary approaches. In L. Berkowitz (Der.), *Advances in Experimental Social Psychology* (Cilt 1, ss. 191–229). Academic Press.

Pennycook, G., & Rand, D. G. (2018). The implied truth effect: Attaching warnings to a subset of fake news stories increases perceived accuracy of stories without warnings. *Management Science*, 66(11), 4944–4957.

Pennycook, G., et al. (2020). Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. *Psychological Science*, 31(7), 770–780.

Roozenbeek, J., & van der Linden, S. (2019). The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, 22(5), 570–580.

Sunstein, C. R. (2018). *#Republic: Divided democracy in the age of social media.* Princeton University Press.

Bölüm 3

Biz, Onlar ve Algoritmalar: Kutuplaşma ve Güven Krizi

🎯 TARTIŞMA SORULARI

1. Yankı odaları ve filtre balonları nasıl oluşur? Farkları nelerdir?
2. Neden kendimizle benzer görüşteki insanlarla iletişim kurarız?
3. Suskunluk sarmalı dijital çağda nasıl işler?
4. Komplo teorilerine neden inanırız?
5. Bilgi düzensizlikleri toplumsal kutuplaşmaya nasıl yol açar?

Giriş

Bu bölüm ilk olarak sosyal medyanın bizi nasıl sadece kendimiz gibi düşünen insanlarla dolu yankı odalarına hapsettiğini inceler; algoritmaların bizi ekran başında tutmak için sürekli hoşumuza giden şeyleri gösterip farklı sesleri nasıl kıstığını ve bunun sonucunda kendi fikrimizin tek doğru olduğunu sanma yanılgımızı ele alır. Ardından siyasi tartışmaların neden bir fikir alışverişinden çıkıp "biz ve onlar" kavgasına dönüştüğünü tartışır; karşı tarafı sadece "farklı düşünen biri" değil, "düşman" olarak görmemize neden olan korku ve öfke duygularının mantığımızı nasıl devre dışı bıraktığını ortaya koyar. Son olarak ise güvensizliğin ve kafa karışıklığının nasıl yayıldığını ele alır; uzmanlara inanmak yerine neden komplo teorilerine sığındığımızı, yalanın gerçeği nasıl gölgelediğini ve şüphenin nasıl kasıtlı biçimde kullanıldığını analiz eder.

Neden Birbirimizi Duymuyoruz?

1990'ların başı, 20. yüzyılın son büyük iyimserlik dalgasının zirvesini temsil ediyor; hem jeopolitik hem de teknolojik alanlarda küresel ölçekte bir paradigma değişimini tetikleyen iki büyük sarsıntının eş zamanlı etkisiyle tarihi bir dönüm noktası olarak kabul ediliyordu. Bu dönemin en belirleyici unsuru, yaklaşık yarım asır boyunca dünyayı nükleer savaş tehdidi altında iki kutba ayıran ideolojik kutuplaşma dönemini bitiren Soğuk Savaş'ın sona ermesiydi. 9 Kasım 1989'da Berlin Duvarı'nın yıkılması ve 1991'de Sovyetler Birliği'nin resmen dağılmasıyla simgeleşen bu süreç, Marksist-Leninist totalitarizme karşı liberal demokrasinin ve merkezi planlamaya karşı serbest piyasa kapitalizminin kesin bir zaferi olarak yorumlandı. Bu atmosfer, siyaset bilimci Francis Fukuyama'nın 1992 tarihli *Tarihin Sonu ve Son İnsan* adlı çalışmasıyla[23] teorik bir zemine oturtularak Batı liberal demokrasisinin nihai yönetim

[23] Fukuyama, F. (2012). *Tarihin sonu ve son insan* (Z. Dicleli, Çev.). Profil Yayıncılık. (Orijinal eserin yayın tarihi 1992)

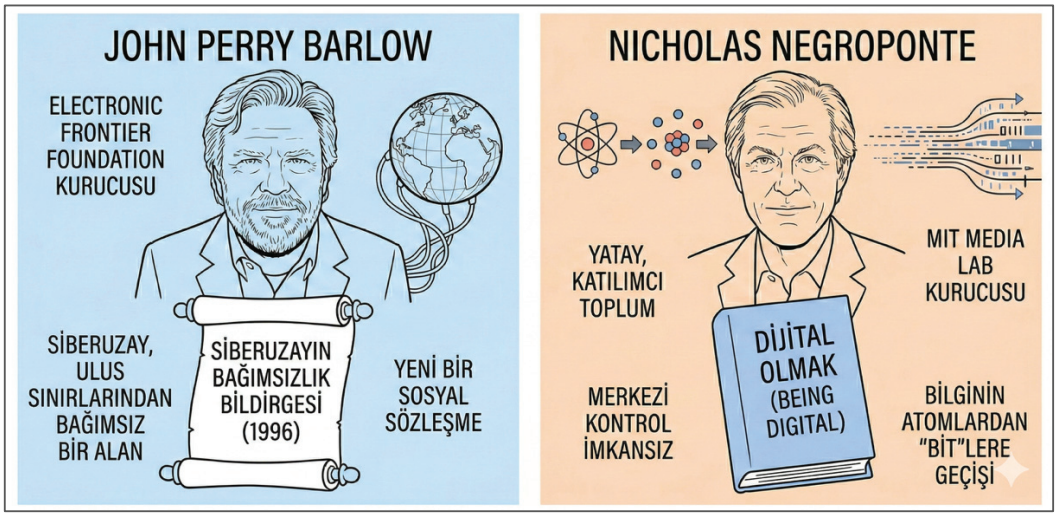
modeli olduğu fikrini pekiştirdi ve Batı'da, büyük güç çatışmalarının yerini küresel iş birliği ile uluslararası hukukun üstünlüğünün alacağı yeni bir dünya düzenine girildiği inancını güçlendirdi.

Jeopolitik iyimserliği somut bir zemine oturtan asıl devrim ise bilgi teknolojilerinde yaşandı; Tim Berners-Lee'nin CERN'de geliştirdiği world wide web (www) protokolü sayesinde, daha önce ARPANET gibi sadece uzmanların kullandığı sınırlı ağlar, 1990'ların ortasında grafik tarayıcıların da yardımıyla halka açıldı ve internet laboratuvarlardan çıkıp evlerimize girdi. Bu teknolojik sıçrama, sınırların anlamsızlaşacağı, şeffaflığın artacağı ve bireylerin geleneksel medya otoritesinden kurtulacağı inancını doğurdu. Soğuk Savaş'ın bitişiyle birleşen bu teknolojik atılım, küresel çapta güçlü bir tekno-iyimserlik rüzgârı estirdi; o dönemin ruhuna göre internet, sadece ekonomik bir araç değil, demokrasiyi yayacak, sansürü bitirecek ve kürsel bir bilişsel ortaklık kuracak sihirli bir değnekti. Kendilerini "siber-ütopyacılar" olarak adlandıran dönemin öncüleri, bu ağları hiyerarşiyi ve eşitsizliği yok edecek, insanlık tarihinin en büyük, merkeziyetsiz demokratikleşme projesi olarak selamlıyorlardı. Bu dijital rüyanın mimarları arasında öne çıkan iki isim, dönemin özgürlükçü ruhunu tam olarak özetliyordu. Electronic Frontier Foundation'ın kurucusu John Perry Barlow, 1996'da yayımladığı *Siberuzayın Bağımsızlık Bildirgesi*[24] ile adeta sanal dünyanın manifestosunu yazdı. Barlow, hükümetlere açıkça meydan okuyarak internetin, devletlerin kanunlarından ve sınırlarından bağımsız, tamamen özgür bir alan olduğunu ve kendi sosyal sözleşmesini yaratacağını haykırıyordu. Benzer bir heyecanla, MIT Media Lab'in kurucusu Nicholas Negroponte de *Dijital Olmak (Being Digital)* kitabında[25] devrimci bir dönüşümü müjdeliyordu. Negroponte'ye göre insanlık, "fiziksel

[24] Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. The WAC Clearinghouse. https://wacclearinghouse.org/rhetnet/barlow/barlow_declaration.html

[25] Negroponte, N. (1995). *Being digital*. Knopf.

atom”lar çağından “dijital bit”ler çağına geçiyordu ve bu yeni dünyada merkezi kontrol imkansızlaşacak, yerini herkesin eşit söz hakkına sahip olduğu, hiyerarşisiz ve katılımcı bir toplum alacaktı.



Şekil 3.1.1 *Önde gelen figürler ve iddiaları*

Siber-ütopyacılığın teorik temelleri, 20. yüzyılın etkili iletişim kuramcılarının vizyonlarına dayanıyordu ve internet, bu teorilerin nihayet somutlaştığı ideal mecra olarak görüldü. Bu iyimser bakış açısının merkezinde, Kanadalı iletişim kuramcısı Marshall McLuhan'ın 1960'larda ortaya attığı "küresel köy"[26] kavramı yer alıyordu; McLuhan, elektronik medyanın etkisiyle coğrafi mesafelerin anlamsızlaşacağını öngörmüştü. Siber-ütopyacılar için internet bu öngörünün en güçlü kanıtıydı; çünkü fiziksel sınırları kaldırarak "coğrafyanın sonunu" getiriyor, televizyon ve gazete gibi merkezi medya tekellerini kırarak bireylere kendi yayınlarını yapma gücü veriyordu. Böylece internetin, herkesin herkesle doğrudan iletişim kurabildiği, karşılıklı anlayış ve empatinin geliştiği, yeniden canlanmış devasa bir küresel topluluk yaratacağı düşünülüyordu.

[26] McLuhan, M. (1994). *Understanding media: The extensions of man*. McGraw-Hill.

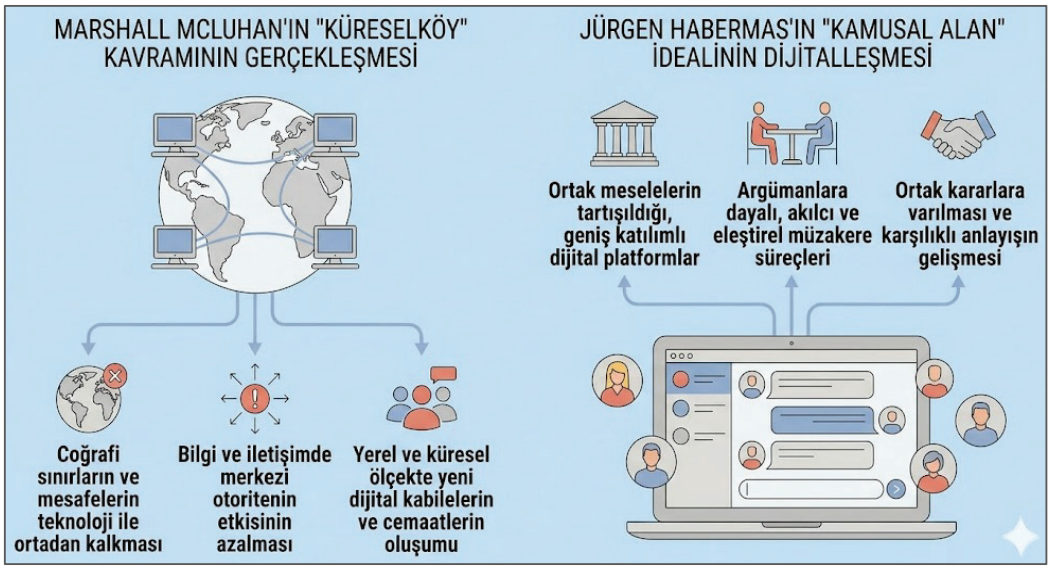
Siber-ütopyacılığın ikinci büyük teorik dayanağı, Alman düşünür Jürgen Habermas'ın meşhur "kamusal alan"[27] kavramıydı. Habermas, 18. yüzyıl Avrupa'sında insanların kahvehanelerde veya salonlarda bir araya gelerek siyaseti akılcı bir şekilde tartıştığı özgür ortamı idealize etmişti; internetin öncüleri ise dijital dünyayı bu idealin çok daha büyük ve kusursuz bir versiyonu olarak kurguladılar. Onlara göre internet, farklı kültürlerden ve zıt görüşlerden milyarlarca insanın buluştuğu modern ve devasa bir "dijital agora" olacaktı. Bu sanal meydanda, kimin ne kadar güçlü veya zengin olduğu değil, sadece argümanların mantığı önem kazanacak; manipülasyondan ve duygusal tepkilerden arınmış, tamamen akla dayalı bu özgür tartışmalar sayesinde toplumlar önyargılarını aşarak evrensel bir uzlaşma zemininde buluşabilecekti.

Erken dönem siber-ütopyacılara göre internetin vaadi hem çok net hem de devrimciydi: Dijital dünya, cehaletin ve önyargıların sonunu getirip, küresel barışın ve katılımcı demokrasinin geliştiği bir ortam yaratacaktı. Bu bakış açısı, teknolojinin gücüyle karmaşık toplumsal ve siyasal sorunların aşılabileceğine, insanlığın daha adil ve mantıklı bir geleceğe geçiş yapabileceğine dair sarsılmaz bir umudu temsil ediyordu. Henüz dijitalleşmenin yaratacağı sorunların hiç fark edilmediği, sadece sunduğu fırsatlara odaklanılan bu iyimser dönem tarihe bir altın çağ arayışı olarak geçti.

Bugün içinde yaşadığımız dijital ortam, Antik Yunan'daki o özgür tartışma meydanı "agora"dan ne yazık ki oldukça uzaktır; teknoloji ve siyaset bilimcilerin "splinternet", parçalanmış internet olarak tanımladığı bu yeni yapı, sanal duvarlar ve ideolojik sınırlarla bölünmüş, birbirinden kopuk adacıklara dönüşmüştür. Birbirini duymayan, hatta birbirine karşı seçici bir

[27] Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* (T. Burger, Çev.; F. Lawrence'ın katkılarıyla). Polity Press. (Orijinal eserin yayın tarihi 1962)

iletişimsizlik ve düşmanlık besleyen bu kümeler, kendi içine kapalı izole topluluklar halini almıştır. Bu grupların her biri kendi iç doğrularını mutlak hakikat sayarken, dışarıdan gelen her farklı sesi "düşman propagandası", "yanlış bilgi" veya "kötü niyetli manipülasyon" olarak etiketleyerek reddetmekte, böylece gruplar arası etkileşim ve öğrenme kapılarını tamamen kapatmaktadır.



Şekil 3.1.2 *Siber-ütopyacılığın kökleri: 20. Yüzyılın iletişim vizyonları*

Yaşadığımız bu derin ayrışma ve dijital yalnızlık, sanıldığı gibi sadece basit bir fikir uyuşmazlığından ibaret değildir; asıl büyük tehlike, bir toplumu bir arada tutan ve "müşterekler" dediğimiz o ortak zeminin yavaş yavaş yok olmasıdır. Müşterekler; hepimizin doğru kabul ettiği gerçekleri, ahlaki değerleri ve ülkenin öncelikli konularını kapsayan temel uzlaşma noktalarıdır. Ancak günümüzde ne üzerinde anlaştığımız ortak bir hakikat, ne herkesin kabul ettiği ortak bir gündem, ne de kelimelere aynı anlamı yüklediğimiz ortak bir dilimiz kalmıştır.

Bu ayrışmanın yıkıcı etkileri, günlük etkileşimlerimizde somutlaşmaktadır. Dijital dünyanın bir köşesinde "ulusal kahraman" veya "vizyoner" ilan

edilen bir isim, hemen yanındaki bir başka grupta "halk düşmanı" veya "hain" olarak damgalanabilmektedir; dolayısıyla aynı eylem, bulunulan yere göre tamamen zıt ahlaki anlamlar kazanmaktadır. Sorun sadece kişilerle sınırlı kalmamakta, gerçekliğin kendisi de bu durumdan nasibini almaktadır. Bir grubun tartışma-sız bilimsel veri kabul ettiği iklim krizi veya aşı gibi konular, diğer grup tarafından küresel bir manipülasyon veya kurgusal bir senaryo olarak reddedile-bilmektedir. Gerçeklik artık objektif bir dayanak olmaktan çıkmakta, grubun inancına göre şekillenen esnek bir araca dönüşmektedir. Ne yazık ki bu güven ve hakikat krizi sadece ekranlarda kalmamakta; siyasetten ekonomiye, kişisel ilişkilerimize kadar yayılarak toplumsal hayatı olumsuz etkilemektedir. Ortak veriler ve etik değerler üzerinde uzlaşamadığımız için, rasyonel bir tartışma veya demokratik bir zemin bulmak da imkansızlaşmaktadır.

Dijital dünyanın bizi hapsettiği yankı odalarından veya algoritmaların manipülasyonundan şikâyet etsek de bu duvarların temelinde aslında insana dair özelliklerin yattığını gözden kaçırmamalıyız. Teknoloji, özümüzde var olan bir eğilimi sadece güçlendirmektedir; bu eğilim, sosyolojide "homofili", benzerlik ilkesi (*homophily*) olarak tanımlanan, bireylerin yaş, eğitim veya siyasi görüş gibi konularda kendilerine benzeyen kişilere yönelme arzusudur. 1954 yılında Lazarsfeld ve Merton tarafından kavramsallaştırılan ve kültürümüzde "tencere yuvarlanır kapağını bulur" atasözüyle karşılık bulan bu olgu, sosyal ilişkilerin yapısal bir kuralı niteliğindedir. Nitekim McPherson ve arkadaşlarının 2001 tarihli çalışması, modern toplumlardaki sosyal bağların yaklaşık %80'inin homofiliye dayandığını ortaya koymaktadır; çünkü insanlar, kendilerine benzeyenlerle bir arada bulunarak bilişsel ve duygusal bir konfor alanı yaratmayı tercih etmektedir.[28]

[28] McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, *27*, 415–444.

Kendisiyle aynı düşünen ve benzer özellikler taşıyan insanlarla birlikte olmak, bireye psikolojik ve sosyal açıdan üç temel fayda sağlamaktadır. Bunlardan ilki, ortak değerlerin ve kültürel kodların paylaşılması sayesinde anlaşmanın kolaylaşmasıdır; bu durum zihinsel çabayı azaltarak iletişimi hızlandırmakta ve "bilişsel akıcılık" yaratmaktadır. İkinci avantaj, kişinin fikirlerinin grubu tarafından daimî olarak onaylanmasıyla ortaya çıkmaktadır. Bu onaylanma hali, beyindeki ödül mekanizmasını çalıştırarak benlik saygısını güçlendirmekte ve bireyin kendi doğrularına olan inancını artırmaktadır. Üçüncü olarak ise bu homojen gruplar, tartışma ve eleştiriden uzak, gerilimin olmadığı güvenli bir liman sunarak çatışma riskini düşürmekte ve grup içi uyumu maksimize etmektedir.

Şekil 3.1.3 *Homofili: Sosyal ağlarda benzerlik eğilimi*

Homofili, kökeni insanlık tarihine dayanan bir eğilim olsa da dijital çağda yapısal bir dönüşüm geçirmiştir. İnternet öncesi dönemde fiziksel ve coğrafi sınırlar, bireyleri özellikle şehirlerde, kamusal alanlarda "öteki" ile karşılaşmaya mecbur bırakırken, bu zorunlu temas önyargıların azalmasına olanak tanımaktaydı. Ancak dijital dünya sosyal ayrışmanın maliyetini sıfıra

indirmiştir; kullanıcılar artık hoşlanmadıkları görüşleri hiçbir fiziksel veya sosyal bedel ödemeden tek tıkla engelleyebilmektedir. Bu mekanizma, bireylerin dünyanın herhangi bir yerindeki benzerleriyle zahmetsizce kapalı mikro-topluluklar kurmasını sağlayarak homofiliyi hiper-aktif bir seviyeye taşımakta ve bizleri yankı odalarına, filtre balonlarına sürüklemektedir. Kendi kapalı gruplarımızın içine o kadar gömülürüz ki, dış dünyanın da bizimle aynı fikirde olduğunu varsaymaya başlarız; seçim sonuçlarında yaşanan toplumsal şaşkınlıkların temelinde yatan bu duruma "yanılsamalı çoğunluk etkisi" adı verilmektedir.

Yankı Odaları

Sosyal medya çağında sıkça birbirine karıştırılan "yankı odası" ve "filtre balonu" kavramları, aslında oluşum şekilleri ve etkileri bakımından birbirinden tamamen ayrılır. Bu ayrımı netleştirmek için önce "yankı odası"na odaklanalım. Yankı odası, bireyin tamamen kendi hür iradesiyle ve bilinçli tercihleriyle oluşturduğu kapalı bir iletişim ortamıdır. Bu ortamda kişi, sadece kendi dünya görüşünü ve önyargılarını destekleyen sesleri duymayı seçerken; hoşuna gitmeyen eleştirileri, karşıt kanıtları veya farklı fikirleri sistematik olarak dışlar, hatta engeller. Bu durum, bilgiye ulaşım kanallarının kasıtlı olarak daraltıldığı ve yalnızca içeride yankılanan sesin doğru kabul edildiği bir epistemik kapanma halidir.

İnternetin demokratik potansiyeline dair övgülerin zirve yaptığı bir dönemde, hukuk profesörü Cass Sunstein 2001 yılında yayımladığı *Republic.com* (yeni adıyla *#Republic*) eseriyle bu tehlikeyi erkenden fark etmiştir.[29] Sunstein'a göre internetin sağladığı sınırsız filtreleme gücü demokrasi için varoluşsal bir risk taşımaktadır; çünkü sağlıklı bir demokrasi, farklı fikirlerin

[29] Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press https://doi.org/10.2307/j.ctv8xnhtd

çarpıştığı planlanmamış karşılaşmalara muhtaçtır. İnsanların kendileri gibi düşünmeyenlerle tesadüfen de olsa karşılaşması, toplumsal hoşgörünün temelidir. Ancak yankı odalarında sürprize veya tesadüfe yer yoktur; burada sadece kendi inançlarımızın sürekli tekrarı mevcuttur. Birey dijital dünyayı kendi suretinde şekillendirdiğinde, ortaya Nicholas Negroponte'nin tabiriyle sadece kişinin kendi tercihlerini, görüşlerini ve ilgilendiklerini takip ettiği yansıtan bir Günlük Ben (*Daily Me*) gazetesi çıkmaktadır[30].

Radikal bir siyasi Facebook/Telegram grubu, bir komplo teorisi forumu, fanatik bir aşı karşıtı topluluk veya aşırı milliyetçi bir futbol takımı forumu örneklerinde olduğu gibi bir yankı odasının içinde yalnızca bilginin akışı değil, aynı zamanda bireylerin düşünce yapısı da çarpıtılmaktadır. Bu kapalı devrede "epistemik kapanma" süreci derinleşmekte; grup, dış dünyadan gelen ana akım medya veya bilimsel kaynaklara karşı tam bir düşmanlık geliştirmektedir. Bilgi hiyerarşisi tersine dönmekte; sadece içerideki liderlerin onayladığı bilgi "hakikat" sayılırken, dış dünya "yalan" veya "propaganda" olarak etiketlenmektedir. Bununla birlikte, bireysel teyit yanlılığı da kurumsal bir ritüele dönüşmektedir. Grup üyeleri, sadece inançlarını pekiştiren içerikleri paylaşmakta; aksi yönde somut bir kanıt sunulduğunda ise kolektif bir bağışıklık sistemi devreye girmektedir. Grubun saflığını korumak adına, bu habere anında saldırılmakta ve karşıt görüşü paylaşan kişi linç edilerek dışlanmaktadır. Ayrıca sosyal psikolojinin "grup içi kutuplaşma"

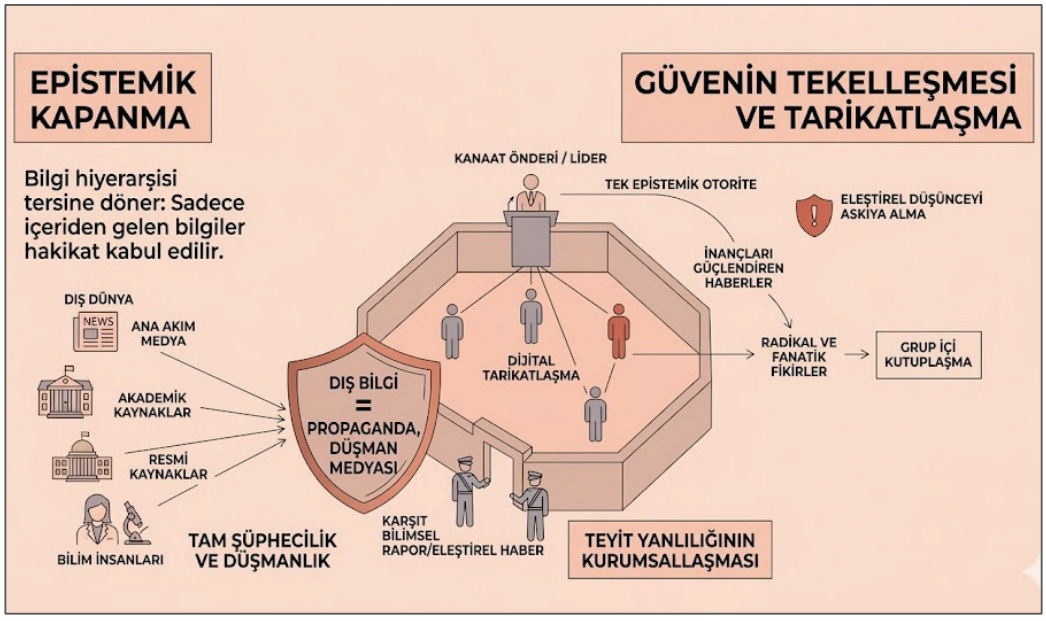
KAVRAM:
SEÇİCİ MARUZ KALMA

Neyi açıklar?: Seçici maruz kalma (*selective exposure*), bireylerin kendi görüş ve ideolojileri ile uyumlu olmayan bilgi kaynaklarına karşı önyargılı olmalarını ve bunlarla uyumlu bilgi kaynaklarını takip etme eğilimlerini ifade eder.

Neden önemli?: Bu durum, dijital dünyada yankı odalarının oluşmasına neden olan en önemli psikolojik motivasyonlardan biridir.

[30] Negroponte, 1995.

ilkesi gereği, benzer düşünen bireyler bir araya geldiklerinde fikirleri daha uç noktalara kaymakta ve başlangıçtaki ılımlı görüşler zamanla radikal bir fanatizme evrilmektedir. Son olarak güven tekelleşmekte; bireyler dış kaynaklara güveni yitirip hakikatin tek kaynağı olarak grup liderlerini görmeye başlamakta, bu da dijital bir "tarikatlaşma" süreci yaratmaktadır.



Şekil 3.1.4 *Epistemik kapanma ve dijital tarikatlaşma: Yankı odasının derinleşmesi*

X (eski adıyla Twitter) veya Reddit gibi platformlar, yankı odası mimarisinin doğal olarak gelişebileceği en elverişli zeminleri sunmaktadır. Bu platformların tasarımı, bireyin kendi dijital duvarlarını örmesini sağlayan iki temel araca dayanır. İlki, kullanıcının bilgi kaynaklarını ve güveneceği kişileri bizzat seçerek kendi gerçekliğini inşa etmesine olanak tanıyan "takip et" mekanizmasıdır. İkinci olarak ise kullanıcının takip tercihleri ve etkileşim geçmişi, platformun algoritması tarafından öğrenilir. Algoritma, kullanıcının sevdiği türdeki içeriği daha fazla göstererek yankı odasının duvarlarını daha da yükseltir. Bu, kullanıcıyı daha çok platformda tutmak için tasarlanmış bir

optimizasyon olsa da sonuçta entelektüel izolasyona yol açar.

Eğer bir liberal kullanıcı yalnızca liberalleri, bir muhafazakâr kullanıcı yalnızca muhafazakârları ya da bir aşı karşıtı yalnızca komplo teorisyenlerini takip ediyorsa, bu kişiler fiilen farklı gezegenlerde yaşıyor demektir. Bu kapalı odaların içinde benzer düşüncelerin sesleri yankılanıp büyürken, karşıt seslere tahammülü imkânsız kılan bir gürültüye dönüşür. Yankı odasındaki kişi için en büyük tehlike, kendi sesinin tekrar eden yankısını, tüm toplumun sesi veya tek hakikat sanmasıdır. Bu yanılsama, demokratik diyaloğu ve toplumsal uzlaşmayı imkânsız hale getirir.

Filtre Balonları

Yankı odasının duvarlarını bizzat kendi tercihlerimizle örsek de "filtre balonu"[31] dediğimiz görünmez fanus, algoritmalar tarafından bizden habersizce inşa edilmektedir. İnternet aktivisti Eli Pariser'ın literatüre kazandırdığı bu kavram, arama motorlarının deneyimlerimizi kişiselleştirerek bizi nasıl yalıttığını göstermektedir. Pariser, dijital dünyanın tarafsız bir ayna olmadığını 2011 yılında gerçekleştirdiği meşhur BP (*British Petroleum*) deneyi ile kanıtlamıştır. Farklı görüşlere ve yaşam tarzlarına sahip iki arkadaşından Google'da aynı anda BP araması yapmalarını isteyen Pariser, şaşırtıcı bir tabloyla karşılaşmıştır. Algoritmanın muhtemel çevre ve/ya politik ekonomi ilgi alanlarını tespit ettiği kişi için ekran tamamen felaketin etkilerine odaklanmış; petrol sızıntısının yarattığı çevre tahribatı, ölen deniz canlıları ve hisse senetlerindeki düşüş gibi çevresel ve finansal analizlerle dolup taşmıştır. Buna karşın, tüketici profiline sahip ikinci kişinin ekranı felaket görüntülerinden tamamen arındırılmıştır. Bu kullanıcıya yalnızca en yakın benzin istasyonları, yakıt promosyonları ve kurumsal duyurular gösterilirken, küresel

[31] Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

çapta yankı uyandıran o büyük felakete dair tek bir haber veya görsel dahi sunulmamıştır. Bu çarpıcı deney, dijital dünyanın en temel dinamiklerinden birini gözler önüne sererek; aynı anda aynı aramayı yapan kullanıcıların aslında iki farklı internet deneyimlediğini ve kişiselleştirmenin bir tercih değil, platformların çalışma prensibi olduğunu kanıtlamıştır. Google, Facebook veya X gibi dev yapıların temelinde yatan algoritmalar; geçmiş aramalarımızdan tıkladığımız bağlantılara, konumumuzdan demografik özelliklerimize kadar uzanan devasa bir veri yığınını analiz ederek neyi görmek isteyeceğimizi şaşırtıcı bir hızla tahmin etmektedir. İşte dijital ekosistemde filtre balonunu yaratan temel güç de bu tahmin mekanizmasıdır; zira algoritmanın asıl amacı, dikkatimizi çekecek ve duygusal tepki uyandıracak içerikleri önceliklendirerek bizi platformda mümkün olduğunca uzun süre tutabilmektir.

Algoritmaların bu işleyiş biçiminin kaçınılmaz yan etkisi, dünya görüşümüze ters düşen, bizi rahatsız eden veya inançlarımızı sorgulatan her türlü bilginin sistemli ve şeffaf olmayan bir şekilde filtrelenmesidir. Bu süreç, bireyi sadece kendi düşüncelerini onaylayan içeriklerle ve benzer görüşteki insanlarla çevrili kapalı bir dijital alana hapsetmektedir. Kısa vadede bize keyifli ve konforlu bir deneyim sunsa da bu kişiselleştirme uzun vadede farklı fikirlere karşı empatiyi köreltmekte, toplumsal kutuplaşmayı derinleştirmekte ve sosyal güveni zedelemektedir. Eli Pariser'ın belirttiği gibi, bu durum dijital alanda yalnızca kendi sesimizin yankısını duyduğumuz yalıtılmış bir fanus yaratır. Her bireyin kendine özel hazırlanmış tek tip bir bilgi ile beslendiği bu ortamda, vatandaşların ortak bir gerçeklik zemininde buluşması imkânsızlaşır; sonuç olarak dijital dünya, bireyi bilgiyle güçlendirmek yerine, onu farkında bile olmadığı bir "algoritmik sansür" ile karşı karşıya bırakmaktadır.

Filtre balonu, modern dijital ekosistemlerin temel yapı taşlarından biri haline gelmiştir. Google, Facebook, Netflix ve TikTok gibi devasa platformlar; tıklamalarımızdan izleme geçmişimize, beğenilerimizden konum bilgilerimize

kadar tüm dijital ayak izlerimizi titizlikle analiz etmektedir. Bu algoritmalar, potansiyel olarak ilgimizi çekmeyecek içerikleri sistematik olarak filtreleyerek, sadece etkileşime gireceğimiz ve bizi platformda daha uzun süre tutacak içerikleri önümüze getirir. Sonuç olarak ortaya çıkan bu kişiselleştirilmiş ama tekil bilgi evreni, her kullanıcı için dış dünyadan yalıtılmış, kendine has dijital bir oda yaratmaktadır.

🎬 İZLE

Ekranınızda gördüğünüz sonuçlar neden yanınızdaki arkadaşınızdan farklı? Eli Pariser, algoritmaların bizim için ördüğü görünmez duvarları anlatıyor.

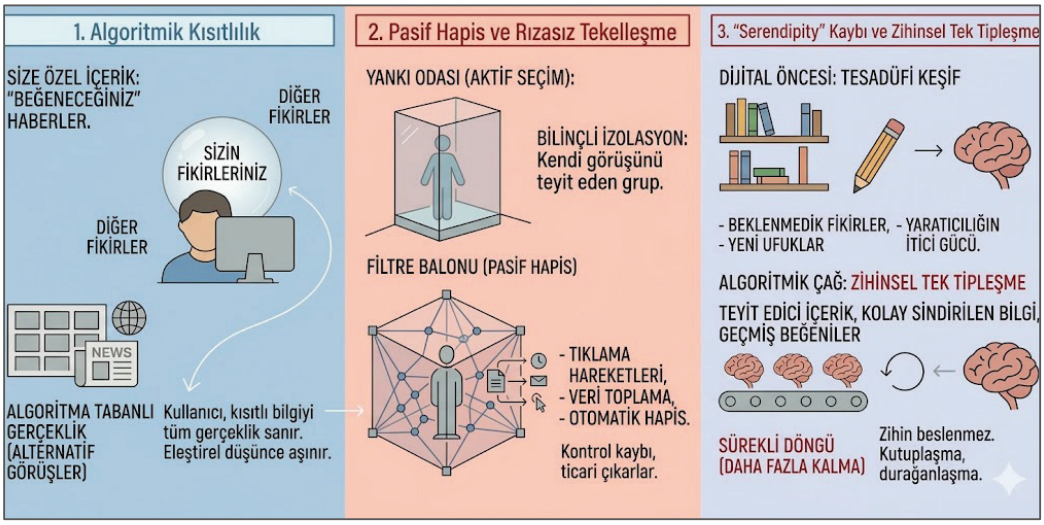
🔗 Videoyu izlemek için:

https://www.youtube.com/watch?v=B8ofWFx525s

Bu dijital fanusta yaşamanın sosyolojik ve bilişsel açıdan son derece kritik sonuçları vardır. Bunlardan ilki ve en sinsisi, kullanıcının bir balon içinde olduğunun farkında bile olmamasıyla ortaya çıkan görünmezlik ve algısal kısıtlılık durumudur. Algoritmalar şeffaf çalışmaz; Google veya Facebook size "Siyasi görüşüne uymadığı için şu haberi gizledik" diye bir uyarı vermez. Bunun sonucunda kullanıcı, ekranında gördüğü sınırlı bilgi kümesini tüm gerçeklik zanneder ve bu yanılsama toplumsal empatiyi köreltir. İkinci tehlike ise rızamız dışında gerçekleşen pasif hapis durumudur. Yankı odasına birey kendi iradesiyle, bilinçli bir seçimle girerken; filtre balonuna tıklama geçmişi ve dijital ayak izleri üzerinden, tamamen habersizce hapsedilir. Algoritmaların ticari çıkarlar doğrultusunda, kullanıcıdan izin almadan yürüttüğü bu süreç, bireyin bilgi akışı üzerindeki kontrolünü tamamen kaybetmesine yol açmaktadır. Dijital fanusta yaşamanın üçüncü kritik sonucu, yaratıcılığın temel kaynağı olan "beklenmedik keşiflerin" kaybı ve bunun yol açtığı entelektüel obezitedir. Eskiden bir kütüphane rafında gezinirken, aradığınız kitabın hemen yanında tesadüfen duran bambaşka bir eserle karşılaşıp yepyeni

ufuklara açılmanız mümkündü; işte özgün düşünceyi besleyen bu plansız keşiflerdir. Ancak algoritmalar, sizi platformda daha uzun süre tutabilmek amacıyla bu değerli tesadüfleri sistemli bir şekilde ortadan kaldırır. Size sürekli geçmişte bildiğiniz, sevdiğiniz ve onayladığınız içerikleri sunarak zihni tek bir diyete mahkûm eder. Bu durum, tıpkı sağlıksız fast-food tüketiminin bedeni hantallaştırması gibi, zihni de sürekli kolay sindirilen ve teyit edici bilgilerle doldurarak ciddi bir "entelektüel obezite" yaratır.

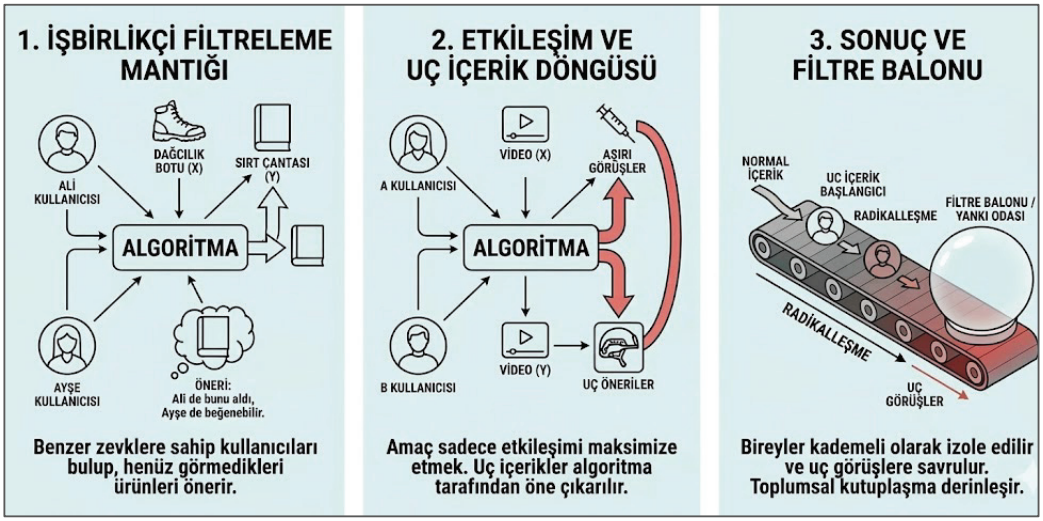
Bu döngüde zihin beslenmez, sadece şişer; yeni ve zorlayıcı perspektiflerle karşılaşmadığı için derinleşemez ve nihayetinde birey empatiden yoksun, durağan bir hale gelir.



Şekil 3.1.5 *Filtre balonunun kritik ve tehlikeli sonuçları*

İnternet dünyasının dev şirketleri, bizi platformlarında daha uzun süre tutabilmek amacıyla dijital deneyimimizi kişiselleştirir ve bu süreçte "işbirlikçi filtreleme" adı verilen temel bir teknoloji kullanır. Bu yöntemin mantığı şaşırtıcı derecede basittir: Algoritma, benzer zevklere sahip kullanıcıları gruplayarak bir tahmin yürütür. Eğer A kullanıcısı hem X hem de Y içeriğini tüketmişse ve B kullanıcısı sadece X'i tüketmişse, sistem B'nin de büyük

ihtimalle Y'yi seveceğini varsayar. Örneğin bir e-ticaret sitesinde Ali hem dağcılık botu hem de sırt çantası aldığında, sadece botu alan Veli'ye sistem hemen çantayı önerir. Aynı mantık sosyal medyada da işler; eğer bir kullanıcı hem "uzaylılar piramitleri inşa etti" hem de "aşılar otizme neden olur" videolarını izlemişse, sadece uzaylı videosunu izleyen bir başka kullanıcıya algoritma yüksek öncelikle o aşı karşıtı videoyu sunacaktır.



Şekil 3.1.6 *Algoritmik kişiselleştirme ve işbirlikçi filtreleme*

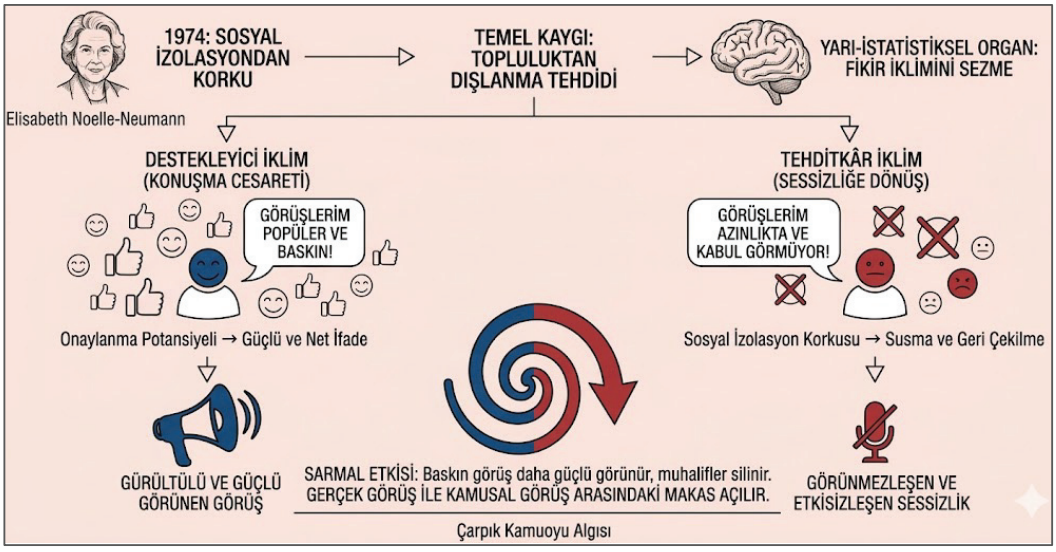
Mühendislik açısından bakıldığında bu sistemler verimliliği artırmayı hedefleyen masum yapılar gibi görünebilir; ancak işin içine sosyal ve politik içerikler girdiğinde bu mantık hızla sosyolojik bir felakete dönüşebilir. Algoritmaların ahlaki bir terazisi veya doğruluk kaygısı yoktur; onların tek amacı, tıklama ve izleme süresi gibi etkileşimleri maksimize etmektir. Ne yazık ki bizi ekrana kilitleyen içerikler genellikle en uç, en öfkeli ve en tartışmalı olanlardır. Siz masumane bir merakla bir komplo teorisine tıkladığınızda, sistem işbirlikçi filtreleme mantığıyla hemen devreye girer ve benzer kullanıcıların tükettiği çok daha radikal görüşleri önünüze getirir. Bu süreç, kullanıcıyı adım adım daha aşırı ve doğrulanmamış içeriklere sürükleyerek,

radikalleşmeyi adeta otomatikleştiren tehlikeli bir makine gibi işler.

Özellikle YouTube'un önerilen videolar algoritması, bu tehlikeli dinamiğin en somut örneği olarak öne çıkmaktadır. Araştırmalar, vejetaryenlik gibi masum bir konuyla başlayan izleme deneyiminin, algoritmanın yönlendirmesiyle kısa sürede şiddet içeren veya yasa dışı eylemleri öven radikal içeriklere evrildiğini göstermiştir. Bu süreç, bireyleri farkında olmadan ana akım dünyadan koparak yankı odalarına hapsetmekte; şirketlerin verimlilik amacıyla kurduğu bu yapılar, ne yazık ki toplumsal kutuplaşmayı derinleştiren ve güveni yok eden sosyolojik fay hatları yaratmaktadır.

Suskunluk Sarmalı

Dijital çağ, iletişim biçimlerimizi kökten değiştirirken benzer görüş ve yaşam tarzları etrafında sıkıca kenetlenen "dijital kabileler" olgusunu ortaya çıkarmıştır. Bu yeni aidiyet biçimi kimliklerimizi güçlendirse de ifade özgürlüğümüz üzerinde kısıtlayıcı bir etki yaratmaktadır. Sosyal medya platformları her ne kadar yüz milyonların konuştuğu özgür bir agora, bir meydan illüz-



Şekil 3.1.7 *Suskunluk sarmalının teorik arka planı ve işleyişi*

yonu sunsa da gerçekte dışlanma ve dijital linç korkusunun hâkim olduğu bir ortamdır. Çoğunluğun damgalanma endişesiyle temkinli davranarak sessizliğe gömüldüğü bu atmosfer, ne yazık ki toplumsal tartışmaların niteliğini düşürmekte ve kutuplaşmayı daha da derinleştirmektedir.

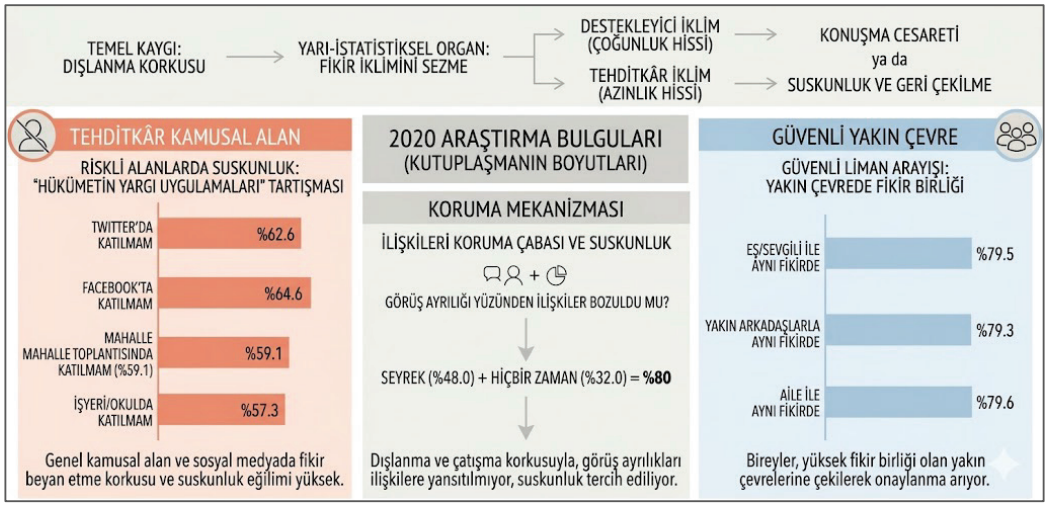
Bu yaygın sessizlik halinin teorik temeli, Alman siyaset bilimci Elisabeth Noelle-Neumann'ın 1974 yılında geliştirdiği "suskunluk sarmalı" teorisine dayanmaktadır.[32] Noelle-Neumann, teorinin merkezine insan doğasının en temel kaygılarından biri olan sosyal izolasyon ve toplumdan dışlanma korkusunu yerleştirir; çünkü birey tarihsel olarak hayatta kalabilmek için topluluğa muhtaçtır ve bu dışlanma tehdidi rasyonel kararların önüne geçen güçlü bir psikolojik baskı yaratır. Bu nedenle bireyler, kamusal alanda bir fikir beyan etmeden hemen önce, bilinçaltlarında çalışan bir mekanizmayı devreye sokarak ortamı analiz ederler. Bu mekanizma sayesinde dış dünyayı sürekli gözlemleyen kişi, eğer kendi görüşünün baskın olduğunu hissederse onaylanma cesaretiyle konuşur; ancak azınlıkta kaldığını sezerse, dışlanmamak adına otomatik bir savunma mekanizmasıyla sessizliğe gömülür.

Bu bireysel refleksler, toplumsal düzeyde bir kısır döngüye, kaçınılmaz bir sarmala dönüşür. Baskın olduğu düşünülen görüş, taraftarlarının yüksek sesle konuşması ve muhaliflerin dışlanma korkusuyla susması nedeniyle, gerçekte olduğundan çok daha güçlü ve yaygınmış gibi algılanır. Sayıca çoğunlukta olsalar dahi sessizliği seçenler kamusal alandan silinip görünmezleşirken; toplumun iç dünyasındaki gerçek düşünceler ile kamusal alanda ifade edilenler arasındaki makas giderek açılır. Sonuç olarak ortaya çıkan bu tablo, kamuoyu algısının gerçeği yansıtmadığı çarpık bir illüzyondan ibarettir.

Dijital çağda dışlanmanın bedeli, geçmişe göre çok daha ağır ve küresel bir boyuta ulaşmıştır. Masum bir hata, yanlış anlaşılan bir şaka veya

[32] Noelle-Neumann, E. (1974). The spiral of silence: A theory of public opinion. *Journal of Communication*, *24*(2), 43–51. https://doi.org/10.1111/j.1460-2466.1974.tb00367.x

bağlamından koparılan tek bir cümle bile, saatler içinde milyonların katıldığı organize bir linç hareketine dönüşebilir. Bu öfke dalgası sadece sanal dünyada kalmaz; işverenlerin dijital ayak izlerini sürekli taraması nedeniyle insanlar bir paylaşım yüzünden işlerini ve mesleki itibarlarını kaybedebilir, hatta özel bilgilerinin ifşa edilmesiyle (*dox*'lama) fiziksel tehdit ve tacizle karşı karşıya kalabilirler. Sürecin en yıkıcı noktası olan "iptal kültürü" (*cancel culture*) ise bireyi tamamen yalnızlaştırır, toplumdan izole eder ve kamusal alanda bir daha konuşamaz hale getirir.



Şekil 3.1.8 *Türkiye'de suskunluk sarmalı: 2020 Araştırma bulguları ve işleyişi*

Sosyal medya platformları, suskunluk sarmalı etkisini geçmişe kıyasla çok daha tehlikeli ve hızlıdır. Sarmal, adeta bir girdaba dönüştürmüştür. Geleneksel dünyada dışlanma yerel ve geçiciyken, dijital dünyada bu bedel küresel, anlık ve kalıcı hale gelmiştir. Bu yüksek risk ortamı ve dijital linç tehdidi, bireylerin fikirlerini ifade etme cesaretini ciddi oranda kırmaktadır. Nitekim Pew Research Center'ın araştırması, insanların sosyal medya platformlarında (*Facebook, Twitter*) fikirlerini beyan etme konusunda, aile yemek masası veya iş yeri toplantısı gibi gerçek hayattaki ortamlara kıyasla çok

daha az istekli olduğunu açıkça göstermektedir[33]. Bu çekingenliğin temelinde dijital hafızanın kalıcılığı yatar; on yıl önce atılmış bir tweet veya bağlamından koparılmış bir yorum, bugün kişinin kariyerini ve itibarını yok edecek bir yargılama aracına dönüşebilmektedir.

Suskunluk sarmalının dijital dünyada kazandığı bu ivme, toplumun genel görünümüne dair kökten çarpık bir algı yaratarak "sessiz çoğunluk" ile "gürültülü azınlık" arasındaki uçurumu derinleştirir. Sosyal medyaya baktığımızda toplumun sürekli öfkeli ve nefret dolu olduğu yanılgısına kapılsak da bu durum aslında platformların çalışma mantığının bir sonucudur. Merkeze yakın, uzlaşmacı ve makul çoğunluk, dijital linç veya dışlanma korkusuyla görüşlerini ifade etmekten kaçınarak sessizliğe gömülürken; algoritmalar tam tersi bir işleyişle hareket eder. Kullanıcıyı platformda daha uzun süre tutmayı hedefleyen bu sistemler, çatışma ve öfkenin yarattığı yüksek etkileşimi ödüllendirdiği için, radikal uçların sesini adeta bir megafonla yükselterek ana akıma taşır. Sonuç olarak, bu "megafon etkisi" yüzünden en aşırı ve marjinal sesler sanki toplumun merkeziymiş gibi algılanır ve sanal bir kutuplaşma illüzyonu oluşur.

🔍 **KAVRAM:** DOX'LAMA

Neyi açıklar?: Bireylerin özel bilgilerinin rızaları dışında dijital ortamlarda ifşa edilmesini açıklar.

Neden Önemli?: Hedef alınan bireylerin fiziksel tehdit, taciz ve siber zorbalık riskine girmesine yol açan ağır sonuçları olabilir. İnsanların dijital platformlarda linç edilme korkusuyla sessiz kalmayı tercih ettiği suskunluk sarmalı etkisini tetikleyerek ifade özgürlüğünü ve demokratik tartışmayı kısıtlayabilir.

Bu sürecin en yıkıcı sonucu, toplumun kendine dair algısının kökten bozulmasıdır. Sağduyulu ve uzlaşmacı sesler sessizliğe gömülüp kamusal alandan çekildiğinde, meydan boş kalmaz; aksine radikal uçlar sanki toplumun

[33] Hampton, K., Rainie, L., Lu, W., Dwyer, M. ve Shin, I. (2014). *Social media and the 'spiral of silence'*. Pew Research Center.

merkeziymiş gibi algılanmaya başlar. Çevresini olduğundan çok daha öfkeli ve kutuplaşmış zanneden bireyler, bu yanılsamanın yarattığı korkuyla kendi içlerine kapanarak dijital kabilelerine sıkışır. Bu yanlış algı, suskunluk sarmalını daha da hızlandırarak toplumu gerçekte olduğundan çok daha çatışmalı ve parçalanmış gösteren tehlikeli bir döngü yaratır; nihayetinde bu durum, toplumsal güveni yıkan ve demokratik tartışma zeminini ortadan kaldıran kritik bir sosyolojik kırılmadır.

Fikirlerimiz Nasıl Uçlara Savrulur? Grup Kutuplaşması

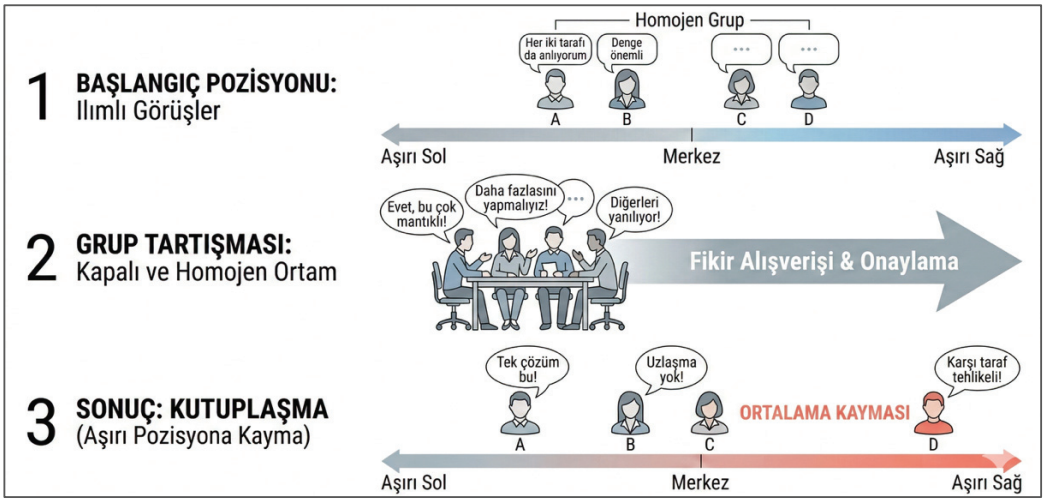
Sosyal bilimci Cass Sunstein'ın "grup kutuplaşması yasası", insanların bir araya gelip tartıştıklarında nasıl daha makul veya orta yola gelmek yerine, başlangıçtaki fikirlerinin daha uç versiyonlarına savrulduklarını açıklayan sosyal psikolojik bir fenomendir.[34] Bu yasa, yankı odalarının neden sadece bilgi kirliliği yaratmakla kalmayıp aynı zamanda toplumu radikalleştirdiğini çarpıcı bir şekilde açıklar. Benzer görüşlere sahip bireyler kapalı bir grupta tartıştıklarında, beklenen uzlaşmanın aksine, fikirler başlangıç noktasından çok daha uç ve keskin bir konuma savrulur. Sunstein'ın kapalı odada tartışan insanlar için öngördüğü radikalleşmeyi, algoritmalar tek başınıza ekran başında yaşamanıza neden olur. Sosyal psikolojinin temel taşlarından kabul edilen, özellikle Serge Moscovici ve Marisa Zavalloni'nin 1969'da yürüttüğü deneyler[35], bu olgunun tutarlılığını net bir şekilde ortaya koymaktadır. Bireyler; siyaset, sosyal yaşam veya etik gibi konularda başlangıçta nispeten ılımlı ve merkeze yakın görüşlere sahip olsalar bile, kendileriyle benzer fikirlere sahip homojen bir grupla kapalı bir ortamda tartışmaya girdiklerinde süreç

---

[34] Sunstein, C. R. (1999). *The law of group polarization* (John M. Olin Program in Law and Economics Working Paper No. 91).

[35] Moscovici, S., & Zavalloni, M. (1969). The group as a polarizer of attitudes. *Journal of Personality and Social Psychology, 12*(2), 125–135. https://doi.org/10.1037/h0027568

şaşırtıcı bir şekilde değişir. Bu fikir alışverişinin nihayetinde hem grup üyelerinin bireysel duruşu hem de grubun ortak kararı, başlangıç noktasından çok daha uç, keskin ve uzlaşmaz bir konuma savrulur; grup, kendi tercih ettiği yöne doğru kaçınılmaz olarak kutuplaşır.



Şekil 3.1.9 Grup Kutuplaşması

Bir örnek üzerinden gidelim: Başlangıçta sadece kontrollü bir göç yönetimini ve demografik yapının korunmasını savunan ılımlı bir grup düşünün. Bu bireyler, dışarıdan eleştirel bir ses duymadan, kapalı bir çevrede sadece birbirleriyle tartıştıklarında, sürecin sonunda "Tüm sınırlar derhal kapatılsın, yasal yollarla gelenler dahil hepsi sınır dışı edilsin, ülke etrafına fiziki duvar örülsün" gibi radikal taleplere savrulabilirler. Ilımlı kaygıların bu denli keskin çözümlere dönüşmesinin ardında iki temel psikolojik mekanizma yatar. Birincisi, grup içinde saygınlık kazanma ve "en sadık dava insanı" görünme arzusuyla tetiklenen sosyal rekabettir; bu yarışta ılımlılık yetersizlik veya korkaklık gibi algılanırken, radikallik cesaret ve ilkelilik olarak ödüllendirilir. İkincisi ise "ikna edici argümanlar havuzu"dur; ortamda karşıt görüşleri çürüten hiçbir tez bulunmadığından, bireyler sürekli kendi fikirlerini destekleyen tek yönlü bir bilgi akışına maruz kalır ve bu durum inançlarını

sorgulanamaz bir kesinlikle kemikleştirir.

Sosyal medya platformlarının algoritmaları, Cass Sunstein'ın ortaya koyduğu grup kutuplaşması yasasını devasa bir hızla otomatikleştirerek literatürde "tavşan deliği" olarak adlandırılan fenomeni yaratır. Bir kullanıcı, örneğin aşılar veya siyasi konular hakkında ılımlı bir içerikle etkileşime girdiğinde, algoritma onu dengeli veya bilimsel kaynaklara yönlendirmek yerine, ekran süresini maksimize etmek amacıyla tasarlanmış çok daha aşırı ve komplo odaklı içeriklere sürükler. Dijital dünyada ılımlılık sıkıcı, aşırılık ve öfke ise yüksek etkileşim anlamına geldiği için; kullanıcı aslında kendi seçimlerini yaptığını sanırken, farkında olmadan ılımlı bir şüpheden radikal bir fanatizme veya nefret söylemine doğru kayan otomatik bir yürüyen merdivene bindirilmiş olur. Bu yapı, günümüzdeki terör örgütlerinden örneğin IŞİD'in dijital propaganda kanalları, QAnon gibi siyasi komplo tarikatlarına kadar pek çok yapının "dijital asker toplama" ve radikalleşme stratejisinin temelini oluşturur. İnsanlar, bir günde radikalleşip terörist olmazlar; bu durum, yankı odalarının kısıtlı bilgi havuzları ve algoritmik beslemenin yönlendirmesiyle aylar süren bir "kuluçka" döneminin sonucudur. Kutuplaşma, böylece sosyal bilimden, dijital güvenliğin ve toplumsal huzurun temel sorununa dönüşür.

TEMEL ÇIKARIMLAR

Bu bölüm, internetin dünyayı birleştirme vaadinin aksine, bizi nasıl yankı odalarına hapsettiğini ve toplumsal kutuplaşmayı derinleştiren mekanizmaları inceler. Sorunun kaynağı sadece kötü niyetli teknoloji değil, insan doğasındaki "benzeri sevme" (homofili) eğiliminin dijital platformlarca ticari bir modele dönüştürülmesidir. Bu yapı, toplumsal "müşterekleri" (ortak zemin ve hakikat) yok ederek, bireylerin farklı görüşlerle temasını keser ve onları kendi içlerine kapalı gruplara ayırır.

Temel Kavramlar ve Mekanizmalar

Homofili ve Konforun Bedeli: Zihinsel konfor için insanlar kendine benzeyenleri arar. Dijital dünya bu ayrışmayı zahmetsiz hale getirir. Size benzeyen insanlarla olmak konforludur ancak zihni köreltebilir; farklı görüşler ise zihni biler. Yankı odası, bu konforun bedeli olarak entelektüel körlük yaratır.

Seçim Yanılsaması (Yankı Odası vs. Filtre Balonu): Yankı odasını biz inşa ederiz, ancak filtre balonunu algoritmalar bizden habersiz örer. "İstediğim haberi okuyorum" derken aslında algoritmanın geçmiş verilerimize bakarak bizim için seçtiği içeriği tüketiriz. Özgür irade, dijital mimari tarafından sınırlandırılmıştır ve bu balonu delmenin tek yolu, algoritmaya kafa karıştırıcı sinyaller vererek (karşıt görüşleri okuyarak) "Ben tek tip değilim" mesajı iletmektir.

Suskunluk Sarmalı ve Sessizliği Kırmak: İnsanlar dijital linç ve dışlanma korkusuyla makul görüşlerini ifade etmekten kaçınır, algoritmalar ise en uç sesleri öne çıkarır. Bu sarmal, sadece herkes sustuğu için çalışır. Makul ve saygılı bir dille "Ben farklı düşünüyorum" diyen bir kişi, sarmalı kırabilir ve diğer sessizlere cesaret verebilir.

Grup Kutuplaşması ve Tavşan Deliği: Benzer düşünen insanlar kapalı bir grupta tartıştıklarında, fikirler yumuşamak yerine daha radikal uçlara savrulur. Sosyal medya algoritmaları, kullanıcıyı ekranda tutmak için sürekli "bir tık daha aşırı" içeriği önererek, tavşan deliği etkisiyle bu radikalleşme sürecini otomatikleştirir ve bizi ılımlı şüpheden fanatizme sürükler.

3.1. KENDİNİZİ TEST EDİN

Soru 1: Eli Pariser'in "filtre balonu" kavramı ile Cass Sunstein'ın "yankı odası" kavramı arasındaki temel fark nedir?

A) Yankı odası dijital ortamdadır, filtre balonu gerçek hayattadır.

B) Yankı odası bireyin tercihiyle, filtre balonu ise algoritmaların seçimiyle oluşur.

C) Filtre balonu yankı odasına göre daha zararsızdır.

D) Yankı odasında her türlü farklı sesi duymak mümkündür.

Soru 2: Elisabeth Noelle-Neumann'ın "suskunluk sarmalı" teorisine göre, insanlar neden gerçek fikirlerini açıkça söylemekten çekinirler?

A) Konu hakkında yeterli bilgileri olmadığı için

B) Toplumdan dışlanmaktan korktukları için

C) Konuşmayı pek sevmedikleri için

D) Sosyal medya platformunun kuralları yasakladığı için

Soru 3: "Grup kutuplaşması" yasasına göre, zaten benzer düşünen insanlar bir araya gelip kapalı bir grupta tartıştıklarında ne olur?

A) Birbirlerinin hatalarını düzeltir ve daha ılımlı bir orta yolda buluşurlar.

B) Konudan sıkılırlar ve grup dağılır.

C) Fikirleri daha da keskinleşir ve radikal uçlara savrulurlar.

D) Fikirlerinde hiçbir değişiklik olmaz.

3.1. MERAKLISINA EK KAYNAKLAR

Jamieson, K. H. ve Cappella, J. N. (2008). *Echo chamber: Rush Limbaugh and the conservative media establishment*. Oxford University Press.

Kristof, N. (2009, 18 Mart). The Daily Me. *The New York Times*. https://www.nytimes.com/2009/03/19/opinion/19kristof.html

Bilgi Düzensizlikleri ve Kutuplaşmanın Boyutları

Siyaset bilimi ve sosyoloji derslerinde Türkiye, kendine has inişli çıkışlı tarihiyle uzun yıllardır demokratikleşme süreçleri için önemli bir vaka analizi olarak incelenirdi. Ancak son on yılda yaşadığımız derin toplumsal ayrışma, ülkemizi sadece bir "örnek" olmaktan çıkarıp küresel bir sorunun adeta prototipi haline getirdi. Toplumu derinden sarsan bu fenomenin adı kutuplaşmadır. Geldiğimiz nokta itibarıyla Türkiye, literatürde artık bu sorunun "sıfır noktası" olarak görülüyor. Bugün hissettiğimiz bu gerilim, geçmişteki, örneğin 1970'lerdeki siyasi ayrışmalardan oldukça farklıdır. O dönemde Soğuk Savaş'ın etkisiyle yaşanan sağ-sol tartışmaları, temelde ekonomik modeller (devletçilik mi, serbest piyasa mı?) veya dış politika tercihleri (NATO mu, bağlantısızlık mı?) gibi somut ve rasyonel konular üzerine kuruluydu. İnsanlar ne kadar zıt fikirlere sahip olsalar da nihayetinde kendilerini aynı ülkenin, aynı geminin yolcuları olarak görmeye devam edebiliyorlardı.

Karşı Tarafı Nasıl Görüyoruz? Duygusal Kutuplaşma

Bugün yaşadığımız süreci en iyi açıklayan tanım Stanford Üniversitesi'nden Shanto Iyengar ve arkadaşlarının (2012)[36] geliştirdiği "duygusal kutuplaşma" kavramıdır. Bu kavram, siyasi fikir ayrılığının ötesine geçerek, meselenin karşı tarafa duyulan kimlik temelli bir nefrete ve duygusal bir düşmanlığa dönüşmesini ifade eder.

Türkiye'nin mevcut durumunu doğru analiz edebilmek ve yanlış teşhislerden kaçınmak için, kutuplaşmayı niteliklerine göre ikiye ayırmamız gerekir. Bunlardan ilki olan ideolojik kutuplaşma, tarafların vergi oranları, faiz kararları veya eğitim müfredatı gibi somut politikalar ve yöntemler üzerinde

[36] Iyengar, S., Sood, G., & Lelkes, Y. (2012). Affect, not ideology: A social identity perspective on polarization. *Public Opinion Quarterly*, *76*(3), 405–431. https://doi.org/10.1093/poq/nfs038

anlaşamadığı durumdur. Rasyonel bir zemine dayanan ve verilerle tartışılabilen bu ayrışma, aslında farklı fikirlerin yarışmasını sağladığı için demokrasinin sağlıklı ve işlevsel bir parçasıdır. Ancak Türkiye'de bugün asıl yıkıcı etkiyi yaratan sorun duygusal kutuplaşmadır. Bu türde ayrışma politikalar üzerinden değil; kimlikler, değerler ve duygular üzerinden gerçekleşir. Taraflar birbirini sadece "farklı politika öneren vatandaşlar" olarak görmeyi bırakıp, karşıt görüşü "vatan haini", "ahlaksız" veya "ülke için tehdit" olarak etiketlemeye başlar. Bu durum, siyaseti demokratik bir fikir mücadelesi olmaktan çıkarıp, karşı tarafın insanlığını yok sayan tehlikeli bir varoluşsal savaşa dönüştürür.

Türkiye'de şu an gözlemlediğimiz derin kriz, açıkça ikinci tür olan duygusal kutuplaşmanın baskın hale geldiğini gösteriyor. Bu durum, Carl Schmitt'in siyasetin özünü "dost ve düşman ayrımı" olarak tanımladığı o keskin iklimi hatırlatıyor; siyaset artık bir fikir yarışı değil, kimin "bizden" kimin "düşman" olduğunu belirleme savaşına dönüşmüş durumda ve bu ayrım gündelik hayatımızın her alanına sızıyor.[37] Böyle bir ortamda, demokrasinin en temel değeri olan "hakikat" önemini yitiriyor ve siyasetin mantıksal zemini çöküyor. Artık bir bilginin doğruluğuna kanıtlara veya verilere bakarak değil, tamamen "kimin söylediğine" bakarak karar veriyoruz. Eğer bir iddia "bizim mahalleden" birinden geliyorsa onu sorgusuz sualsiz doğru kabul ediyoruz; ancak aynı bilgi, matematiksel bir gerçek bile olsa, "karşı mahalleden" geliyorsa, onu otomatik olarak yalan, propaganda veya kötü niyetli bir operasyon olarak damgalıyoruz. Yankı odaları ve filtre balonları da bu durumu iyice pekiştirerek farklı grupların ortak bir gerçeklikte buluşmasını imkânsız hale getiriyor.

Türkiye örneğine geçmeden önce, insan zihninin nasıl hızla gruplaştığını

[37] Schmitt, C. (1932). *The concept of the political*. University of Chicago Press.

ve bu sürecin nasıl yıkıcı bir nefret aracına dönüştüğünü kavramamız gerekir. Bu dönüşümün kökenlerini anlamak için sosyal psikolojinin en temel teorilerinden birine, Henri Tajfel'in çalışmalarına bakmalıyız. İkinci Dünya Savaşı'nda ailesini Nazi kamplarında yitiren Polonya asıllı İngiliz psikolog Tajfel, savaş sonrasında zihnini tek bir soruya odaklamıştı: Sıradan insanlar, ortada somut bir çıkar çatışması yokken nasıl bu kadar kolay "biz" ve "onlar" diye ayrışıp komşularına düşman kesilebiliyor? Tajfel, bu sorunun yanıtını öğrencisi John Turner ile geliştirdiği "sosyal kimlik teorisi"nde buldu.[38] Bu teoriye göre insanlar, benlik saygılarını sadece kişisel başarılarından değil, aynı zamanda ait oldukları sosyal grubun (iç grup) statüsünden de devşirirler. Psikolojik bir ihtiyaç olarak kendi grubumuzu yüceltirken, sınırın ötesinde kalanları (dış grup) aşağılama ve ötekileştirme eğilimi gösteririz. Birey "Ben kimim?" sorusuna yanıt ararken, aslında "Kiminle değilim?" sorusunu da yanıtlayarak kimliğini güçlendirir; bu da ayrımcılığın rasyonel bir çıkar çatışmasından ziyade, derin psikolojik bir mekanizma olduğunu gösterir.

Sosyal Kimlik Teorisi'nin deneysel dayanağını oluşturan ve sosyal psikoloji literatürünün en çarpıcı çalışmaları arasında yer alan Henri Tajfel'in Bristol Üniversitesi'ndeki "minimal grup paradigması" deneyleri, insan doğasının ayrımcılığa ne kadar yatkın olduğunu acımasız bir netlikle ortaya koymuştur. Tajfel bu deneylerde, tarihsel düşmanlık, rekabet ya da ideolojik çatışma gibi "büyük nedenler" olmaksızın, yalnızca rastgele bir gruplamanın bile ayrımcılığı tetiklemeye yetip yetmeyeceğini test etmeyi amaçlamıştır. Bu doğrultuda, katılımcı olan okul çağındaki öğrenciler, yazı-tura sonucu, bir ressama duyulan beğeni ya da tişört rengi gibi tamamen keyfi ve anlamsız kriterlere göre ikiye ayrılmıştır. Gruplar arasında önceden hiçbir tanışıklık

[38] Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. İçinde M. A. Hogg & D. Abrams (Der.), *Intergroup relations: Key readings in social psychology* (ss. 94–109). Psychology Press.

veya çıkar çatışması bulunmamasına rağmen, katılımcılara ellerindeki sınırlı kaynağı dağıtma yetkisi verildiğinde şaşırtıcı bir tablo ortaya çıkmıştır; insanlar, sadece kendi gruplarına ait oldukları için "bizden" gördüklerine daha fazla kaynak aktararak açık bir iç grup kayırmacılığı sergilemişlerdir. Ancak deneyin en sarsıcı bulgusu, katılımcıların rasyonel davranıp kendi gruplarının mutlak kazancını maksimize etmek yerine, karşı grubun kazancını minimize etmeye odaklanmaları olmuştur; özetle bireyler, "bizim grubumuz biraz daha az kazansın, yeter ki karşı taraf bizden çok daha azını alsın" mantığıyla hareket ederek, mutlak kazançtan ziyade gruplar arasındaki farkı açmayı ve öteki tarafa zarar vermeyi tercih etmişlerdir.

Bu deneyin ortaya koyduğu sonuçlar, ayrımcılığın sanıldığı gibi rasyonel bir çıkar hesabına dayanmadığını, aksine tamamen psikolojik bir refleks olduğunu kanıtlamıştır. İnsan zihni, kendi benlik saygısını korumak ve kimliğini güçlendirmek için sürekli olarak bir "biz" ve "onlar" ayrımına ihtiyaç duyar. Bu mekanizma o kadar hassastır ki, tişört rengi veya yazı-tura sonucu gibi en küçük ve anlamsız bir farklılık bile, zihin tarafından düşmanlık yaratmak için yeterli ve meşru bir gerekçe olarak kullanılır. Kısacası birey, "Ben kimim?" sorusuna yanıt ararken, aslında "Kiminle değilim?" sorusunu yanıtlayarak kendini tanımlar; bu da ayrımcılığın mantıksal bir nedene ihtiyaç duymadan, sadece psikolojik bir tatmin aracı olarak kendiliğinden ortaya çıkabileceğini göstermektedir.

KAVRAM: NEFRET SÖYLEMİ

Neyi açıklar?: Belirli bir gruba din, ırk, renk, cinsiyet veya diğer kimlik faktörlerine göre saldıran ve ayrımcı bir dil kullanan söylemleri ifade eder.

Neden Önemli?: Duygusal kutuplaşmanın hâkim olduğu ortamlarda, karşı tarafı hain vb. ifadelerle etiketlemek nefret söylemini tetikler.

Aramızdaki Mesafe Ne Kadar Derin? Türkiye Örneği

Minimal grup paradigması, insan zihninin ayrımcılık üretmek için büyük sebeplere ihtiyaç duymadığını kanıtlamıştı; ancak Türkiye gibi tarihsel derinliği olan toplumlarda bu "büyük sebeplerden" zaten bolca mevcuttur. Tajfel'in bahsettiği etiketleme mekanizması, ülkemizin halihazırda var olan laik-dindar, Türk-Kürt veya sağ-sol gibi tarihsel ve kültürel fay hatlarıyla birleştiğinde, etkisi katlanarak artan yıkıcı bir kutuplaşmaya dönüşür. Bu ayrışma, basit bir tişört rengi tercihinin çok ötesine geçerek bireyin tüm benliğini kuşatan bir "kimlik cüzdanı" halini almıştır. Bir siyasi partiye oy vermek, artık sadece bir yönetim tercihi değil; o partinin temsil ettiği ahlak anlayışını, dünya görüşünü ve yaşam tarzını bütünüyle sahiplenmek demektir. Parti rozeti, kişinin en temel kimlik göstergesi haline gelir. Kutuplaşma derinleştikçe, farklı gruplara mensup bireyler sadece sandıkta değil; izledikleri diziden yedikleri yemeğe, çocuklarını gönderdikleri okuldan kullandıkları dile kadar hayatın her alanında birbirlerinden koparak kimliklerine hapsolurlar. Bu, Tajfel'in bahsettiği iç grup kayırmacılığının hayatın tamamına yayılmasıdır. Bu ortamda "ötekine" zarar verme arzusu, ekonomik kaynakların paylaşımını aşarak kamusal alanda ve medyada sözlü şiddete ve nefret söylemine evrilir. Tajfel'in deneyindeki o çarpıcı mantık, bugün milyonlarca insanın gündelik siyasi refleksine sirayet etmiştir: "Benim grubum tam olarak kazanmasa da olur, yeter ki karşı taraf kaybetsin." Bu yaklaşım, rasyonel bir siyasi uzlaşının önündeki en büyük zihinsel engeldir.

Türkiye'de bugün karşı karşıya kaldığımız dijital kutuplaşma, boş bir levha üzerine inşa edilmiş yeni bir olgu değil, aksine ülkenin köklü sosyo-politik yapısının dijital ortama yansımasıdır. Bu durumu anlamlandırmak için Türk sosyolojisinin en önemli isimlerinden Şerif Mardin'in "merkez-çevre" paradigmasına bakmamız gerekir. Mardin'e göre, Osmanlı'dan Cumhuriyet'e

miras kalan bu ayrışma, Batı toplumlarındaki gibi ekonomik sınıflar arasında değil; kültürel kodlar, ideolojiler ve yaşam tarzları arasında gerçekleşmiştir. Bu ikili yapıda "merkez", modern devlet aygıtını, bürokrasiyi ve orduyu temsil eden; yaşam tarzı olarak sekülerizmi ve Batılılaşmayı benimsemiş, genellikle büyük şehirlerde yaşayan eğitimli elitlerden oluşur. Buna karşılık "çevre", taşrayı, kırsalı ve geleneksel değerleri temsil eden; dini hassasiyetleri güçlü ve muhafazakâr geniş halk kitlelerini kapsar. Merkezin tanımladığı modernleşme projelerine karşı tarihsel bir direnç gösteren çevre unsurları, sistem içinde uzun süre ikincil konumda kalmış ve seslerini genellikle popülist siyasi hareketler aracılığıyla duyurmaya çalışmıştır; işte bugünkü "siber kültür savaşları" da bu tarihsel fay hattının üzerinde şekillenmektedir.

📌 **ÖRNEK VAKA:** Vezir Mohammed Nourtani Olayı

Zonguldak'ta kaçak bir maden ocağında çalışırken hayatını kaybeden ve cesedi yakılan Afgan işçi Vezir Mohammad Nourtani'nin ölümü sonrasında sosyal medyada gelişen tepkiler incelenmiştir (Kotan, 2025).Oldukça zor bir vaka üzerine olan bu araştırma, X platformundaki tartışmaların birbirine kapalı iki ana yankı odasına bölündüğünü saptamıştır: Bir yanda insan hakları temelli adalet çağrıları yapanlar, diğer yanda ise olayı "sessiz istila" gibi kalıplaşmış anlatılarla bir güvenlik tehdidi olarak sunan göçmen karşıtı gruplar. Bu vaka, olayın sosyal medya platformlarında nasıl hızla rasyonel bir tartışma zemininden kopup, "duygusal kutuplaşma" ve "grup kutuplaşması" dinamiklerini tetiklediğini somutlaştırır.

Makaleye ulaşmak için:
🔗 https://resaid.bilgi.org.tr/konferans-mayis-2025/

Cumhuriyet tarihi boyunca bu iki toplumsal kesim, yalnızca ideolojik düzlemde değil, fiziksel ve sosyal yaşam pratiklerinde de keskin sınırlarla birbirinden ayrışmıştır. Nişantaşı veya Cihangir ile Sultanbeyli veya Bağcılar örneklerinde görüldüğü gibi farklı semtlerde ikamet etmek, ayrı eğitim

kurumlarına gitmek ve birbirine zıt medya kanallarını takip etmek bu mesafeyi iyice derinleştirmiştir. Müzik zevklerinden yeme-içme alışkanlıklarına kadar uzanan bu kültürel farklılaşma ve fiziksel kopukluk, paradoksal bir şekilde çatışma riskini baskılayan bir unsur işlevi görmüştür; taraflar arasında doğrudan ve sürekli bir temas alanı oluşmadığı için, toplumsal gerilim uzun süre sıcak bir çatışmaya dönüşmeyen bir tür "soğuk savaş" dengesinde kalmıştır.

🎧 DİNLE

Turkuazlab Podcast serisinde İstanbul Bilgi Üniversitesi'nden Prof. Dr. Erkan Saka ile *Sosyal Medya, Yanlış Bilgi ve Kutuplaşma* başlıklı bir söyleşi gerçekleştirildi.

🔗 Dinlemek için: https://open.spotify.com/episode/6MveqnGK2hAQCcCr6KfyXX?si=Wd2xPTwpTwmT_Q1WVOzvog

2000'li yılların başında internetin, 2010'larda ise sosyal medyanın yaygınlaşması, Türkiye'deki tarihsel ayrışmanın dinamiklerini kökten değiştirmiştir. Sosyal medya, coğrafi sınırları ortadan kaldırarak Şerif Mardin'in "merkez" ve "çevre" kavramlarını[39] sanal bir kamusal alanda, aynı "hashtag" altında bir araya getirmiştir. Sosyolojide "bağlam çöküşü" olarak tanımlanan bu olgu, Nişantaşı'nın seküler bireyi ile Sultanbeyli'nin muhafazakâr bireyi gibi, geleneksel olarak birbirine uzak sosyal grupları aynı dijital platformda ve yorum akışında doğrudan karşı karşıya getirmiştir. Bu dijital karşılaşma, daha önce "soğuk savaş" düzeyinde seyreden kültürel gerilimi ısıtarak bir

[39] Mardin, Ş. (1973). Center-periphery relations: A key to Turkish politics? *Daedalus*, *102*(1), 169–190.

"sürtünme ekonomisi" yaratmıştır; platformların öfkeyi ve kutuplaşmayı ödüllendiren algoritmik yapısı, tarihsel kültürel kodlarla birleşince ortaya bir "siber-kültür savaşı" çıkmıştır. Artık çatışmanın odağı klasik siyaset veya ekonomi değil; bir köprü ismi, dizi karakterinin kıyafeti veya yaşam tarzı sembolleri üzerinden yürüyen kimlik krizleridir.

Teorik tartışmaları bir kenara bırakıp Türkiye'nin toplumsal röntgenini çeken somut verilere odaklandığımızda, İstanbul Bilgi Üniversitesi TurkuazLab bünyesinde yürütülen "Türkiye'de Kutuplaşmanın Boyutları" (2020) araştırması,[40] durumun ciddiyetini çarpıcı bir şekilde ortaya koymaktadır. Siyasi rekabetin çok ötesine geçen bu tabloyu anlamak için, grupların birbirine olan kabul düzeyini ölçen Bogardus Sosyal Mesafe Ölçeği verilerine bakmak yeterlidir. Bu ölçek Türkiye'ye uyarlanarak katılımcılara "kendi partilerine en uzak hissettikleri partinin taraftarlarıyla" ne kadar yakınlaşabilecekleri sorulmuştur. Katılımcıların yaklaşık yüzde 75'i çocuklarının "karşı partinin" taraftarıyla evlenmesini, yüzde 70'i onlarla iş yapmayı, yüzde 66'sı komşu olmayı ve yüzde 64'ü çocuklarının arkadaşlık etmesini istememektedir. Bu sarsıcı oranlar, siyasi kutuplaşmanın ticaretten komşuluğa, hatta aile kurmaya kadar hayatın tüm sızdığını ve toplumsal dokuda "öteki" ile temasın kesildiği derin bir uçurum yarattığını kanıtlamaktadır.

İZLE

Türkiye'de kutuplaşmanın boyutlarını ve toplumsal etkilerini daha detaylı öğrenmek için, Turkuazlab tarafından hazırlanan açık erişimli çevrim içi eğitim aracını kullanabilirsiniz.
🔗 Derse katılmak için:
http://www.turkuazlabsaha.org

[40] Erdoğan, E., & Uyan-Semerci, P. (2020). *Türkiye'de Kutuplaşmanın Boyutları 2020*. İstanbul Bilgi Üniversitesi Yayınları.

Aynı araştırmada katılımcılara yöneltilen "Kendi partililerinizi ve en uzak bulduğunuz parti taraftarlarını hangi sıfatlarla tanımlarsınız?" sorusu, mevcut siyasi kutuplaşmanın artık ahlaki bir kutuplaşmaya evrildiğini göstermektedir. Bu durum, karşıt görüşlü grupların sadece farklı fikirlere sahip insanlar olarak değil, aynı zamanda kötü niyetler taşıyan birer düşman olarak algılandığını simgeler. Ortaya çıkan tabloya göre bireyler, kendi gruplarını "vatansever", "onurlu" ve "dürüst" gibi sıfatlarla tanımlayarak bir iç grup yüceltmesi yaparken; karşı tarafı "vatan haini", "zalim" ve "bencil" olarak etiketleyerek şeytanlaştırmaktadır. Bu ahlaki üstünlük yanılgısı yerleştiğinde, kendini "vatansever", ötekini ise "hain" olarak kodlayan zihin için etik bariyerler kalkar; dolayısıyla karşı tarafa yönelik üretilen yalan haberler, montaj videolar veya manipülatif içerikler birer ahlaki sorun olmaktan çıkıp, haklı davanın meşru araçları olarak görülmeye başlanır. Sonuç olarak kutuplaşma, sadece hangi partiye oy verdiğimizi belirleyen basit bir siyasi tercih meselesi olmaktan çıkmış; gerçeklik algımızı, ahlaki terazimizi ve toplumsal güveni temelden sarsan çok boyutlu bir ayrışma mekanizmasına dönüşmüştür.

Korku ve Aidiyet Duygusu Kararlarımızı Nasıl Etkiliyor?

Türkiye'deki seçmen davranışını ve bilgi tüketim dinamiklerini anlamlandırmak için en kritik kavram, klasik siyasi bağlılık modellerinin yetersiz kaldığı günümüzde öne çıkan "negatif partizanlık"tır. Geleneksel siyaset sosyolojisinde geçerli olan "pozitif partizanlık" modelinde seçmen, kendi partisine, liderine ve ideolojisine duyduğu sevgi ve aidiyet duygusuyla hareket ederken; bugün bu motivasyon yerini çok daha farklı bir dürtüye bırakmıştır. Başta Abramowitz ve Webster'ın (2016) çalışmaları[41] olmak üzere güncel araştırmalar, seçmen davranışını şekillendiren ana unsurun artık kendi

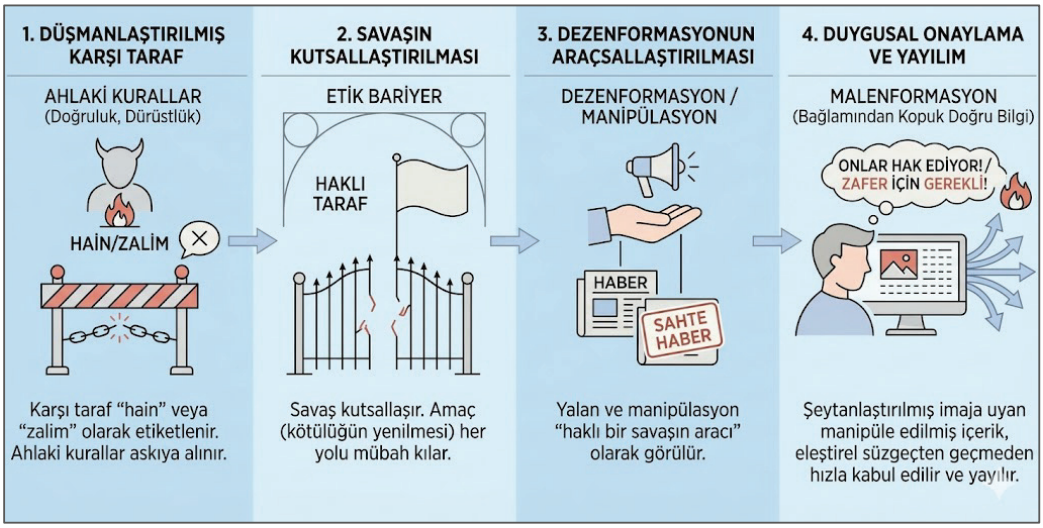
[41] Abramowitz, A. I., & Webster, S. W. (2016). The rise of negative partisanship and the nationalization of U.S. elections. *Electoral Studies*, *41*, 12–22. https://doi.org/10.1016/j.electstud.2015.11.001

partisine duyulan sevgiden çok, karşı tarafa duyulan nefret ve onların iktidara gelmesinden kaynaklanan korku olduğunu ortaya koymaktadır. Bu yeni psikolojik iklimde bireyler, kendi partilerini kusursuz buldukları için değil; karşı tarafın kazanmasını kimliklerine ve yaşam tarzlarına yönelik varoluşsal bir tehdit olarak gördükleri için sandığa gitmektedirler.

Negatif partizanlığın işleyiş mekanizmasına ve sonuçlarına baktığımızda, seçmen davranışının artık rasyonel bir tercih olmaktan çıkıp duygusal bir savunma refleksine dönüştüğünü görürüz. Bu yeni düzende sandığa gitme motivasyonunun kaynağı umut değil, derin bir korkudur; seçmen kendi partisini kusursuz bulduğu için değil, karşı tarafın iktidara gelmesini kimliğine ve yaşam tarzına yönelik varoluşsal bir tehdit olarak algıladığı için oy verir. Bu durum, siyasi kutuplaşmayı elitlerin tekelinden çıkarıp doğrudan tabana yayar ve karşı partiyi meşru bir rakipten ziyade yok edilmesi gereken bir "düşman" statüsüne indirgeyerek toplumsal uzlaşma zeminini yok eder. Bu korku iklimi, dezenformasyon üreticileri için de verimli bir zemin oluşturur; çünkü "karşı taraf gelirse yaşam tarzımız biter" ya da "ülke elden gider" şeklindeki felaket senaryoları, umut dolu mesajlardan çok daha hızlı yayılır ve kitleleri konsolide eder. Sonuç olarak rasyonellik çöker; tehdit algısıyla hareket eden seçmen, duyduğu bilginin doğruluğunu sorgulamak yerine, o tehdide karşı "tedbir" almayı önceler ve gerçeği aramak yerine korkularını doğrulayan manipülatif içeriklere inanmayı tercih eder.

Negatif partizanlık, modern siyasetin sağlıklı işleyişini tehdit eden bir hastalık olarak, seçmenleri rasyonel düşünceden uzaklaştırıp duygusal bir savunma hattına hapseder. Bu durum bilgi ekosistemine de zarar verir; çünkü seçmenler gerçeği öğrenmek yerine, korkularını doğrulayan manipülatif içeriklere ve felaket senaryolarına inanmayı tercih ederler. Karşı tarafın meşru bir rakipten ziyade yok edilmesi gereken bir "düşman" olarak görüldüğü bu atmosferde, demokratik müzakere kültürü ve toplumsal uzlaşma

zemini derinden sarsılır. Türkiye gibi kutuplaşmanın yüksek olduğu ülkelerde, seçmen davranışını ve bilgi tüketim kalıplarını çözümlemek için bu kavramı anlamak hayati önem taşır.



Şekil 3.2.1 *Etik bariyerlerin kalkması ve dezenformasyon*

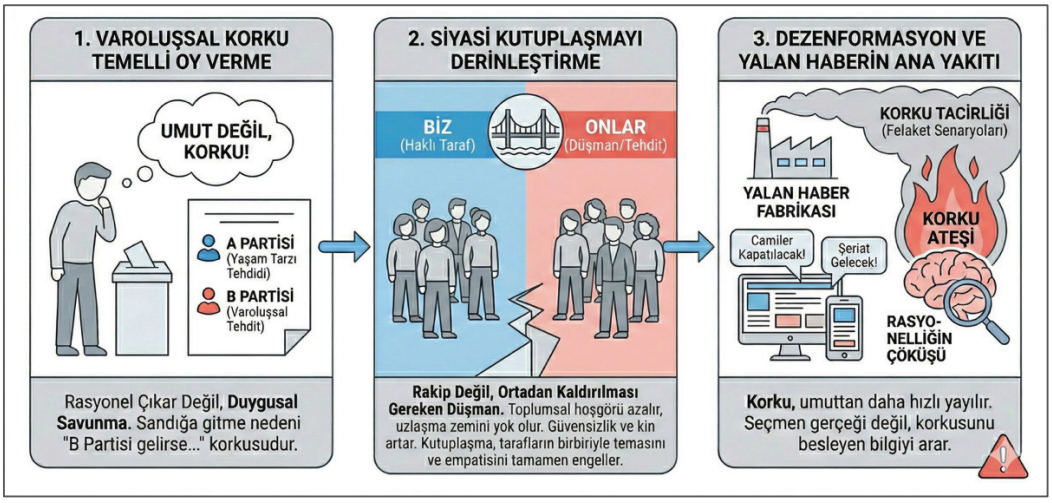
Türkiye'deki bilgi akışını anlamak için, süreci yalnızca bireysel bir değerlendirme olarak değil, "Mahalle" adı verilen kolektif bir kimlik yapısı üzerinden okumak gerekir. Sosyolojik bir kavram olarak mahalle, fiziksel bir sokaktan ziyade bireyin dünya görüşünü şekillendiren zihinsel ve duygusal bir sığınaktır. Nozick'in "epistemik kapanma" kavramıyla örtüşen bu yapıda, gruplar kendi temel inançlarıyla çelişen dış kaynaklı bilgilere karşı direnç gösterir ve kapılarını kapatır. Bir bilginin bu korunaklı alana girebilmesi, adeta zorlu bir vize sürecini andırır; bilgi, öncelikle yazarlar, fenomenler, popüler gazeteciler veya topluluk liderleri gibi kanaat önderleri tarafından süzgeçten geçirilir ve ancak grubun yerleşik kabulleriyle veya "büyük anlatısı"yla uyumlu bulunursa "doğru" kabul edilerek içeri alınır. Eğer karşılaşılan bilgi, "mahallenin" kutsal kabul ettiği anlatıyı zedeleyecek, ona eleştirel bir boyut katacak veya alternatif bir bakış açısı sunacak nitelikteyse, içeri girmesi

imkânsızlaşır ve derhal reddedilir. Bu tür "istenmeyen" bilgiler, içeriğine bakılmaksızın "dış güçlerin propagandası", "terör örgütlerinin dezenformasyonu", "vatana ihanet" veya "kripto saldırı" gibi etiketlerle damgalanarak kapıdan çevrilir. İşleyen bu süreç, bireylerin kendi özgün gerçekliklerini inşa etmelerini engeller ve onları, önceden kurgulanmış kolektif bir gerçekliği sorgusuz sualsiz onaylamaya yöneltir; böylece hakikat arayışı mantıksal bir süreç olmaktan çıkıp, kişinin grubuna olan bağlılığını ispatladığı bir sadakat testine dönüşür.

Epistemik kapanmanın yarattığı bu katı mahalle yapısı içinde, grubun genel kabulünün dışına çıkarak doğruyu söylemek veya eleştirel bir tutum takınmak, artık takdir edilen bir erdem değil, birey için göze alınması zor bir sosyal risktir. Mahallenin yazılı olmayan kurallarına uymayan her çıkış, anında "ihanet" olarak etiketlenir; örneğin muhalif bir ismin iktidarın somut bir başarısını takdir etmesi "dönek" veya "yandaş" olarak yaftalanmasına yol açarken, iktidara yakın birinin bariz hataları eleştirmesi "hain veya düşman" ilan edilmesine neden olabilir. Bu dışlanma mekanizması, Elisabeth Noelle-Neumann'ın "suskunluk sarmalı" teorisinde belirttiği gibi, bireyleri sosyal izolasyon korkusuyla sessizliğe iter ve insanlar gerçek düşüncelerini saklayarak grubun yalanlarını dahi savunmak zorunda kalır. Bu iklimde hakikat arayışı anlamını yitirir ve süreç, mantıksal bir tartışma zemininden çıkıp kişinin ait olduğu kabileye kayıtsız şartsız bağlılığını ispatladığı bir "sadakat testine" dönüşür.

Türkiye'deki toplumsal ve siyasal bölünmüşlüğün en temel taşıyıcı kolonlarından biri, artık klasik haber verme işlevinden saparak siyasi bir seferberlik aracına dönüşen medya ekosistemidir. Batı demokrasilerinde görülen yorum farklarının çok ötesine geçen bu durum, medya organları arasındaki geçirgenliğin neredeyse tamamen kaybolmasına ve toplumun devasa bir "çift kutuplu yankı odası" içine hapsolmasına neden olmuştur. Mevcut yapıda bir

blok, ülkenin sürekli kalkındığı, dev projelerle büyüdüğü ve küresel bir lider olduğu ideal bir gerçeklik sunarken; diğer blok, temel hakların yok edildiği ve ekonomik sistemin çöktüğü distopik bir gerçeklik çizmektedir. Ortaya çıkan bu keskin "paralel gerçeklikler" nedeniyle vatandaşlar, takip ettikleri kaynağa göre kendilerini ya refah içindeki bir ülkede ya da karanlık bir rejimde yaşıyormuş gibi hissetmekte, bu durum ise toplumun asgari müştereklerde buluşmasını ve sağlıklı bir tartışma zemini kurmasını imkânsız kılmaktadır.



Şekil 3.2.2 *Negatif partizanlık ve varoluşsal korku siyaseti*

Kutuplaşmanın ulaştığı en tehlikeli boyut, tarafların farklı yorumlara sahip olmasının ötesine geçerek, bizzat olayın kendisi üzerinde dahi mutabakat sağlayamamalarıdır. Geçmişte geçerli olan gerçekler aynı, yorumlar farklı paradigması yerini, temel olguların algılanışının bile ayrıştığı bir yapıya bırakmış; bu durum kurumlara duyulan toplumsal güveni derinden sarsmıştır. Örneğin seçim gecelerinde iki temel haber kaynağının saatlerce birbirine taban tabana zıt veriler sunması, bir tarafın zafer ilan ederken diğerinin manipülasyon iddiasında bulunmasına yol açarak resmî kurumlara olan itimadı zedelemektedir. Benzer şekilde, tarihsel olarak büyük felaketlerin toplumları

birleştirici etkisi, 6 Şubat depremlerinde gerçekleşmemiştir. İnsani yardım süreci dahi "devletin varlığı" veya "yardım organizasyonunun kimin tarafından yürütüldüğü" gibi başlıklar üzerinden hızla siyasi bir tartışma zeminine kayarak derin bir ayrışmaya neden olmuştur.

Güvenin zedelendiği bu ortam, "Baraj patladı" veya "Yağmacılar şehri bastı" örneklerinde görüldüğü gibi, yalan haber ve dezenformasyonun bir orman yangını hızıyla yayılmasına son derece elverişli bir zemin hazırlar. Kamu kurumlarının doğru ve güvenilir bilgi akışını sağlamakta gecikmesi veya zorlanması durumunda, ortaya çıkan boşluk manipülatif içerikler tarafından hızla doldurulur. Neticede Türkiye'deki bu çift kutuplu medya yapısı, yalnızca farklı görüşlerin var olduğu bir çeşitlilik sunmakla kalmaz; aynı zamanda ortak toplumsal gerçekliğin tahrip edilmesine ve kurumsal güvenin çökmesine yol açar. Bu durum, seçimler, doğal afetler veya krizler gibi her kritik anı, potansiyel bir dezenformasyon ve kutuplaşma patlamasına dönüştürmektedir.

Ontolojik güvenliğin zedelendiği ve geleceğin belirsizleştiği bu kaygan zeminde, bireyler derin bir anlam ve kontrol açlığı hissederler; işte bu açlık, en güçlü sığınağını komplo teorilerinde bulur. Görünürde kaotik, rastlantısal ve korkutucu olan olaylar karşısında bu teoriler, kişiye sahte fakat rahatlatıcı bir düzen ve öngörülebilirlik hissi sunar. Bu bakış açısına göre dünyada yaşanan hiçbir şey tesadüf değildir; her krizin veya felaketin arkasında mutlaka gizli, güçlü ve planlı bir "görünmez el" vardır. Bu kurgusal düzen, dünyanın karmaşıklığını basitleştirerek bireye "bilişsel bir kapanış" sağlarken, aynı zamanda olayların perde arkasını bildiği inancıyla, hissettiği çaresizliğe karşı bir "kontrol illüzyonu" ve "özel bilgiye sahip olma" üstünlüğü yaratır. Dolayısıyla, bilimsel otoriteye ve kurumlara güvenin çöktüğü toplumlarda komplo teorileri, basit birer hurafe olmaktan çıkıp, bireyin varoluşsal kaygılarını dindirmeye çalışan psikolojik bir savunma mekanizmasına dönüşür. Dolayısıyla

komplo teorileri, gerçek bir otorite ve bilgi kaynağına duyulan güvenin çökmesiyle oluşan boşluğu dolduran, psikolojik bir savunma mekanizması işlevi görmeye başlar.

Otorite Krizi ve Yalancının Temettüsü

Bu süreç, modern toplumların bilim insanları, hükümetler, medya, akademik kurumlar gibi bilgi ve otorite kaynaklarına duyduğu güvenin de çöküşünü beraberinde getirir. Güvenilir bilgi kaynaklarının bile sürekli sorgulandığı, itibarının zedelendiği bir ortamda, toplum ”yalancının temettüsü/kâr payı” (*liar's dividend*) sarmalına girer.

Yalancının temettüsü, dezenformasyonun yıkıcı bir yan etkisidir: Bir kez yalan söylediği veya dezenformasyon yaydığı ortaya çıkan kişi veya kurum, gelecekte doğruyu söylese bile, bu yalanları bahane ederek, hedef kitlenin her şeyi reddetme eğilimi geliştirmesini sağlar. Bir başka deyişle, kötü niyetli aktörler-yalancılar, ürettikleri dezenformasyon sayesinde, gerçek bilgi kaynaklarının da güvenilirliğini erozyona uğratan genel bir güvensizlik ortamından fayda sağlarlar. Bu durum, komplo teorilerine olan inancı daha da pekiştirir, çünkü insanlar için hiçbir şeye inanmamak, bir şeye inanmaktan daha güvenli hale gelir.

. TEMEL ÇIKARIMLAR

Bu bölüm, Türkiye'de siyasi fikir ayrılıklarının nasıl bir "kimlik savaşına" dönüştüğünü ve bu sürecin toplumsal güveni nasıl yok ettiğini inceler. Artık sadece politikalar üzerinden tartışmıyoruz; karşı tarafı bir "düşman" olarak kodlayan duygusal bir kutuplaşmanın içine hapsolmuş durumdayız. Bu durum, ortak bir toplumsal gerçekliğin parçalanmasına ve herkesin kendi

"mahallesindeki" doğrulara sığınarak diğer her şeye kulaklarını kapatmasına yol açmaktadır.

Temel Kavramlar ve Mekanizmalar

Duygusal Kutuplaşma: Günümüzde kutuplaşma, vergiler veya eğitim gibi somut konuların ötesine geçmiştir. Artık karşıt görüşlü birini sadece farklı düşünen bir vatandaş olarak değil, ülkeye zarar veren "ahlaksız bir düşman" olarak görme eğilimi hakimdir. Bu zehirli iklimde siyaset, fikirlerin yarıştığı bir alan olmaktan çıkıp, "kimin bizden kimin düşman" olduğuna karar verilen bir varoluş savaşına dönüşmüştür.

Ailelere Kadar Sızan Bölünme (Sosyal Mesafe): Kutuplaşma sadece siyasetin konusu olmaktan çıkıp günlük hayatın ve en kişisel ilişkilerin içine sızmıştır. Türkiye'de toplumun büyük çoğunluğu (%75), çocuğunun "öteki/karşı taraftan" biriyle evlenmesine sıcak bakmamaktadır. Birbirimizle ticaret yapmayı veya komşu olmayı reddettiğimizde, karşı tarafı tanımaz hale geliriz; bu da onlar hakkındaki her türlü kötüleme ve komplo teorisine inanmamızı kolaylaştırır.

Korkuyla Beslenen Bağlılık (Negatif Partizanlık): İnsanları sandığa götüren ana motivasyon artık kendi partisine duyduğu sevgi değil, öteki/karşı tarafın kazanmasından duyduğu derin korkudur. "Karşı taraf seçilirse yaşam tarzım tehlikeye girer" düşüncesi, bireyleri mantıklı analiz yapmaktan uzaklaştırıp duygusal bir savunma pozisyonuna iter. Bu korku ikliminde, kendi tarafının söylediği bariz yalanları bile "mahallesini savunmak" adına kabullenmek bir sadakat ispatı haline gelir.

Ayrı Dünyalar ve Güvenin Kaybolması: Medyanın iki kutba ayrılmasıyla birlikte, toplum artık aynı olay karşısında tamamen zıt gerçeklikler tüketiyor. Bir tarafın "başarı" dediğine diğer taraf "felaket"

diyor. Bu durum, seçim gecelerinden büyük depremlere kadar her kritik anın birer güven krizine dönüşmesine neden oluyor. Kurumlara olan güven sarsıldığında, insanlar gerçek bilgiyi aramak yerine sadece kendi mahallesinin sesini duyduğu bir dünyada yaşamaya başlar.

3.2. KENDİNİZİ TEST EDİN

Soru 1: Shanto Iyengar'ın tanımladığı "duygusal kutuplaşma"yı, sıradan görüş ayrılıklarından ayıran temel fark nedir?

A) İnsanların karşı partilileri düşman olarak görmesi

B) İnsanların vergi oranları gibi somut politikalarda uzlaşamaması

C) Sadece seçim dönemlerinde ortaya çıkması

D) Medya sahiplerinin kendi aralarındaki ticari rekabeti

Soru 2: TurkuazLab araştırmasına göre, Türkiye'de insanların yaklaşık %75'i "öteki" parti taraftarlarıyla ilgili hangi tutuma sahiptir?

A) Onlarla iş yapmak isterler.

B) Çocuklarının onlarla evlenmesini istemezler.

C) Onları daha zeki bulurlar.

D) Onlarla komşu olmak isterler.

Soru 3: "Negatif partizanlık" kavramı neyi ifade eder?

A) Kendi partisini çok sevmek

B) Siyasetten nefret etmek ve oy kullanmamak

C) Partisine olan sevgisinden çok, karşı partiye olan nefretiyle motive olmak

D) Parti taraftarlarının tüm partileri negatif şekilde eleştirmesi

3.2. MERAKLISINA EK KAYNAKLAR

Erdoğan, E., & Uyan-Semerci, P. (2020). *Kutuplaşmayı anlamak* [Çevrim içi eğitim aracı]. TurkuazLab. http://www.turkuazlabsaha.org/class/kutuplasmayi-anlamak

Sarsılan Hakikat ve Yeni Tehditler

Gerçeklik Algımızı mı Kaybediyoruz?

Hannah Arendt, 1951 yılında kaleme aldığı "Totalitarizmin Kaynakları" adlı eserinde bugün karşı karşıya olduğumuz dijital bilgi krizini önceden haber veren sarsıcı bir tespitte bulunur. Arendt'e göre bir propaganda makinesinin nihai amacı, insanları sadece belirli bir yalana ikna etmek gibi basit bir hedefle sınırlı değildir. Asıl yıkıcı olan amaç, bireylerin gerçek ile kurgu, doğru ile yanlış arasındaki ayrımı yapma yetisini tamamen ortadan kaldırmaktır.[42] Ona göre totaliter bir sistemin arzuladığı ideal insan tipi, davasına körü körüne bağlı olanlardan ziyade, artık hakikat ile yalan arasında bir fark kalmadığına inananlardır. Bu durum, 21. Yüzyılın bilgi ekosisteminde yaşadığımız ve hakikatin ontolojik çöküşü olarak adlandırabileceğimiz derin bir kırılmayı tarif eder. Artık sorun sadece yalan haberlerin yayılması değil, bireylerin gerçeğin doğasına olan güveninin sarsılmasıdır. Dijital dünyada her şeyin manipüle edilebildiği bu ortamda insanlar neyin gerçek olduğunu bilemedikleri gibi, gerçeğin artık önemsiz olduğu düşüncesine de kapılmaktadırlar. Sonuçta toplum paylaşılan bir gerçeklik zemininden koparak, sadece duygu ve kimliklerin çatıştığı bir belirsizlik alanına sürüklenmektedir.

Dijital dünyada hakikatin nasıl sarsıldığını iki temel belirti üzerinden anlayabiliriz. Birincisi; yapay zekâ ile üretilen videolar, belgeler ve ses kayıtları yüzünden artık neyin gerçek olduğunu ayırt etmenin neredeyse imkânsız hale gelmesidir. Bu durum, bilginin en temel kuralı olan doğrulanabilirlik ilkesini işlemez kılıyor. İkincisi ve belki de daha yıkıcı olanı, insanların artık gerçeğin önemsiz olduğuna inanmaya başlamasıdır. Tartışmalar ortak bir doğrudan kopup sadece duygu ve kimlik çatışmalarına dönüştüğünde, nesnel

[42] Arendt, H. (1951). *The origins of totalitarianism*. Schocken Books.

hakikat yerini grupların kendi "alternatif gerçekliklerine" bırakıyor. Hannah Arendt'in yıllar önce uyardığı gibi, sistemli manipülasyonun asıl hedefi insanları sadece bir yalana inandırmak değil, onların doğru ile yanlış arasındaki ayrımı yapma yetisini tamamen yok etmektir. Bugünün dijital dünyasındaki yankı odaları ve filtre balonları, Arendt'in bahsettiği bu tehlikeyi teknolojik araçlarla yeniden üreterek bizi gerçeklikten koparıyor.

Şekil 3.3.1 *Hannah Arendt ve "Totalitarizmin Kaynakları"*

Toplumsal kutuplaşmanın ve fay hatlarının derinleştiği bir ortamda, bilgiye ve kurumlara karşı takındığımız tavır sağlıklı bir sorgulamadan yıkıcı bir inançsızlığa doğru tehlikeli bir dönüşüm geçirir. Bir toplumun genel sağlığı ve demokratik işleyişi açısından şüphecilik ile kinizm arasındaki ayrımı doğru yapabilmek hayati bir öneme sahiptir. İlk olarak, yapıcı bir eleştiri yöntemi olan şüpheciliği ele alalım; şüpheci birey, önüne gelen her bilgiyi pasif bir şekilde kabul etmek yerine aktif bir sorgulama sürecini benimser. Eleştirel düşüncenin ve bilimsel yöntemin temel taşı kabul edilen bu yaklaşımda birey; "Bu bilginin arkasındaki kanıt nerede?", "İddiayı destekleyen somut veriler nelerdir?" ve "Bilginin kaynağı güvenilir mi yoksa bir çıkar çatışması mı

mevcut?" gibi temel soruları sorar. Şüphecinin asıl motivasyonu gerçeğe ulaşmaktır; sorgulamayı doğru bilgiyi bulmak için bir araç olarak kullanır ve yanlış bir bilgiyle karşılaştığında bunu düzeltmeye, yerine doğru olanı koymaya isteklidir. Bu sağlıklı tutumun doğal bir sonucu olarak medyanın, siyasetçilerin ve kurumların hesap verebilirliği artar, bu da nihayetinde demokrasiyi güçlendirir.

Buna karşılık kinizm, şüpheciliğin yoldan çıkmış, umutsuz ve her şeyi toptan reddeden yıkıcı bir halidir. Kinik bir bakış açısında artık bilginin içeriği önemini yitirmiş, yerini kaynağa yönelik toptancı ve olumsuz bir yargıya bırakmıştır. Kinik birey "Hepsi yalan söylüyor", "Kanıtları da uydururlar" veya "Herkesin gizli bir ajandası var" gibi iddialarla gerçeğe ulaşma çabasından tamamen vazgeçmiştir. Çözüm aramak yerine toptan bir inkâr ve alaycılığın hâkim olduğu bu ruh halinde, birey sadece kendi peşin hükümlerini teyit etmeye odaklanır. Kinizmin toplumsal sonuçları ise oldukça yıkıcıdır; kimsenin kimseye inanmadığı bir ortamda ortak bir gelecek vizyonu inşa edilemez ve kolektif bir direnç gösterilemez, bu da aslında demokrasinin ve sivil toplumun ölümü anlamına gelir. Kurumlara, medyaya ve hatta komşulara duyulan temel güven zedelendiği için toplum parçalanır ve bireyler dış dünyayı düşmanca algıladıkları kendi yankı odalarına çekilirler. Belki de en paradoksal durum, her şeye inanmayı reddeden kinik zihnin, eleştirel sorgulama yeteneğini kaybettiği için kendi grubunun sunduğu komplo teorilerine ve basitleştirilmiş açıklamalara en kolay kanan, manipülasyona en açık zihin haline gelmesidir. Sonuç olarak, sağlıklı bir toplumsal yapı için şüpheciliği teşvik etmek ancak zehirli bir kinizme kayışı engellemek temel bir zorunluluktur.

Sosyolojide güven, modern toplumun işleyişini sağlayan ancak çoğu zaman fark etmediğimiz hayati bir mekanizmadır. Güven, aslında hayatın devasa karmaşasını sadeleştiren bir araçtır. Her karşılaştığımız durumu veya kişiyi en ince ayrıntısına kadar analiz etmeye kalksaydık, modern yaşamın

hızı ve ölçeğiyle başa çıkamazdık. Günlük hayatta bu görünmez inanç ağına ne kadar bağımlı olduğumuzu gösteren pek çok pratik örnek vardır: Örneğin, bir uçağa bindiğimizde pilotun aldığı eğitimi veya uçağın teknik bakım detaylarını tek tek sorgulamayız; bunun yerine havacılık sistemine ve onu denetleyen kurumlara dair kolektif bir "sistemsel güven" duyarız. Aynı şekilde, eczaneden aldığımız bir ilacı laboratuvarda analiz etmek yerine, Sağlık Bakanlığı'na ve bilimsel prosedürlerin doğruluğuna güveniriz. Toplumsal etkileşimin "görünmez çimentosu" olan bu güven duygusu, hayatı tahmin edilebilir ve yaşanabilir kılarak toplumun bir arada kalmasını sağlar.

Şekil 3.3.2 *Bilgiye karşı tutumlar: Şüphecilik ve kinizm*

Ancak bu güven duygusunda, son yıllarda küresel ölçekte derin çatlaklar oluşmaya başlamıştır. Her yıl yayınlanan ve dünya genelinde önemli bir gösterge kabul edilen Edelman Güven Barometresi verileri[43], toplumsal güvenin tarihsel olarak en düşük seviyelere gerilediğini ve bu güvensizlik dalgasının dört temel kurumsal sütunu hedef aldığını ortaya koymaktadır. İlk olarak, hükümetler ve resmî kurumlar; siyasi kutuplaşma, şeffaflık eksikliği

[43] Edelman. (2024). *2024 Edelman trust barometer global report*.

ve kriz yönetimindeki hatalar nedeniyle vatandaşların inancını büyük ölçüde sarsmıştır. İkinci sütun olan medya ise geleneksel haber kaynaklarının siyasallaşması, tık tuzağı içerikler ve sosyal medyadaki dezenformasyon akışı yüzünden halk nezdindeki güvenirliğini kaybetmektedir. Sivil toplum kuruluşları, bağımsızlıklarına ve fon kaynaklarına dair şüpheler nedeniyle toplumsal değişimi tetikleme güçlerini yitirirken; bilimsel kurumlar ve uzmanlar da özellikle pandemi ve iklim değişikliği gibi hayati konuların siyasallaşmasıyla yükselen uzman düşmanlığı akımının hedefi haline gelmiştir.

Kurumsal güven kaybının ötesinde, toplumun en küçük yapı taşlarına kadar işleyen daha sarsıcı bir sorunla karşı karşıyayız: kişilerarası güvenin çöküşü. Dünya Değerler Araştırması gibi küresel veriler, Türkiye gibi toplumsal gerilimin ve kutuplaşmanın yoğun olduğu ülkelerde, insanların birbirine duyduğu güvenin dramatik bir şekilde %10'un altına gerilediğini göstermektedir. Bu istatistik, gündelik hayatta karşılaştığınız, iş yaptığınız veya komşu olduğunuz her 10 kişiden 9'una temel düzeyde bile güvenmediğiniz anlamına gelir.

Kişilerarası ve kurumsal güvenin bu denli zayıfladığı bir toplumsal yapı, dezenformasyon ve komplo teorilerinin kök salması için en elverişli ortamı sunar. Resmi makamlara, güvenilir haber kaynaklarına ve bilimsel verilere olan inanç sarsıldığında, ortaya çıkan otorite boşluğu hızla kontrolsüz ve hatalı bilgilerle doldurulur. Bu süreçte, doğrulanmış resmî açıklamaların yerini sosyal medyada veya kapalı gruplarda yayılan fısıltı gazetesi alır; böylece kanıtlanmamış söylentiler kitleler tarafından toplumsal bir gerçeklik gibi kabul edilmeye başlanır. Bireyler, nesnel ve doğrulanmış kaynaklar yerine kendi ideolojik yankı odalarında yankılanan alternatif gerçeklik kaynaklarına yönelerek ciddi bir yetki kayması yaşarlar. Ancak unutulmamalıdır ki güven, toplumsal iş birliğinin ve kolektif eylemin temel ön koşuludur; güvenin çözüldüğü yerde dayanışma zayıflar, politik uzlaşma imkânsız hale gelir ve

toplum birbirine kuşkuyla bakan izole gruplara ayrışır. Bu durum, toplumsal bütünlüğün kaybına yol açarak kutuplaşmayı derinleştiren en temel itici güçlerden biri haline gelir.

Gerçekliği Savunmasız Bırakan Stratejiler Neler?

Derin öğrenme ve yapay zekâ teknolojilerindeki çığır açan ilerlemeler, dezenformasyon ve hakikat sonrası siyaset literatürüne yukarıda da ele aldığımız yalancının temettüsü kavramını kazandırmıştır. Hukuk profesörleri Robert Chesney ve Danielle Citron tarafından 2018 yılında tanımlanan bu kavram, deepfake teknolojisinin varlığını sadece sahte içerik üretmek için değil; aksine, ortaya çıkan gerçek ve doğrulanabilir kanıtları itibarsızlaştırmak amacıyla kullanmayı ifade eder.[44] Buradaki temel strateji, teknolojinin gerçeği taklit etme gücünü bir kalkan olarak kullanmaktır; böylece kötü niyetli aktörler, kendilerini suçlayan her türlü somut kanıtı "bu bir yapay zekâ kumpasıdır" diyerek reddetme fırsatı, bir tür haksız kâr elde ederler. Bu durum, toplumda zaten var olan "her şey sahte olabilir" algısını besleyerek, gerçek kayıtların bile otomatik bir şüphe mekanizmasının hedefi haline gelmesine ve kamuoyu nezdinde değerini yitirmesine yol açar. Nihayetinde yalancının temettüsü,

> 🔍 **KAVRAM:** DEEPFAKE
>
> **Neyi açıklar?:** "Deep learning" ve "fake" kelimelerinden türetilen bu kavram, yapay zekâ kullanılarak görüntü veya videoda yer alan kişi veya nesnenin başka bir kişi ya da nesne ile yer değiştirilmesiyle üretilen içerikleri tanımlamak için kullanılır.
>
> **Neden önemli?:** Bu teknoloji, sistematik tekrarlarla birleşerek toplumda aslında hiç yaşanmamış olaylara dair sahte fakat güçlü kolektif anıların oluşmasına yol açabilir. Gerçek kanıtların etkisini kaybetmesine ve bireylerin kendi hafızalarına olan güvenlerinin zedelenmesine neden olabilir.

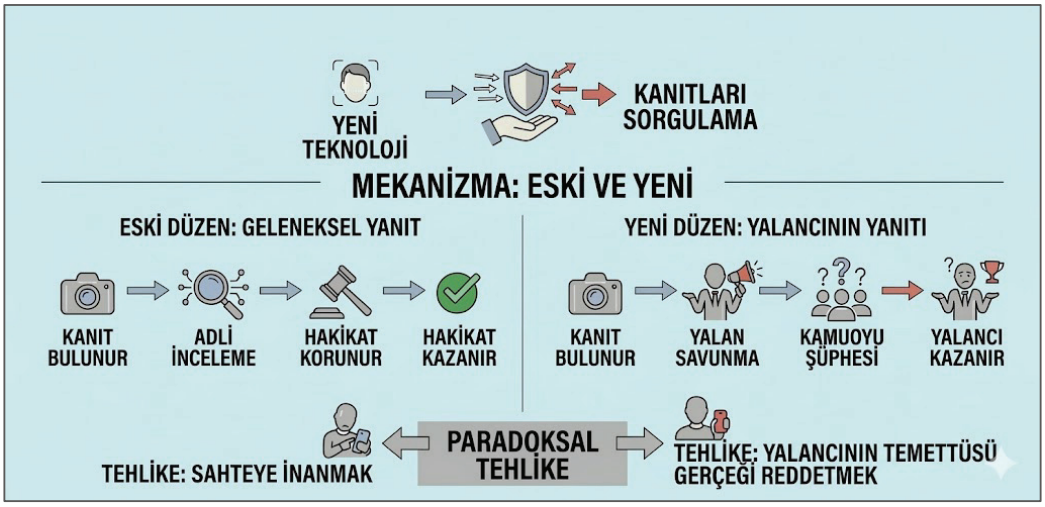
[44] Chesney, R., ve Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs*, *98*(1), 147–155.

dezenformasyonun maliyetini düşürürken, en güvenilir görsel ve işitsel kanıtların dahi inandırıcılığını yok ederek toplumsal güveni ve ortak gerçeklik algısını temelden sarsmaktadır.

Bu deepfake savunmasının bu kadar etkili olmasının temel nedeni, toplumun genelinde yerleşmiş olan psikolojik iklimdir. Yapay zekâ ve deepfake teknolojilerine dair medyada çıkan yoğun haberler sonucunda, toplumda hakikatin çöktüğü ve her şeyin sahte olabileceği algısı kökleşmiştir. Artık vatandaşlar, teknolojinin sadece basit görseller değil, son derece inandırıcı sahte videolar ve sesler üretebildiği gerçeğinin farkındadır. Bu güvensizlik ortamında, suçlanan bir siyasetçinin veya figürün "Bu kayıt deepfake kumpasıdır" şeklindeki savunması, şüpheci zihinlerde hemen karşılık bulur; halk, "Artık her şeyi yapıyorlar, kim bilir işin aslı nedir" diyerek bu savunmayı kolayca benimser. Sonuçta ortaya çıkan şüphe tohumu, bilimsel olarak gerçekliği kanıtlanabilecek somut bir kanıtın bile sırf "Deepfake olabilir" ihtimaliyle itibarsızlaşmasına ve kamuoyu nezdinde güvenirliğini yitirmesine yol açar. Suçlanan aktör ise teknolojinin yarattığı bu bulanık sudan ve toplumsal güvensizlikten büyük bir haksız kâr, yalancının temettüsü elde etmiş olur.

Yalancının temettüsü kavramının yarattığı en büyük yıkım, sadece sofistike sahte videoların üretilmesi değil, gerçekliğin kanıtlanabilirliği ilkesinin temelinden sarsılmasıdır. Eskiden hakikatin en sarsılmaz dayanakları olarak kabul edilen görsel ve işitsel kayıtlar, günümüzde artık otomatik bir şüphe mekanizmasının hedefi haline gelmiştir. Bu tehlikeli süreç yalnızca siyasi skandallarla sınırlı kalmayıp; hukuk sisteminden gazeteciliğe, hatta en mahrem kişisel ilişkilere kadar hayatın her alanına sızmaktadır. Artık bir insanın “Kendi gözümle gördüm, kulağımla duydum” şeklindeki en temel beyanı bile, “Ama bu bir deepfake olabilir” karşı argümanı karşısında yetersiz kalabilmektedir. Hakikate dair yaşanan bu erozyon, toplumsal güveni sistematik olarak çürütürken kutuplaşmayı da beslemektedir; çünkü bireyler artık gerçeği

somut kanıtlarda aramak yerine, yalnızca kendi mahallesinde kabul gören anlatılara inanmayı tercih etmektedir.



Şekil 3.3.3 *Yalancının temettüsü: Robert Chesney ve Danielle Citron (2018)*

Günümüz toplumlarının karşı karşıya kaldığı en büyük meydan okumalardan biri, dezenformasyonun rastlantısal bir yan ürün değil, modern iletişim savaşlarının temelini oluşturan sistematik bir strateji olarak üretilmesidir. Bu stratejik yaklaşımın merkezinde, Stanford Üniversitesi'nden Robert Proctor'un geliştirdiği agnotoloji (*agnotology*) kavramı yatar; agnotoloji, bilgisizliğin veya cehaletin sadece bir eksiklikten ibaret olmadığını, aksine aktif ve kasıtlı bir üretim sürecinden kaynaklandığını savunur.[45] Bu süreçte belirli çıkar grupları, bilinen gerçekleri tartışmalı hale getirmek ve toplumda şüphe tohumları ekmek için bilimsel söylemleri ve halkla ilişkiler stratejilerini bir araç olarak kullanırlar. Agnotolojinin en bilinen örneği, 1950'lerde tütün endüstrisinin uyguladığı ve sigara ile kanser arasındaki bağı doğrudan inkâr etmek yerine "kanıtlar yetersiz ve tartışmalıdır" söylemine sığındığı

[45] Proctor, R. N., & Schiebinger, L. (Der.). (2008). *Agnotology: The making and unmaking of ignorance*. Stanford University Press.

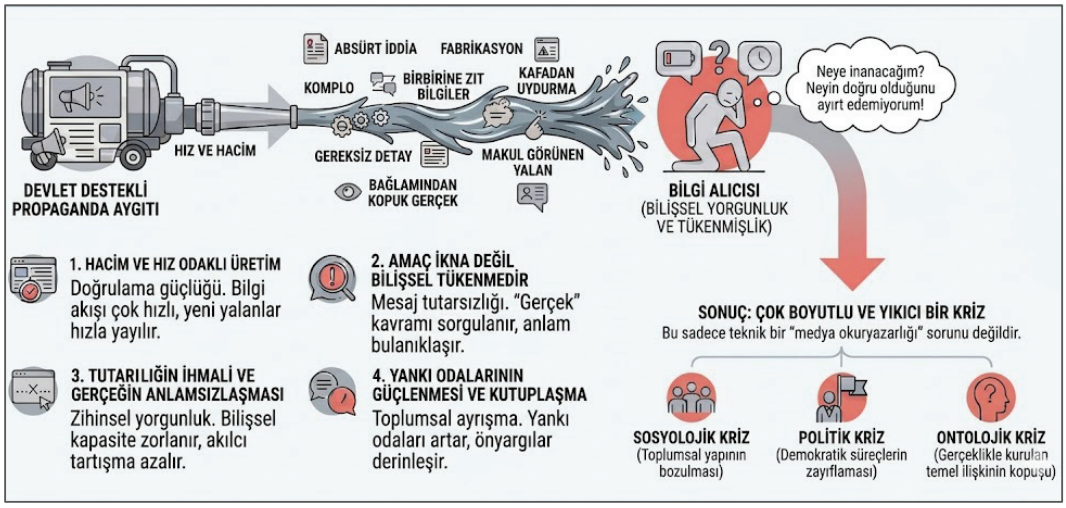
stratejidir. Bu taktiğin asıl amacı uzmanları ikna etmek değil, halkın zihninde bir kafa karışıklığı ve belirsizlik yaratarak kesin kanıtları bile sadece sıradan birer görüşe indirgemektir. Böylece, toplumda yaratılan bu şüphe iklimi sayesinde eyleme geçilmesi ve düzenlemeler yapılması geciktirilir; nitekim günümüzde iklim değişikliğinden aşı karşıtlığına kadar pek çok dezenformasyon kampanyasının temelinde hala bu agnotolojik yöntemler yatmaktadır.

Modern dezenformasyon tekniklerinin en saldırgan ve sistematik uygulamalarından biri olan "yalan (yangın) hortumu" (*firehose of falsehood*), bilişsel düzeyde bir yıpratma savaşıdır. Agnotolojinin, bilinçli bilgisizlik üretme biliminin modern ve sofistike bir uzantısı olan bu strateji, geleneksel ikna çabalarının aksine bilginin yayılma hızı ve hacmi üzerinden etki yaratmayı amaçlar. Tıpkı bir yangın hortumundan fışkıran kontrolsüz su gibi, hedef kitleye aynı anda o kadar çok, hızlı ve birbiriyle çelişen doğru, yanlış, makul veya absürt bilgi pompalanır ki; bu yoğun bombardıman karşısında vatandaşlar, gazeteciler veya analistler neyin gerçek olduğunu ayırt etmeye çalışırken tamamen yorgun ve bitkin düşer. Sonuçta birey, hakikati arama çabasını sürdüremeyecek kadar bilişsel bir tükenmişlik yaşayarak doğruluk arayışından vazgeçme noktasına gelir.

Bu stratejiyi, bir odanın içindeki fısıltıları duymaya çalışan birine, dev hoparlörlerden aynı anda onlarca farklı ve gürültülü ses dinletmeye benzetebiliriz; kişi bir süre sonra hangi sesin gerçek olduğunu anlamaya çalışmaktan vazgeçip kulaklarını kapatmak zorunda kalır. Bu dezenformasyon modelinin temel mantığı ve ana hedefleri dört ana sütun üzerine inşa edilmiştir. İlk sütun olan hacim ve hız odaklı üretim, bilginin miktarını ve yayılma hızını bir yıpratma aracı olarak kullanır. Strateji gereği üretilen içerik o kadar yoğundur ki, teyit mekanizmalarının veya geleneksel medyanın bu iddiaları çürütmeye yetişmesi imkânsız hale gelir; bir yalan henüz etkisiz hale getirilmeden, farklı kanallardan on yeni ve çelişkili yalan hızla piyasaya sürülür.

Buradaki temel hedef, kamuoyunun dikkatini sürekli dağıtmak ve hakikati arama çabasını bir zaman ve kaynak israfı haline getirmektir.

İkinci sütun ise tutarlılığın ihmal edilmesi ve gerçeğin anlamsızlaştırılmasıdır. Geleneksel propagandanın aksine, bu modelde mesajların birbiriyle tutarlı olması gerekmez; iddiaların çelişkili olması, izleyicinin bir ana anlatı kurma çabasını boşa çıkararak epistemolojik kafa karışıklığını derinleştirdiği için bir avantaj olarak görülür. Sonuç olarak asıl amaç, sadece belirli bir siyasi görüşü yerleştirmek değil, bizzat "gerçek" kavramını kamuoyu nezdinde anlamsızlaştırarak itibarsızlaştırmaktır.



Şekil 3.3.4 *Modern dezenformasyonun en agresif hali: "Yalan hortumu"*

"Yalan hortumu" stratejisinin üçüncü ayağı, asıl hedefin birilerini ikna etmek değil, toplumda bilişsel tükenmişlik yaratmak olduğunu ortaya koyar. Çelişkili iddiaların ve kesintisiz bilgi akışının altında ezilen birey, "Ne söylenirse söylensin gerçeği bulmak artık imkânsız" diye düşünerek nihilist bir şüpheciliğe sürüklenir. Toplumun mantıklı ve kanıta dayalı tartışma zeminini kaybetmesiyle sonuçlanan bu durum, kamusal alanı bir arada tutan ortak bağları koparak kutuplaşmayı hızlandırır.

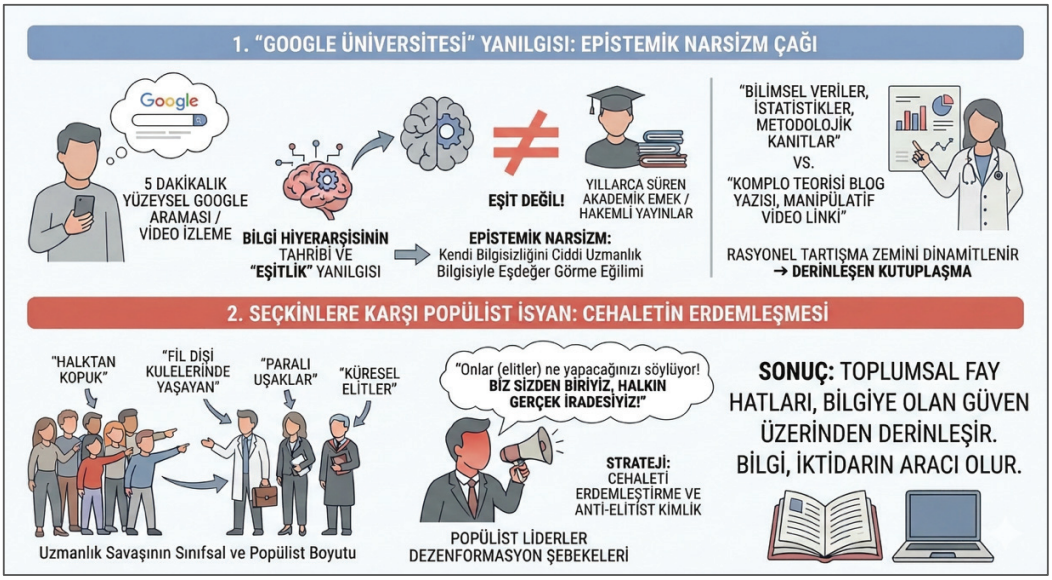
Stratejinin dördüncü sütunu ise bu tükenmişliğin bireyleri yankı odalarına hapsetmesini ve kutuplaşmayı kemikleştirmesini ele alır. Gerçeği aramanın anlamsızlığına inanan kişi, kaotik bilgi dünyasından korunmak için bir savunma mekanizması geliştirerek sadece kendi inançlarını ve siyasi kimliğini doğrulayan kapalı topluluklara geri çekilir. Algoritmaların da beslediği bu içe kapanma süreci, farklı gruplar arasında sadece siyasi değil, gerçeklik algısında da devasa bir epistemolojik uçurum yaratır. Bu durum, toplumun ortak bir zeminde buluşmasını engelleyerek demokratik karar alma süreçlerini temelden sarsar. Bir sonraki bölümde detaylandırılacak olan uzmanlara olan inanç kaybı ve komplo teorilerinin yaygınlaşması da bu olumsuz durumu arttırmaktadır

Neden artık uzmanlara inanmıyoruz?

Toplumsal yapının temelini oluşturan güven duygusundaki aşınma, modern toplumların karşı karşıya olduğu en kritik sorunlardan biri haline gelmiştir. Bu erozyonun en somut ve tehlikeli sonucu ise kurumsal bilgiye, uzmanlığa ve rasyonel hiyerarşiye karşı açılan topyekûn savaştır. Profesör Tom Nichols, *Uzmanlığın Ölümü (The Death of Expertise: The Campaign Against Established Knowledge and Why It Matters*) adlı eserinde, internetin yarattığı bilgi bolluğunun bu süreci nasıl tetiklediğini derinlemesine analiz eder.[46] İnternet, bilgiye erişimi devrim niteliğinde demokratikleştirip eski otoritelerin tekelini kırmış olsa da bu süreçte ham bilgi ile bilgelik, deneyim ve uzmanlık arasındaki temel hiyerarşiyi de tahrip etmiştir. Günümüzde Nichols'ın "epistemik narsisizm" olarak adlandırdığı bir eğilimle, bireyler sadece birkaç dakikalık internet araştırması sonucunda, ömrünü o alana adamış uzmanlarla eşit bilgi düzeyine ulaştıkları yanılgısına kapılmaktadır. Bu durum, rasyonel tartışma

[46] Nichols, T. (2017). *The death of expertise: The campaign against established knowledge and why it matters*. Oxford University Press.

zeminini dinamitleyerek uzmanlık bilgisini elitist bir baskı aracı gibi gören popülist bir isyana zemin hazırlamaktadır. Sonuç, rasyonel bir uzlaşı değil, derinleşen bir kutuplaşmadır.



Şekil 3.3.5 *Toplumsal güvende erozyon ve uzmanlığa karşı topyekûn savaş*

Uzmanlığa karşı açılan bu savaş, basit bir bilgi hiyerarşisi itirazının ötesine geçerek, derin bir sınıfsal öfkeye ve popülist bir isyana dönüşmüştür. Günümüzde akademisyenler, bilim insanları ve medya profesyonelleri, popülist söylemlerle sistematik olarak "halktan kopuk", "fildişi kulelerinde yaşayan" veya "küreselci elitler" olarak damgalanmaktadır. Bu bakış açısına göre bilimsel gerçekler artık tarafsız veriler değil; maske zorunluluğu veya iklim krizi önlemleri örneğinde olduğu gibi, halkın yaşam tarzına müdahale eden üstten bakışlı birer baskı aracı olarak algılanmaktadır. Popülist liderler ve dezenformasyon şebekeleri, bu kurumsal güvensizliği "Onlar size ne yapacağınızı söylüyor, ama biz sizden biriyiz" diyerek ustaca körükler. Bu strateji sonucunda cehalet ve kurallara uymama eğilimi, paradoksal bir şekilde "saf ve otantik" halkın sembolü, hatta bir erdem ve özgürlükçü bir duruş

olarak yüceltilir. Bilgi, iktidarın bir aracı olarak görülürken; cehalet, elitlere karşı bir kimlik beyanına dönüşür. Sonuç olarak toplumsal fay hatları artık sadece siyasi görüşler üzerinden değil, bilgiye ve uzmanlığa duyulan güven düzeyleri üzerinden de derinleşmektedir.

Komplo Teorileri Boşlukları Nasıl Dolduruyor?

Popüler kültürün ve yaygın kanının aksine, komplo teorilerine inanan bireyleri "aptal", "cahil" veya "paranoyak" gibi sıfatlarla etiketlemek bilimsel açıdan büyük bir yanılgıdır. Araştırmalar, komplo inancının zekâ, eğitim düzeyi veya ruh sağlığı ile ters orantılı olmadığını; hatta bazı durumlarda yüksek eğitimli insanların bu anlatılara daha fazla yatkınlık gösterebildiğini ortaya koymaktadır. Bu durumun temelinde, "güdülenmiş muhakeme" (*motivated reasoning*) adı verilen bir beceri yatar; birey bir komployа inanmaya meyilliyse, yüksek bilişsel yeteneklerini bu inancını destekleyecek karmaşık argümanlar üretmek ve karşıt verileri ustalıkla rasyonelize etmek için kullanır. Bu bireyler aslında zihinsel kapasitelerini gerçeği bulmak için değil, kendi ön kabullerini doğrulayacak kanıtlar inşa etmek için seferber ederler. Özünde bu eğilim, dünyanın kaotik ve rastgele olduğu düşüncesinden duyulan korkuyu bastırmak için ”her şeyin gizli bir planın parçası olduğu” sahte düzenine sığınma ihtiyacından kaynaklanır. Dolayısıyla, bir kişi ne kadar donanımlıysa, inanmak istediği hikâyeyi bilimsel görünümlü kılıflara uydurma ve eleştirileri çürütme becerisi de o kadar yüksek olur.

Psikologlar Karen Douglas[47] ve Rob Brotherton[48] tarafından yürütülen çalışmalar, komplo teorilerine inanmanın basit bir bilgi eksikliğinden ziyade, aslında insanın dünyayla kurduğu bağın birbiriyle ilintili üç temel psikolojik

[47] Douglas, K. M., Sutton, R. M., & Cichocka, A. (2017). The psychology of conspiracy theories. *Current Directions in Psychological Science*, *26*(6), 538–542.

[48] Brotherton, R. (2015). *Suspicious minds: Why we believe conspiracy theories*. Bloomsbury Sigma.

ihtiyacını karşılama çabası olduğunu göstermektedir. Bu ihtiyaçlardan ilki olan epistemik ihtiyaç, bir şeyi anlama ve açıklama arzusu, insan zihninin en temel düzeyde her zaman bir düzen ve öngörülebilirlik arayışında olmasından kaynaklanır. Oysa gerçek dünya genellikle kaotiktir; örneğin küresel bir pandeminin bir hayvan pazarından başlaması ya da çok ünlü bir ismin basit bir trafik kazasında ölmesi, beynimizin neden-sonuç mantığını zorlayarak bilişsel bir huzursuzluk yaratır. İşte bu noktada devreye giren ve ”orantılılık yanlılığı” olarak adlandırılan psikolojik eğilim, zihnimizin büyük ve yıkıcı olayların mutlaka büyük, karmaşık ve kasıtlı bir nedeni olmalı şeklinde bir denklik kurmasına yol açar. Komplo teorileri, bu kaotik ve rastgele dünyaya bir mantık ve sözde bir düzen getirerek birey için bir çözüm üretir; çünkü her şeyin gizli bir planın parçası olduğu ve birileri tarafından yönetildiği fikri, dünyanın tamamen başıboş ve kaos içinde olduğu düşüncesinden psikolojik olarak çok daha az korkutucudur. Sonuç olarak, ”Dünyayı güçlü aileler veya gizli odaklar yönetiyor” gibi bir inanca tutunmak, ”Dünyayı aslında kimse yönetmiyor ve her şey kontrolsüz tesadüflerle ilerliyor” gerçeğinin yarattığı dehşet duygusundan kaçmamızı sağlayarak bireye sahte bir kontrol algısı ve iç huzuru kazandırır.

🎧 **DİNLE**

Turkuazlab Podcast Serisi’nde Kadir Has Üniversitesi’den Doç. Dr. Onurcan Yılmaz *Kutuplaşma, Komplo Teorileri ve Gruplararası İlişkiler* başlıklı bir söyleşi gerçekleştirdi.

🔗 Dinlemek için: https://open.spotify.com/episode/1cGb1ZtGdE5mtuvNHUlzKa?si=ghCXvW_DQZmJIEzQnbl34A

Komplo teorilerinin karşıladığı ikinci temel gereksinim, bireyin güvenlik ve kontrol arayışını hedefleyen varoluşsal ihtiyaçtır. İnsan zihni, dünyayı anlamlı, sürekli ve güvenilir bulma isteği olarak tanımlanan ontolojik güvenlik duygusuna ihtiyaç duyar; ancak dezenformasyon ve toplumsal krizler bu

güveni sarsarak dünyayı tutarsız ve tehditkâr bir yer haline getirir. Özellikle doğal afetler, ekonomik çöküşler, savaşlar veya pandemiler gibi büyük toplumsal kriz dönemlerinde, bireyin hayatı kökten sarsılır ve kendi yaşamı üzerindeki kontrolü kaybetme hissi zirveye çıkar. İşte bu anlarda komplo teorileri, birey için adeta bir sığınak işlevi görür. Kaotik ve rastlantısal olaylara karşı sahte de olsa bir düzen, amaç ve kontrol hissi sunarak bireyin yaşadığı yaygın anksiyeteyi hafifletmeye çalışır. Bu teorilere sığınan birey, kaybettiği psikolojik kontrolü "Ben pasif bir kurban değilim; oyunu gördüm, ipleri elinde tutan kuklacıyı tanıyorum, perde arkasındaki gerçeği biliyorum" diyerek geri kazanmaya çalışır. Başkalarının bilmediği gizli ve hayati bir bilgiye sahip olma düşüncesi ve seçilmiş bir azınlık olduğu hissini vererek benlik saygısını destekler. Sonuç olarak kişi, dışsal tehditler karşısında çaresiz kalmak yerine, tehdidin kaynağını tanımlayarak, bu tanım gerçekçi olmasa bile, ona karşı psikolojik bir direniş gösterdiğine inanır. Bu durum, belirsizliğin yarattığı dehşete karşı bireye geçici bir güçlenme, farkındalık ve iç huzuru sağlayan bir kontrol illüzyonu yaratır.

Komplo teorilerine olan eğilimin üçüncü ve oldukça güçlü bir diğer kaynağı ise bireyin sosyal ve benlik merkezli ihtiyaçlarını karşılama arzusudur. Bu teoriler, inanan kişiye hem bir tatmin hem de güçlü bir topluluk hissi sunar. Bu sürecin en belirgin yansıması, bireyin kendini toplumun genelinden ayıran bir seçilmiş azınlık parçası olarak görmesidir; kişi, uyuyan çoğunluğun aksine uyanık olduğunu ve herkesin göremediği hayati gerçekleri fark ettiğini düşünerek bir tür ayrıcalık hissi yaşar. Özellikle toplumda dışlanmış, marjinalleşmiş ya da statü kaybına uğramış gruplar için komplo teorileri, kaybedilen sosyal saygınlığı geri kazanmanın bir yolu haline gelir. Bu özel bilgiye sahip olma duygusu, bireyi bir anda bilen ve önemli bir konuma yükselterek onun benlik saygısını destekler. Sonuç olarak, komplo teorileri sadece dünyadaki karmaşayı açıklamakla kalmaz; aynı zamanda bireyin kendi kimliğini

ve değerini sosyal bir çerçevede yeniden inşa etmesine yardımcı olur.

TEMEL ÇIKARIMLAR

Bu bölüm, bilginin sadece kirlenmediği, aynı zamanda hakikatin ontolojik olarak çöktüğü bir dönemi inceler. Artık sadece yalan haberlerle değil, bizzat gerçeğin doğasına olan inancın sarsılmasıyla karşı karşıyayız. Bu süreçte kurumsal güven ve uzmanlık bilgisi itibar kaybederken, bireyler kaosu açıklamak ve kontrol hissi kazanmak için komplo teorilerine ve toptan inançsızlığa sığınmaktadır. Sonuç olarak, ortak bir gerçeklik zemininde buluşamayan bir toplumda rasyonel tartışma imkânsız hale gelmekte ve demokratik güven temelden sarsılmaktadır.

Temel Kavramlar ve Mekanizmalar

Şüphecilikten Kinizme Kayış: Sağlıklı bir şüphecilik gerçeğe ulaşmak için kanıt ararken; kinizm, "herkes yalan söylüyor" diyerek gerçeğe ulaşma çabasından tamamen vazgeçmektir. Kinik birey, tüm bilgi kaynaklarını kirli gördüğü için kendi peşin hükümlerine daha sıkı sarılır ve paradoksal olarak manipülasyona daha açık hale gelir.

Yalancının Temettüsü (T*he Liar's Dividend*): Yapay zekâ ve Deepfake teknolojilerinin varlığı, kötü niyetli aktörlere kendilerini suçlayan her türlü gerçek kanıtı "bu bir kumpastır" diyerek reddetme fırsatı (temettü) sağlar. Bu durum, görsel ve işitsel kayıtların doğrulanabilirliğini ortadan kaldırarak toplumda "hiçbir şeye inanmamak daha güvenlidir" algısını pekiştirir.

Agnotoloji ve Yalan Hortumu: Bilgisizliğin kasıtlı olarak üretilmesini inceleyen agnotoloji, şüphe yaratarak eyleme geçilmesini engellemeyi amaçlar. "Yalan Hortumu" stratejisinde ise topluma o kadar hızlı ve çelişkili bilgi pompalanır ki, birey doğruyu yanlıştan ayırt etmeye çalışırken bilişsel tükenmişlik yaşayarak hakikat arayışından tamamen vazgeçer.

Epistemik Narsisizm (Uzmanlığın Ölümü): İnternet bilgiye erişimi kolaylaştırsa da 5 dakikalık bir Google aramasının yılların akademik uzmanlığına eşit olduğu yanılgısını yaratmıştır. Bireyin kendi yüzeysel araştırmasını derin bir uzmanlık bilgisiyle eşdeğer görmesi, "epistemik narsisizm" olarak adlandırılır ve bu durum rasyonel tartışma zeminini yok eder.

Komplo Teorilerinin Psikolojik Sığınağı: Komplo teorileri sadece bilgi eksikliğinden değil; bireyin düzen, güvenlik ve kontrol ihtiyacını karşılama arzusundan beslenir. Dünyanın kaotik ve tesadüfi olduğu fikrinden korkan birey, her şeyin arkasında kötü niyetli bir "büyük plan" olduğu inancıyla sahte bir iç huzur ve seçilmiş azınlık olma ayrıcalığı kazanır.

3.3. KENDİNİZİ TEST EDİN

Soru 1: "Yalancının temettüsü" (*the liar's dividend*) kavramı, deepfake teknolojisinin hangi tehlikesine işaret eder?

A) Sahte videoların gerçek sanılmasına

B) Deepfake'in varlığının *gerçek* kanıtları da *sahte* şüphesiyle itibarsızlaştırmasına

C) Deepfake üretiminin oldukça maliyetli olmasına

D) Yapay zekanın dünyayı ele geçirmesine

Soru 2: Psikologlara göre, insanların komplo teorilerine inanmasının temel *varoluşsal* nedeni nedir?

A) Kaotik ve güvensiz bir dünyada, kontrol hissi ve anlam arayışı

B) Zekâ ve algı seviyelerinin düşük olması

C) Çok fazla bilim kurgu film ve dizileri izlemeleri

D) Bilimsel verilere aşırı güvenmeleri

Soru 3: Tom Nichols'un *Uzmanlığın Ölümü* kitabında eleştirdiği ve internetin neden olduğu yanılgı nedir?

A) İnternetin oldukça yavaş olması

B) Çevrim içi eğitimin ve açık erişim yayınların artması, yaygınlaşması

C) İnternetten hızla edinilen bilginin, konunun uzmanlarının bilgisiyle eşit görülmesi

3.3. MERAKLISINA EK KAYNAKLAR

Cepdibi, A. K. (2025). Güçsüzlük hakikatin aldatmak iktidarın özünde mi var? Hakikat-sonrası çağa Hannah Arendt'in ışığında bakmak. E. Erdoğan, P. Uyan-Semerci ve G. Uysal-Gündoğdu (Der.), *Bilgi düzensizliklerine karşı toplumsal bilişsel dirençlilik* içinde. İstanbul Bilgi Üniversitesi Yayınları.

Erdoğan, E. (2025). Komplo teorileri: Psikolojik mekanizmalar ve demokratik siyaset için sonuçları. *Sosyoloji Divanı*, (26), 29-57.

Snyder, T. (2017). *On tyranny: Twenty lessons from the twentieth century*. Tim Duggan Books.

Oran, İ. (2025). Türkiye ve uluslararası literatürde bilgi düzensizliği, yanlış bilgi ve hakikatin önemsizleşmesi: Bibliyometrik bir karşılaştırma. E. Erdoğan, P. Uyan-Semerci ve G. Uysal-Gündoğdu (Der.), *Bilgi düzensizliklerine karşı toplumsal bilişsel dirençlilik* içinde. İstanbul Bilgi Üniversitesi Yayınları.

Bölüm 4

Dijital Dünyada Doğrulara Ulaşma Rehberi

🎯 TARTIŞMA SORULARI

1. Yanal okuma tekniği ve Dur, Araştır, Bul, İz, Sür (*SIFT*) metodolojisi tam olarak nasıl uygulanır?
2. Görsel ve videoların sahteliğini anlamak için hangi dijital araçlar kullanılır?
3. Sosyal medyadaki bot hesapları ve manipülasyon ağlarını nasıl tespit ederiz?
4. Bir fotoğrafın veya videonun çekildiği "tam konumu" (jeolokasyon) harita üzerinde nasıl buluruz?
5. İnternetten silinen veya değiştirilen bilgilere ulaşmak mümkün mü?

Giriş

Bu modülde, dijital ortamdaki bilgilerin, görsellerin ve videoların doğruluğunu teknik araçlar ve sistematik yöntemler kullanarak nasıl teyit edeceğinizi öğreneceksiniz. Öncelikle, bir kaynağın güvenilirliğini sadece kendi içeriğine bakarak değil, dış kaynaklarla karşılaştırarak değerlendiren yanal okuma (*lateral reading*) stratejisi ve bu süreci adım adım uygulayan SIFT (***S**top, **I**nvestigate the **S**ource, **F**ind Better Coverage, **T**race Claims to the Original Context*-Dur, Sorgula, Bul, İzini Sür*)* metodolojisi işlenecektir. Ardından, sahte veya bağlamından koparılmış fotoğrafları tespit etmek için tersine görsel arama motorlarının kullanımı ile videoları kare kare analiz ederek manipülasyonları yakalayan InVID & WeVerify gibi profesyonel yazılımlar tanıtılacaktır. Görsel içeriklerdeki mimari ve coğrafi ipuçlarını kullanarak bir olayın tam konumunu harita üzerinde saptayan coğrafi konumlama, jeolokasyon (*geolocation)* teknikleri ve yapay zekâ ile üretilen sahte içeriklerin ayırt edici fiziksel özellikleri incelenecektir. Son olarak, internetten silinen veya değiştirilen verilere ulaşmayı sağlayan Wayback Machine gibi dijital arşiv araçları ve sosyal medyadaki etkileşimi manipüle eden sahte bot hesapların analizi ele alınacaktır.

İZLE

RESAID tarafından hazırlanan açık erişim derslerin *Doğrulama Teknikleri ve Dijital Okuryazarlık* başlıklı bölümünü izlemeniz konuyu daha kolay anlamanıza yardımcı olacaktır.

Doğrulama Teknikleri
https://youtu.be/TmOo7eNuFJ0
Dijital Medya Okuryazarlığı ve Eleştirel Düşünme
https://youtu.be/0c-S6vUeTno
Yanlış Bilgi ve Mücadele Stratejileri
https://youtu.be/NjVAPYO9kM4

Dikey Okumadan Yanal Okumaya Geçiş

Geleneksel Okuma Alışkanlığının Sınırları

Dijital çağın karmaşık bilgi ekosisteminde kaybolmadan yolunuzu bulmak, bir başka deyişle sıkı bir "dijital dedektif" olmak için; servet değerinde adli bilişim yazılımlarına, derin kodlama bilgilerine ya da gizli bir ajanlık geçmişine ihtiyacınız yok. Bu kaosun içinde ayakta kalmak ve hakikati yakalamak için yapmanız gereken tek bir şey var: Yıllardır size öğretilen ve artık bir reflekse dönüşen okuma alışkanlığınızı kökten değiştirmek. Bizler okul sıralarında, geleneksel eğitim sisteminin disiplini içinde hep "dikey okuma" dediğimiz bir yönteme programlandık. Önümüze bir kitap, bir gazete ya da akademik bir yazı geldiğinde ne yaparız? Başlıktan başlar, bir asansör gibi satır satır iner, yazarın kurduğu hikâyeye odaklanır ve sayfa bitince dururuz. Bu bizim fabrika ayarımızdır. Bu "dikey" yaklaşım, basılı dünyanın kuralları içinde harika işliyordu. Çünkü o dünyada, bir yazı önünüze gelmeden önce devreye giren editörler ve yayıncılar vardı. Bu "kalite kontrol bekçileri", okuduğunuz metnin belli bir doğruluk ve profesyonellik standardında olmasını garanti ederdi. Ancak dijital dünyada bir editoryal süzgeç yok; bu yüzden eski dünyanın haritasıyla bu yeni dünyada yolumuzu bulmak maalesef mümkün değil. Artık cebinde akıllı telefonu olan herkes, neredeyse sıfır maliyetle anında bir yayıncıya dönüşebilir.

Bu yüzden, bir web sitesini ya da sosyal medya gönderisini sadece dış görünüşüne, tasarımının şıklığına veya dilinin ciddiyetine bakarak dikey okumak, bir başka deyişle ona sadece içsel göstergelerine, kendi vitrinine bakarak not vermek, yapabileceğiniz en tehlikeli hatadır. Bu safça yaklaşım, aslında bir dolandırıcıya gidip "Sana güvenebilir miyim?" diye sormaktan farksızdır. Alacağınız cevap şaşmaz ve tereddütsüzdür: "Elbette, ben en güvenilir kaynağım!". Bu yöntemle, dolandırıcının tuzağına kendi isteğinizle düşmüş

olursunuz. İşte bu tehlikeli illüzyondan kurtulmak ve dijital ormanda hayatta kalmak için tek bir çaremiz var: Geleneksel "dikey okuma" alışkanlığımızı bir kenara bırakıp, stratejimizi "yanal okuma" tekniği ile güncellemek.

Yanal Okuma Tekniği Nedir?

İnternet, bilgiye erişim konusunda eşi görülmemiş bir kolaylık sunarken, aynı zamanda doğru ile yanlışın, bilimsel gerçekle propagandanın iç içe geçtiği karmaşık ve tehlikeli bir bilgi ekosistemine dönüşmüştür. Bu kaotik ortamda, bir bilginin güvenilirliğini hızlı ve doğru bir şekilde değerlendirme becerisi, artık sadece akademik bir merak konusu olmaktan çıkmış; her birey için hayati bir dijital okuryazarlık yetkinliği haline gelmiştir.

Stanford Üniversitesi'nden Eğitim Profesörü Sam Wineburg ve araştırma ekibi, yayımladıkları ufuk açıcı çalışma[49] ile bu kritik becerinin farklı kullanıcı grupları arasındaki dağılımını gözler önüne sermiştir. " sivil eleştirel okuryazarlık" (*civic critical literacy*) adı verilen bu deneyin temel amacı, internet üzerindeki bir kaynağın güvenilirliğine karar verme süreçlerinde insanların gerçekte nasıl bir zihinsel yol izlediğini anlamak olmuştur.

Wineburg'ün bu kapsamlı çalışması, bilgi eleştirisi konusunda çok farklı seviyelerde yetkinliğe sahip üç ayrı grubu karşılaştırmalı bir mercek altına almıştır. İlk grubu, teknolojiyle iç içe büyüyen, dijital arayüzlere doğuştan aşina olan ve "dijital yerliler" olarak adlandırılan Stanford öğrencileri oluşturmuştur; beklenti, bu genç kitlenin dijital dünyada hızla ve etkin bir şekilde hareket edeceği yönünde olmuştur. İkinci grupta, akademik disiplinleri gereği birincil kaynakları titizlikle inceleyen, yazarın niyetini ve bağlamı sorgulama konusunda uzmanlaşmış tarih profesörleri yer almıştır. Üçüncü grup ise

[49] Wineburg, S., & McGrew, S. (2019). Lateral reading: Reading less and learning more when evaluating digital information. *Teachers College Record, 121*(11), 1–40.

işi bizzat gündelik bilgi akışını doğrulamak ve yanlış bilgiyi avlamak olan doğrulama kuruluşlarında profesyonel biçimde çalışanlardan (*fact-checkers*) meydana gelmiştir.

Katılımcılara zorlu bir görev verilmiş ve onlardan halk sağlığına ilişkin tartışmalı bir konuda yayın yapan iki farklı web sitesini inceleyerek hangisinin daha güvenilir olduğunu belirlemeleri istenmiştir. Sitelerden biri (Site A), tıp dünyasının köklü ve saygın otoritesi sayılan "Amerikan Pediatri Akademisi" (AAP) iken; diğeri (Site B), isim benzerliği ile onu taklit eden ancak aslında bilimsel uzlaşıya karşı çıkan ve nefret söylemi yayan "Amerikan Çocuk Doktorları Koleji" (ACPeds) adlı paravan bir örgüt olmuştur. Deneyin sonuçları, modern bilgi tüketimi alışkanlıkları hakkında oldukça çarpıcı bir gerçeği gün yüzüne çıkarmıştır: Yüksek dijital beceriye veya geleneksel akademik eleştirel düşünme yeteneğine sahip olmak, internetteki bir kaynağın güvenilirliğini tespit etmek için tek başına yeterli olmamaktadır.

Deneyin sonuçlarına bakıldığında, hem dijital yerli olan Stanford öğrencilerinin hem de kaynak eleştirisi uzmanı tarih profesörlerinin büyük bir çoğunluğu, şaşırtıcı bir şekilde, propaganda amaçlı kurulan Site B'nin güvenilir olduğuna inanmış veya karar verme sürecinde büyük zorluk yaşamıştır. Bu grupların düştüğü yanılgının temel nedeni, izledikleri hatalı strateji, bir başka deyişle dikey okuma olmuştur. Bu gruplar, Site B'nin dijital sınırları içerisinde kalarak, siteyi yalnızca kendi iç dinamikleriyle değerlendirmeyi tercih etmiştir. "Hakkımızda" sayfalarını incelemiş, sitenin kurumsal görünümlü logosuna, profesyonel web tasarımına ve bilimsel referans süsü verilmiş dipnotlarına odaklanmışlardır. Sonuç olarak site, kendi kapalı döngüsü içinde tutarlı ve kurumsal bir görünüm sergilemiştir. Dışarıdan bağımsız bir sorgulama yapmadıkları için, bu gruplar aslında bilginin kaynağını değil, sunumun kalitesini puanlamış ve yanıltıcı sitenin tuzağına düşmüşlerdir. Profesyonel teyitçiler, doğrulama kuruluşlarında çalışanlar ise tamamen farklı bir strateji

izleyerek ezici bir başarı göstermiştir. Onların bu başarısının arkasındaki sır, yanal okuma adı verilen yöntem olmuştur. Teyitçiler Site B'ye girdikleri anda, içeriği detaylıca okuyarak vakit kaybetmek yerine, saniyeler içinde o sayfadan ayrılmayı seçmişlerdir. Hızla 5-6 yeni internet sekmesi (*tab*) açmış ve arama motorlarına site hakkında şu kritik soruları yöneltmişlerdir:

- "American College of Pediatricians nedir?"
- "Kim tarafından finanse ediliyor?"
- "Hakkında Wikipedia ne diyor?"
- "Güvenilir mi?"

Teyitçiler, sitenin içeriğine değil, sitenin hakkında dış dünyanın, bir başka deyişle saygın kurumların ve bağımsız kaynakların ne dediğine odaklanmışlardır. Sonuçta uyguladıkları bu yanal araştırma sayesinde, saniyeler içinde Site B'nin saygın bir tıp kurumu olmadığını; tam tersine siyasi ve ideolojik amaçlarla kurulmuş, bilim dışı, nefret grupları arasında sınıflandırılan bir örgüt olduğunu tespit etmişlerdir. Güvenilirlik kararı, tamamen dışarıdan gelen sinyallere dayandırılmıştır. Sam Wineburg'ün bu çalışması, dijital güvenilirlik değerlendirmesi için temel bir kuralı ortaya koymuştur: Bir web sitesinin veya herhangi bir dijital kaynağın güvenilirliğini anlamak için, o kaynağın kendisine bakmak yetersiz ve çoğu zaman tehlikeli bir yöntem olmaktadır. Çünkü her kaynak, kendi güvenilirliğini iddia etmekte doğal bir çıkar sahibidir. Wineburg'ün literatüre geçen o meşhur benzetmesiyle ifade edilecek olursa: "Bir berbere, saç tıraşına ihtiyacınız olup olmadığını soramazsınız."

Sonuç olarak gerçek dijital okuryazarlık, kaynakta kalıp onu analiz etmek, dikey okuma değil; kaynaktan çıkarak onu diğer güvenilir kaynaklarla çapraz kontrole tabi tutmak olan yanal okuma becerisinde yatmaktadır. Yanal okuma, günümüzün karmaşık bilgi ekosisteminde doğruyu yanlıştan ayırt etmenin en etkili ve en hızlı yolu olarak karşımıza çıkmaktadır.

Dijital çağda, bilgiye erişim hızı baş döndürücü bir seviyeye ulaşırken, güvenilir kaynakları şüpheli olanlardan ayırt etme becerisi hayati bir önem taşımaktadır. Bu bağlamda, dijital okuryazarlığın temel direği olarak kabul edilen yanal okuma, gözlerin sayfa üzerinde aşağı doğru ilerlediği geleneksel dikey okumanın aksine, bakış açısının tarayıcı sekmeleri arasında yatay bir düzlemde kaydırılmasını gerektirmektedir. Bir içeriğin detaylarına dalmadan veya onu tüketmeye başlamadan önce, o içeriği sunan kaynağın güvenilirliğinin doğrulanması süreci, bu yöntemin esasını oluşturmaktadır.

Şüpheli veya daha önce hiç tanımadığınız örneğin "GercekHaberler.com" gibi jenerik isimli bir web sitesi ya da Twitter'da "@KulistenBilgi" gibi popüler olmayan anonim bir hesap ile karşılaşıldığında, izlenmesi gereken standart protokol "kaynağı doğrulamak için sekmeleri açın" kuralına dayanmaktadır. Bu süreçte atılması gereken ilk adım, başlık ne kadar kışkırtıcı, şok edici veya ilgi çekici olursa olsun, haberi okumaya başlamadan önce duygusal bir refleks vermekten kaçınarak okuma işlemini derhal durdurmak ve soğukkanlılığı korumaktır.

Hemen ardından, mevcut içeriğin bulunduğu sayfayı kapatmadan veya ondan ayrılmadan, tarayıcıda yeni bir sekme açılarak, örneğin Google gibi bir arama motoruna gidilmesi gerekmektedir. Açılan bu yeni sekmede, haberin içeriği yerine doğrudan kaynağın kendisi spesifik ve doğrulayıcı sorularla sorgulanmalıdır. Bu aşamada arama motoruna, örneğin bir web sitesi için "GercekHaberler.com kimin?", "GercekHaberler.com güvenilir mi?" veya "GercekHaberler.com ne zaman kuruldu?" gibi sorular; şayet kaynak bir sosyal medya hesabı ise "@KulistenBilgi kimdir?" veya "@KulistenBilgi doğruluk sicili" gibi ifadeler yazılarak arama yapılmalıdır.

Aramanın devamında kaynağın kendi iddiaları yerine, diğer saygın ve bağımsız kuruluşların o kaynak hakkında ne söylediği araştırılmalıdır. Türkiye’de özellikle teyit.org ve Doğruluk Payı gibi yerel veya uluslararası

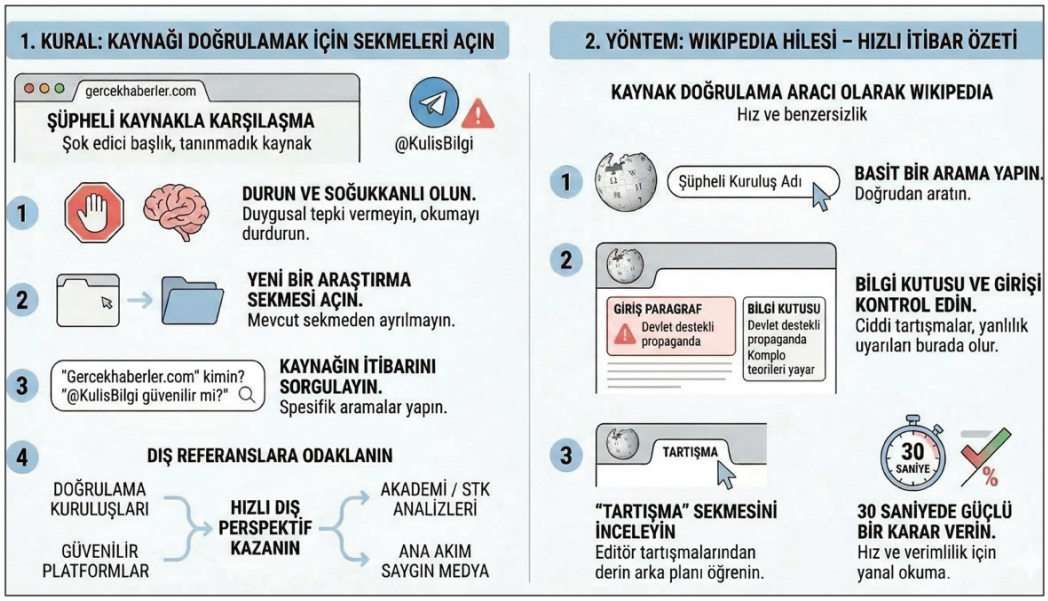
doğrulama kuruluşlarının raporlarına, Evrim Ağacı gibi bilimsel içerik platformlarına, medya izleme grupları ve üniversite araştırmaları gibi akademik veya STK analizlerine ve son olarak kaynağın itibarının diğer büyük ve güvenilir haber kuruluşları tarafından nasıl ele alındığına odaklanılması önem arz etmektedir. Bu stratejik süreç, bir haberin içeriğini analiz etmeye başlamadan önce, yayımcı mecranın kalitesi ve olası taraflılığı hakkında okuyucuya hızlı ve dışa dönük bir perspektif sunmaktadır.

Şekil 4.1.1 *Dijital güvenilirlik değerlendirmesi: Sam Wineburg ve Stanford deneyi (2017)*

Akademik dünyada Wikipedia nadiren birincil kaynak olarak kabul edilse de dijital okuryazarlık bağlamında bir kaynak doğrulama aracı olarak benzersiz bir hıza ve işleve sahip olmaktadır. Bu stratejik kullanımda, şüphelenilen medya kuruluşu, düşünce kuruluşu veya sivil toplum örgütü doğrudan Wikipedia üzerinde aratılmaktadır. Araştırmacıların sağdaki özet bilgi kutusuna ve makalenin giriş paragraflarına göz atması yeterli olmaktadır; zira bir kuruluşun geçmişinde ciddi tartışmalar, yanlılık veya doğruluk sorunları mevcutsa, Wikipedia bu kritik bilgileri genellikle makalenin en başına, temel tanımın hemen yanına eklemiştir. Örneğin, bir kuruluşun "devlet destekli

propaganda aracı olduğu", "bir siyasi parti ile doğrudan bağlantılı bulunduğu" veya "komplo teorileri yaydığı" gibi hayati bilgiler, okuyucuya 30 saniye içinde kaynağın genel "itibar özetini" sunmaktadır. Ayrıca, makalenin üst kısmında yer alan "tartışma" (*talk*) sekmesinin incelenmesi, derinlemesine bir arka plan bilgisi sağlamaktadır. Bu sekmeye tıklandığında, Wikipedia editörlerinin o kuruluş hakkındaki bilgilerin sunumu üzerine yürüttüğü tartışmalar okunabilmekte; bu tartışmalar genellikle kuruluşun en sorunlu yönlerini, taraflılıklarını ve güvenilirlik sorunlarını şeffaf bir şekilde ortaya çıkarmaktadır. Wikipedia'nın bu stratejik kullanımı, bir kaynağın itibarını sıfırdan araştırmak için harcanacak dakikaları kısaltmakta ve güvenilirlik hakkında hızlıca güçlü bir karar verilmesini mümkün kılmaktadır. Sonuç olarak, yanal okuma bir hız ve verimlilik meselesidir; bilginin içeriğine odaklanmadan önce, onu yayımlayanın niteliğine odaklanmak esas olmaktadır.

Dört Adımda Doğrulama: SIFT Metodolojisi



Şekil 4.1.2 *Kaynak doğrulama teknikleri*

Dijital çağın getirdiği yoğun bilgi bombardımanı altında, doğru ile yanlışı, manipülasyon ile gerçeği ayırt edebilmek artık hayati bir beceri niteliği taşımaktadır. Washington State Üniversitesi'nden dijital okuryazarlık uzmanı Mike Caulfield, bu karmaşık doğrulama sürecini herkesin kolaylıkla uygulayabileceği, akılda kalıcı ve pratik bir çerçeveye oturtmuştur: SIFT yöntemi (*Stop, Investigate, Find, Trace* /Dur, Sorgula, Bul, İzini Sür). Caulfield'ın geliştirdiği bu sistematik yaklaşım[50], kullanıcıları pasif birer bilgi tüketicisi olmaktan çıkarıp, aktif ve şüpheci birer dijital dedektife dönüştürmeyi amaçlamaktadır.

Dur: Duygusal Tepkini Dondur

Bu adım, genellikle uygulanması en zor, ancak sonuçları itibarıyla sürecin en kritik aşamasını oluşturmaktadır. Bir içerikle karşılaşıldığında iç dünyada aniden beliren yoğun bir öfke, derin bir korku, şoke edici bir coşku veya şiddetli bir haklılık hissi gibi kıvılcımlar, beyindeki sistem 1'in bir başka deyişle duygusal ve hızlı çalışan mekanizmanın direksiyona geçtiğinin açık bir işareti olmaktadır. Böylesi bir durumda izlenmesi gereken eylem planı şüpheye yer bırakmayacak kadar nettir: Okuma eylemi anında kesilmeli, içerik akışı durdurulmalı ve parmaklar "paylaş", "retweet" veya "beğen" butonlarından derhal çekilmelidir. Bu stratejik duraksamanın temel gerekçesi, manipülasyon ve

> 🔍 **KAVRAM:** BİLİŞSEL CİMRİLİK
>
> **Neyi açıklar?:** İnsan beyninin, enerjisini korumak ve verimliliği artırmak amacıyla minimum zihinsel çaba harcayarak sonuca ulaşma eğilimini ifade eder.
>
> **Neden önemli?:** Bilişsel cimrilik; beynin enerji tasarrufu sağlamak amacıyla derinlemesine sorgulama yerine hızlı ve zahmetsiz sezgisel kısayolları tercih etmesine neden olarak, bireyleri yanlış bilgilere ve manipülasyona karşı savunmasız bıraktığı için önemlidir.

[50] Caulfield, M. (2019). *Web literacy for student fact-checkers*. Pressbooks.

dezenformasyonun, özellikle tık tuzağı (*clickbait*) ve öfke tuzağı (*rage bait*) adı verilen yöntemlerle doğrudan sistem 1'i hedef almasıdır. Sistem 1 devredeyken rasyonel sorgulama yeteneği kilitlenmektedir; dolayısıyla fiziksel olarak durmak, anlık tepki verme dürtüsünü kırmakta ve rasyonel, analitik ve yavaş çalışan sistem 2'yi devreye sokmaktadır.

Bu bilinçli duraksama sağlandıktan sonra, kişinin kendisine şu stratejik soruları yöneltmesi gerekmektedir: "Bu kadar güçlü bir duyguyu hissetmem bir tesadüf müdür; bu içeriği bana kim ve neden sunmaktadır?", "Karşımdaki bilgi doğru olsa bile, buna bu kadar hızlı bir tepki vermem zorunlu mudur?" ve "Bu içerik, sadece benim kendi ön yargılarımı (*confirmation bias*) desteklediği için mi bana bu kadar inandırıcı gelmektedir?"

Araştır: Kaynağı Yanal Olarak Araştır

Bir içeriğin derinliklerine inmeden önce, onu sunan kaynağın kimliğini ve niyetini anlamak, doğrulama sürecinin en kritik adımını oluşturmaktadır; zira dijital dünyada bilgi, ancak kaynağının güvenilirliği kadar değer taşımaktadır. Bu aşamada, dijital okuryazarlık uzmanı Mike Caulfield'ın geliştirdiği ve profesyonel teyitçilerin altın kural olarak kabul ettiği yanal okuma tekniği devreye girmektedir. Geleneksel dikey okuma alışkanlığının aksine, okuyucunun metni yukarıdan aşağıya doğru okumayı bırakıp tarayıcıda yeni sekmeler açması ve yatayda ilerlemesi gerekmektedir. Çünkü bir web sitesinin profesyonel tasarımı, kurumsal logoları veya etkileyici "hakkımızda" yazıları, o sitenin güvenilir olduğuna dair bir kanıt sunmamaktadır; dolandırıcıların ve propaganda odaklarının da takım elbise giyebileceği unutulmamalıdır. Bu nedenle, sitenin kendi kendini tanımlamasına güvenmek yerine, bağımsız ve dış kaynakların o site hakkında neler söylediğine odaklanılması esas kabul edilmektedir. Bu dışsal araştırma süreci, kaynağın dijital ayak izlerini takip eden stratejik sorularla derinleştirilmelidir.

Öncelikle, içeriği kaleme alan yazarın kimliği titizlikle sorgulanmalı; metnin gerçek ve tanınmış bir uzman tarafından mı, yoksa jenerik bir takma ad veya sahte bir profil (*troll*) kullanan anonim aktörlerce mi yazıldığı tespit edilmelidir. Bununla birlikte, dijital dedektifliğin teknik boyutu devreye sokularak, sitenin alan adının ne zaman tescil edildiği WHOIS gibi araçlarla sorgulanmalıdır. Son olarak, sitenin tarafsızlığını test etmek adına, başka kaynakların bu platformu "güvenilir bir mecra" mı yoksa "devlet destekli bir propaganda organı" mı olarak tanımladığına dikkat edilmesi, doğru bilgiye ulaşmanın en güvenli yolu olmaktadır.

Bul: Daha İyi ve Geniş Kapsamlı Kaynak Bul

Bir iddia ne kadar büyük ve sarsıcıysa, onu doğrulayan kaynak yelpazesinin de o denli geniş olması gerektiği temel bir dijital okuryazarlık ilkesi kabul edilmektedir. SIFT yönteminin bu kritik aşaması, kullanıcıyı kendisine sunulan tek bir hikâyeye mahkûm olmaktan kurtarmayı amaçlamaktadır. Bu süreçte uygulanan "çapraz okuma" tekniği, iddianın anahtar cümlelerinin kopyalanarak genel arama sonuçları yerine özellikle Google Haberler (*News*) sekmesinde aratın. Dijital dedektifliğin "büyük olay" kuralına göre; şayet "dev bir barajın patladığı", "ünlü bir liderin istifa ettiği" veya "küresel bir salgının başladığı" gibi çığır açıcı bir haber, sadece anonim bir sosyal medya hesabında veya adı sanı duyulmamış bir blogda yer alıyorsa, bu bilgi %99,9 oranında asılsız sayılmaktadır. Zira BBC, Reuters, Associated Press veya Anadolu Ajansı gibi küresel haber ağlarının ve ulusal yayıncıların sessiz kaldığı "büyük" bir olay, doğrulama eşiğini geçememiş demektir; gerçek ve büyük olaylar asla tek bir kaynağın tekelinde kalmamakta, aksine hızla yayılarak güvenilir mecralarca teyit edilmektedir.

İzini Sür: Orijinal Bağlama ve Kaynağa Ulaş

İnternet ortamı, bilginin her paylaşımda kaçınılmaz olarak aşındığı, kırpıldığı ve bağlamından koparıldığı devasa bir kulaktan kulağa oyunu sahası olarak işlev görmektedir. Bu karmaşık bilgi zincirini geriye doğru sararak orijinal kaynağa ulaşmak, dijital okuryazarlığın en belirleyici adımı kabul edilmektedir. Karşılaşılan bir ekran görüntüsü, GIF veya kısa video klibin kökenini tespit etmek amacıyla *Google Lens*, *TinEye* veya *Yandex Görsel Arama* gibi araçlar kullanarak Tersine Görsel Arama yapılması, görselin eski bir olaydan alınıp alınmadığını veya manipüle edilip edilmediğini şüpheye yer bırakmayacak şekilde ortaya çıkarmaktadır. Görsel teyidin ötesinde, metin ve video kliplerin orijinal versiyonlarına ulaşmak, "bağlam kontrolü" açısından hayati bir zorunluluk taşımaktadır. Zira 10 saniyelik bir klipte sadece "Ben rüşvet aldım..." dediği duyulan bir siyasetçinin, videonun tamamı izlendiğinde aslında "Bana 'rüşvet aldın' iftirası attılar" dediği anlaşılabilmekte; kasten kesilen küçük bir kısım, gerçeği taban tabana zıt bir yalana dönüştürebilmektedir. Sonuç olarak dijital dünyada bilgi, ancak ve ancak kendi orijinal bütünü ve bağlamı içerisinde gerçek anlamını kazanmaktadır.

Sonuç: Şüphe Bir Kas Gibidir

Günümüzde, internet üzerinden yayılan bilgi miktarı kontrolsüz bir hızla artmaktadır. Bu durum, özellikle sağlık ve bilim gibi hassas konularda, yanlış bilginin yayılmasını kolaylaştırmaktadır. Yanal okuma bir sitenin güvenilirliğini anlamak için o siteden ayrılıp, güvenilir ve tarafsız dış kaynaklara başvurma yöntemidir. Bu, profesyonel bilgi doğrulayıcıların, teyitçilerin kullandığı temel tekniktir. Bir web sitesinin size sunduğu vitrine hapsolmak yerine, mevcut sekmeyi açık bırakıp hemen yanına yeni tarayıcı sekmeleri açarak dış dünyada küçük bir keşfe çıkmalısınız. Arama motoruna sitenin adını yazıp yanına "Nedir?", "Güvenilir mi?" veya "Kim tarafından finanse ediliyor?" gibi

sorular eklediğinizde, karşınıza çok daha şeffaf bir tablo çıkacaktır. Örneğin, yukarıdaki senaryomuzda olduğu gibi kendi başına profesyonel görünen "Dünya Doktorlar Birliği" ismini sorguladığınızda; bağımsız kaynaklar veya resmi sağlık kuruluşları size bu yapının aslında hiçbir tıbbi akreditasyonu olmayan bir lobi grubu olduğunu saniyeler içinde gösterebilir. Buradaki en kritik gerçek şudur: Bir kaynağın kendi hakkında ne iddia ettiği değil, güvenilir dış dünyanın o kaynak hakkında ne söylediği esastır. Dikey okuma ile oluşturulan o sahte güven algısı, yanal okuma sayesinde yıkılır ve yanıltıcı içerikler daha en başında elenmiş olur.

Yanal okuma ve SIFT gibi dijital okuryazarlık metodolojileri, yalnızca bir kez okunup geçilecek teorik bilgilerden ibaret olmayıp, kazanılması gereken zihinsel birer alışkanlık niteliği taşır. Bu süreci, tıpkı düzenli spor antrenmanları gibi, kullandıkça güçlenen bir kasın gelişimi olarak düşünmek gerekmektedir. İnsan beyni, "bilişsel cimrilik" olarak adlandırılan verimlilik ve enerji tasarrufu prensibiyle çalıştığı için, başlangıçta her iddiayı doğrulamak adına yeni sekmeler açmak veya kaynakları kontrol etmek zihne yorucu ve zaman alıcı bir eylem gibi görünebilmektedir. Beynin en az enerjiyle en hızlı sonuca ulaşma eğiliminden kaynaklanan bu doğal direnç, ancak söz konusu tekniklerin ısrarla uygulanmasıyla aşılabilmekte ve şüphe kası güçlendirilerek dijital okuryazarlık kalıcı bir reflekse dönüşmektedir.

Ancak kritik eşik aşıldığında, bir başka deyişle bu doğrulama adımları yeterince tekrar edildiğinde, zihin en kısa yolu otomatikleştirir. Bu eylemler, zamanla bilinçli bir çabadan çıkar ve bir refleks haline gelir. Artık bir manşet gördüğünüzde, içinizdeki şüphe mekanizması tetiklenir ve eliniz, bilginin kaynağını kontrol etmek için otomatik olarak Ctrl+T (veya Mac'te Cmd+T) tuşlarına gider. Yeni bir sekmede, okuduğunuz haberin temelini oluşturan iddiayı aratır, diğer güvenilir kaynaklar ne diyor diye hızla göz gezdirirsiniz. İşte tam da bu otomasyonun gerçekleştiği an, sorgulamanın ikinci doğanız

haline geldiği o kritik nokta, sizin için bir dönüm noktasıdır. O an, pasif, şüpheci olmayan ve manipülasyona açık olan bilinçsiz tüketici statüsünden çıkıp, bilgiyi aktif olarak işleyen, değerlendiren ve doğrulayan dijital dedektif kim-

📌 ÖRNEK SENARYO: "HAKKIMIZDA" TUZAĞI

İnternette araştırma yaparken karşınıza ".org" uzantılı, ismi oldukça ciddi ve tasarımı profesyonel görünen bir web sitesi çıktığını hayal edin. Örneğin, çocuk sağlığı üzerine çarpıcı iddialarda bulunan "Dünya Doktorlar Birliği" gibi bir siteye girdiğinizde, refleks olarak hemen "Hakkımızda" sayfasına tıklayıp sitenin kendi yazdığı misyonu okuyor ve oradaki beyaz önlüklü doktor fotoğraflarına bakarak bir güven puanı veriyorsanız, aslında "dikey okuma" tuzağına düşüyorsunuz demektir.

Bu yöntem oldukça tehlikelidir; çünkü bir kaynağı sadece kendi sunduğu vitrine bakarak değerlendirmek, bir dolandırıcıya "Sana güvenebilir miyim?" diye sormaktan farksızdır. Alacağınız cevap her zaman "Elbette, ben en güvenilir kaynağım!" olacaktır. Sitede gördüğünüz o güven veren logolar, profesyonel fotoğraflar ve "bağımsız topluluk" gibi ifadeler, aslında sizin dikey okuma alışkanlığınızı kullanarak zihninizi yanıltmak için tasarlanmış birer maskedir. "Bu site bir .org uzantısına sahip, kâr amacı gütmüyor, doktorlardan oluşuyor ve güvenilir görünüyor. İddiaları doğru olabilir." sonucuna varırsınız ki bu "vitrin" odaklı yaklaşım, sizi sitenin kendi kapalı döngüsüne hapseder ve dışarıdaki gerçeklerden koparak yanıltıcı sonuçlara ulaşmanıza neden olur. Gerçeğe ulaşmak için bu dikey bakıştan sıyrılmalı ve sekmeler arasında yatay bir yolculuğa çıkmaya hazırlanmalısınız.

liğine büründüğünüz andır. Bu, sadece bilgi güvenliğiniz için değil, aynı zamanda sağlıklı bir dijital vatandaşlık için de elzemdir.

Bu noktaya gelindiğinde, zihinsel yazılımımızı başarıyla güncellediğimizi söyleyebiliriz. Artık doğru bir bakış açısına sahibiz: gördüğümüz hiçbir şeye ilk anda inanmamak, her zaman kaynağına inmek ve yanal doğrulama yapmak. Ancak bu bakış açısının tam anlamıyla etkili olabilmesi için, onu somut,

elle tutulur kanıtlara dönüştürecek teknik araçlara ihtiyacımız var. Çünkü dijital manipülasyonlar her zaman metin bazlı değildir; genellikle görseller, videolar ve sesler üzerinden yapılır.

Bir fotoğrafın bağlamından koparılıp koparılmadığını veya üzerinde dijital oynama yapılıp yapılmadığını sadece çıplak gözle tespit etmek, günümüz teknolojisinde neredeyse imkânsız hale gelmiştir. İnsan gözü, dijital hilelerin sofistike doğası karşısında yetersiz kalmakta ve görselin manipüle edilip edilmediğini ayırt etmekte zorlanmaktadır. Bu nedenle, manipülasyonları objektif bir şekilde saptayabilmek için duyularımıza değil, doğru teknik araçlara ihtiyacımız vardır.

TEMEL ÇIKARIMLAR

Bu bölüm, dijital okuryazarlığın sadece teknik bir beceri değil, zihinsel bir refleks değişimi olduğunu vurgular. Okulda öğrendiğimiz geleneksel okuma, bir metni baştan başlayıp, sonuna kadar okumak, dijital dünyada bizi savunmasız bırakır. Bir kaynağın güvenilirliğini anlamak için ona, onun "vitrinine" bakmak yerine, tarayıcıda yeni sekmeler açarak dış dünyanın o kaynak hakkında ne dediğine bakmak gerekir.

Temel Kavramlar ve Mekanizmalar

Dikey vs. Yanal Okuma: Dikey okuma, bir web sitesinin içinde kalarak tasarımına ve "hakkımızda" sayfasına aldanmaktır; bu, bir dolandırıcıya "Sana güvenebilir miyim?" diye sormaya benzer. Yanal okuma ise siteden ayrılıp, sekmeleri açarak başka kaynakların o site hakkında ne dediğini kontrol etmektir.

SIFT Metodolojisi: Bilgi kirliliğiyle başa çıkmak için geliştirilen 4 adımlı protokoldür: **S**top (dur/duygusal fren yap), **I**nvestigate (kaynağı araştır),

Find (daha iyi kaynak bul), **T**race (orijinal bağlama git).

Wikipedia İstihbaratı: Wikipedia, akademik bir kaynak olmasa da bir kaynağın "itibarını" (propaganda aracı mı, güvenilir mi?) saniyeler içinde kontrol etmek için kullanılabilecek bir araç olabilir.

4.1. KENDİNİZİ TEST EDİN

Soru 1: SIFT metodolojisinin ilk adımı olan "dur" (*stop*), hangi durumda uygulanmalıdır?

A) İnternet bağlantısı kopup, bizi öfkelendirdiğinde

B) Bir içerik bizde aniden yoğun bir öfke, korku veya şok yarattığında

C) Yazı çok uzun olduğundan bizi sıktığında

D) Bilgisayarın şarjı azalıp, bizi paniklettiğinde

Soru 2: Bir web sitesinin güvenilirliğini analiz ederken, o siteye takılıp kalmak yerine; tarayıcıda yeni sekmeler açarak başka kaynakların o site hakkında ne dediğini araştırmaya ne ad verilir?

A) Dikey okuma

B) Yanal okuma

C) Derin okuma

D) Hızlı okuma

Soru 3: SIFT yönteminin "izini sür" (*trace*) adımı neyi amaçlar?

A) Haberin kimler tarafından paylaşıldığını aramayı ve bulmayı

B) Yorumları okuyarak, yorumlardan farklı argümanları bulmayı

C) Takipçi sayısını artırmak için iz sürmeyi

D) Bilginin, fotoğrafın veya videonun değiştirilmemiş, orijinal kaynağına ulaşmayı

4.1. MERAKLISINA EK KAYNAKLAR

Ersöz, M. (2023, 29 Nisan). *Afet dönemlerinde kullanılabilecek teyitçilik araçları*. Teyit. https://teyit.org/teyitpedia/afet-donemlerinde-kullanilabilecek-teyitcilik-araclari Cambridge Üniversitesi, BBC Media Action, & Jigsaw. (t.y.). *Yanlış bilgilere yönelik pratik önceden çürütme (prebunking) kılavuzu*.

Silverman, C. (Der.). (2014). *Verification handbook: A definitive guide to verifying digital content for emergency coverage*. European Journalism Centre.

Görsel Analiz ve Fotoğraf Doğrulama

İngilizcede yaygın olarak kullanılan ve kökeni çok eskilere dayanan bir deyim vardır: Görmek inanmaktır *("Seeing is believing")*. Bu ifade, nesnel gerçekliğin en güvenilir kanıtının gözlem olduğu fikrine dayanır. Ancak, içinde yaşadığımız bu hiper-dijital çağda, bu eski deyiş, *tarihin en tehlikeli yanılgısı* ve bir zafiyet noktası haline gelmiştir. Artık görmek, sorgulamayı bırakmak anlamına gelme riski taşımaktadır. Beynimiz, evrimsel süreçte geliştirdiği kısayollar nedeniyle, özellikle görüntülere karşı derin bir yatkınlığa sahiptir. Görsel üstünlük etkisi, görsel bilginin metinsel veya işitsel bilgiden çok daha hızlı, etkili ve maalesef *sorgusuz* bir şekilde işlendiğini ve hafızaya kaydedildiğini gösterir. Bu etki, dijital dezenformasyonun temel dayanağıdır.

Basit bir örnekle açıklayalım: Bir kişi, "Paris yanıyor" diye bir tweet atsa, zihnimizde hemen bir şüphe mekanizması (sistem 2) devreye girer. Kaynağı kimdir? Başka bir yerde haber var mı? Ancak, alevler içinde kalan bir Eyfel Kulesi'nin fotoğrafını veya videosunu gördüğümüz anda, beynimizin daha sezgisel ve hızlı karar veren kısmı olan sistem 1 anında devreye girer ve görüntüyü "kanıt" olarak kabul ederiz. Bu bilişsel hız, eleştirel düşünme filtresini atlamamıza neden olur.

Dijital dünyada ise karşılaşılan bir fotoğraf veya video, artık gerçeğin sorgulanamaz bir kanıtı olmaktan çıkıp, teknik müdahalelere açık basit birer veri dosyası haline gelmiştir. Günümüz teknolojisinde bu veri dosyaları temel olarak üç farklı yöntemle manipüle edilmektedir: İlk olarak, Photoshop ve benzeri düzenleme yazılımları aracılığıyla görüntüdeki öğeler silinebilmekte, yenileri eklenebilmekte veya görselin yapısı tamamen değiştirilebilmektedir. İkinci ve daha sinsi olan yöntem, tamamen gerçek olan bir fotoğrafın örneğin eski bir depremden alınarak sanki güncel bir sel felaketinde yaşanmış bir görüntü gibi sunulması, bir başka deyişle "yanlış etiketlenerek" orijinal

bağlamından koparılmasıdır.

Üçüncü ve en yeni tehdit ise, yapay zekâ (YZ) destekli araçlarla gerçekte hiç yaşanmamış olayların veya var olmayan kişilerin sıfırdan üretildiği ikna edici "sentetik medya" içeriklerinin oluşturulmasıdır. Tüm bu manipülasyon olanakları, dijital ortamda görülen her görsel içeriğe, doğruluğu kanıtlanana kadar bir "olağan şüpheli" muamelesi yapma zorunluluğunu doğurmuştur.

Bu Fotoğraf İlk Kez Nerede ve Ne Zaman Paylaşıldı?

Dijital dedektifliğin en temel ve en etkili yöntemlerinden biri olan tersine görsel arama tekniği, internet ortamında hızla yayılan görsel tabanlı yanlış bilginin en güçlü panzehiri niteliğini taşımaktadır. Geleneksel internet aramalarında kullanıcılar arama çubuğuna anahtar kelimeler girerek ilgili görsellere ve web sayfalarına ulaşırken; bu yöntemde süreç tam tersine işlemekte ve arama motoruna metin yerine doğruluğundan şüphe duyulan fotoğrafın kendisi veya bağlantı adresi (URL) yüklenmektedir. Bu sayede arama motoru, kelimeler yerine pikselleri analiz ederek yüklenen görselin dijital dünyadaki geçmişini, orijinal kaynağını ve hangi bağlamlarda kullanıldığını deşifre etmekte, kullanıcıya görsel kanıtların izini sürme imkânı tanımaktadır.

Bu basit ama etkili teknik, dijital dedektiflere görselin tarihçesini ve gerçek bağlamını ortaya çıkaran hayati ipuçları sunmaktadır. Tersine görsel arama sayesinde, şüpheli bir fotoğrafın internetin sonsuz arşivinde daha önce kullanılıp kullanılmadığı ve ilk olarak hangi tarihte ortaya çıktığı saptanarak, görüntünün güncel bir olaya ait olup olmadığı kesinlik kazanmaktadır. Ayrıca bu yöntem, fotoğrafın en yüksek çözünürlüklü ve kırpılmamış orijinal haline ulaşılmasını sağlayarak, manipülatörlerin bağlamı değiştirmek amacıyla yaptıkları kadraj oyunlarını veya çözünürlük düşürme hilelerini ifşa

etmektedir. Özellikle "bağlamdan koparma" yoluyla üretilen dezenformasyonu saniyeler içinde çökerten bu araç, kötü niyetli bir aktörün on yıl önceki eski bir fotoğrafı alıp "şu anki olay yeri" iddiasıyla yaymaya çalıştığı yalanları anında yakalamaktadır.

İZLE

Tersine görsel aramanın nasıl yapılacağını izlemek için Malumatfuruş tarafından hazırlanan videoyu izleyebilirsiniz.

https://www.youtube.com/watch?v=yb48qi6mvIY

Dijital dünyada her arama motorunun kendine has bir algoritması ve uzmanlaştığı bir alan bulunduğu için, elinizdeki vakanın niteliğine göre en doğru aracı seçmeniz çok önemlidir. Araştırmanızda bir nesneyi, tarihi bir binayı veya ticari bir ürünü tanımlamanız gerekiyorsa, ilk başvuracağınız adres genellikle geniş veri tabanıyla Google Lens olmalıdır; ancak Google'ın gizlilik politikaları nedeniyle insan yüzlerini eşleştirme konusunda kasıtlı olarak kısıtlandığını unutmamanız gerekir. Eğer hedefiniz bir fotoğraftaki kişinin kimliğini saptamak veya görselin farklı açılardan çekilmiş yüksek çözünürlüklü hallerini bulmaksa, "yüz tanıma" konusunda uzmanlaşmış olan Yandex Images'dan yararlanabilirsiniz. Daha agresif algoritmalar kullanan bu motor, özellikle arka plan eşleştirmelerinde ve insan yüzlerini tespit etmede güçlü bir araç olarak kabul edilir.

Görselin içeriğinden ziyade tarihçesini ve zaman akışını sorguladığınız durumlarda ise TinEye kullanılabilir. TinEye, bir fotoğrafın internete yüklendiği "ilk tarihi" saptayarak, güncel olduğu iddia edilen bir görselin aslında yıllar öncesine ait olduğunu kanıtlamanızı ve bağlam manipülasyonlarını saniyeler içinde çökertmenizi sağlar. Son olarak, eğer elinizdeki fotoğraf kesilmiş, kırpılmış veya sadece küçük bir parçasından ibaretse, Bing Images iyi

bir performans sergileyebilir. Google'ın bazen gözden kaçırdığı detayları yakalayan Bing, eldeki yarım parçadan hareketle fotoğrafın orijinal bütününü veya benzer karelerini bulma konusunda analiz uzmanı işlevi görerek, yapbozun eksik parçalarını tamamlamanıza yardımcı olur.

👉 DENE

thispersondoesnotexist.com sitesini ziyaret edin. Karşınıza çıkan her yüz, o saniyede bir yapay zekâ algoritması (GAN) tarafından üretilmiştir. Bu insanlar gerçekte hiç var olmamıştır. Bu yüzlerdeki YZ'a özgü hataları yakalamaya çalışın.

Dört farklı arama motoruna tek tek görsel yükleyerek zaman kaybetmek yerine, bu süreci otomatikleştiren "RevEye" veya "InVID & WeVerify" gibi tarayıcı eklentilerini kullanmak tercih edilebilir. Chrome veya Firefox tarayıcınıza kolayca kurabileceğiniz bu akıllı araçlar sayesinde, internette karşılaştığınız herhangi bir görselin üzerine sağ tıkladığınızda açılan menüden Google, Yandex, Bing ve TinEye gibi dev motorların hepsinde aynı anda tarama başlatabilir; böylece teyit sürecini hızlandırarak saniyeler içinde en kapsamlı sonuçlara zahmetsizce ulaşabilirsiniz.

Görüntü Gerçek mi? Üretildi mi? Cheepfake & Deepfake

Dijital çağda, bir görselin gerçekliğini sorgulamak temel bir okuryazarlık becerisi haline gelmiştir. Görsel dezenformasyon, üretiminde kullanılan teknolojiye göre temelde iki ana kategoriye ayrılmaktadır; medya ve kamuoyu genellikle yüksek teknoloji ürünü yapay zekâ sahteciliklerini, "deepfake" kavramını tartışsa da gerçek dünyada yaygınlığı ve hızlı yayılma potansiyeli açısından asıl büyük tehlike ucuz/basit sahtecilik "cheapfake" adı verilen yöntemdir. Bu manipülasyon türü, genellikle karmaşık yapay zekâ

teknolojilerine veya ileri düzey yazılımlara ihtiyaç duymadan, basit düzenleme araçları veya sadece yanıltıcı bir bağlam kullanılarak üretilen ve doğrudan izleyicinin duygularını hedef alan son derece etkili bir dezenformasyon yöntemidir. Bir videonun hızının değiştirilerek konuşmacının sarhoş ya da agresif gösterilmesi veya bir fotoğrafın anlamını değiştirecek şekilde kırpılması da bu kategoride yer alır. Ancak yöntemin en yaygın ve tehlikeli biçimi, görselin teknik olarak hiç değiştirilmediği ancak tamamen farklı bir olaymış gibi sunulduğu "yanlış etiketleme"dir. Somut bir örnekle; 2020 yılındaki İzmir depremine ait tamamen gerçek bir fotoğrafın, yıllar sonra "Hatay'da son durum" başlığıyla paylaşılması durumunda, fotoğrafın kendisi üzerinde oynama yapılmadığı için yapay zekâ tespit araçları bu hileyi yakalamakta başarısız olmaktadır. Dolayısıyla teknik bir müdahaleden ziyade bağlamın çarpıtıldığı bu tür vakalarda gerçeği ortaya çıkarmanın tek yolu, tersine görsel arama araçlarını kullanarak görüntünün dijital geçmişini taramak ve orijinal tarihini tespit ederek yalanı çürütmektir.

🔍 **KAVRAM:** DEEPFAKE

Neyi açıklar?: "Deep learning" ve "fake" kelimelerinden türetilen bu kavram, yapay zekâ kullanılarak görüntü veya videoda yer alan kişi veya nesnenin başka bir kişi ya da nesne ile yer değiştirilmesiyle üretilen içerikleri tanımlamak için kullanılır.

Neden önemli?: Bu teknoloji, sistematik tekrarlarla birleşerek toplumda aslında hiç yaşanmamış olaylara dair sahte fakat güçlü kolektif anıların oluşmasına yol açabilir. Gerçek kanıtların etkisini kaybetmesine ve bireylerin kendi hafızalarına olan güvenlerinin zedelenmesine neden olabilir.

Adından da anlaşılacağı üzere "derin öğrenme" teknolojisine dayanan deepfake, yapay zekâ algoritmaları kullanılarak üretilen ve gerçeğinden ayırt edilmesi oldukça zor olan ileri düzey bir sahtecilik türüdür. Bu teknoloji sayesinde, daha önce hiç var olmamış bir görsel sıfırdan yaratılabilmekte veya gerçek bir videodaki kişinin yüzü ve sesi, başka birininkiyle kusursuzca değiştirilebilmektedir. Örneğin, Papa Francis'in üzerinde modern, beyaz bir şişme montla görüldüğü viral fotoğraf, gerçek bir kare değil,

Midjourney gibi araçlarla üretilmiş sentetik bir içeriktir. Bu tür görseller tamamen yeni ve benzersiz olduğu için, standart Tersine Görsel Arama motorları herhangi bir geçmiş kayıt bulamamakta ve yetersiz kalmaktadır; bu nedenle bir deepfake'i yakalamanın en etkili yolu, teknolojinin bıraktığı biyolojik ve fiziksel tutarsızlıkları insan gözüyle dikkatle incelemektir.

Şekil 4.2.1 *Görselin kaynağı: Karapınarlı, S. (2023, 27 Mart). Papa Francis'in beyaz mont giydiği fotoğrafın gerçek olduğu iddiası. Teyit. https://teyit.org/analiz/papa-francisin-beyaz-mont-giydigi-fotografin-gercek-oldugu-iddiasi*

Tersine görsel arama araçları, internette önceden var olan fotoğrafları bulmakta son derece başarılı olsa da GAN (***G****enerative* ***A****dversial* ***N****etworks*) teknolojisiyle saniyeler içinde üretilen ve aslında hiç yaşamamış insanlara ait "yapay zekâ yüzleri" karşısında çaresiz kalmaktadır. Bot hesaplarda ve dolandırıcılık vakalarında sıkça kullanılan bu benzersiz portreler, arama motorlarında taratıldığında "Sonuç Bulunamadı" yanıtını döndürmekte ve bu "dijital sessizlik" aslında sahteliğin en güçlü kanıtı olmaktadır. Bu tür görselleri

çıplak gözle yakalamak için bir dedektif gibi yapay zekanın henüz çözemediği anatomik hatalara odaklanmak gerekir; zira yapay zekâ, göz bebeklerini tam daire yerine amip gibi yamuk çizebilmekte, gözlerdeki ışık yansımasını farklı yönlere koyarak fizik kurallarını ihlal etmekte veya bir kulakta küpe varken diğerini unutarak simetriyi bozmaktadır. Ayrıca gözlük çerçevelerinin ciltle erimiş gibi görünmesi, diş sayısındaki anormallikler ve arka plandaki nesnelerin rüya gibi bulanıklaşıp şekilsizleşmesi sahteciliği ele veren diğer hatalardır. Gözle tespitin zor olduğu durumlarda ise "Hive Moderation" veya "Illuminarty" gibi algoritmik araçlar kullanılarak görselin kaynağı teyit edilebilmektedir.

Deepfake teknolojisi her ne kadar hızla gelişse de insan anatomisi ve fizik kurallarını taklit ederken hala arkasında, dikkatli bir gözlemle yakalanabilecek belirgin özgün hatalar bırakmaktadır. Bir görselin yapay zekâ ürünü olup olmadığını anlamak için bakılması gereken ilk ve en önemli yer ellerdir; çünkü yapay zekâ sıklıkla altı parmaklı, eksik veya birbirine geçmiş jöle kıvamında eller çizerek kendini açıkça ele vermektedir. Benzer bir başarısızlık metinlerde de görülür; görseldeki tabelalar, kitap kapakları veya giysilerdeki yazılar genellikle okunamaz, alfabe dışı garip sembollerden oluşan anlamsız bir yapıdadır. Ayrıca gözlük çerçevelerinin farklı kalınlıklarda olması veya küpelerin simetrisindeki uyumsuzluklar, arka plandaki ağaç veya fayans desenlerinin bulanıklaşarak mantıksızca birbirine geçmesi ve yüzlerin hiçbir gözenek veya kırışıklık barındırmayan aşırı pürüzsüz "plastik" bir dokuya sahip olması, karşımızdaki görüntünün gerçek değil, sentetik bir üretim olduğunu kanıtlayan kritik detaylardır.

Pikseller ve Hatalar Sahteliği Nasıl Ele Verir?

Her dijital fotoğraf veya video dosyası, çıplak gözle görülmeyen ancak dosyanın tüm yaratılış hikayesini barındıran ve "EXIF" (*exchangeable image file*

format) olarak adlandırılan gizli bir pasaport taşımaktadır. Görselin "dijital DNA'sı" kabul edilen ve teyit etmek için birincil kanıt kaynağı olan bu veri; olayın zaman çizelgesini saniye hassasiyetiyle doğrulayan zaman damgasından, çekimi yapan cihazların marka ve model bilgilerine kadar hayati ipuçları sunmaktadır. Ayrıca diyafram açıklığı (*f-stop*), ISO hassasiyeti ve pozlama süresi gibi teknik ayarları da belgeleyen bu sistemin sunduğu en kritik kanıt, cihazın GPS özelliğinin açık olması durumunda görselin tam coğrafi koordinatlarını (enlem/boylam) kaydederek, görüntünün gerçekten iddia edilen konumda çekilip çekilmediğini kesin bir şekilde ortaya koymasıdır.

Şekil 4.2.2 *EXIF verileri*

Dijital dedektiflik sürecinde karşılaşılan en büyük teknik engel, X (eski adıyla Twitter), Facebook, Instagram ve WhatsApp gibi yaygın sosyal medya platformlarının uyguladığı katı veri temizleme politikalarıdır. Bu platformlar, hem kullanıcıların hassas GPS konum bilgilerini ifşa olmaktan koruyarak gizliliği sağlamak hem de sunucu maliyetlerini düşürüp yükleme hızını artırmak amacıyla dosya boyutunu küçültmek istemektedir. Bu iki stratejik nedenden

dolayı sosyal medyaya yüklenen bir fotoğrafın arka planındaki değerli EXIF verileri sistem tarafından otomatik olarak silinmektedir; dolayısıyla bu mecralardan indirilen bir görselin dijital kimliğine bakarak çekildiği tarihi veya konumu tespit etmeye çalışmak, veriler paylaşım anında yok edildiği için genellikle sonuçsuz kalan bir çabadır.

Şekil 4.2.3 *Yapay zekâ ile oluşturulmuş görsel*

Sosyal medya platformlarının aksine, EXIF verisinin silinmediği ve güvenilir bir teyit aracı olarak kullanılabildiği belirli güvenli alanlar hala mevcuttur. Örneğin, bir fotoğrafın sıkıştırılmadan orijinal boyutuyla e-posta üzerinden gönderilmesi veya Google Drive ve Dropbox gibi dosya paylaşım servislerine yüklenmesi durumunda, dosyanın dijital kimliği genellikle bozulmadan kalır. Buna ek olarak, görüntüye doğrudan çekildiği kameradan, telefondan veya hafıza kartından erişildiğinde de veri kaybı yaşanmaz. Ayrıca görsel kalitesini korumayı öncelik haline getiren bazı profesyonel haber ajansları veya fotoğraf portfolyo siteleri, dosyaların meta verilerini kasıtlı olarak tutabilir.

Bir görselin arka planındaki gizli EXIF verilerini ortaya çıkarmak ve

analiz etmek için hem pratik çevrimiçi araçlardan hem de profesyonel yazılımlardan yararlanılmaktadır. İnternet tabanlı çözümler arasında, dosya yükleyerek veya sadece görselin bağlantı adresini girerek saniyeler içinde detaylı rapor sunan Jeffrey's Image Metadata Viewer en hızlı ve popüler seçeneklerden biriyken; FotoForensics platformu, EXIF verilerini okumanın ötesine geçerek görsel üzerinde düzenleme yapılıp yapılmadığını anlamayı sağlayan hata seviyesi analizi (ELA) gibi ek özellikler sunmaktadır. Daha profesyonel ve yerleşik bir inceleme için ise Adobe Photoshop veya Lightroom gibi yazılımların "dosya bilgisi" menüleri kullanılırken; çok sayıda formatı destekleyen ve komut satırı üzerinden çalışan son derece güçlü ExifTool aracı da kullanılmaktadır. Ancak bu teknik süreçte unutulmaması gereken hayati bir kural vardır: Bir fotoğrafın EXIF verisine sahip olması onun kesinlikle orijinal olduğunu kanıtlamaz; çünkü bu veriler özel yazılımlarla kolayca manipüle edilebilir veya tamamen silinebilir. Dolayısıyla EXIF verileri nihai bir kanıt değil, teyit sürecinin başlangıç noktası olarak kabul edilmeli ve elde edilen tarih veya konum bilgileri, mutlaka hava durumu raporları ya da uydu görüntüleri gibi diğer açık kaynak verileriyle çapraz kontrolden geçirilmelidir.

Mobil Dedektiflik: Her Yerde Teyit

Dezenformasyonla mücadelenin genellikle büyük ekranlı bilgisayarlar başında yürütülen bir faaliyet olduğu sanılsa da gerçek hayatta yalan haberle çoğunlukla bir otobüs yolculuğunda veya kafe kuyruğundayken, elimizde sadece bir telefon varken karşılaşmaktayız. Bilgisayarın işlem gücünden yoksun olduğumuz bu anlarda devreye giren "Mobil Doğrulama" sürecindeki en büyük teknik engel, mobil tarayıcıların görsel arama butonlarını gizlemesidir; ancak bu sorun, Chrome veya Safari ayarlarından "Masaüstü Sitesi İste" seçeneği aktif edilerek kolayca aşılabilmektedir. Chrome veya Safari'de görselin olduğu sayfayı açarak ayarlar menüsünden (üç nokta veya 'Aa' ikonu)

📌 **ÖRNEK SENARYO:** “SAVAŞIN ORTASINDAKİ ÇOCUK”

Senaryo: Sosyal medyada, elinde oyuncak ayısıyla yıkıntılar arasında ağlayan, son derece dramatik bir çocuk fotoğrafı hızla yayıldı ve viral oldu. Gönderinin altındaki açıklama net ve çarpıcıydı: "Gazze'de bu sabah." Fotoğraf kısa sürede binlerce beğenildi ve kullanıcılar tarafından yoğun duygusal tepkilerle paylaşıldı. Görselin yarattığı duygusal etki, eleştirel düşüncenin önüne geçti.

1. Adım: Detaylı Görsel İnceleme: Görselin duygusal etkisi bir kenara bırakılarak teknik detaylara odaklanılır; zira YZ araçları insan anatomisi ve arka plan kurgusunda hala belirgin hatalar yapmaktadır. Görselde çocuğun elinde standart 5 parmak yerine 4 parmak olduğu ve bunların gerçek dışı şekilde büküldüğü ve arka plandaki duvar dokusunda YZ’nın ürettiği anlamsız metin benzeri semboller görselin deepfake olabileceğine dair güçlü kanıtlardır.

2. Adım: Tersine Görsel Arama ve Kaynak Tespiti: Görselin internetteki geçmişini ve kaynağını belirlemek için Yandex Images veya Google Lens gibi araçlarla tersine görsel aranır. YZ araçları her seferinde benzersiz piksellere sahip yeni görüntüler ürettiği için arama motorları fotoğrafın aynısını bulamasa da görseldeki ışık, kompozisyon ve atmosfer ile benzeyen binlerce içerik tespit edebilir. Bu görsellerin çoğunluğunun Midjourney veya DALL-E gibi yapay zekâ üretim araçlarının kullanıcı forumlarında paylaşıldığının görülmesi, görselin YZ kaynaklı olduğu tezini güçlendirir.

3. Adım: Niyet ve Bağlamın Değerlendirilmesi: İçeriğin kim tarafından ve hangi amaçla dolaşıma sokulduğunu anlamak için SIFT metodu (*source/kaynak takibi*) uygulanmalıdır. Bu aşamada görseli paylaşan orijinal hesaba gidilerek profil ve geçmiş gönderileri analiz edilir. Bu senaryoda, hesabı incelediğimizde kullanıcının kendisini açıkça “yapay zekâ sanatı meraklısı” olarak tanımladığı ve profilinin benzer YZ ürünü görsellerden oluştuğu görülmektedir. Kullanıcı, bu görseli aslında bir "sanat eseri" veya "dijital illüstrasyon" olarak paylaşmış, gerçek bir olaya ait olduğu iddiasında bulunmamıştır. Ancak görsel, daha sonra kötü niyetli hesaplar tarafından orijinal kaynağından koparılarak; kırpılmış, yanlış bağlam eklenerek ("Gazze'de bu sabah" gibi) ve kaynağı gizlenmiştir. Sonuçta görselin kendisi bir deepfake iken (YZ ürünü), kamuoyuna yayılma biçimi cheapfake yöntemidir. Duygusal içeriğin deepfake teknolojisiyle üretilmesi ve cheapfake yöntemleriyle (basit bağlam manipülasyonu) yayılması, dezenformasyonun etkisini katlanarak artırmıştır.

"masaüstü sitesi iste" (*request desktop site*) seçeneğini işaretleyerek bu seçeneği aktif hale getirebilirsiniz. Böylece arama motorlarının kamera ikonuna erişim sağlayabilir ve görsel yükleyerek arama yapabilirsiniz.

Profesyonel bir doğrulama uzmanının cebindeki bu donanımı tamamlayan üç temel araç vardır. İlk sırada, bir fotoğrafı cihazınıza indirmeye gerek kalmadan sadece üzerine basılı tutarak nesneleri, mekanları ve metinleri saniyeler içinde tanımlamanızı sağlayan Google Lens gelir. İkinci araç, tek bir fotoğrafı aynı anda Google, Yandex ve Bing gibi çoklu veri tabanlarında tararatak zaman kazandıran Search By Image (veya Reversee) uygulamalarıdır. Listeyi tamamlayan üçüncü ve en stratejik araç ise; özellikle YouTube ve X (Twitter) video bağlantılarını kullanarak görüntüleri karelerine (*keyframes*) ayıran ve mobil video doğrulamada teyitçilere büyük güç katan InVID & WeVerify uygulamasıdır.

TEMEL ÇIKARIMLAR

"Görmek inanmaktır" sözü dijital çağda en büyük yanılgıya dönüşmüştür. Beynimiz görsellere inanmaya programlıdır, ancak fotoğraflar bağlamından koparılabilir veya yapay zekâ ile üretilebilir. Bu bölüm, görselin teknik olarak gerçek olsa bile bağlamının (tarih ve yer) sahte olabileceğini ve bunu tespit etmek için "tersine görsel arama" araçlarının kullanılması gerektiğini açıklar.

Temel Kavramlar ve Mekanizmalar

Tersine Görsel Arama (*Reverse Image Search*): Google Lens, TinEye veya Yandex kullanarak, kelimelerle değil görselin kendisiyle arama yapmaktır. Bu mekanizma, fotoğrafın daha önce nerede yayınlandığını bularak bağlam manipülasyonunu (eski bir fotoyu yeni gibi sunma) ifşa eder

Cheapfake vs. Deepfake: Cheapfake, teknik bilgi gerektirmeyen "yanlış etiketleme" veya basit kırpmalardır ve dezenformasyonun %95'ini oluşturur. Deepfake ise yapay zekâ ile üretilen, hiç var olmamış görüntülerdir.

Sıfır Sonuç Paradoksu: Bir insan yüzü aratıldığında hiçbir sonuç çıkmıyorsa, bu o kişinin "benzersiz" olduğunu değil, muhtemelen yapay zekâ (GANs) tarafından saniyeler önce üretildiğini ve dijital ayak izi olmayan sahte bir yüz olduğunu gösterir.

Ayna Hilesi: Manipülatörler, algoritmaları şaşırtmak için fotoğrafı yatay olarak çevirirler (sağ el sol el olur). Eğer sonuç bulamazsanız, fotoğrafı telefonunuzun editöründe "aynala/çevir" yapıp tekrar aratın. Orijinali o zaman bulabilirsiniz.

Detay Avcılığı: Fotoğrafın tamamını aratmak sonuç vermiyorsa, Bing'in veya Yandex'in "kırpma" özelliğini kullanın. Arka plandaki o küçük tabelayı, duvardaki saati veya raftaki logoyu aratın.

4.2. KENDİNİZİ TEST EDİN

Soru 1: Bir insan yüzü fotoğrafını arama motorlarında arattığınızda "hiçbir sonuç bulunamadı" (sıfır sonuç paradoksu) uyarısı alıyorsanız, bu durum neyin işareti olabilir?

A) Arama motorunun bozuk olabileceğini

B) Yüzün YZ tarafından üretilmiş olabileceği

C) İnternet bağlantısının kesilmiş olabileceğini

Soru 2: YZ ile üretilen sahte insan fotoğraflarını (*deepfake*) ayırt etmek için insan gözüyle bakıldığında en sık görülen özgün hata hangisidir?

A) Saç renginin çok parlak olması

B) Ellerdeki parmak sayısının yanlış veya şekilsiz olması

C) Kıyafetlerin çok şık, çok renkli olması

D) Arka planın çok net, berrak olması

Soru 3: Sosyal medya platformlarından indirilen fotoğrafların "EXIF" (çekildiği tarih, yer, cihaz bilgisi) verilerine neden güvenilemez?

A) Platformlar gizlilik ve hız nedenleriyle bu verileri siler.

B) EXIF verileri çok karmaşık, okunulmazdır.

C) Telefonlar bu verileri kaydetmezler.

4.2. MERAKLISINA EK KAYNAKLAR

Harding, L. (2022). "The Ghost of Kyiv: How a Myth Was Born". The Guardian.

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., vd. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*.

Silverman, C. (Der.). (2014). Verification handbook: A definitive guide to verifying digital content for emergency coverage. European Journalism Centre.

Şahin, Z. (2024, 13 Mayıs). *Teyit sözlük: Tersine görsel arama nedir?* Teyit. https://teyit.org/teyitpedia/teyit-sozluk-tersine-gorsel-arama-nedir

Urbani, S. (2019). *First Draft's essential guide to verifying online information*. First Draft.

Video Doğrulama: Hareketli Görüntüleri Analiz Etme Yöntemleri

Dezenformasyon çağında fotoğraf manipülasyonu gerçeğin yalnızca donmuş bir anını çarpıtırken; video manipülasyonu zamanın akışını, bağlamı ve dolayısıyla izleyicinin deneyimlediği duyguyu bükerek statik bir görselin asla ulaşamayacağı çok daha derin ve yıkıcı bir etki yaratmaktadır. Bireyin rasyonel karar alma süreçlerini atlayarak doğrudan duygusal merkezleri hedef aldığı için "duygusal nükleer silahlar" olarak tanımlanan videoların bu olağanüstü gücü, temelde beynimizdeki "Ayna Nöronlar" mekanizmasına dayanır. Beynimiz, bir başkasının eylemini, duygusunu veya durumunu gözlemlediğinde, bu eylemi sanki kendimiz yapıyormuşuz gibi içsel olarak simüle eden bu özel nöron gruplarını aktive eder. Ağlayan, gülen, korkan veya öfkelenen bir insan figürünü içeren bir video izlediğimizde, beynimizdeki ilgili motor ve duygu merkezleri tetiklenir. Bu biyolojik simülasyon, anlık ve derin bir empati bağı kurulmasına neden olur. Bu güçlü biyolojik bağ, rasyonel ve analitik düşünme sistemimizi, bir başka deyişle Nobel ödüllü psikolog Daniel Kahneman'ın terminolojisiyle sistem 2'yi hızla devre dışı bırakır. Video, izleyiciye bir "kanıt" sunar: "Gözümle gördüm, hareket ediyordu, gerçek olmalı." Bu güçlü, ilkel güven hissi, eleştirel şüphe mekanizmasını ve mantıksal sorgulamayı anında öldürür. İzleyici, içeriğin doğruluğunu sorgulamaktan çok, o içeriğin yarattığı duygusal tepkiye odaklanır.

Video manipülasyonu, evdeki basit bir bilgisayarla yapılabilen kesme-biçme işlemlerinden, ileri düzey yapay zekâ mühendisliğine kadar uzanan geniş ve tehlikeli bir yelpazedir. Bu yelpazenin bir ucunda, yüksek teknoloji gerektirmeyen ancak etkisi yıkıcı olabilen ucuz sahtecilik "cheapfake" yer alır. Bu yöntemle videoların bağlamı değiştirilmekte, görüntülerin hızıyla oynanmakta veya eski bir olay güncelmiş gibi servis edilerek kitleler basit

tekniklerle kolayca kandırılabilmektedir.

Yelpazenin diğer ve çok daha karanlık ucunda ise derin sahtecilik "deepfake" bulunur; burada yapay zekâ ve makine öğrenimi algoritmaları devreye girerek bir kişinin yüzünü veya sesini kusursuzca taklit etmekte, kişiye asla söylemediği sözleri söyleterek toplumsal güveni kökünden sarsan, ikna ediciliği son derece yüksek bir tehdit oluşturmaktadır.

Video Manipülasyon Teknikleri

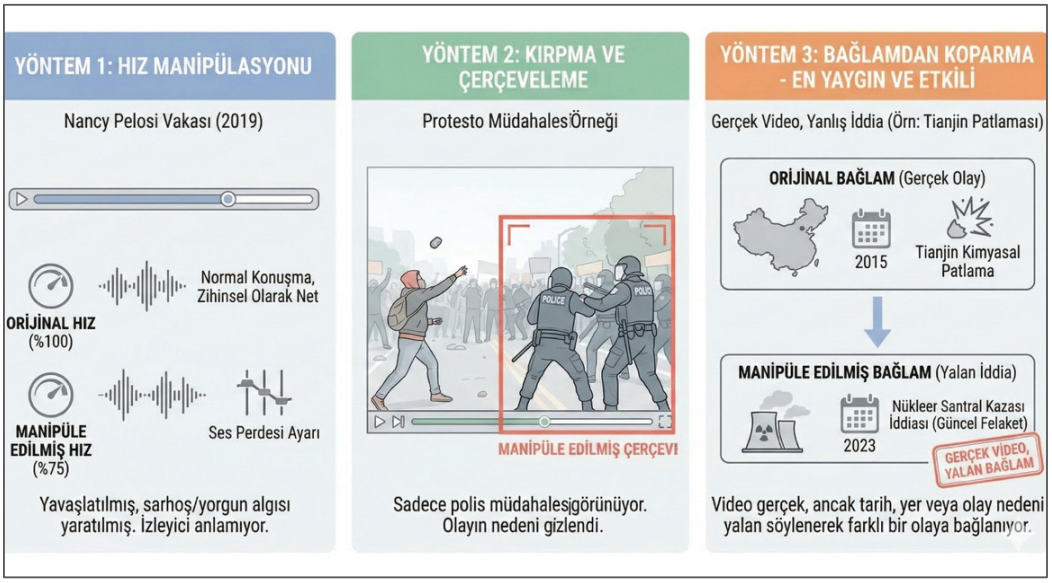
Dijital çağda video içerikleri üzerinden yapılan manipülasyonlar, gerçeği algılama biçimimizi tehdit eden en kritik unsurlar arasında yer almaktadır. Bu tehdidi doğru biçimde çözümleyebilmek ve etkili savunma mekanizmaları geliştirebilmek için, kullanılan manipülasyon tekniklerini iki temel kategori altında ele almak gerekir. Bu sınıflandırma, bir videonun doğruluğunu değerlendirmek için başvuracağımız araç ve yöntemleri doğrudan belirler.

Cheapfake

İnternet ortamında karşımıza çıkan ve kitleleri derinden etkileyen video manipülasyonlarının %95'inden fazlasını oluşturan ucuz sahtecilik (*cheapfake*) kategorisi, sanılanın aksine karmaşık nöral ağlara, yapay zekaya veya yüksek işlem gücüne sahip süper bilgisayarlara ihtiyaç duymamaktadır. Adobe Premiere gibi profesyonel yazılımların yanı sıra CapCut, TikTok veya Instagram gibi herkesin cebinde bulunan basit mobil uygulamalarla dahi saniyeler içinde üretilebilen bu içerikler; teknik mükemmellikten ziyade üretimdeki hız ve kolaylığa dayanmakta, izleyicinin algısal zaaflarını ve bağlamı sorgulamama eğilimini hedef alarak dezenformasyonun hızla yayılmasına neden olmaktadır.

Cheapfake yöntemlerinden biri olan hız manipülasyonu, videonun oynatma hızıyla kasten oynanarak kişinin fiziksel veya zihinsel durumu

hakkında yanıltıcı bir algı yaratılmasını hedefler. Bu tekniğin yıkıcı etkisi, 2019 yılında ABD Temsilciler Meclisi Başkanı Nancy Pelosi'nin hedef alındığı vakada tüm çıplaklığıyla görülmüştür. Manipülatörler, videonun hızını orijinalin %75'ine düşürürken, yavaşlatma sırasında sesin doğal olarak kalınlaşmasını engelleyen profesyonel bir "ses perdesi ayarı" (*pitch correction*) kullanmışlardır. İzleyicinin teknik müdahaleyi fark etmesini imkânsız kılan bu ince ayar sonucunda Pelosi; kelimeleri uzatarak konuşan, sarhoş veya zihinsel yetilerini kaybetmiş biri gibi gösterilmiş ve milyonlarca kişi bu basit ama etkili kurguya inandırılmıştır.



Şekil 4.3.1 *Başlıca cheapfake yöntemleri*

Cheapfake yöntemlerinin en yaygın olanlarından kırpma ve çerçeveleme, videonun orijinal kadrajını bilinçli olarak daraltıp gerçeğin bütününü izleyicinin gözünden saklama sanatıdır. Bu teknikte manipülatör, olay örgüsünün sadece kendi anlatısını destekleyen kısmını gösterip geri kalanını karanlıkta bırakır. Örneğin bir protesto videosunda, göstericinin polise molotof kokteyli fırlattığı an kadrajın dışında bırakılıp sadece polisin müdahalesi

gösterildiğinde; olayın neden kısmı silinerek izleyici tek taraflı ve yönlendirilmiş bir polis şiddeti algısına hapsedilmektedir.

Cheapfake yöntemleri arasında en yaygın ve tespit edilmesi en zor olanı bağlamdan koparmadır; çünkü bu manipülasyon türünde videonun kendisi teknik olarak %100 gerçektir ve üzerinde hiçbir dijital oynama yapılmamıştır. Manipülatörler, geçmişte yaşanmış gerçek bir olayı arşivden çıkarıp tarihini, mekanını veya sebebini değiştirerek sanki şu an yaşanıyormuş gibi sunmaktadır. Örneğin, 2015 yılında Çin'in Tianjin kentinde yaşanan devasa bir kimyasal patlama görüntüsü, yıllar sonra "Nükleer santralde kaza oldu" başlığıyla paylaşılabilmekte veya geçmişteki kalabalık bir siyasi miting videosu, güncel bir adayın mitingiymiş gibi servis edilerek kitleler kandırılabilmektedir. Gözümüzün gördüğü görüntü ne kadar gerçek olursa olsun, videonun altına yazılan etiketin yalan olması, gerçeği tamamen tersyüz etmeye yetmektedir.

Deepfake

Video manipülasyonunun en gelişmiş formu olan ve teknolojinin sınırlarını zorlayan deepfake, basit kurgu yöntemlerine dayanan cheapfake'in aksine yüksek mühendislik ve makine öğrenimi yetenekleri gerektirmektedir. Temelinde GANs (*Generative Adversarial Networks*-Çekişmeli Üretici Ağlar) adı verilen karmaşık nöral ağların yattığı bu teknolojide, görüntüler üzerinde basit bir kesme-biçme veya düzenleme işlemi yapılmamakta; bunun yerine mevcut piksellerin üzerine yapay zekâ tarafından eğitilmiş modeller aracılığıyla sentetik veriler işlenerek video, adeta dijital bir dokuma gibi piksel piksel yeniden üretilmektedir.

Deepfake teknolojisinin en bilinen yüzü olan yüz değiştirme tekniği, bir kişinin yüzünü başka bir bedene kusursuzca monte ederek o kişiyi hiç bulunmadığı ortamlarda veya asla yapmadığı eylemlerin içindeymiş gibi

gösterebilmektedir. Ancak manipülasyonun daha sinsi boyutu, kişinin yüzünün ve sesinin korunduğu fakat ağız hareketlerinin yapay zekâ ile değiştirildiği dudak senkronizasyonu (*lip-sync*) yönteminde gizlidir; bu teknikte hedef kişinin dudakları milimetrik hassasiyetle manipüle edilerek, siyasi liderlere veya tanınmış kişilere aslında hiç söylemedikleri skandal sözler sanki kendi ağızlarından çıkmışçasına söyletilmektedir.

📌 ÖRNEK VAKA

Deepfake teknolojisinin yarattığı tehlikeyi ve dezenformasyonun yıkıcı potansiyelini anlamak için, Ukrayna-Rusya savaşının ilk günlerinde ortaya çıkan ve tüm dünyada yankı uyandıran sahte Zelenski videosuna bakmak yeterlidir. Ukrayna-Rusya savaşının ilk günlerinde, dezenformasyonun yıkıcı potansiyelini gösteren bir deepfake video ortaya çıktı. Bu manipülasyonda, Ukrayna Devlet Başkanı Zelenski'nin askerlerine "silah bırakın ve teslim olun" çağrısı yaptığı iddia edilmiş; ancak dikkatli bir analiz, videonun amatör bir yapay zekâ ürünü olduğunu kısa sürede ortaya çıkarmıştır. Her ne kadar videodaki yüz hatları gerçeğe yakın dursa da Zelenski'nin vücut hareketlerinin bir insan doğallığından uzak şekilde aşırı donuk ve robotik olması, yüzündeki gölgelerin ortam ışığıyla uyuşmaması ve sesindeki mekanik, monoton tınılar, bu görüntünün dijital bir sahtecilik olduğunu kanıtlamaya yetmiştir.

Vidoyu izlemek için:
🔗 https://www.youtube.com/watch?v=jIoY8RQglvY

Deepfake teknolojisi her geçen gün evrim geçirip sınırları zorladığı için, bu sofistike yalanları yakalayacak dijital tespit mekanizmaları da sürekli bir güncelleme yarışı içinde olmak zorundadır. Ancak manipülasyonların büyük çoğunluğunu oluşturan cheapfake türü içerikleri tespit etmek için karmaşık yazılımlara veya ileri teknolojiye ihtiyaç duyulmamaktadır; bu basit kurguları çürütmek ve gerçeği görmek, çoğunlukla sadece eleştirel düşünme becerisini

devreye sokmak ve videonun bağlamını basitçe kontrol etmekle mümkündür

Şüpheli Videoları Sorgulama Rehberi

Dijital çağda bir bilginin doğruluğunu sorgulamak ve teyit etmek, artık yalnızca gazetecilerin değil, her vatandaşın sahip olması gereken temel bir beceriye dönüşmüştür. Özellikle video ve ses içeriklerinde kullanılan manipülasyon teknikleri giderek karmaşıklaştıkça, doğrulama yaklaşımlarımızı da daha derinlikli ve çok katmanlı hale getirmek kaçınılmazdır.

Fotoğraf İzinden Video Doğrulama

Videoları doğrulamanın temel ve değişmez ilkesi, arama motorlarının videoları "izleyemediği" ancak fotoğrafları "görebildiği" gerçeğine dayanır; zira teknik olarak her video, saniyede 24 veya 60 kare hızla akan hareketsiz fotoğrafların oluşturduğu bir hareket illüzyonudur. Bu akışı bir bütün olarak aratmak mümkün olmadığından, videoyu parçalarına ayırıp incelememiz gerekmektedir. Ancak binlerce kareyle tek tek uğraşmak zaman kaybı olacağından, başarılı bir doğrulamanın sırrı "anahtar kare" (*keyframe*) seçiminde gizlidir. Sahnenin en net olduğu, ışığın parladığı veya yüzlerin, plakaların ve logoların belirginleştiği anları seçip tersine görsel arama motorlarına sunduğumuzda; bulanık karelerin yarattığı kirlilikten kurtularak videonun gerçek kaynağına, tarihine ve bağlamına hızla ulaşmamız mümkün olmaktadır.

InVID ile Otomatik Video Analizi

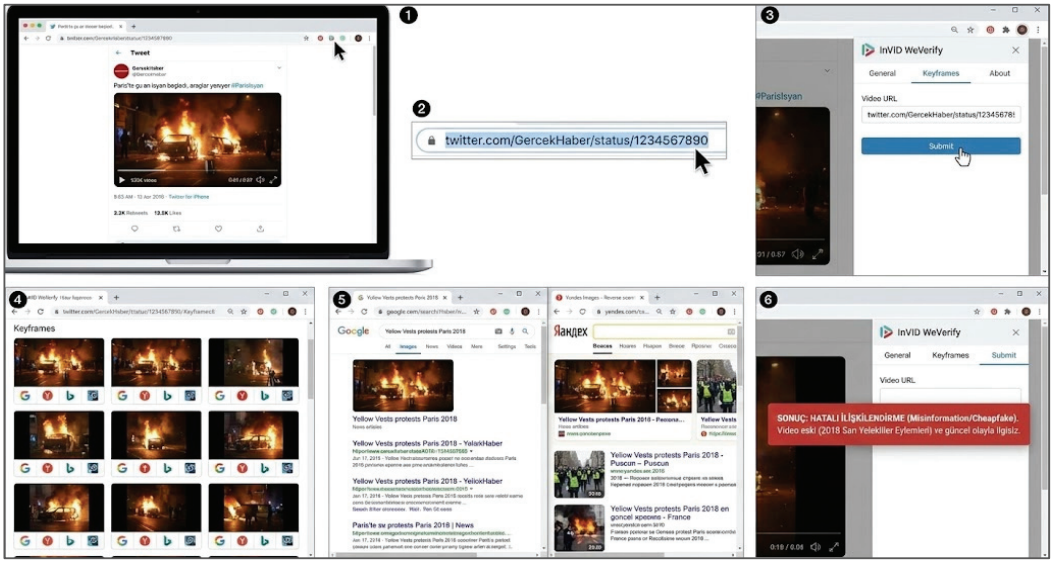
InVID & WeVerify tarayıcı eklentisi; Avrupa Birliği'nin "Horizon 2020" programı kapsamında finanse edilerek özellikle gazeteciler, araştırmacılar ve doğrulama kurumları için geliştirilmiş profesyonel bir teyit aracıdır. Chrome ve Firefox gibi tarayıcılara entegre olarak çalışan bu güçlü yazılım, karmaşık video analiz süreçlerini herkes için erişilebilir hale getirmektedir.

Bir kriz anında ya da hızla gelişen toplumsal olaylar sırasında karşımıza çıkan şüpheli bir videonun doğrulanması, belirli ve sistematik adımlar izlenerek yapılır. Örneğin X platformunda "Paris'te şu an isyan başladı, araçlar yanıyor" başlığıyla paylaşılan, yanan arabaları gösteren bir video ile karşılaştığınızı düşünün. İlk adım, doğrulama için gerekli teknik altyapıyı kurmaktır. Bunun için kullanılan tarayıcıya (Chrome veya Firefox) InVID WeVerify eklentisi yüklenir. Ardından şüpheli videonun doğrudan bağlantı adresi (URL) kopyalanır. Eklenti aktive edildikten sonra anahtar kareler (*keyframes*) sekmesine girilir, kopyalanan bağlantı ilgili alana yapıştırılır ve gönderim yapılır. Bu noktada InVID aracı videoyu otomatik olarak analiz eder; zaman çizelgesini tarayarak videonun en net, ayırt edici ve bilgi taşıma potansiyeli yüksek 10 ila 20 anahtar karesini yüksek çözünürlüklü görseller halinde ayıklar. Ayıklanan bu karelerin her birinin altında Google, Yandex, Bing ve TinEye gibi farklı tersine görsel arama motorlarının ikonları belirir ve tek tıklamayla bu görseller eş zamanlı olarak farklı platformlarda aranabilir. Özellikle birden fazla arama motoru kullanmak kritik önemdedir; zira bazı motorlar (örneğin Yandex) eski veya belirli coğrafyalara ait içerikleri bulmada daha başarılı olabilir. Son aşamada elde edilen arama sonuçları dikkatle değerlendirilir: Eğer görseller daha önce 2016 yapımı bir filmde, 2018'deki Sarı Yelekliler protestolarında ya da başka bir ülkede yaşanmış eski bir olayda kullanılmışsa, video "hatalı ilişkilendirme" kategorisine girer; bir başka deyişle görüntü gerçek olsa bile iddia edilen güncel olayla ilgili değildir ve yanlış bilgi tespit edilmiş olur. Buna karşılık sonuçlar yeni tarihli ve paylaşılan iddia ile tutarlıysa, video büyük olasılıkla gerçektir; ancak nihai teyit için coğrafi konum doğrulaması gibi ek adımların mutlaka uygulanması gerekir.

InVID, teyitçilerin işini kolaylaştıran bir dizi ek araç da sunar. YouTube videolarının otomatik olarak oluşturulan ve genellikle en iyi görseli içeren kapak fotoğrafını en yüksek çözünürlükte indirip doğrudan aratmanıza

olanak tanır. X platformunun karmaşık tarih ve konum filtrelerini basit bir arayüzle kullanarak bir olayın ilk kaynağına hızla ulaşabilirsiniz. Bu, bir olayın ilk defa ne zaman ve nerede paylaşıldığını bulmak için kritiktir. Dahası, videodaki bulanık bir tabelayı veya plakayı pikselleri bozmadan okumanızı sağlayan "dijital büyüteç" özelliğinin yanı sıra, dosyanın teknik kimliği olan metadata verilerini analiz ederek videonun ne zaman ve hangi cihazla üretildiğini ortaya çıkarmanız mümkündür.

Görsel Kanıtlar: Yapay Zekanın Özgün Hatalarını Yakalamak



Şekil 4.3.2 *InVID ile analiz örneği*

Eski tarihli veya bağlamından koparılmış videoları InVID gibi araçlarla doğrulamak nispeten kolay bir süreçken; güncel olaylarda karşımıza çıkan ve konuşan insanları içeren yeni videolar, bizi deepfake, derin sahtecilik şüphesiyle yüzleşmeye zorlar. Yapay zekâ teknolojisi her ne kadar hızla gelişip sınırları zorlasa da insan biyolojisini ve fizik kurallarını taklit etme konusunda henüz kusursuz değildir. Dikkatli bir göz; düzensiz göz kırpma reflekslerinden ağız ve diş yapısındaki bozulmalara, aksesuarların doğal olmayan

hareketinden ışık ve gölge uyumsuzluklarına kadar dijital dünyanın bıraktığı biyolojik ve fiziksel parmak izlerini takip ederek bu sahteciliği ifşa edebilir.

Deepfake videolar, her ne kadar giderek daha gerçekçi görünse de insan biyolojisini kusursuz biçimde taklit edebilmiş değildir. Bu tür videolarda en sık karşılaşılan ipuçlarından biri göz kırpma davranışıdır: Gerçek insanlar düzenli bir ritimle, dakikada ortalama 15–20 kez göz kırparken, deepfake'lerde bu hareket ya gereğinden fazla hızlı ve tik benzeri ya da tam tersine yavaş, düzensiz ve doğallıktan uzaktır. Bir diğer dikkat çekici zayıflık ağız ve diş bölgesinde ortaya çıkar. Yapay zekâ, dişlerin karmaşık yapısını ve ağız içindeki detayları üretmekte zorlanır; bu nedenle dişler çoğu zaman tek parça beyaz bir yüzey gibi görünür ya da yamuk ve orantısızdır. Konuşma sırasında dudak kenarlarında ve ağız çevresinde bulanıklaşmalar ya da kesintili hareketler de sıkça fark edilir. Daha ileri düzey analizlerde ise kan akışı ve nabız izleri önemli bir gösterge sunar: Gerçek bir insanın yüzünde kalp atışıyla birlikte deride çok küçük renk değişimleri meydana gelirken, deepfake videolarda yaşayan bir bedene özgü bu mikro hareketler bulunmaz. Bu biyolojik uyumsuzluklar, dikkatli bakıldığında deepfake içerikleri ayırt etmede güçlü ipuçları sağlar.

Yapay zekâ ne kadar gelişirse gelişsin, fizik kurallarını kusursuzca taklit etmekte zorlanır ve dikkatli bir göz için olay mahalinde mutlaka ipuçları bırakır. Örneğin videodaki kişinin gözlükleri veya şapkası, yüz hareketleriyle uyumsuz bir şekilde havada "yüzüyorsa" ya da yüze vuran ışığın yönü ile arka plandaki gölgeler birbirini tutmuyorsa, bu durum kişinin o ortama sonradan monte edildiğinin en belirgin kanıtıdır. Ancak insan gözünün bu detayları yakalamakta yetersiz kaldığı durumlarda nöbeti teknoloji devralır; Deepware Scanner veya Microsoft Video Authenticator gibi dijital araçlar, videodaki piksellerin sıkıştırma izlerini ve geometrik hatalarını tarayarak bize matematiksel bir "sahtelik skoru" sunar ve %100 garanti vermese de yüksek

skorlar şüphelerimizi teyit etmek için güçlü bir dayanak oluşturur.

İşitsel Kanıtlar: Ses Klonlamayı Kulakla Deşifre Etmek

Deepfake teknolojisinin en sinsi ve hızla büyüyen tehdidi, görüntüden ziyade kulaklarımızı hedef alan "audio deepfake" ses klonlama teknolojisidir. Özellikle siyaset ve iş dünyasında itibar suikastlarının yeni silahı haline gelen bu yöntem, ElevenLabs gibi gelişmiş araçlar sayesinde korkutucu bir kolaylığa erişmiştir. Artık bir kişiye ait sadece 30 saniyelik sıradan bir ses kaydını yapay zekaya dinletmek, o kişinin ses tonunu birebir kopyalayarak ona hiç söylemediği sözleri söyletmek için yeterlidir. Bu teknoloji, sadece kitlesel manipülasyon aracı olarak kalmayıp, aynı zamanda telefon üzerinden yürütülen dolandırıcılık faaliyetlerinde de aktif olarak kullanılan tehlikeli bir silaha dönüşmüştür.

👉 DENE

Chrome veya Firefox tarayıcınıza InVID & WeVerify eklentisini kurun. Twitter'da viral olan bir videoyu bu eklenti ile anahtar karelere ayırın ve tek tıkla tersine görsel arama yaparak videonun ilk nerede yayınlandığını bulun.

Deepfake sesler, giderek daha ikna edici hale gelse de insan sesini bütünüyle taklit edebilmiş değildir. Gerçek bir insan konuşurken nefes alır, yutkunur, düşünürken kısa duraksamalar yapar ve “ıı”, “eee”, “şey” gibi küçük tereddütler gösterir; bu kusurlar konuşmayı doğal kılar. Yapay zekâ tarafından üretilen sesler ise çoğu zaman fazla pürüzsüz, kesintisiz ve nefessizdir. İnsan konuşmasına özgü bu küçük düzensizlikleri üretmekte zorlanırlar. Ses kayıtları profesyonel bir düzenleme programında (Audacity, Adobe Audition gibi) incelendiğinde bu yapaylık daha net ortaya çıkar: Montajlanmış veya üretilmiş seslerde konuşma kesildiğinde arka plan gürültüsü de aniden

kaybolur ya da yapay biçimde tekrar ederken, gerçek kayıtlarda arka plan sesi genellikle süreklidir. Ayrıca klonlanmış seslerde, özellikle tiz frekanslarda, hafif metalik veya robotik bir tını da hissedilebilir. Bu akustik tutarsızlıklar, deepfake sesleri ayırt etmek için önemli ipuçları sunar.

Video Analizinin Ötesinde

Şimdiye kadar videonun içeriğine odaklanıp kimin konuştuğunu veya görüntünün montajlanıp montajlanmadığını teknik olarak çözdük; ancak bu, dijital dedektifliğin sadece ilk ve en temel adımıydı. Bir videonun teknik olarak "gerçek" olması, bir başka deyişle üzerinde dijital bir oynama yapılmamış olması, onun anlattığı hikâyenin de doğru olduğunun garantisi değildir. Dedektifliğin en kritik ve zorlu virajı tam da burada başlar: Elimizdeki materyali iddia edilen olay örgüsünün içine yerleştirmek. Zira bir video teknik açıdan kusursuz ve gerçek olsa bile, tamamen yanlış bir bağlamda, bambaşka bir zaman veya mekânda çekilmiş olabilir. Gerçek bir video tamamen yanlış bir bağlamda veya yanlış bir iddiayı desteklemek için kullanılıyor olabilir.

Videonun sahte olmadığını teknik olarak kanıtlasak bile, dijital dedektifliğin en kritik sınavı videoyu doğru olay örgüsünün içine, doğru mekân ve zamana yerleştirmektir. Örneğin, sosyal medyada "İzmir'de sel felaketi" etiketiyle paylaşılan gerçek bir video, aslında yıllar önce Atina'da yaşanmış bir olaya ait olabilir; bu yüzden videonun içindeki bir dağ silüetinden sokak tabelasına, hatta asfaltın dokusuna kadar her detayı inceleyerek jeolokasyon bir başka deyişle coğrafi konum tespiti yapmak şarttır. Mekânsal doğrulama kadar kritik olan diğer soru ise "Ne zaman?" sorusudur; çünkü "son dakika" diye sunulan görüntüler aslında arşivlerden çıkarılmış olabilir. Bu noktada insanların kıyafetleri, ağaçların yaprakları, kar ve buz varlığı gibi mevsimsel ipuçlarını gözlemlemenin ötesine geçerek, güneşin konumu ve gölge boylarını analiz eden bilimsel yöntemlerle videonun çekildiği tam saat ve tarih

hesaplanarak hava durumu kayıtlarıyla doğrulanabilir.

TEMEL ÇIKARIMLAR

Videolar, ayna nöronlar sayesinde rasyonel düşünceyi (sistem 2) devre dışı bırakıp doğrudan duygusal tepkiyi (sistem 1) tetikler. Bu bölüm, videoların bir bütün olarak aratılamayacağını, bu yüzden onları karelere ayırarak incelemek gerektiğini ve yapay zekâ, deepfake videolarının biyolojik hatalarını nasıl yakalayacağımızı öğretir.

Temel Kavramlar ve Mekanizmalar

InVID & WeVerify: Videoları en net "anahtar karelerine" (*keyframes*) ayıran ve bu kareleri tersine arama motorlarında taratan profesyonel tarayıcı eklentisidir. Video doğrulamanın temel aracıdır.

YZ'ya Özgü Hatalar: YZ henüz insan biyolojisini kusursuz taklit edemez. Deepfake videolarda düzensiz göz kırpma, nefes almama, diş yapısındaki bozukluklar ve "yüzen aksesuarlar" (gözlük, küpe simetrisi) sahteliği ele veren hatalardır.

Ses Klonlama (*Audio Deepfake*): Kişinin sesinin yapay zekâ ile taklit edilmesidir. "Nefessiz konuşma", arka plan gürültüsünün aniden kesilmesi ve aşırı akıcılık, sahte sesin temel göstergeleridir.

4.3. KENDİNİZİ TEST EDİN

Soru 1: InVID & WeVerify aracı, şüpheli videoları doğrulamak için temel olarak hangi teknik yöntemi kullanır?

A) Videoyu doğrulamaz, otomatik olarak siler.

B) Videoyu anahtar karelere ayırarak tersine görsel arama yapar.

C) Videoyu çeken kişinin kimlik numarasını bulma tekniği kullanır

D) Videodaki sesleri metne çevirerek, kontrol eder.

Soru 2: Bir ses kaydının "ses klonlama" ürünü olduğundan şüpheleniyorsanız, ilk olarak neye dikkat etmelisiniz?

A) Sesin yüksekliği ve hangi dil de olduğu

B) Konuşmanın içeriği, neyi anlattığı

C) Nefes alış, duraksama ve arka plan sesi

Soru 3: İnternette dolaşan video manipülasyonlarının en yaygın türü hangisidir?

A) Deepfake (Yüz değiştirme)

B) Cheapfake / Shallowfake (Bağlamdan koparma, hızlandırma/yavaşlatma)

C) CGI (Bilgisayar efektleri)

4.3. MERAKLISINA EK KAYNAKLAR

Bellingcat. (2021). *Bellingcat's online investigation toolkit*. https://bellingcat.gitbook.io/toolkit

Gregory, S. (2019). *Deepfakes and synthetic media: Updated survey of solutions*. Witness.org.

Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence*. Data & Society.

Villasenor, J. (2019). *Deepfakes, artificial intelligence, and the law*. Brookings Institution.

Mekansal Doğrulama: Jeolokasyon

Dezenformasyon aktörleri, bir görüntü veya videonun algısını değiştirmek istediklerinde genellikle teknik olarak en zahmetsiz yöntem olan bağlam manipülasyonuna başvururlar. Bu kişiler, görselin altına tamamen gerçek dışı bir açıklama ekleyerek veya arşivdeki eski bir olayı yeni yaşanmış gibi sunarak izleyiciyi kolayca yanıltabilirler. Ancak, bir fotoğrafın veya videonun arka planındaki fiziksel gerçekliği, coğrafi detayları değiştirmek, şayet arkalarında devlet destekli devasa bir siber operasyon ya da yüksek bütçeli bir film

📌 ÖRNEK SENARYO

İddia: Sosyal medya platformlarında hızla yayılan bir video, çorak ve kayalık bir arazide ilerleyen zırhlı askeri araçları ve üniformalı personeli göstermektedir. Paylaşımı yapan anonim hesaplar şu iddiayı öne sürer: "ABD, Küba'ya yönelik büyük bir askeri operasyon başlattı!"

İlk Analiz ve Görsel Kanıtlar: Video kare kare incelemeye alınır. Araçların ve üniformaların genel görünümü Amerikan ordusuna benzemektedir. Ancak bir doğrulama analisti, videonun arka planındaki "sessiz tanıklara" odaklanır:

Bitki Örtüsü ve Coğrafya: Görüntüdeki bitki örtüsü incelendiğinde, Küba'nın kıyı şeridinde veya iç kesimlerinde görülmesi beklenen tipik Karayip florasından ziyade, daha çok Güney Amerika'nın iç bölgelerine özgü yüksek rakım kaktüsleri ve bodur çalılar göze çarpar**.**

İnsan Yapımı Yapılar: Videoda saniyelerle görünen bir elektrik direğinin tasarımı ve yol kenarındaki bir hız sınırı tabelasının fontu incelenir. Bu tasarım kodlarının Küba veya ABD standartlarına uymadığı, bölgedeki farklı bir ülkenin altyapı tipolojisini yansıttığı tespit edilir.

Sonuç ve Teyit: Bu coğrafi ve fiziki ipuçları ışığında bir Jeolokasyon (Yer Belirleme) çalışması başlatılır. Analist; Google Earth, Sentinel uydu görüntüleri ve panoramik sokak görünümlerini kullanarak video karesindeki benzersiz yapıları (belirli bir dağ silüeti ve özgün bir kavşak yapısı) harita üzerinde eşleştirir. Yapılan titiz çalışma, videonun iddia edildiği gibi Küba'da çekilmediğini, aslında Kolombiya'nın dağlık bir bölgesinde gerçekleştirilen rutin bir askeri tatbikata ait olduğunu kesin olarak ortaya koyar.

stüdyosu imkanları yoksa neredeyse imkansızdır. Manipülasyonun bu teknik sınıra takıldığı noktada jeolokasyon devreye girer ve değiştirilemeyen mekânsal ipuçlarını analiz ederek görüntünün gerçekte nerede çekildiğini tespit eder.

Jeolokasyon, bir fotoğraf veya video karesi gibi dijital görsellerde yer alan bina cepheleri, sokak tabelaları, bitki örtüsü, gölge açıları, hava durumu işaretleri, araç plakaları ve gün batımı yönü gibi her türlü görsel ipucunu sistematik bir şekilde kullanarak, o görselin dünya üzerindeki tam coğrafi koordinatlarını bir başka deyişle enlem ve boylamını tespit etme sürecidir. Sadece teknik bir dijital beceri olmanın ötesinde, yüksek düzeyde detay odaklı gözlem ve eleştirel düşünme yeteneği gerektiren bu süreç, dijital dedektifliğin ve teyit mekanizmalarının en ileri seviyesini temsil eder. Dezenformasyonla mücadele sürecinde jeolokasyon, bir görüntünün nerede çekildiğini harita üzerinde somut verilerle doğrulayarak gerçeği kesin olarak kanıtlamanın en temel yöntemidir.

Nasıl Yapılır?

Jeolokasyon, bir görselin coğrafi konumunu rastgele harita incelemeleriyle değil, "huni tekniği" adı verilen ve arama alanını sistematik olarak daraltan bilimsel bir yöntemle belirleme sürecidir. Genişten özele doğru ilerleyen bu süreç üç temel aşamadan oluşur: Makro, mezo ve mikro.

Makro Seviye: Hangi Yarım Küre / Hangi Ülke?

Güneşin yönü ve gölgeler, en temel coğrafi ipuçlarından biridir. Bir görselin coğrafi konumunu belirleme sürecinin bu ilk aşamasında, genel atmosfere ve küresel ölçekteki belirleyicilere odaklanılarak arama alanı bir kıta veya ülke grubuna indirgenmeye çalışılır. Bu noktada en temel ve somut coğrafi kanıt, güneş ışığının yönü ve nesnelerin oluşturduğu gölgelerdir. Görseldeki

binaların veya nesnelerin gölgeleri, özellikle öğle saatlerinde güney yönüne doğru düşüyorsa, bu durum fotoğrafın Kuzey Yarım Küre'de çekildiğine işaret eder. Tam tersine, gölgelerin kuzey yönüne düştüğü bir senaryo ise bizi Güney Yarım Küre'ye, örneğin Avustralya, Güney Afrika veya Arjantin gibi bölgelere götürür. Yön tespitinin yanı sıra, güneşin ufuk çizgisindeki yüksekliği veya alçaklığı gibi doğuş ve batış açıları da dünya üzerinde yaklaşık olarak hangi enlemde bulunulduğuna dair kaba ama değerli bir teknik veri sağlar.

Bir görselin hangi ülkede çekildiğini tespit etmeye çalışırken, karayollarındaki trafik akış yönü ve araçların teknik tasarımı en net bilgileri sunan somut göstergelerdir. Dünyanın büyük bir çoğunluğunda, örneğin Türkiye, Amerika Birleşik Devletleri ve Avrupa'nın genelinde araçlar sağ şeritten ilerler ve buna bağlı olarak direksiyonlar aracın sol tarafında bulunur. Buna karşılık, eğer görselde trafik sol şeritten akıyorsa ve direksiyon sağ tarafta ise, arama alanı doğrudan İngiltere, Kıbrıs, Japonya, Avustralya, Hindistan ve Yeni Zelanda gibi belirli ülkelere indirgenerek diğer seçenekler hızla elenir. Direksiyon konumunun net görülmediği durumlarda ise otobüslerin veya ticari araçların kapı yerleşimleri incelenir; çünkü kapılar her zaman trafiğin aktığı yönün aksine, kaldırım tarafına bakacak şekilde tasarlandığı için bu detay akış yönünü kesin olarak doğrular.

Doğa, coğrafi konum tespitinde bize en kapsamlı haritayı sunan somut bir kanıt kaynağıdır. Bu haritayı okumak için öncelikle bitki türlerine odaklanılır; örneğin palmiye ağaçlarının varlığı Akdeniz kıyıları, Karayipler veya Güneydoğu Asya gibi tropikal ve subtropikal iklimleri gösterirken, geniş yapraklı ormanlar ılıman bölgeleri, çam ormanları ise daha soğuk veya yüksek rakımlı arazileri işaret eder ve özel olarak okaliptüs ağaçları bizi doğrudan Avustralya kıtasına götürür. Bitki örtüsünün yanı sıra toprak rengi de belirleyici bir faktördür; Afrika ve Avustralya'nın bazı bölgelerine özgü kırmızıya çalan laterit topraklar, Avrupa genelinde yaygın olan gri ve kahverengi topraklar

veya İzlanda ve Hawaii gibi bölgelerdeki volkanik siyah topraklar, jeolojik yapı hakkında net bilgiler verir. Tüm bunlara ek olarak, kar ve buz kütleleri, kuraklık çatlakları veya muson mevsimine işaret eden yüksek su seviyeleri gibi iklimsel izler de görselin çekildiği bölgeyi daraltmak için kullanılan temel göstergelerdir.

İZLE

Google News Initiative tarafından yayınlanan videoları izleyerek, viral hale gelen görsellerdeki kesin konumların nasıl tespit edileceğini öğrenebilirsiniz.

https://www.youtube.com/watch?v=0WpUiTyn7fE

Coğrafi konum tespitinde arama alanını daraltmak için görseldeki tabelalar, reklam panoları ve duvar yazıları gibi tüm yazılı materyallerin dili ve alfabesi somut birer kanıt olarak incelenir. Örneğin, yazılarda Kiril alfabesinin görülmesi doğrudan Rusya, Ukrayna, Belarus, Bulgaristan ve bazı Balkan ülkelerini işaret ederken, Arap alfabesi arama alanını Orta Doğu ve Kuzey Afrika ülkelerine yönlendirir. Latin alfabesi Türkiye, Batı Avrupa ve Amerika kıtaları gibi çok geniş bir coğrafyada kullanılsa da harflerin üzerindeki aksan işaretleri incelenerek metnin Çekçe, Lehçe, Fransızca veya İspanyolca olduğu ayırt edilebilir ve böylece konum belirli bir ülke grubuna indirgenebilir. Benzer şekilde, Asya dillerine ait karakterlerin Çince, Korece veya Japonca olup olmadığının teknik olarak ayrıştırılması da konumu netleştiren belirleyici bir faktördür.

Mezo Seviye: Hangi Şehir / Hangi Bölge?

Coğrafi konum tespitinde aday ülke belirlendikten sonra, arama alanını belirli bir şehre veya bölgeye daraltmak için mimari tarz ve yapı malzemeleri gibi somut yerel detaylar incelenir. Bu süreçte binaların tasarım özellikleri

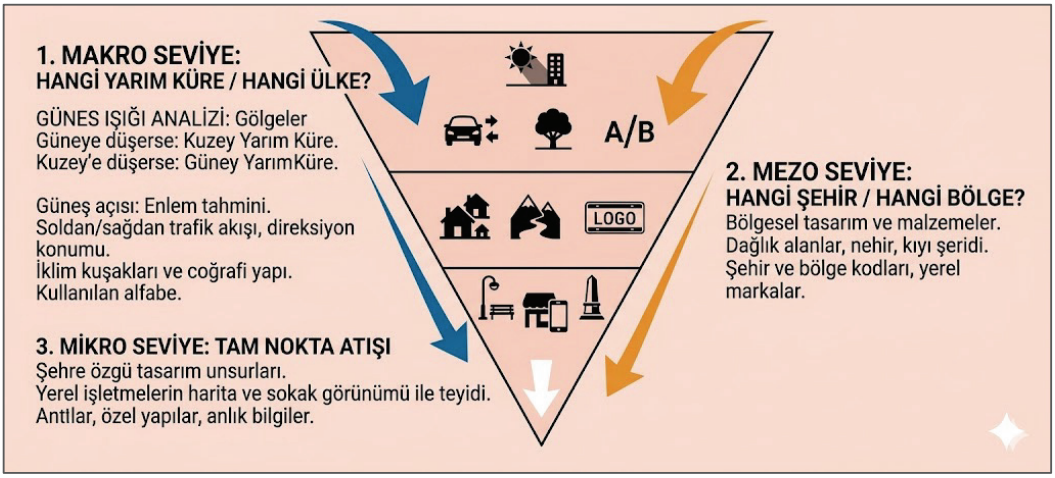
iklimsel ve kültürel ipuçları sunar; örneğin kiremit çatılar genellikle Akdeniz ve sıcak iklim bölgelerine özgü iken, İskandinavya veya Alpler gibi yoğun kar yağışı alan yerlerde kar yükünü azaltmak için tasarlanmış dik açılı metal veya arduaz çatılar, Ortadoğu coğrafyasında ise düz beton çatılar yaygın olarak görülür. Çatı yapısının yanı sıra dış cephedeki detaylar da konumu netleştirir; pencerelerde panjur veya kepenk kullanımı Güney Avrupa ve Akdeniz mimarisini işaret ederken, binaların yüksekliği ve birbirine olan yakınlığı o bölgenin imar planı ve şehirleşme yoğunluğu hakkında belirleyici teknik veriler sağlar.

Coğrafi konum belirleme sürecinde çevredeki doğal peyzajın incelenmesi, arama alanını daraltmak için kritik veriler sunar. Bu analiz kapsamında öncelikle ufuk çizgisinde görünen dağların veya tepelerin sivri, yayvan ya da volkanik şekilleri ile üzerlerindeki bitki örtüsü detaylıca gözlemlenerek, elde edilen bu formlar Google Earth veya dijital haritaların topoğrafya katmanlarıyla karşılaştırılır. Dağların yanı sıra görselde yer alan nehir, göl veya deniz gibi su kaynakları da belirleyici bir rol oynar; suyun renginin, örneğin Nil Nehri'ne özgü kahverengi tortulu yapıya benzemesi veya kıyı şeridinin kumlu ya da kayalık olması gibi fiziksel özellikler, bölgenin tespit edilmesinde somut kanıtlar sağlar.

Coğrafi konum belirleme sürecinde görselde yer alan resmi yazılar ve sayısal kodlar en somut kanıtları oluşturur. Bu kapsamda araç plakalarının formatı, renkleri ve üzerindeki ülke ya da bölge kodları incelenerek, örneğin Türkiye'deki 06 Ankara veya 34 İstanbul kodları gibi verilerle konum tespiti yapılır. Plakaların yanı sıra dükkân tabelalarında veya ilanlarda yer alan telefon numaralarındaki alan kodları da doğrudan şehri işaret eden kritik göstergelerdir; örneğin İstanbul için 0212 veya Ankara için 0312 kodlarının görülmesi bölgeyi kesinleştirir. Ayrıca yerel market zincirleri, bankalar, benzin istasyonları veya kamu kurumlarına ait kurumsal logolar ve isimler de coğrafi konumu daraltmak ve doğrulamak için kullanılan belirleyici unsurlardır.

Mikro Seviye: Tam Nokta Atışı

Coğrafi konum belirleme sürecinde şehir tespit edildikten sonra, arama alanını belirli bir caddeye, sokağa veya tam bir koordinat noktasına indirgemek için görseldeki en ince detaylara ve benzersiz işaretleyicilere odaklanılır. Bu aşamada, her şehrin veya ilçenin kendine has tasarım özelliklerini yansıtan sokak mobilyaları ve belediye altyapısı somut birer kanıt olarak kullanılır. Çöp kutularının rengi, şekli, üzerlerindeki belediye logoları ve geri dönüşüm ayrım sistemleri incelenirken; park ve sokak banklarının materyali ile tasarımı da bölgeye özgü ipuçları sağlar. Ayrıca kaldırım taşlarının deseni, rengi ve zemin kaplama malzemesi, aydınlatma direklerinin tipi ve lamba tasarımları ile trafik işaretlerinin yerleştirilme şekli gibi fiziksel unsurlar analiz edilerek görselin çekildiği nokta kesin olarak belirlenir.



Şekil 4.4.1 *Coğrafi konum belirleme: Huni tekniği*

Coğrafi konum tespitinde en kesin sonuca ulaşmak için, görsel üzerinde net bir şekilde okunan mağaza isimleri veya yerel işletme tabelaları belirlenerek Google Maps, Yandex Haritalar gibi platformlarda ilgili şehir sınırları içinde aratılır. Arama sonucunda birden fazla olası konumla karşılaşılması durumunda, Google Street View üzerinden elde edilen sokak görüntüleri ile

eldeki görseldeki mimari detaylar, kaldırım taşları ve sokak mobilyaları birebir karşılaştırılarak doğru nokta tespit edilir. Bu işletme verilerinin yanı sıra heykeller, anıtlar, camiler, kiliseler veya özgün mimariye sahip köprüler gibi benzersiz yapılar da konumu genellikle tek bir noktaya indirgeyen sabit işaretleyiciler olarak kullanılır. Ayrıca otobüs duraklarında yer alan hat numaraları, reklam panolarındaki etkinlik tarihleri veya otopark biletlerinde görülen saat bilgileri gibi geçici veriler de konum ve zaman doğrulamasında somut kanıtlar sağlar.

Hangi Araçlar Kullanılabilir?

Jeolokasyon, bir görsel veya videonun coğrafi konumunu saptama sürecidir. Dijital dedektifler ve OSINT (açık kaynak istihbaratı) uzmanları için kritik öneme sahip olan bu süreç, gelişmiş yazılımlar ve özel teknikler gerektirir. Pasaporta veya fiziksel seyahate gerek yoktur; aşağıdaki dijital araçlar ve yöntemler, sanal bir dünya turu atarak kesin konumu belirlemenizi sağlar:

Google Earth Pro (Masaüstü Sürümü)

Google Earth'ün web tabanlı basit sürümünün aksine, bilgisayara indirilen "pro" sürümü, jeolokasyon görevleri için vazgeçilmez, çok boyutlu bir analiz platformudur. Yalnızca mevcut uydu görüntülerine değil, geçmiş verilere ve gelişmiş görsel manipülasyon özelliklerine erişim sağlar. Haritalara hep kuş bakışı bakmaya alışkınız ama bu özellik kuralları değiştirir. Program içinde kamerayı eğip bükerek dağları, vadileri ve yüksek binaları sanki oradaymışsınız gibi üç boyutlu olarak inceleyebilirsiniz. Elinizdeki bir videoda görünen ufuk çizgisini, örneğin bir dağ sırasını veya şehrin silüetini haritadaki görüntüyle birebir eşleştirebilirsiniz. Bakış açısını değiştirerek "Bu videoyu çeken kişi tam olarak hangi yöne bakıyordu?" sorusunu kolayca çözebilirsiniz.

Tarihsel görüntülerle zaman yolculuğu, jeolokasyonun en kritik

özelliğidir. Zaman çubuğunu kaydırarak bir sokağın veya arazinin 2023, 2015, 2005 ve hatta çok daha eski yıllardaki uydu görüntüleri arasında saniyeler içinde geçiş yapabilirsiniz. Bu sayede dedektiflik yapabilirsiniz: "Videoda bu bina var ama haritada yok. Demek ki ya harita eski ya da video bina yapılmadan önce çekilmiş" gibi fikirleri test edersiniz. İnşaat alanlarını, yıkılan yapıları veya değişen yolları takip ederek videonun hangi tarihlerde çekilmiş olabileceğini kolayca bulursunuz.

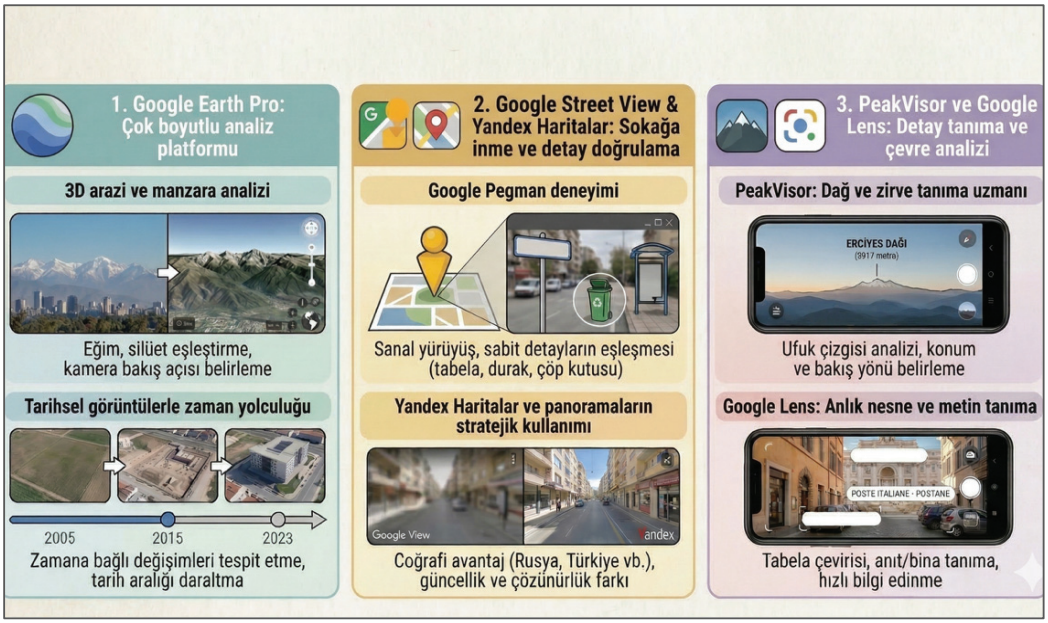
Google Street View & Yandex Haritalar: Sokağa İnmek

Uydu görüntüleri size sadece "O bina orada mı?" sorusunun cevabını verirken, sokak seviyesindeki araçlar kapı numaraları, dükkân tabelaları, trafik işaretleri ve kaldırım desenleri gibi küçük ama kritik detayları doğrulamanızı sağlar. Google'ın o meşhur sarı adamı "Pegman"i haritaya sürükleyip bıraktığınızda, seçtiğiniz sokakta sanal bir yürüyüşe çıkabilirsiniz. Bu aşama temel doğrulama içindir: Videoda gördüğünüz bir dükkân tabelası, çöp kutusu, ağaç türü veya otobüs durağı Street View'daki görüntüyle birebir eşleşiyor mu? Bu yöntem, konumu sadece birkaç metre yanılma payıyla kesinleştirmenize yardımcı olur.

Ancak harita denince aklınıza sadece Google gelmemeli; burada stratejik bir avantaj yakalamak gerekir. Rusya, Ukrayna, Beyaz Rusya ve Türkiye (özellikle İstanbul ve Ankara gibi büyük metropoller) için Yandex'in sokak görüntüleri (*panoramas*) genellikle Google Street View'dan daha güncel olabilir ve/veya daha yüksek çözünürlükte detaylar sunabilir. Bazı bölgelerde Yandex, Google'ın hiç kapsamadığı sokakları görüntülemiş olabilir. Bu nedenle, jeolokasyon yaparken bu iki aracı birbirini tamamlayıcı olarak kullanmak zorunludur.

PeakVisor ve Google Lens: Detay Tanıma ve Çevre Analizi

Büyük harita araçları genel konumu bulmanızı sağlar, ancak bazen nokta atışı yapmak için videodaki küçük ama belirleyici detayları yakalamanız gerekir. Bu akıllı uygulamalar, görüntüdeki dağları, binaları veya tabelaları saniyeler içinde tanıyarak arama alanınızı yüzlerce kilometreden tek bir noktaya indirmenize yardımcı olur.



Şekil 4.4.2 *Dijital jeolokasyon araçları ve analiz yöntemleri*

PeakVisor, bir videonun veya fotoğrafın ufuk çizgisindeki dağların şeklini, yüksekliğini ve aralarındaki açıyı analiz eder. Ufuktaki dağ silüetini yüklediğinizde veya harita üzerinde baktığınızda, size "Bu silüet, Kayseri'deki Erciyes Dağı'nın kuzey yamacına bakılarak çekilmiş" gibi kesin coğrafi tanımlar yapabilir. Konumun deniz seviyesinden yüksekliğini ve bakış yönünü belirlemede kritiktir.

Google Lens, bir videodan alınan ekran görüntüsündeki tabelaları, anıtları, ünlü binaları veya araç modellerini anında tarar. Yabancı dildeki bir

tabelayı çevirmek, videodaki bir heykelin kime ait olduğunu öğrenmek veya bir binanın ne amaçla kullanıldığını, örneğin "Bu bina İtalya'da bir postane binası" gibi saptamak için kullanılır. Bu anahtar bilgiler sayesinde saatlerce harita taramak yerine, doğrudan doğru konuma odaklanarak süreci hızlandırırsınız.

İpuçlarını Görmek

Jeolokasyon, bir fotoğrafa basitçe bakıp geçmek değil; o karenin sunduğu tüm görsel ve çevresel verileri analiz ederek coğrafi konumu saptamak anlamına gelir. Burada asıl mesele, sadece pasif bir eylem olan bakmak ile detayları kritik bir gözle analiz eden görmek arasındaki o temel farkı yakalamaktır. Konum belirlemede başarı, çoğu insanın önemsiz arka plan sanıp geçtiği en küçük ve en sıradan detayları bile birer kanıta dönüştürebilmekten geçer.

Dünyanın en sıkıcı görünen nesneleri, bazen bir fotoğrafın nerede çekildiğini ele veren en güvenilir kanıtlara dönüşebilir. Bunun en şaşırtıcı örneği elektrik altyapısıdır. Belki günlük hayatta kafamızı kaldırıp bakmayız ama her ülkenin, hatta bölgelerin bile kendine has direk standartları ve tasarımları vardır. Bir ülkenin ekonomik durumu ve mühendislik ekolü, sokakta göreceğiniz direğin tipini belirler. Örneğin, bir fotoğrafta beton direkler görüyorsanız muhtemelen Avrupa veya Asya'nın gelişmiş bir bölgesindesinizdir. Buna karşılık, yolunuz Kuzey Amerika'ya veya İskandinav ülkelerine düştüğünde altyapının genellikle ahşap direklerden oluştuğunu fark edersiniz. Hatta yüksek gerilim hatlarını taşıyan o dev metal kafes kulelerin geometrik desenleri bile ülkelere göre patentli farklılıklar gösterir.

İşin asıl ustalığı ise başınızı biraz daha yukarı kaldırdığınızda, direklerin tepesindeki izolatörlere, o küçük porselen veya cam disklere odaklandığınızda başlar. Telleri direkten ayıran bu parçaların şekli, sayısı ve rengi

rastgele değildir; tamamen ülkenin elektrik standartlarına bağlıdır. Öyle ki, *Geoguessr* gibi konum bulma oyunlarının profesyonel oyuncuları, sadece bu izolatörlerin dizilimine bakarak birbirine çok benzeyen Polonya ile Rusya arasındaki farkı saniyeler içinde ayırt edebilir. Dış mekandaki bu ipuçlarına ek olarak, iç mekân fotoğraflarında da benzer bir kesinlik söz konusudur. Fotoğrafta göreceğiniz basit bir elektrik prizi veya fiş standardı (tip A, B, C gibi), dünyayı bölgelere ayıran en net haritalardan biridir. Duvardaki tek bir priz deliği bile, arama alanınızı yüzlerce ülkeden birkaç taneye indirmenizi sağlayabilir.

Şekil 4.4.3 *Jeolokasyon: Çevresel veri analizinde ipuçları*

Fotoğraf analizi sırasında gökyüzündeki detaylar genellikle ihmal edilir, oysa yoğun hava trafiği, kritik bir jeolokasyon bilgisi sağlayabilir. Eğer bir fotoğrafta gökyüzünde belirgin, uzun ve kalın uçak izleri (*contrails*) varsa, bu o bölgenin uluslararası veya yoğun iç hat uçuş rotaları üzerinde olduğunu gösterir. Bu durum, Afrika'nın veya Sibirya'nın seyrek nüfuslu bölgelerinden ziyade, Batı Avrupa, Kuzey Amerika veya Doğu Asya gibi yoğun hava

sahalarını işaret eder. Bu bilgi, halka açık uçuş takip sitelerinin, örneğin, FlightRadar24 veya ADS-B Exchange geçmiş verileriyle eşleştirilebilir. Fotoğrafın çekildiği varsayılan zaman dilimine ait yoğun uçuş trafiği haritaları incelenerek, o rotanın gerçekten o bölgeden geçip geçmediği doğrulanabilir. Bu, konumu belirli bir coğrafi koridora daraltmada son derece etkilidir. Gökyüzündeki bir diğer hayati ipucu Güneş'in kendisidir. Güneşin pozisyonu ve nesnelerin gölgelerinin uzunluğu/açısı, fotoğrafın çekildiği mevsimi, günü ve yaklaşık saati belirlemekte kullanılabilir.

İnsan yapımı bu yapılar, özellikle çatı üstü veya cephe montajlarında, coğrafi yönelime dair güçlü ve güvenilir işaretler verir. Kuzey Yarım Küre'de güneş panelleri ve televizyon çanak antenleri enerji veya sinyal verimliliğini maksimize etmek için genellikle güneş ışınlarının en dik geldiği yöne güneye bakmak zorundadırlar. Bu kural, size pusula veya manyetik kuzey bilgisi olmadan fotoğrafın çekildiği yerdeki güney yönünü saptama imkânı verir. Fotoğraftaki bir çatıda antenlerin baktığı yönü güney kabul ederek, diğer ipuçlarını, yolun yönü, binaların yerleşimi) harita üzerinde ona göre arayabilir ve konum aralığınızı daraltabilirsiniz. Tam tersine, Güney Yarım Küre'de Ekvator'un güneyi, bu yapılar optimum verim için kuzeye bakarlar.

Güneş panellerinin ve bazen çanak antenlerin ufka göre eğim açısı, doğrudan o yerin coğrafi enlemi ile ilişkilidir. Güneş ışınlarının enlem derecesine eşit bir açıyla gelmesi istenir. Ekvator'a yakın bölgelerde paneller neredeyse yatay, düşük eğim monte edilirken, kutuplara yakın bölgelerde paneller çok daha dik bir açıyla monte edilir. Fotoğraftaki eğim açısını tahmin etmek, konumun tahmini enlemini belirlemeye yardımcı olur.

👉 DENE:

Senaryo: Sosyal medyada hızla yayılan ve yüksek etkileşim alan bir video paylaşımı: "İstanbul Esenyurt sular altında, yetkililer seyrediyor!" başlığıyla paylaşılan video, şiddetli bir sel felaketini gösteriyor.
Amaç: Video içeriğinin iddia edilen yer ve zamanda gerçekten Esenyurt'ta çekilip çekilmediğini bilimsel ve dijital yöntemlerle doğrulamak.

1. Görsel ve Metinsel Kanıtların İncelenmesi (Mikro Analiz)
Bu aşamada videonun içindeki en küçük detaylar bile coğrafi konumu ve bağlamı ortaya çıkarabilecek ipuçlarıdır.

Metin ve Tabelaları Oku/Çözümle:
Videoyu Durdurma ve Görüntü İyileştirme: Yüksek çözünürlüklü ekran görüntüleri (snapshot) almak için InVID/WeVerify gibi araçlar veya ekran kaydediciler kullanılmalıdır.
Dil ve Alfabe Analizi: Tabelalar, reklam panoları, araç plakaları ve dükkân vitrinlerindeki yazıların dili incelenmelidir.
Kurumsal Kimlik Kontrolü: Banka, market zinciri veya yerel bir markanın tabelası varsa, o markanın iddia edilen şehirde (Esenyurt/İstanbul) şubesinin olup olmadığı kontrol edilir.

Altyapı ve Kentsel Tasarım Analizi:
Yol Çizgileri ve İşaretlemeler: Türkiye'de yaygın olarak kullanılan yol kenarı ve şerit çizgilerinin standart rengi (genellikle beyaz) ile videodakinin karşılaştırılması. Bazı ülkelerde (örneğin ABD, İngiltere'nin bazı bölgeleri) sarı çizgiler kullanılır.
Kaldırım ve Kent Mobilyaları: İstanbul Büyükşehir Belediyesi'nin (İBB) veya yerel belediyenin standart olarak kullandığı kaldırım taşlarının deseni, rengi ve rögar kapaklarının üzerindeki mühür/logo incelenir. Türkiye'deki standart çöp kutuları, otobüs durakları veya trafik lambalarının tasarımı farklı bir ülkenin tasarımıyla karşılaştırılmalıdır.
Araçlar: Görüntüdeki araçların (otomobiller, otobüsler, polis/ambulans araçları) plakaları, modelleri ve direksiyonlarının konumu (sol/sağ) ülkeye özgü standartlarla teyit edilir.

2. Tersine Görüntü ve Video Arama:
Bu aşamada videonun ilk kez ne zaman ve hangi bağlamda internete yüklendiği tespit edilir.
Kare/Görüntü Alma ve Arama Motoru Kullanımı: Videodan alınmış en belirgin ve net kareler (yüzler, binalar, belirgin nesneler içeren) kaydedilir.
Çapraz Arama Motorları: Google Görseller (Image Search), Yandex Görsel Arama, Bing Görsel Arama ve özellikle Çin menşeli görseller için Baidu kullanılmalıdır. Yandex, Rusya ve çevre ülkelerdeki görsellerde oldukça başarılıdır.
InVID/WeVerify Eklentisi: Bu araç, videoyu karelere ayırarak otomatik tersine arama yapma ve videonun meta verilerini (ilk yüklenme tarihi, orijinal kaynak) bulma konusunda uzmandır.

Sonuçların Analizi: Arama sonuçlarında video veya karenin çok daha eski bir tarihte ve farklı bir coğrafi konumda (Örneğin, "2 yıl önce Atina'daki sel" veya "2020 Tiflis su baskını") paylaşıldığı tespit edilebilir. Bu, videonun bağlamının çalındığı veya manipüle edildiği anlamına gelir.

Zamansal Doğrulama (*Chronolocation*)

Dijital dezenformasyonun en sık başvurduğu yöntemlerden biri, eski bir içeriği yeni bir olaymış gibi sunmaktır. Bu bağlam kaydırması, aşağıdaki gibi temel sorularla açığa çıkarılabilir. Bir video veya fotoğraf, bir saldırının "sabah saat 08:00'de" gerçekleştiğini iddia edebilir. Ancak görseldeki nesnelerin gölgelerinin yönü ve uzunluğu, aslında öğleden sonra 16:00'yı veya akşam saatlerini işaret ediyor olabilir. Gölgeler, adeta bir dijital güneş saati görevi görerek bize gerçeği fısıldar.

Mevsimsel çelişkiler de doğrulamaya katkı sunar. Bir içeriğin "kışın, kar fırtınası sırasında çekildiği" iddia edilebilir. Oysa görüntüdeki ağaçlar gür ve yemyeşildir, yaprak döken türlerin dalları çıplak değildir. Ya da tam tersi, "yaz aylarında" çekildiği söylenen bir görselde insanlar kalın kışlık giysiler

içinde olabilir. Bitki örtüsünün durumu, bir bölgenin mevsim döngüsü hakkında kesin kanıt sunar. İddia edilen zamanda o bölgede kaydedilen hava

📌 ÖRNEK VAKA:

BBC Africa Eye ekibinin, Kamerun'da sivilleri infaz eden askerlerin videosunu doğrulama süreci, jeolokasyon tarihinin en büyük derslerinden biridir. İddia: Sosyal medyada yayılan videoda askerler sivilleri öldürüyordu. Hükümet "Bu video sahte, Mali'de çekilmiş" dedi.

Çözüm Adımları

Dağ Sırtı (*Ridge Matching*): Dedektifler, videonun arka planında çok silik bir dağ sırtı fark etti. Google Earth Pro'da Kamerun'un kuzeyindeki dağları tarayarak bu sırtın birebir aynısını buldular (Topografik Eşleşme). Konum: Krawa Mafa köyü.

Binalar: Videoda görünen duvarları yıkık bir bileşik uydu görüntülerindeki yapılarla eşleşti.

Zaman (Gölge Analizi): Askerlerin gölgesinin uzunluğundan ve açısından, olayın tam olarak hangi mevsimde ve saat kaçta gerçekleştiğini hesapladılar. (İlerleyen sayfalarda detaylandıracağız).

Sonuç: Hükümetin yalanı çürütüldü, askerler yargılandı. Sadece Google Earth kullanılarak adalet sağlandı.

Videoyu izlemek için:

🔗 https://www.youtube.com/watch?v=XbnLkc6r3yc

🔗 https://www.bbc.com/turkce/haberler-dunya-45625532

durumu, yağmur, açık hava, yoğun bulutluluk, kar gibi bilgileri, görseldeki atmosferle karşılaştırıldığında büyük tutarsızlıklar ortaya çıkabilir. Olayın geçtiği iddia edilen gün ve saatteki uydu görüntüleri veya meteorolojik kayıtlar, görselin gerçekte ne zaman çekildiğini saptamada önemli bir teyit mekanizmasıdır.

TEMEL ÇIKARIMLAR

Bir görüntünün nerede çekildiğini bulmak için, o yerin sunduğu fiziksel ve çevresel ipuçlarını, gölgeleri, bitkileri ve mimariyi analiz etme sanatıdır. Coğrafya yalan söylemez. Örneğin arka plandaki bir dağ silüeti veya güneşin açısı, olayın iddia edilen yerde değil, bambaşka bir ülkede gerçekleştiğini kanıtlayabilir.

Temel Kavramlar ve Mekanizmalar

Google Earth Pro (Masaüstü): 3 boyutlu arazi analizi ve en önemlisi "Tarihsel Görüntüler" özelliği ile binaların geçmişteki durumunu incelemeyi sağlar.

Huni Tekniği: Konum tespitinde arama alanını sistematik daraltma yöntemidir: Makro (kıta/ülke tespiti için trafik yönü, iklim), mezo (şehir tespiti için mimari, plakalar) ve mikro (tam nokta tespiti için sokak mobilyaları, tabelalar).

Yön ve Gölge Analizi: Kuzey Yarım Küre'de (örn. Türkiye) çanak antenler ve güneş panelleri Güneye bakar. Bu kural pusula olmadan yön bulmayı sağlar. Gölgelerin uzunluğu ve yönü ise zamanı ve mevsimi ele verir.

4.4. KENDİNİZİ TEST EDİN

Soru 1: Google Earth Pro'nun web sürümünde olmayan ve jeolokasyon için hayati önem taşıyan özelliği hangisidir?

A) Sokak görünümü

B) Geçmiş uydu görüntülerine erişim

C) Arama çubuğu

D) Zoom yapma

Soru 2: Bir fotoğrafın Kuzey Yarım Küre'de çekildiğini anlamanın en pratik yollarından biri nedir?

A) Ağaçların eğimi

B) Güneş panellerinin ve çanak antenlerin yönü

C) Gökyüzünün rengi ve bulutların ilerleme yönleri

Soru 3: "Huni tekniği" jeolokasyonda neyi ifade eder?

A) Makro; mezo ve mikro analizini sırayla yapmayı

B) Doğrudan ilgili sokağı, binayı, yeri aramayı

C) Huni şeklinde bir alet yardımı ile yeri bulmayı

4.4. MERAKLISINA EK KAYNAKLAR

Higgins, E. (2021). *We are Bellingcat: Global crime, online sleuths, and the bold future of news*. Bloomsbury Publishing USA.

Toprak, E. (2019, 28 Aralık). *Google Haritalar yardımıyla nasıl iz süreriz?* Teyit. https://teyit.org/teyitpedia/google-haritalar-yardimiyla-nasil-iz-sureriz

Dijital Hafıza, Arşivler ve Bot Analizi

Dijital dünyada var olan en büyük ve tehlikeli yanılgı, klavyedeki sil (*delete*) tuşunun, bir içeriği sanal evrenden tamamen yok etme gücüne sahip olduğuna dair yanlış inançtır. Oysa internet, kendi tasarım mimarisi ve temel protokolleri gereği unutmayan, hatta unutamayan bir yapı olarak kurgulanmıştır. Bir veri paketi, bir görsel, bir yorum ya da herhangi bir dijital içerik, internete bir kez yüklendiği anda, üzerindeki mutlak kontrolünüzü anında kaybedersiniz. Bu andan itibaren veri, yalnızca yüklendiği orijinal sunucuda kalmaz; küresel çapta binlerce farklı sunucuya kopyalanır, milyonlarca kullanıcı cihazının önbelleklerine (*cache*) alınır ve en önemlisi, arama motorları ile arşivleme botları, örneğin Internet Archive'ın botları tarafından sürekli olarak endekslenir. Bu, verinin silinse bile başka bir yerde yaşamaya devam edeceği anlamına gelir.

Dezenformasyon ve manipülasyon kampanyalarını yürüten kötü niyetli aktörler-bot hesaplar, troller ve siber çeteler, yaydıkları yalanların veya yanlış bilgilerin gerçeği teyit eden kaynaklar tarafından çürütülmeye başladığı anlarda ya da bu eylemleri nedeniyle ciddi bir hukuki risk veya itibar kaybı doğduğunda, panikleyerek tüm delilleri yok etmek için gönderilerini hızla silmeye çalışırlar. Ancak, bu çaba çoğu zaman beklenen sonucu getirmez; tam tersine, psikolojik ve sosyolojik bir fenomene "Streisand etkisi"ne yol açar. Bu etki, en basit tanımıyla şudur: *Bir bilgiyi, bir görüntüyü veya bir olayı gizlemeye, sansürlemeye veya dijital ortamdan kaldırmaya yönelik agresif ve görünür bir çaba göstermek, o şeyin tam tersi bir tepkiyle daha çok dikkat çekmesine, daha geniş kitlelere yayılmasına ve orijinal içeriğin çok daha hızlı bir şekilde kopyalanıp yeniden paylaşılmasına neden olur.* Bu durum, silinen içeriğin dijital ayak izlerinin çok daha güçlü bir şekilde pekişmesine yol açar. Tahmin edileceği üzere Barbra Streisand'a referans ile bu isim verilmiştir.

Dijital Zaman Makineleri: Arşivleme Araçları

Bir dedektifin en büyük gücü, sadece bugünü değil, özellikle dünü ve hatta silinmiş olanı görebilme yeteneğidir. Dijital çağda, gerçeği ortaya çıkarmak genellikle zamanın akışına direnen, arşivlenmiş kanıtlara dayanır. Internetin hafızasını kazarak olayların orijinal seyrini anlamamızı sağlayan temel araçlar sırasıyla incelenecektir.

İz Sürme Araçları: Zaman Yolculuğu

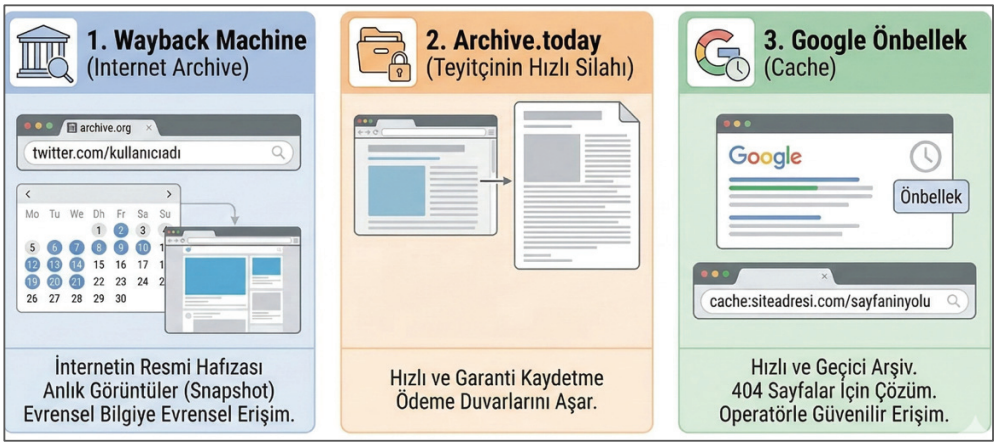
Dijital içerik hızla üretilir, değiştirilir ve silinir. Bir dijital dedektif için, bir bilginin en eski ve en doğru haline ulaşmak hayati önem taşır. İşte bu amaçla kullanılan, en güçlü üç zaman makinesi:

Wayback Machine (Internet Archive)

San Francisco merkezli, kâr amacı gütmeyen dev bir dijital kütüphane olan Internet Archive, internetin resmi hafızası olarak kabul edilir. 1996'dan bu yana, trilyonlarca web sayfasının anlık görüntülerini (*snapshot*) titizlikle saklar. Amacı, "evrensel bilgiye evrensel erişim" sağlamaktır. Kullanımı oldukça basittir. Archive.org adresine giderek, silindiğinden şüphelendiğiniz, değiştirildiğini düşündüğünüz veya orijinal halini merak ettiğiniz herhangi bir web sitesinin, blogun veya hatta bir Twitter profilinin, genellikle kullanıcı adını içeren direkt URL adresini arama çubuğuna yazarsınız. Sorgunun ardından karşınıza çıkan etkileşimli bir takvim, sitenin o güne kadar kaydedildiği tüm tarihleri gösterir. Mavi renkte daire içine alınmış tarihler, o gün içinde sitenin bir veya birden fazla kez başarıyla kaydedildiğini işaret eder. Bu tarihlere ve ardından çıkan saat dilimlerine tıklayarak, sitenin o anki tam görsel kopyasına ulaşabilirsiniz. Siyasi veya ekonomik önemi olan bir haber sitesi, yaptığı hatayı veya değişen fikrini gizlemek amacıyla manşetini veya içeriğini sessizce yenilemiş olabilir. Örneğin, sabah 09:00'da atılan "Dolar kritik eşiği

aştı" başlığı, öğleden sonra 15:00'te "Dövizde sakin hareketlilik" olarak değiştirilmişse; Wayback Machine'de o günün sabah saatine ait kayda tıklayarak, sitenin orijinal ve kanıt teşkil eden halini net bir şekilde görebilirsiniz.

Archive.today (Kişisel Favori / Teyitçinin Hızlı Silahı)



Şekil 4.5.1 *İnternette iz sürme araçları*

Teyit ve OSINT (açık kaynak istihbaratı) toplulukları arasında, özellikle hızlı ve garanti bir kaydetme mekanizması sunması nedeniyle Wayback Machine'den daha çok tercih edilen, son derece pratik bir araçtır. Archive.today'in en önemli avantajlarından biri, bir makaleyi arşivlerken ödeme duvarı, abone olmadan okunamayan içerik sınırlamasını da aşarak içeriğin tamamının statik kopyasını oluşturabilmesidir. Bu sayede, arşivlenen içeriğe herkesin erişimi mümkün olur. Bu platform, sayfanın o anki HTML ve görsel yapısını *dondurur*. Bu, sitenin kendi sunucularındaki reklamlar, zamanla değişen widget'lar, yorumlar gibi dinamik içerikler değişse bile arşivlenen kopyanın milimetrik olarak sabit kalacağı anlamına gelir. Bu nedenle, özellikle sosyal medya gönderileri silinmeden hemen önce kaydedildiğinde, mahkemeler gibi resmî kurumlarda bile güçlü ve inkâr edilemez bir dijital delil olarak kabul edilmesini sağlar.

Google Önbellek (Cache)

Google'ın kendisi, dünyanın en büyük ve en hızlı dijital arşivleyicilerinden biridir. Arama motoru, web'i tararken (*indexing*) ziyaret ettiği her sayfanın basit bir kopyasını kendi sunucularında tutar. Bu kopya, sitenin hızlı yüklenmesini sağlamak ve geçici kesintilere karşı bir yedek sunmak amacıyla oluşturulur. Erişmeye çalıştığınız bir sayfa geçici olarak silinmişse veya "sayfa bulunamadı" (*404 not found*) hatası veriyorsa, Google'ın önbelleğine bakmak hızlı bir çözüm sunar. Google'ın hafızasına ulaşmanın iki yolu olsa da ilki olan arayüz üzerinden erişim giderek zorlaşmaktadır. Normalde arama sonuçlarının yanındaki üç noktaya tıklayarak "önbellek" seçeneğini seçmek yeterliydi ancak Google bu özelliği menülerden gizlemeye başladığı için bu yöntem artık her zaman sonuç vermeyebilir. Bu nedenle en güvenilir ve kalıcı yol bir arama operatörü kullanmaktır. Arama çubuğuna "cache:" yazıp hemen bitişiğine sitenin adresini eklediğinizde (örneğin cache:teyit.org/yeni-haber biçiminde), sistem sizi arayüzle uğraştırmadan Google'ın o sayfayı en son ne zaman taradığını gösteren kopyaya anında ulaştırır

Trol ve Botlar

Dijital çağda bilgiye erişimin kolaylaşmasıyla birlikte, manipülasyon ve dezenformasyon da karmaşıklaşmıştır. Bir konunun sosyal medyada hızla yükselmesi veya "trend topic" (tt) olması, her zaman organik bir halk ilgisinin göstergesi değildir. Çoğu zaman, bu durumun arkasında gizli bir operasyon, *astroturfing* yatar. Astroturfing, İngilizce'de *astroturf*, suni çim kelimesinden türemiştir ve *grassroots* tabandan gelişen hareket olarak bilinen doğal, tabandan gelen sivil aktivizm hareketlerinin sahte bir taklididir. Astroturfing, bir merkezin veya çıkar grubunun- siyasi parti, şirket, yabancı devlet aktörü vb. kontrolünde olmasına rağmen, sanki bağımsız ve doğal bir halk desteği

varmış gibi gösterilen sahte bir kamuoyu oluşturma stratejisidir. Bu strateji genellikle ücretli troller, bot hesaplar veya manipüle edilmiş "gerçek" kullanıcılar aracılığıyla, aynı anda yüzlerce veya binlerce hesabın belirli bir hashtag'i, mesajı veya yalan haberi yaymasıyla hayata geçirilir. Amaç, sosyal medya algoritmalarını manipüle ederek konuyu ana akım medyaya taşımak ve kamuoyu gündemine oturtmaktır. Dijital dezenformasyon ve FIMI operasyonlarının temel bileşeni, yazılımlar tarafından yönetilen sosyal medya hesaplarıdır.

Bot Nedir ve Ne İşe Yarar?

Bot kavramı aslında robot kelimesinin kısaltmasıdır ve sosyal medyada bir insan tarafından değil otomatik veya yarı otomatik bir yazılım tarafından yönetilen hesapları tanımlar. Dijital ekosistemde bu yazılımlar hem yararlı hem de zararlı roller üstlenebilir. İyi botlar olarak bilinen grup topluma hizmet eden ve anlık bilgi sağlayan faydalı otomasyonlardır. Örneğin yaklaşan bir fırtınayı haber veren hava durumu hesapları veya acil durum ve deprem bildirimlerini saniyesinde paylaşan sistemler hayatı kolaylaştıran dost yazılımlara örnektir.

Madalyonun karanlık yüzünde ise dezenformasyon ve manipülasyon operasyonlarının başrol oyuncusu olan kötü botlar yer alır. Bu yazılımların temel görevi aynı anda binlerce hesaptan aynı yalan bilgiyi yaymak veya belirli bir propagandayı retweet ederek etkileşimi yapay şekilde şişirmektir. Sosyal medya algoritmalarını manipüle eden bu dijital ordular, yalan bir içeriğin "trend topic" olmasını sağlayarak organik kullanıcıların ana sayfalarında daha fazla görünür kılınmasını hedefler. Genellikle tek bir merkezden yönetilen bu yapılar bot çiftlikleri olarak bilinen büyük ağların birer parçasıdır.

Bot Nasıl Tespit Edilir?

Bot tespiti ve yayılım analizi, günümüzde akademik çalışmaların ve teyitçilik mekanizmalarının merkezinde yer almaktadır. Indiana Üniversitesi'nin geliştirdiği OSoMe (*Observatory on Social Media*) araçları, bu alanda endüstri standardı kabul edilir.

İZLE

Bot hesaplarla ilgili mekanizmaları anlamak için, +90 tarafından hazırlanan *Kim gerçek kim sahte? Bot Hesaplar nasıl çalışıyor?* başlıklı videoyu izleyebilirsiniz.

https://www.youtube.com/shorts/hSTMA2QRdE4

Bot tespiti ve yayılım analizi günümüzde akademik çalışmaların ve teyitçilik mekanizmalarının merkezinde yer almaktadır. Indiana Üniversitesi tarafından geliştirilen OSoMe araçları bu alanda endüstri standardı olarak kabul edilir ve bunların başında eski adıyla BotOrNot olarak bilinen Botometer gelir. Şüpheli bir Twitter hesabının arkasında bir insan mı yoksa bir yazılım mı olduğunu anlamak için kullanılan bu araçta sisteme bir kullanıcı adı girildiğinde gelişmiş makine öğrenimi algoritmaları devreye girer. Bu akıllı algoritmalar hesabı yüzlerce farklı kritere göre analiz eder.

İnceleme sürecinde öncelikle tweet atma sıklığına ve zamanlamasına odaklanılarak hesabın bir insanın yetişemeyeceği makine hassasiyetinde veya anormal bir sıklıkta paylaşım yapıp yapmadığı kontrol edilir. Bunun yanı sıra hesabın takipçilerinin de bot olup olmadığı ve takip edilen hesapların tek bir merkezden yönetilip yönetilmediği gibi ağ yapıları mercek altına alınır. Ayrıca atılan tweetlerin dil bilgisi yapısı ve içerik tekrarları incelenerek binlerce farklı hesapta aynı anda birebir aynı metnin paylaşılıp paylaşılmadığına bakılır. Analiz sonucunda Botometer kullanıcıya sıfır ile beş arasında bir puan verir. Sıfır puana yakın değerler gerçek bir insanı işaret ederken dört buçuk

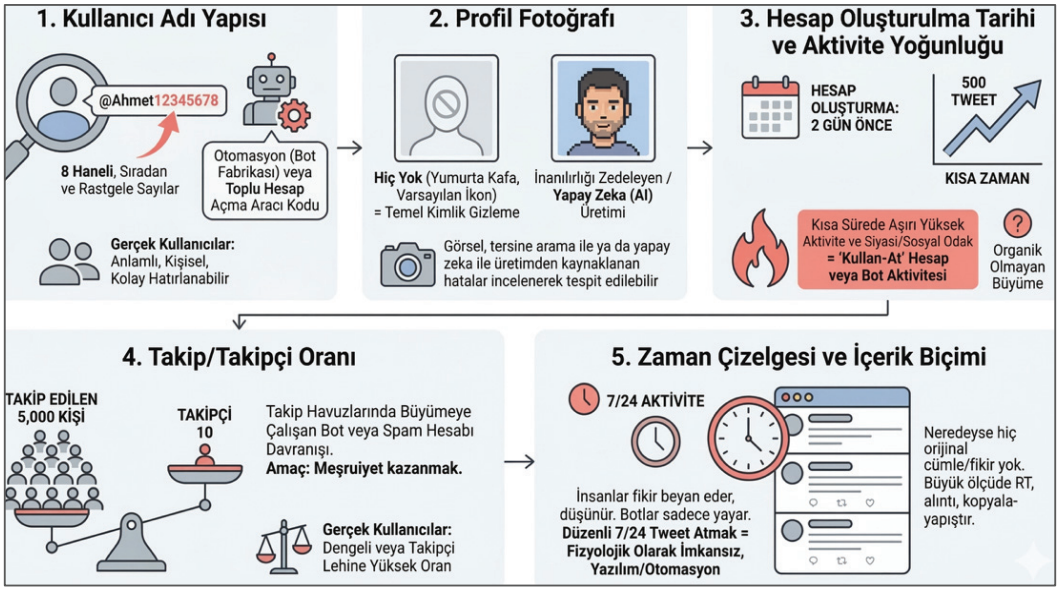
ve üzeri bir skor hesabın neredeyse kesinlikle bir yazılım tarafından yönetilen bir bot olduğu anlamına gelir ve bu hesaplara karşı dikkatli olunması gerekir.

Hoaxy, sosyal medyada dolaşan bir bilginin, etiketin veya anahtar kelimenin izlediği yolu görsel bir haritaya dönüştüren güçlü bir analiz aracıdır. Bu araç sayesinde o bilginin yayılımının insanlar tarafından doğal bir şekilde mi yoksa botlar tarafından yapay olarak mı gerçekleştiğini kolayca ayırt edebilirsiniz. Hoaxy içeriğin ilk çıkış noktasını tespit eder ve diğer hesaplara sıçrama hızını mercek altına alır; şayet bir haber merkezi bir hesaptan çıkar çıkmaz saniyeler içinde binlerce hesaba yayılıyorsa bu durumun doğal bir insan etkileşimi olması imkansızdır. Sistem bu şüpheli trafiği ve yapay ağ yapısını etkileşim grafikleriyle gözler önüne serer, böylece manipülasyonun hangi merkezden yönetildiğini ve kullanılan bot ağının büyüklüğünü somut bir şekilde görerek perde arkasındaki aktörleri tespit etmeniz kolaylaşır.

Dijital ortamdaki bilgi kirliliğiyle mücadelede yapay zekâ araçları ne kadar gelişse de insan gözü hala en kritik rolü oynar çünkü teknik araçlar yanılabilirken insan zihni bağlamsal tutarsızlıkları çok daha iyi yakalar. Bir hesabın gerçek mi yoksa manipülasyon ağının bir parçası mı olduğunu anlamak için ilk bakışta kullanıcı adı ve profil fotoğrafına odaklanmak gerekir. Eğer karşınızda @Ahmet12345678 gibi ismin sonuna rastgele dizilmiş sekiz haneli sayılarla biten bir kullanıcı adı varsa şüphelenmelisiniz; gerçek insanlar hatırlanabilir isimler seçerken bu tür kodlar otomatik yazılımlar tarafından atanır. Profil fotoğrafının hiç olmaması veya güven vermeyen bir görsel olması da güçlü bir işarettir. Fotoğraf varsa bile tersine görsel arama yapıldığında çalıntı çıkabilir ya da ellerdeki ve gözlüklerdeki geometrik bozukluklardan görselin yapay zekâ üretimi olduğu anlaşılabilir.

Hesabın ne zaman açıldığı ve kimleri takip ettiği de maskeyi düşüren önemli detaylardır. Örneğin sadece iki gün önce açılmış bir hesap kısa sürede yüzlerce siyasi tweet atmışsa bu durum organik bir büyüme değil, gündemi

manipüle etmek için hazırlanmış kullan-at hesap aktivitesidir. Ayrıca takipçi dengesizliğine de dikkat etmek gerekir; bir hesap beş bin kişiyi takip ederken sadece on takipçiye sahipse bu genellikle takip havuzlarında büyümeye çalışan ve kendini meşru göstermeye çalışan bir spam botun davranışıdır.



Şekil 4.5.2 *Sosyal medyada sahte ve bot hesapları tespit etme yöntemleri*

Son olarak zaman çizelgesine ve içerik biçimine bakarak hesabın ruhunu analiz edebilirsiniz. Gerçek insanlar fikir beyan edip tartışırken botlar sadece yayma görevi üstlenir; bu yüzden hesap sürekli retweet veya kopyala-yapıştır içerikler paylaşıyor ve hiç özgün cümle kurmuyorsa durum şüphelidir. Üstelik hesap günün her saati aralıksız tweet atıyorsa karşınızdaki kesinlikle bir yazılımdır çünkü insanlar uyur ve fizyolojik olarak 7/24 kesintisiz aktivite sergilemeleri mümkün değildir.

Koordineli Sahte Davranış

Sosyal medya platformlarının, özellikle Facebook (Meta)'nın, geniş çaplı manipülasyon ağlarını ve bot ordularını tanımlamak için kullandığı anahtar terim

"koordineli sahte davranış" (*Coordinated Inauthentic Behavior-CIB)* olarak adlandırılır. CIB, sadece "yalan haber paylaşmak" suçundan çok daha kapsamlıdır. CIB'nin özündeki suç, "olmadığın biri gibi davranarak organize hareket etmektir." Bir başka deyişle, eylemlerin koordinasyonu ve kimlik maskelemesi esastır. CIB, genellikle ulusal veya uluslararası düzeyde, siyasi veya ekonomik çıkarlar doğrultusunda, kamuoyunu manipüle etmek için organize edilmiş bir grup hesap veya sayfalar tarafından gerçekleştirilen, aldatıcı davranışları ifade eder.

Rusya merkezli bir trol çiftliğinin, coğrafi ve kültürel kimlik maskelemesi yaparak, kendini ABD'de yaşayan "Teksaslı Yurtseverler", "Afro-Amerikan Aktivistler" veya başka bir yerel grup gibi tanıtması bir CIB örneği sayılabilir. Bu sahte kimlikler aracılığıyla gruplar kurularak veya sayfa/hashtag kampanyaları başlatılarak, hedef ülkedeki kutuplaşmanın körüklenmesi, güvenin aşındırılması ve mevcut toplumsal fay hatlarının derinleştirilmesi amaçlanır.

CIB ağlarının tespit edilmesinde kullanılan en güçlü kanıt, koordinasyonun kendisidir. Bu hesapların tamamının aynı dakika veya dar bir zaman dilimi içinde aynı linki paylaşması, aynı görseli veya aynı ifade kalıbını kullanması bunun bir örneğidir. Hesapların sistematik olarak birbirlerini beğenmesi, yorum yapması ve paylaşımlarını yükseltmesi de başka bir kanıt sayılabilir. Bu, organik bir etkileşim değil, bir komut merkezi tarafından yönetilen bir "dijital sürü" davranışıdır. Analistler, bu koordinasyon desenlerini ve ağ bağlantılarını inceleyerek manipülasyonun kaynağını ve amacını ortaya çıkarır.

TEMEL ÇIKARIMLAR

İnternette "sil" tuşu bir illüzyondur. Bu bölüm, silinen içeriklerin dijital zaman makineleriyle nasıl geri getirileceğini ve sosyal medyada kamuoyu algısını yöneten insan görünümlü yazılımların-botların nasıl tespit edileceğini inceler. Manipülasyon genellikle *astroturfing* yoluyla yapılır.

Temel Kavramlar ve Mekanizmalar

Dijital Zaman Makineleri: Wayback Machine, bir sitenin geçmişteki kopyalarını takvim üzerinde gösterir. **Archive.today** ise sayfayı "dondurarak" statik bir kopya alır ve ödeme bariyerlerini aşar; mahkemelerde delil niteliği taşır.

Botometer ve Hoaxy: Botometer, bir hesabın bot olma ihtimalini (0-5 puan) hesaplarken; Hoaxy, bilginin yayılım haritasını çıkararak "organik" mi yoksa botlar tarafından "yapay" olarak mı yayıldığını görselleştirir.

Streisand Etkisi: Bir içeriği internetten silmeye veya gizlemeye çalışmanın, o içeriğin daha fazla dikkat çekmesine ve yayılmasına neden olması durumudur.

4.5. KENDİNİZİ TEST EDİN

Soru 1: Bir web sitesinin veya tweetin silinmiş eski hallerini görmek için kullanılan "dijital zaman makinesi" hangisidir?

A) Wayback Machine

B) Photoshop

C) Google Maps

D) Tinder

Soru 2: Sosyal medyada *astroturfing* ne anlama gelir?

A) Uzayla ilgili derinlemesine araştırmalar yapmak

B) Sosyal medyada yoğun bir biçimde doğa fotoğrafları paylaşmak

C) Botlar ve troller aracılığıyla, suni bir halk tepkisi yaratmak

Soru 3: Bir Twitter hesabının bot olup olmadığını anlamak için Botometer aracı hangi verileri analiz eder?

A) Profil fotoğrafını

B) Tweet atma sıklığını, takipçi ağını, dil yapısını ve etkileşimlerini

C) Kullanıcının kimlik numarasını, hesabın şifresini

4.5. MERAKLISINA EK KAYNAKLAR

Archive.org. (2024). *The Wayback Machine*. https://web.archive.org

Davis, C. A., Varol, O., Ferrara, E., Flammini, A., & Menczer, F. (2016). BotOrNot: A system to evaluate social bots. In *Proceedings of the 25th International Conference Companion on World Wide Web* (ss. 273–274).

Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, and political operatives*. Yale University Press.

Indiana University Observatory on Social Media (OSoMe). (t.y.). *Botometer & Hoaxy tools*. https://osome.iu.ed

Bölüm 5

Küresel Bilgi Savaşları:

FIMI, Bilişsel Savaş ve Araçları

🎯 TARTIŞMA SORULARI

1. Güvenlik odağı teknik altyapılardan doğrudan insan zihnine nasıl kaymıştır?
2. "Sentetik etki" operasyonları ve "bilgi aklama" döngüsü nasıl işlemektedir?
3. Bilişsel harp stratejileri, insan psikolojisinin hangi biyolojik ve zihinsel açıklarını hedef almaktadır?
4. Bilişsel güvenlik mimarisi kapsamında devlet, kurumlar ve sivil toplum için hangi savunma modelleri önerilmektedir?
5. Türkiye'nin jeopolitik konumu, maruz kaldığı bilgi operasyonları ve gelecek dönem riskleri nelerdir?

Giriş

Modern dünyada güvenlik kavramı, fiziksel sınırların ötesine taşınarak insan zihninin bir bilişsel savaş alanı olarak tanımlandığı yeni bir boyuta evrilmiştir. Bu bölümde, tehdidin siber altyapıdan insan psikolojisine kaydığı "sentetik etki" dönemi, bir başka deyişle de içinde bulunduğumuz "hibrit savaşın sisi"ni analiz edilmektedir. Dezenformasyonun, profesyonel bir "bilgi aklama" mekanizmasıyla nasıl meşruiyet kazandırıldığı ve FIMI (Yabancı Bilgi Manipülasyonu ve Müdahalesi) aktörlerinin bu süreçte oynadığı rol incelenmektedir. İnsan zihninin nörolojik açıklarının nasıl birer güvenlik zafiyetine dönüştürüldüğü ele alınırken, bu asimetrik tehdide karşı devlet ve toplumun tüm katmanlarını kapsayan bütüncül bir direnç modelinin gerekliliği tartışılmaktadır. Son olarak, küresel bilgi fay hatlarının merkezinde yer alan Türkiye'nin 2030 projeksiyonu; nöro-siyasetten biyometrik veri savaşlarına uzanan risk haritası üzerinden değerlendirilmekte ve hakikatin savunulması bir ulusal güvenlik önceliği olarak konumlandırılmaktadır.

Tehdidin Evrimi: FIMI, ABC Modeli ve "Sentetik Etki"

Dijital iletişimin ilk dönemlerinde, bilgi kirliliğine karşı savunma hattı oldukça basitti ve "yalan haber" kavramı üzerine kuruluydu. Bu yaklaşımın temelinde yatan mantık şuydu: Bir bilgi, olgusal olarak doğru mu, yoksa yanlış mı? Yanlış olduğu tespit edilen bilgiler, doğruluk kontrolü yapan kuruluşlarca hızla çürütülerek sorunun çözüleceğine inanılıyordu. Bu model, bilginin kaynağı ve niyeti gibi karmaşık faktörleri göz ardı eden, iyi niyetli ancak basit bir ikili karşıtlık (doğru/yanlış) üzerine kuruluydu. Ancak, 2016 ABD Başkanlık Seçimleri, Birleşik Krallık'taki Brexit referandumu ve ardından hızla yayılan küresel pandemi süreçleri, bu basit çözümün siber alandaki stratejik tehditlerin karşısında ne kadar yetersiz, hatta safça olduğunu net bir şekilde

ortaya koydu. Sorun, artık münferit kişilerin yaydığı basit yalanlar olmaktan çıkmıştı.

Günümüzde karşı karşıya olunan asıl tehdit, yalnızca yanlış bilgi yayan bireyler değildir. Dijital savaş alanı, artık devlet destekli, istihbarat servislerince planlanan, büyük bütçelerle finanse edilen ve çok net, stratejik hedeflere sahip operasyonlara ev sahipliği yapmaktadır. Bu operasyonların karmaşıklığı şuradan gelmektedir: Bu tür sofistike etkileme kampanyalarında, çoğu zaman yalan söylenmeyebilir. Manipülasyon, içeriğin doğruluğunda değil, yayılma biçiminde ve niyetinde gizlidir.

Bu çerçevede Mehmet Ali Tuğtan, Carl von Clausewitz'in klasik savaş teorisini modern hibrit savaş bağlamında ele alırken farklı disiplinlerden yararlanır. Bilişsel psikoloji ve nörobilim kullanarak, Clausewitz'in "savaşın sisi" kavramını günümüze uyarlayıp "hibrit savaşın sisi" kavramını tanımlar. Geleneksel savaşta sis, bilgi eksikliği veya yanlış istihbarattan kaynaklanır. Hibrit savaşta ise bilgi fazlalığı ve çarpıtılması, manipülasyon ve dezenformasyonla oluşur. Bu sisin insan zihnindeki etkisini Eagleman ve Kahneman'ın teorileriyle açıklar. Özellikle beynin sezgisel karar verme eğilimlerini kullanarak toplumun gerçeklikle bağını koparmayı hedefler. Kısacası, Hibrit Savaşın Sisi, rasyonel karar alma süreçlerini bozarak kamuoyunun savaşa dair algısını ve desteğini manipüle eder. RESAID Politika Belgeleri'nde yer alan "Clausewitzci Bir Hibrit Savaş Teorisi (2024)" başlıklı çalışmasında Tuğtan,[51] hibrit savaşı tüm yönleriyle açıklayan bir teori sunmayı amaçlar. Teorinin merkezinde Clausewitz'in "friksiyon" kavramı vardır. Friksiyon, modern hibrit savaşta insan zihnini hedef alır. Geleneksel savaşta sis önce orduyu, sonra hükümeti ve halkı etkilerken, hibrit savaşta bu sıralama tersine döner. Önce halkı, sonra hükümeti ve en son orduyu hedef alır. Hibrit savaşın yarattığı

[51] Tuğtan, M. A. (2024). *Clausewitzci bir hibrit savaş teorisi* (Politika Belgesi No. 1). RESAID https://resaid.bilgi.org.tr

zihinsel friksiyonla başa çıkmak için sadece bireysel medya okuryazarlığı yeterli değildir. Devlet düzeyinde stratejik bir yanıt ve gözetim gereklidir.

Yine politika belgeleri arasında yer alan Salih Bıçakcı'nın (2025) analizine göre de günümüzde karşı karşıya olduğumuz durum, geleneksel anlamdaki basit bir "bilgi kirliliği" olmaktan çıkmış, çok daha sofistike ve tehlikeli bir aşamaya evrilmiştir: "Sentetik etki" (*synthetic influence*) adı verilen, stratejik ve çok katmanlı bir süreçtir. Bu kavram, modern bilişsel harp ve hibrit savaşın temelini oluşturmaktadır.[52] Sentetik etki, bireysel ve toplumsal algıyı hedef alarak gerçeği yeniden tanımlamayı amaçlayan, modern teknolojinin sağladığı dört temel unsurun yıkıcı bir sinerjisiyle ortaya çıkar. Manipülasyon sürecinin ilk ve en kritik aşamasını yapay zekâ destekli üretim araçları ile *deepfake* teknolojileri oluşturur. GPT gibi büyük dil modelleri ve gelişmiş görsel/video üretim araçları kullanılarak, gerçekte yaşanmamış olaylara, söylenmemiş sözlere ve mevcut olmayan kanıtlara dayanan içerikler saniyeler içinde üretilir. Metinler, görseller ve videolar o kadar ikna edici bir benzerlik taşır ki, insan gözü veya basit denetim mekanizmaları tarafından sahte, deepfake oldukları kolayca anlaşılamaz. Bu, güvenilir kaynaklara duyulan şüpheyi kökleştiren en kritik adımdır.

Üretilen bu sentetik içeriklerin etkisini yüzlerce kat artıran ikinci mekanizma ise sosyal medya platformlarının kalbinde yer alan algoritmik yayılım mekanizmaları ve otomatik bot ağlarıdır. Üretilen sentetik içeriklerin etki gücünü yüzlerce kat artıran bu mekanizma, sosyal medya platformlarının kalbinde yer alır. Platformların temel işlevi olan etkileşim ve bağlılık odaklı öneri algoritmaları, kutuplaştırıcı, duygusal ve abartılı içerikleri, kullanıcıların önüne öncelikli olarak çıkarır.

---

[52] Bıçakcı, S. (2025). *Yapay zekâ çağında bilişsel güvenlik: Sentetik etkiye karşı ulusal esnek-dayanıklılık oluşturmak* (Politika Belgesi No. 4). RESAID. https://resaid.bilgi.org.tr/politika-belgeleri/

Otomatik bot ağları ve koordineli davranışlar (*Coordinated Inauthentic Behavior*-CIB) ile bu içerikler, geleneksel medyadan çok daha hızlı ve yoğun bir şekilde hedef kitlelere yayılır. Bu sayede, sahte bir gündem, meşru bir kamuoyu algısı yaratılarak toplumsal tepkiler tetiklenir. Sentetik etkinin son ve belki de en önemli durağı insan bilişsel zaaflarının stratejik hedeflendiği "Bilişsel Harp" aşamasıdır. Bu aşamada insan psikolojisinin kırılganlıkları kullanılmaktadır. Üretilen içeriklerin dili ve konusu, doğrudan insanların duygusal tepkilerini-öfke, korku, kaygı, nefret tetiklemek üzere tasarlanır. Hedef, bireylerin rasyonel düşünme sistemlerini devre dışı bırakarak, ön yargılarını ve bilişsel kısayollarını (*cognitive biases*) kullanmaktır. Özellikle Doğrulama Yanılgısı, insanların kendi inançlarını destekleyen bilgiyi arama ve inanma eğilimi, manipülatörler için en verimli alandır. Bu sayede, sahte içerik dahi olsa, kişinin mevcut dünya görüşünü pekiştirdiği için kolayca kabul edilir.

Bu çok yönlü sürecin nihai hedefi, gerçeği taklit eden ancak temel amacı toplumsal ve siyasi manipülasyon olan yapay bir gerçeklik inşa etmektir. Sentetik Etki, sadece yanlış bilgi vermez; bireylerin kendi muhakeme yeteneklerine ve resmî kurumlara olan güvenlerini sistematik olarak aşındırır. Sonuç olarak, bireyler hangi bilginin güvenilir olduğunu ayırt edemez hale gelir ve bu gerçeklik krizi, karar alma mekanizmalarını felç ederek ulusal güvenlikten demokratik süreçlere kadar her alanda istikrarsızlığa yol açar.

Sentetik etki operasyonları, geleneksel dezenformasyonun ötesine geçerek, gerçek ve teyit edilebilir toplumsal sorunları yapay bir hız, yoğunluk ve manipülatif niyetle büyüterek hedef ülkenin bilişsel alanını hedef alan sofistike siber-psikolojik harp yöntemleridir. Bu operasyonlar, dört temel aşamada işler. İlk aşama hedefin tespiti aşamasıdır. Yabancı, düşman bir devlet veya devlet dışı aktör, hedef ülkenin en derin ve hassas toplumsal fay hatlarını, kronikleşmiş sorunlarını veya güncel krizlerini titizlikle analiz eder. Bu, basit bir dezenformasyon konusu değil, toplumun geniş kesimlerince

kesinlikle doğru ve teyit edilebilir kabul edilen bir dayanaktır.

Bu operasyonların potansiyel hedefleri arasında toplumun uzun süredir çözülemeyen kimlik çatışmalarına dayalı etnik ve dini ayrışmalar başı çeker. Ayrıca halkın doğrudan hissettiği yüksek enflasyon, işsizlik ve yaşam maliyeti gibi derin ekonomik krizler manipülatörler için oldukça elverişli bir zemin sunar. Güven kaybını tetikleyecek gerçek kanıtlara dayanan siyasi skandallar ve yolsuzluklar ile kriz anlarında ortaya çıkan kamu hizmeti eksiklikleri, afet veya pandemi yönetimi zafiyetleri de saldırganların öncelikli odak noktaları arasındadır. Bu aşamada amaç, yanlış bir şey üretmek değil, zaten var olan gerçek bir acı noktayı operasyonun başlangıç ateşi olarak belirlemektir.

İkinci aşama amplifikasyon ve hızlandırma aşamasıdır. Bu aşamada belirlenen "doğru" bilgi, veri, video veya olay, konvansiyonel medya hızının çok ötesinde, yapay bir güçle büyütülür ve hedefe pompalanır. Bu aşamada kritik olan, bilginin kendisi değil, bu bilginin yayılma biçimi, hızı ve manipülatif yoğunluğudur. Bu süreçte kullanılan temel araçların başında, binlerce sahte hesap üzerinden belirlenen hashtag, görsel ve mesajları eş zamanlı olarak otomatik biçimde yayan yapay zekâ destekli bot ağları gelir. Botların yarattığı bu yapay gündemi besleyen profesyonel trol çiftliklerindeki insan operatörler ise organik kullanıcılarla etkileşime girerek gerilimi tırmandırma görevini üstlenir. Orijinal kaynağın güvenilirliğini taklit eden sahte haber siteleri ve paravan medya kuruluşları üzerinden içeriklerin yeniden yayınlanmasıyla bu yapay etkiye bir meşruiyet görünümü kazandırılır. Tüm bu dağıtım süreci, sosyal medya platformlarının doğal algoritmalarını maksimum düzeyde sömürecek şekilde yüksek trafik saatlerine ve kritik olay anlarına senkronize edilerek algoritmik bir eş zamanlılıkla yürütülür.

Sentetik etki operasyonlarının geleneksel propagandadan ayrıldığı en önemli nokta, bilginin kaynağının doğruluğudur. Bilginin içeriği (örneğin; "Enflasyon %80'e ulaştı" veya "X siyasetçi gerçekten yolsuzluk yaptı") teknik

olarak doğru olsa bile, bu operasyonlardaki temel amaç, kamuoyunu bilgilendirmek veya bir gerçeği ortaya çıkarmak değildir.

Bu operasyonların arkasında yatan temel niyet, var olan toplumsal gerilimi, kaosu ve güvensizliği yapay bir şekilde derinleştirerek hedef ülkenin ulusal istikrarını ve karar alma mekanizmalarını bozmaktır. Bilişsel manipülasyon sürecinde asıl hedef, bilginin doğruluğundan şüphe etmeyen vatandaşın devlet kurumlarına ve medya organlarına olan genel güvenini kaybetmesidir. Saldırganlar gerçek bir krizi yapay olarak büyüterek algılanan tehdit boyutunu orantısızca artırırlar ve mevcut toplumsal gruplar arasındaki nefret ile düşmanlığı körükleyerek iç savaş benzeri bir ortamın zeminini hazırlarlar. Operasyonun nihai başarısı, yaratılan yapay kaosun, ülkenin demokratik süreçlerine, ekonomik istikrarına ve güvenlik aygıtlarına sızmasıyla ölçülür. Yapay olarak büyütülen kriz, hükümetin meşruiyetini sorgulatır, halkı sokağa döker ve ülkenin uluslararası alandaki itibarını zedeler. Sentetik etki, gerçeği çarpıtmak yerine, gerçekliğin kendisini istikrarsızlaştırarak FIMI (Yabancı Bilgi Manipülasyonu ve Müdahalesi) hedeflerine ulaşır.

Geleneksel "dezenformasyon" kavramının bu karmaşık tehdit yapısını açıklamada yetersiz kalması üzerine, uluslararası aktörler yeni bir savunma doktrini geliştirmeye başlamıştır. Avrupa Birliği Dış İlişkiler Servisi (EEAS), bu bağlamda Yabancı Bilgi Manipülasyonu ve Müdahalesi (*Foreign Information Manipulation and Interference*-FIMI) kavramını merkezine almıştır.[53] FIMI, bilgi güvenliği yaklaşımında temel bir değişimi temsil eder; artık sadece içeriğe (ne söylendiği) değil, aynı zamanda yayılma yöntemine (Bot ağları, algoritmik büyütme vb. davranışlar) ve yayılma amacına (demokratik, ekonomik veya sosyal düzeni bozma niyeti) odaklanılmaktadır. Bu değişim,

[53] European External Action Service. (2024). *2nd EEAS report on foreign information manipulation and interference threats: A framework for networked defence*. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

modern siber güvenlik yaklaşımlarının, sadece "yalanları" kovalamaktan çok, yapay olarak koordine edilen zararlı davranışları ve niyetleri analiz etmesi gerektiğini ortaya koymaktadır. Sentetik Etki, siber güvenlik, bilgi güvenliği ve ulusal güvenlik politikalarının kesişim noktasında duran, dijital çağın en karmaşık tehdididir.

Avrupa Dış Eylem Servisi'nin (EEAS) ve uluslararası güvenlik literatürünün temel tanımına göre FIMI; *"Yabancı aktörlerin, demokratik değerleri, kurumları ve süreçleri hedef alan, kasıtlı, manipülatif ve koordineli eylemleridir."*[54] Bu tanım, klasik propaganda veya yanlış bilgiden ayrılan, uluslararası ilişkilerde yeni ve sinsi bir tehdidi işaret eder.

Şekil 5.1.1 *"Siber-psikolojik harp" yöntemi olarak gerçeğin silahlaştırılması*

FIMI'yi tanımlayan ve onu operasyonel bir tehdit haline getiren yapının temelinde üç ana kaide bulunur ve bunlardan ilki operasyonun sınır ötesi

[54] European External Action Service. (2026, 27 Ocak). *Information integrity and countering foreign information manipulation & interference (FIMI)*. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

niteliğini vurgulayan yabancı kaynak unsurudur. Tehdidin kaynağı hedef ülkenin dışındaki bir devlet veya yapı olsa da günümüzde bu yabancılık olgusu ağ bağlantılı meşruiyet taktikleriyle gizlenerek yerel vekil unsurlar üzerinden sanki içeriden ve tabandan geliyormuş gibi sunulmaktadır. Bir yabancı istihbarat servisi, Sliz'in (2025) Afrika'daki dezenformasyon haritalandırmasında örneklendirdiği gibi[55] Afrika veya Avrupa'daki yerel bir aktivist grubu fonlayarak kendi mesajını onlara söyletir. Böylece mesaj dışarıdan değil, içeriden, tabandan geliyormuş gibi görünür. FIMI'nin operasyonel kalbi, Bergmanis-Korāts ve arkadaşlarının (2025) NATO StratCom analizlerinde[56] vurguladığı üzere, içeriğin yanlışlığından ziyade davranışın manipülatif olmasıdır. Bu kapsamda doğru bilginin zarar verme kastıyla bağlamından koparıldığı malenformasyon taktiğinin yanı sıra hedef kitleyi bilgiye boğarak doğruyu ayırt etme kapasitesini felç eden flooding yöntemi uygulanır.

Teknolojinin gelişimiyle birlikte artık sadece botlar değil yapay zekâ modelleri de devreye girerek saniyeler içinde binlerce özgün ve ikna edici içerik üretmekte ve böylece gerçeklik algısını sentetik olarak yeniden inşa etmektedir. Son olarak FIMI'yi farklı kılan müdahale niyeti faktörü devreye girer ve bu aşamada hedef ülkenin egemenliğine yönelik saldırgan bir tavırla seçim sonuçlarını değiştirmek, karar alma mekanizmalarını felç etmek ve toplumsal kutuplaşmayı derinleştirmek gibi yıkıcı hedefler güdülür.

---

[55] Sliz, J. (2025, Ekim). *Truth Africa: Regional map of disinformation in Africa* [Konferans sunumu]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenya.

[56] Bergmanis-Korāts, G., Vecmanis, R. R., & Isupova, M. (2025). *Virtual manipulation brief 2025: From war and fear to confusion and uncertainty*. NATO Strategic Communications Centre of Excellence (NATO StratCom COE).

📌 **ÖRNEK VAKA:** MH17 ÖRNEĞİ

Bilgiye boğma taktiğinin en çarpıcı örneklerinden biri 2014 yılında Ukrayna üzerinde düşürülen MH17 sefer sayılı Malezya uçağı olayında yaşanmıştır. Olayın hemen ardından Rusya kaynaklı kanallar tek bir tutarlı yalan söylemek yerine aynı anda birbiriyle çelişen birçok farklı senaryoyu dolaşıma sokarak karmaşa yaratmayı hedeflemiştir. Uçağın bir Ukrayna jeti tarafından vurulduğu, uçakta zaten ölülerin bulunduğu veya olayın bir CIA operasyonu olduğu gibi tutarsız iddialar aynı anda yayılmıştır. Saldırganların buradaki temel amacı halkı tek bir yalana inandırmak değil aksine o kadar yoğun bir bilgi gürültüsü yaratmaktır ki uçağın Rus füzesiyle vurulduğu gerçeğinin bu gürültü arasında kaybolmasını sağlamaktır. Bu taktik kitlelerin gerçeği asla bilemeyecekleri hissine kapılarak olay karşısında duyarsızlaşmasına ve ilgisizleşmesine neden olur.

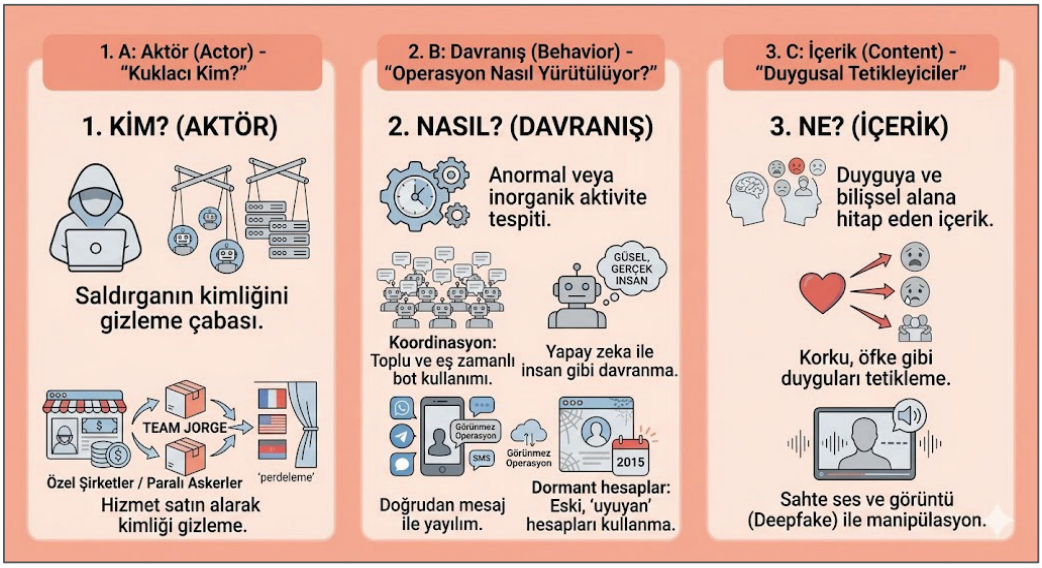
🔗 https://www.bellingcat.com/tag/mh17/

Tehdidi Analiz Etmek: ABC Modeli

Bir bilgi operasyonunu analiz etmek için küresel çapta kabul gören standart yöntem Camille François tarafından geliştirilen ABC modelidir[57]. Bu model 2025 yılı itibarıyla yapay zekâ destekli yeni taktiklere göre güncellenmiştir. Modelin ilk ayağını oluşturan aktör analizi saldırının arkasındaki kuklacıyı bulmayı hedefler ancak dijital dünyada saldırganın kimliğini tespit etmek oldukça zordur çünkü devletler artık kendi ellerini kirletmek yerine özel şirketlerden veya karanlık ağdaki siber paralı askerlerden hizmet olarak dezenformasyon satın alarak kendilerini gizleyen bir perdeleme yöntemi kullanmaktadır. Modelin en kritik katmanı olan davranış analizi ise operasyonun nasıl yürütüldüğüne odaklanır ve içerik yasal olsa bile davranışın doğal

[57] François, C. (2019). *Actors, behaviors, content: A disinformation ABC* (Working Paper). Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression.

olmamasını bir manipülasyon kanıtı olarak kabul eder. Bu kapsamda binlerce hesabın aynı anda aynı mesajı yaydığı koordinasyon çalışmaları ve yıllardır kullanılmayan eski hesapların operasyon anında uyandırılması sıkça görülen taktiklerdir. Graphika'nın raporlarına göre yapay zekâ botları artık güvenlik duvarlarını aşmak için bilerek gramer hatası yapmakta ve argo kullanarak gerçek bir insan gibi davranmaktadır.[58] Ayrıca Google Cloud raporlarına göre[59] saldırganlar sadece sosyal medya duvarlarında değil e-posta ve mesajlaşma uygulamaları üzerinden kişisel kutulara sızarak görünmez operasyonlar yürütmektedir. Son aşama olan içerik analizi ise mantıktan ziyade doğrudan duygusal tetikleyicilere odaklanır ve içerikler korku ile öfke gibi duygularla bilişsel alanı hedef alacak şekilde tasarlanarak liderlerin hiç



Şekil 5.1.2 *Bilgi operasyonunu analiz etmek için kullanılan "ABC modeli"*

[58] Le Roux, J., & Ronzaud, L. (2025, Ekim). *OrdinAIry people: Network of Telegram accounts uses fake personas and generative AI models to target English- and Russian-language audiences online*. Graphika.

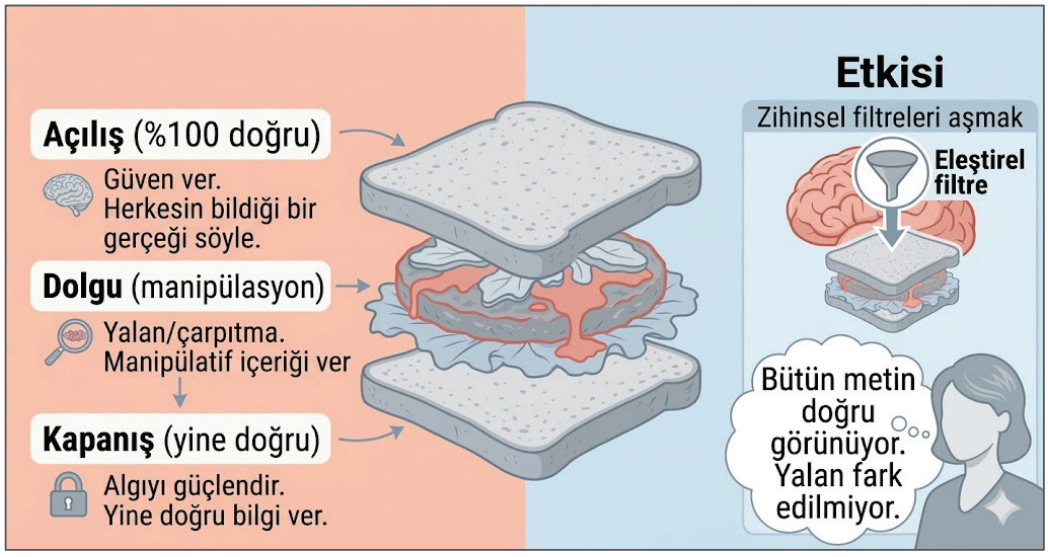
[59] Wahlstrom, A. (2025, Ekim). *Direct dissemination tactics & precision targeted information operations* [Konferans sunumu]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenya.

söylemedikleri sözleri söylemiş gibi gösteren deepfake teknolojileriyle desteklenir.

Mikro-Taktikler: Yalanı Gizleme Sanatı

Bilişsel harp alanında üretilen içerikler, geleneksel yalan ve dezenformasyonun ötesine geçerek, gerçeği çarpıtmayı ve tespit edilmeyi zorlaştırmayı hedefleyen sofistike "bilgi simyası" taktiklerini kullanır. Bu taktikler, hedef kitlenin zihinsel savunma mekanizmalarını aşmayı ve manipülatif mesajın güvenilirliğini artırmayı amaçlar:

Manipülasyon Sandviçi



Şekil 5.1.3 *Yalanı doğruların arasına gizleyerek güven kazanma: "Manipülasyon sandviçi"*

Bilişsel manipülasyonun en etkili ve sinsi yöntemlerinden biri kabul edilen "manipülasyon sandviçi", dezenformasyon operatörlerinin hedef kitlenin güvenini kazanmak ve eleştirel düşünme mekanizmalarını devre dışı bırakmak için içeriği katmanlı bir yapıda kurgulamasını ifade eder. Bu süreçte mesaj,

kaynağa karşı ilk güveni inşa eden tartışmasız ve %100 doğru bir bilgiyle (üst ekmek) başlatılır; güven sağlandıktan hemen sonra ise metnin merkezine asıl verilmek istenen manipülatif yalan veya çarpıtma (dolgu) yerleştirilir. Mesajın, içeriğin genel olarak güvenilir olduğu algısını pekiştiren bir başka doğru bilgiyle (alt ekmek) sonlandırılması sayesinde, doğruların arasına ustaca gizlenen bu yalan hedef kitlenin zihinsel filtrelerinden çok daha kolay ve dirençsiz bir şekilde geçerek fark edilmesini zorlaştırır.

Bağlamdan Koparma

"Bağlamdan Koparma" taktiği, özünde gerçek olan söz, görüntü veya olayların anlamını kökten değiştirecek şekilde sunulması prensibine dayanır; bu süreçte bir konuşmanın sadece belirli bir cümlesinin kesilmesi veya bir fotoğrafın zaman ve mekân bilgisi olmadan paylaşılması gibi yöntemler izlenir. Örneğin, barışçıl bir sivil protesto sırasında yaşanan kısa süreli bir arbede anı, eylemin genel barışçıl doğası yok sayılarak sanki tüm gösteri şiddet içeriyormuş gibi lanse edilebilir veya bir liderin mizahi bir ifadesi, bağlamından koparılarak tehlikeli bir beyanmış gibi sunulabilir. Bu taktiğin nihai amacı, yalan üretmekten ziyade var olan gerçekliği manipülatif bir algı yaratacak şekilde yeniden çerçevelemektir.

Savunma Mazereti Bilgisi

“Savunma mazereti bilgisi” (*information alibi*) veya "aynada suçlama" (*accusation in a mirror*) olarak bilinen bu taktik, saldırganın kendi planladığı eylemlerin sorumluluğunu henüz gerçekleşmeden düşmana yükleyerek kendini aklama ve suçlamayı savuşturma mekanizmasıdır. Bu süreçte saldırgan taraf, eyleme geçmeden önce kendi kontrolündeki medya kanalları üzerinden "Düşmanın X saldırısına hazırlandığına" dair yoğun bir propaganda kampanyası başlatır. Örneğin bir devlet, kritik altyapılara yönelik büyük bir siber

saldırı düzenlemeden hemen önce "Komşu ülkenin bize siber saldırı hazırlığında olduğuna dair istihbarat aldık" şeklinde haberler yayarak, saldırı gerçekleştiğinde kamuoyunun ve uluslararası toplumun suçu "düşmanda" aramasına zemin hazırlar. Bu stratejinin temel amacı; kamuoyunun dikkatini dağıtmak, gelecekteki suçlamalara karşı "önleyici yalan" üzerinden bir savunma hattı kurmak ve saldırganın kendi eylemlerine meşruiyet kazandırmaktır.

TEMEL ÇIKARIMLAR

Bu bölüm, bilgi güvenliği tehditlerinin basit bir "yalan haber" sorunundan, devlet destekli ve teknoloji odaklı "Sentetik Etki" operasyonlarına nasıl evrildiğini incelemektedir.

Temel Kavramlar ve Mekanizmalar

Sentetik Etki: tehdidin basit bir "yalan haber" olmaktan çıkıp, yapay zekâ ve teknoloji ile gerçeğin yeniden inşa edildiği çok katmanlı bir sürece evrildiğini ifade eder. Hedef, bireylerin muhakeme yeteneğini ve kurumlara güvenini aşındırarak bir "gerçeklik krizi" yaratmaktır.

FIMI: Dezenformasyondan farklı olarak, içeriğin doğruluğuna değil; davranışın manipülatifliğine, koordinasyonuna ve arkasındaki yabancı niyete odaklanan yeni güvenlik doktrinidir. Güvenlik birimleri artık ne söylendiğine, içerik değil, nasıl yayıldığına, davranış bakmaktadır.

Bilgiye Boğma (*Flooding*): Hedef kitleyi tek bir yalana inandırmak yerine, bilgi alanını çelişkili senaryolarla, gürültü doldurarak gerçeğin ayırt edilmesini imkânsız hale getirme taktiğidir.

5.1. KENDİNİZİ TEST EDİN

Soru 1: Avrupa Dış İlişkiler Servisi (EEAS) tarafından geliştirilen FIMI (Yabancı Bilgi Manipülasyonu ve Müdahalesi) doktrinini, geleneksel "dezenformasyon" yaklaşımından ayıran temel fark nedir?

A) Sadece sosyal medyada botlarla yaygınlaştırılması

B) Birçok yalan haber içermesi, bu şekilde iç içe geçmesi yalanlarla katmanlı bir etki yaratması

C) İçeriğin doğruluğundan ziyade, davranışın manipülatif ve eylemin yabancı koordineli olması

D) Sadece seçim dönemlerinde görülerek, etki yaratması

Soru 2: Yapay zekâ ve algoritmik yayılımın birleşimiyle oluşan yeni nesil tehdit kavramı nedir?

A) Siber zorbalık

B) Sentetik etki

C) Tık tuzağı

D) Sansür

Soru 3: Bilgi operasyonlarında kullanılan "koordineli sahte davranış" (CIB) ve "astroturfing" taktiklerinin temel stratejik amacı nedir?

A) İnternette yaygın bir ağ kurarak, bu ağdan faydalanıp, ürün satışı yaparak kar etmek

B) Sahte bir "halk desteği" algısı yaratarak, algoritmaları ve gerçek kullanıcıları manipüle etmek

C) Sadece eğlence amaçlı içerik üreterek, internet hızını yavaşlatmak

5.1. MERAKLISINA EK KAYNAKLAR

Bıçakcı, S. (2025). Sihirli reçete mi, kara kutu mu: Siber krizlere karşı esnek-dayanıklılık anlatısının incelenmesi. *REFLEKTİF Sosyal Bilimler Dergisi*, *6*(1), 59-80. https://doi.org/10.47613/reflektif.2025.202

European External Action Service. (2023, 12 Nisan). *Foreign information manipulation and interference (FIMI)* [Factsheet]. European Union. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

İldem, T. (2024). *Dezenformasyonla mücadelede toplumsal dirençliliğin güçlendirilmesi: Uluslararası kuruluşların ve özellikle NATO'nun rolü* (Politika Belgesi No 2). RESAID. https://resaid.bilgi.org.tr/politika-belgeleri/

Tuğtan, M. A. (2022). Hibrid savaşın sisi. *REFLEKTİF Sosyal Bilimler Dergisi*, *3*(2), 269-286. https://doi.org/10.47613/reflektif.2022.70

Bilgi Aklama Döngüsü ve Yapay Zekâ Araçları

Dijital çağın ilk evrelerinde dezenformasyon, genellikle bireysel trollerin veya küçük, fanatik grupların el yordamı ile yürüttüğü amatör bir faaliyetti. Ancak 2025 yılına geldiğimizde, karşımızdaki tablo tamamen değişmiştir. Bugün FIMI (Yabancı Bilgi Manipülasyonu ve Müdahalesi), tıpkı küresel bir otomotiv fabrikası veya lojistik devi gibi çalışan, endüstriyel ölçekli bir sektördür.

Bu sektörde, Ar-Ge departmanları, hedef kitle analizi yapar. Üretim bantları, Yapay Zekâ ile içerik üretimi sağlar. Dağıtım ağları, botnetler ve vekil sunuculardır. Bıçakcı'nın (2025) "Yapay Zekâ Çağında Bilişsel Güvenlik" raporunda vurguladığı üzere, bu dönüşümün en büyük motoru Üretken Yapay Zekâ (*GenAI*) olmuştur. Eskiden yüzlerce insanın günlerce çalışarak organize edebileceği bir etki operasyonu, bugün tek bir operatör ve gelişmiş bir büyük dil modeli (*Large Language Model*- LLM) ile dakikalar içinde, çok daha düşük maliyetle ve çok daha sofistike bir şekilde hayata geçirilebilmektedir.

Bu bölümde, manipülatif bir içeriğin "merdiven altı" bir forumdan çıkıp ulusal bir gazetenin manşetine nasıl taşındığını böylece bilgi aklamanın nasıl gerçekleştiğine bakacağız. YZ'nın insan taklidi yaparak güvenlik duvarlarını nasıl aşabildiğini ve devletlerin mesajlaşma uygulamaları üzerinden yürüttüğü "görünmez savaşları" inceleyeceğiz.

Finans dünyasındaki "kara para aklama" kavramı, suç gelirlerinin yasal sisteme sokularak kaynağının gizlenmesi sürecini anlatır. Bilgi güvenliği literatüründe kullanılan "bilgi aklama" kavramı da aynı mantıkla işler: Kaynağı düşman bir devlet istihbaratı olan manipülatif bilginin, bir dizi aracı (*proxy*) kullanılarak "yabancı" etiketinden arındırılması ve hedef ülkenin kamuoyunda "yerli, organik ve meşru" bir tartışma konusu haline getirilmesidir.

NATO StratCom COE ve EEAS analizlerine göre, başarılı bir Bilgi Aklama

operasyonu üç temel aşamadan oluşur: Yerleştirme, Katmanlama ve Bütünleştirme. İlk aşama olan yerleştirme bir psikolojik operasyonun (PsyOps) veya Yabancı Bilgi Manipülasyonu ve Müdahalesi (FIMI) kampanyasının fiilen başladığı, manipülatif veya dezenformasyon içeriğinin dijital ekosisteme kasıtlı olarak bırakıldığı hayati başlangıç evresidir.

Devlet aktörleri operasyonel içeriği asla kendi resmi, doğrulanabilir kanalları üzerinden yayınlamazlar. Büyükelçilik sosyal medya hesapları, Dışişleri Bakanlığı web siteleri veya resmi devlet haber ajansları gibi kaynakların doğrudan kullanılması, içeriğin anında devlet propagandası etiketi almasına neden olur. Bu durum, bilginin kitleler nezdindeki inandırıcılığını ve yayılma potansiyelini başlangıçta yok eder. Bu nedenle, operasyonun temel prensibi, bilginin kaynağını kasıtlı olarak bulanıklaştırmaktır. Bu bulanıklaştırma, hem devlete içeriği inkâr etme imkânı sunar hem de içeriğe organik bir köken görünümü vererek kitlesel yayılımını kolaylaştırır.

Manipülatif içerik, genellikle denetimin zayıf olduğu, anonimliğin yüksek olduğu ve filtrelenmemiş bilginin bir norm olarak kabul edildiği dijital alanlara bırakılır. Bu platformlar, denetim mekanizmalarını atlatmayı kolaylaştırır ve içeriğin hızla kök salmasını sağlar. Bu süreçte ilk olarak bir takım marjinal forumlar veya Reddit'in alt grupları ile Discord ve Telegram'daki kapalı kanallar kullanılarak içeriğin sanki halk arasında konuşulan organik bir gündem olduğu izlenimi yaratılır. Ardından, bu içeriğe dijital bir varlık kazandırmak ve ana akım medyanın atıf yapabileceği ilk kaynak bağlantısını- URL oluşturmak amacıyla, künyesi ve editörleri belirsiz gölge haber siteleri veya bloglar devreye sokulur. Son aşamada ise devlet bağlantılı yan medya organları, marjinal içerikle ana akım arasında bir köprü kurarak, devlet anlatılarını akademik analiz veya bağımsız gazetecilik maskesi altında meşrulaştırır.

Bu tohum ekme aşamasının yegâne ve en temel amacı, manipülatif bilginin internette bir URL veya dijital kimlik olarak var olmasını sağlamaktır.

Bu, operasyonun ilerleyen aşamalarında içeriğe atıfta bulunmak, "Bakın, internette bu konuda bir haber/analiz var" diyebilmek için zorunlu bir referans noktası oluşturur. Bu noktada bilgi henüz geniş kitlelere, ana akım medyaya veya etkili sosyal medya fenomenlerine ulaşmamıştır. Başarılı bir operasyon için bu tohumun sonraki aşamalarda filizlenmesi kritik önem taşır.

İkinci aşama olan katmanlama aşamasının temel amacı, bilginin operasyonel kaynağı, örneğin yabancı bir istihbarat servisi, ile bilginin toplum içindeki kabul edilebilirliği ve güvenilirliği arasındaki doğrudan bağı tamamen koparmaktır. Bu kopuş, dezenformasyonun bir yabancı propaganda olarak düşünülmesini zorlaştırarak yerel bir "hakikat" algısı yaratır.

Bilgi aklama sürecinin merkezinde, manipülatif içeriğin güvenilir yerel aktörler ve platformlar aracılığıyla "organik" ve "meşru" bir görünüm kazanmasını sağlayan ve Prakash (2025) tarafından tanımlanan "ağ bağlantılı meşruiyet" (*networked legitimacy*) mekanizması[60] yer almaktadır. Yabancı bir aktör, hedef ülkenin iç dinamiklerine sızmak ve kendi kimliğini gizleyen bir tampon bölge oluşturmak amacıyla yerel vekilleri devreye sokar. Bu ağın ilk grubunu, operasyonun kaynağını bilen ve genellikle maddi çıkar, ideolojik ortaklık veya siyasi nüfuz elde etme motivasyonuyla hareket eden marjinal medya ve yorumculardan oluşan "bilinçli işbirlikçiler" oluşturur. Ancak siber-etki operasyonlarının en büyük kaldıraç gücünü, manipülasyonun yabancı kaynağını bilmeden, sadece kendi dünya görüşlerini veya öfkelerini doğruladığı, onaylama yanılgısı için içeriği bir "hakikat" çağrısı olarak yayan "kullanışlı aptallar" (*useful idiots*) sağlar. Gerçek aktivistler veya sıradan vatandaşlardan oluşan bu kitle, mesaja halkın sesi niteliği kazandırarak yabancı kaynağın tespitini neredeyse imkânsız hale getirir.

---

[60] Prakash, P. (2025, Ekim). *Networked legitimacy: Disinformation, hate spin, and the overlooked pathways of foreign influence* [Konferans sunumu]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenya.

Bilginin kaynağını maskeleyen teknik ve sosyal yükseltme süreci, "tohumlama" aşamasıyla başlar; bu evrede operasyonel içerik öncelikle anonim imaj panoları veya kapalı Telegram grupları gibi izlenmesi zor, marjinal platformlara sızdırılır. Ardından, Graphika (2025) raporlarında da işaret edilen bot ağları devreye girerek "yapay büyütme" taktiğini uygular ve bu iddiayı ana akım platformlarda algoritmaların dikkatini çekecek bir hızda "trend topic" haline getirir. Sürecin en kritik evresi olan "yerelleştirme ve meşrulaştırma" aşamasında ise yerel bir influencer, amatör araştırmacı veya haber yorumcusu, botların yarattığı bu yapay hareketliliği gerçek bir kamuoyu tepkisi zannederek içeriği bulur ve kendi kitlesine uygun şekilde yeniden paketleyerek yayar.

Sürecin sonunda, dezenformasyonun kaynağı tamamen değiştirilmiştir. Eski kaynak artık "Yabancı İstihbarat" değil; yeni kaynak, hedef kitlenin güvendiği ve duygusal bağ kurduğu yerel bir figürdür: "popüler yerel YouTuber," "saygın gazeteci XXX," veya "mahallemizin aktivisti YYY." Bilginin kökeni birkaç katman derine itilmiş ve başarılı bir şekilde yerelleştirilmiştir. Hedef kitlenin algısında, haber artık yabancı bir propaganda değil, "bizden biri" olarak gördükleri, güvendikleri ve "gerçekleri söylediğine" inandıkları bir kanaldan gelmiştir. Bu durum, dezenformasyonun toplumsal direncini kırar ve kitleler tarafından hızla kabul edilmesini sağlar.

Üçüncü aşama olan bütünleştirme aşamasında, aklanmış bilgi artık meşru bir haber veya tartışma konusu olarak ana akım medyaya, siyasi partilerin gündemine veya meclis kürsüsüne girer. Saygın bir ulusal gazete veya televizyon kanalı, sosyal medyadaki bu yoğunluğu, botlarla şişirilmiş yapay bir yoğunluk olduğunu anlamadan fark eder. Haberi doğrulamadan, "Sosyal medyada dolaşan iddialara göre..." veya "Vatandaşlar tepkili..." başlığıyla verir. Bir bilgi, ana akım medyada yer aldığı veya bir milletvekili tarafından soru önergesi olarak verildiği anda, o bilginin yanlışlığını kanıtlamak

neredeyse imkânsız hale gelir. Çünkü bilgi artık kurumsal bir kimlik kazanmıştır. Bilgi aklama döngüsü tamamlanmış, zehir sisteme zerk edilmiştir.

Doppelgänger Operasyonu ve Kurumsal Güven Hırsızlığı

Avrupa Dış Eylem Servisi (EEAS) tarafından yayımlanan 2024 FIMI Raporu[61] bilgi manipülasyonu ve dış müdahale (FIMI) tekniklerinin evriminde kritik bir noktaya işaret etmektedir. Avrupa ve çevre coğrafyalarda en sık uygulanan ve etki gücü en yüksek olan yöntemlerden biri "ruh ikizi" anlamına gelen *doppelgänger* operasyonudur. Bu teknik, basit bir yalan haber üretme eyleminin çok ötesine geçerek, doğrudan halkın en güvendiği kurumsal yapılara, medya kuruluşlarına ait marka güvenini çalmaya odaklanan sofistike bir siber-bilişsel hileler bütünüdür. Doppelgänger, iki temel vektör üzerinden ilerler: Teknik altyapı hilesi ve bilişsel sömürü. Operasyonun teknik omurgasını oluşturan bu aşamada, saldırganlar hedef ülkenin en prestijli, güvenilir ve geniş kitlelere hitap eden medya kuruluşlarını hedef alır. Bu kuruluşların başında, *Le Monde, Bild, The Guardian, Der Spiegel* gibi Avrupa devleri ile *Hürriyet* veya *BBC Türkçe* gibi yerel ve uluslararası güvenilir yayıncılar gelmektedir. Operasyonun teknik omurgasını oluşturan Adres Benzerliği (*Typosquatting*) yöntemiyle saldırganlar, hedefledikleri prestijli kuruluşların web sitelerini tasarım, renk paleti ve mizanpaj açısından birebir kopyalayarak kullanıcının görsel hafızasını istismar ederler. Reset Tech (2025) [62] raporunda da vurgulandığı gibi, bu kusursuz taklidin en kritik farkı ise URL yapısında gizlenir; saldırganlar orijinal adreste (örneğin *lemonde.fr*) yapılan çok küçük bir harf değişikliği veya uzantı farkıyla (örneğin *lmonde.fr* veya *lemonde.news*)

[61] European External Action Service. (2024). *2nd EEAS report on foreign information manipulation and interference threats: A framework for networked defence*.

[62] Reset Tech. (2025). *The dormant danger: How Meta ignores large-scale inauthentic behavior networks of malicious advertisers*. Reset.tech.

sahte bir dijital gerçeklik inşa ederek kullanıcıları tuzağa düşürmektedir.

Klon sitelerin teknik altyapısı hazırlandıktan sonra, manipülatif içeriğin hedef kitleye ulaştırılması amacıyla geniş çaplı bir dağıtım ağı devreye sokulur. Reset Tech raporunda, bu içerikler genellikle Facebook reklamları, X bot ağları ve Telegram kanalları gibi yüksek erişimli platformlar üzerinden, kullanıcının güvendiği gazetenin orijinal görsel kimliği taklit edilerek yayıldığı bilgisi yer alır. Sosyal medya akışında bu tanıdık görsellerle karşılaşan kullanıcı, görsel hafızasının rehberliğinde hareket ederek, tıkladığı bağlantının her zaman takip ettiği güvenilir haber kaynağına ait olduğunu varsayar. Ancak kullanıcı sahte siteye ulaştığında, tasarım ve logo açısından tamamen meşru bir kaynakla karşılaştığını düşünse de okuduğu metin gerçek bir editoryal içerik değildir; bu metinler, EEAS (2024)[63] analizlerinde belirtildiği gibi, FIMI operatörleri tarafından "ekonominin çöktüğü" veya "dış desteğin kesildiği" gibi kriz temalı başlıklarla ülkenin iç ve dış politikasını etkilemek amacıyla kurgulanmış manipülatif dezenformasyonlardır.

Doppelgänger operasyonunun başarısı, insan zihninin doğal işleyişindeki kritik bir zaafı sömürmesine dayanır. Bölüm 2'de detaylı ele aldığımız Nobel ödüllü Daniel Kahneman'ın tanımladığı bilişsel ikili sistem devreye girer: Bu süreçte ilk olarak, hızlı, sezgisel ve otomatik tepkilerden sorumlu olan sistem 1 devreye girer; kullanıcı sosyal medyada tanıdık bir haber görseli veya logosu gördüğünde, beyin saniyenin altında bir hızla bu girdiyi işleyerek kaynağa "güvenilir" etiketini yapıştırır. Mantıksal analiz, şüphecilik ve detay kontrolünden, örneğin URL'deki harf hatasını fark etmekten sorumlu olan sistem 2 ise yavaş çalıştığı için, sistem 1'in yarattığı hızlı güven algısı karşısında devreye girme ihtiyacı hissetmez. Bu algısal körlük nedeniyle çoğu kullanıcı, okuduğu haberin doğruluğunu sorgulama veya adres

[63] European External Action Service (EEAS). (2024). *2nd EEAS report on foreign information manipulation and interference (FIMI) threats*. European Union.

çubuğundaki küçük manipülasyonu fark etme zahmetine girmeden bilişsel tuzağa düşmüş olur.

İZLE

"Doppelgänger" operasyonunun saygın medya kuruluşlarını nasıl taklit ettiğini ve bu dezenformasyon ağlarının arka plandaki işleyişini, uzman Camille François'nın anlatımıyla izleyebilirsiniz.

https://www.youtube.com/watch?v=NtAEv3KqORA

Doppelgänger tekniği, sadece yalan haber yaymakla kalmaz; en temel bilişsel mekanizmamızı hackleyerek, yalanı güvenilir bir ambalaj içinde sunar ve böylece halkın bilgi kaynaklarına duyduğu genel güveni sistematik olarak aşındırır. Bu durum, hibrit savaşın en etkili bilişsel harp taktiklerinden biri olarak kabul edilmektedir.

Yapay Zekâ ve İnsansı Kusurların Taklidi

2023 yılı öncesinde, sosyal medya manipülasyonu ve yabancı etki operasyonlarında (FIMI) kullanılan botlar teknolojik olarak ilkeldi. Bu botlar, genellikle aynı mesajı binlerce kez kopyalayıp yapıştıran, profil fotoğrafları "yumurta" ikonundan ibaret olan ve bu sayede hem platform algoritmaları hem de dikkatli kullanıcılar tarafından kolayca tespit edilip hızla silinen "aptal" otomasyonlardı. Ancak 2025 yılı itibarıyla, dijital alanında köklü bir değişim yaşanmıştır. Graphika'nın çığır açan "OrdinAIry People" raporunda detaylandırdığı üzere, YZ ve büyük dil modellerinin (*Large Language Models*-LLM) entegrasyonu sayesinde oyunun kuralları tamamen değişmiştir. Artık botlar, YZ marifetiyle "insanlaştırılmış" durumdadır. Bu yeni nesil botlar, bilişsel harp ve hibrit savaşın en etkili araçları haline gelmiştir.

Yeni nesil FIMI operasyonları, insan davranışının kusurlarını ve dilin

karmaşıklığını taklit ederek dijital savunma mekanizmalarını alt etmeye odaklanmıştır. Graphika'nın derinlemesine analiz ettiği, bazı operasyonlarda, yapay zekâ destekli hesapların kusursuz ve robotik bir dil kullanımından özellikle kaçındığı tespit edilmiştir. Bu hesaplar bilerek ve isteyerek hatalı gramer kullandığı, sık sık yazım yanlışları yaptığı, hatta cümle yapısını bozarak devrik ifadeler kullandığı ve konuşmalara argo kelimeler serpiştirdiği gözlemlenmiştir. Mükemmel, aşırı resmi, hatasız ve monoton bir dil kullanımı, modern sosyal medya algoritmaları ve uyanık kullanıcılar için doğrudan "bot" şüphesi uyandırmaktadır. Öte yandan, insana özgü hatalar içeren, yazım hatası yapan, cümleleri devrik kuran, bazen konuyla alakasız duygusal ve aşırı tepkiler veren, hatta mizah yapmaya çalışan bir hesap, çok daha ikna edici bir "gerçek insan" profili çizmektedir. Bu kasıtlı kusurluluk, botun tespit edilme ihtimalini düşürmektedir.

Yapay zekâ, klasik Turing Testi'nde olduğu gibi insan zekasını kusursuzca taklit etmek yerine, psikolojik bir dönüşümle "insani kusurları" taklit etme yolunu seçmiştir. Bu strateji, botların sosyal medyada sıradan bir kullanıcı gibi algılanarak dijital gözetim testlerinden başarıyla geçmesini sağlamaktadır.

Geleneksel FIMI operasyonlarında, hedef ülkenin dilini, örneğin Türkçe, Lehçe veya Svahili gibi ülkenin dilini mükemmel seviyede bilen ve operasyonu yürütecek insan operatörler istihdam etmek bir zorunluluktu. Bu durum, operasyonların ölçeğini ve coğrafi yayılımını kısıtlıyordu. Bugün ise büyük dil modelleri (LLM) ve üretken yapay zekâ araçları sayesinde bu kısıtlama tamamen ortadan kalkmıştır. Artık tek bir merkezden yönetilen az sayıda operatör, LLM araçlarını kullanarak, hedef dilin sadece gramerini değil; aynı zamanda o dilin kültürel kodlarına, popüler deyimlerine, yerel şakalarına, sokak jargonuna ve o anki politik bağlamına tamamen hâkim binlerce özgün ve bağlamsal içerik saniyeler içinde üretebilmektedir.

Bu teknolojik sıçrama, etki operasyonlarının ölçeklenebilirliğini daha önce görülmemiş, korkutucu boyutlara taşımıştır. Bir hedef ülkenin kamuoyunu manipüle etmek için gereken kaynak ve zaman maliyeti dramatik bir şekilde düşmüştür. Manipülasyon artık sadece metinle sınırlı değildir; ses ve görüntü gibi yüksek güvenilirlik atfedilen biçimler de hedef alınmaktadır. Yapay zekâ, "kanıt" olarak sunulan içeriği sentetik olarak üretme yeteneğine kavuşmuştur.

Özellikle seçim dönemleri veya siyasi kriz anlarında, etkili liderlerin seslerinin klonlanarak, sanki bir "gizli ortam dinlemesi" sonucu elde edilmiş gibi gösterilen sahte kayıtların hızla sızdırılması temel taktiklerdendir. Yapılan psikolojik araştırmalar, sesin, insan beyninde görüntüden bile daha yüksek bir "gerçeklik" ve "samimiyet" algısı yarattığını göstermektedir. Bu, kamuoyunu derinden sarsacak manipülasyonlar için ideal bir araçtır. Savaş veya büyük kriz anlarında, hedef ülkenin askeri veya sivil otoritelerini temsil eden üst düzey yetkili sahte kişilerin deepfake videoları ile askerlere "teslim olun" çağrısı yapılması veya halka "panik yayacak" yanlış bilgiler verilmesi amaçlanmaktadır. Bu sentetik kanıtlar, kritik karar verme anlarında kaosu artırmak ve düşmanın direncini kırmak için tasarlanmıştır.

Doğrudan Yayılım: Görünmez Tünel

Geleneksel dezenformasyon ve etki operasyonları, Twitter (X), Facebook ve Instagram gibi halka açık sosyal medya platformlarını, "kamusal meydan"ı hedef alıyordu. Ancak bu mecraların zamanla geliştirdiği algılama mekanizmaları, teyitçiler, platformların uyarı etiketleri ve içerik silme politikaları, devlet aktörlerinin etki alanını daralttı. Bu nedenle, Google Cloud Tehdit İstihbaratı'ndan Alden Wahlstrom'un (2025) analizlerine göre[64], devlet

[64] Wahlstrom, A. (2025, Ekim). *Direct dissemination tactics & precision targeted information operations* [Konferans sunumu]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenya.

aktörleri stratejik bir kayma yaşayarak daha mahrem ve denetimsiz dijital alanlara sızmaktadır. Bu yeni ve sinsi taktiğe "doğrudan yayılım" adı verilmektedir. Doğrudan yayılımın temel amacı, kitlelere yönelik genel bir yalan yerine, bireylerin en güvendiği kanallar aracılığıyla, kişiselleştirilmiş ve dolayısıyla yüksek güvenilirlikteki sahte bilgiyi doğrudan "gelen kutusuna" ulaştırmaktır. Doğrudan Yayılım taktiğinin uygulandığı ana saha, "karanlık sosyal" olarak adlandırılan dijital ortamlardır. Karanlık sosyal, paylaşımların kaynağının ya da yayılım zincirinin platformlar tarafından dahi takip edilemediği, uçtan uca şifreleme ile korunan veya özel iletişim kanallarını ifade eder. WhatsApp, Telegram, Signal gibi uçtan uca şifreli mesajlaşma uygulamaları bu alanın çekirdeğini oluşturur. Ayrıca, birebir iletişim kurulan e-posta ve SMS trafiği de dışarıdan denetlenemezliği nedeniyle karanlık sosyal kapsamında değerlendirilir. Kamusal meydanda yayılan bir yalan, teyitçiler, yapay zekâ algoritmaları veya diğer kullanıcılar tarafından hızla tespit edilebilir, uyarı etiketi alabilir veya kaldırılabilir. Karanlık sosyalde ise bu içerikler, platformlar tarafından erişilemediği için tamamen denetimsiz kalır ve yalanın yayılma hızını kesen hiçbir mekanizma devreye giremez.

Doğrudan yayılımın operasyonel işleyişi, Wahlstrom'un (2025) belirttiği üzere[65], hedef kitle üzerinde maksimum etki yaratmak amacıyla birbirini izleyen üç stratejik aşamadan oluşur. Süreç, saldırganların dark web veya sızıntılar yoluyla elde ettikleri büyük veri tabanlarını demografik ve politik filtrelere tabi tuttuğu hedefleme safhasıyla başlar. Ardından, elde edilen bu verilerle kurgulanan kişiselleştirilmiş mesajlaşma evresine geçilir; burada "Merhaba Ahmet" gibi isme özel hitaplar kullanılarak alıcının direnci kırılır ve mesajın sıradan bir spam olmadığı izlenimi yaratılır. Operasyonun finalinde ise güven inşası ve aciliyet devreye girer; "bankacı bir dosttan alınan gizli bilgi"

[65] Wahlstrom, A. (2025, Ekim). *Direct dissemination tactics & precision targeted information operations* [Konferans sunumu]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenya.

süsü verilmiş finansal manipülasyon örneklerinde olduğu gibi, mahrem alana sızan bu mesajlar birer dost tavsiyesi maskesiyle yüksek panik ve hızlı reaksiyon üretmeyi hedefler. Doğrudan Yayılım taktiği, iki temel sebepten dolayı geleneksel dezenformasyondan çok daha tehlikelidir:

Mesaj, kamusal meydanın kaotik ve güvensiz ortamında değil, kullanıcının en mahrem dijital alanı olan "gelen kutusunda" veya özel mesajlaşma uygulamasında belirir. Bu durum, bilginin bir "dosttan gelmiş" veya "özel olarak paylaşılmış" algısını güçlendirerek güvenilirlik seviyesini dramatik şekilde artırır. Alıcı, bilginin kaynağını sorgulamak yerine, acilen harekete geçme eğilimi gösterir. Bu yöntemle yayılan yalanlar, kamuya açık bir alanda olmadığı için yetkili kurumlar, sivil toplum örgütleri veya teyit mekanizmaları tarafından anında fark edilemez. Yetkililer, manipülasyonun gerçekleştiğini ve yalanın yayıldığını ancak kriz patlak verdiğinde, örneğin, yüz binlerce insanın bankaya koşup döviz çekmeye çalışması gibi somut bir toplumsal kaos yaşandığında fark edebilir. Bu gecikme, saldırının etkisinin katlanarak artmasına neden olur.

Uyuyan Hesaplar ve Hizmet Olarak Dezenformasyon

Reset Tech (2025) raporu, dezenformasyon ve etki operasyonlarının "Aktör" bileşeninde dikkat çekici bir profesyonelleşme ve ticarileşme sürecini gözler önüne sermektedir.[66] Geleneksel "trol orduları" modelinin ötesine geçilmiş, daha sofistike ve tespit edilmesi zor aktör tipleri ortaya çıkmıştır. Sosyal medya platformlarının güvenlik algoritmaları, genellikle yeni açılmış, sıfır takipçili, bir günlük geçmişe sahip hesaplara karşı doğal bir şüpheyle yaklaşır ve bunları hızlıca işaretleyebilir. Saldırganlar bu engeli aşmak için strateji

[66] Reset Tech. (2025). *The dormant danger: How Meta ignores large-scale inauthentic behavior networks of malicious advertisers*. Reset.tech.

değiştirmiştir. Operasyonel aktörler, yıllar önce açılmış, düzenli olarak gerçek paylaşımlar yapmış, dolayısıyla platform nezdinde "güvenilirlik puanı" yüksek olan gerçek kullanıcı hesaplarını hedef alır. Bu hesaplar ya kimlik avı veya kötü amaçlı yazılımlarla ele geçirilir ya da özel karaborsalardan doğrudan satın alınır.

Ele geçirilen bu hesaplar, operasyonun başlayacağı kritik güne kadar pasifize edilir ve "uyuyan hücre" misali sessizce bekletilir. Bu bekleme süresi, hesapların algoritmalara yakalanma riskini en aza indirir. Kritik bir eşikte, örneğin, seçim günü, büyük bir terör saldırısı sonrası veya jeopolitik bir kriz anında bu hesapların tamamı birden aktive edilir ve koordine bir şekilde FIMI mesajını yaymaya başlar. Hesapların "uzun geçmişi" ve "organik tarihçesi" olduğu için, platformların yapay zekâ ve denetim algoritmaları bunları sıradan bot veya yeni açılmış hesaplar kadar kolayca engellemekte veya kaldırmakta zorlanır, bu da dezenformasyonun yayılım hızını ve etkisini artırır. Artık dezenformasyon, devletler, siyasi partiler veya kurumsal rakipler için "kendi ellerini kirletmeden" elde edebilecekleri bir dış kaynak hizmetine dönüşmüştür. "Team Jorge" gibi uluslararası skandallarda görüldüğü üzere, bu alanda uzmanlaşmış özel şirketler küresel bir pazar oluşturmuştur.

Günümüzde dezenformasyon ekosistemi, müşterilerin ihtiyaçlarına özel "paket programlar" satın alabildiği ve geleneksel e-ticaret işlemlerine benzer bir işleyişe sahip olan ticari bir yapıya dönüşmüştür. Bu "hizmet olarak dezenformasyon" pazarında sunulan seçenekler arasında; 5.000 adet onaylı ve yüksek etkileşimli hesapla koordine yayılım sağlamak, belirli bir konuyu iki gün boyunca dünya gündeminde tutacak trend topic çalışmaları yürütmek ve hedef alınan kişi ya da kurumları itibarsızlaştırmak için üretilmiş deepfake içerikler temin etmek yer almaktadır. Etki operasyonlarının ölçeğini ve erişilebilirliğini artıran bu ticarileşme, devlet dışı aktörlerin dahi sofistike FIMI operasyonları düzenlemesine olanak tanıyarak siber güvenlikten ulusal

güvenliğe kadar uzanan çok boyutlu yeni bir tehdit ortamı oluşturmaktadır.

TEMEL ÇIKARIMLAR

Bu bölüm, dezenformasyonun bir "içerik" sorunundan çıkarak endüstriyel bir "operasyonel sürece" nasıl dönüştüğünü analiz etmektedir. Aşağıdaki kavramlar, yabancı devlet aktörlerinin ve siber suç ağlarının dijital ekosistemi manipüle etmek için kullandığı teknik altyapıyı ve yöntemleri tanımlar.

Temel Kavramlar ve Mekanizmalar

Bilgi Aklama (*Information Laundering*): Kaynağı düşman bir devlet istihbaratı veya yasa dışı bir örgüt olan manipülatif bilginin, bir dizi aracı (vekil/proxy) kullanılarak "yabancı" etiketinden arındırılması ve hedef ülkenin kamuoyunda "yerli, organik ve meşru" bir tartışma konusu haline getirilmesi sürecidir. Bu süreç üç aşamada gerçekleşir.

Ağ Bağlantılı Meşruiyet (*Networked Legitimacy*): Manipülatif bilginin, hedef kitle tarafından güvenilir kabul edilen yerel aktörler (influencerlar, aktivistler, yerel gazeteciler) tarafından paylaşılmasıyla kazandığı yapay güvenilirliktir. Bu mekanizma sayesinde dış kaynaklı bir operasyon, "halkın sesi" veya "taban hareketi" gibi görünür.

Operasyon Doppelgänger ve Typosquatting (*Adres Benzerliği*): Rusya bağlantılı aktörlerce sıkça kullanılan bu teknik, hedef ülkenin en güvenilir medya kuruluşlarının (Örn: *Le Monde, Bild, Hürriyet*) web sitelerinin birebir kopyalanmasını içerir.

YZ Kamuflajı ve "Kötü Gramer" (*AI Camouflage / Bad Grammar*): Graphika'nın "OrdinAIry People" raporunda tanımlandığı üzere, yeni nesil yapay zekâ botlarının tespit edilmemek için "kusursuz

makine dili" yerine, bilerek yazım hataları yapması, argo kullanması ve duygusal tepkiler vererek "gerçek insan" taklidi yapması stratejisidir. Bu taktik, platformların otomatik bot yakalama algoritmalarını atlatmak için geliştirilmiştir.

Doğrudan Yayılım (*Direct Dissemination*): Dezenformasyonun halka açık sosyal medya platformları ("kamusal meydan") yerine; e-posta, SMS, WhatsApp veya Telegram gibi şifreli ve denetlenemeyen "karanlık sosyal" (dark social) kanalları üzerinden, kişiselleştirilmiş mesajlarla doğrudan bireylerin gelen kutusuna iletilmesidir. Bu yöntem, "içeriden bilgi" veya "dost tavsiyesi" süsü verilerek yüksek güven ve aciliyet hissi yaratır.

Uyuyan Hesaplar (*Dormant Accounts*): Saldırganların yeni hesap açmak yerine, yıllardır kullanılmayan ancak geçmişte gerçek paylaşımlar yapmış "eski ve güvenilir" hesapları ele geçirip (hackleyip) veya satın alıp, operasyon gününe kadar pasif tutmasıdır. Operasyon anında bu hesaplar "uyandırılır" ve platformların güvenlik filtrelerine takılmadan içerik yayar. Bu yöntem Reset Tech tarafından "uyuyan tehlike" olarak tanımlanmıştır.

5.2. KENDİNİZİ TEST EDİN

Soru 1: "Bilgi aklama" döngüsünde, dezenformasyonun asıl kaynağını gizlemek ve operasyona yerel bir "ağ bağlantılı meşruiyet" kazandırmak amacıyla kullanılan aracı aktörlere ne ad verilir?

A) Editörler

B) Kullanışlı aptallar

C) Yazılımcılar

D) Teyitçiler

Soru 2: EEAS raporlarında vurgulanan ve *Le Monde* veya *Bild* gibi güvenilir medya kuruluşlarının web sitelerini birebir kopyalayarak (URL hilesi/typosquatting) "marka güvenini çalmayı" hedefleyen teknik hangisidir?

A) Phishing

B) DDoS saldırısı

C) Doppelgänger

D) Ransomware

Soru 3: Graphika'nın 2025 raporuna göre, yapay zekâ destekli botların "robotik" görünmekten kaçınmak ve güvenlik filtrelerine yakalanmadan "gerçek insan" taklidi yapabilmek için ne taktiği kullanır?

A) Hiç yorum yapmama, sessiz kalma

B) Sadece emoji kullanarak, duyguları yansıtma

C) Bilerek gramer hataları yapma, kusurlu davranma

D) Sadece akademik dil kullanarak, kavramları tanıtma

5.2. MERAKLISINA EK KAYNAKLAR

EUvsDisinfo. (2025, 5 Aralık). *The rise of the disinformation-for-hire industry*. https://euvsdisinfo.eu/the-rise-of-the-disinformation-for-hire-industry/

European External Action Service. (2025). 3rd EEAS report on foreign information manipulation and interference threats: Exposing the architecture of FIMI operations. European Union.

İnsan Zihni, Bilişsel Harp ve Nöro-Teknolojik Tehditler

Savaş tarihi, çatışma alanlarının sürekli genişlemesinin bir kronolojisidir. İnsanlık önce karada, sonra denizde savaşmayı öğrendi. 20. yüzyılda gökyüzü ve uzay, 21. yüzyılın başında ise siber alan birer çatışma sahası olarak doktrinlere girdi. Ancak 2020'lerin ortalarına geldiğimizde, NATO ve büyük askeri güçler, savaşın altıncı ve belki de en belirleyici operasyonel alanını resmen tanımladılar: İnsan Zihni. Bir önceki bölümde incelediğimiz yapay zekâ botları, deepfake videoları ve klonlanmış haber siteleri, kendi başlarına birer amaç değildir; bunlar sadece birer "taşıyıcı sistemdir". Bu sistemlerin taşıdığı savaş başlığı ise Bilişsel Harp taktikleridir.

NATO Müttefik Dönüşüm Komutanlığı'nın (ACT) tanımına göre Bilişsel Harp; *"insan beyninin bilgi işleme mekanizmalarını hackleyerek, bireylerin ve toplumların algılarını, düşüncelerini ve nihayetinde davranışlarını değiştirmeyi amaçlayan"* bir savaş türüdür.[67] Amaç artık bir ülkenin topraklarını fiziksel olarak işgal etmek değildir; o ülkede yaşayan insanların gerçeklik algısını işgal etmektir. Eğer düşmanınızın ne düşüneceğini ve nasıl hissedeceğini kontrol edebiliyorsanız, tek bir kurşun atmadan savaşı kazanmışsınız demektir. Sun Tzu'nun *"Savaşmadan kazanmak en büyük zaferdir"* düsturu[68], bugün nöro-bilimsel bir gerçekliğe dönüşmüştür.

Bilişsel harp kavramı, sıklıkla geleneksel Psikolojik Harekât (*PsyOps*) veya kamu diplomasisi ile karıştırılsa da çağımız güvenlik ve savunma doktrinlerinde bu kavramların ayrı ve farklı stratejik düzeyleri temsil ettiği kabul edilmektedir. NATO'nun yeni nesil savaş doktrinleri, bu üç disiplin arasındaki yapısal ve stratejik farkları net bir şekilde ortaya koymaktadır. Bilişsel harp,

---

[67] Claverie, B., & du Cluzel, F. (2022). *Cognitive Warfare: The Future of Cognitive Dominance*. NATO Science & Technology Organization.

[68] Tzu, S. (2018). *Savaş sanatı*. Salon Yayınları.

temelde bir evrim ve derinleşmedir; hedef kitlenin sadece davranışını değil, bilişsel mimarisini hedef alır.

Tablo 5.3.1. *Stratejik iletişimden bilişsel harbe: Amaç, hedef ve yöntem farklılıkları*

Özellik	Psikolojik Harekât (PsyOps)	Kamu Diplomasisi	Bilişsel Harp
Amaç Düzeyi	Taktiksel ve Eylemsel	Stratejik ve İmaj Odaklı	Stratejik, Bütüncül ve Zihinsel Yapı Odaklı
Zamanlama	Kısa vadeli, kriz veya çatışma zamanları	Orta ve uzun vadeli, barış zamanı	Sonsuz, kesintisiz (7/24), barış/kriz/savaş ayrımı yok
Hedef Kitle	Tanımlı, sınırlı ve spesifik gruplar (Örn: Düşman askerleri)	Uluslararası kamuoyu, karar vericiler	Tüm toplum, tüm bireyler ve kurumlar
Hedeflenen Değişim	Kısa vadeli tutum ve davranış değişikliği	İmaj, güven ve sempati yaratma	"Nasıl düşünüldüğünün" ve "bilginin nasıl işlendiğinin" kalıcı değişimi

Geleneksel PsyOps, genellikle belirli bir zamanda, sınırlı bir coğrafyada ve tanımlı bir hedef kitleye yönelik, kısa vadeli bir tutum değişikliği yaratmayı amaçlar. Odak noktası, anlık eylemsel sonuçlardır. PsyOps, özellikle çatışma bölgelerinde veya askeri operasyonlar sırasında etkinleşir. Örneğin bir çatışma bölgesinde düşman askerlerine "teslim olun, güvendesiniz" broşürleri atmak veya radyo yayını yapmak. Bu eylemlerin amacı askerin o anki davranışını, savaşmayı bırakıp teslim olmayı tetiklemektir. Elde edilen tutum değişikliği, genellikle operasyonel ortam sona erdiğinde kalıcılığını yitirir.

Bilişsel harp, *PsyOps*'un çok ötesinde, hedef kitlenin sadece neye inandığını değil, "nasıl düşündüğünü," "bilgiyi nasıl filtrelediğini" ve "karar verme mekanizmalarını" değiştirmeyi amaçlayan bütüncül bir stratejidir. Amacı, toplumsal bağışıklık sistemini kalıcı olarak zayıflatmaktır. Bilişsel harp,

toplumsal belleğe, kolektif mantık yürütme biçimine ve gerçeği ayırt etme yeteneğine saldırır. Toplumun kendi gerçekliğini sorgulamasını hedefler. Temel stratejik hedef, toplumun bilişsel dayanıklılığını kırmaktır. Bu, vatandaşların bilgi kirliliğine, manipülasyona ve kutuplaşmaya karşı direncini sıfırlamayı amaçlar. Kamu kurumlarına, hükümet, ordu, medya, yargı olan güvenin kalıcı olarak yok edilmesi, Bilişsel Harbin en kritik başarı kriteridir. Güvenin yıkıldığı bir toplum, dış müdahaleye karşı savunmasız hale gelir. Ele aldığımız üzere bu sentetik etki, toplumun dışarıdan görünmez bir programlamayla kendi kendine zarar vermeye-kutuplaşma, iç çatışma, ekonomik panik, sosyal infial gibi olaylara itilmesidir. Düşman, artık dışarıda değil, toplumun kendi içindeki çatlaklarda ve bireylerin zihinlerindedir.

Bilişsel Harp, geleneksel savaş ayrımı tanımaz. Barış zamanı, kriz zamanı veya sıcak çatışma ayrımı yoktur; 7/24 devam eden, sonsuz ve sınırları belirsiz bir süreçtir. Savaş, artık akıllı telefonunuza gelen her bildirimle, her sosyal medya akışıyla ve her manipülatif haber başlığıyla devam etmektedir. Bilişsel alan, sürekli ve kesintisiz bir muharebe alanına dönüşmüştür.

Biyolojik Açıklar

Siber güvenlik terminolojisinde donanım için *hardware* ve yazılım için *software* kullanılır. Bilişsel güvenlik ve modern enformasyon savaşı disiplininde ise insan beyni, biyolojik yapısına atfen *wetware*, biyolojik/ıslak donanım olarak adlandırılır. Bu, insan zihninin, tıpkı bir bilgisayar sistemi gibi, belirli mantıksal ve biyolojik "açıklara" sahip olduğu varsayımına dayanır. Nasıl ki her bilgisayar yazılımında bir *bug*, hata veya bir "arka kapı" bulunabilirse, insan beyninin milyonlarca yıllık evrimsel süreci boyunca hayatta kalmayı sağlamak üzere oluşmuş ancak modern dijital ortamda saldırganların istismar edebileceği "bilişsel açıklar" mevcuttur. FIMI operatörleri, bu açıkları istismar etmek için nörobilim, davranışsal psikoloji ve sosyal mühendislik

prensiplerini bir silah olarak kullanır. Amaç, rasyonel karar mekanizmasını bypass ederek kitlelerin duygu durumları ve ön yargıları üzerinden manipülasyonu sistemli bir şekilde gerçekleştirmektir.

İnsan beyni, ikinci bölümde detaylı olarak ele aldığımız üzere, temel olarak hayatta kalmaya programlanmış bir organdır. Evrimsel olarak acil bir tehdit algılandığında, örneğin yırtıcı bir hayvanla karşılaşma, mantıklı düşünme, analiz yapma, sonuçları öngörme ve otokontrolden sorumlu olan prefrontal korteksi devre dışı bırakır. Bu durum, kaynağı sorgulama veya eleştirel analiz gibi enerji tüketen süreçlerin durdurulması anlamına gelir. Bu esnada, ilkel ve hızlı tepkilerden (savaş, kaç veya don) sorumlu olan amigdala kontrolü ele alır. İkinci bölümde aktardığımız üzere bu duruma amigdala haczi denir. Dezenformasyon ve manipülasyon içerikleri, bu biyolojik mekanizmayı hedef alacak şekilde tasarlanır. İçerikler asla "nötr", "sakinleştirici" veya "sıkıcı" değildir. Aksine, kişide aşırı ve yoğun duygusal tepkiler uyandıracak şekilde kurgulanır.[69]

Birey, bu tür bir haberi gördüğünde biyolojik olarak "savaş ya da kaç" moduna zorlanır. Bu "tehdit tepkisi" anında eleştirel düşünme, kaynak sorgulama veya şüphe etme yetisi fiziksel ve kimyasal olarak imkansızlaşır. Haber veya paylaşımın içeriği değil, yarattığı duygusal şok önemlidir. Bu duygusal yükten kurtulmanın en hızlı yolu, bilgiyi hızla başkalarına aktarmaktır. Sosyal medyada "paylaş" butonuna basmak, beyin için evrimsel olarak bir "rahatlama" eylemi olarak algılanır. Bu mekanizma, yalanların viral hızda yayılmasının temel biyolojik sebebidir. Doğrulama yanlılığı, bireyin, zaten sahip olduğu inançları, değerleri veya grup görüşlerini destekleyen bilgileri tercih etme, hatırlama ve bu bilgilere daha yüksek değer biçme eğilimidir. Beynimiz, ait olduğumuz grubun görüşlerini destekleyen bir bilgi ile karşılaştığında

[69] NATO StratCom COE. (2025). *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty*.

bunu bir "ödül" olarak işler. Buna karşın, mevcut inançlarla çelişen veya kabilenin görüşlerine karşı çıkan bilgiler ise fiziksel acı, tehdit veya dışlanma riski gibi algılanır. Dijital platformlardaki algoritmalar ve özellikle bot ağları, bu yanlılığı güçlendirerek bireyleri yankı odalarına hapseder. Birey, bu odalarda yalnızca kendi görüşünü onaylayan, kendi duygusal tepkilerini körükleyen ve kendi kabilesinin sesini yansıtan içeriklere maruz kalır.

BİLGİ KUTUSU

Öncelik Etkisi: İnsan beyni, bir konu hakkında duyduğu ilk bilgiye inanma ve onu "referans noktası, çıpa" (*anchor)* olarak kabul etme eğilimindedir. Kriz anlarında ilk yalanı söyleyen taraf, algıyı çıpalar. Sonradan gelen doğrulamalar veya yalanlamalar, zihinde yer etmiş bu ilk bilgiyi sökmekte zorlanır. Çünkü beyin, ilk bilgiyi "gerçek", sonradan geleni ise "o gerçeği değiştirmeye çalışan bir müdahale" olarak kodlar.

Safsata Tufanı (G*ish Gallop*): Adını tartışmacı Duane Gish'ten alan bu taktik, rakibi veya izleyiciyi, yanıtlayamayacağı kadar çok sayıda, art arda, yarı-doğru, tutarsız veya tamamen uydurma iddialara boğma yöntemidir. Amaç bir tartışmayı mantıkla kazanmak değil, karşı tarafı "savunma moduna" hapsetmektir. Her bir yalanı çürütmek dakikalar alırken, yalanı söylemek saniyeler sürer. İzleyici, bu bilgi bombardımanı karşısında yorulur ve "Ateş olmayan yerden duman çıkmaz, bu kadar çok iddia varsa birkaçı doğrudur" yanılgısına düşer.

Sen de yancılık / "Ama onlar da..." Taktiği (W*hataboutism*): Sovyet döneminden kalma bu klasik taktik, yöneltilen bir eleştiriye cevap vermek veya o eleştiriyi çürütmek yerine, suçlayıcıya karşı tamamen farklı bir suçlamayla karşılık verme sanatıdır. "Evet, biz bu hatayı yaptık ama bak siz de geçmişte şunu yapmıştınız" diyerek konuyu saptırır. Bu taktik, beynin ahlaki yargılama mekanizmasını felç eder. Amaç haklı çıkmak değil, her iki tarafın da "kirli" olduğu algısını yaratarak gerçeğin değerini sıfırlamaktır.

Çerçeveleme (F*raming*): Olguların sunuluş biçimini değiştirerek, algılanış biçimini manipüle etmektir. Aynı olayı aktarırken seçilen kelimeler, zihinsel bir çerçeve çizer. Örneğin, bir grubu "özgürlük savaşçıları" olarak nitelendirmek ile "yasadışı militanlar" olarak nitelendirmek, okuyucunun o gruba dair tüm duygusal tepkisini baştan belirler. Manipülatörler, olayları kendi anlatılarına uygun "çerçevelerin" içine yerleştirerek sunar, böylece izleyici resmi sadece o pencereden görür.

FIMI aktörleri bu mekanizmayı, toplumda doğal olarak var olmayan suni ayrımlar yaratarak kullanır. Amaç, insanları bu yapay kimlikler üzerinden kutuplaştırmak ve birbirine düşman etmektir. Bu strateji, toplumsal dokuyu parçalayan klasik "böl ve yönet" stratejisinin modern ve dijital ortama uyarlanmış halidir. Sosyal uyumu ve kolektif rasyonelliği bozarak devletlerin iç istikrarını hedef alır. Hakikat Yanılsaması Etkisi, bir bilginin mantıksal içeriğinden veya gerçekliğinden bağımsız olarak ne kadar çok ne kadar farklı kaynaktan ve ne kadar sık tekrar edilirse, beynin onu o kadar "tanıdık" ve dolayısıyla "doğru olma ihtimali yüksek" olarak kodlaması olgusudur. İnsan beyni, enerji tasarrufu ilkesiyle çalışır ve her bir bilgiyi yeniden detaylı bir eleştirel analize tabi tutmak yerine, "tanıdıklık" seviyesini bir güvenilirlik göstergesi olarak kullanmaya eğilimlidir. Bir iddia tekrar tekrar duyulduğunda, beyin bu iddiayı zaten işlediği ve "güvenli" bir bilgi olarak etiketlediği için eleştirel filtreyi zayıflatır.

Bir önceki bölümde detaylandırılan koordineli sahte davranış (*Coordinated Inauthentic Behavior*-CIB) yürüten bot ordularının ve trol ağlarının temel işlevi tam olarak budur. Tek bir yalanı, kısa süre içinde milyonlarca kez tekrarlayarak ve farklı sahte kaynaklar üzerinden dolaşıma sokarak, beynin "aşinalık filtresini" hacklerler. Bu sistematik tekrarlama, yalanın zihinde gerçeğin yerine ikame edilmesini sağlar ve bilişsel harp sahasının en etkili silahlarından biridir. Doğrulama yanlılığının yanı sıra, profesyonel FIMI operatörleri insan zihninin bilgi işleme süreçlerindeki şu spesifik "yazılım hatalarını" (*bugs*) istismar eder.

Nöro-Teknolojik Tehditler: Zihnin “Şeffaflaşması”

Bilişsel harbin evrimi, sadece psikolojik manipülasyon ve sosyal mühendisliğin sınırlarını aşarak, insan zihninin biyolojik ve nörolojik katmanlarına

doğru ilerlemektedir. Bu yeni ve ürkütücü aşama, "nöro-savaş" (*neuro-warfare*) kavramıyla somutlaşmaktadır. Bu tehdidin boyutları, 2025'te EU DisinfoLab konferansında Virginia Mahieu tarafından sunulan "Neurotech, AI & Disinformation" başlıklı çığır açıcı raporda detaylıca gözler önüne serilmiştir.[70] Rapor, gelecekteki bilgi operasyonlarının (FIMI) temel hedefinin, bireylerin düşünce süreçlerini ve duygusal durumlarını gerçek zamanlı olarak izlemek ve manipüle etmek olacağını işaret etmektedir. Günümüzde kullandığımız akıllı saatler, fitness takipçileri, hatta beyin dalgalarını (EEG) ölçen gelişmiş kulaklıklar ve gelecekte yaygınlaşacak olan Beyin-Bilgisayar Arayüzleri (BCI), insan zihnini dışarıdan erişilebilir, ölçülebilir ve analiz edilebilir bir veri kaynağına dönüştürmektedir. Bu cihazlar, nörolojik sinyallerimizi dijitalleştiren bir köprü görevi görmektedir

DİNLE

BBC World Service tarafından hazırlanan ve dezenformasyonun küresel ölçekte nasıl bir stratejik araca dönüştüğü ve devletlerin bu karmaşık ağlarla nasıl mücadele ettiğinin tartışıldığı *The Real Story: Information Wars* başlıklı bölümünü dinleyebilirsiniz.

Dinlemek için:
https://www.bbc.com/audio/play/w3cswx1g

Mevcut sosyal medya platformları ve dijital ekosistem, kullanıcıların tıklamaları, beğenileri ve izleme süreleri gibi davranışsal verilerini analiz ederek psikometrik profiller oluştursa da nöro-teknolojik devrimle birlikte bu süreç radikal bir evrim geçirmektedir. Yakın gelecekte, nöro-teknolojik cihazlar sayesinde toplanacak olan kalp atış hızı (HRV), galvanik deri tepkisi (GSR) ve göz bebeği büyümesi gibi otonom sinir sistemi verileri, bireylerin anlık stres, öfke veya rahatlama düzeylerini açıkça ortaya koyacaktır. Bu hassas veri

[70] Mahieu, V. (2025, 16 Ekim). *Neurotech, AI & disinformation: Risks on the horizon* [Conference presentation]. EU DisinfoLab 2025 Conference, Ljubljana, Slovenia.

madenciliği süreci ayrıca, EEG sinyalleri ve olaya ilişkin potansiyeller (ERP) aracılığıyla beyin dalgası tepkilerini (alfa, beta, teta, gama) ölçerek, hangi uyaranın beyinde tam olarak ne tür bir bilişsel tepki yarattığının tespit edilmesine olanak tanıyacaktır. Bu veri madenciliğinin asıl tehlikesi, düşüncelerimiz kelimelere dökülmeden, hatta tam olarak şekillenmeden analiz edilebilmesidir. Örneğin, bir siyasi liderin konuşmasını, bir reklam kampanyasını veya bir dezenformasyon haberini izlerken, beyninizin hangi bölümünün, korku merkezi olan amigdala mı, yoksa güven ve ödül merkezinin mi aktif olduğu anlık olarak ölçülebilir. Bu, 2016'daki Cambridge Analytica skandalının çok daha derin, nörolojik ve biyolojik bir versiyonudur. Artık bir bireyin psikolojik hassasiyetleri sadece davranış tahminleriyle değil, biyolojik kanıtlarla tespit edilebilecektir. Bir kişi bir fikri beğenmediğini söylese bile, nöro-verileri gerçekte korktuğunu veya inandığını ortaya çıkarabilir.

Nöro-veri madenciliği ile elde edilen derin profiller, bilgi operasyonlarını yürüten FIMI aktörlerinin saldırı stratejilerini kökten değiştirerek hedefi soyut kitlelerden bireyin anlık biyolojik ve duygusal durumuna kaydırmaktadır. Bu süreçte yapay zekâ destekli sistemler, kullanıcının nöro-teknolojik cihazlarından akan kalp atış hızı, stres seviyesi ve EEG sinyalleri gibi gerçek zamanlı verileri sürekli analiz etmektedir. Sistem, bu veriler ışığında bireyin yorgun, stresli, öfkeli veya bilişsel yük altında olduğu savunmasız anları hassasiyetle tespit edebilmektedir. Bilişsel direncin en düşük olduğu bu kritik anlar saptandığında, sistem tam zamanlı bir senkronizasyonla devreye girerek, bireyin nöro-profiline göre en yüksek etkiyi yaratacak manipülatif içeriği, dezenformasyon veya propagandayı kullanıcının dijital akışına düşürmekte ve saldırıyı kişiselleştirmektedir. Bu strateji, "bilişsel mikro-hedefleme" olarak adlandırılır. Geleneksel mikro-hedefleme sadece demografik ve psikografik verilere dayanırken, bilişsel mikro-hedefleme, saldırıyı bireyin o anki biyolojik ve bilişsel zayıflık noktasına göre zamanlar ve optimize eder.

Bu düzeyde bir hassasiyetle uygulanan bilişsel saldırılar, bireyin karar verme yetisine sızarak, demokratik süreçleri, kamuoyunu ve nihayetinde ulusal güvenliği görünmez bir şekilde tehlikeye atma potansiyeli taşımaktadır. Nörosavaş, modern savaşın en kişisel ve sinsi cephesini temsil etmektedir.

TEMEL ÇIKARIMLAR

Bu bölüm, savaşın fiziksel coğrafyalardan, insan zihninin "bilişsel mimarisine" kayan operasyonel bir evrimini anlatmaktadır.

Temel Kavramlar ve Mekanizmalar

Bilişsel Harp: İnsan beyninin bilgi işleme mekanizmalarını "hackleyerek" algı, düşünce ve davranışı değiştirme stratejisidir.

Wetware (Islak Donanım): İnsan beyninin evrimsel süreçle şekillenmiş biyolojik yapısının, siber güvenlik terminolojisindeki "donanım/yazılım" analojisiyle ele alınmasıdır. Bu yaklaşım, zihnin belirli mantıksal ve biyolojik "açıklara" sahip olduğunu varsayar.

Nöro-Savaş (*Neuro-Warfare*): Bilgi operasyonlarının (FIMI) ulaştığı en ileri aşamadır. Bireyin duygusal durumlarını ve düşünce süreçlerini; kalp atış hızı, göz bebeği büyümesi ve EEG sinyalleri gibi biyometrik veriler üzerinden gerçek zamanlı izleyip manipüle etmeyi hedefler.

Bilişsel Mikro-Hedefleme: Bireyin akıllı saat gibi nöro-teknolojik cihazlarından alınan anlık verilerle, öfkeli, stresli, yorgun, en savunmasız olduğu anlarının tespit edilip, o ana özel manipülatif içeriğin dijital akışa düşürülmesidir.

5.3. KENDİNİZİ TEST EDİN

Soru 1: NATO'nun tanımladığı "Bilişsel Harp" ile geleneksel "Psikolojik Harekât" (*PsyOps*) arasındaki temel fark nedir?

A) Biri askerleri hedefler, diğeri ise özellikle sivilleri hedef alır.

B) PsyOps kısa vadeli ve taktikseldir; diğeri ise stratejiktir, süreklidir ve beynin işleyişini hedef alır.

C) Biri internet aracılığı ile gerçekleşir, diğeri ise radyoyu temel iletişim aracı olarak seçer, radyo üzerinden yaygınlaştırmayı gerçekleştirir.

D) Aralarında bir fark yoktur.

Soru 2: İnsan beyninin, tehdit veya öfke anında mantıklı düşünme merkezini olan prefrontal korteksi devre dışı bırakıp duygusal tepki merkezini devreye sokması durumuna ne ad verilir?

A) Amigdala haczi

B) Dopamin orucu

C) Placebo etkisi

D) Stockholm sendromu

Soru 3: Tartışmalarda rakibi mantıkla yenmek yerine; onu yanıtlayamayacağı kadar çok sayıda, art arda, yarı-doğru veya tamamen uydurma iddiaya boğarak "savunma moduna" hapsetmeyi amaçlayan taktik aşağıdakilerden hangisidir?

A) Sen de yancılık / "Ama onlar da..." taktiği (*Whataboutism*)

B) Çerçeveleme (*Framing*)

C) Safsata tufanı (*Gish gallop*)

D) Öncelik etkisi

5.3. MERAKLISINA EK KAYNAKLAR

Pomerantsev, P. (2019). This is not propaganda: Adventures in the war against reality. Hachette UK.

Bilişsel Güvenlik ve Toplumsal Direnç

2010'lu yıllar, ulusal güvenlik mimarisinin temel taşlarını, altyapısal siber savunma üzerine oturtmuştu. Devletlerin ve kritik sektörlerin, enerji santralleri, finansal sistemler, telekomünikasyon ağları, siber güvenlik yatırımları, esasen bu fiziksel ve mantıksal altyapıyı korumaya odaklanmıştı. Bu dönemin temel güvenlik varsayımı, basit bir prensibe dayanıyordu: "Eğer güvenlik duvarı (firewall) ve diğer teknik savunma katmanları yeterince güçlüyse, düşman içeri sızamaz, sistem bütünlüğü korunur." Bu yaklaşım, tehdidi dışarıdan gelen bir yazılım veya kod saldırısı olarak tanımlıyordu. Ancak, 2020'lerin ortalarına, özellikle de 2025 yılına geldiğimizde, güvenlik ortamının bu eski varsayımı tamamen geçersiz kılındı. FIMI operasyonları ve gelişmiş hibrit savaş stratejileri, bu teknik savunma hattını, doğrudan atlayarak etkisiz hale getirmiştir. Günümüzün sofistike saldırganları, değerli zamanlarını karmaşık sunucuları veya veri tabanlarını hacklemekle harcamamakta; onun yerine, o sunucuları kullanan, yöneten ve nihayetinde devlet adına karar alan insanları hacklemektedir. Bu, hedefi sistemden insan beynine kaydıran devrimsel bir değişimdir. Bu yeni tehdit ortamı, ulusal güvenlik doktrinlerinde köklü bir terminoloji ve strateji değişikliğini zorunlu kılmaktadır. İhtiyaç duyulan şey, sadece siber savunmanın güçlendirilmesi değil, bilişsel güvenlik (*Cognitive Security-CogSec*) alanının ulusal stratejinin merkezine alınmasıdır.

Bilişsel Güvenlik'in temel amacı, klasik sansür mekanizmalarının aksine, bilgi akışını kısıtlamak veya manipüle etmek değildir. Tam tersine, bilgi ekosistemini "sentetik etki"ye bir başka deyişle yapay olarak üretilmiş dezenformasyon, deepfake, algoritmik manipülasyona karşı dayanıklı ve dirençli hale getirmektir. Bu, bireylerin ve toplumun, “hibrit savaşın sisi”ne rağmen kendilerine sunulan bilginin kaynağını, amacını ve geçerliliğini

sorgulama yeteneğini güçlendirmeyi hedefler. Bu paradigmik kayma, savunma konseptinin tanımını temelden değiştirmektedir. Savunma, artık sadece ağları izleyen veya sınırları koruyan "teknik" bir görev olmaktan çıkmış; çok katmanlı, entegre bir "stratejik, hukuki ve sosyolojik" devlet politikasına dönüşmüştür.

İZLE

Doç. Dr. Salih Bıçakcı'nın *Siber Güvenlik ve Yeni Dünyanın Yeni Problemi* başlıklı konuşmasını dinleyebilirsiniz. İzlemek için:
https://www.youtube.com/watch?v=0WpUiTyn7fE

Yeni güvenlik çağında, bir ülkenin savunma bakanlığının veya ulusal istihbarat teşkilatının başarısı sadece askeri gücü, siber altyapısının sağlamlığı veya fiziksel sınırlarının güvenliğiyle ölçülmeyecektir. Asıl başarı kriteri, vatandaşlarının zihinsel bütünlüğünü, toplumsal uyumunu ve eleştirel karar alma yeteneğini bilgi harp sahasının yıkıcı etkilerinden ne kadar koruyabildiği olacaktır. Bilişsel harp, bir ülkenin sivil iradesini felç etmeyi amaçladığı için, bilişsel güvenlik, modern ulus devletin bekası için hayati bir zorunluluk haline gelmiştir.

FIMI-ISAC ve Bilgi Paylaşımı Ağları

Dezenformasyonun sınır tanımayan, anlık ve viral doğası, geleneksel savunma mekanizmalarını işlemez kılmaktadır. Bugün Polonya'da bir seçim öncesi uygulanan sofistike bir manipülasyon taktiği, ertesi gün modifiye edilmiş bir versiyonuyla Fransa'daki bir halk sağlığı krizinde kullanılabilmektedir. Bu hız ve adaptasyon kabiliyeti, savunmanın da ulusal sınırları aşan, ulus-üstü ve hayati önem taşıyan tüm sektörleri kapsayan bir koordinasyonla yürütülmesini zorunlu kılar.

Bu ihtiyaca somut bir yanıt olarak, Katarina Klingova'nın (EU

DisinfoLab, 2025) sunumunda detaylandırdığı FIMI-ISAC (*Foreign Information Manipulation and Interference-Information Sharing and Analysis Center*) modeli öne çıkmaktadır.[71] Bu model, bilgi kirliliği ve manipülasyonla mücadelede iş birliğinin somutlaşmış, operasyonel bir örneğidir.

Geleneksel istihbarat servislerinin çalışma prensibi, bilgiyi gizli tutma ve kaynağı koruma eğilimine dayanır. Ancak FIMI mücadelesinde, bilginin değeri saklandıkça azalır, paylaşıldıkça katlanarak artar. Erken tespit edilen bir manipülasyon kampanyası hakkında bilgi paylaşımı yapılmadığı takdirde, aynı kampanya kısa süre sonra başka bir ülkede başarılı olabilir. FIMI-ISAC modeli, bu paradoksu kırarak aşağıdaki kilit aktörleri operasyonel bir iş birliği masasında bir araya getirir:

Devlet Kurumları (Hükümetler, Dışişleri, Güvenlik Birimleri): Tehdidin nihai hedefini ve jeopolitik boyutunu en iyi bilen, diplomatik ve hukuki tepki mekanizmalarını devreye sokabilecek aktörlerdir.

Sosyal Medya ve Teknoloji Platformları (Meta, X, Google vb.): Manipülasyonun gerçekleştiği dijital altyapının sahipleridir. Kampanyaya ait ham veriye, hesap bilgileri, etkileşim metrikleri ve en önemlisi, bot ağlarını ve zararlı içerikleri platformdan silme (*takedown*) butonuna sahip olan yegâne oyunculardır.

Akademi ve Sivil Toplum Kuruluşları: Genellikle sahada, yerel dilde ve en erken aşamada tehdidi tespit eden saha gözlemcileridir. Hükümetlerin erişmekte zorlandığı bağımsız veriye ve topluluk düzeyinde derinlemesine analize sahiptirler. Bu STK'lar, manipülasyonun yerel kültüre özgü nüanslarını ortaya çıkarır. Bu disiplinler arası ve ulus-üstü yapı, bir ülkede tespit edilen bir manipülasyon kampanyasının Taktik, Teknik ve Prosedürler-

[71] Klingova, K. (2025). *FIMI-ISAC & its FIMI defenders: Collective defense for democracy* [Konferans sunumu]. EU DisinfoLab Conference.

TTP'lerinin anında diğer tüm üye ülkelere ve platformlara bildirilmesini sağlar. Örneğin, bir bot ağının kullandığı yapay zekâ ile oluşturulmuş profil fotoğrafı yaratma algoritmasının benzersiz deseni tespit edildiğinde, bu "dijital parmak izi" anında ağdaki tüm savunucularla paylaşılır ve saldırının küresel ölçekte, henüz yayılmadan bloklanmasını mümkün kılar.

Siber güvenlik alanında saldırganların eylemlerini kategorize etmek için MITRE ATT&CK çerçevesi nasıl temel bir standartsa, bilişsel güvenlik ve dezenformasyon analistleri için de DISARM (*Disinformation Analysis and Risk Management*) çerçevesi aynı derecede kritik bir rol üstlenmektedir. DISARM, FIMI saldırılarını standart, evrensel bir dille kodlama ve sınıflandırma sistemidir. DISARM, saldırganın eylemini tanımlayan standart kodlar sunar. Örneğin, "T0075: Manipüle edilmiş görsel kullanımı" bir taktik kodu iken, "T0082: Sahte uzman (*pseudo-expert*) kullanımı" ise başka bir manipülasyon tekniğini ifade eder. "S0010: Kaynağın itibarsızlaştırılması" da bir stratejiyi belirtebilir. Bu ortak dil ve kodlama sistemi sayesinde, farklı ülkelerdeki savunmacılar bir saldırıyı aynı terminolojiyle, hızlı ve net bir şekilde analiz edebilir. En önemlisi, yapay zekâ destekli savunma sistemleri, bu standart kodlara göre eğitilebilir. Bir saldırı keşfedildiğinde, sistemler hızlıca bu kodlarla etiketlenmiş saldırılara karşı otomatik savunma protokollerini devreye sokar. Bu, savunmanın saldırganın dilini konuşması ve böylece ondan bir adım önde olması için hayati bir ön koşuldur. Bu koordineli ve standartlaştırılmış yaklaşım, dağınık ve birbirinden habersiz savunma çabalarının ötesine geçerek, küresel bir tehdide karşı organize ve ölçeklenebilir bir direnç mekanizması oluşturur.

Güvenin Korunması ve Kurumsal Dayanıklılık

Bilişsel güvenliğin en can alıcı ve zorlu cephesi, bir devletin toplumsal algıdaki "güven çıpası" olarak işlev gören kilit kurumlarının FIMI operasyonlarına

karşı savunulmasıdır. Mariana Diaz Garcia'nın (UNICRI, 2025) ve Max Bernhard'ın (2025)[72] derinlemesine saha ve analiz çalışmaları, bu kritik kurumların özellikle seçim kurulları, nükleer enerji alanındaki yetkililer ve sağlık otoriteleri gibi toplumsal istikrarı doğrudan etkileyen yapıların nasıl bir bilişsel savaş alanına dönüştüğünü ve savunma stratejilerinin ne olması gerektiğini net bir şekilde ortaya koymaktadır. Seçimler, devletlerin bilişsel savaş bağlamında karşı karşıya kaldığı FIMI operasyonlarının adeta "şampiyonlar ligi finali"dir. Saldırganların birincil amacı, sanılanın aksine, belli bir adayı kazandırmak veya kaybettirmekten öte, seçim sisteminin kendisine ve temel demokratik sürece olan toplumsal güveni temelden yıkmaktır. Bu strateji, devletin meşruiyetini sarsmayı ve kronik siyasi kutuplaşmayı derinleştirmeyi hedefler. Saldırganlar genellikle rasyonel kanıtlarla çürütülmesi zor, duygusal ve şüphe uyandıran anlatıları kullanır: "Oylar çalınıyor", "Sistem baştan aşağı hileli kurgulandı", "Ölüler ve hayali seçmenler oy kullandı" gibi iddialar, özellikle seçim sonuçlarının netleşmediği gergin anlarda hızla yayılır ve kitlesel psikolojik etki yaratır. Seçim kurullarının geleneksel kapalı süreç yönetimini terk etmesi ve oyların nasıl sayıldığı, tutanakların nasıl birleştirildiği, veri akışının güvenliği gibi teknik süreçleri halkın anlayabileceği en basit dilde, sürekli ve tekrarlı olarak anlatması hayati öneme sahiptir. Bu, sadece süreç güvenliğini değil, süreç algısının güvenliğini de sağlar.

Seçim günü veya hemen sonrasında ortaya atılan her türlü bilişsel saldırı iddiasına karşı, anında harekete geçebilecek "dijital kriz masaları" kurulmalıdır. Amaç, ortaya atılan bir dezenformasyonun saatler değil, dakikalar içinde resmi, görsel ve doğrulanabilir verilerle, örneğin onaylı tutanak görseli, kamera kaydı, blokzincir tabanlı doğrulama kanıtı vb. çürütülmesini

[72] Bernhard, M. (2025). *German elections under attack: Lessons learned for fact-checking and FIMI investigations* [Sunum]. Correctiv.

sağlamaktır. Zira bilişsel savaşta, sessizlik, şüphenin ve yalanın yayılması için en elverişli ortamı yaratır.

Toplumsal infiali en hızlı tetikleyen bilişsel saldırılar, fiziksel tehdit algısı üzerinden yapılanlardır. Tıpkı gerçek olmayan bir nükleer sızıntı dedikodusu veya abartılı bir salgın hastalık haberi gibi, bu tür senaryolar toplumda ani ve kontrolsüz paniğe, kaosa ve devlet otoritesine karşı güvensizliğe yol açabilir. Mariana Diaz Garcia (2025)[73], radyolojik, biyolojik ve nükleer dezenformasyonun (*CBRN Disinfo*) doğrudan toplumsal panik ve kaosu tetiklemek üzere FIMI aktörleri tarafından aktif olarak kullanıldığını bilimsel çalışmalarla kanıtlamıştır. Kriz anlarında işleyen temel kural şudur: "Bilgi boşluk kabul etmez." Eğer nükleer enerji alanındaki yetkililer, sağlık bakanlığı, afet kurumu gibi ilgili kurumlar ve/ya resmi otorite bir krizin ilk 1 saati içinde net, tutarlı ve güvenilir bir dille konuşmazsa, o boşluğu FIMI aktörleri, korku ve panik yaratan yalanlar, komplo teorileri ve abartılı senaryolarla dolduracaktır.

Bıçakcı'nın savunduğu üzere, devletlerin sadece dezenformasyonu "yalanlama" reaksiyonuyla yetinmesi yeterli değildir.[74] Aksine, kendi "pozitif, güçlü ve veriye dayalı anlatısını" aktif olarak kurması gerekmektedir. Pasif bir savunma pozisyonunda kalmak, bilişsel maçı kaybetmeye mahkumdur. Kritik olan, doğru bilgiyi, yalandan daha hızlı, daha akılda kalıcı, daha duygusal ve daha etkileyici bir formatta sunarak bilişsel alanda inisiyatifi ele almaktır. Veri görselliği, infografikler ve uzman onayları bu anlatı üstünlüğünün temel araçlarıdır.

---

[73] Diaz Garcia, M. (2025). *Institutional resilience against nuclear and radiological disinformation* [Sunum]. UNICRI.

[74] Bıçakcı, S., 2025. s.2

Hukuki Kalkanlar ve Düzenlemeler: "Brüksel Etkisi"

Bilişsel güvenliğin sağlanmasında ve enformasyon savaşlarına karşı koymada bireysel sorumluluk ve kurumsal iletişim stratejileri hayati öneme sahip olsa da savaşın asıl yapıldığı meydan olan dijital platformların özel şirketlerin mutlak kontrolünde olması, mücadeleyi zorlaştıran temel bir paradoksu ortaya koyar. Bu nedenle, devletlerin ve uluslararası yapıların en caydırıcı ve etkin silahlarından biri, platformların gücünü dengeleyen ve hesap verebilirliği sağlayan "Hukuk" mekanizmasıdır. Hukuk, teorik bir araç olmaktan çıkıp, bilişsel güvenliğin en somut ve zorlayıcı kalkanı haline gelmiştir.

Avrupa Birliği'nin (AB) kabul ettiği ve Joe McNamee[75] gibi uzmanlarca yakından analiz edilen Dijital Hizmetler Yasası (DSA), dijital altyapının işleyişine köklü bir müdahale niteliği taşıyarak modern dünyanın "internet anayasası" olarak kabul edilmektedir. Bu yasa, büyük teknoloji platformlarının kamusal alandaki etkilerini düzenleyerek, bilişsel harp ve FIMI tehditleriyle mücadelede yeni bir dönemi başlatmıştır.

DSA'nın en devrimci maddelerinden biri, teknoloji devlerini, platformlarının temel işleyiş mekanizması olan algoritmaları konusunda şeffaflığa zorlamasıdır; bu kapsamda platformlar, öneri sistemlerinin nasıl işlediğini ve hangi kriterlere göre içerik sunduğunu detaylıca ifşa etmek zorundadır. Ayrıca, özellikle dezenformasyon ve nefret söylemi içeren içeriklerin neden hızla yayılarak "viral" hale geldiğini bilimsel bir temelde izah etmeleri istenmektedir. Seçim manipülasyonu, halk sağlığına yönelik tehditler veya bilişsel güvenlik riskleri gibi "sistemik risklerin" nasıl yönetildiği ve bu risklere karşı hangi proaktif tedbirlerin alındığı şeffaf bir denetime açılarak, platformların karar alma süreçlerindeki "kara kutu"nun perdesinin aralanması ve keyfi

[75] McNamee, J. (2025). *Policy ketchup: Update on EU digital regulations* [Konferans sunumu]. EU DisinfoLab.

uygulamaların önüne geçilmesi hedeflenmektedir. DSA, yalnızca platformların kendi raporlarına güvenmek yerine, bağımsız araştırmacıların ve sivil toplum kuruluşlarının, özellikle FIMI tehditlerine karşı çalışan platformların işleyişini dışarıdan denetlemesini sağlayacak mekanizmalar sunar.

Yetkilendirilmiş ve akredite edilmiş araştırmacıların, platformların kural ihlallerini, dezenformasyonun yayılma hızını ve algoritmik etkileri inceleyebilmesi için anonimleştirilmiş ve gizliliğe uygun şekilde platform verilerine erişimi zorunlu kılınır. Bu, bilginin akışını kontrol eden platformların kendi kendini denetlemesi yerine, dışarıdan bağımsız ve akademik bir gözle denetlenebilmesine imkân tanır.

Hukuki düzenlemelerin caydırıcılığı, uygulanan yaptırımların sertliğiyle doğrudan ilişkilidir. DSA, platformların kurallara uymasını sağlamak için son derece güçlü bir mali baskı mekanizması oluşturmuştur. Yasanın gerekliliklerini yerine getirmeyen ve özellikle sistemik riskleri yönetmede başarısız olan platformlara, küresel yıllık cirolarının %6'sına varan devasa oranlarda cezalar kesilebilir. Bu ölçekteki bir yaptırım potansiyeli, dezenformasyonla ve bilişsel harp unsurlarıyla mücadeleyi, platformlar için bir "kurumsal sosyal sorumluluk" ya da "iyi niyet" meselesi olmaktan çıkarıp, doğrudan bir "mali zorunluluk" ve "hukuki uyum" meselesi haline getirir. Şirketler, kâr marjlarını korumak adına, bilişsel güvenliği tehdit eden içerikleri ve algoritmik zaafları öncelikli olarak ele almak zorunda kalır. Özetle, DSA gibi hukuki düzenlemeler, bilişsel güvenliği özel şirketlerin etik kararlarına terk etmek yerine, devletlerin ve uluslararası birliğin zorlayıcı gücüyle platformları kamu yararına hizmet etmeye ve enformasyon manipülasyonuna karşı etkin bir savunma hattı kurmaya mecbur bırakmaktadır.

"Bütüncül Toplum" Yaklaşımı ve Topyekün Savunma

Geleneksel savunma anlayışının sınırları, bilgi operasyonları ve hibrit savaş

tehditlerinin karmaşıklığı karşısında zorlanmaktadır. Bu yeni ortamda, EEAS (Avrupa Dış Eylem Servisi) raporlarında ve özellikle Kuzey Avrupa (Finlandiya, İsveç) ulusal güvenlik doktrinlerinde öne çıkan en güçlü ve etkili model, savunmanın yalnızca devletin tekelinden çıkarılıp tüm topluma bir sorumluluk olarak yayılmasıdır. Bu yaklaşım, stratejik direnç inşa etmenin temel taşı olarak kabul edilir ve "topyekûn savunma" olarak adlandırılır. Bu model, yalnızca askeri caydırıcılığı değil, aynı zamanda toplumsal bilişsel alanı korumayı da hedefleyen, çok katmanlı bir yaklaşım gerektirir. Devlet, sivil toplum ve medya arasında net sorumluluk alanları tanımlanarak, sinerjik bir savunma hattı oluşturulur. Bu savunma hattının en kritik devlet ayağını, siyasi etkiden arındırılmış uzman kuruluşlar oluşturur.

Psikolojik Savunma Kuruluşları

Bu ajansların görevi, eleştirel düşünceyi köreltmek veya "halka ne düşüneceğini söylemek" değildir. Temel misyonları, ulusal güvenlik çıkarları doğrultusunda, dış kaynaklı, kasıtlı manipülasyon ve yanlış bilgi akımlarına karşı halkı erken uyarmaktır. Bu mekanizmalar, spekülasyon veya panik yaratmaktan kaçınarak, yalnızca teyit edilmiş operasyonları şeffaf bir şekilde ifşa eder. Bir "Yalan Hortumu" gibi çalışarak, yayılan manipülatif bilginin etkisini hızla minimize etmeyi hedeflerler. Bu uzman kuruluşların bağımsızlığı, güvenilirliklerinin sürdürülmesi için hayati öneme sahiptir.

Kriz İletişimi ve Stratejik Açıklık

Devletin, büyük bir FIMI operasyonu sırasında güvenilirliğini koruması esastır. Bu, şeffaf, tutarlı ve tek sesli bir kriz iletişimi stratejisi ile mümkündür. Bilgiyi saklamak yerine, doğru bilgiyi hızla ve anlaşılır bir şekilde yaymak, dezenformasyonun yayılma hızını keser. Devletin bürokratik yapısının veya resmi söyleminin ulaşmakta zorlandığı toplumsal katmanlarda, sivil toplum

kuruluşları ve bağımsız yapılar hayati bir savunma hattı kurar.

Doğrulama Platformları ve Araştırmacılar

Bağımsız doğrulama platformları, yayılan yanlış bilgiyi sistematik olarak çürüterek, dezenformasyonun viral etkisini azaltır. Bağımsız araştırmacılar, manipülasyon kampanyalarının arkasındaki aktörleri, yöntemleri ve hedefleri ortaya çıkarır.

Medya Okuryazarlığı ve Eğitim Dernekleri

Bu yapılar, eleştirel düşünce yeteneğini ve dijital okuryazarlığı toplumun en temel seviyesine yayarak, bireyleri manipülasyona karşı daha dirençli hale getirir. Bu, pasif bir "savunma" değil, aktif bir "bilişsel bağışıklık" inşa etme sürecidir.

Finansal ve Editoryal Bağımsızlık Dengesi

Devlet, bu yapıların hayati önemini kabul etmeli ve faaliyetlerini desteklemelidir. Ancak bu destek, editoryal bağımsızlığa veya yayın içeriğine müdahale etme hakkını vermemelidir. Aksi takdirde, bu sivil yapılar hızla "devlet propagandası" damgası yer, güvenilirliklerini kaybeder ve en önemlisi işlevsizleşerek düşmanın hedeflediği etkiye ulaşmasına yol açar. Geleneksel medya, FIMI operasyonlarının etkilerini katlayarak artıran veya azaltan merkezi bir role sahiptir.

Gazetecilik Etiği ve Eğitim

Gazetecilerin, farkında olmadan bir FIMI operasyonunun parçası olmaları veya manipülatif bir iddiayı meşrulaştırmaları, Bilgi Aklama döngüsüne girmeleri riski yüksektir. Bu riski minimize etmek için gazetecilere yönelik özel eğitimler kritik öneme sahiptir.

Kaynak Sorgulama Prensibi

Bir iddiayı haberleştirirken, bilginin kaynağını derinlemesine sorgulamak, içeriğin doğruluğu kadar, kaynağın motivasyonu ve geçmişini de araştırmayı gerektirir. Ulusal güvenlik boyutu olan bir bilgi operasyonu söz konusu olduğunda, bu sorgulama, basit bir editoryal süreçten çıkarak, ulusal güvenliğin bir parçası haline gelir. Manipülasyonun yayılmasına aracılık etmektense, haberi yayımlamama sorumluluğu, doğrulanamayan veya yabancı bir operasyona hizmet eden iddialarda bazen en doğru eylemdir.

TEMEL ÇIKARIMLAR

Bu bölüm, ulusal güvenliğin teknik bir "siber" sorundan, toplumsal ve bilişsel bir "direnç" sorununa nasıl evrildiğini özetlemektedir.

Temel Kavramlar ve Mekanizmalar

Güvenlik Paradigmasının Yeni Merkezi: Geleneksel güvenlik anlayışı sunucuları ve sınırları korumaya odaklanırken; yeni doktrin sistemleri yöneten insanların zihinsel bütünlüğünü ve karar alma mekanizmalarını "sentetik etki"ye karşı korumayı merkeze almaktadır. Tehdit artık donanımı değil, "ıslak donanım" (*wetware*) olarak adlandırılan insan zihnini hedeflemektedir.

Hiyerarşiden Ağ Tabanlı İş Birliğine Geçiş: Devletlerin hiyerarşik ve bürokratik yapıları, otonom ve hızlı hareket eden FIMI ağlarına (botlar, troller) karşı tek başına yetersiz kalmaktadır. Etkin bir savunma için devlet kurumları, teknoloji platformları ve sivil toplumun entegre olduğu, tehdit istihbaratının anlık paylaşıldığı (FIMI-ISAC) "kolektif bir ağ yapısı" zorunludur.

Stratejik İletişim ve Proaktif Bilgilendirme: Kriz anlarında (seçim, afet vb.) kurumların sessiz kalması veya gecikmesi, manipülasyonun yayılmasına zemin hazırlayan en büyük risk faktörüdür. Savunma stratejisi, sadece yalanlamaya değil; doğru, hızlı ve şeffaf bilgi akışıyla bilgi boşluğunu doldurmaya ve "bilişsel inisiyatifi" ele almaya dayanmalıdır.

Düzenleyici Denetim ve Algoritmik Şeffaflık: "Brüksel etkisi" ve Dijital Hizmetler Yasası (DSA) örneğinde görüldüğü üzere; teknoloji platformlarının algoritmik şeffaflığa zorlanması ve sistemik riskler nedeniyle mali olarak sorumlu tutulması, tekil içerik silme çabasından çok daha caydırıcı ve sonuç alıcı bir yapısal çözümdür.

5.4. KENDİNİZİ TEST EDİN

Soru 1: "FIMI-ISAC" ve benzeri yapıların bilişsel güvenlikteki temel işlevi nedir?

A) Sansür uygulamak

B) Devlet kurumları arasında gizli iletişimi sağlamak ve çeşitli araçlarla mesajın yaygınlaşmasını sağlamak

C) Devlet, özel sektör ve sivil toplum arasında tehdit istihbaratını ve saldırı tekniklerini gerçek zamanlı paylaşmak

D) Sosyal medya hesaplarını kapatmak

Soru 2: Kriz anlarında dezenformasyonun çok hızla yayılmasının başlıca sebebi nedir?

A) İnternet hızının artması

B) Yetkili kurumların sessiz kalarak yarattığı bilgi boşluğu

C) Yardım ekiplerinin sahaya acil müdahalesi için mesajlaşmanın çok yoğun olması

Soru 3: Avrupa Birliği'nin Dijital Hizmetler Yasası (DSA) gibi düzenlemeler, dezenformasyonla mücadelede hangi stratejik değişimi temsil eder?

A) Hatalı kullanıcıları ağır bir biçimde cezalandırmak

B) Sorumluluğu bireyden alıp, algoritmaları ve platformları hesap verebilirliğe zorlamak

C) İnternete erişimi kısıtlamak ya da interneti tamamen kapatarak, paylaşımı engellemek

D) Devletlerin kendi sosyal medya platformlarını kurmasını sağlamak

5.4. MERAKLISINA EK KAYNAKLAR

European Commission. (2025, 10 Ekim). *The impact of the Digital Services Act on digital platforms*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms

Bölüm 6

Toplumsal Bağışıklık: Eğitim, İletişim ve Psikolojik Savunma

🎯 TARTIŞMA SORULARI

1. Zihnimizi yalanlara karşı önceden aşılamak mümkün mü?
2. Psikolojik aşılama nedir ve bilgi düzensizliklerine karşı nasıl çalışır?
3. Ön-çürütme ve geleneksel teyitçilik arasındaki farklar nelerdir?
4. Oyunlaştırma, geleneksel eğitimlerden daha kalıcı sonuçlar verebilir mi?
5. En yakınımız yalan bir habere inandığında nasıl ikna ederiz?

Giriş

Bilgi düzensizlikleri çağında, sadece doğruyu yanlıştan ayırmak artık yeterli değildir; asıl mesele, manipülasyona karşı zihinsel bir zırh kuşanmaktır. Bu bölüm, dezenformasyonla mücadeleyi bir adım öteye taşıyarak, bireyleri ve toplumları pasif birer bilgi tüketicisi olmaktan çıkarıp, bilişsel açıdan dirençli ve aktif savunuculara dönüştüren stratejileri mercek altına almaktadır. Okuyucu, "ön-çürütme" (*prebunking*) yöntemlerini, manipülasyonu bizzat deneyimleterek öğreten oyunlaştırma tekniklerini ve kutuplaşmış zihinlerdeki direnci aşmayı sağlayan iletişim modellerini keşfedecektir. Bölüm boyunca, hayati önem taşıyan yanal okuma becerisinden yapay zekâ okuryazarlığına kadar uzanan bir yelpazede, demokratik hakları ve özgürlükleri korumak için gerekli olan yetkinlikler ve çözüm önerileri bütüncül bir çerçevede sunulacaktır.

Psikolojik Aşılama ve Ön-Çürütme

Geleneksel teyitçilik ve doğrulama faaliyetleri, yanlış bilginin yayılımının yol açtığı bilgi ekosistemindeki kirliliğin temizlenmesi ve kamusal güvenin korunması için şüphesiz hayati öneme sahiptir. Bu çabalar, yanlış iddiaları çürütmek, bağlamlarını açıklığa kavuşturmak ve doğru bilgiyi sunmak suretiyle bilgi kirliliğiyle mücadelede önemli bir rol oynar. Ancak, yapılan araştırmalar, bu yöntemlerin doğası gereği "reaktif", tepkisel olduğunu ve yanlış bilgi savaşında üstesinden gelinmesi gereken iki büyük yapısal sorunla karşı karşıya kaldığını net bir şekilde göstermektedir.[76]

[76] Lewandowsky, S., & van der Linden, S. (2021). Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology*, *32*(2), 348–384. https://doi.org/10.1080/10463283.2021.1876983

Bunlardan birincisi Hız Asimetrisi olarak adlandırılır: Yanlış bilgi, doğru ve doğrulanmış bilgiden çok daha hızlı, daha duygusal ve dolayısıyla çok daha geniş bir alana yayılma eğilimindedir. MIT'nin yaptığı araştırmalar, yalan haberlerin doğrulardan altı kat daha hızlı yayıldığını ve derinlere nüfuz ettiğini ortaya koymuştur. Mark Twain'e atfedilen o meşhur ve zamansız sözde olduğu gibi, *"Gerçek daha ayakkabılarını bağlarken, yalan dünyayı üç kez dolaşır."* Düzeltme metni ve teyit raporu yayınlandığında, hedef kitle çoktan yanlış bilgiye yoğun bir şekilde maruz kalmış, hatta bu yanlış bilginin yarattığı duygusal etkiyle (korku, öfke, şaşkınlık) ilgili olarak zihinlerinde güçlü bir kanaat ve önyargı oluşturmuştur. Bu asimetri, reaktif çabaların her zaman bir adım geride kalmasına neden olur.

İkinci olarak, en somut kanıtlar ve en sağlam argümanlarla bir bilginin yanlış olduğu bilimsel olarak çürütülse ve hatta bu yürütme hedef kitle tarafından kabul edilse bile, o bilgi insan hafızasında bir tortu bırakmaya, bilişsel izler oluşturmaya devam eder. Buna da "devam eden tesir etkisi" adı verilir. [77] Bu olgu, yanlış bilginin resmi olarak geri çekilmesinden veya çürütülmesinden sonra bile, bireylerin akıl yürütme, karar verme ve olayları yorumlama süreçlerini etkilemeye devam etmesi anlamına gelir. İnsanlar rasyonel olarak "bu bilgi yanlışmış, kanıtlar bunu gösteriyor" deseler bile, bilinçaltlarında o yanlış bilginin yarattığı korku,

🔍 **KAVRAM:** ÖN-ÇÜRÜTME

Neyi açıklar?: Ön-çürütme (prebunking) tıpkı tıbbi aşılamada olduğu gibi, bireyleri henüz yanlış bilgiyle karşılaşmadan önce manipülasyon taktiklerinin zayıflatılmış örneklerine maruz bırakarak zihinsel direnç kazandıran "proaktif" stratejidir.

Neden önemli?: Bireyin manipülasyonu tanımasını sağlayan "bilişsel antikorlar" üreterek, yanlış bilginin zihinde yer etmesini ve yayılmasını baştan engeller.

[77] Ecker, U. K. H., Lewandowsky, S., & Tang, D. T. W. (2010). Explicit warnings reduce but do not eliminate the continued influence of misinformation. *Memory & Cognition*, *38*(8), 1087–1100. https://doi.org/10.3758/MC.38.8.1087

öfke, güvensizlik gibi duygu ve ilk izlenim, ileriki kararlarını ve tutumlarını etkilemeyi sürdürür. Bu durum, özellikle yüksek duygusal yüke sahip konularda doğrulama çabalarının etkinliğini ciddi şekilde düşürür. Bu reaktif mücadeledeki yapısal ve bilişsel engeller göz önüne alındığında, modern bilgi güvenliği stratejisi bir paradigma değişimi gerektirmektedir. Odak noktasının, yayılan yanlış bilginin yarattığı yangını söndürmeye çalışmaktan, bir başka deyişle hasar yönetimi yapmaktan, yangının çıkmasını ve yayılmasını baştan önlemeye kayması esastır.

İZLE

CBC News tarafından hazırlanan *60 Minutes* isimli programda dezenformasyonun panzehiri olan p*rebunking* stratejisini mercek altına alıyor. Prof. Sander van der Linden'in zihni manipülasyondan koruyan video ve oyunların çalışma mantığını attığı videoyu izleyebilirsiniz.

İzlemek için:
https://www.youtube.com/watch?v=1RmxeZHPeHg&t=53s

İşte tam bu noktada, geleneksel teyitçiliği tamamlayıcı ve güçlendirici, proaktif, önleyici bir yaklaşım olan psikolojik aşılama teorisi devreye girer. Tıpkı biyolojik aşının vücudu hastalığa karşı koruması gibi, psikolojik aşılama da zihni yanlış bilgiye, manipülatif argümanlara ve ikna tekniklerine karşı önceden hazırlayarak bilişsel bir bağışıklık sistemi oluşturmayı amaçlar. Yanlış bilginin kurbanı olmadan önce bireylere dozunda ve zayıflatılmış manipülasyon teknikleri gösterilerek, bu tekniklere karşı direnç kazanmaları sağlanır. Bu yaklaşım, sadece yanlış bilgiyi çürütmekle kalmaz, aynı zamanda bireylerin gelecekte karşılaşacakları bilinmeyen manipülasyonlara karşı da genel bir direnç geliştirmelerini hedefler.

Teorik Çerçeve: Aşılama Teorisi

Sosyal psikolog William J. McGuire tarafından 1960'larda Soğuk Savaş'ın yoğun propaganda ortamında geliştirilen Aşılama Teorisi[78], bireylerin inançlarına yönelik ikna edici saldırılara karşı nasıl direnç geliştirdiğini açıklayan çığır açıcı bir iletişim modelidir. Teori, tıbbi aşılamanın biyolojik mantığını iletişim ve ikna biliminin temel prensiplerine uyarlamaktadır. Tıpkı bir virüsün vücuda girmesi gibi, dezenformasyon, manipülasyon veya güçlü bir karşı argüman da bireyin mevcut inanç sistemine, tutumlarına ve bilgi dünyasına bir "saldırı" teşkil eder. McGuire'in temel önermesi, bu saldırıların önceden tahmin edilip zayıf bir dozda sunulmasıyla psikolojik bir bağışıklık yaratılabileceğidir. Tıbbi aşılamada vücut, virüsün zayıflatılmış veya inaktive edilmiş bir formuyla karşılaştığında, bağışıklık sistemini harekete geçirir. Bu deneme tehdidi sayesinde vücut, virüsü tanır, ona karşı savaşır ve gelecekteki gerçek ve güçlü saldırılara karşı koymak üzere özel antikorlar üretir.

Psikolojik aşılamadaki mekanizma da bireyin zihinsel süreçlerinde benzer şekilde işler. Bireye, karşılaşabileceği manipülasyonun, dezenformasyonun veya karşıt argümanın zayıflatılmış bir dozu önceden sunulur. Bu doz, inancı tamamen değiştirecek güçte değildir, sadece bir tehdit algısı yaratır. Birey bu zayıf argümanla zihninde mücadele eder. Bu süreç, bireyin kendi inancını destekleyen yeni karşı-argümanlar veya çürütmeler geliştirmesini tetikler. İşte bu zihinsel mücadele, "bilişsel antikor" olarak adlandırılan direnç mekanizmasını oluşturur. Bu önceden yaşanmış bilişsel mücadele deneyimi sayesinde, kişi gelecekte aynı konudaki tam ölçekli ve güçlü ikna edici saldırılarla karşılaştığında hazırlıklı olur ve bu saldırılara karşı otomatik bir direnç geliştirir.

---

[78] McGuire, W. J. (1964). Inducing resistance to persuasion: Some contemporary approaches. İçinde L. Berkowitz (Der.), *Advances in experimental social psychology* (Cilt 1, ss. 191–229). Academic Press. https://doi.org/10.1016/S0065-2601(08)60052-0

Compton ve Pfau (2004) tarafından belirtildiği üzere, etkili ve başarılı bir bilişsel aşının oluşturulabilmesi için iki temel yapıtaşının bir arada kullanılması gerekmektedir.[79] Bu sürecin ilk adımı olan ön uyarı (tehdidin farkındalığı), bireyin mevcut inançlarına, tutumlarına veya bilgi dünyasına yönelik yakın zamanda bir saldırı (manipülasyon girişimi veya karşıt argüman) olacağı konusunda açıkça uyarılmasıdır. Bu uyarı, bireyde psikolojik bir gerilim ve tehdit algısı yaratarak, inançlarını savunma ihtiyacını tetikler. Zihinsel bir "kalkan kaldırma" refleksi devreye girer. Örneğin, "Dikkat et, bu konuda yakında seni manipüle etmeye veya fikrini değiştirmeye çalışacak bir bilgi ile karşılaşacaksın" şeklindeki bir ikaz, inancı destekleyecek materyali tek başına sağlamadığı için genellikle yeterli olmasa da bilişsel savunma sürecini başlatmak için zorunlu bir aşamadır.

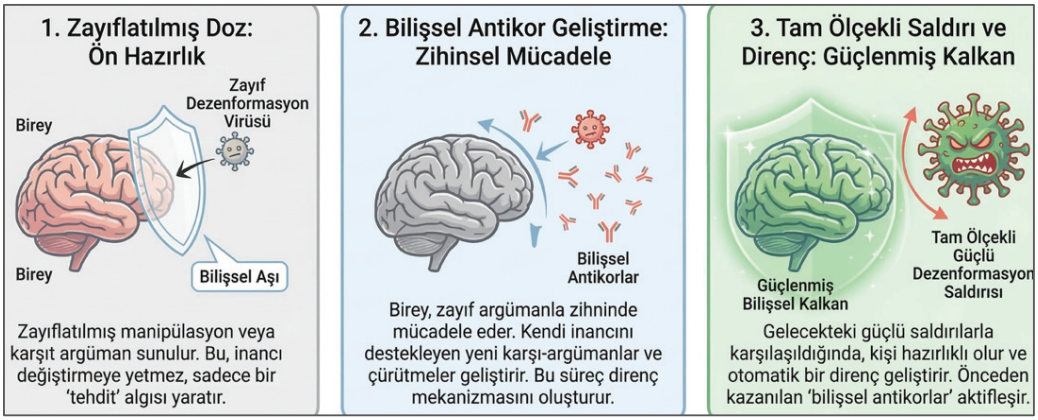
Bilişsel aşılamanın ikinci ve belirleyici adımı olan antikorların üretilmesi ön-çürütme bireye gelecekte yöneltilmesi muhtemel saldırının zayıflatılmış bir modelini, "aşısını" sunmakla başlar. Bu süreç, bireye hem beklenen saldırının içeriği hakkında bilgi verir hem de bu saldırıya karşı nasıl mücadele edeceğinin pratik yolunu öğretir. Birey, savunma mekanizmasını, bilişsel antikorlarını bu pratik uygulama ile geliştirir. Örneğin bir dezenformasyonun temel iddiası sunulur ve hemen ardından bu iddianın kullandığı yanlış kaynak, bağlamdan koparma veya duygusal manipülasyon hilesi açıklanarak geçerli kanıtlarla çürütülür. Aşılama Teorisi, özellikle dezenformasyonla mücadele, sağlık iletişimi ve siyasi propaganda alanlarında bireylerin manipülatif etkilere karşı direncini

Uygulama: Ön-Çürütme (*Prebunking*) ve Aşılama Teorisi

Dezenformasyonla mücadelede, bilginin yayılma hızına yetişmek geleneksel

[79] Compton, J., & Pfau, M. (2004). Use of inoculation to foster resistance to credit card marketing targeting college students. *Journal of Applied Communication Research, 32*(4), 343–364.

çürütme (*debunking*) yöntemlerini yetersiz bırakmaktadır. Bu noktada, sosyal psikolojiden ilham alan Aşılama Teorisi, dijital medya ortamında pratik karşılığını "ön-çürütme" adı altında bulmuştur. Prebunking, bir yalanın veya manipülasyonun yayılmasından *önce* insanları buna karşı hazırlamayı amaçlar. Klasik çürütme (*debunking*), bir olaydan veya yalan yayıldıktan *sonra* reaktif olarak yapılırken, ön-çürütme, proaktif bir savunma mekanizması oluşturur. Aşılama teorisine göre, tıpkı biyolojik aşıların vücuda zayıflatılmış virüs vererek bağışıklık sistemi oluşturması gibi, insanlara dezenformasyonun zayıflatılmış bir "dozunun" verilmesi, zihinsel bağışıklık oluşturur. Bu doz, genellikle manipülasyon taktiklerinin veya gelecekteki yalanların potansiyel örneklerinin ifşa edilmesi şeklinde sunulur.



Şekil 6.1.1 *Bilişsel aşılamanın işleyişi*

BBC Media Action ve Jigsaw (Google'ın teknoloji ve fikri mülkiyet inkübatörü) tarafından hazırlanan kapsamlı rehberler[80] ve akademik çalışmalar[81],

[80] Google Jigsaw, BBC Media Action, & University of Cambridge. (2024). *A practical guide to prebunking misinformation*. https://prebunking.withgoogle.com/docs/A_Practical_Guide_to_Prebunking_Misinformation.pdf

[81] Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances*, *8*(34), eabo6254.https://doi.org/10.1126/sciadv.abo6254

prebunking stratejisini temelde iki ana yaklaşımla ele almaktadır. Bunlardan ilki konu temelli prebunking yaklaşımıdır. Bu yaklaşım, belirli ve öngörülebilir bir konuda yayılması yüksek ihtimal olan somut bir yalanı veya iddiayı hedef alır. Amaç, o konuya özgü yanlış bilgiyi, yayılmadan önce doğrudan adresleyip çürütmektir. Yetkililer, kurumlar veya güvenilir medya organları, seçim, doğal afet, sağlık krizi gibi yaklaşan bir olay bağlamında ortaya çıkması beklenen spesifik bir dezenformasyon anlatısını önceden tahmin eder ve buna karşı doğru, kanıta dayalı bilgiyi proaktif olarak sunar. Örneğin, kritik bir seçim öncesinde "oyların çalınacağı veya siber saldırı olacağı" yönündeki dedikoduların yayılacağı öngörülerek, Seçim Kurulu'nun önceden güvenlik önlemlerini ve şeffaflık prosedürlerini detaylıca açıkladığı bir basın toplantısı düzenlemesi bu stratejinin somut bir uygulamasıdır.

Konu temelli yaklaşımın uygulanmasında karşılaşılan sınırlılıklar ve zorluklar, öncelikle Kapsam Sınırlılığı ile kendini gösterir; dijital ortamdaki potansiyel yalanların çeşitliliği ve yayılma hızı, her bir yalanı önceden tahmin etmeyi ve tek tek çürütmeyi pratik açıdan imkânsız kılmaktadır. Ayrıca, henüz kamuoyunda yaygınlaşmamış bir yalanı veya komplo teorisini zikrederek çürütmeye çalışmak geri tepme riski (*backfire effect*) doğurabilir; bu durum, "uçan spagetti canavarı" etkisi olarak da bilinen, fikri ilk kez duyanların aklına şüphe tohumları ekilmesi ve zikredilen yalanın doğrulanmış bilgiden daha akılda kalıcı olması riskini barındırır. İkincisi ise taktik temelli ön-çürütmeli oyunlaştırmadır. Bu yöntem, güncel akademik araştırmalarla desteklenen ve en etkili, esnek ve ölçeklenebilir prebunking stratejisi olarak kabul edilir. Odak, belirli bir yalanın içeriği

KAVRAM: ÇÜRÜTME

Neyi açıklar?: Yanlış bilgi yayıldıktan sonra, somut kanıtlar ve düzeltmeler kullanılarak bu bilginin yanlışlığının ortaya konduğu reaktif (tepkisel) müdahale sürecidir.

Neden önemli?: Bilgi kirliliğini temizlemek için gerekli olsa da yalanın yayılma hızına yetişemediği ve hafızadaki izlerini tamamen silemediği için tek başına yeterli değildir.

değil, yalanın üretiminde kullanılan evrensel manipülasyon taktikleridir.

Sosyal medya platformlarında sadece belirli yanlış bilgilerin etiketlenmesi veya uyarı konulması, kullanıcıların etiketlenmemiş diğer yanlış haberleri "zımnen doğrulanmış" veya "güvenilir" olarak algılamasına neden olabilir. Kullanıcılar, "Eğer bu haber yanlış olsaydı, üzerinde uyarı olurdu" şeklindeki hatalı bir çıkarımla, etiketlenmemiş dezenformasyona daha kolay inanma eğilimi gösterirler. Bu durum, uyarı sistemlerinin, etiketlenemeyen devasa yalan havuzunu istemeden de olsa meşrulaştırma riskini doğurur. Bu durum ima edilen hakikat etkisi (*the implied truth effect*) olarak tanımlanmaktadır.[82]

İnsanlara, yanlış bilginin yayılma sürecinde kullanılan ortak manipülasyon tekniklerinin (sahte uzmanlık kullanma, duygusal dil/korku tellallığı, günah keçisi yaratma, tutarsızlık/mantık hataları, kutuplaştırıcı dil) ne olduğunu, nasıl çalıştığını ve nasıl tanınacağını öğretmek. Buna genellikle "oyunlaştırma" (*gamification*) veya kısa video formatları eşlik eder.

Dezenformasyonun içeriği ve konuları sürekli değişse de temel psikolojik manipülasyon taktikleri aynı kalır. Taktikleri ifşa etmek, gelecekteki yüzlerce farklı yalan türüne karşı koruma sağlar. Schmid ve Betsch'in (2019) çalışması, dezenformasyonu çürütürken sadece konuyu değil, kullanılan manipülasyon tekniğini ifşa etmenin izleyiciyi ikna etmede çok etkili olduğunu kanıtlamıştır.[83] Somut bir örnek senaryo üzerinden gidilirse, kullanıcılara haber başlıklarındaki "ihanet", "felaket" veya "derhal" gibi kelimelerin nasıl bir "duygusal dil kullanımı" taktiği olduğunu öğreten 30 saniyelik eğitici bir video

[82] Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). The implied truth effect: Attaching warnings to a subset of fake news headlines increases perceived accuracy of headlines without warnings. *Management Science*, *66*(11), 4944–4957. https://doi.org/10.1287/mnsc.2019.3478

[83] Schmid, P., & Betsch, C. (2019). Effective strategies for rebutting science denialism in public discussions. *Nature Human Behaviour*, *3*(9), 931–939. https://doi.org/10.1038/s41562-019-0632-4

izletilmesi etkili bir yöntemdir. Bu eğitimi alan bir birey, gelecekte konu mülteciler, iklim değişikliği veya sağlık krizleri olsa dahi, maruz kaldığı haberin içeriğini bilmese bile kullanılan manipülasyon tekniğini otomatik olarak tanıma becerisi kazanabilirler. Bu yaklaşım, araştırmacılar tarafından "Geniş Spektrumlu Aşılama" olarak adlandırılır.[84] Bu bağışıklık, bireyin zihinsel filtresini güçlendirir ve gelecekte karşılaşacağı çok çeşitli dezenformasyon türlerine karşı genel bir direnç kazanmasını sağlar. Taktik temelli prebunking, sosyal medya platformları üzerinden küresel ölçekte uygulanabilir ve bireyleri pasif alıcıdan, aktif ve eleştirel birer medya tüketicisine dönüştürmeyi hedefler.

Bir Ön-Çürütme (*Prebunking)* Kampanyası Nasıl Tasarlanır?

Dezenformasyon ve manipülasyon karşısında bireyleri ve toplumu "aşılamak" olarak tanımlanan ön-çürütme kritik bir psikolojik savunma stratejisidir. Bu yaklaşım, yanlış bilginin yayılmasından önce, o bilginin temelini oluşturan manipülatif teknikleri ve taktikleri önceden ifşa ederek kişileri zihinsel olarak hazırlar ve dirençlerini artırır. Etkili bir ön-çürütme kampanyası, rastgele bilgi vermekten ziyade, hedeflenen ve psikolojik temellere dayanan belirli adımları izlemelidir. BBC ve Jigsaw'un önerdiği bu sistematik yaklaşım, manipülasyonun mekaniğini izleyiciye zararsız bir bağlamda göstermeyi amaçlar (BBC & Jigsaw, 2024).

Bu sürecin ilk adımı olan tehdidin kapsamlı tanımlanması aşamasında yalnızca yayılması beklenen yanlış bilginin spesifik içeriği değil (Örn: "Oylar çalındı" iddiaları), aynı zamanda bu bilginin yayılma motivasyonu ve hedef kitlesi de analiz edilmelidir. Hangi manipülasyon taktiklerinin (Örn: Günah keçisi ilan etme, temsiliyet hatası, duygusal tetikleme) bu tehdidin taşıyıcısı

[84] Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications*, *5*(1), Makale 65. https://doi.org/10.1057/s41599-019-0279-9

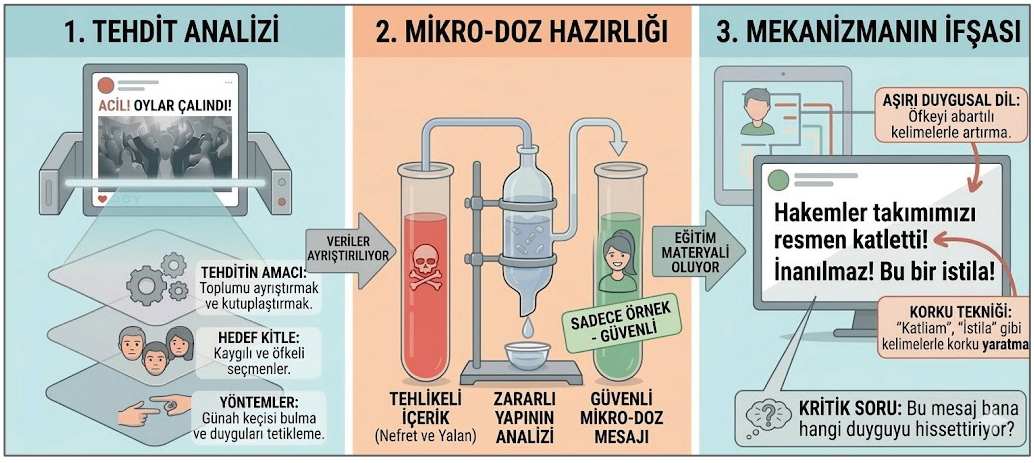
olacağı önceden belirlenmelidir. Örneğin bir seçim döneminde, "oylar çalındı" gibi doğrudan yanlış bilgiye ek olarak, azınlık grupları hedef alan günah keçisi taktiği veya toplumsal ayrışmayı körükleyen kutlama taktiği de tehdit kapsamına alınmalıdır.

Prebunking kampanyalarının tasarımında hayati bir aşama olan zayıflatılmış dozun (mikro-doz) titizlikle hazırlanması, izleyiciyi öfkelendirmeden veya doğrudan zararlı dezenformasyona maruz bırakmadan manipülasyonun mekanizmasını gösteren güvenli bir antikor geliştirmeyi amaçlar. Hazırlanan örnek, gerçek bir nefret söylemi veya zararlı içerik barındırmamalıdır. Manipülasyonun yapısını, içeriğini devre dışı bırakarak öğretmelidir. Örneğin, gerçek ve riskli bir siyasi yalan yerine, bir spor takımı veya hayali bir ürün hakkında kurgulanmış komik, aşırı duygusal bir mesaj kullanılarak "duygusal tetikleme" taktiğinin nasıl çalıştığı risksiz bir şekilde gösterilebilir.

Prebunking sürecinin üçüncü aşaması olan taktiklerin açık ve basit bir şekilde ifşa edilmesi, mikro-doz örneği sunulduktan hemen sonra devreye girer; bu aşamada, örneğin neden manipülatif olduğu net bir dille açıklanarak öğrenilen mekanizmanın gerçek hayattaki uygulamalara aktarılması sağlanır. Süreçte basit ve akılda kalıcı etiketlerin kullanılması esastır; örneğin, "Bakın, bu mesaj sizi panikletmek için özellikle 'istila', 'tehlike' gibi ağır kelimeler kullanıyor. Bu, bir 'korku tellallığı' taktiğidir" şeklindeki somut açıklamalarla izleyicinin bir mesajla karşılaştığında "Bu bana hangi duyguyu hissettirmeye çalışıyor?" sorusunu sorması hedeflenir. Prebunking içeriğinin başarısı, hedef kitleye ulaşma biçimine bağlıdır. İçerik, hedef kitlenin en çok zaman geçirdiği platformlarda (YouTube reklamları, TikTok, Instagram, hatta oyun içi reklamlar) dağıtılmalıdır. İçerikler kısa, ilgi çekici, eğlenceli ve kolay paylaşılabilir olmalıdır. Genellikle 60-90 saniyelik video formatı en etkili kabul edilir. Geleneksel "doğruluk kontrolü" makalelerinden farklı olarak, prebunking bir eğitim/eğlence formatında sunulmalıdır.

Dezenformasyon ve yanlış bilgi akışıyla yürütülen karmaşık mücadele, yalnızca teknolojik araçlara veya hukuki düzenlemelere indirgenemez. Bu savaşın nihai cephesi, bireyin kendi zihnidir. Platformların algoritmalarını "temizlemesi" veya devletlerin yeni yasalar çıkarması, sorunun kaynağını değil, belirtilerini hafifletebilir. Kalıcı ve güçlü bir savunma hattı inşa etmek için, toplumsal bağışıklık sistemini güçlendirmek esastır. Bu, bireyleri dışarıdan gelen manipülasyon girişimlerine karşı bilinçli, eleştirel ve dayanıklı kılmak anlamına gelir.

Toplumsal bağışıklığın merkezinde, bireylerin kendi düşünce süreçlerini koruma yeteneği yatar. Bu amaçla kullanılan en etkili yöntemlerden ikisi, "psikolojik aşılama" ve "ön-çürütme " teknikleridir. Bu yaklaşımlar, topluma pasif bir inanç sistemi yerine aktif bir düşünme becerisi kazandırarak, adeta "bilişsel antikorlar" üretir.



Şekil 6.1.2 *Bilişsel aşılama geliştirme süreci*

Psikolojik aşılama, tıpkı biyolojik bir aşı gibi, bireyi manipülatif tekniklerin zayıf dozlarıyla önceden tanıştırır. Kullanılan temel aldatma mekanizmalarını göstererek, gerçek bir dezenformasyon saldırısı geldiğinde kişinin buna karşı zihinsel bir direnç mekanizması geliştirmesini sağlar. Bu

yaklaşımın temel felsefesi, insanlara neye inanacaklarını dikte etmek yerine, onlara "nasıl düşüneceklerini," "bilgiyi nasıl sorgulayacaklarını" ve "kaynağa nasıl şüpheyle yaklaşacaklarını" öğretmektir. Bu, demokratik bir toplumun düşünce özgürlüğünü koruyarak edinebileceği en güçlü ve en etik zırhtır. Bireyin eleştirel düşünme yeteneği ne kadar gelişirse, dış manipülasyona karşı olan savunma kalkanı o kadar sağlam olur.

📌 ÖRNEK VAKA:

Google Jigsaw, ön-çürütme stratejisinin somut bir uygulamasını Polonya, Çekya ve Slovakya'da gerçekleştirdi. Rusya-Ukrayna savaşının ardından bu ülkelerde Ukraynalı mültecilere yönelik dezenformasyonun artması bekleniyordu.

Müdahale Biçimi: Kampanya, mültecilerin kendileri hakkındaki yalanları doğrudan çürütmek yerine, dezenformasyonun arkasındaki iki ana taktiğe odaklandı: "Korku Tellallığı" ve "Günah Keçisi İlan Etme". 90 saniyelik videolar, bu taktiklerin nasıl işlediğini, duyguları nasıl manipüle ettiğini izleyicilere gösterdi.

Kanıtlanmış Etki: Kampanyanın sonuçları, prebunking'in etkili bir bilişsel aşı olduğunu gösterdi (Lewandowsky et al., 2024). Videoları izleyen katılımcıların, izlemeyen kontrol grubuna kıyasla, manipülatif başlıkları ve içerikleri tespit etme becerisinde anlamlı ve ölçülebilir bir artış gözlemlendi. Bu sonuç, bireylerin belirli bir bilgiye değil, bilginin kendisini taşıyan manipülasyon taktiğine karşı bağışıklık kazandığını kanıtlamaktadır.

Videoları izlemek için:
🔗 https://www.youtube.com/playlist?list=PL12X50gJBP-RoxFWCaofWntrPj3DgDB5Jh

Bu teorik altyapıyı somut ve erişilebilir bir pratiğe dönüştürmenin en eğlenceli ve etkili yollarından biri "oyunlaştırma" tekniğidir. Oyunlar, katılımcı ve deneyimsel bir öğrenme ortamı sunarak, soyut kavramların içselleştirilmesini kolaylaştırır. Bu bağlamda, psikolojik aşılama teorisini kullanarak geliştirilen ve küresel çapta tanınan bir örnek olan bir sonraki bölümde detaylı ele alacağımız *Bad News* oyunu incelenmeye değerdir. Bu oyun,

kullanıcının bizzat bir dezenformasyon yayıcısı rolüne bürünmesini sağlar. Oyuncular, "kötü olmayı öğrenerek iyi kalmayı" sağlayan tersine bir pedagoji deneyimlerler. Bir yalan haber imparatorluğunu nasıl kuracaklarını, trolleri nasıl yöneteceklerini ve hangi manipülasyon taktiklerini kullanacaklarını deneyimleyerek öğrenirler. Bu deneyim, kullanıcının gerçek hayatta bu taktiklerle karşılaştığında onları hızla tanımasını ve etkisiz hale getirmesini sağlar.

TEMEL ÇIKARIMLAR

Bu bölüm, tıbbi aşılamadan ilham alan proaktif bir yaklaşımı savunur: Bireylerin zihnine, henüz yalanla karşılaşmadan önce manipülasyonun zayıflatılmış bir dozunu vererek bilişsel antikorlar üretmelerini sağlamak. Amaç, insanlara neye inanacaklarını dikte etmek değil, manipülasyon tekniklerini tanımalarını sağlayarak zihinsel bağışıklık kazandırmaktır.

Temel Kavramlar ve Mekanizmalar

Aşılama Teorisi (*Inoculation Theory*): Bireyi, gelecekteki güçlü bir manipülasyon saldırısına karşı hazırlamak için, tehdidin zayıflatılmış bir versiyonuna önceden maruz bırakarak direncini artırma sürecidir.

Devam Eden Etki (*Continued Influence Effect*): Bir bilginin yanlış olduğu kanıtlansa bile, bireyin belleğinde tortu bırakarak kararlarını ve duygularını etkilemeye devam etmesi fenomenidir.

Geniş Spektrumlu Bağışıklık: Belirli bir yalanı değil, o yalanın üretiminde kullanılan taktiği (Örn: Korku tellallığı) öğrenen zihnin, gelecekte karşılaşacağı farklı konulardaki benzer manipülasyonları da otomatik olarak tanımasıdır.

6.1. KENDİNİZİ TEST EDİN

Soru 1: Aşılama teorisine göre, bireyin manipülasyona karşı direnç kazanması için maruz kalması gereken şey nedir?

A) Manipülasyonun zayıflatılmış bir örneği

B) Sadece doğrulanmış, steril bilgi

C) Uzun süreli medya okuryazarlığı dersleri

D) Hiçbir bilgiye maruz kalmamak

Soru 2: "İma edilen hakikat etkisi" neyi ifade eder?

A) Bir haberin çok paylaşılmasının onun doğru olduğunu ima etmesi

B) Belirli yalan haberlerin etiketlendiği bir ortamda, kullanıcıların etiketsiz olan diğer yalan haberleri "doğru" varsayma eğilimi

C) Doğru haberlerin yalan gibi görünmesi ve yalanın doğrudan daha hızlı yayılması

Soru 3: "Bad News" gibi oyunların dezenformasyonla mücadeledeki temel felsefesi nedir?

A) Oyunculara hangi haberin doğru olduğunu ezberletmek

B) Oyuncuları bir "trol" rolüne sokarak, manipülasyon taktiklerini "içeriden" öğrenmelerini ve bu sayede bağışıklık kazanmalarını sağlamak

C) Gençleri hedefleyerek, bu genç oyuncuları internetten soğutarak, dezenformasyona maruz kalmamalarını sağlamak

6.1. MERAKLISINA EK KAYNAKLAR

Shatz, I. (2021, 3 Temmuz). *Geri tepme etkisi: İnsanlar, inançlarıyla çelişen gerçekler karşısında gerçekleri kabul etmek yerine neden inançlarına daha sıkı sarılıyor?* (T. M. Gür, Çev.; Ç. M. Bakırcı, Der.). Evrim Ağacı. https://evrimagaci.org/geri-tepme-etkisi-insanlar-inanclariyla-celisen-gercekler-karsisinda-gercekleri-kabul-etmek-yerine-neden-inanclarina-daha-siki-sariliyor-10649

Oyunlaştırma (*Gamification*): “Kötü” Olmayı Öğrenerek “İyi” Kalmak

Geleneksel medya okuryazarlığı eğitimleri, günümüzün hızla değişen dezenformasyon ortamında yetersiz kalmaktadır. Bu yaklaşımlar genellikle pasif ve teorik bilgi aktarımına dayanır. Uygulanan didaktik modelde, bir uzmanın "bu haber yanlıştır, çünkü kaynağı belirsizdir" gibi analiz ve bilgileri katılımcılara *doğrudan* aktarmasıyla yetinilir. Oysa modern bilişsel bilimler ve pedagoji, insanların bilgiyi pasif dinlemek yerine aktif olarak deneyimleyerek, uygulayarak ve keşfederek çok daha kalıcı ve derinlemesine öğrendiğini kesin olarak kanıtlamaktadır. Kadim bilgeliğin bir yansıması olan Konfüçyüs'ün ünlü sözü bu durumu mükemmel bir şekilde özetler: *"Duyarım ve unuturum. Görürüm ve hatırlarım. Yaparım ve anlarım."* Pasif tüketim, unutmaya mahkûmdur; aktif katılım ise bilişsel anlayışa ve kalıcı davranış değişikliğine yol açar.

Yapay Zekâ destekli manipülasyon tekniklerinin hızı, hacmi ve karmaşıklığı düşünüldüğünde, sadece pasif öğrenme modelleri (haber izleme, makale okuma, ders dinleme) artık toplumsal bağışıklığı sağlamakta yetersiz kalmaktadır. Bu nedenle, paradigmaların değiştirilmesi ve bilginin yalnızca *tüketilmesi* yerine *üretilmesi* deneyimine odaklanılması zorunlu hale gelmiştir. Çözüm, pasif izlemeden aktif aşılama yöntemine geçiş yapmaktır. Bu bilimsel öğrenme ilkesiyle hareket eden Cambridge Üniversitesi'ndeki araştırmacılar, kritik bir başarı modeli olan siber güvenlikteki "kırmızı takım" (*red teaming*) stratejisini dezenformasyon ve medya okuryazarlığı eğitimi alanına uyarlamıştır.

Red teaming stratejisi, siber güvenlikte bir savunma sisteminin, örneğin bir kurumun bilişim altyapısının zayıf yönlerini ve potansiyel açıklarını gerçekçi bir şekilde tespit etmek için "kötü niyetli hacker gibi düşünmek"

esasına dayanır. Bir saldırganın motivasyonunu, araçlarını ve hedeflerini anlamadan etkin bir savunma inşa edilemez. Benzer bir mantıkla, bireylerin zihinsel savunma mekanizmalarını ve bilişsel güvenliğini güçlendirmek için de bir süreliğine "manipülatör/dezenformasyon baronu gibi düşünmeyi" öğrenmemiz gerekmektedir. Bu yaklaşım, sadece savunma mekanizmasını değil, saldırının kaynağını ve işleyişini de anlamayı hedefler.

Oyunlaştırma, aktif aşılama yönteminin temel uygulama aracıdır. Bu, bireyi manipülasyonun bizzat "mutfağına" sokan, yüksek düzeyde katılım gerektiren stratejik bir araçtır. Aktif aşılama yöntemi, katılımcının manipülasyon tekniklerini sadece teorik olarak öğrenmesini değil, simülasyon veya oyun ortamında bizzat uygulayarak, üreterek ve deneyimleyerek anlamasını hedefler. Bu deneyim, bireye kendi bilişsel haklarını koruyacak, manipülasyonun etkilerine karşı direnç gösterecek zihinsel zırhı, bilişsel antikorları kazandırır.

Aktif Aşılama modelinin temel uygulaması, katılımcıları bilindik "iyi" ve gerçeği savunan rolden çıkarıp, *red teaming* mantığıyla paralel olarak, karşıt bir role sokmaktır. Katılımcılar; yalan üreten, kutuplaştıran, duygusal manipülasyon yapan ve kaos yaratan "manipülatör, dezenformasyon kaynağı veya trol" rolünde oynamaya teşvik edilirler. Bu "içeriden bakış açısı", bireylerin manipülasyon tekniklerini (trollemek, duygu sömürüsü, sahte uzmanlık yaratma, kutuplaştırma taktikleri, komplo teorisi inşa etme) derinlemesine anlamasını sağlar. Kendi elleriyle bir yalan kampanyası inşa etme sürecinden geçen katılımcılar, bu tekniklerin nasıl işlediğini, hangi psikolojik tetikleyicileri kullandığını ve toplumu nasıl etkilediğini somut olarak kavrarlar. Böylece, bu tekniklerle gerçek hayatta karşılaştıklarında, onları anında tanıyabilir ve duygusal veya bilişsel olarak tuzağa düşmekten kaçınabilirler. Bu durum, tıpkı bir sihirbazlık hilesinin sırrını öğrenen birinin, o numarayı artık safça izlemek yerine ardındaki mekanizmayı görmesi ve hileye kanmaması gibidir.

Kazanılan bu bilişsel farkındalık, toplumsal bağışıklığın en güçlü temelini oluşturur.

Örnekler: İnsan Haklarını Güçlendiren Oyunlar

Akademik araştırmalar ve sivil toplum kuruluşlarının (STK) uygulamaları, eğlence amaçlı tasarlanmayan, aksine belirli toplumsal sorunları çözmeyi, kritik insan haklarını korumayı ve toplumun direnç kapasitesini artırmayı hedefleyen ciddi oyunlar konseptini merkeze almıştır. Bu oyunlar, pasif öğrenme yerine aktif deneyimlemeyi sağlayarak bilişsel ve psikolojik savunma mekanizmalarını kalıcı olarak güçlendirmeyi amaçlamaktadır.

2018 yılında Cambridge Üniversitesi'nden Dr. Jon Roozenbeek ve Prof. Sander van der Linden tarafından geliştirilen Bad News isimli çığır açıcı oyun, "psikolojik aşılama teorisinin" dijital alandaki en başarılı ve en çok araştırılan uygulamasıdır. Temel amacı, bireylere manipülasyon taktiklerini *içeriden* öğreterek onlara karşı bağışıklık kazandırmaktır. Bu oyunda oyuncu, etik sınırları aşan ve toplumu manipüle etmeyi hedefleyen bir "dezenformasyon baronu" veya "trol fabrikası yöneticisi" rolünü üstlenir. Bu rol, oyuncuyu, sıklıkla maruz kaldığı dezenformasyonun üreticisi konumuna yerleştirir. Asıl görev, "güvenilirlik" puanını sıfırlamadan, tamamen ifşa olmadan, "takipçi" sayısını maksimize etmektir. Oyuncu, bu amaca ulaşmak için dezenformasyonun taklit, duygu sömürüsü, kutuplaştırma, komplo teorileri üretme, karalama ve trolleme'den oluşan altı temel taktiğini bizzat uygulamalıdır. Oynama sonrasında yapılan randomize kontrollü çalışmalar[85] (RCT), oyunu

[85] Basol, M., Roozenbeek, J., & van der Linden, S. (2020). Good news about bad news: Gamified inoculation boosts confidence and cognitive immunity against fake news. *Journal of Cognition*, *3*(1), 1–9. https://doi.org/10.5334/joc.91; Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on "inoculation" theory can reduce susceptibility to misinformation across cultures. *Harvard Kennedy School Misinformation Review*, *1*(2). https://doi.org/10.37016/mr-2020-008

sadece 15 dakikalık kısa bir süre oynayan bireylerin, gerçek hayatta karşılaştıkları manipülatif içerikleri tespit etme yeteneğinde, bilişsel antikor üretimi ortalama %21 oranında kalıcı bir artış olduğunu bilimsel olarak kanıtlamıştır. Bu, enformasyon çağında temel bir insan hakkı olan bilgi edinme hakkının korunmasını sağlayan temel bir dijital aşı görevi görür.

İZLE

Jon Roozenbeek'in Cambridge Üniversitesi'nde geliştirdikleri "Get Bad News" ve "Go Viral!" oyunlarının arkasındaki bilimsel yaklaşımı ve bu oyunların toplumsal etkilerini anlattığı videoyu izlemek için:

https://www.youtube.com/watch?v=6FKR9tA5Fjw

Özellikle demokratik süreçleri ve seçimleri hedef alan dış müdahalelere karşı bir savunma mekanizması olarak tasarlanan Harmony Square ABD Dışişleri Bakanlığı Küresel Katılım Merkezi (GEC) ve İç Güvenlik Bakanlığı (DHS) gibi kritik kurumların desteğiyle geliştirilmiştir. Oyun, Seçme ve Katılma Hakkı ile sivil toplumsal dokunun korunmasına odaklanmıştır. Oyuncu, her şeyin yolunda gittiği, barışçıl ve işleyen bir topluluk olan "Harmony Square" kasabasına "baş dezenformasyon sorumlusu" olarak atanır. Oyuncunun stratejik görevi, toplumsal kutuplaşmayı tırmandırmak, mevcut güveni yıkmak ve yaklaşan yerel veya ulusal seçimleri içeriden sabote etmektir. Oyun, katılımcılara, "Ananaslı pizza sevenler ve sevmeyenler" gibi absürt, önemsiz ve basit konuların bile, profesyonel troller ve otomatik hesaplar-botlar tarafından nasıl hızla kutuplaştırıcı bir silaha dönüştürülebileceğini ve bunun kasıtlı olarak toplumsal dokunun parçalanmasına yol açtığını deneyimleme fırsatı sunar. Bu, özellikle seçim dönemlerinde hassas olan demokratik süreçlere direnç kazandırır.

Küresel salgın döneminde Dünya Sağlık Örgütü (WHO) ve Birleşik Krallık hükümeti iş birliğiyle geliştirilen Go Viral! oyunu, doğrudan Sağlık hakkını

ve halk sağlığı iletişimini hedef alan infodemi ile mücadele etmek amacıyla tasarlanmıştır. Oyuncunun hedefi, hızla yayılan bir virüs hakkında kasten korku yaymak, güvenilmez ve sahte uzmanlar yaratarak itibar kazanmak ve popüler komplo teorilerini besleyerek kendi "yankı odasını" oluşturmaktır. Bu süreçte, halk sağlığı kurumlarının güvenilirliği sistematik olarak baltalanır. Oyun, katılımcıların duygusal manipülasyonun, özellikle korku ve panik tellallığının ve sosyal medya algoritmalarıyla oluşan "filtre balonu" mekanizmasının, bilimsel gerçekleri ve kanıta dayalı tıbbi bilgileri nasıl hızla perdelediğini ve geçersiz kıldığını görmesini sağlar. Bu deneyim, özellikle aşı karşıtı propaganda ve sağlık mitlerine karşı yüksek düzeyde direnç geliştirilmesine yardımcı olur.

Crunky Uncle oyunu, karikatürler ve mizahı pedagojik bir araç olarak kullanarak, özellikle bilim inkarcılığına karşı mücadeleye odaklanır. Oyunun temel hedeflerinden biri, iklim değişikliği inkârı gibi kritik alanlardaki manipülasyonu ortaya çıkarmaktır. Oyun mekaniği, oyunculara dezenformasyonun temelini oluşturan 5 temel mantık hatasını ve retorik hilelerini (örneğin, kaygan zemin, saman adam argümanı, uzman statüsü çalma) öğretir. Bu hatalar, karikatürize edilmiş ve sürekli eleştiren huysuz bir amca karakteri üzerinden esprili bir dille sunulur. Bu yaklaşım, karmaşık bilimsel konuları bile inkâr eden argümanların ne kadar yüzeysel olduğunu ortaya koyar. Bu oyun Türkçe'ye Huysuz Dayı olarak çevrilmiştir.

Yerel Deneyimlerle Bilişsel Dayanıklılık: RESAID Oyun Ekosistemi

Küresel ölçekteki *Bad News* veya *Harmony Square* gibi öncü örnekler, "Aktif Aşılama" yönteminin dijital dezenformasyonla mücadeledeki başarısını kanıtlamıştır. Ancak dezenformasyon, sadece teknik bir sorun değil, aynı

zamanda kültürel ve yerel bir olgudur. Bir toplumun kriz anlarındaki refleksleri, kullandığı dilin nüansları ve tarihsel travmaları, manipülatörler için özgün birer oyun alanı sunar. Bu gerçeklikten yola çıkan RESAID (Creating Social Cognitive Resilience Against Information Disorders) projesi, Türkiye ve bölge özelindeki bilgi ekosistemini simüle eden, yerel dezenformasyon dinamiklerine odaklanan dört temel oyun geliştirmiştir. Bu oyunlar, katılımcıyı pasif bir gözlemci olmaktan çıkarıp, manipülasyonun mutfağına ve karar vericilerin yerine davet eder.

InfoChief (Bilgi Şefi): Haklar ve Güvenlik Arasındaki İnce Çizgi

Dezenformasyonla mücadele, sadece bir "yalan haber" sorunu değil, aynı zamanda demokratik değerlerin korunması mücadelesidir. *InfoChief* katılımcıyı bir kriz yönetim ekibinin parçası yaparak etik ve politik kararların ağırlığını hissettirir. Bir afet veya kriz döneminde, oyuncu önüne gelen "aksiyon kartlarını" kullanmak zorundadır. Örneğin, interneti kısıtlamak güvenliği (dezenformasyonun yayılmasını durdurarak) artırabilir; ancak bu karar özgürlük puanını düşürür ve toplumda Uyum Yorgunluğu yaratır. Bu deneyim oyuncuya "meşruiyet krizi" riskini gösterir. Eğer uyum yorgunluğu 50'yi geçerse, halkın kurumlara olan güveni sarsılır. Bu deneyim, dezenformasyonla mücadelenin temel hak ve özgürlükleri feda etmeden yürütülmesi gereken stratejik bir denge olduğunu öğretir.

Catch and Match (Yakala ve Eşle): Manipülasyon Aktörlerini Tanımak

Bu oyun, dezenformasyonu bir içerik parçası olmaktan çıkarıp bir "aktörler ve stratejiler ağı" olarak görmeyi sağlar. Oyunculara, dezenformasyon yayan çeşitli figürlerin (trol ağları, botlar, kampanya ajansları, "huysuz dayı" tiplemeleri vb.) davranış kalıpları ipuçları olarak sunulur. "Tek bir merkezden yönetilir", "Duygusal ve aidiyet odaklı bir dil kullanır" gibi verilerden yola

çıkarak anonim aktörlerin kimliği deşifre edilmeye çalışılır. Katılımcı, içeriğin ne söylediğinden çok, içeriğin *kim tarafından, neden ve nasıl* üretildiğine odaklanma yetisi kazanır. Bu, dezenformasyonun ardındaki motivasyonu (finansal kazanç, ideolojik kutuplaştırma, kaos yaratma) anlamak için kritik bir adımdır.

Fanus: Kendi Yankı Odana Ayna Tutmak

Psikolojik dayanıklılığın en zor aşaması, bireyin kendi bilişsel önyargılarıyla yüzleşmesidir. *Fanus*, sosyal medya algoritmalarının bizi içine hapsettiği "benzer fikirli insanlar çemberini" görselleştiren bir öz-yansıtma aracıdır. Oyuncu, en sık fikir alışverişinde bulunduğu kişileri ve onlarla olan fikir benzerliği derecesini sisteme girer. Oyun, bu verileri kullanarak oyuncuya kendi "fanusunun" (yankı odasının) bir modelini sunar. Fanusun ne kadar şeffaf veya ne kadar kapalı olduğu, oyuncunun farklı görüşlere ne kadar erişebildiğinin bir göstergesidir.

Sparkline: Dijital Akışın İçinde Doğruyu Aramak

Misinformation Game isimli oyundan uyarladığımız *Sparkline*, katılımcıları doğrudan bir sosyal medya platformunun arayüzüne yerleştiren bir etkileşim simülasyonudur. Oyunun temel felsefesi, bireyin dijital ortamda hem bir tüketici hem de bir yayıncı olduğu gerçeğine dayanır. Oyuncu, orman yangınları veya iklim krizi gibi toplumun duygusal olarak en hassas olduğu dönemlerde bir "akış" (*timeline*) içine girer. Karşısına çıkan gönderiler, gerçek hayatta karşılaşılabilecek karmaşıklıktadır: Bazıları bilimsel verilere dayanırken, bazıları "Lityum bataryalar kasten yangın çıkarıyor" gibi teknik görünen komplo teorileri içerir. Oyuncunun her "beğenme", "paylaşma" veya "ihbar etme" eylemi, ekranın köşesindeki güvenilirlik puanı (*credibility*) ve takipçi sayısı göstergelerini anlık olarak değiştirir. Oyun, popülerlik ile hakikat

arasındaki çatışmayı simüle ederek, oyuncunun "yankı uyandırma" dürtüsünü dizginlemesini ve eleştirel bir filtre geliştirmesini amaçlar.

Bu dörtlü oyun ekosistemi, dezenformasyona karşı sadece bir savunma değil, bir "yapabilirlik" (*capability*) kazandırır. Tıpkı tıbbi bir aşılamada olduğu gibi, bu oyunlarla kazanılan direnç zamanla azalabilir. Bu nedenle RESAID, bu araçları okul müfredatlarına ve STK eğitimlerine entegre ederek düzenli "hatırlatma dozları" sağlamayı hedefler. Bir toplumun demokratik direnci, bireylerin manipülasyonun "mutfağını" ne kadar iyi tanıdığına bağlıdır. "Kötü olmayı öğrenerek iyi kalmak", dijital çağda zihinsel özgürlüğümüzü korumanın en modern ve etkili yoludur.

YZ Tehdidi ve Psikolojik Bağışıklığın Sürdürülebilirliği

Günümüzde bilişsel savunma alanındaki en büyük meydan okuma, Üretken Yapay Zekâ (*GenAI*) teknolojilerinden gelmektedir. Bu teknolojinin iki yönlü ve paradoksal bir rolü bulunmaktadır: GenAI, dezenformasyon üretimini kelimenin tam anlamıyla "süper şarj" etmiştir. Eskiden ciddi insan emeği, dil bilgisi ve yerel kültür bilgisi gerektiren "trol" faaliyetleri artık otomatize edilmiş, maliyeti sıfıra yaklaştırılmış ve hızı katlanmıştır. YZ, *yerelleştirilmiş*, *dil bilgisi hatasız* ve *inanılırlığı son derece yüksek* (hiper-gerçekçi) dezenformasyon materyalleri üretebilmektedir. Özellikle deepfake teknolojisi ile ses ve video içeriği de güvenilmez hale gelmiştir.

YZ tabanlı savunma araçları hızla geliştirilse de bu sistemlerin yanlış pozitif/negatif oranları hala yüksektir. YZ dezenformasyon üreticileri ile YZ tespit edicileri arasındaki bu silahlanma yarışı, teknolojik filtrelerin tek başına %100 güvenilir bir savunma hattı olamayacağını göstermektedir. Bu nedenle, eleştirel düşünen, oyunlaştırma ile güçlendirilmiş insan faktörü en son ve en güvenilir savunma hattı olarak kritik önemini korumaktadır.

Bilişsel psikoloji ve eğitim bilimlerinin acı bir gerçeği vardır: Hiçbir

eğitim veya aşı etkisi sonsuza kadar sürmez; buna "çürüme etkisi" (*decay effect*) denir. Maertens ve arkadaşları (2021) tarafından yapılan boylamsal çalışmalar, *Bad News* gibi oyunların sağladığı manipülasyon direncinin (bilişsel antikorların) zamanla, genellikle 3 ila 6 ay içinde azaldığını bilimsel olarak göstermiştir.[86] Tıpkı tıbbi aşılamada olduğu gibi, bilişsel bağışıklığın sürdürülebilirliği için eğitim sistemlerine ve sosyal medya platformlarına entegre edilmiş düzenli "hatırlatma dozları" kritik öneme sahiptir. Bu dozlar, oyunun sadece birkaç dakika süren kısa versiyonları, mikro-öğrenme modülleri veya kritik taktikleri hatırlatıcı kısa videolar şeklinde tasarlanarak sürekli bilişsel uyanıklık sağlanmalıdır. Bu, toplumsal bağışıklığın dinamik ve sürekli bir süreç olduğunun kabul edilmesini gerektirir.

Dijital çağın getirdiği en büyük tehditlerden biri olan dezenformasyon ve manipülasyon, toplumsal bağışıklık gerektiren bir olgudur. Bu bağlamda, oyunlaştırma, geleneksel eğitim yöntemlerinin ötesine geçen, güçlü ve ölçeklenebilir bir müdahale aracı olarak öne çıkmaktadır. Oyunlaştırma, sadece gençlere yönelik bir eğlence aracı olarak görülmemelidir; her yaştan bireyin dijital ortamdaki haklarını koruması ve siber tehditlere karşı uyanık olması için düşük maliyetli, erişimi kolay ve son derece etkili bir yöntem sunar. Oyunlar, sıkıcı olabilecek bilişsel savunma mekanizmalarını eğlenceli bir deneyime dönüştürerek, bireylerin kendi rızalarıyla ve aktif olarak öğrenme sürecine katılmasını sağlar.

Bir toplumun demokratik direncinin ve siber hijyeninin seviyesi, o toplumdaki bireylerin manipülasyonun mutfağını, yalan haberlerin ve komplo teorilerinin nasıl hazırlandığını ne kadar iyi anladığıyla doğrudan bağlıdır. Bu kritik anlayışı inşa etmenin en güçlü ve modern pedagojiyle uyumlu

[86] Maertens, R., Roozenbeek, J., Basol, M., & van der Linden, S. (2021). Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. *Journal of Experimental Psychology: Applied*, *27*(1), 1–16. https://doi.org/10.1037/xap0000315

stratejilerinden biri, "kötü olmayı öğreterek iyi kalmayı sağlamak" ilkesidir. Bu yaklaşım, bilişsel aşılama temeline dayanır; tıpkı bir virüse karşı vücuda zayıflatılmış antijen verilmesi gibi, bireylere dezenformasyon tekniklerinin minik ve kontrollü dozları sunulur. Birey, bu teknikleri bizzat uygulayarak veya deşifre ederek, bu tekniklere karşı zihinsel antikorlar geliştirir. Bu strateji, bireyin zekasına güvenir, didaktik bir yaklaşımdan kaçınır ve kişiyi pasif bir alıcıdan aktif bir eleştirel düşünür haline getirir.

Bilişsel aşılamadan geçmiş, dezenformasyon tekniklerini tanıyan bir birey için bile, bu bilgilere sahip olmayan ve bir komplo teorisine inanmış bir yakınıyla oyundaki meşhur "enişte" figürü ile tartışmaya girmek zorlayıcı olabilir. Bu tür durumlar, sadece bilgi farkından değil, aynı zamanda derin kişisel bağlar ve duygusal yüklerden dolayı hassastır. Bu tür çatışmacı potansiyeli yüksek durumları, ilişkiyi zedelemeden ve savunmacı tepkilere yol açmadan yönetmek hayati önem taşır.

TEMEL ÇIKARIMLAR

Geleneksel medya okuryazarlığı eğitimleri genellikle "pasif" bilgi aktarımına, didaktik modele dayanır ve günümüzün hızla evrilen manipülasyon ortamında yetersiz kalmaktadır.

Temel Kavramlar ve Mekanizmalar

Hak Temelli Yaklaşım: Dezenformasyonla mücadele teknik bir sorun değil; seçme, sağlık ve ayrımcılığa uğramama haklarını koruyan bir insan hakları mücadelesidir.

Aktif Aşılama: Bireyin sadece doğru bilgiyi dinlemesi değil, manipülasyon taktiklerini (trolleme, duygu sömürüsü vb.) bir simülasyon içinde bizzat üreterek ve uygulayarak öğrenmesi sürecidir.

Çürüme Etkisi: Tıpkı tıbbi aşılarda olduğu gibi, bilişsel aşılamayla kazanılan direncin de zamanla (genellikle 3-6 ay içinde) azalması fenomenidir. Zihin, uyaranlara karşı duyarlılığını yitirebilir.

Hatırlatma Dozu: Çürüme etkisini kırmak ve zihinsel uyanıklığı sürdürmek için periyodik olarak verilmesi gereken kısa, oyunlaştırılmış mikro eğitimlerdi.

6.2. KENDİNİZİ TEST EDİN

Soru 1: *Harmony Square* oyunu, oyunculara hangi spesifik insan hakkını hedef alan manipülasyonları öğretmeyi amaçlar?

A) Sağlık hakkı

B) Seçme ve katılma hakkı

C) Telif hakkı

D) Tüketici hakkı

Soru 2: Yapay zekâ (YZ) çağında neden sadece teknolojik tespit araçlarına güvenemeyiz ve insan odaklı (oyunlaştırma gibi) çözümlere ihtiyaç duyarız?

A) YZ çok pahalı olduğu için teknolojik tespit açısından kullanılamaz

B) İnsanlar oyun oynamayı çok sevdiği için

C) Kanunlar, YZ kullanımını yasakladığı için

D) YZ'nın %100 doğru olmadığı durumlarda, insan aklına ihtiyaç olduğu için

Soru 3: Oyunlardaki "aktif aşılama" yönteminin, geleneksel eğitimden ayrılan temel pedagojik prensibi nedir?

A) Pasif izleme

B) Ezberleme

C) Simülasyon ve rol yapma

D) Cezalandırma (Yanlış yapanı oyundan atma)

6.2. MERAKLISINA EK KAYNAKLAR

Cook, J. 2021. "Cranky Uncle: A game building resilience against climate misinformation", PlusLucis, 3, 13–19

RESAID Project. (2024). *Creating social cognitive resilience against information disorders: Bilgi notu*. İstanbul Bilgi Üniversitesi

Roozenbeek, J., ve Van der Linden, S. 2020. "Breaking Harmony Square: A game that "inoculates" against political misinformation", The Harvard Kennedy School (HKS) Misinformation Review, 1(8). https://doi.org/10.37016/mr-2020-47

UN Human Rights Council. (2021). *Disinformation and freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/47/25). United Nations.

Kutuplaşmış Ortamda Diyalog İmkânı

Dezenformasyonla mücadele stratejilerinde sıklıkla yapılan ve başarısızlığa yol açan en temel varsayım, karşıdaki bireyin yanlış bilgiye sahip olmasının tek nedeninin "bilgisizlik" veya "doğru veriye erişememe" olduğu inancıdır. Bu duruma bilişsel psikoloji ve iletişim bilimleri literatüründe "bilgi açığı modeli" adı verilir. Bu modelin basit ve iyimser mantığına göre, eğer hedef kitleye bilimsel olarak kanıtlanmış, doğru verileri, ikna edici grafikleri, güvenilir raporları ve uzman görüşlerini sunabilirseniz, bu rasyonel bilgi akışı onların yanlış inançlarını değiştirmelerini ve dolayısıyla davranışlarını düzeltmelerini sağlayacaktır.

Ancak, modern bilişsel bilim araştırmaları ve sosyal psikoloji deneyleri, insan karar verme süreçlerinin bu ideal rasyonel modeli nadiren takip ettiğini ortaya koymaktadır. İnsanlar, özellikle kutuplaşmış veya yüksek riskli konularda bir bilgiye inanıp inanmamaya karar verirken, sunulan rasyonel verinin içeriğinden ziyade, kaynağın niyetine ve aidiyetine odaklanırlar. Bu, bir tür bilişsel kısayoldur; bilginin doğruluğunu değerlendirmek yerine, kaynağın güvenilirliğini değerlendirmek daha hızlı ve duygusal olarak daha güvenlidir.

🎧 **DİNLE**

Turkuazlab tarafından hazırlanan podcast serisinde kutuplaşma üzerine farklı disiplinlerden konukların söyleşilerini dinleyebilirsiniz.

🔗https://open.spotify.com/show/1oqMFdD-KIOMAM2zmQZbEuv?si=6a6c13e328a74ec2

Güven, dezenformasyon çağında merkezi bir öneme sahiptir iki ana bileşenden oluşur. Bunlardan ilki yetkinlik bileşenidir. Bu bileşen, kaynağın bilgi ve becerisine odaklanır. Sorulan temel soru şudur: "Bu kişi/kurum,

sunduğu konu hakkında yeterli bilgiye, uzmanlığa ve deneyime sahip mi?" Bu, rasyonel ve teknik bir değerlendirmedir. İkinci bileşen samimiyettir. Bu bileşen, kaynağın niyetine ve sosyal aidiyetine odaklanır. Sorulan temel sorular şunlardır: "Bu kişi bizden mi? Benim/bizim iyiliğimizi mi istiyor? Bize karşı dürüst mü? Benim değerlerimi paylaşıyor mu?" Bu, duygusal ve aidiyete dayalı bir değerlendirmedir.

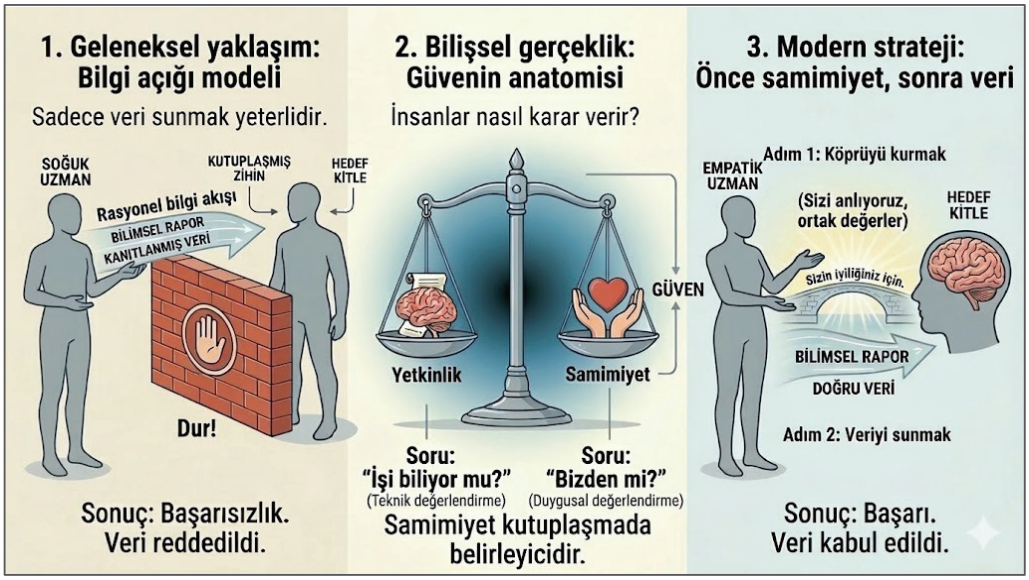
Toplumsal veya siyasal olarak kutuplaşmış bir ortamda, bireyler bilgi kaynağını değerlendirirken yetkinliğe değil, samimiyete net bir öncelik verirler. Bu, şu kritik durumu yaratır: Dünyanın alanında en yetkin, Nobel ödüllü profesörü bile olsa, eğer hedef kitle tarafından "karşı mahalleden", bir başka deyişle kendi değer setlerine yabancı veya düşmanca niyetli olarak algılanıyorsa, sunduğu en doğru, bilimsel ve kanıtlanmış veri dahi anında ve duygusal bir refleksle reddedilir. Bu reddediş, veriyi çürütmeye çalışmaktan ziyade, kaynağı itibarsızlaştırma veya niyetini sorgulama şeklinde gerçekleşir.

Bu bilişsel gerçeklik, dezenformasyonla mücadele eden kamu kurumları, medya kuruluşları ve sivil toplum örgütleri için stratejik bir zorunluluk yaratır. İletişim stratejisi artık sadece "veri aktarımı" üzerine kurulu olamaz. Başarılı bir strateji, veri aktarımından ve yanlış bilginin çürütülmesinden önce, hedef kitleyle aradaki "samimiyet" bileşenini inşa etmeye odaklanmalıdır.

Bu, şu anlama gelir: İletişim kampanyaları, sadece ne kadar doğru olduklarını göstermek yerine, kimin tarafında olduklarını, neyi önemsediklerini ve hedef kitlenin iyiliğini gerçekten istediklerini göstermelidir. Güven inşası olmadan sunulan yetkinlik temelli veri, kutuplaşmış zihinlerde sadece karşıt mahallenin bir propaganda aracı olarak algılanacaktır. Bu nedenle, dezenformasyona karşı verilen savaş, bir bilgi savaşı olmaktan çok, bir güven savaşıdır.

Psikolojik Engel: Geri Tepme Etkisi

Birini ikna etmeye çalışırken karşılaşılan en büyük ve en inatçı direnç biçimi, geri tepme etkisidir.[87] Bu psikolojik fenomen, yaygın kanının aksine, insanların temel inançlarına zıt düşen sağlam, bilimsel veya mantıksal bir kanıtla karşılaştıklarında, fikirlerini makul bir şekilde değiştirmek yerine, tam tersine, eski inançlarına daha da sıkı sarılmalarını ifade eder. Bu etki, özellikle siyasi, dini, ahlaki veya kimliksel öneme sahip konularda zirveye ulaşır ve rasyonel iletişimin neden sıklıkla başarısız olduğunu açıklar.



Şekil 6.3.1 *Yanlış bilgiye karşı "güven"in rolü*

Geri tepme etkisinin kökleri, beynin en ilkel savunma mekanizmalarında yatmaktadır. Fonksiyonel manyetik rezonans görüntüleme (fMRI) çalışmaları, bir bireyin güçlü siyasi, ideolojik veya kişisel kimliğini oluşturan bir inanca doğrudan saldırıldığında, beynin rasyonel muhakeme merkezleri

[87] Nyhan, B., & Reifler, J. (2010). When corrections fail: The persistence of political misperceptions. *Political Behavior*, *32*(2), 303–330. https://doi.org/10.1007/s11109-010-9112-2

yerine, tehdit algılama ve hayatta kalma merkezlerinin aktive olduğunu göstermektedir.

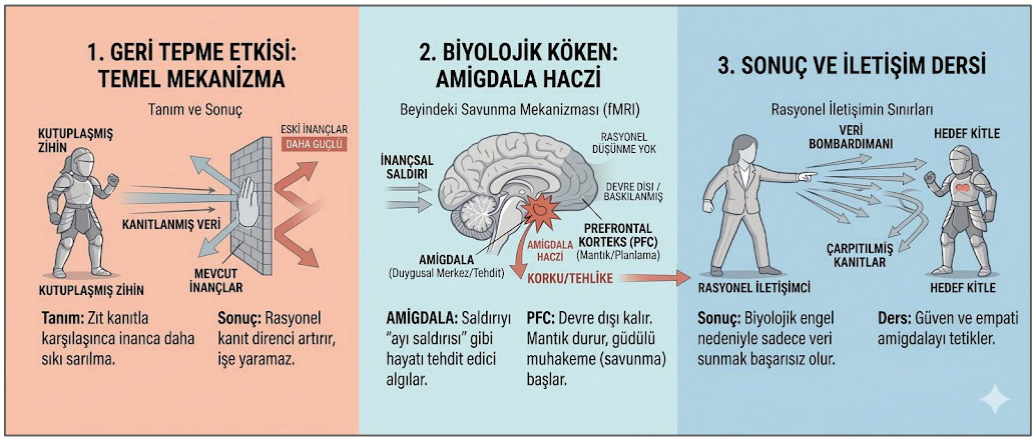
Beynin amigdala bölgesi, korku, tehdit ve tehlike algılamasından sorumlu olan duygusal merkezi, bu tür bir inançsal saldırı sırasında şiddetle aktive olur. Beyin, "savunduğun parti hatalı ve senin bilgin yanlış" şeklindeki bir bilgiyi, biyolojik olarak "ormanda karşına ayı çıktı" veya "fiziksel bir tehlike altındasın" gibi bir hayati tehditle aynı kategoride değerlendirir. Bu "amigdala haczi" anında, beynin mantık, planlama ve eleştirel düşünmeden sorumlu en gelişmiş kısmı olan prefrontal korteks (PFC) adeta "devre dışı" kalır veya baskılanır. Vücut ve zihin, gelen bilgiyi analiz etmek yerine, kendini savunmaya programlanır.

PFC devre dışı kaldığında, kişi sunulan kanıtı kabul etmek yerine, onu çürütmek için duygusal olarak "güdülenmiş muhakeme" yapmaya başlar. Bu, mantıksal bir çıkarım değil, kişinin mevcut inancını korumak için bilinçsizce seçilen, yanlışları, boşlukları veya alternatif yorumları arayan bir bilişsel süreçtir. Kişi, karşıt kanıtı çürütecek yeni "kanıtlar" uydurmaya veya var olanları çarpıtmaya zorlanır.

Geri Tepme Etkisini tetikleyen bir diğer kritik faktör, paylaşılan bilginin kişinin sosyal kimliği ve dünya görüşü ile ne kadar derinden ilintili olduğudur. Eğer paylaşılan bir yalan haber, kişinin ait olduğu grubu, siyasi görüşünü veya temel ahlaki çerçevesini destekliyorsa (Örn: "Zaten X grubu hep tehlikelidir" veya "Y partisi kasıtlı olarak zarar veriyor"), bu haberi yalanlamak, sadece tek bir bilgiyi çürütmek anlamına gelmez. Bu, kişinin tüm dünya görüşünü, sosyal kimliğini ve ait olduğu grubun temel anlatısını tehdit etmek demektir.

İnsanlar, doğruluğundan emin olmadıkları bir habere bile, kendi gruplarının üyeleri inanıyorsa inanmaya eğilimlidirler. Yanlış bile olsa, grup inancına sıkı sıkıya sarılmak, sosyal uyumu korumak ve gruptan dışlanmama

riskini bertaraf etmek için rasyonel bir seçim haline gelir (Kahneman'ın "Hızlı ve Yavaş Düşünme" sistemlerine benzer bir kısa yol). Bu nedenle, bu tür bir inanca karşı sunulan kanıt, sadece bilişsel bir çatışma yaratmakla kalmaz, aynı zamanda varoluşsal bir tehdit algısı oluşturur. Sonuç olarak, kanıta karşı gösterilen direnç çok daha sert olur ve inancın gücü, kanıtın aksine orantılı olarak artar. Kanıtın dozu arttıkça, inanç daha da pekişir.



Şekil 6.3.2 *Geri tepme etkisi ve amigdala haczi*

Stratejiler

Dezenformasyon ve manipülasyon çağında, gerçeği savunmanın geleneksel yöntemleri maalesef yetersiz kalmaktadır. İletişimde sıklıkla yapılan kritik bir hata, yalanı tekrar ederek onu pekiştirmek ve bu yolla farkında olmadan zihinsel bir köprü kurmaktır. Bu duruma çözüm getiren, bilişsel dilbilimci George Lakoff tarafından geliştirilen ve nörobilim temellerine dayanan tekniktir: Hakikat sandviçi modeli.[88] Bu yaklaşım, dezenformasyonu çürütürken, iletişim odağını yalanın kendisinden, doğru bilgiye ve yalanın yayılma taktiğine kaydırmayı hedefler. Medyada ve günlük tartışmalarda en sık karşılaşılan ve

[88] Lakoff, G. (2018). *The all new Don't think of an elephant!: Know your values and frame the debate*. Chelsea Green Publishing.

en az etkili olan tepki biçimi şöyledir: *"İddia: Aşılar kısırlık yapıyor mu? (yalanın tekrarı) -> Cevap: Hayır, yapmıyor."*

Oysa insan beyni, nörolojik düzeyde değillemeleri işleme konusunda zorluk çeker. Bu durum, hepimizin bildiği bir deneyle açıklanabilir: Size "Fil düşünme" dendiğinde, zihninizde ilk canlanan imge bir fildir. Beyniniz, komutu yerine getirmek için önce "fil" kavramını aktive eder, ardından bunu iptal etmeye çalışır. Aynı mekanizma, dezenformasyon bağlamında çalıştığında, "aşı" ve "kısırlık" gibi kritik kelimeleri yan yana kullandığınızda, cevabınız "hayır" olsa bile, beyin bu iki kavram arasında nörolojik bir bağ kurar. Bu bağlantı, zamanla yalanın kaynağını unutturarak, zihinde o iddiaya dair bir "iz" kalmasına neden olur.

🎧 DİNLE

Bilişsel dilbilimci George Lakoff, bu videoda dezenformasyonun beynimizdeki çalışma mekanizmasını ve neden "yalanı tekrar etmememiz" gerektiğini anlattığı bölümü dinleyebilirsiniz.

🔗 https://www.youtube.com/watch?v=KuAYev4mi2M

Hakikat sandviçi modeli, etkili ve gerçeğe odaklı bir iletişim kurmayı amaçlayan üç katmanlı bir yapı üzerine inşa edilmiştir. Amaç, yalanın pekiştirilmesini önlemek ve dinleyicinin zihnini doğrudan doğru çerçeveye yerleştirmektir.

📌 ÖRNEK SENARYO:

"Mülteciler sınavsız üniversiteye giriyor" iddiası

Bu iddia, toplumdaki gençlerin gelecek kaygısını ve sınav stresini istismar eden yaygın bir dezenformasyon örneğidir.

❌ **Yanlış Tepki (Geleneksel Savunma):** *"Hayır, mülteciler sınavsız girmiyor, bu yalan. Herkes sınava girmek zorunda."* (Bu tepki, "mülteci" ve "sınavsız giriş" kelimelerini yan yana getirerek iddiayı zihinsel olarak pekiştirir ve savunma pozisyonunda kalır. Beyin olumsuzlamaları işlerken zorlanır ve yalanı tekrar duymuş olur)

Hakikat Sandviçi Uygulaması:

1. Üst Katman (Gerçek ve Değerler): İletişime ortak bir zemin ve tartışılmaz bir gerçekle başlayın: *"Türkiye'de üniversite eğitimi, liyakate dayalı bir sistemin ürünüdür ve tüm öğrenciler için Yükseköğretim Kurumu (YÖK) tarafından belirlenen merkezi sınav kriterlerine tabidir. Üniversiteler, ulusal ve uluslararası geçerliliği olan, objektif başarı şartları aramaktadır."*

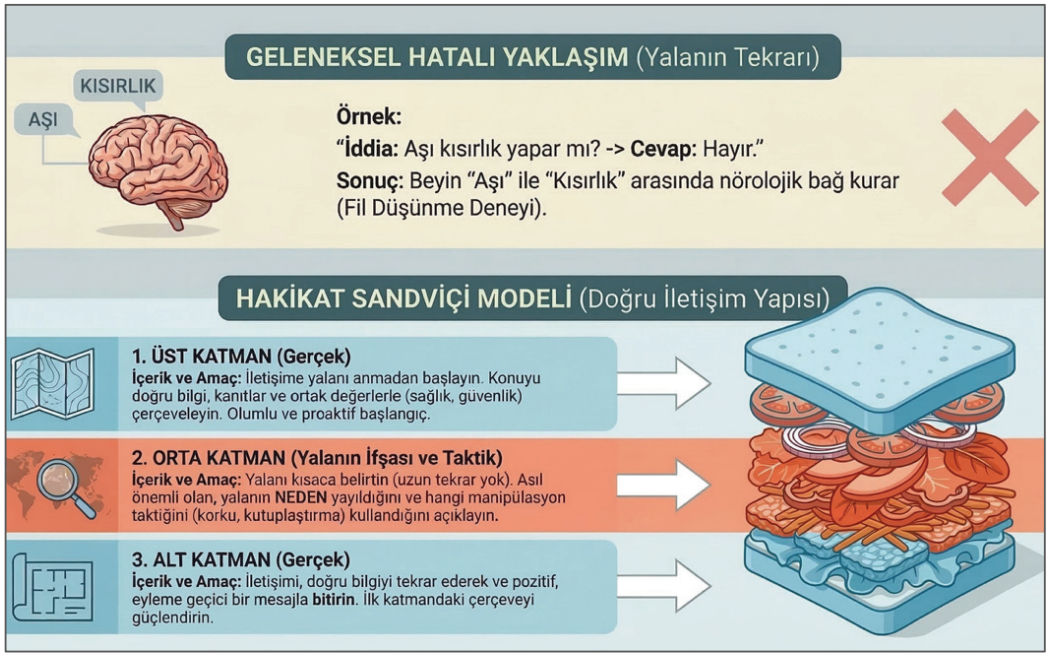
2. Orta Katman (Yalanın İfşası ve Taktik): Yalanı tekrar etmek yerine, bu yalanın neden yayıldığını ve arkasındaki taktiği ifşa edin: *"Ne yazık ki, bazı sosyal medya ağları ve manipülatif gruplar, özellikle gençlerin gelecek kaygısını ve haklı sınav stresini suistimal ederek, onları öfkelendirmek amacıyla 'sınavsız geçiş' gibi asılsız yalanları yaymaktadır. Bu, toplumsal huzuru bozmayı hedefleyen, duygu sömürüsü üzerine kurulu net bir kışkırtma taktiğidir."*

3. Alt Katman (Güçlendirilmiş Gerçek): Konuyu kapatırken doğru bilgiyi detaylandırın ve son sözün "gerçek" olmasını sağlayın: *"Gerçek şu ki, yabancı uyruklu öğrenciler dahi, kendi statülerine uygun olan ve YÖK tarafından akredite edilmiş, belli bir zorluk derecesine sahip Yabancı Öğrenci Sınavı (YÖS) gibi sınavlardan geçmek veya uluslararası geçerliliği olan SAT, ACT gibi test sonuçlarını sunmak zorundadırlar. Kontenjan dahilinde kabul alırlar ve hiçbir kesime sınavsız, kayıtsız bir geçiş hakkı tanınmamaktadır. Üniversiteye kabul, her zaman bilgi ve başarıya dayanır."*

İkinci strateji ise empatik çürütme stratejisidir. Karşınızdaki kişi, arkasına sığındığı anonimlik zırhıyla size saldıran kötü niyetli bir trol değilse; aksine, samimi ancak endişeli bir ebeveyn, güvendiğiniz bir arkadaş ya da aile büyüğü ise, kuru bir bilgi doğrulama yöntemi olan Hakikat Sandviçi yaklaşımı

fazla didaktik, soğuk ve hatta kırıcı kalabilir. Bu tip hassas durumlarda iletişim stratejisinin merkezine Empati yerleşmelidir. Unutulmamalıdır ki, buradaki birincil amaç bir tartışmayı *kazanmak* veya haklı çıkmak değil, öncelikle karşıdaki kişiyle duygusal bir bağ kurmaktır ve ancak bu bağ üzerinden doğru bilgiye zemin hazırlamaktır.

Stratejinin ilk adımı olan "duyguyu onayla ve eşlik et" (samimiyet) aşamasında, paylaşılan içerik yalan veya manipülatif olsa bile, o içeriğin kişide tetiklediği korku, endişe veya vatanseverlik gibi temel duyguların tamamen gerçek olduğu kabul edilmelidir. Bu noktada yapılması gereken, kişinin duygusunu yargılamadan, "Çocukların sağlığı veya ülkemizin güvenliği konusundaki endişeni çok iyi anlıyorum, ben de aynı kaygıları taşıyorum" gibi ifadelerle onaylamaktır. Bu aşamada sergilenen yüksek yetkinlik değil, kişinin hislerine değer verildiğini gösteren samimiyet ve ortak insanlık duygusu kritiktir.



Şekil 6.3.3 *Hakikat sandviçi modeli*

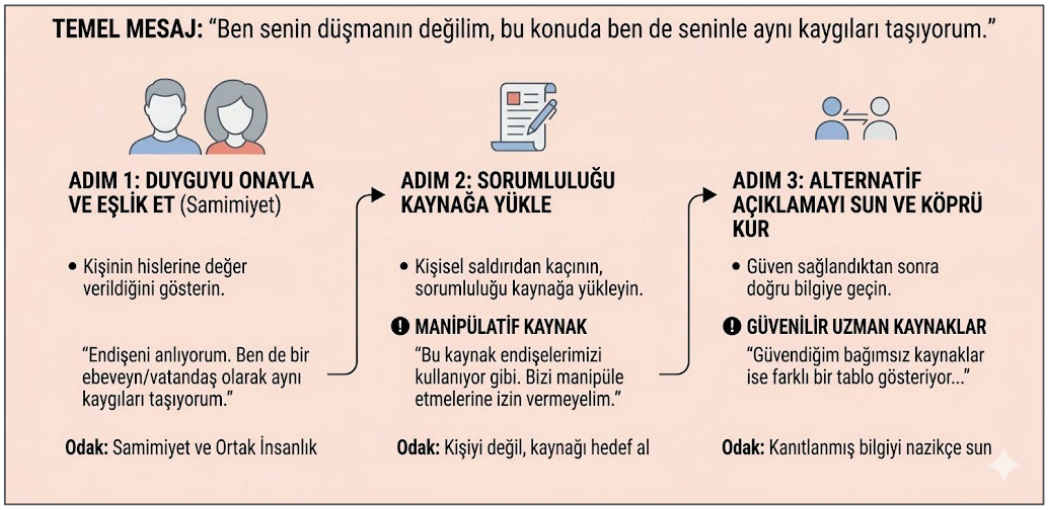
Empatik çürütme sürecinin ikinci adımı olan “suçu kaynağa atmak”tır. Muhatabın "kandırıldığını" veya "saf olduğunu" ima etmekten kesinlikle kaçınılmalıdır; çünkü bu tür imalar kişisel bir saldırı olarak algılanır ve kişiyi anında savunma pozisyonuna iter. İletişim kanalını açık tutmak için yapılması gereken, sorumluluğu kişiye değil manipülasyonun kaynağına yüklemektir. Örneğin, "Haberi yayan kaynağa baktım; sanki bizim bu içten endişelerimizi bir araç olarak kullanıp tık almaya veya ürün satmaya çalışıyorlar, iyi niyetimizin suistimal edilmesine izin vermeyelim" şeklindeki bir yaklaşım, kişinin itibarını korurken öfkesini de doğrudan dezenformasyon kaynağına yönlendirir.

Empatik çürütme sürecinin üçüncü ve son adımı olan “alternatif açıklamayı sun ve köprü kur”, ancak karşı tarafla ortak bir zemin ve güven ilişkisi tesis edildikten sonra uygulanmalıdır. Bu aşamada, doğrudan sert bir çürütme yapmak yerine, "Benim bu konularda güvendiğim, daha bağımsız ve uzman kaynaklar ise olayın tam olarak böyle olmadığını, farklı bir tablo olduğunu gösteriyor..." ifadesiyle, kanıtlanmış doğru bilgiler nazikçe ve suçlayıcı olmayan bir dille sunularak gerçeğe geçiş sağlanır.

Sosyal medyada veya aile WhatsApp grupları gibi toplu iletişim alanlarında, paylaşılan yanıltıcı bir bilgiyi herkesin önünde sert ve çürütücü bir dille düzeltmekten kesinlikle kaçınılmalıdır. Bu tür bir kamusal düzeltme, kişinin sosyal statüsünü ve itibarını doğrudan tehdit ettiği için, muhatap hatasını kabul etmek yerine savunma refleksine geçer ve iletişim kanalları tamamen tıkanır. Bu çıkmazı aşmanın en etkili yolu, kişiyle sadece ikinizin göreceği özel bir kanaldan (DM veya özel mesaj) iletişime geçmektir. Örneğin; "Seni zor durumda bırakmamak için gruba yazmadım ama bu bilgi galiba eski veya montajlanmış olabilir; istersen şu güvenilir kaynağa bir bak, belki kaldırmak istersin" şeklindeki yapıcı yaklaşım kurtarıcıdır. Muhatabın itibarını korumaya odaklı bu ince düşünceli davranış, uyarının kişisel bir saldırı olarak

algılanmasını önleyerek kişinin doğru bilgiyi dikkate almasını sağlayan en nazik ve etkili yöntemdir.

Kutuplaşmış toplumlarda dezenformasyonla mücadele stratejisi, geleneksel bir "bilgi savaşı" paradigmasından köklü bir biçimde ayrılmalıdır. Başarılı bir karşı koyuş, olgusal doğruluğu mutlak zafer olarak görmekten ziyade, temelde bir "ilişki yönetimi" meselesidir. İnsanları yalnızca verilerle, karşı argümanlarla veya literatürde *fact-bludgeoning* olarak adlandırılan kanıtlarla "döverek" ikna etme çabası genellikle ters teper. Bu tür bir yaklaşım, karşı tarafın savunma mekanizmasını tetikler, kimlik temelli inançlarını pekiştirir ve bilgiye olan güveni daha da zedeler.



Şekil 6.3.4 *İkna ve güven inşası için 3 adımlı strateji*

Karşı tarafın savunma mekanizmasını tetikleyerek kimlik temelli inançlarını pekiştiren ve bilgiye olan güveni zedeleyen sert yaklaşımların aksine, etkili bir iletişim süreci; muhataba yargılayıcı bir pozisyondan değil, bir birey olarak değer verildiğinin ve sesinin duyulduğunun hissettirilmesiyle başlamalıdır. Dezenformasyonun genellikle kişilerin varoluşsal korkularına, ekonomik kaygılarına veya aidiyet ihtiyaçlarına dokunduğu gerçeğinden

hareketle, bu temel endişeleri küçümsemek veya rasyonel dışı olarak etiketlemek yerine ciddiye alıp anlamaya çalışmak hayati önem taşır. Bu süreçte karşıdaki kişinin bir düşman değil potansiyel bir ortak olduğu vurgulanmalı; nihai amaç kişiyi yanlış inançlarından vazgeçmeye zorlamak değil, empati ve ortak insani değerler zemininde ortak bir gerçeği ve toplumsal refahı birlikte bulmaya davet etmek olmalıdır.

Unutulmamalıdır ki, dezenformasyonun birincil ve en sinsi amacı bizi birbirimize düşürmek, kutuplaşmayı derinleştirmek ve toplumsal dokuyu parçalamaktır. Bu nedenle, dezenformasyona karşı en büyük ve en güçlü direniş eylemi, birbirimizle konuşmaya devam edebilmek, zorlu konular hakkında bile olsa diyalog kanallarını açık tutabilmek ve farklı görüşlere sahip olsak bile insan onurunu koruyarak iletişim kurma becerisini kaybetmemektir. Diyalog, kutuplaşmanın panzehiridir. Bu bölümde ele alınan bireysel ve kişilerarası iletişim çabalarının ötesine geçerek, dezenformasyona karşı uzun vadeli ve yapısal bir savunma hattı oluşturulması gerekmektedir.

TEMEL ÇIKARIMLAR

Dezenformasyonla mücadele sadece bir "bilgi savaşı" değil, temelde bir "güven ve ilişki yönetimi" meselesidir. İnsanların yanlış bilgiye inanmasının tek nedeni bilgisizlik değildir; asıl neden aidiyet ve güven arayışıdır. Bu bölüm, karşıt inançlara sadece verilerle ve sertçe saldırmanın ters tepeceğini, bunun yerine beynin savunma mekanizmalarını aşmak için önce bağ kurmayı, sonra düzeltmeyi önerir.

Temel Kavramlar ve Mekanizmalar

Geri Tepme Etkisi: Bir inanca doğrudan kanıtla saldırıldığında, beynin tehdit algılayarak, amigdala haczi rasyonel düşünmeyi kapatması ve kişinin eski inancına daha sıkı sarılması fenomenidir.

Hakikat Sandviçi: Yalanı ilk sırada söyleyerek veya tekrar ederek zihinde pekiştirmek yerine; iletişimi "doğru bilgi-yalanın ifşası/taktiği-doğru Bilgi" katmanlarıyla kurma stratejisidir.

Bilgi Açığı Modeli: "İnsanlara sadece doğru veriyi sunarsak fikirlerini değiştirirler" şeklindeki, psikolojik faktörleri yok sayan hatalı varsayımdır.

Empatik Çürütme: "Önce bağ kur, sonra düzelt" ilkesine dayanır. Karşıdaki kişinin duygusunu onaylayıp suçu kişiye değil onu kandıran kaynağa atarak savunma duvarlarını indirme tekniğidir.

6.3. KENDİNİZİ TEST EDİN

Soru 1: "Hakikat sandviçi" tekniğinin temel prensibi nedir?

A) Yalanı en başta söyleyerek dikkat çekmek ve ardından çürütmek

B) Gerçeğe hiç değinmeden, sadece yalanın mantıksızlığını eleştirmek, yalanı tüm boyutları ile ele almak

C) Gerçeği en başa ve en sona koyarak, yalanı bu iki katmanın arasına sıkıştırıp tekrarını minimize etmek

D) Yalan haberi olduğu gibi paylaşıp altına "buna inanmayın" notu düşmek

Soru 2: "Geri tepme etkisi" riskini azaltmak için iletişimde hangi unsura öncelik verilmelidir?

A) Zekâ ve bilgi üstünlüğü

B) Samimiyet ve güven

C) Uzmanlık ve otorite

D) Ses tonunu yükselterek baskınlık kurmak

Soru 3: Bir yakınınızın WhatsApp grubunda bariz bir yalan haber paylaştığını gördünüz. İletişim psikolojisine göre en etkili tepki nedir?

A) Grupta herkesin önünde "Bu paylaştığın yalan, haber kaynaklarını araştırmadan paylaşma!" diyerek uyarmak

B) Tepki olarak grubu sessizce terk etmek

C) Kişiye "Seni zor durumda bırakmamak için gruba yazmadım ama bu bilgi şüpheli olabilir" diyerek nazikçe özel alanda uyarmak

D) Haberi yayan kaynağa siber saldırı düzenlemek

6.3. MERAKLISINA EK KAYNAKLAR

Erdoğan, E. ve Uyan-Semerci, P. (2020). *Türkiye'de kutuplaşmanın boyutları 2020 araştırması*. İstanbul Bilgi Üniversitesi Göç Çalışmaları Uygulama ve Araştırma Merkezi & TurkuazLab. https://turkuazlab.org/ilgili-projelerimiz/turkiyede-kutuplasmanin-boyutlari-2020/

Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E., Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., . . . Zaragoza, M. S. (2020). *The debunking handbook 2020*. George Mason University. https://climatecommunication.gmu.edu/wp-content/uploads/2023/09/DebunkingHandbook2020.pdf

Bilişsel Süreçlerin Yönetimi ve YZ Okuryazarlığı

Geleneksel medya okuryazarlığı kavramı, 20. yüzyılın sonlarında ve 21. yüzyılın başlarında, temel olarak bilgiye erişim ve kaynak doğrulaması üzerine kurulmuştu. Bu klasik modeller, bireylere bir kütüphanede veya basılı bir gazetede "doğru, güvenilir bilgiye nasıl ulaşılacağını" ve sahte bir haberi yüzeysel özelliklerinden nasıl ayırt edeceklerini öğretmeye odaklanmıştır. Bu yaklaşım, bilginin kıt olduğu ve dağıtımının görece merkezi olduğu bir çağ için işlevseldi. Ancak, günümüzün hiper-bağlantılı, doygun dijital ekosisteminde, bu yaklaşımın yetersizliği kritik bir sorun haline gelmiştir. Artık sorun bilgiye erişim değil, bilgi fazlalığı, algoritmik filtreleme, yapay zekâ destekli içerik üretimi ve duygu odaklı içerik akışlarının bireyin dikkatini ve bilişsel kapasitesini sömürme biçimidir. Kullanıcıların zihinsel süreçlerini hedef alan bu yeni yapı, geleneksel okuryazarlığın öngörmediği, çok daha karmaşık bir psikolojik ve bilişsel savunma mekanizmasını gerektirmektedir.

Güncel araştırma ve eğitim felsefeleri, modern eğitimin amacının köklü bir paradigma değişimine uğraması gerektiğini savunur. Temel hedef, bireyin zihinsel işlemci modunu kökten değiştirmek olmalıdır. Eğitim, bireyi sadece bir enformasyon alıcısı olmaktan çıkarıp, maruz kaldığı içeriği, içeriğin üretildiği ve yayıldığı bağlamı ve en önemlisi kendi zihinsel süreçlerini-önyargıları, duygusal tepkileri, düşünce kısayollarını sürekli ve sistematik olarak sorgulayan “aktif, eleştirel ve kendi kendini yöneten bir değerlendiriciye” dönüştürmeyi amaçlamalıdır.

Bu kritik dönüşüm, bireyin dijital dünyada toplumsal bağışıklığını ve psikolojik direncini artırmak için üç ana ve birbiriyle sürekli etkileşim halinde olan sütun üzerine inşa edilir. Bireyin dijital dünyadaki toplumsal bağışıklığını ve psikolojik direncini artırmayı hedefleyen bu kritik dönüşüm, birbiriyle sürekli etkileşim halindeki üç ana sütun üzerine inşa edilmiştir. İlk sütun olan

“bilişsel süreçlerin yönetimi”, bireyin duygusal tepkilerle beslenen otomatik ve hızlı karar alma mekanizmalarını, kısayolları fark edip durdurmasını; bunların yerine dezenformasyona karşı zihinsel bir kalkan işlevi gören yavaş, analitik ve kanıta dayalı düşünce sistemini yerleştirmesini ifade eder. Bu zihinsel zemini tamamlayan “dijital ve yapay zekâ yetkinlikleri”, teknolojiyi sadece kullanmanın ötesine geçerek algoritmaların ve yapay zekânın bilgi akışını nasıl şekillendirdiğini anlamayı, üretilen içeriklerin ardındaki niyetleri okumayı ve dijital ayak izini bilinçli yönetmeyi kapsar. Yapının son ayağı olan “toplumsal direnç” ise bireyin manipülasyon kampanyalarının yarattığı kutuplaşma ve güvensizlik iklimine karşı empati, farklılıklara açıklık ve manipülatif dili hızla tanıma becerileriyle psikolojik bir dayanıklılık geliştirmesini sağlar. Sonuç olarak, 21. yüzyılın medya okuryazarlığı artık sadece bilgiye ulaşım becerisi değil, dijital manipülasyona karşı bir bilişsel savunma stratejisi ve sürekli bir zihinsel uyanıklık halidir.

Bilişsel Süreçleri Değiştirmek: Sezgiden Analize Geçiş

Sosyal medya platformlarının mimarisi (beğeni butonları, hızla akan içerik akışları, sürekli bildirimler) insan beynini, düşünme süreçlerinin daha yüzeysel, hızlı ve duygusal olan "sezgisel işlemleme" (*heuristic processing*) moduna geçmeye zorlar. Nobel ödüllü psikolog Daniel Kahneman'ın çığır açan çalışmasında tanımladığı üzere, bu işleyiş biçimi, zihinsel enerjiden tasarruf eden, otomatik ve duygusal temelli sistem 1'e karşılık gelir. Ne yazık ki, dezenformasyon ve manipülatif içerikler tam olarak bu "zihinsel kısa yolları" hedef alarak ve hackleyerek yayılım gösterme yeteneği kazanır.

Toplumsal bağışıklık eğitiminin temel misyonu, bireylere kendi zihinlerinin otomatik pilotta kullandığı, ancak dezenformasyon bağlamında büyük risk taşıyan iki ana bilişsel kısa yolu tanıtmak ve farkındalık yaratmaktır. Duygu sezgiselliği, bireyin bir içeriğin yarattığı yoğun duygusal tepkiyi

bilginin gerçekliği veya önemi ile yanlışlıkla ilişkilendirmesine yol açar. İçerik ne kadar güçlü bir duygu tetiklerse, beyin o kadar "Bu önemli ve doğru olmalı" şeklinde bir kısa devre yaşar. Dezenformasyonun duygusal kışkırtıcılığı, bu tuzağı kullanarak hızla yayılır.[89] Bulunabilirlik sezgiselliği kısa yolu, bir bilginin kolay hatırlanabilir, sıkça tekrar edilmiş veya birçok farklı kaynakta, özellikle sosyal medyada görülmüş olmasının, o bilginin doğruluğunu kanıtladığı yanılsamasını yaratır. "Bu haberi defalarca Instagram'da, Twitter'da ve üç ayrı WhatsApp grubunda gördüm. Her yerde bu konuşuluyorsa, kesin doğrudur" düşüncesi, tekrarlanan yanlış bilginin gerçeklik algısını nasıl değiştirdiğini gösterir. Beyin, tekrarlanma yoğunluğunu gerçeklik veya önem yoğunluğu ile karıştırır.

Diğer bölümlerde de detaylı ele aldığımız üzere modern ve etkili bir toplumsal bağışıklık eğitimi, bireyin bu otomatik, sezgisel (sistem 1) düşünme modunu bilinçli olarak devre dışı bırakmasını hedefler. Sosyal psikolog Gordon Pennycook ve ekibinin (2020) geliştirdiği "soğruluk sürtmeleri" (*accuracy-nudge*) adı verilen müdahale yöntemi, tam da bu amaca hizmet eder.[90] Bu yöntem, kullanıcıların bir içeriği paylaşmadan veya beğenmeden hemen önce dikkatlerini "sosyal onaydan" (Ne kadar beğeni alacağım? Hangi tepkileri toplayacağım?) "doğruluğa" (Bu bilginin kaynağı güvenilir mi? Bu bilgi gerçek mi?) çevirmesini sağlamaya odaklanır. Eğitim, bireye güçlü bir zihinsel refleks kazandırmayı amaçlar: *Ne zaman bir içerik şiddetli bir duygusal tetiklenme (öfke, şok, korku) yaratırsa, sistem 1 devreye girmişse, anında dur.* Bu duraklama, bireyin hızlı, duygusal tepki modundan (sistem

[89] Lu, J., & Xiao, Y. (2024). Heuristic information processing as a mediating factor in the process of exposure to COVID-19 vaccine information and misinformation sharing on social media. *Health Communication*, *39*(12), 2779–2792. https://doi.org/10.1080/10410236.2023.2288373

[90] Pennycook, G., McPhetres, J., Zhang, Y., Lu, J. G., & Rand, D. G. (2020). Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy-nudge intervention. *Psychological Science*, *31*(7), 770–780. https://doi.org/10.1177/0956797620939054

1) daha yavaş, mantıksal, analitik ve kanıt temelli düşünme moduna (Daniel Kahneman'ın sistem 2'si) geçmesini sağlar. Bu beceri, bir bilginin *doğruluğunu araştırmaktan* bile daha önceliklidir; çünkü bu, bireyin düşünme biçimini ve karar alma mekanizmasını temelden değiştiren bir psikolojik savunma mekanizmasıdır. Amaç, paylaşım dürtüsü gelmeden önce, eleştirel düşünme filtresini devreye sokmaktır.

"Güçlü Anlamda" Eleştirel Düşünme

Bilgi okuryazarlığı, bireylerin yalnızca bilgiye erişimini değil, aynı zamanda bilgiyi anlama, değerlendirme ve etik bir şekilde kullanma becerilerini de kapsar. Bu beceri seti, özellikle dezenformasyon ve manipülasyonun yaygın olduğu çağımızda, toplumsal bağışıklığın temel direklerinden birini oluşturur. Bilgi okuryazarlığı ile doğrudan ilişkili olan eleştirel düşünme, bu bağlamda hayati bir önem taşır. Ancak tüm eleştirel düşünme biçimlerinin aynı amaca hizmet etmediğini ve farklı etkilere yol açtığını anlamak, eğitim ve iletişim stratejileri için kilit noktadır.

Hollis (2019), eleştirel düşünmenin toplumsal bağışıklık ve bireysel gelişim açısından taşıdığı potansiyelleri analiz ederek iki temel türü birbirinden ayırır.[91] Bunlardan ilki olan "zayıf anlamda eleştirel düşünme" (*weak-sense critical thinking*), temelde hakikati aramaktan ziyade mevcut inancı veya pozisyonu korumayı amaçlayan bir savunma mekanizması olarak işler. Bu yaklaşımda birey, eleştirel düşünme becerilerini ve mantıksal argümantasyonu yalnızca kendi dünya görüşünü, inanç sistemini veya aidiyet hissettiği grubun fikirlerini tehdit eden karşıt bilgilere karşı kullanır. Karşıt görüşleri çürütmek veya geçersiz kılmak için yoğun bir zihinsel çaba harcanırken, kişinin

[91] Hollis, H. (2019). Information literacy and critical thinking: Different concepts, shared conceptions. *Information Research*, *24*(4), paper colis1921. http://InformationR.net/ir/24-4/colis/colis1921.html

kendi görüşünü destekleyen manipülatif bilgiler eleştirel bir süzgeçten geçirilmez. Bu durum, bireyin kendi haklılığını sürekli teyit etmesine yol açarak yankı odalarını ve filtre balonlarını güçlendirir, nihayetinde ise toplumsal kutuplaşmayı daha da derinleştirir.

Toplumsal bağışıklık ve bilişsel esneklik için asıl hedeflenen yöntem olan "güçlü anlamda eleştirel düşünme" (*strong-sense critical thinking*), eleştirel sorgulamayı sadece dış dünyaya değil, aynı zamanda bireyin kendi iç dünyasına da yönlendiren ideal düşünme biçimidir. Bu yaklaşım, bireyin sadece kaynak güvenilirliği veya kanıtların gücü gibi dışsal faktörleri değil; kendi dünya görüşünü, yerleşik önyargılarını ve bir bilgiye inanma ya da inanmama isteğinin altındaki psikolojik nedenleri de sorgulamasını şart koşar. Sürecin anahtarı, odağı içselleştirerek "Bu haber yalan mı?" şeklindeki geleneksel sorudan, "Ben neden bu haberin doğru olmasını (veya olmamasını) bu kadar çok istiyorum?" sorusuna geçiş yapmaktır; bu derin içsel sorgulama, bilişsel cesaret ve entelektüel dürüstlük gerektirerek bireyi doğrulama yanlılığı (*confirmation bias*) gibi temel zihinsel tuzaklarla yüzleştirir. Eğitim müfredatlarının ve toplumsal iletişim kampanyalarının temel amacı, bireyleri zayıf anlamda eleştirel düşünme tuzağından çıkarıp, güçlü anlamda eleştirel düşünme becerisiyle donatmaktır. Bu, öğrencilere sadece dış dünyayı analiz etmeyi değil, aynı zamanda kendi iç dünyalarındaki bilişsel önyargıları analiz etmeyi ve yönetmeyi öğretmek anlamına gelir. Bireylerin, bir bilgiye karşı oluşan ilk duygusal tepkilerini fark etmeleri ve bu tepkilerin bilginin rasyonel değerlendirmesini nasıl engellediğini anlamaları, psikolojik savunmanın en önemli adımıdır. Kendi önyargılarını ve inanç temellerini sürekli sorgulayan bireylerden oluşan bir toplum, dezenformasyona karşı daha yüksek bir kolektif bağışıklık geliştirir.

Dijital Navigasyon ve Yapay Zekâ Okuryazarlığı

Zihinsel olarak dezenformasyona karşı bir savunma mekanizması oluşturmak, bu savunmayı etkili teknik ve uygulamalı becerilerle güçlendirmeyi zorunlu kılar. Bilişsel hazırlık tek başına yeterli değildir; pratik, uygulanabilir araçlara ihtiyaç vardır. Dezenformasyonla mücadelede en etkili ve evrensel kabul gören yöntem, Stanford Üniversitesi'nde yapılan araştırmaların[92] sonucunda ortaya konulan ve profesyonel doğruluk kontrolü uzmanlarının "altın standardı" olarak benimsediği önceki bölümlerde de ele aldığımız yanal okuma tekniğidir. Bu yöntem, bir kaynağın güvenilirliğini sorgularken izlenen temel davranış kalıplarını kökten değiştirir.

Geleneksel internet kullanım alışkanlıklarına dayanan "dikey okuma" yaklaşımında kullanıcılar, bir web sitesine ulaştıklarında kaynağın güvenilirliğini yalnızca o sitenin sunduğu içsel sinyallere bakarak değerlendirme eğilimindedir. Bu yanıltıcı süreçte kullanıcı; öncelikle sitenin görsel tasarımının profesyonelliğini, dilbilgisi kurallarına uygunluğunu ve kurumsal görünümünü inceler (iç gözlem). Ardından, sitenin kendi beyanına dayanan "hakkımızda" sayfasına giderek misyon, vizyon ve yönetim kadrosu bilgilerini kontrol eder (kurumsal inceleme). Son olarak, sitenin alan adı uzantısına (.org, .edu, .gov gibi) bakarak kurumsal bir meşruiyete sahip olup olmadığına karar verir (alan adı analizi). Ancak bu yöntem, modern dezenformasyon sitelerinin vitrinlerini profesyonelce kurgulayabilmesi nedeniyle kullanıcıyı sitenin kendi kapalı döngüsüne hapseden tehlikeli bir tuzaktır. Ancak, modern dezenformasyon ve propaganda siteleri, bu "vitrini" son derece kolay ve inandırıcı bir şekilde taklit edebilme yeteneğine sahiptir. Yanıltıcı alan adları, sahte yönetim kurulu üyeleri ve profesyonel site tasarımları, dikey okuma

[92] Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record*, *121*(11), 1–40. https://doi.org/10.1177/016146811912101102

yapan amatör kullanıcıları kolayca tuzağa düşürebilir.

📌 **ÖRNEK UYGULAMA:** FİNLANDİYA MODELİ

Open Society Institute Medya Okuryazarlığı Endeksi'nde birinci sırada yer alan Finlandiya, dezenformasyona karşı "Çoklu Okuryazarlık" modelini uygulamaktadır. 2014 yılında yenilenen ulusal müfredatla birlikte medya okuryazarlığı, tek bir ders olmak yerine tüm disiplinlere entegre edilmiş bir yetkinlik olarak ele alınmıştır. Bu bütüncül yaklaşımda öğrenciler; matematikte istatistik manipülasyonlarını, görsel sanatlarda görüntü tahrifatını, tarih derslerinde propaganda tekniklerini ve dil derslerinde retorik hileleri analiz etmeyi öğrenirler. Modelin temelini; eğitimin anaokulu seviyesinde başlaması, nitelikli öğretmenlere yöntem konusunda otonomi tanınması ve kütüphanelerin her yaş grubu için birer dijital destek merkezi olarak işlev görmesi oluşturur. Finlandiya, bu modelle dezenformasyonu teknolojik bir sorundan ziyade bir eğitim ve demokrasi meselesi olarak konumlandırmaktadır.

Kaynak:
🔗https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

Profesyonel teyitçiler, dikey okuma'nın bu zafiyetini bilerek tam tersi bir strateji uygularlar; şüpheli veya bilinmeyen bir kaynağın web sitesine girildiği anda, o sitede vakit kaybetmek yerine derhal oradan ayrılırlar. Siteden çıkan uzman, tarayıcıda eş zamanlı olarak 3-4 yeni sekme açarak "bağımsız doğrulama" sürecini başlatır. Bu aşamada tüm sorgulama süreci, kaynağın kendi beyanlarına dayanan "Bu kaynak kendi hakkında ne söylüyor?" sorusu yerine, dışsal ve objektif bir bakış açısı sunan "İnternetin geri kalanı bu kaynak, yazar veya iddia hakkında ne söylüyor?" temel sorusu üzerine kurgulanır. Bir kaynağın gerçek güvenilirliği, o kaynağın *kendisi* tarafından sunulan imajla değil; bağımsız, yerleşik ve güvenilir kabul edilen diğer harici kaynakların (örneğin; Wikipedia'daki ilgili madde, uluslararası teyit platformları, köklü ve saygın haber kuruluşlarının araştırmaları veya akademik

yayınlar) o kaynak hakkındaki değerlendirmeleri, eleştirileri ve referansları ile ölçülür. Bu sayede, kaynağın kendi iç propaganda tuzağına düşmek engellenir.

Yapay zekâ teknolojilerinin hızla ilerlediği günümüzde, medya ve bilgi okuryazarlığı kavramı sadece "deepfake" gibi görsel veya işitsel aldatmacaları tanımaktan öteye geçerek derinleşmek zorundadır. Frau-Meigs'in (2024) işaret ettiği gibi, bireylerin pasif birer tüketici olmaktan çıkıp, bilgi akışını yöneten görünmez kuralları, algoritmaları anlayan yeni bir beceri setine sahip olmaları elzemdir.[93] Bu yeni yetkinlik; kullanıcının "Bu içerik bana ne amaçla gösterildi?" sorusunu sorarak Hedef Analizi yapmasını ve içeriğin siyasi eğilimler, korkular veya tüketim alışkanlıkları gibi hangi özel veriler kullanılarak (*micro-targeting*) kendisine sunulduğunu anlamak için veri noktası tespiti gerçekleştirmesini kapsar.

Yapay zekâ tarafından üretilen veya otomatikleştirilmiş sistemler aracılığıyla yayılan dezenformasyon, bazen kusursuz bir yüzeye sahip olabilir; ancak bu kusursuzluğun ardında, insan gözünün veya geleneksel doğrulama yöntemlerinin kolayca atlayabileceği küçük, tutarsız ipuçları "zayıf sinyaller" gizlenir. Bu sinyalleri fark etme yeteneği kritik bir savunma mekanizması olup, üç temel kategoride kendini gösterir: İlk olarak, metin akıcı bir dille yazılmış olsa dahi temel argümanlarında veya çıkarımlarında apaçık mantık hataları, çelişkiler veya dayanağı olmayan sıçramalar içeren mantıksal tutarsızlıklar; ikinci olarak, yüksek çözünürlüklü görsellerdeki ışık-gölge uyumsuzlukları, insan anatomisine uymayan, özellikle el ve dişlerdeki deformasyonlar, fizik kurallarına aykırı yansımalar veya arka plan tekrarları gibi görsel ve fiziksel anormallikler. Son olarak, bir sosyal medya hesabının paylaşım sıklığındaki anormal artışlar, tek konuya odaklanma, robotik yorumlar veya

[93] Frau-Meigs, D. (2024). Algorithm literacy as a subset of media and information literacy: Competences and design considerations. *Digital*, *4*(2), 512–528. https://doi.org/10.3390/digital4020026

sadece tek kaynaktan paylaşım yapma gibi davranışsal anormallikler (bot tespiti), içeriğin organik bir kaynaktan değil, organize bir kampanyanın parçası olarak yayıldığını işaret eder.

Toplumsal ve Demokratik Direnç

İlk bölümde de belirttiğimiz üzere RESAID projesinin temel felsefesini oluşturan Biyoekolojik Model[94], dezenformasyon ve bilgi düzensizlikleriyle mücadelede eğitimi geleneksel bir beceri seti kazanımının ötesine taşır. Bu model, bireyin bilgi ekosistemini ve toplumsal güvenliğini etkileyen tüm katmanları (mikro, mezo, ekso ve makro sistemler) dikkate alarak, eğitimi kolektif bir güvenlik mekanizması ve temel bir insan hakkı meselesi olarak konumlandırır. Bu yaklaşım, toplumsal dayanıklılığın inşasında eğitimin stratejik rolünü vurgular.

Bilgi düzensizlikleri, modern demokrasilerin ve bireysel refahın temelini sarsan derin bir tehdit oluşturarak, manipülatif içerikler ve kasıtlı yanlış bilgiler yoluyla bireylerin akılcı ve sağlıklı karar alma süreçlerini doğrudan felç etmektedir. Bu tehdit, öncelikle sağlık hakkı bağlamında kendini gösterir; pandemi dönemlerinde de tecrübe edildiği üzere, kanıta dayalı olmayan ve komplo teorileriyle beslenen yanlış bilgiler, bireylerin bilimsel temelli kararlar almasını engelleyerek halk sağlığını tehlikeye atarken, eğitimin rolü bireyi doğru değerlendirme yetisiyle donatarak bu temel hakkı korumaktır. Benzer şekilde seçme hakkı açısından bakıldığında; özellikle seçim dönemlerinde yürütülen hedefli dezenformasyon kampanyaları, seçmenlerin algılarını çarpıtıp özgür iradeyle tercih yapma yetisini zayıflatmakta, eğitim ise bu noktada siyasi katılımın manipülasyondan arınmış bir zeminde gerçekleşmesini sağlayan hayati bir demokrasi kalkanı işlevi görmektedir.

---

[94] Bronfenbrenner, U. (2005). *Making human beings human: Bioecological perspectives on human development*. Sage.

DİNLE

InfodemiLab tarafından hazırlanan ve sağlık hakkı bağlamında bilgi düzensizliklerini ele alan podcast bölümlerini dinleyebilirsiniz.

https://open.spotify.com/show/6SpabfqM7Eds2Ct5wu4Qai?si=6c358df5d84d4b97

Dezenformasyonun nihai hedefi, bireyin dışarıdan gelen bir etkiyle yönlendirilmesini sağlamaktır. Relihan'ın (2025) çalışmaları, karmaşık sorunları basitleştiren sahte ikilemler yaratma, toplumun belirli bir kesimini tüm sorunların kaynağı ilan eden günah keçisi ilanı gibi psikolojik manipülasyon taktiklerinin önceden tanınmasının önemini vurgular. Eğitim, bireylere korku ve öfke gibi duygusal tetikleyicileri fark etme yetisi kazandırarak, onların manipülatörler tarafından duygusal olarak "hacklenmesini" ve tepkilerinin yönlendirilmesini engeller. Bu savunmanın merkezinde yer alan bilişsel aşılanma stratejisi ise, zihni zayıflatılmış manipülasyon argümanlarına önceden maruz bırakarak gelecekteki saldırılara karşı direnç geliştirilmesini sağlar; böylece bireyin kararlarının dış aktörlerin çıkarına değil, tamamen kendi hür iradesi ve rasyonel değerlendirmesine dayanmasını teminat altına alan temel bir psikolojik savunma mekanizması işlevi görür.

Dezenformasyonun en yıkıcı sosyal sonuçlarından biri, toplum içinde derin siyasi ve sosyal fay hatları yaratarak kutuplaşmayı körüklemesidir. "biz vs. onlar" gibi ayrıştırıcı anlatılar, çoğunlukla duygusal tepkiler ve önyargılar üzerine inşa edilir. Eğitim, bu ayrıştırıcı anlatıları sadece içeriksel değil, aynı zamanda teknik düzeyde, kaynak, yayılma biçimi, hedef kitlesi gibi noktaları analiz etme becerisi sunar. Bir anlatının ardındaki propaganda mekanizmasını anlamak, bireylerin o anlatıya duygusal yatırım yapmasını zorlaştırır. Kutuplaşmanın azalması, farklı görüşlere sahip gruplar arasında diyalog ve iş

birliği potansiyelini artırır. Eğitim yoluyla dezenformasyona karşı toplumsal bir direnç oluşturulması, kamusal alana olan inancı ve kolektif sorun çözme kapasitesini güçlendirir, böylece demokrasinin sağlıklı işleyişi için elzem olan sosyal sermayeyi korur.

Bu bölümde detaylı biçimde incelediğimiz bilişsel aşılama, eğitsel oyunlaştırma, empatik iletişim stratejileri ve bilişsel çerçeve dönüşümü gibi yaklaşımlar, dezenformasyonla mücadeleyi salt bir "teknik" filtreleme veya içerik kaldırma operasyonundan çıkararak, meselenin derinlikli ve hayati öneme sahip "insani" boyutuna taşır. Bu stratejiler, bireyin sadece yanlış bilgiyi tanımasını değil, aynı zamanda manipülatif niyetleri sezebilmesini ve duygusal tetikleyicilere karşı direnç geliştirmesini sağlayan bir "toplumsal bilişsel bağışıklık" sistemi inşa etmeyi amaçlar.

Ancak, tıpkı fiziksel bağışıklık sisteminde olduğu gibi, eğitimle ve bilinçli çabayla kazanılan bu bilişsel savunma reflekslerinin zamanla zayıflaması, bilimsel literatürde çürüme etkisi (*decay effect*) olarak bilinen bir gerçektir. İnsan zihni, yeni ve cazip uyaranlara karşı doğal bir ilgi duyarken, tekrar eden veya eskiyen bilgilere karşı dirençli hale gelebilir. Dezenformasyon aktörlerinin taktikleri sürekli evrimleştiği ve yeni psikolojik manipülasyon teknikleri geliştirdiği düşünüldüğünde, toplumsal direnci bir defalık bir eğitimle sağlamak yeterli olmayacaktır.

Bu zayıflamayı önlemek ve toplumsal bilişsel direnci sürekli yüksek tutmak elzemdir. Bu nedenle, ulusal sağlık otoritelerinin uyguladığı tıbbi aşı takvimlerine benzer şekilde, dezenformasyonla mücadele eğitimleri de ömür boyu sürecek bir yapıya kavuşturulmalıdır. Bu yapı, "hatırlatma eğitimleri" şeklinde tasarlanmalıdır. Uzun ve sıkıcı dersler yerine, bu hatırlatma dozları kısa, etkileşimli, günlük yaşam akışına entegre edilebilecek şekilde oyunlaştırılmış modüller (örneğin, 5 dakikalık senaryo tabanlı simülasyonlar, kısa quizler) olarak sunulmalıdır. Kullanıcıların en çok zaman geçirdiği sosyal

medya platformları, haber uygulamaları, hatta bankacılık/e-devlet uygulamaları gibi dijital arayüzlere uygun, bağlamsal hatırlatmalar şeklinde entegre edilerek farkındalık düzeyi sürekli canlı tutulmalıdır. Bireyin en çok maruz kaldığı dezenformasyon türüne (örneğin, siyasi kutuplaşma, sağlık bilgileri, ekonomik manipülasyon) göre kişiselleştirilmiş "hatırlatma dozları" sunularak etkinliği maksimize edilmelidir.

Nihayetinde, dezenformasyonla sürekli ve başarılı bir mücadele, teknoloji ile insan psikolojisinin kesiştiği bu alanda, statik bir savunma hattı yerine, sürekli güncellenen ve taze tutulan dinamik bir toplumsal bilişsel savunma sistemi kurmaktan geçer. Bu, uzun vadede demokratik süreçlerin sağlığını ve toplumsal huzuru korumanın anahtarıdır.

TEMEL ÇIKARIMLAR

Yeni nesil medya okuryazarlığı, sadece teknik bir bilgi bulma becerisi değil; bireyin sistem 1 (hızlı/duygusal) tepkilerini bilinçli olarak baskılayıp, sistem 2 (yavaş/analitik) düşünceyi devreye soktuğu köklü bir bilişsel dönüşümdür. Gerçek bağışıklık, sadece başkalarının yalanlarını yakalamakla (zayıf anlamda eleştirel düşünme) değil; bireyin kendi önyargılarını ve "ben buna neden inanmak istiyorum?" sorusunu sorarak kendi inançlarını sorguladığı güçlü anlamda eleştirel düşünme ile sağlanır.

Temel Kavramlar ve Mekanizmalar

Sistem 1 ve Sistem 2: Daniel Kahneman'ın tanımladığı beyin işleyiş modelidir. Sistem 1, dezenformasyonun hedef aldığı hızlı, otomatik ve duygusal moddur. Sistem 2 ise yavaş, enerji harcayan ve analitik düşünme modudur. Eğitimin amacı, paylaşım yapmadan önce sistem 2'yi devreye sokmaktır.

Yanal Okuma (*Lateral Reading*): Bir kaynağın güvenilirliğini, o kaynağın kendi sayfasında kalarak (dikey okuma) değil; tarayıcıda yeni sekmeler açıp bağımsız kaynakların o site hakkında ne dediğini araştırarak doğrulama stratejisidir.

Güçlü Anlamda Eleştirel Düşünme (*Strong-Sense Critical Thinking*): Eleştirel okları sadece dış dünyaya değil, kişinin kendi dünya görüşüne ve önyargılarına da yöneltmesi halidir. Zıttı olan "zayıf anlamda" düşünme ise sadece karşıt görüşleri çürütmek için kullanılır.

Biyoekolojik Model: Medya okuryazarlığını sadece teknik bir beceri olarak değil; sağlık hakkı ve seçme ve seçilme hakkı gibi temel insan haklarını koruyan, bireyin çevresiyle etkileşimini esas alan bütüncül yaklaşımdır.

6.4. KENDİNİZİ TEST EDİN

Soru 1: Stanford Üniversitesi araştırmalarına dayanan "yanal okuma" tekniği, bir web sitesinin güvenilirliğini kontrol ederken ne yapmayı önerir?

A) Siteyi detaylıca incelemeyi

B) O site hakkında bağımsız kaynakların ne dediğini araştırmayı

C) Sadece alan adı uzantısına (.com, .org) bakmayı

D) Haberi yazan gazeteciye e-posta atmayı

Soru 2: Yapay zekâ çağında medya okuryazarlığının yeni bir boyutu olan YZ okuryazarlığı, kusursuz görünen sahte içerikleri tespit etmek için aşağıdaki ipuçlarından hangisini aramayı öğretmez?

A) İçeriğin ne kadar çok beğenildiğini

B) Metindeki mantıksal tutarsızlıkları

C) Görsellerdeki fiziksel anormallikleri

D) Bot benzeri davranışsal ipuçlarını

Soru 3: Güçlü anlamda eleştirel düşünme ile zayıf anlamda eleştirel düşünme arasındaki temel fark nedir?

A) Zayıf olan sadece başkalarını eleştirirken; güçlü olan kişinin kendi görüşlerini de sorgulamasını içerir.

B) Güçlü olan daha fazla zekâ ve analitik bakış gerektirir.

C) Zayıf olan sadece metinleri inceler, güçlü olan videoları, görselleri derinlemesine analiz eder.

D) Aralarında bir fark yoktur.

6.4. MERAKLISINA EK KAYNAKLAR

Bronfenbrenner, U., & Morris, P. A. (2006). The bioecological model of human development. In R. M. Lerner & W. Damon (Der.), *Handbook of child psychology: Theoretical models of human development* (Cilt. 1). Wiley. https://doi.org/10.1002/9780470147658.chpsy0114

Digital Inquiry Group. (2020). *Intro to lateral reading*. Civic Online Reasoning. https://cor.inquirygroup.org/curriculum/lessons/intro-to-lateral-reading/

Bölüm 7

Dijital Yönetişim, Hukuk ve Etik: "Brüksel Etkisi"nden Küresel Standartlara

🎯 TARTIŞMA SORULARI

1. Brüksel etkisi dijital platformları ve küresel standartları nasıl şekillendiriyor?
2. Bilgi düzensizlikleri ile mücadelede devletlerin ve teknoloji şirketlerinin rolü nedir?
3. İfade özgürlüğü ve erişim özgürlüğü farkı nedir?
4. Dezenformasyon zincirini kırmakta bireylerin sorumlulukları nelerdir?
5. Bilgi düzensizliklerine karşı mücadelede sivil toplum ve akademinin sorumlulukları nelerdir?

Giriş

Bu bölüm, dezenformasyonla mücadelenin sadece bireysel bir dikkat veya teyitçilik çabası değil, aynı zamanda sistemsel bir dijital yönetişim zorunluluğu olduğu gerçeğinden hareketle kurgulanmıştır. Önceki bölümlerde ele alınan bireysel savunma mekanizmalarının ötesine geçilerek, dijital ekosistemin kaynağında nasıl temizlenebileceği ve algoritmik yapıların nasıl denetlenebileceği tartışılacaktır. İnternetin denetimsiz dönemini sona erdiren eş-düzenleme modeli ve Avrupa Birliği'nin pazar gücünü kullanarak küresel standartları belirlediği Brüksel Etkisi mercek altına alınacaktır. Ayrıca, devletlerin güvenliği nasıl sağlayabileceğine dair kritik bir etik zemin sunan ifade özgürlüğü ile erişim özgürlüğü ayrımı ve devlet-platform-sivil toplum iş birliğine dayalı çok paydaşlı çözüm haritası detaylıca ele alınacaktır.

İZLE

RESAID tarafından hazırlanan açık erişim derslerin *Çok Boyutlu Müdahale ve Yaklaşımlar* başlıklı bölümü izlemeniz konuyu daha kolay anlamanıza yardımcı olacaktır.

Giriş
https://youtu.be/4EpVw8olTXc
Türkiye ve Ötesinden Müdahale Yaklaşımları
https://youtu.be/qqRHCfSzYbM

Platform Yönetişiminin Evrimi

Dezenformasyonla mücadele tartışmaları, kaçınılmaz olarak şu temel soruya dayanır: Bireysel bilinç, içinde bulunulan bilgi ortamı yapısal olarak zararlı ve sistematik riskler barındırıyorsa ne ölçüde etkili olabilir? Dijital ortam, tarafsız bir kamusal alan olmaktan ziyade, belirli ekonomik teşvikler, teknik tercihler ve politik kararlar doğrultusunda tasarlanmış bir alandır. Kullanılan

“zehirli kuyu” metaforu, durumu açıklar: Suyu kaynatmayı öğretmek yerine, suyun kaynağının sistematik biçimde kirlenmesini engellemek gerekir. Algoritmalar, dikkat çekmek ve kullanıcıları platformda tutmak için öfke, korku ve çatışma gibi yüksek etkileşim üreten içerikleri öne çıkarır. Bu mimari, yanlış bilginin yayılmasını yalnızca mümkün değil, aynı zamanda avantajlı hale getirir. Sorun, tek tek kullanıcıların dikkatsizliğinden değil, dikkatli olmayı sürekli zorlaştıran bir mimarinin varlığından kaynaklanmaktadır. Bu nedenle dezenformasyonla mücadele, yalnızca bireysel eğitimle sınırlı değil, aynı zamanda sistemsel bir yönetişim zorunluluğudur.

İnternetin ilk dönemlerindeki "teknolojinin kendi kendini düzenleyeceği" varsayımı ve platformların tarafsız aracı olarak konumu, inovasyonu hızlandırsa da veri ihlalleri, seçim manipülasyonları ve nefret kampanyaları gibi ciddi yan etkilerle yetersiz kaldı. "Kendi kendini düzenleme" fikrinin kamu yararını korumakta başarısız olması, dijital yönetişim tartışmalarını kaçınılmaz hale getirdi. Yönetişim, burada yalnızca devlet müdahalesi değil, devletler, teknoloji şirketleri, sivil toplum ve akademinin sorumluluklarının paylaşıldığı daha geniş bir düzen arayışıdır. Amaç, ifade özgürlüğünü zedelemeden kamusal alanı sistematik zararlardan koruyacak bir denge kurmaktır.

İnternetin kısa tarihi, dijital altyapının doğuşundan günümüzün karmaşık küresel düzenleme arayışlarına kadar uzanan, mutlak özgürlükten (liberteryanizm) düzenlenmiş sorumluluğa doğru evrilen dinamik bir sarkaç hareketini andırır. Bu sarkaç, temel olarak iki büyük dönemeçten geçmiştir: siber ütopyanın hüküm sürdüğü kendi kendini düzenleme dönemi ve günümüzün eş-düzenleme arayışları. İnternetin ilk 20 yılında, yaklaşık 1990'ların ortalarından 2010'ların sonuna kadar, Web 1.0 ve Web 2.0'ın başları, dijital dünyaya hâkim olan ideoloji "siber ütopyacılık" veya "teknoloji liberteryanizmi" idi. Bu görüş, teknolojinin doğası gereği özgürleştirici olduğuna, devletlerin

internete müdahale etmemesi gerektiğine ve teknolojinin yol açtığı sorunları da yine kendi iç dinamikleriyle (piyasa güçleri ve topluluk kuralları) çözeceğine varsaydı. Bu dönemin temel hukuki ve felsefi taşı, ABD'de kabul edilen İletişim Ahlakı Yasası'nın Madde 230'u (*Section 230 of the Communications Decency Act*) idi. Bu kritik madde, internet platformlarına benzersiz bir koruma kalkanı sağladı: Facebook, X veya YouTube gibi platformlar, kullanıcıların paylaştığı içeriklerin yasal sorumluluğu açısından bir "yayıncı" değil, sadece bir "platform" veya "interaktif bilgisayar hizmeti sağlayıcısı" olarak kabul edildi. Bu platformlar, kullanıcıların paylaştığı yalanlardan, hakaretlerden, nefret söyleminden veya hukuka aykırı diğer içeriklerden sorumlu tutulamazdı. Yasa koyucular, bu dokunulmazlığın, internetin serbestçe gelişmesini, inovasyonu teşvik etmesini ve ifade özgürlüğünü korumasını amaçladı. Bu hukuki dokunulmazlık ve pazar baskısı, platformların devasa ve eşi benzeri görülmemiş bir hızla büyümesini sağladı. Ancak, bir süre sonra ciddi bir yan etki ortaya çıktı: Sorumsuzluk. Teknoloji şirketlerinin kâr maksimizasyonunu kullanıcı güvenliği ve toplumsal refahın önüne koyması, dijital dünyadaki denetimsiz "Vahşi Batı" döneminin sonunu getiren temel faktör olmuştur. 2018'deki Cambridge Analytica skandalıyla milyonlarca Facebook kullanıcısının verilerinin siyasi manipülasyon için izinsiz kullanılması, Myanmar'da Rohingya Müslümanlarına yönelik soykırıma varan şiddetin Facebook üzerinden yayılan nefret söylemiyle körüklenmesi ve yabancı aktörlerin algoritmaları kullanarak demokratik seçimlere müdahale etmesi bu sürecin en çarpıcı örnekleridir. Yaşanan bu olaylar zinciri, teknoloji devlerinin kamu yararını feda ettiğini ve kendi kendilerini etkin bir şekilde denetleyemediklerini tartışmasız bir şekilde ortaya koyarken, sebep olduğu toplumsal zararlarla birlikte "siber ütopyacılık" dönemini de fiilen sona erdirmişti.

Kendi kendini düzenleme modelinin başarısızlığının ardından, internetin geleceğine dair iki uç modelden, devletin her şeyi kontrol ettiği “Leviathan”

modeli ve her şeyin piyasaya bırakıldığı “Laissez-Faire” modeli, kaçınılarak daha dengeli bir yol aranmaya başlandı. Bu model, internetin temel özgürlüklerini korurken, platformları yol açtıkları zararlar konusunda sorumlu tutmayı amaçlar. "Eş-düzenleme" olarak adlandırılan bu sistemde sorumluluklar, kamu otoritesi ve özel sektör arasında paylaşılır; devlet veya AB gibi ulusüstü kurumlar, "seçim bütünlüğünün sağlanması" veya "nefret söyleminin 24 saatte kaldırılması" gibi temel hedefleri ve kamu yararı sonuçlarını belirlerken, teknoloji şirketleri bu hedeflere ulaşmak için gerekli "davranış kodları"nı ve teknik çözümleri geliştirmekle yükümlüdür. Bu modelin en somut ve kapsamlı örnekleri ise, platformları şeffaflık ve risk yönetimi konusunda bağlayıcı kurallara tabi tutan Avrupa Birliği'nin Dijital Hizmetler Yasası (DSA) ve Dijital Piyasalar Yasası (DMA) ile hayata geçirilmiştir. Bu yasalar, platformların şeffaflık, risk değerlendirmesi ve hesap verebilirlik yükümlülüklerini katılaştırmaktadır. DSA, platformları içerik denetimi ve dezenformasyonla mücadele konusunda daha sıkı kurallara uymaya zorlar.

Dezenformasyon Hakkında Uygulama Kuralları *(Code of Practice on Disinformation)* eş-düzenlemenin klasik bir örneğidir. Google, Meta, TikTok gibi büyük platformlar, AB Komisyonu'nun gözetiminde, dezenformasyonla mücadele etmek için kendi iç politikalarını, algoritmik şeffaflık önlemlerini ve iş birliklerini taahhüt ederler. AB Devletleri, bu taahhütlerin yerine getirilip getirilmediğini bağımsız denetçiler aracılığıyla kontrol eder. Bu yeni dönem, internetin ne tamamen serbest ne de tamamen kontrol altında olduğu, aksine paylaşılan bir sorumluluk mekanizması üzerinden ilerlediği bir geleceğe işaret etmektedir. Sarkaç, artık mutlak özgürlükten, hedefleri kamu otoritesi tarafından belirlenen, uygulanması ise teknoloji şirketlerinin sorumluluğunda olan düzenlenmiş bir dengeye doğru kaymıştır.

Avrupa Birliği ve "Brüksel Etkisi"

Dijitalleşmenin hâkim olduğu çağda küresel güç, yalnızca ekonomik ve askeri kapasiteye değil, aynı zamanda kuralları belirleme becerisine dayanır. Bu durumu özetleyen popüler ifade şöyledir: *"ABD icat eder, Çin kopyalar (ve duvar örer), Avrupa ise kuralları yazar."* Bu söylem, Avrupa Birliği'nin teknolojik yeniliklerin merkezi olmasa bile, bu yenilikleri düzenleyen hukuki çerçeveleri oluşturmadaki benzersiz etkisini vurgular. Hukuk profesörü Anu Bradford'ın kavramsallaştırdığı "Brüksel etkisi" (*The Brussels effect*), AB düzenlemelerinin, özellikle büyük çok uluslu şirketlerin uyum karmaşasından kaçınmak için bu kuralları fiilen küresel standart haline getirmesini ifade eder. GDPR ile başlayan bu etki, yeni dijital yasalarla zirveye ulaşmıştır.[95]

AB, son yıllarda dijital ekonominin ve toplumsal yaşamın her veçhesini kapsayan, çığır açıcı bir düzenleyici çerçeve oluşturmuştur. Bu yapı, teknolojiye "serbestlik" felsefesiyle yaklaşan geleneksel ABD Silikon Vadisi modelinden radikal bir kopuşu ve dijital alanda hesap verebilir bir hukuk düzenine geçişi temsil etmektedir. AB'nin bu dört temel yasası, sadece Avrupa pazarını değil, küresel dijital yönetişim standartlarını da derinden etkileme potansiyeli taşımaktadır: Bu kapsamlı çerçevenin temelinde, mahremiyeti temel bir insan hakkı olarak kodlayan Genel Veri Koruma Tüzüğü (GDPR) yer alırken; Dijital Hizmetler Yasası (DSA)[96] çevrimiçi içerik yönetimini ve algoritmik hesap verebilirliği sağlayarak platformların sorumluluklarını artırmaktadır. Piyasa dengelerini gözetmek adına Dijital Pazarlar Yasası (DMA) yapısal rekabetçiliği yeniden tanımlayarak teknoloji tekellerini hedeflerken, Yapay Zekâ

[95] Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

[96] European Commission. (2022). *The Digital Services Act: Ensuring a safe and accountable online environment*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

Yasası (*AI Act)* ise yapay zekâ sistemlerini risk temelli bir ürün güvenliği mantığıyla düzenlemektedir.

AB'nin kendi iç pazarı, 450 milyondan fazla tüketiciyi temsil eden büyüklüğü nedeniyle, küresel şirketlerin görmezden gelemeyeceği bir güce sahiptir. Bu pazar gücünü düzenleyici standartlara dönüştürme yeteneği, sosyolog Anu Bradford'un kavramsallaştırdığı "Brüksel etkisi" olarak adlandırılır. Bu etki, AB standartlarının fiilen küresel norm haline gelmesi sürecini açıklar.

2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğü GDPR, bireyin verileri üzerindeki kontrolünü temel bir insan hakkı statüsüne yükselterek dijital çağın ilk büyük düzenleyici "tsunamisini" tetiklemiştir. ABD'deki Google, Facebook gibi büyük teknoloji şirketleri, AB pazarına erişim için GDPR'ın zorunlu kıldığı yüksek veri koruma standartlarına uymak zorunda kalmıştır. AB uyum maliyetlerinden kaçınmak için, çoğu zaman bu standartları küresel operasyonlarının tamamına yaymayı tercih etmişlerdir. Bu durum, fiilen küresel "de facto" (fiili) standartlar yaratmıştır. GDPR, Brezilya (LGPD), Güney Kore, Japonya, Şili ve hatta birçok ABD eyaleti (örneğin Kaliforniya CCPA) için ulusal veri koruma yasalarının çıkarılmasında model olmuştur. Bu, AB modelinin doğrudan benimsenmesi anlamına gelen "De Jure Brüksel etkisi"nin somut bir göstergesidir. Temelde "veri" odaklı olan GDPR, algoritmaların işleyişini, sistematik riskleri ve platformların toplumsal etkilerini kontrol etme konusunda yetersiz kalmıştır. Bu eksiklik, ikinci ve daha iddialı düzenleyici dalgayı (*DSA, DMA, AI Act*) zorunlu kılmıştır.

2023-2024'te tam yürürlüğe giren Dijital Hizmetler Yasası DSA, internet platformlarının temel sorumluluklarını yeniden tanımlamıştır. Bu yasa, platformların yasadışı içeriği *reaktif* olarak, bildirim üzerine kaldırması gereken geleneksel "bildir ve kaldır" yaklaşımından, platformun kendi sistematiğini sorgulayan *proaktif* "risk değerlendirmesi ve azaltımı" yaklaşımına geçişi simgeler. DSA, platformların içerik yayılımına neden olan algoritmik

sistemlerine odaklanır. Platformlar artık, "sadece aracı" oldukları savunmasının arkasına saklanamaz; algoritmalarının nasıl çalıştığını, neden belirli içerikleri öne çıkardığını ve riskleri nasıl yönettiklerini açıklamak zorundadırlar. Aylık 45 milyondan fazla AB kullanıcısına sahip olan platformlar (Meta, Google, Amazon vb.), en yüksek yükümlülüklere tabidir. Bu yükümlülükler, bağımsız denetimler, araştırmacılara veri erişimi sağlama ve sistemik risk yönetimi planları sunmayı içerir. VLOP/VLOSE'ler[97], platformlarının temel haklara, demokratik süreçlere, halk sağlığına ve ruh sağlığına yönelik potansiyel sistematik riskleri düzenli olarak belirleme, analiz etme ve bu riskleri azaltacak önlemleri uygulama zorunluluğu altındadır. DSA kurallarına uymayan platformlara, küresel yıllık cirolarının %6'sına varan oranlarda caydırıcı astronomik cezalar kesilebilme yetkisi getirilmiştir.

Dijital Pazarlar Yasası DMA, geleneksel tekel karşıtı yasaların yavaş ve reaktif doğasına karşı bir önlem olarak tasarlanmıştır. Yasa, Google, Apple, Meta ve Amazon gibi temel platform hizmetlerini kontrol eden ve pazara girişi kısıtlayabilen "eşik bekçilerini" (*gatekeeper*) hedef alır. Geleneksel rekabet hukukunun aksine, DMA rekabete aykırı davranış *öncesinde* (*ex-ante*) net, bağlayıcı yapılması ve yapılmaması gerekenleri listeler. Amaç, pazardaki rekabetçi yapıyı bozmadan önce müdahale ederek, küçük oyuncuların büyümesini sağlamak ve tüketici tercihlerini artırmaktır.

Temel Kısıtlamalar vardır. Bunlardan ilki eşik bekçileri, kendi ürün ve hizmetlerini, rakiplerinin ürünlerinden sistematik olarak daha üstün bir konuma (arama sonuçları, uygulama mağazaları) yerleştiremez. İşletme kullanıcılarının platformda ürettikleri verilere erişimi ve taşınabilirliği engellenemez. Özellikle mesajlaşma servisleri için birlikte çalışabilirlik zorunluluğu getirilmiştir. Ayrıca, üçüncü taraf uygulama mağazalarına ve ödeme

[97] European Commission. (t.y.). *DSA: Very large online platforms and search engines*. European Commission-Digital Strategy. https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

sistemlerine izin verilmesi gerekmektedir. AB'nin "Brüksel etkisi"nin en yeni ve belki de en iddialı örneği olan Yapay Zekâ Yasası AI Act, yapay zekayı geleneksel bir "ürün güvenliği" mantığıyla ele alır. Risk tabanlı bir yaklaşım benimseyerek, YZ sistemlerini potansiyel zararlarına göre sınıflandırır ve uyumluluk yükümlülüklerini bu riske göre belirler. Yasa, özellikle insan davranışını manipüle etmek için "subliminal teknikler" kullanan YZ uygulamalarını ve belirli dar istisnalar hariç kamuya açık alanlarda gerçek zamanlı biyometrik-yüz tanımlamayı açıkça yasaklayarak etik ve hukuki sınırları çizmiştir.

Avrupa Birliği'nin Yapay Zekâ Yasası (*AI Act*), yapay zekâ sistemlerini potansiyel risk seviyelerine göre dört temel kategoride sınıflandırarak düzenlemektedir. En üstte, devlet tarafından sosyal puanlama yapılması veya insan davranışını manipüle eden subliminal tekniklerin kullanılması gibi temel haklarla çelişen uygulamaları içeren "kabul edilemez risk" kategorisi yer alır ve bu sistemler kesinlikle yasaklanmıştır. İkinci basamakta, tıbbi teşhis, işe alım süreçleri veya kredi notlandırma gibi insanların yaşamını ve güvenliğini doğrudan etkileyen "yüksek risk" grubundaki sistemler bulunur; bu uygulamalar piyasaya sürülmeden önce kapsamlı risk değerlendirmesi, yüksek veri kalitesi ve insan denetimi gibi sıkı uyumluluk kurallarına tabi tutulur. Üçüncü olarak, deepfake videolar veya chatbotlar gibi "sınırlı risk" taşıyan sistemler için temel şart şeffaflıktır; kullanıcıların bir yapay zekâ ile etkileşimde olduklarını bilmeleri ve içeriğin yapay zekâ tarafından üretildiğine dair açıkça uyarılmaları zorunludur. Son olarak, bu kategorilerin dışındaki video oyunları veya spam filtreleri gibi uygulamalar "minimal risk" sınıfına girer ve pazar serbestisini korumak adına herhangi bir özel düzenlemeye tabi tutulmadan serbest bırakılır.

GDPR'dan AI Act'e uzanan bu düzenleyici yolculukla AB, sadece kendi vatandaşlarının haklarını koruyan bir pazar olmaktan çıkıp, teknoloji yönetişiminin, hukukun ve etiğin küresel norm koyucu merkezine dönüşmüştür.

"Brüksel etkisi," dijital dünyanın geleceğinin sadece Silikon Vadisi'nin inovasyon hızıyla değil, Avrupa'nın dikkatli, insan merkezli düzenleyici koridorlarında belirlenen hesap verebilirlik, şeffaflık ve etik standartlarla da şekillendiğini tartışmasız bir biçimde göstermektedir. Bu dört direk, teknoloji şirketlerini sadece teknik olarak değil, etik ve hukuki olarak da yeni bir düzene uyum sağlamaya zorlamaktadır.

Sansür, Güvenlik ve Algoritmik Köpürtme

Dijital çağda, devletlerin ve devasa çevrimiçi platformların (*big tech*) bilgi akışını yönetme çabaları, demokrasinin temel direklerinden ikisi olan ifade özgürlüğü ile kamu düzenini ve bireyleri koruma amacı taşıyan bilgi güvenliği/bütünlüğü arasında karmaşık ve tehlikeli bir çatışma alanını ortaya çıkarır. Bu denge, modern düzenlemelerin ve etik tartışmaların merkezindedir.

Tarihsel distopyalar, özellikle George Orwell'in *1984* romanındaki kurgusal "hakikat bakanlığı" modeli, devletin mutlak hakem olarak neyin "doğru" neyin "yanlış" olduğuna karar verdiği bir sistemi simgeler. Açık ve demokratik toplumlar için, devletin içerik üzerinde doğrudan ideolojik veya politik denetim kurması kesinlikle kabul edilemez bir risktir. Bu riski bertaraf etmek amacıyla müdahale mekanizmalarını sansür algısı yaratan "içerik tabanlı" yaklaşımdan uzaklaştırıp, AB'nin Dijital Hizmetler Yasası (DSA) örneğinde olduğu gibi "prosedür ve davranış tabanlı" bir zemine oturtmak zorundadır. Bu çerçevede devletin, belirli bir siyasi partiye yönelik iddiaların silinmesini talep etmesi doğrudan politik sansür sayılarak kabul edilemezken; yapay zekâ güdümlü bot ağlarının yarattığı "koordineli sahte davranış"ın (CIB) engellenmesini istemesi, kamusal tartışmayı boğan manipülatif taktikleri hedef aldığı için demokratik ve gerekli bir müdahale olarak görülür. Dolayısıyla demokratik denetim, içeriğin taşıdığı fikre veya mesaja değil, onun yayılma biçimine ve arkasındaki kötü niyetli davranışa odaklanmalıdır. Dijital

çağ etiğinin temelini oluşturan bu yaklaşım, araştırmacı Renée DiResta'nın "İfade özgürlüğü, erişim özgürlüğü değildir" ilkesiyle özetlenir; buna göre bir kişinin konuşma hakkı saklı olsa da platformların bu konuşmayı algoritmalarla milyonlara yapay olarak ulaştırma zorunluluğu yoktur.[98]

İfade özgürlüğü geleneksel anlamda, yasal sınırlar (hakaret, tehdit, şiddete teşvik vb.) içinde kalmak kaydıyla, bireylerin saçmalama, yanlış bilgi paylaşma veya eleştiride bulunma hakkı anayasal bir güvence altındadır. Bu, bireyin *konuşma* hakkıdır. Erişim özgürlüğüyse kimsenin, bir platformun güçlü algoritmaları tarafından milyonlarca kullanıcının ana akışına, trendlerine veya bildirimlerine zorla çıkarılma hakkı olmaması anlamına gelir. Bu, *konuşmanın milyonlara ulaşma garantisi* hakkı değildir. Bir bilginin algoritmik olarak köpürtülmesi bir hak değil, platformun tasarım tercihinin ve iş modelinin bir sonucudur. Algoritmalar, etkileşim maksimizasyonunu hedeflediği için, çoğu zaman kutuplaştırıcı, şok edici ve yanlış içerikleri hızla ön plana çıkarır.

Modern düzenlemeler bu ayrımı temel alır. Amaç, bireyin yasal konuşmasını susturmak değil, konuşmaya yapay olarak eklenmiş olan ve kamusal alanı bozmayı hedefleyen yapay megafonu elden almaktır. Konuşmayı tamamen kaldırmak yerine, onun yapay ve manipülatif yayılımını kısıtlamayı hedefler. Bu, platformun kendi kurallarını (örneğin, CIB yasağı) daha etkin uygulamaya zorlanması anlamına gelir. Bu yaklaşım, sansür suçlamasıyla bilgi güvenliği ihtiyacını dengeleme arayışının güncel ve en önemli çözüm önerisidir.

[98] DiResta, R. (2018). Free speech is not the same as free reach. *Wired*.

Sonuç: Bilgi Düzensizlikleriyle Mücadelede Çok Paydaşlı Yönetişim

İnfodemi krizi, modern toplumların karşı karşıya olduğu en karmaşık ve çok boyutlu zorluklardan biridir. Bu sorun, ne sadece otoriter bir devletin sansür mekanizmalarıyla ne de tek başına teknoloji devlerinin algoritmik güncellemeleriyle çözülebilecek basit bir teknik arıza veya geçici bir aksaklıktır. Dezenformasyon, derin köklerini sosyal psikolojiye, kâra dayalı ekonomik teşviklere ve hızla artan siyasi kutuplaşmaya dayandıran, bu nedenle de topyekûn bir toplumsal yanıtı, tüm aktörlerin uyum içinde çalışmasını gerektiren sistemik bir tehdittir. Bu bağlamda, uluslararası politika çevrelerinde ve akademik çalışmalarda kabul görmeye başlayan "çok paydaşlı yönetişim" modeli, bu karmaşık zorluğun üstesinden gelmek için geleceğin çözüm haritasını sunmaktadır. Bu model, sadece hükümetler veya sadece sosyal medya şirketleri gibi sorumluluğun tek bir merkeze yüklenmesi yerine, krizin farklı veçhelerine müdahale edebilecek kilit aktörler arasında dengeli, şeffaf ve koordineli bir iş birliğini öngörür. Modelin temel direkleri ve her bir paydaşın kritik görevleri aşağıda detaylandırılmıştır:

Devletlerin dezenformasyonla mücadeledeki rolü, içeriği denetleyen veya sansürcü bir aktör olmaktan kesinlikle uzak durarak, dijital alan için adil, hukuka uygun ve şeffaf oyun kurallarını belirleyen düzenleyici çerçeveyi sağlamaktır. Bu çerçeve, ifade özgürlüğünün temel insan hakkı olarak korunmasını garanti altına alırken, aynı zamanda demokratik sürece, kamu sağlığına ve ulusal güvenliğe yönelik sistemik riskleri yönetmeyi amaçlar.

Devletler, Avrupa Birliği'nin çığır açan Dijital Hizmetler Yasası (DSA) gibi kapsamlı mevzuatlarla somutlaşan düzenlemeler oluşturmalıdır. Bu düzenlemeler dijital platformların şeffaflık yükümlülüklerini (özellikle algoritmalarının işleyişine dair), yasa dışı içeriğin (örneğin terör propagandası,

çocuk istismarı) kaldırılmasına yönelik hızlı ve adil prosedürleri, kullanıcıların içerik kaldırma kararlarına itiraz etme ve haklarını arama mekanizmalarını tanımlamalıdır.

Düzenlemeler, nefret söylemi, terör propagandası ve seçim manipülasyonu gibi demokratik düzeni tehdit eden unsurlara karşı net ve hukuki "kırmızı çizgiler" çekmek zorundadır. Ancak bu yapılırken, eleştirel siyasi söylem veya tartışmalı fikirlerin ifade özgürlüğü kapsamında kalmasına özen gösterilmelidir.

En önemli nokta, düzenlemelerin içerik denetimini tamamen platformların inisiyatifine bırakmak yerine, onların sistemik riskleri (örneğin algoritmaların kutuplaşmayı, dezenformasyonu veya çocuklara yönelik riskleri artırması) proaktif olarak analiz etme, azaltma ve yönetme yükümlülüğünü hukuki olarak tesis etmesidir.

İnternet ekosisteminin en güçlü aktörleri olan teknoloji platformları, dezenformasyonun yayılma hızını ve ölçeğini belirleyen algoritmik ve teknik altyapıya sahiptir. Bu nedenle, sorumlulukları sadece yasalara uymaktan öte, sistemlerini kâr maksimizasyonundan ziyade etik ilkelere ve kamusal yarara göre yeniden tasarlamayı kapsar.

Platformlar, dezenformasyonun ve yasalara aykırı içeriğin kendi platformlarında nasıl yayıldığını, hangi algoritmik seçimlerin (öneri sistemleri, sıralama mekanizmaları) bu yayılmayı hızlandırdığını şeffaf bir şekilde açıklamakla yükümlüdür. "Veriyi açma" prensibi uyarınca, güvenilir, bağımsız araştırmacıların ve denetleyici otoritelerin bu sistemleri incelemesine ve denetlemesine olanak tanıyan erişim mekanizmaları kurulmalıdır.

Platformlar, kullanıcıların etkileşimini (tıklama, paylaşma, yorum yapma) maksimize etmeyi hedefleyen, dolayısıyla çoğu zaman kışkırtıcı ve yanlış bilginin yayılmasına yol açan iş modellerinden acilen uzaklaşmalıdır. Güvenilir ve kaliteli içeriği ödüllendiren, manipülasyonu zorlaştıran,

yavaşlamayı ve eleştirel düşünmeyi teşvik eden arayüzler ve etkileşim mekanizmaları (örneğin, okumadan paylaşmaya kısıtlama) geliştirmelidir.

İçerik denetimi (moderasyon) için yeterli, dil ve kültüre duyarlı (Türkçe, Arapça, Urduca vb. dillerde yeterli personel) kaynakları tahsis etmek zorunludur. Özellikle seçim dönemlerinde, çatışma veya kriz anlarında proaktif tedbirler almak ve anlık durum odaları kurarak koordinasyonu sağlamak gereklidir.

Bu paydaş grubu, yönetişim modelinin en kritik unsuru olan "denge ve denetleme" mekanizmasını oluşturur. Hükümetlerin ve platformların eylemlerini bağımsız ve eleştirel bir mercekle izleyerek hesap verebilirliği sağlar, bilgi boşluğunu doldurur.

Sivil toplum kuruluşları (STK'lar) ve akademik kurumlar, platformların gönüllü taahhütlerini veya yasal zorunluluklarını (örneğin DSA'ya uyum, şeffaflık raporları) gerçekten yerine getirip getirmediğini sistematik olarak denetlemelidir. Platformlar tarafından açılan verileri analiz ederek, dezenformasyon kampanyalarının kökenlerini, yayılma dinamiklerini ve platformların müdahalelerinin etkinliğini değerlendiren bağımsız raporlar yayımlanmalıdır.

Akademi, dezenformasyonun toplumsal, psikolojik ve siyasi etkileri üzerine derinlemesine araştırmalar yaparak, etki odaklı çözümler ve sağlam politika önerileri sunmalıdır. Aynı zamanda, bağımsız doğruluk kontrolü (*fact-checking*) ağları kurarak yanlış bilginin yayılımını anlık olarak kesmeli ve medya okuryazarlığı programlarını yaygınlaştırmalıdır.

Sivil toplum, devletler ve platformlar arasındaki düzenleyici diyaloglarda ve politika geliştirme süreçlerinde, kamusal çıkarı, insan haklarını ve ifade özgürlüğünü temsil eden eleştirel bir ses olmalıdır.

Dezenformasyonun çözümünde genellikle sadece bir "hedef" olarak görülen, ancak kritik öneme sahip olan aktör, bilgi tüketicisinin kendisidir. Toplumsal dayanıklılık, her bir bireyin eleştirel düşünme, bilgiyi seçme ve

sorumlu hareket etme becerisine bağlıdır.

Eğitimin her seviyesine entegre edilecek programlarla, bireylerin sadece teknik cihaz kullanma becerilerini değil, aynı zamanda bilgiyi kaynak, güvenilirlik, önyargı ve manipülasyon teknikleri açısından sorgulama yeteneklerini güçlendirmek esastır. Bu, sadece bir ders değil, eleştirel düşünce kültürünün yerleştirilmesi demektir.

Bireylerin kaliteli, güvenilir ve doğrulanmış bilgiye yönelik taleplerini artırmaları, manipülatif, kışkırtıcı ve duygusal tepkilere dayanan içeriği reddetmeleri gerekir. Bu bilinçli talep, uzun vadede platformların algoritmalarını olumlu yönde etkileyecek ve kaliteli içeriği öne çıkarmaya zorlayacak güçlü bir pazar ve baskı unsuru yaratır. Bireylerin şüpheli veya duygusal olarak kışkırtıcı içeriği hemen paylaşmak yerine, doğruluğunu kontrol etme ve güvenilir kaynaklardan teyit etme alışkanlığını geliştirmesi zorunludur. Her birey, dezenformasyonun son halkası olmaktan kaçınarak, yayılım zincirini kırma sorumluluğunu taşır.

Bu çok paydaşlı ekosistem, sivil toplum ve akademinin bağımsız denetimi ve analiz yeteneği ile bireylerin bilinçli tüketimi bir araya gelmedikçe, hiçbir yasa, hiçbir algoritmik güncelleme ve hiçbir doğruluk kontrolü tek başına "hakikat sonrası" çağın getirdiği zorlukları aşamaz. Kalıcı çözüm, dijital ekosistemin salt ekonomik kâr maksimizasyonu yerine, demokratik ilkelere, insan haklarına ve kamusal güvenliğe göre yeniden inşa edilmesine yönelik ortak ve sürekli bir sorumlulukta yatmaktadır. Dezenformasyonla mücadele, bir "teknik düzeltme" değil, bir "toplumsal sözleşme" meselesidir.

TEMEL ÇIKARIMLAR

Dezenformasyonla mücadele, artık sadece bireylerin "doğruyu yanlıştan ayırma" becerisine (medya okuryazarlığına) indirgenemeyecek kadar karmaşık, sistematik bir yönetişim sorunudur.

Temel Kavramlar ve Mekanizmalar

Brüksel Etkisi: Avrupa Birliği'nin (AB) teknolojik üretimde lider olmasa bile, devasa pazar gücünü kullanarak dijital dünyanın kurallarını tek taraflı belirleme gücüdür.

İfade Özgürlüğü Erişim Özgürlüğü Değildir: Renée DiResta tarafından formüle edilen bu ayrım, dijital etiğin temelidir. Bir kişinin yalan söyleme veya saçmalama hakkı (ifade özgürlüğü) olabilir; ancak platformların bu yalanı algoritmalarla milyonlarca kişinin önüne zorla çıkarması, köpürtmesi ile benzer bir durum değildir. Müdahale, kişinin sesini kısmaya değil, ona verilen "yapay megafonu" elinden almaya odaklanmalıdır.

Sistematik Risk Yönetimi: AB Dijital Hizmetler Yasası (DSA) ile gelen bu kavram, platformların tek tek içerik silmek yerine, algoritmalarının toplum üzerinde yarattığı büyük riskleri (ruh sağlığı, seçim manipülasyonu vb.) proaktif olarak analiz etmesini ve azaltmasını zorunlu kılar.

Koordineli Sahte Davranış: Demokratik devletlerin sansürcü "Doğruluk Bakanlığı" konumuna düşmemesi için geliştirilen denetim mekanizmasıdır. Müdahale, içeriğin "ne dediğine" (bu fikir yanlıştır demeye) değil; içeriğin "nasıl yayıldığına" odaklanır. Eğer içerik, bot ağları ve sahte hesaplar üzerinden yapay bir şekilde yayılıyorsa, platform bu davranışı engeller.

7.1. KENDİNİZİ TEST EDİN

Soru 1: "Brüksel etkisi" kavramı, dijital yönetişim bağlamında neyi ifade eder?

A) Brüksel'in internet altyapısının zayıf olmasını

B) AB'nin çıkardığı dijital yasaların teknoloji şirketlerini küresel ölçekte standartlarını yükseltmeye zorlamasını

C) Avrupa'nın Avrupa Birliği ülkeleri için kendi sosyal medya platformunu kurmasını ve denetlemesi

D) AB'nin interneti sansürlemesini

Soru 2: Dijital Hizmetler Yasası (DSA) gibi modern düzenlemelerin, "sansür" suçlamasından kaçınmak için benimsediği temel yaklaşım nedir?

A) Devletin tüm içerikleri tek tek kontrol etmesi, ayrı ayrı sorunlu kısımları ilgili platformlarla görüşmesi

B) Anonim hesapları yasaklamak

C) İnterneti yavaşlatarak, denetlemeyi sağlayarak yayılımı sağlamak

D) İçeriğin kendisine değil; algoritmaların şeffaflığına, risk analizine ve platformların süreçlerine odaklanmak

Soru 3: "İfade özgürlüğü, erişim özgürlüğü değildir" ilkesi neyi savunur?

A) İnsanların fikirlerini söylemesinin yasaklanması gerektiğini

B) Her fikrin algoritma tarafından herkese ulaştırılması gerektiği, bu nedenle algoritmaların tüm üyelerine birden fazla iletmesi gerektiğini vurgulaması

C) Bir şeyi söyleme hakkınızın olması, platformun bunu milyonlarca kişiye yapay olarak ulaştırmak zorunda olduğu anlamına gelmediğini

D) Sadece paralı üyelerin konuşabileceğini

7.1. MERAKLISINA EK KAYNAKLAR

Balkan, E. ve Ünver, A. (2023). *Dezenformasyonla mücadele: Politika çerçevesi* (Siber Politikalar ve Dijital Demokrasi Programı). Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM). https://edam.org.tr/Uploads/Yukleme_Resim/pdf-27-09-2023-00-42-46.pdf

Balkan, E. ve Ülgen, S. (2023). *Dezenformasyonla mücadelede özdenetim ve düzenlemenin rolü* (Siber Politikalar ve Dijital Demokrasi Programı). Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM). https://edam.org.tr/Uploads/Yukleme_Resim/pdf-11-09-2023-23-57-27.pdf

EU DisinfoLab. (2025, 18 Aralık). *The disinformation landscape across Europe*. https://www.disinfo.eu/publications/disinformation-landscapes-in-european-countries/

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. https://doi.org/10.12987/9780300235029

İldem, T. (2024). *Dezenformasyonla mücadelede toplumsal dirençliliğin güçlendirilmesi: Uluslararası kuruluşların ve özellikle NATO'nun rolü* (Politika Belgesi No. 2). RESAID.

Onuk, E. (2025). Yanlış bilginin sorunsallaştırılması: Küresel politika söylemleri ve yayılım dinamikleri. E. Erdoğan, P. Uyan-Semerci & G. Uysal-Gündoğdu (Der.), *Bilgi düzensizliklerine karşı toplumsal bilişsel dirençlilik* içinde. İstanbul Bilgi Üniversitesi.

Küresel Savunma Ağı ve Kurumsal Roller

Tablo 7.1.1 *Küresel savunma ağı ve küresel roller*

	TEMEL YAKLAŞIM VE ROL	ANA ARAÇLAR VE ÇERÇEVELER
AVRUPA BİRLİĞİ (AB)	**"Düzenleyici Güç & Güvenlik"** FIMI'yi bir güvenlik tehdidi olarak ele alır. Kendi kendini düzenlemeden yasal bağlayıcılığı olan yasalara geçişin öncüsüdür.	**FIMI Toolbox:** Tespit, caydırma ve diplomatik yanıt araçları. **DSA (Dijital Hizmetler Yasası):** Platformlara risk analizi ve şeffaflık zorunluluğu. **AI Act:** Yapay zekâ ve deepfake şeffaflığı. **EDMO & EUvsDisinfo:** Doğrulama ve ifşa mekanizmaları.
NATO	**"Davranışsal Savunma & Hibrit Savaş"** Bilgi manipülasyonunu hibrit savaşın bir parçası sayar. İfade özgürlüğünü korumak için içeriğe değil, davranışa odaklanır.	**ABCDE Çerçevesi:** Aktör, davranış, içerik, derece, etki analizi. **NATO Rapid Response Group:** Tehditleri anlık tespit mekanizması. **Siber Savunma:** Kümülatif siber/bilgi saldırılarının 5. Maddeyi tetikleyebileceği kabulü.
BİRLEŞMİŞ MİLLETLER (BM)	**"Norm Belirleyici & Bilgi Dürüstlüğü"** Küresel normlar ve "bilgi dürüstlüğü" (information integrity) üzerine odaklanır. İnsan hakları temellidir.	**Global Digital Compact:** Üye devletlerin güvenli bilgi ekosistemi taahhüdü. **3R Yaklaşımı:** Araştırma (*research*), risk analizi, yanıt (*response*). **Barış İçin Yeni Gündem:** Siber çatışmaların önlenmesi.
DİĞER AKTÖRLER (G7, OECD, OSCE)	**"Koordinasyon ve Yönetişim"** Demokrasiler arası istihbarat paylaşımı ve şeffaflık standartları.	**G7 RRM:** Hızlı Müdahale Mekanizması (Rapid Response Mechanism). **OECD:** "Facts not fakes" (Yalanlar değil gerçekler) girişimi. **OSCE:** Güven artırıcı önlemler (CBMs).

Uluslararası Stratejiler ve Karşılaştırmalı Yaklaşımlar

Tablo 7.1.2 *Uluslararası stratejiler ve karşılaştırmalı yaklaşımlar*

YAKLAŞIM MODELİ	TEMEL FELSEFE & ARAÇLAR	TEMSİLCİ ÜLKELER & UYGULAMALAR	OLASI RİSKLER
KISITLAYICI-CEZALANDIRICI	**"Güvenlik Tehdidi Olarak Dezenformasyon"** Dezenformasyonu bir suç olarak tanımlar. "Yalan Haber" yasalarıyla hapis ve para cezası öngörür. Devlet, gerçeğin koruyucusu rolündedir.	**Singapur (POFMA):** Bakanlara içeriği sildirme yetkisi. **Türkiye:** "Halkı yanıltıcı bilgiyi yayma" suçu (TCK 217/A). **Macaristan, Polonya:** Olağanüstü hâl yasalarıyla medyayı kontrol etme.	Sansür ve otosansür. "Gerçek" kavramının politize edilmesi. Muhalif seslerin susturulması.
DÜZENLEYİCİ-KURUMSAL	**"Yönetişim Sorunu Olarak Dezenformasyon"** Bireyleri değil, platformları (aracıları) sorumlu tutar. Şeffaflık yasaları ve hesap verebilirlik mekanizmaları kurar.	**Almanya (NetzDG):** Platformlara 24 saatte yasa dışı içeriği silme zorunluluğu. **Fransa (VIGINUM):** Seçim dönemlerinde manipülasyonu izleyen devlet ajansı. **İrlanda:** Teknoloji devlerinin AB merkezleri burada olduğu için sıkı denetim.	Bürokrasinin genişlemesi. Platformların "aşırı silme" (*over-removal)* yapması. Risk söyleminin normalleşmesi.
DİRENÇ-EĞİTİMSEL	**"Toplumsal Bağışıklık" (İskandinav Modeli)** Yasağa değil, vatandaşın bilincine odaklanır. Dezenformasyon bir "eğitim ve halk sağlığı" sorunudur.	**Finlandiya:** Anaokulundan başlayan "çoklu okuryazarlık" müfredatı. **İsveç:** Psikolojik savunma kuruluşları (Yalanı değil, yabancı etkiyi hedefler). **Estonya/Litvanya:** Rusya tehdidine karşı sivil "Elf" orduları ve stratejik iletişim.	Yapısal eşitsizliklerin göz ardı edilmesi. Her sorumluluğun bireye yüklenmesi.
HİBRİT/ÇOK AKTÖRLÜ	**"Ağ Bağlantılı Yönetişim"** Devlet, medya ve sivil toplumun iş birliği.	**Tayvan:** "Mizah ile söylenti savuşturma" (*Humor over rumor).* 60 dakikada yanıt. **İspanya/İtalya:** Ulusal stratejilerde doğrulama platformlarıyla (*fact-checkers*) ortaklık.	STK'ların araçsallaştırılması. Sorumluluğun bulanıklaşması.
DEVLET DESTEKLİ SALDIRI	**"Dezenformasyonun Silahlaştırılması"** Dezenformasyonla savaşıyormuş gibi görünüp, onu bir dış politika aracı olarak kullanmak.	**Rusya:** "Yalan (yangın) hortumu" (*firehose of falsehood*) modeli. Çelişkili ve yoğun propaganda. **Çin:** Bilgi bastırma (*great firewall*) ve pozitif propaganda.	Küresel bilgi ekosisteminin zehirlenmesi. Güven erozyonu.

CEVAP ANAHTARI

Bölüm	Soru 1	Soru 2	Soru 3
1.1.	C	C	B
2.1.	C	B	B
2.2.	B	C	C
2.3.	B	B	D
3.1.	B	B	C
3.2.	A	B	C
3.3.	B	A	C
4.1.	B	B	D
4.2.	B	B	A
4.3.	B	C	B
4.4.	B	B	A
4.5.	A	C	B
5.1.	C	B	B
5.2.	B	C	C
5.3.	B	A	C
5.4.	C	B	B
6.1.	A	B	B
6.2.	B	D	C
6.3.	C	B	C
6.4.	B	A	A
7.1.	B	D	C

Bilgi Düzensizliklerine Karşı Toplumsal Bilişsel Dirençlilik Yaratmak-RESAID çalışmamızın temel bir parçası olan bu kitabı, internet kullanan, sosyal medyada vakit geçiren ve haber okuyan, yaşı veya mesleği ne olursa olsun herkesin kullanımına açık bir kaynak olarak tasarladık. Çünkü biliyoruz ki dijital dünyada doğruyu bulmak, hepimizi çok yakından ilgilendiren ortak bir ihtiyaç. Bu bağlamda içinde olduğumuz dijital dünyada doğru bilgiye erişimi, günümüzde diğer tüm haklarımızın hayata geçebilmesi için temel bir insan hakkı olarak görüyoruz. Dijital dünyadaki bilgi düzensizliklerini yalnızca teknik bir iletişim sorunu değil; doğru bilgiye erişimimizi, özgür irademizi ve demokratik süreçlere katılımımızı doğrudan tehdit eden bir insan hakları meselesi olarak değerlendiriyoruz. Dezenformasyon ve manipülasyon teknikleri, toplumu kutuplaştırarak ortak bir gerçeklik zemini üzerinde buluşmamızı engelliyor. Ancak inanıyoruz ki bu gidişat bireylerden sivil topluma, devletlerden uluslararası kurumlara kadar tüm aktörlerin sorumluluk almasıyla dönüştürülebilir. Bu kitabın kutuplaşmanın yerini dayanışmaya bıraktığı, eleştirel düşüncenin hepimize rehberlik ettiği, daha şeffaf ve güvenli bir bilgi ekosistemi inşa etmeye katkı sunmasını umuyoruz.

Bu kitaba çevrim içi erişmek için karekodu okutabilir veya resaid.bilgi.org.tr adresini ziyaret edebilirsiniz.

Tanıtım nüshasıdır, para ile satılamaz.

Avrupa Birliği tarafından ortak finanse edilmektedir

CREATING SOCIETAL COGNITIVE RESILIENCE AGAINST INFORMATION DISORDERS
resaid
JEAN MONNET CENTRE OF EXCELLENCE

İstanbul Bilgi Üniversitesi