



TÜRKİYE'DE DİJİTAL OKURYAZARLIK: EKONOMİK, GÜVENLİK VE DEZENFORMATİF HUSUSLARA İLİŞKİN PERSPEKTİFLER

Azem Yıldırım
Dijan Balkaroğlu

Araştırmacı
Araştırmacı



Türkiye'de Dijital Okuryazarlık: Ekonomik, Güvenlik ve Dezenformatif Husurlara İlişkin Perspektifler

OCAK // 2023

Azem YILDIRIM

Araştırmacı

Dijan BALKAROĞLU

Araştırmacı



Bu rapor Ekonomi ve Dış Politika Araştırma Araştırmalar Merkezi (EDAM) tarafından TikTok Türkiye için hazırlanmıştır.

YÖNETİCİ ÖZETİ

Dijital okuryazarlık genel olarak okuma, yazma, teknik beceriler ve eleştirel düşünmeyi kullanarak dijital dünyamızda gezinme yeteneği olarak tanımlanır. Başka bir deyişle, bilgiyi bulmak, değerlendirmek ve iletmek için teknolojiyi kullanmakla ilgilidir. Bu tanım doğrultusunda rapor, dijital okuryazarlık sorununun merkezinde yer alan dijital ekonomiye katılma becerisi, çevrimiçi gizlilik ve dijital ve sosyal medya dezenformasyonuna ilişkin durum gibi alanlara ışık tutmaktadır.

DİJİTAL EKONOMİ

Dijital ekonomi, dijitalleştirilmiş bilginin ana üretim faktörü olarak kullanıldığı ekonomik faaliyetlerin toplamı olarak tanımlanabilir. Değerlendirmesini bağlantı (ve iletişim), cihazlar (ve nesnelerin

interneti), kurumsal bilişim, eğlence ve ödemeler olmak üzere beş kriter üzerinden yapan Financial Times Omdia Dijital EkonomilerEndeksi'ne göre Türkiye genel sıralamada yirminci sırada yer alırken, kredi kartı işlem hacminde yedinci, aylık aktif Facebook kullanıcısı sayısında sekizinci ve YouTube kullanıcısı sayısında on birinci sırada yer almaktadır. Aynı şekilde, dijital ekonominin artan hacmi, insanların giderek daha fazla çevrimiçi işlem yapması nedeniyle dijital okuryazarlıkta da bir artışa işaret etmektedir. Ancak gelişmiş ülkelerle aradaki farklar devam etmektedir. Bu farklar sadece finansal ve altyapısal kapasite farklılıkları ile değil, aynı zamanda dijital hizmetlerin kullanımı ile güçlü bir korelasyon gösteren eğitim seviyesi ile de açıklanabilir. İngev ve Oxford Üniversitesi tarafından hazırlanan Türkiye'de Dijital Vatandaşlık raporuna göre, üniversite ve üzeri mezunları %72'si e-ticaret kullandığını belirtirken, bu oran lise, ortaokul ve ilkokul mezunları için sırasıyla %52, %33 ve %23'e düşmektedir.

Türkiye'nin dijital hizmetlerin benimsenmesi açısından özellikle başarılı olduğu bir alan da dijital kamu hizmetleridir. Örneğin, 2021 yılında Türk vatandaşlarının %68,7'si e-devlet platformunu kullanmıştır. Buna göre, 2022 BM E-Devlet Araştırması, Türkiye'yi "çok yüksek düzeyde beşeri sermaye gelişimi ve orta ila çok yüksek düzeyde altyapı gelişiminden yararlanarak" çevrimiçi hizmetler endeksinin çok yüksek segmentinde yer alan on iki üst-orta gelirli ülkeden biri olarak tanımlamaktadır.

Politika Önerileri

Dijital okuryazarlık, önümüzdeki dönemde milyonlarca ailenin refahı ile derinden bağlantılı olacaktır. Rapor, bir önceki önerimiz doğrultusunda, Türkiye'deki işgücünün giderek artan bir bölümünün daha yüksek eğitim seviyelerine ihtiyaç duyacağını göstermektedir. İhtiyaç duyulan beceriler arasında daha yüksek bilişsel, sosyal ve teknolojik beceriler yer almaktadır. Teknolojik becerilere olan talebin %63 oranında artacağı tahmin edilmektedir. Eleştirel düşünme gibi daha yüksek bilişsel beceriler ve temel dijital becerileri içeren teknolojik beceriler dijital okuryazarlıkla bağlantılıdır. Hem hükümetin milli eğitim yoluyla hem de işverenlerin yeniden beceri kazandırma programları yoluyla işgücünün bu geçişe hazır olmasını sağlaması zorunludur. OECD, dijital alanlarda mesleki eğitimin ve yetişkin öğreniminin güçlendirilmesinin, üretken sektörün teknolojik değişim potansiyelinden daha iyi yararlanmasına yardımcı olacağını önermektedir. Daha temel bir çözüm ise dijital çözümlerin eğitimin tüm alanlarına entegre edilmesidir. Daha önce de belirttiği gibi, dijital okuryazarlık eleştirel düşünme, okuma ve yazma gibi teknik olmayan becerileri de içermektedir. Bu becerileri öğretmek için dijital yöntemleri kullanan öğretim yöntemleri, tıpkı geleneksel okuryazarlık öğretiminin bir noktadan sonra harfler ve hecelerden metinleri anlama ve kompozisyon yazmaya doğru ilerlemesi gibi öğrencilerin dijital okuryazarlığını artıracaktır. Bu sadece milli eğitimle de sınırlı kalmamalıdır. İş dünyası veya diğer ekonomik faaliyetlerle ilgili her türlü eğitimde, öğretilen materyallerin dijital uygulamaları dikkate alınmalıdır.

ÇEVİRİMİÇİ GÜVENLİK

Eleştirel düşünme ve dijital sistemlerin nasıl çalıştığına dair temel bilgiler gibi dijital okuryazarlık unsurları siber güvenlikle bağlantılıdır. Bazı bağlantılar otomatik olarak bir şeyler indirdiği için her bağlantıya tıklamamak gerektiğini ya da sadece rakamlardan oluşan şifrelerin kırılmasının daha kolay olduğunu bilmek, temel dijital bilginin güvenliği nasıl artırabileceğine dair birkaç örnektir. Ayrıca, daha geniş anlamda eleştirel düşünme, hangi bağlantının şüpheli olduğunu veya iletişim kurulan kişinin dolandırıcı olup olmadığını değerlendirmeye yardımcı olabilir. Çocukların dijital okuryazarlık ve güvenlik becerilerini inceleyen bir LSE çalışması, örneğin güvenlik becerileri ile eleştirel okuryazarlık becerilerinin pozitif yönde ilişkili olduğunu ve potansiyel olarak birbirlerini güçlendirdiğini ortaya koymuştur. Çevrimiçi güvenlik uygulamalarının iyileştirilmesinin önündeki en önemli engellerden biri sosyo-ekonomik eşitsizliklerdir. Dijital beceriler kullanımla birlikte gelişse de sosyo-ekonomik durum, yaş ve cinsiyet gibi eşitsizlikler bu becerilerin gelişimini etkilemeye devam etmektedir. Gaziantep ve Kilis'teki lise öğrencileri üzerinde yapılan bir araştırma, erkek öğrencilerin dijital güvenlik farkındalığı açısından kız öğrencilerden önemli ölçüde daha yüksek puan aldığını ortaya koymuştur.



Politika Önerileri

İlk olarak, dijital güvenlik bilincinin ve bu konudaki temel becerilerin ikinci doğa haline geldiği bir dijital güvenlik kültürüne ihtiyaç vardır. Bu da tüm paydaşların, yani hükümet, kamu ve özel kuruluşlar ve genel olarak dijital vatandaşların eş zamanlı olarak harekete geçmesiyle sağlanabilir. Kamu ve sivil toplum kanalları aracılığıyla kamuoyu farkındalığı kampanyalarının uygulanması ve sosyal medya sağlayıcıları tarafından platform tarafından başlatılan hatırlatmalarla tamamlanması, güvenlik önlemlerinin alınmaması durumunda ortaya çıkabilecek zararların kullanıcılara anlatılmasına yardımcı olabilir.

İkinci olarak, dijital okuryazarlıktaki eşitsizlik, sosyo-ekonomik statü ve cinsiyet gibi diğer eşitsizliklerle ilişkilidir. Ağ altyapısının eşitsiz dağılımının bir rolü olabilir, ancak yine de daha düşük dijital okuryazarlık seviyeleri dezavantajlı grupları dijital güvenlik tehditlerine karşı daha savunmasız hale getirerek tüm dijital ekosistemi daha yüksek düzeyde kırılganlığa maruz bırakmaktadır. Bu nedenle eşitsizlik uçurumlarını kapatmak üzere tasarlanmış kamu programları dijital okuryazarlıktaki eksikliklerin giderilmesinde etkili olacaktır.

Aynı şekilde, toplumsal cinsiyet eşitsizliğinin dijital dünyada da şekillendiğinin altı çizilmelidir. Kadınların ve kız çocuklarının dijitali benimsemesi ile erkeklerin ve erkek çocuklarının benimsemesi arasında önemli bir fark vardır. Ancak, bu farklılıkların altında yatan nedenleri ortaya koyan veriler, özellikle genç nesiller arasında henüz çok yeni olduğundan, mevcut araştırmalar kapsamlı politika önerileri sunmaya elverişli değildir. Farklı sosyoekonomik ve coğrafi geçmişlerden gelen kadınlar arasında daha önce bahsedilen faktörlerin katkı düzeylerini belirlemek için kapsamlı veriye dayalı araştırmalar şiddetle tavsiye edilmektedir, böylece gerekli politikalar özel bir şekilde uygulanabilecektir.

DEZENFORMASYONLA MÜCADELE

Yanlış bilginin yayılma yolları çeşitlidir ve her biriyle mücadele etmek farklı teknikler ve müdahaleler gerektirmektedir. Dahası, teknoloji ve toplum daha da geliştikçe yeni kanallar ortaya çıkmaktadır. Dezenformasyon sayısız kişisel veya başka saiklerle yayılsa da, sosyo-politik boyutu hem demokrasi hem de sosyal uyum için önemli bir tehdit oluşturmaktadır. Hükümetlerin ve uluslararası kuruluşların bu olguyla mücadeleye özellikle ilgi duymalarının nedeni de budur. Türkiye bu eğilimin bir istisnası olmamıştır. Türkiye'de "Dezenformasyon Yasası" olarak da bilinen 7428 sayılı Torba Yasa 18 Ekim 2022 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Sosyal medya platformları, mesajlaşma uygulamaları gibi üst düzey platformlar ve çevrimiçi gazetelere yönelik ek düzenleme ve gerekliliklere ek olarak, yasanın tartışmalı bir yönü de dezenformasyonu suç haline getirme şeklindedir. Yasaya göre, dört temel kriterin aynı anda yerine getirilmesi halinde "yanıltıcı bilgi yaymak" suç haline gelmektedir: Kamu düzenini ve genel sağlığı bozacak şekilde endişe, korku veya panik yaratmak amacıyla ülkenin iç ve dış güvenliğine ilişkin yanlış bilgileri alenen yaymak.

Yasa şu ana kadar ifade özgürlüğü ve özel hayatın gizliliğini ciddi şekilde kısıtladığı gerekçesiyle eleştirilmiştir. İnsan Hakları İzleme Örgütü, Venedik Sözleşmesi ve Article 19 gibi örgüt ve organlar, devletin gerçeği ve niyeti belirleme sorumluluğunu üstlendiği ve belirsiz kriterlere dayanarak davranışı suç haline getirdiği gözlemine dayanan endişelerini dile getirmektedir.

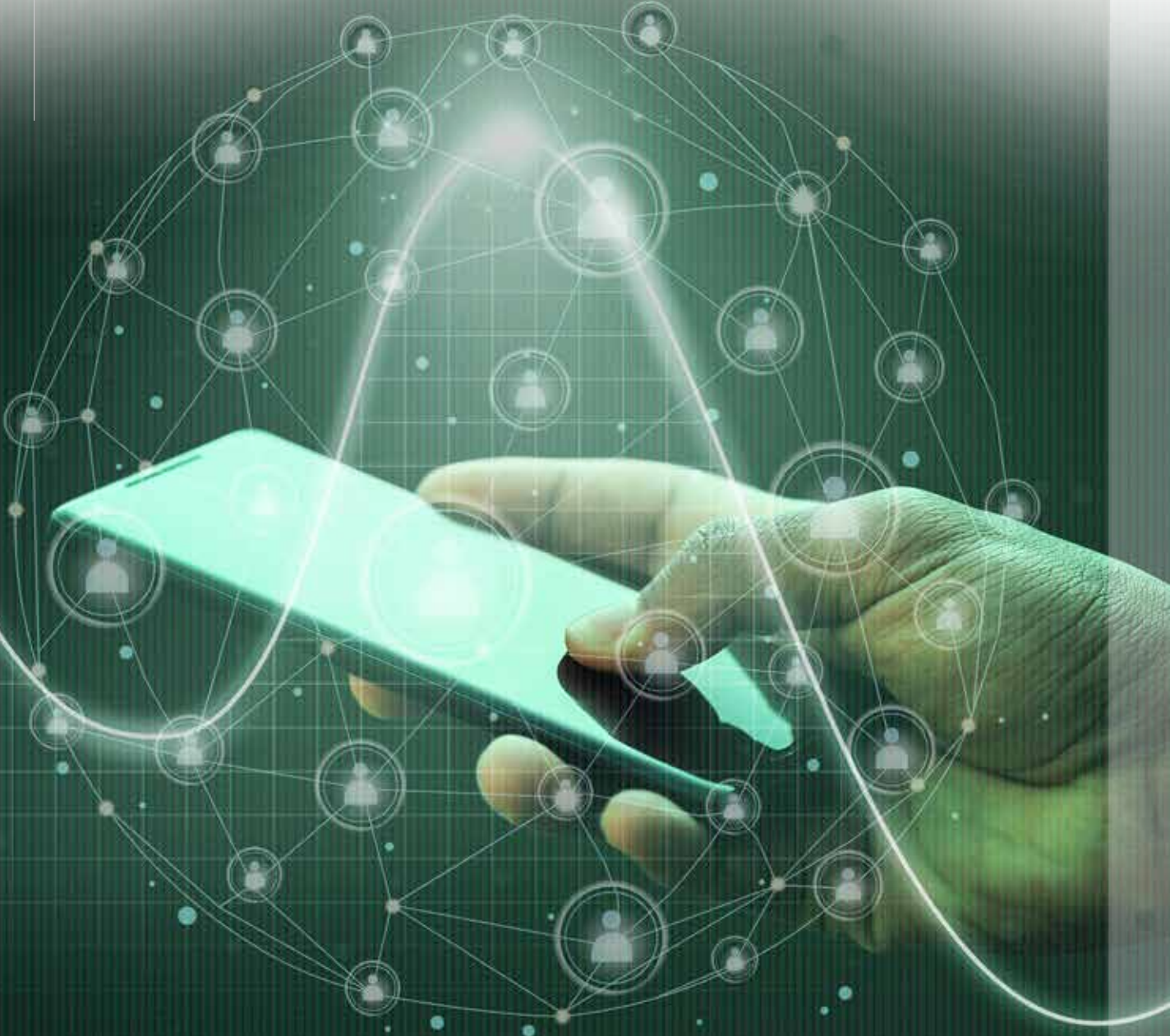
Politika Önerileri

Dezenformasyon ve onun yıkıcı etkileriyle mücadele etmek isteyen hükümetler için temel mesele, bir yandan dezenformasyonu önlemeye çalışmak, diğer yandan da toplumların dezenformasyona karşı daha dirençli olmalarını sağlayacak çözümler üretmek olarak tanımlanabilir. Yalan haber ve dezenformasyonla mücadelede demokratik ülkelerin benimsediği yaklaşım yol göstericidir. Bu ülkelerde dezenformasyon veya yalan haber kaynaklarına yönelik cezai yaptırımlar çok sınırlıdır ve sadece aşırı (terör) vakalar için geçerlidir. Öte yandan haberleri taşıyan platformlara da yükümlülükler getirilmesi tercih edilmiştir. Benzer bir yaklaşım, dezenformasyonla mücadelede Avrupa çapında kural koyucu olarak hareket eden Avrupa Komisyonu tarafından da benimsenmektedir.

Bilgi ekosisteminin güçlendirilmesi, Batı demokrasilerinde dezenformasyonla mücadele için kamu düzeyinde alınan tedbirlerin bir diğer ayağını oluşturmaktadır. Bu çerçevede dijital okuryazarlığın güçlendirilmesi, "doğrulama yapan kişilerin (fact checker)" desteklenmesi ve yalan haberlerin tespit edilmesine yönelik çalışmaların yapılması, medyada çoğulculuğun sağlanması ve ifade özgürlüğünün korunması gibi hedefler ön plana çıkmaktadır.

Sonuç olarak, bilgi ekosistemini korumak için yeni kurallara ve mekanizmalara ihtiyaç olduğu artık açıktır. Bu bağlamda yasa koyucunun da bir tercih yapması gerekmektedir. Nitekim yalan haberle mücadelede demokratik ülkeler ile otoriter sistemler arasında net bir ayrım ortaya çıkmıştır. Otoriter sistemlerde yasalar,

kamunun ön planda olduđu, zorlayıcı ve polisin hakim olduđu, basın ve ifade özgürlüğüne zarar veren tedbirlere ağırlık verirken, demokratik ülkeler ise tam tersine devletin yol göstericiliği ilkesine dayanmakta ve bilginin bu şekilde manipüle edilmesine esasen karşı çıkmaktadır. Sivil toplumun, gazetecilerin, doğrulama yapan kişilerin ve platformların daha fazla sorumluluk taşıdığı çözümleri benimsemişlerdir. Bu kritik tercih, demokrasilerin özünde yer alan toplumsal sözleşmedeki güvenlik ve özgürlük dengesini korumak için yapılmıştır. Türkiye'de yeni kabul edilen dezenformasyon yasasının uygulanması bağlamında bu genel çerçeveyi hatırlamak faydalı olacaktır.



DİJİTAL OKURYAZARLIK NEDİR?

Okuryazarlığın geleneksel tanımı kişinin ana dilinde okuma ve yazma becerisi iken, bu tanım yirminci yüzyılın ortalarında sorgulanmaya başlanmıştır¹. Gelişmekte olan ülkelerin teknolojik yeterlilikte geri kalma korkusu, teknolojinin hızlı büyümesi ve gelişmesiyle birleşince Paul Gilster 1997 yılında “Dijital Okuryazarlık” kavramını ortaya atmıştır. Gilster dijital okuryazarlığı, çok çeşitli kaynaklardan bilgisayar aracılığıyla çeşitli formatlarda sunulan bilgileri anlama ve kullanma becerisi olarak tanımlamıştır². Günümüzde, dijital bilgi aracı olarak bilgisayarların yanına internet özellikli diğer çeşitli cihazlar da eklenebilmektedir. Dolayısıyla okuryazarlık kavramı geleneksel okuryazarlığın ötesine geçmektedir. Microsoft tarafından yapılan daha yeni bir başka tanım ise “okuma, yazma, teknik beceriler ve eleştirel düşünmeyi kullanarak dijital dünyamızda gezinme yeteneği” olarak ifade edilmektedir. Bilgiyi bulmak, değerlendirmek ve iletmek için akıllı telefon, bilgisayar, e-okuyucu ve daha başka teknolojileri kullanmaktır³. Dijital medya aracılığıyla sunulan bilgiyi anlamaya ve kullanmaya dikkat çeken Gilster'dan farklı olarak, burada vurgunun belirli becerilerin yardımıyla tüm bir dijital dünyada “gezinmek” olduğuna dikkat etmek gerekir. Bu tanım aynı zamanda terimin daha ekonomik veya ticari bir şekilde anlaşılmasına da yol açmaktadır. Dijital okuryazarlık ve erişilebilirliğin sağladığı birbirine bağlanabilirlik, ya geleneksel olarak fiziksel hizmetlerin dijitalleştirilmesinden faydalanarak ya da tamamen dijital yeni fırsatlar için yeni yollar açarak ekonomik olasılıkları da beraberinde getirmektedir.

Dijital okuryazarlıkla ilgili bir diğer husus da dijital ve sosyal medya ile başa çıkmadaki önemidir. Dijital medya, geleneksel medyadan farklı olarak tek yönlü bir bağlantıya sahip değildir. Geleneksel medyada içerik yalnızca tek yönlü olarak iletilir. Dijital medyada ise kullanıcı artık bir zincirin son halkası değil, neredeyse sonsuz bir ağıın ortasındaki bir düğümdür; herkes ve her şey birbiriyle bağlantılıdır. Sonuç olarak, geleneksel medyanın aksine, katılımın önündeki engeller çok daha düşüktür ve herkes içerik yayınlayabilir ve istese de istemese de bir izleyici kitlesi bulabilir. Buna göre, TikTok'un dijital okuryazarlığa bakış açısı, örneğin, kişisel gizlilik, internet koruması ve dezenformasyona karşı koymaya odaklanmıştır⁴.

Bu tanımlara ve son gelişmelere dayanarak, bu raporu dijital okuryazarlıkla ilgili üç alana odaklamaya karar verdik. İlk olarak, dijital ekonomiye katılma becerisine odaklanıyoruz. Tüketicilerin bakış açısından, devlet tarafından sağlananlar gibi çevrimiçi hizmetlere ve e-bankacılık ve e-ticaret gibi diğer hizmetlere erişim farkındalığının dijital okuryazarlıkla nasıl sağlandığına bakıyoruz. Bu bölümü, Türkiye'de işin dijitalleşmesi bağlamında dijital becerilerin durumuna ilişkin kısa bir genel bakışla tamamlıyoruz. Gerçekten de dijital okuryazarlık, hizmetlerin kullanımını kolaylaştırmanın yanı sıra, Türkiye ekonomisinin sürekli dijitalleşen yapısı göz önüne alındığında, arz tarafında da kilit bir rol oynamaktadır. Daha sonra, kullanıcıların bu konudaki bilinç ve becerileri açısından

1 Kurt, Adile, Derya Orhan Göksün, Fatih Yaman, Mehmet Solak, and Fatih Türkan. “Bilgi ve İletişim Teknolojileri Işığında Türkiye’de Yapılan Okuryazarlık Çalışmalarındaki Eğilim” Eğitim Teknolojileri Araştırmaları Dergisi, Haziran 2014.

2 Lankshear, Colin, and Michele Knobel. “Digital Literacy and Digital Literacies” Nordic Journal of Digital Literacy, Ocak 2015, 13.

3 Microsoft. “Digital Literacy Courses, Programs & Resources | Microsoft Digital Literacy.” Erişim tarihi Ekim 27, 2022. <https://www.microsoft.com/en-us/digital-literacy>.

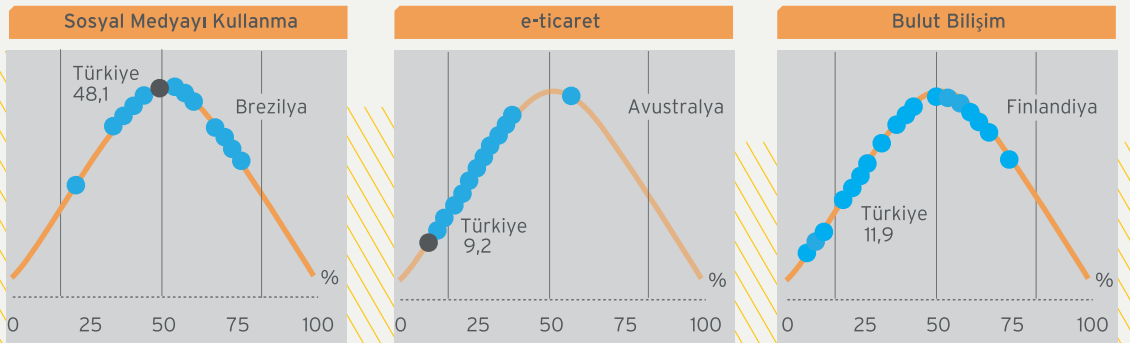
4 Newsroom | TikTok. “TikTok Unveils Digital Literacy Edition of Its Wellness Hub to Reinforce Commitment to Online User Safety and Education,” Mayıs 13, 2022. <https://newsroom.tiktok.com/en-sg/tiktok-unveils-digital-literacy-edition-of-wellness-hub>.

Türkiye'nin hangi noktada olduğunu belirlemek için internet güvenliği ve gizliliğine bakıyoruz. Son olarak, raporun önemli bir bölümünü, şu anda ulusal yasama ve politika gündeminde önemli bir yer tuttuğu için dezenformasyona ayırdık. Bu bölümde, dezenformasyonun üstesinden gelmenin bir yolu olarak dijital okuryazarlığa işaret ediyoruz.

DİJİTAL EKONOMİYE KATILIM BECERİSİ

Dijital ekonomi sıkça kullanılan bir kavram olmasına rağmen, bu kavram için özlü bir tanım yapmak zor olabilir. Esasen dijital ekonomi, dijitalleştirilmiş bilginin ana üretim faktörü olarak kullanıldığı ekonomik faaliyetlerin toplamı olarak tanımlanabilir. Bireyler ve işletmeler arasındaki dijital bağlantılar, veriler, internet özellikli makineler ve nesnelerin interneti bu bağlamda dijital ekonominin arka planını oluşturmaktadır⁵.

Benzer bir metodoloji kullanan FT Omdia Dijital Ekonomiler Endeksi'ne göre Türkiye, 2022 yılında karşılaştırılan 51 ülke arasında 20. sırada yer almaktadır⁶. Bu endeks değerlendirmesini beş kriter üzerinden yapmaktadır: bağlantı (ve iletişim), cihazlar (ve nesnelerin interneti), kurumsal bilişim, eğlence ve ödemeler. Türkiye genel sıralamada 20. sırada yer almasına rağmen, kredi kartı işlem hacminde 7., aylık aktif Facebook kullanıcısı sayısında 8. ve YouTube kullanıcısı sayısında 11. sırada yer almaktadır. Çevrimiçi net reklam cirosunda ise 20. sırada yer almaktadır. Bu göstergeler Türkiye'nin dijital tüketim açısından görece avantajlı bir konumda olduğuna işaret etse de endeksin e-ticaret kullanımı veya e-devlet hizmetlerine erişim gibi unsurları içermemesi kapsamlı bir analiz yapılmasını engellemektedir.



5 Atıcı, Gonca. Digital and Digitalized Economy in EMs: A Focus on Türkiye. Emerging Markets. IntechOpen, 2020. <https://doi.org/10.5772/intechopen.94494>.

6 Omdia. "FT Omdia Digital Economies Index 2022-26," Haziran 23, 2022.

Statista'nın 2021 Dijital Piyasalara Bakış⁷ raporunun Türkiye bölümü, dijital ekonominin hacmini dijital medya, e-ticaret ve e-hizmetler sektörlerinin yıllık cirolarını baz alarak ölçmektedir. Bu rapora göre 2018 yılında 5,58 milyar dolar olan dijital ekonomi hacmi 2021 yılında yaklaşık 13,1 milyar dolara ulaşmıştır. E-ticaret 2021'deki hacmin %89'unu tek başına oluşturmuştur.

Dijital ekonominin artan hacmi, insanların giderek daha fazla çevrimiçi işlem yapması nedeniyle dijital okuryazarlıkta da bir artışa işaret etmektedir. E-ticaret alanında bu durum, hem tüketicilerin hem de dijital ortamda faaliyet gösteren KOBİ sahiplerinin çevrimiçi ticaret yapma yetkinliğini geliştirdiğini göstermektedir. Ancak gelişmiş ülkelerle aradaki farklar devam etmektedir. OECD'nin 2021 tarihli bir raporunda, Türk KOBİ'lerinin dijital devrimi henüz tam olarak benimsemediği ileri sürülmektedir. Raporda, solda gösterilen sosyal medya kullanımı, e-ticaret ve bulut bilişimin benimsenmesine ilişkin grafikler bu gecikmenin göstergeleri olarak sunulmaktadır⁸. Bu faktörler aynı zamanda finansal ve altyapısal kapasite ile ilgili olsa da, dijital okuryazarlığın da bir rol oynadığını kabul etmek gerekir. Burada genel eğitim seviyesi ile dijital okuryazarlık arasında bir bağlantı kurmak mümkündür. Ingev ve Oxford Üniversitesi tarafından hazırlanan Türkiye'de Dijital Vatandaşlık raporu, eğitim seviyesinin dijital hizmetlerin kullanımıyla güçlü bir ilişki içinde olduğunu göstermektedir⁹. Öyle ki üniversite ve üzeri mezunların %72'si e-ticaret kullandığını belirtirken, bu oran lise, ortaokul ve ilkokul mezunlarında sırasıyla %52, %33 ve %23'e düşmektedir. Aynı eğilim e-bankacılık gibi diğer dijital hizmetler ve hatta yaygın olarak kullanılan e-devlet portalı olan E-Devlet için de geçerli olup üniversite ve ortaokul mezunları arasında %30'luk bir fark bulunmaktadır. Bu durumun işaret ettiği en basit çözüm, yetişkinlere yönelik tamamlayıcı programlarla birlikte genel olarak yükseköğretime yatırım yapmaktır.

Türkiye'nin dijital hizmetlerin benimsenmesi açısından başarılı olduğu alanlardan biri de dijital kamu hizmetleri, yani e-devlet olmuştur. Kamu hizmetlerinin dijitalleştirilmesi maliyetleri düşürmekte, daha şeffaf ve erişilebilir hale getirmekte ve genel olarak hükümetin etkinliğini artırmaktadır¹⁰. E-devlet hizmetleri bir zamanlar dijital alternatif olarak görülürken, 2022 BM E-Devlet Araştırması, yoğun dijitalleşmeyle birlikte çevrimdışı ve çevrimiçi kamu hizmetleri arasındaki çizginin kaybolduğunu ortaya koymaktadır¹¹. Rapor, dijital devletin artık "tek başına ya da yardımcı" bir araç olmaktan çıkıp kamu kurumlarının işleyişinin ve hizmet sunumunun ayrılmaz bir parçası haline geldiği kritik bir noktada olduğunu iddia etmektedir. Bu nedenle ulusal hükümetler için riskler daha yüksektir çünkü bu alandaki kötü yönetim siber güvenlik, veri gizliliği ve genel olarak kalkınma açısından zorluklar yaratmaktadır. Eylemsizlik, ekonomik ve sosyal kalkınma açısından kaçırılmış fırsatlar anlamına geldiği için de tehlikelidir.

Yukarıda bahsi geçen BM araştırması, Türkiye'yi "çok yüksek düzeyde beşeri sermaye gelişimi ve orta ila çok yüksek düzeyde altyapı gelişiminden faydalanarak" çevrimiçi hizmetler endeksinin çok

7 Statista. "Digital Economy - Türkiye." Erişim tarihi Ağustos 09, 2022. <https://www.statista.com/outlook/co/digital-economy/turkey>. Ağustos 2022 kurları kullanılarak.

8 OECD. "OECD SME and Entrepreneurship Outlook 2021 | En | OECD." Haziran 28, 2021. <https://www.oecd.org/publications/oecd-sme-and-entrepreneurship-outlook-2021-97a5bbfe-en.htm>.

9 "DİJİTAL VATANDAŞLIK: Erişim, Tutum ve Davranışlar - Sunum." Ingev, University of Oxford, Ekim 2021. <https://s.gazeteduvar.com.tr/storage/files/documents/2021/11/02/ingev-calistay-sunum-dijital-vata-tifw.pdf>.

10 Nam, Taewoo. "Does E-Government Raise Effectiveness and Efficiency?: Examining the Cross-National Effect." Journal of Global Information Management 27 (Temmuz 1, 2019): 120-38. <https://doi.org/10.4018/JGIM.2019070107>.

11 "E-Government Survey - The Future of Digital Government." UN Department of Economic and Social Affairs, 2022. <https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf>.

yüksek segmentinde yer alan on iki üst-orta gelirli ülkeden biri olarak tanımlanmaktadır¹². Kamu hizmetlerinin dijitalleştirilmesi, Ulusal E-Devlet Stratejisi ve Eylem Planı'nda ifade edildiği üzere Türkiye'nin uzun vadeli dijitalleşme politikasının bir parçası olmuştur¹³. Türkiye ayrıca Asya ülkeleri arasında en yüksek onuncu E-Devlet Gelişmişlik Endeksine sahiptir. TÜİK'e göre 2021 yılında Türk vatandaşlarının %68,7'si e-devlet platformunu kullanmıştır¹⁴. 2008'de başlatılan platform, 886 kurum tarafından sağlanan 6.665 dijital hizmet sunmaktadır ve 60 milyonun üzerinde kullanıcı sayısına sahiptir¹⁵. Türkiye e-devlet açısından yeterli kaliteye ulaşmış olsa da Avrupa ülkeleriyle karşılaştırıldığında E-Devlet Gelişmişlik Endeksi açısından sondan dördüncü sırada yer aldığı için hala gelişime açık alanlar bulunmaktadır. E-devlet hizmetlerine erişimdeki eğitim açığı göz önünde bulundurulduğunda, yetişkinler için tamamlayıcı programlarla birlikte genel olarak yükseköğretime yatırım yapmak basit bir çözüm olabilir.

Kullanıcılar açısından dijital okuryazarlık, ekonomi üzerindeki etkilerine ilişkin hikayenin yalnızca yarısıdır. Giderek dijitalleşen bir dünyada dijital okuryazarlık, üreticiler için dijital öncesi dönemdeki geleneksel okuryazarlık kadar önemlidir. BM'nin dijital kamu hizmetlerine ilişkin görüşü aslında tüm dijital ekonomi için genelleştirilebilir; dijital okuryazarlığın gerekli olduğu bilgi ve iletişim teknolojileri becerileriyle donatılmış bir işgücüne sahip olmayı başaramamak ya da yanlış yönetmek, yeni iş çağını yakalamayı kaçırmak anlamına gelir. McKinsey'in 2020 tarihli bir raporu, Türkiye'nin bu konuda sahip olduğu fırsatları ve zorlukları net bir şekilde ortaya koymaktadır¹⁶. Raporda, mevcut teknolojilerle 2030 yılına kadar her on meslekten altısının %30 oranında otomatikleştirilebileceği iddia edilmektedir. Otomasyon bir yandan belirli alanlarda ihtiyaç duyulan insan gücünü azaltacaktır. Öte yandan, yeni teknolojilerin benimsenmesinin de yeni işler yaratması beklenmektedir. Söz konusu olan, işleri otomatikleştirilecek çalışanlar ile teknolojik açıdan yoğun yeni işleri yapabilecek çalışanlar arasındaki değiş tokuştur. İkinci kategoride yer alanların gerekli dijital okuryazarlığa sahip olması gerekirken, ilk kategoride yer alanların da bu okuryazarlığı edinmeleri ve böylece açıkta kalmamaları gerekecektir. Bununla birlikte, rapor net olarak 3,1 milyon ek iş yaratılmasını öngörmektedir. 21,1 milyon çalışanın mevcut işverenleriyle çalışmaya devam edebilmeleri için dijital becerilerini geliştirmeleri gerekecektir. Yazarlar, 2030 yılına kadar 7,6 milyon kişinin önemli ölçüde yeniden beceri kazandırma ve iş değiştirmelerden etkileneceğini ve 7,7 milyon kişinin gerekli becerilere sahip olarak işgücüne katılacağını tahmin etmektedir.

Sayılar hiç de az değildir. Dijital okuryazarlık, önümüzdeki yıllarda dijitalleşme yoğunlaştıkça milyonlarca ailenin refahı ile derinden bağlantılı olacaktır. Rapor, bir önceki önerimiz doğrultusunda, Türkiye'deki işgücünün giderek artan bir bölümünün daha yüksek eğitim seviyelerine ihtiyaç duyacağını göstermektedir. İhtiyaç duyulan beceriler arasında daha yüksek bilişsel, sosyal ve teknolojik beceriler yer almaktadır. Teknolojik becerilere olan talebin %63 oranında artacağı tahmin edilmektedir. Eleştirel düşünme gibi daha yüksek bilişsel beceriler ve temel dijital becerileri içeren

12 "E-Government Survey - The Future of Digital Government." UN Department of Economic and Social Affairs, 2022, 13 <https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf>.

13 Ozan, Mehmet Seyda. "Türkiye'de Ulusal E-Devlet Stratejisi ve Eylem Planının Bilgi Ve İletişim Teknolojileri Üzerinden Değerlendirilmesi," 2020.

14 TÜİK. "Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2022," Ağustos 26, 2022. [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanim-Arastirmasi-2022-45587](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2022-45587).

15 Unal, Arife Yıldız. "E-Devlet Kapısında Kullanıcı Sayısı 60 Milyonu Geçti." Anadolu Ajansı, Kasım 8, 2022. <https://www.aa.com.tr/tr/gundem/e-devlet-kapisinda-kullanicisi-60-milyonu-gecti/2658630>.

16 McKinsey. "The Future of Work in Türkiye," Şubat 28, 2020. <https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-in-Turkiye>.

teknolojik beceriler dijital okuryazarlıkla bağlantılıdır. Hem hükümetin milli eğitim yoluyla hem de işverenlerin yeniden beceri kazandırma programları yoluyla işgücünün bu geçişe hazır olmasını sağlaması zorunludur. OECD'nin 2021 Türkiye Ekonomik Araştırması, yetersiz internet altyapısı ve dijital becerilerdeki eksikliklerden kaynaklanan darboğaz nedeniyle Türk firmalarının dijitalleşmeden büyük kazançlar elde edemediğini belirtmektedir. OECD, dijital alanlarda mesleki eğitimin ve yetişkin öğreniminin güçlendirilmesinin, üretken sektörün teknolojik değişim potansiyelinden daha iyi yararlanmasına yardımcı olacağını önermektedir.¹⁷ Ayrıca, öğrenciler için dijital eğitime odaklanmanın, dijital ekonominin doğasında var olan sosyoekonomik uçurumu azaltacağı belirtilmektedir.

teknolojik beceriler dijital okuryazarlıkla bağlantılıdır. Hem hükümetin milli eğitim yoluyla hem de işverenlerin yeniden beceri kazandırma programları yoluyla işgücünün bu geçişe hazır olmasını sağlaması zorunludur. OECD'nin 2021 Türkiye Ekonomik Araştırması, yetersiz internet altyapısı ve dijital becerilerdeki eksikliklerden kaynaklanan darboğaz nedeniyle Türk firmalarının dijitalleşmeden büyük kazançlar elde edemediğini belirtmektedir. OECD, dijital alanlarda mesleki eğitimin ve yetişkin öğreniminin güçlendirilmesinin, üretken sektörün teknolojik değişim potansiyelinden daha iyi yararlanmasına yardımcı olacağını önermektedir.¹⁷ Ayrıca, öğrenciler için dijital eğitime odaklanmanın, dijital ekonominin doğasında var olan sosyoekonomik uçurumu azaltacağı belirtilmektedir.

¹⁷ Florence, GUERINOT. "OECD Economic Surveys: Türkiye 2021." OECD Economic Survey, 2021, 78.

İNTERNET GÜVENLİĞİ VE GİZLİLİK BİLİNCİ

Dijital dünya ile etkileşim yoğunlaştıkça, siber saldırıların potansiyel yüzeyi de artmaktadır¹⁸. Basitçe söylemek gerekirse, kullanıcı daha fazla parolaya sahip oldukça parolanın ihlal edilme olasılığı da artmaktadır. Daha da kötüsü, kullanıcı artan internet hizmetleri kullanımına paralel olarak önlem almazsa, güvenlik açığı artmaktadır. İnterneti ve ilgili hizmetleri etkin bir şekilde kullanmak için potansiyel riskleri belirlemek ve önlem almak bir zorunluluk haline gelmiştir. Bu konudaki farkındalık ve dijital hijyen uygulamalarını gerçekleştirme becerisi, dijital okuryazarlıkla birlikte gelmektedir. Son kullanıcıların karşılaştığı siber güvenlik tehdidi türleri şunlardır :¹⁹

- **Kötü Amaçlı Yazılım Saldırıları:** Farklı yazılım virüslerinin mağdurun cihazına ya tehlikeye atılmış bir ağ üzerinden ya da mağdurun istemeden, örneğin şüpheli bir bağlantıya tıklayarak kötü amaçlı yazılımı indirmesi yoluyla bulaşması.
- **Kimlik Avı Saldırıları:** Saldırganın güvenilir bir kişiyi (bir yetkili, arkadaş veya teknik asistan gibi) taklit ederek mağdurun hassas bilgileri vermesini sağlaması.
- **Parola Saldırısı:** Saldırganın özel bir yazılım kullanarak mağdurun şifresini kırması.
- **Bağlantıyı İzinsiz İzleme Saldırısı:** Saldırganın, mağdurdan hassas bilgiler elde etmek için verileri ele geçirerek mağdurun iletişimini gizlice dinlemesi.

Bu örnekler, dijital okuryazarlığın eleştirel düşünme ve dijital sistemlerin nasıl çalıştığına dair temel bilgiler gibi yönlerinin siber güvenlikle bağlantılı olduğunu göstermektedir. Bazı bağlantılar otomatik olarak bir şeyler indirdiği için her bağlantıya tıklamamak gerektiğini ya da sadece rakamlardan oluşan şifrelerin kırılmasının daha kolay olduğunu bilmek, temel dijital bilginin güvenliği nasıl artırabileceğine dair birkaç örnektir. Ayrıca, daha geniş anlamda eleştirel düşünme, hangi bağlantının şüpheli olduğunu veya iletişim kurulan kişinin dolandırıcı olup olmadığını değerlendirmeye yardımcı olabilir. Nitekim, çocukların dijital okuryazarlık ve güvenlik becerilerini inceleyen bir LSE çalışması, güvenlik becerileri ile eleştirel okuryazarlık becerilerinin pozitif yönde ilişkili olduğunu ve potansiyel olarak birbirini güçlendirdiğini ortaya koymuştur²⁰.

Türkiye'de bu konularda farkındalık olduğuna dair bazı göstergeler mevcuttur. Ipsos tarafından 2020 yılının sonlarında 31 ülkede gerçekleştirilen bir anket bunu açıkça ortaya koymaktadır. Türkiye'nin "2021 yılında çevrimiçi hesaplarının hacklenmesinin muhtemel olduğunu düşünen yetişkinlerin oranında" listenin başında yer alması, yetişkinlerin %50'sinin "muhtemel" ve yalnızca %33'ünün "mümkün değil" yanıtını vermesi nedeniyle kesinlikle endişe vericidir²¹. Daha fazla bilgi vermek gerekirse, anket 2020 yılının sonlarında Ipsos tarafından 31 ülkede 15.700 katılımıyla gerçekleştirilmiştir²².

18 Fortinet. "What Is an Attack Surface? Definition and How to Reduce It." Erişim tarihi Ekim 28, 2022. <https://www.fortinet.com/resources/cyberglossary/attack-surface>.

19 Jaiswal, Sarvesh. "Different Types of Cyber Security Threats & Attacks | Emeritus India." Emeritus - Online Certificate Courses | Diploma Programs (blog), Haziran 30, 2022. <https://emeritus.org/in/learn/different-types-of-cyber-security-threats/>.

20 Haan, J. de, E. Kuiper, Sonia Livingstone, and N. Sonck. "Digital Literacy and Safety Skills." LSE, 2011. [http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20\(1sero\).pdf](http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20(1sero).pdf).

21 Statista. "Share of Adults Who Think It Is Likely That Their Online Accounts Will Be Hacked Into in 2021, by Country," Aralık 2020. <https://www.statista.com/statistics/1228062/opinion-online-security-worldwide/>.

22 AtlasVPN. "VPN Usage by Country 2022," 2022. <https://atlasvpn.com/vpn-adoption-index>.

Toplamda %34'lük bir kesim saldırıya uğrama ihtimalinin yüksek olduğunu düşünürken, %45'lik bir kesim ise bu ihtimali düşük görmüştür. Dahası, 2022 yılının ilk yarısında Türklerin %8,75'i VPN kullanmış ve bu da ülkeyi küresel karşılaştırmada on üçüncü sıraya yerleştirmiştir. Bununla birlikte, Ingev çalışmasından da görülebileceği gibi, eğitim seviyesine dayalı uçurum burada da belirgindir²³ :

	Yabancıardan gelen arkadaşlık isteklerini kabul etmiyorum	Sosyal medyada kişisel verilerimi nasıl koruyacağımı biliyorum	Sosyal medya sitelerindeki gizlilik ayarlarımı nasıl kullanacağımı biliyorum	İnternette okuduğum bilgilerin doğruluğunu farklı kaynaklardan kontrol ederim.	Parola gibi bilgileri asla kimseye paylaşmam.	Nasıl güçlü bir parola oluşturacağımı biliyorum.	Antivirüs yazılımı kullanıyorum
Üniversite ve üstü	%62	%72	%73	%70	%64	%67	%63
Lise	%61	%64	%63	%57	%57	%55	%49
Ortaokul	%58	%54	%54	%50	%48	%49	%43
İlkokul	%52	%38	%38	%38	%40	%30	%30
Eğitimsiz	%44	%40	%40	%15	%26	%22	%19

Ekonomik bağlamda olduğu gibi, eşitsizlikler burada da çevrimiçi güvenlik açısından dijital okuryazarlık söz konusu olduğunda kendini göstermektedir. Bu eşitsizlikler eğitim seviyesiyle de sınırlı değildir; LSE çalışması dijital becerilerin kullanımla birlikte geliştiğini ancak sosyo-ekonomik durum, yaş ve cinsiyet gibi eşitsizliklerin bu becerilerin gelişimini etkilemeye devam ettiğini ortaya koymuştur..²⁴ Gaziantep ve Kilis'teki lise öğrencileri üzerinde yapılan bir çalışma da bu sonucu doğrulamaktadır. Yazarlar, erkek öğrencilerin dijital güvenlik farkındalığı açısından kız öğrencilerden önemli ölçüde daha yüksek puan aldığını tespit etmişler²⁵. Bu tür eşitsizlik uçurumlarının kapatılması, dijital okuryazarlıktaki eksikliklerin giderilmesinde kilit öneme sahiptir.

Farkındalık, beceri ve güçlendirme, OECD'nin operasyonel dijital güvenlik risk yönetimi için belirlediği dört temel ilkedendir²⁶. Tamamlayıcı Belge, tüm paydaşların (yani hükümet, kamu ve özel kuruluşlar ile ekonomik ve sosyal faaliyetlerinin tamamı ya da bir kısmı için doğrudan ya da dolaylı olarak dijital ortama bel bağlayan bireylerin) bu ilkeye uyması gerektiğini, zira birinin riskleri göz ardı etmesinin diğerleri için de zararlı olabileceğini belirtmektedir. Tüm paydaşların harekete geçmesi halinde dijital okuryazarlık ve çevrimiçi riskler konusunda farkındalık kültürü oluşturulabilir. Milli eğitim, ilgili becerilerin geliştirilmesi ve eşitsizliklerin üstesinden gelinmesinde önemli bir bileşen olsa da, bir noktadaki internet güvenliği ve gizlilik eksiklikleri birbirine bağlı diğer dijital ekosistemlerin bütünlüğüne zarar verebileceğinden, bireylerin yanı sıra özel sektör de inisiyatif almalıdır.

23 "DİJİTAL VATANDAŞLIK: Erişim, Tutum ve Davranışlar - Sunum." Ingev, University of Oxford, Ekim 2021. <https://s.gazeteduvar.com.tr/storage/files/documents/2021/11/02/ingev-calistay-sunum-dijital-vata-tifw.pdf>.

24 Haan, J. de, E. Kuiper, Sonia Livingstone, and N. Sonck. "Digital Literacy and Safety Skills." LSE, 2011. [http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20\(Isero\).pdf](http://eprints.lse.ac.uk/33733/1/Digital%20literacy%20and%20safety%20skills%20(Isero).pdf).

25 Talan, Tarık, and Cemal Aktürk. "Orta Öğretim Öğrencilerinin Dijital Okuryazarlık ve Bilgi Güvenliği Farkındalığı Seviyelerinin İncelenmesi." Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi 18, no. 1 (Nisan 29, 2021): 158-80. <https://doi.org/10.33437/ksusbd.668255>.

26 OECD. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. OECD, 2015. <https://doi.org/10.1787/9789264245471-en>. Merriam-Webster. "Definition of Disinformation." Erişim tarihi Ekim 18, 2022. <https://www.merriam.com>

DEZENFORMASYON VE DİJİTAL OKURYAZARLIK

Dezenformasyon nedir ve dijital okuryazarlıkla bağlantısı nasıldır?

Dijital okuryazarlıkla ilgili en önemli konulardan biri dezenformasyondur. Yalan bilginin kasıtlı olarak yayılması son yıllarda özellikle acil bir konu haline gelmiştir.

Dezenformasyonun sözlük tanımı “kamuoyunu etkilemek veya gerçeği gizlemek amacıyla kasıtlı olarak ve genellikle gizlice yayılan (söylenti yayma gibi) yalan bilgi şeklindedir²⁷. Bu tanım aynı zamanda dezenformasyon ile yanlış bilgilendirme arasındaki farka da işaret etmektedir. Yanlış bilgilendirme temelde herhangi bir yanlış bilgidir. Öte yandan dezenformasyon, yanlış bilgilendirmenin yayılmasının ardındaki niyeti de kapsamaktadır. Dezenformasyon genellikle hedefe yöneliktir ve gerçeği belirli çıkarlar doğrultusunda manipüle etmeyi amaçlamaktadır. Bu çıkarlar siyasi olabilir; dezenformasyon bir rakibe karşı gizli bir karalama kampanyası şeklinde olabilir. Finansal da olabilir. Hem geleneksel hem de dijital medya kaynakları, hizmetlerinden para kazanmak için izleyici katılımına bağlıdır. Dolayısıyla, şok edici ya da abartılı içeriklerle daha büyük bir kitleyi cezbetmek bu tür aktörler için faydalı olabilir. Son zamanlarda haber ve eğlence arasındaki çizginin bulanıklaşması²⁸ bu meseleyi daha da vahim hale getirmiştir.

Günümüzde dezenformasyon ve dijital alanı birbirinden ayrı düşünmek neredeyse imkansızdır, ancak dezenformasyonun uzun bir geçmişi vardır. Aslında belgelenmiş ilk örneği M.Ö. 1274 yılına, Mısır Kralı 2. Ramses'in sonuçsuz kalan savaşını kasıtlı olarak büyük bir zafer olarak göstermesine kadar uzanmaktadır. Çok sayıda tapınak duvarına zafer sahneleri çizdirmiş ve bunu kutlayan şiirler yayınlamıştır²⁹. Daha yakın zamanlarda, yazılı medyanın ortaya çıkmasından sonra, yalan haberler ve aldatmacalar ortaya çıkmaya başlamıştır. Ay uygarlığıyla ilgili uydurma bir hikayenin anlatıldığı 1835 tarihli Büyük Ay Aldatmacası, New York Sun gazetesinin yüzyıllık ticari başarıya ulaşmasına yardımcı olmuştur³⁰. Dolayısıyla dijital medya ana akım haline gelmeden çok önce de yukarıda özetlenen saiklerle dezenformasyon örnekleri bulmak mümkündür. Bu örnekler aynı zamanda, günümüzde pek çok hükümetin atlamaya hevesli olduğu bilgi yayma kanallarının basitçe kısıtlanması ya da yasaklanmasının uygun bir çözüm olmadığı konusunda da bize ön fikir vermektedir; tapınak duvarlarının yerini gazete sayfaları almıştır ve bunların yerini de günümüzde web sayfaları ve uygulamalar almaktadır. Bilgi yayma kanalları var oldukça ve geliştikçe, dezenformasyon kanalları da gelişecektir.

Dijital dezenformasyonun bugün bu kadar endişe yaratmasının nedeni, yeniliğiyle bağlantılı olan etkinliğidir. Bir bakıma, gazetecilik etiğinin yerleşmesinden önce, okuryazarlığın düşük olduğu bir

27 Merriam-Webster. "Definition of Disinformation." Erişim tarihi Ekim 18, 2022. <https://www.merriam-webster.com/dictionary/disinformation>.

28 The Center for Digital Ethics and Policy. "From the Newsroom to the Television Screen: The Blurred Line between News and Entertainment," Eylül 2019. <https://digitalethics.org/essays/newsroom-television-screen-blurred-line-between-news-and-entertainment>.

29 Loktionov, Alex. "Ramesses II, Victor of Kadesh: A Kindred Spirit of Trump?" The Guardian, Aralık 5, 2016, sec. Science. <https://www.theguardian.com/science/blog/2016/dec/05/ramesses-ii-victor-of-kadesh-a-kindred-spirit-of-trump>.

30 Posetti, Julie, and Alice Matthews. "A Short Guide to the History of 'fake News' and Disinformation," n.d. https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20the%20History%20of%20Fake%20News%20and%20Disinformation_JCFJ%20Final.pdf.

ortamda yazılı basının patlama yaptığı zamanlara benzer bir durumdayız. Dijital sosyal medya da bugün benzer şekilde çok hızlı bir şekilde genişlemektedir. Tarihsel örnekten farklı olarak, erişim kolaylığı önemlidir, ancak düşük dijital okuryazarlık seviyeleri, yazılı medyanın başlangıcındaki gerçek okuryazarlık eksikliğine benzer sorunlar yaratmaktadır. Bunun en iyi kanıtı yankı odaları ve filtre balonları gibi dijital medyaya özgü sorunlardır. Dijital kitleler, bilgi aldıkları kaynak ve kanal türleri üzerinde daha fazla söz sahibidir. Bazı durumlarda bu kişiselleştirilebilirlik, insanların alternatif ya da karşı görüşlere kapalı bir bilgi ortamı yaratmalarına ve önceden var olan inançlarını pekiştirmelerine neden olmaktadır³¹. Yankı odalarının kasıtlı olarak yaratılması gerekmez; dijital bir sosyal ağı, genellikle benzer dünya görüşlerine sahip arkadaşlarınız ve ailenizle paylaşmak, fark edilmeyen bir yankı odasına neden olabilir. Öte yandan filtre balonu da benzer şekilde çalışmaktadır ancak sosyal medya ve arama motoru algoritmaları tarafından yaratılır. Basitçe söylemek gerekirse, çoğu algoritma girdi geçmişini daha ileri öneriler ve besleme tasarımları için bir temel olarak aldığından, halihazırda sahip olunan düşünce ve inançları da pekiştirip güçlendirebilir. Yankı odalarının ve filtre balonlarının etkileri ve yaygınlığı konusunda kanıtların karışık olduğunu belirtmek önemlidir³². Ancak bu olguların tanımlanması, dezenformasyon sorununun iki katmanı olduğuna işaret etmektedir. Bunlardan biri, platform seçimlerinin ve algoritmaların işleyişinin yalan bilginin yayılmasını etkilediği dezenformasyonun teknolojik ve algoritmik yönüyle ilgilidir. Diğer katman ise izleyicilerin eylemleri, seçimleri ve çevrimiçi bilgi ile genel etkileşimleri ile ilgilidir; bu da dezenformasyonun yarattığı zorlukların üstesinden gelmede dijital okuryazarlığın önemine işaret etmektedir.

Dezenformasyon türleri

Bir önceki bölümde dezenformasyonu yanlış bilgilendirme ile ilişkili olarak tanımlamıştık. Kavramı daha fazla ayırtmadan önce, dezenformasyonun yanlış bilgilendirme ve kötü amaçlı bilgilendirme arasındaki konumunu netleştirmek daha iyi olacaktır. Yukarıda açıklandığı üzere, yanlış bilgilendirme, herhangi bir kötü niyet olmaksızın yalan bilginin paylaşılmasıdır. Kötü amaçlı bilgilendirme ise, özünde doğru olan ancak kamunun çıkarlarından ziyade kişisel veya kurumsal çıkarlara hizmet edecek şekilde sunulan bilgilerin kasıtlı olarak paylaşılması anlamına gelmektedir. Bir bilginin bağlamını manipüle etmek yaygın bir kötü amaçlı bilgilendirme yöntemidir³³.

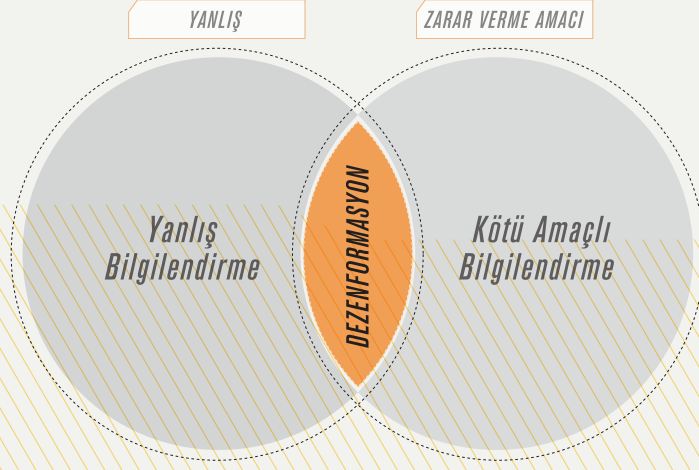
Dezenformasyon, yanlış bilgilendirme ve kötü amaçlı bilgilendirmenin kesiştiği noktada konumlandırılabilir. Dezenformasyon, yanlış bilgilendirmede bulunan sahtelik ile kötü amaçlı bilgilendirmenin kötü niyetini aynı anda içermektedir³⁴.

31 Ross Arguedas, Amy, Craig T. Robertson, Richard Fletcher, and Rasmus Kleis Nielsen. "Echo Chambers, Filter Bubbles, and Polarisation: A Literature Review." Reuters Institute for the Study of Journalism, Ocak 19, 2022. <https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review>.

32 Ibid.

33 Staats, Beth. "Misinformation, Disinformation, Malinformation: What's the Difference?" Minitex, Şubat 2021. <https://minitex.umn.edu/news/elibrary-minnesota/2022-05/misinformation-disinformation-malinformation-whats-difference>.

34 Wardle, Claire. "Understanding Information Disorder." First Draft News. First Draft, Eylül 2020. <https://firstdraftnews.org/443/long-form-article/understanding-information-disorder/>.



Yanlış bilgilendirme bazen dezenformasyondan kaynaklanmaktadır çünkü yalan bilgiyi paylaşan ilk aktör, bunu kötü niyet olmaksızın paylaşan bir izleyici ağına dayanır. Aile içi kısa mesaj zincirleri örneği buna iyi bir örnektir. Dahası, terimlerin kendileri de genellikle birbirini dışlamaz çünkü niyet atfetmek ya da gerçeğin nerede bitip yalanın nerede başladığını belirlemek her zaman kolay değildir.

Claire Wardle tarafından formüle edilen 7 tür yalan ve yanlış bilgi, bu kavramları daha ayrıntılı bir şekilde açıklığa kavuşturan iyi bir kılavuzdur³⁵.

Hiciv ve parodi: Bunlar tamamen eğlence amaçlı yapılsa da bazıları bunları gerçek sanabilir ve içeriklerini doğru sanarak yayabilir. Ayrıca, siyasi hiciv ve parodi, içeriğin doğruluğu kasıtlı olarak bulanık bırakıldığında bazen dezenformasyon çabalarının bir parçasıdır.

Yalan bağlantı: Bazen içerikten çıkarılan başlıklar, görseller veya alıntılar kasıtlı olarak yanıltıcıdır. Bu durum çoğunlukla, platformun içeriğin doğruluğundan ziyade içerikle etkileşim sağlamakla ilgilendiği "tık tuzağı (clickbait)" içeriklerde görülür.

Yanıltıcı içerik: Burada, bilginin yanlış olması gerekmez, ancak yerleştirilmesi ve sunumu, izleyiciyi bir kişi veya konuya ilişkin temelsiz bakış açılarına veya fikirleri benimsemeye yönlendirecek şekilde yapılır. Bunun özellikle tehlikeli bir versiyonu, bir konu ya da kişiyle ilgili gerçeklerin spekülasyonla karıştırıldığı ya da tezlerin gerçekmiş gibi sunulduğu sahte gerçeklerdir. Bu gibi durumlarda gerçeği kurgudan ayırmak daha da zorlaşır.

Yalan içerik: Gerçek içerik bazen izleyicileri kandırmak için yanlış bir şekilde bağlamsallaştırılır. Bu, konuşmacının aslında desteklemediği bir görüşü destekliyormuş gibi göstermek için cümlenin ortasındaki bir ifadeyi kırmak olabilir. Türkiye'de sık rastlanan bir başka örnek de, geçmişte yaşanan haberlerin güncel olaylarla ilişkilendirilerek yeniden servis edilmesi ve böylece insanların bu iki olayın aynı anda yaşandığı veya aralarında bir bağlantı olduğu yönünde yanıltılmasıdır.

Sahte içerik: Kötü niyetli aktörler bazen dezenformasyon yaymak için başka, daha güvenilir kaynaklar gibi davranırlar. Örneğin, pandemi sırasında, üzerinde kamu kurumlarının ve uluslararası kuruluşların logoları bulunan ve bu logolara gerçeklik havası veren çok sayıda sahte belge ortaya çıkmıştır. Kamuoyunda ciddi ve saygın olarak algılanan kurumlara yönelik yüksek güven seviyesi göz önüne alındığında, bu durum Türkiye için özellikle aciliyet arz eden bir konudur.

Manipüle edilmiş içerik: Bilgi, görüntü ve hatta ses ve videoları manipüle etme araçları hızla gelişmektedir. Kötü düzenlenmiş bir görüntüyü tespit etmek o kadar da zor olmasa da, yapay montaj videolar (deepfakes) gibi yeni teknolojiler, gerçeği belirlemenin ana yolu olan temel insan algısını atlamaya çalıştıkları için özellikle tehlikelidir.

Uydurma içerik: Son olarak, dezenformasyonun ana kanalı olan tamamen uydurma içerik vardır. Bunu sahte haberlerde ve komplo teorilerinde görmekteyiz.

Yanlış bilginin yayılma yolları çeşitlidir ve her biriyle mücadele etmek farklı teknikler ve müdahaleler gerektirmektedir. Dahası, teknoloji ve toplum daha da geliştikçe yeni kanallar ortaya çıkmaktadır. Dezenformasyon sayısız kişisel veya başka saiklerle yayılsa da, sosyo-politik boyutu hem demokrasi hem de sosyal uyum için önemli bir tehdit oluşturmaktadır. Hükümetlerin ve uluslararası kuruluşların bu olguyla mücadeleye özellikle ilgi duymalarının nedeni de budur. Bu nedenle, dezenformasyonun bu konuları nasıl etkilediğine ilişkin bir tartışmanın olduğu bir bölüm gerektirmektedir.



Demokrasi ve Sosyal Uyum Üzerindeki Etkileri

Dezenformasyonun sinsiliği, geniş kitleleri ikna etmek zorunda kalmadan hedeflerine ulaşabilmesinden kaynaklanmaktadır. Şu ana kadar yankı odaları ve filtre balonlarından, insanların enformasyonel olarak daha geniş dijital kamuyundan izole edildiği ve yalan bilgiye dönüşebilecek tek taraflı ve giderek yoğunlaşan bakış açılarına maruz kaldığı iki örnek olarak bahsettik. Ancak dezenformasyon aynı zamanda rasyonel tartışmaları dışarıda bırakarak kendine alan açmaktadır. Kötü niyetli aktörler dezenformasyonu yeterince yüksek miktarlarda yaydığına, tartışmadaki "gürültü" miktarı gerçek sinyalleri gizleyerek gerçeklerin ve fikirlerin iletişimini engelleyebilir. Bu durumda izleyiciler, ister kamu yararına ister dezenformasyon yayma amacıyla hareket ediyor olsunlar, aktörlerden herhangi birine güvenmeyi reddederek herhangi bir bakış açısını dikkate almamaya karar verebilirler.

Bu durum siyasi tartışmalara uygulandığında, vatandaşların dezenformasyona ikna oldukları için değil, artık kime güveneceklerini bilmedikleri için kurumlara olan güvenlerini kayb ettikleri bir "siyasetten çekilme" ile sonuçlanmaktadır³⁶. %59'unun görüşlerini internette ifade etmekten çekindiği bulgusu, Türkiye'de bunun halihazırda gerçekleşmekte olduğunun bir işareti olabilir. Siyasetten geri çekilmenin demokratik kurumlar üzerindeki aşındırıcı etkisine ek olarak, etkin katılım, bilgilendirilmiş seçmen ve gündemin vatandaşlar tarafından kontrolü gibi demokrasinin temel özelliklerini engelleyerek, bu fikrin kendisinin de altını oymaktadır³⁷. Dolayısıyla, ifade özgürlüğünün sınırlandırılması ve insanların çevrimiçi katılımdan caydırılması, bu tür dezenformasyonun etkilerini artırmaktan başka bir işe yaramayacaktır.

Daha ilımlı grupları depolitize etmenin yanı sıra, seçim kampanyaları sırasında ortaya çıkanlar gibi kutuplaşmış siyasi ortamlar, kötü niyetli aktörlerin yalan bilgi yoluyla siyasi ayrılıkları derinleştirmesine olanak tanımaktadır. Örneğin 2016 ABD başkanlık seçimlerinde, Rusya merkezli grupların her iki tarafı da radikalleştirmek amacıyla dezenformasyon sağlayan sosyal medya sayfaları kurduğu ortaya çıkmıştır³⁸. Bu örnekte de görüldüğü üzere, yabancı kaynaklı dezenformasyon da daha geniş bir meselenin büyük bir bileşenidir çünkü bu aktörler kökenlerini gizlemek için sosyal ağların opaklığına güvenebilirler.

Kutuplaşma sadece siyasi alanda dezenformasyona davetiye çıkarmamaktadır. Pandemi, genel olarak toplumsal uyumun bundan zarar görebileceğini göstermiştir. Türkiye'de virüs, aşılarda ve 5G ile ilgili çok sayıda komplo teorisi bir araya getirilerek yanlış bir anlatı oluşturulmuştur³⁹. Kısacası, dezenformasyon taraftarları 5G ağ istasyonlarının virüsün yayılmasında etkili olduğu ve aşılarda 5G aracılığıyla uzaktan etkinleştirilecek mikroçipler içerdiği hikayelerini yaymıştır. Sonuç olarak teknoloji ve aşı paranoyası birlikte ortaya çıkmıştır⁴⁰. Kritik bir kamu sağlığı politikasını baltalayan

36 Butcher, Paul. "Disinformation and Democracy: The Home Front in the Information War." European Policy Centre, Ocak 30, 2019.

37 Dahl, Robert A. "Democracy - Features of Ideal Democracy." Britannica. Erişim tarihi Ekim 21, 2022. <https://www.britannica.com/topic/democracy/Features-of-ideal-democracy>.

38 K.N.C. "Digital Disinformation Is Destroying Society but We Can Fight Back." The Economist, Ocak 17, 2020. <https://www.economist.com/open-future/2020/01/17/digital-disinformation-is-destroying-society-but-we-can-fight-back>.

39 Yılmaz, Mert Can. "5G ile yeni koronavirüs arasında bağ olduğu iddiaları Türkiye'ye nasıl geldi?" Teyit, Nisan 2020. <https://teyit.org/5g-ile-yeni-koronavirüs-arasında-bağ-olduğu-iddiaları-türkiye-ye-nasıl-geldi>.

40 Yılmaz, Mert Can. "5G ile yeni koronavirüs arasında bağ olduğu iddiaları Türkiye'ye nasıl geldi?" Teyit, Nisan 2020. <https://teyit.org/5g-ile-yeni-koronavirüs-arasında-bağ-olduğu-iddiaları-türkiye-ye-nasıl-geldi>.

bu durum, sosyal bağlara zarar vermenin ötesine geçerek aslında sağlık ve ölüm oranlarını etkilemiştir. Bu örnek aynı zamanda “Büyük Dezenformasyon” kavramını gündeme getirmek için de uygundur. Türkiye’de merkezi bir mesele olmasa da, pek çok ülkede pandemiyle ilgili dezenformasyonla mücadeleyle yönelik ilk girişim, bilimsel gerçekler olarak kabul edilenler etrafındaki tartışmayı sınırlandırmaya çalışmak olmuştur. Bilimsel fikir birliği geliştikçe, başlangıçta sabit, ampirik gerçekler olarak algılanan onaylanmış anlatılar da değişmiştir. DSÖ’nün maskelerle ilgili tavsiyeleri buna iyi bir örnektir. Kurumların bir anlatıyı onaylaması ve dezenformasyon olarak gördüklerini toplumsal alanın dışına itmesi, ancak daha sonra geri adım atarak aynı gayretle de olsa farklı bir anlatı ortaya koyması şeklindeki bu yaklaşımın, güven kaybına yol açarak dezenformasyonun çökücülüğünü artırdığı ileri sürülmektedir⁴¹.

Bu, içerik odaklı müdahalelerin verimsiz olduğunun gösterildiği bir örnektir. Tartışma odaklı çözümleri merkeze alan politika önerilerimize geçmeden önce, Türkiye’nin yakın tarihli Dezenformasyon Yasası üzerine son bir tartışma, sonraki önerilerimizin daha iyi konumlandırılmasına yardımcı olacaktır.

Türkiye’de dezenformasyon önlemleri

Türkiye’de dezenformasyonun daha detaylı analizine geçmeden önce, kamuoyunun bu olguya bakış açısına ve bu olguyla etkileşimine genel bir bakış sunmak daha doğru olacaktır. Aşağıdaki metin, Türkiye Raporu tarafından hazırlanan “Yeni Dünya, Yeni Uygulamalar: Dijital Okuryazarlık” başlıklı araştırma raporun tartışmasıdır⁴². Rapor, Ağustos 2022’de 1.500 katılımcı ile gerçekleştirilen bir anketin bulgularına dayanmaktadır.

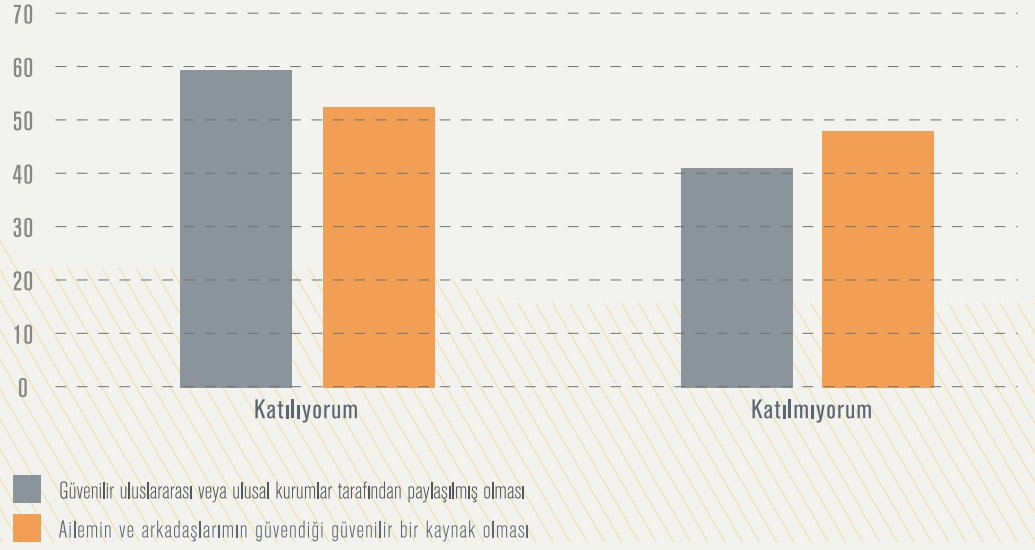
Türkiye’de insanların büyük çoğunluğu internetteki bilgilerin doğruluğuna şüpheyle yaklaşmaktadır. Katılımcıların %63’ü internetteki bilgilerin çoğunun gerçeği yansıtmadığını düşünmektedir. Dijital bilgiye yönelik şüphecilik bunun da ötesine geçmiş olup, %58 oranında kişi, sosyal medyada trend olan konuların gerçeği yansıtmadığını düşünmektedir. Burada dezenformasyonun ilerleyen bölümlerde daha ayrıntılı olarak inceleyeceğimiz bir yönüne ilişkin ilk ipucunu elde ediyoruz; bu rakam sadece çevrimiçi bilgiye yönelik genel güvensizliğin bir uzantısı olsa da, karşılaşılan çoğu bilginin yalan olduğu algısının tüm çevrimiçi bilgilerin reddedilmesine yol açtığı bir kırılma noktası da olabilir.

Bu sonuçlara dayanarak, dijital olarak aktif nüfusun çoğunluğunun yeni dijital bilgilerle karşılaştığında en kötüsünü varsaydığını söylemek abartılı olmayacaktır. Bunun üstesinden gelmek için, çevrimiçi bilginin doğruluğuna dair bir inanç oluştururken, katılımcıların çoğunluğu bilginin güvenilir bir uluslararası veya ulusal kurum tarafından paylaşıldığında (%59) ve kaynak arkadaşlar ve aile tarafından güvenilir olarak görüldüğünde (%52) daha güvenilir hale geldiğini belirtmiştir.

41 Friedersdorf, Conor. “How ‘Big Disinformation’ Can Overcome Its Skeptics.” The Atlantic, Nisan 21, 2022. <https://www.theatlantic.com/ideas/archive/2022/04/anti-disinformation-laws-social-media/629612/>.

42 “New World, New Practices: Digital Literacy.” Türkiye Raporu, Ağustos 2022.

İnternette bulduğunuz bilgilerin doğruluğuna inanmanızda kaynağın hangi özellikleri rol oynamaktadır?
%



Bu da kurumlara duyulan güvenin ve bir kaynağın sosyal kabulünün algılanan güvenilirliğini nasıl etkilediğini göstermektedir. Bu nedenle, yakın sosyal çevreler tarafından katalize edilebilen yankı odalarına ek olarak sahte/paravan kuruluşlar ve uzmanlar konusuna daha yakından bakacağız. Gerçekten de Türkiye'de bir akrabadan dezenformasyon içeren bir kısa mesaj almak nadir değildir. Bu tür aile temelli bilgi paylaşım ağları dezenformasyona karşı özellikle savunmasızdır çünkü sevdiklerini bilgilendirme ve koruma dürtüsü genellikle söz konusu bilgiyi doğrulamaya yönelik rasyonel kaygıların önüne geçmektedir.

Güvenilirliğin bir başka göstergesi de bilgiyi yayan kaynağın görünürdeki popülerliği olabilir. Ancak katılımcıların %71'i takipçi sayısının bilgi kaynağına duydukları güveni etkilemediği konusunda hemfikirdir. Bununla birlikte, genç yaş grupları bu aktörlerin popülerliğinden daha fazla etkilenmektedir. Dahası, %54'lük bir kesim tanınmış bir kişinin hesabından paylaşılan bilginin daha güvenilir olduğuna katılmazken, 18-24 yaş grubunda bu oran %34,2'ye düşmektedir. Anonim hesapların algılanan güvenilirliği konusunda da benzer bir dinamik söz konusudur. Genel olarak %71 bu tür hesapları ciddiye almadıklarını söylerken, bu oran 18-24 yaş grubunda %61,5'e düşmektedir. Genç kuşakların çevrimiçi bilgilerle etkileşimi yaşlı kuşaklardan önemli ölçüde farklıdır. Bu nedenle, dezenformasyonu analiz ederken gençlere özel dikkat gösterilmelidir.

Özetle, Türkler genel olarak dijital bilgiye şüpheli ve temkinli yaklaşmaktadır; en azından kendilerini bu şekilde algılamaktadırlar. Bununla birlikte, %59'unun görüşlerini internette ifade etmekten çekindiğini de belirtmek gerekmektedir. Buradaki tablo dezenformasyonla ilgili bazı sorunlara ve çözümlere işaret etmektedir. İnsanların çoğunluğu internetteki bilgileri olduğu gibi kabul etmemekte, ancak görüşlerini ifade etmekten de çekinmektedir. Buradan iki sonuç çıkarılabilir. Ya dezenformasyon o kadar etkili değildir; yaygındır ancak ciddiye alınmamaktadır ve insanlar bilgiye karşı koymak için harekete geçmemektedir. Dezenformasyonun Türkiye'de etkili olduğu kanıtlandığı için (nefret kampanyaları, ırkçılık vb.) bu büyük olasılıkla doğru değildir. İkinci ve daha olası sonuç ise, insanlar sorunun farkında olsalar ve kendilerini bundan izole edebileceklerini düşünseler de, dijital okuryazarlık eksikliği ve dezenformasyon yöntemleri bunu yapmalarını engellemektedir. Dezenformasyon yayan sesli azınlığı güçlendirdiği için çevrimiçi tartışmaya katılmaktan çekinmek bunun sadece bir örneğidir.



Türkiye'nin Yeni Dezenformasyon Yasası

Türkiye'de "Dezenformasyon Yasası" olarak da bilinen 7428 sayılı Torba Yasa 18 Ekim 2022 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Sosyal medya platformları, mesajlaşma uygulamaları gibi üst düzey platformlar ve çevrimiçi gazetelere yönelik ek düzenleme ve gerekliliklere ek olarak, yasanın tartışmalı bir yönü de dezenformasyonu suç haline getirme şeklindedir. Yasaya göre, dört temel kriterin aynı anda yerine getirilmesi halinde "yanıltıcı bilgi yaymak" suç haline gelmektedir:

- Kamuoyuna yalan bilgi yayılması,
- Ülkenin iç ve dış güvenliğine ilişkin olması,
- Endişe, korku veya panik yaratma niyetiyle yapılması,
- Kamu düzenini ve genel sağlığı bozacak şekilde olması.

Suçlu bulunmaları halinde failler 1-3 yıl hapis cezasına çarptırılmaktadır. Ayrıca, kimliklerini gizledikleri ve/veya bir örgüt çerçevesinde faaliyet gösterdikleri tespit edilirse, ceza %50 oranında artmaktadır. Yasa dezenformasyonu "kasıtlı olarak yalan haber üretme ve yayma eylemi" olarak tanımlasa da, yasada atıfta bulunulan "yanıltıcı bilgi", "gerçeğe aykırı bilgi" veya "halk arasında endişe, korku veya panik yaratma niyeti" için yasal tanımlar yapmamaktadır. Sosyal ağ sağlayıcıları, soruşturmanın bir parçası olarak kullanıcı verilerini yasal makamlara sağlamakla yükümlüdür ve uyumsuzluk durumunda bant genişliklerinde %90'lık bir azalma ile karşı karşıyadır.

Yasa şu ana kadar ifade özgürlüğü ve özel hayatın gizliliğini ciddi şekilde kısıtladığı gerekçesiyle eleştirilmiştir. İnsan Hakları İzleme Örgütü⁴³, Venedik Sözleşmesi⁴⁴ ve Article 19⁴⁵ gibi kurum ve organlar bu değerlendirmeye dayanan endişelerini dile getirmişlerdir. Bu rapor bağlamında, Dezenformasyon Yasası, önceki bölümlerde değinilen diğer politika yanıtlarına benzer eksiklikler içermektedir. Esasen, devlet gerçeği ve niyeti belirleme sorumluluğunu üstlenmekte ve belirsiz kriterlere dayalı olarak davranışı suç saymaktadır. Bu yaklaşım ters etki yaratabilir. İlk olarak, "ülke güvenliği" ve "kamu düzeni" gibi açık uçlu kriterler siyasi yorumlara açık kapı bırakmaktadır ki eleştirmenlerin bunu bir "sansür yasası" olarak yorumlamasının bir nedeni de budur. Yasanın uygulanması keyfi olarak algılanırsa, dijital alanda zaten daralmış olan kamusal tartışma alanını daha da daraltabilir. Bunun zaten dezenformatif aktörlerin amaçlarından biri olduğunu belirtmiştir. Devletin de kasit atfedeceği gerçeğiyle birleştiğinde, çoğu sosyal medya kullanıcısı da dahil olmak üzere iyi niyetli bilgi yayıncılarının katılım konusundaki tereddütlerinin artması, doğru bilginin yayılmasını da engelleyebilir. Sonuçta, dezenformasyona karşı denge unsuru doğrulama yapan üçüncü taraf kişiler, kullanıcılar ve platformlar olmaktan çıkıp merkezi hükümetin organları haline gelmektedir. Gerekli kapasite ve yetkinlik oluşturulana kadar, devlet kurumlarının ve yasal aktörlerin dezenformasyonla mücadelede daha az etkili olması şaşırtıcı olmayacaktır.

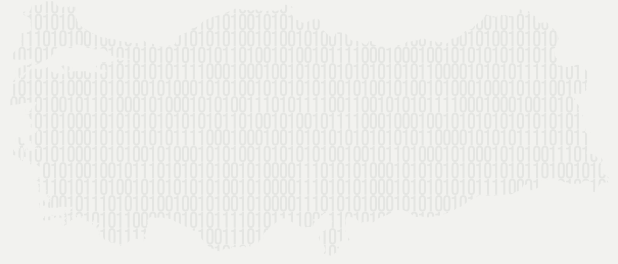
43 Human Rights Watch, "Türkiye: Dangerous, Dystopian New Legal Amendments," Ekim 14, 2022. <https://www.hrw.org/news/2022/10/14/Türkiye-dangerous-dystopian-new-legal-amendments>.

44 Venice Commission, "Urgent Joint Opinion of the Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the Draft Amendments to the Penal Code Regarding the Provision on "false or Misleading Information" - Issued Pursuant to Article 14a of the Venice Commission's Rules of Procedure," Ekim 7, 2022. <https://venice.coe.int/webforms/documents/?pdf=CDL-PI%282022%29032-e>.

45 ARTICLE 19, "Türkiye: Dangerous, Dystopian New Legal Amendments," Ekim 14, 2022. <https://www.article19.org/resources/Türkiye-dangerous-dystopian-new-legal-amendments/>.

Dahası, bilgi (ve dolayısıyla gerek) durağan olmadığından, dezenformasyonun kriminalize edilmesi daha önce tartışılan “Büyük Dezenformasyon” ile ilgili sorunları daha da kötüleştirebilir. Kriminalizasyon bu şekilde insanlar arasında hükümete karşı daha derin bir antipatiyi besleyebilir, hatta muhtemelen komplo teorisyenlerinin çekiciliğini arttırabilir.

POLİTİKA ÖNERİLERİ



Dijital Ekonomiye Katılım için:

Umberto Eco'nun bir zamanlar dediği gibi: “Birine bir şey öğretmek için televizyonu kullanmak istiyorsanız, önce ona televizyonu nasıl kullanacağını öğretmelisiniz.” Bugün aynı şey genel olarak dijital teknolojiler için de geçerlidir ve bu teknolojileri kullanmanın amacı öğretmenin çok ötesine geçmektedir. Dijital okuryazarlık, Türkiye'nin dijitalleşmeden elde edeceği kazanımları kaçırmaması için elzemdir. Potansiyel faydalardan yararlanamamanın yanı sıra, işgücünün dijital okuryazar olacak şekilde eğitilmemesi, işleri otomatikleştirildiğinde milyonlarca çalışanın fırsatlarının azalacağı anlamına da gelebilir. Küçük işletmeler ve perakendeciler açısından dijital okuryazarlık hala bir darboğazdır. Bu nedenle e-ticarette son dönemde yaşanan patlama, bu darboğazın aşılması halinde elde edilebilecek başarının bir göstergesi olarak görülmelidir.

Dijital okuryazarlık eğitiminin iyileştirilmesi ilk akla gelen çözümdür. Bu, işgücünün yeniden eğitilmesi için elzemdir ve başarısız olması halinde önemli büyüklükte sosyo-ekonomik etkileri olabileceğinden özel şirketler, kamu sektörü ve sivil toplum kuruluşları tarafından ele alınmalıdır. Ancak bu sadece bugün görünen bir semptomun çözümü olabilir. Daha temel bir çözüm ise dijital çözümlerin eğitimin tüm alanlarına entegre edilmesidir. Daha önce de belirtildiği gibi, dijital okuryazarlık eleştirel düşünme, okuma ve yazma gibi teknik olmayan becerileri de içermektedir. Bu becerileri öğretmek için dijital yöntemleri kullanan öğretim yöntemleri, tıpkı geleneksel okuryazarlık öğretiminin bir noktadan sonra harfler ve hecelerden metinleri anlama ve kompozisyon yazmaya doğru ilerlemesi gibi öğrencilerin dijital okuryazarlığını arttıracaktır. Bu sadece milli eğitimle de sınırlı kalmamalıdır. İş dünyası veya diğer ekonomik faaliyetlerle ilgili her türlü eğitimde, öğretilen materyallerin dijital uygulamaları dikkate alınmalıdır.

İnternet Güvenliği ve Gizliliği için:

Buradaki önerilerimiz Dijital Ekonomi için olanlarla aynı ruhu paylaşmaktadır. Geliştirilmiş eğitim çağrısı burada da geçerlidir. Ancak vurgulanması gereken bir husus, dijital güvenlik ihlallerinin yüksek etkili doğası nedeniyle, bu alandaki dijital okuryazarlık çabalarının eğitim ve resmi öğretimin

ötesine geçmesi gerektiğidir. Dijital güvenlik bilincinin ve bu konudaki temel becerilerin ikinci doğa haline geldiği bir dijital güvenlik kültürüne ihtiyaç vardır. Sonuçta gece kapımızı kilitlemeyi okulda öğrenmüyoruz. Günlük güvenlik uygulamaları kültürümüze o kadar yerleşmiştir ki pek çok kişi bunları sezgisel olarak benimsemektedir. Dijitalleşen dünyada da aynı şey olmalıdır. İlgili bölümde ana hatlarıyla belirtildiği üzere, bu da tüm paydaşların, yani hükümet, kamu ve özel kuruluşlar ve genel olarak dijital vatandaşların eş zamanlı olarak harekete geçmesiyle sağlanabilir.

Özellikle dikkat edilmesi gereken bir diğer husus da dijital okuryazarlıktaki eşitsizliğin sosyo-ekonomik durum ve cinsiyet gibi diğer eşitsizliklerle bağlantılı olmasıdır. Ağ altyapısının eşit olmayan dağılımı bunda rol oynuyor olabilir. Bununla birlikte, bu durum dezavantajlı grupları dijital güvenlik tehditlerine karşı daha savunmasız hale getirmektedir. Bu tür tehditler mağdurdan başka kişilere ve sistemlere de zarar verebileceğinden, bu tür eşitsizliklerin azaltılmaması tüm ekosistemleri daha savunmasız hale getirmektedir.

Aynı şekilde, toplumsal cinsiyet eşitsizliğinin dijital dünyada da şekillendiğinin altı çizilmelidir. Kadınların ve kız çocuklarının dijitali benimsemesi ile erkeklerin ve erkek çocuklarının benimsemesi arasında önemli bir fark vardır. Uluslararası Telekomünikasyon Birliği (ITU) dünyadaki kadınların %50'sinden fazlasının çevrimdışı olduğunu bildirmektedir. Akıllı telefon ve bilgisayar eksikliğinden kaynaklanan erişilebilirlik sorunlarının temelinde, kadınların ve kız çocuklarının internetin sunduğu tüm olanaklardan yararlanamadığı gerçeği de yatmaktadır. Genel olarak erkekler kadınlara kıyasla daha fazla dijital hizmet ve platform kullanmaktadır. Ancak, bu farklılıkların altında yatan nedenleri ortaya koyan veriler, özellikle genç nesiller arasında henüz çok yeni olduğundan, mevcut araştırmalar kapsamlı politika önerileri sunmaya elverişli değildir. Genel eğitimdeki eşitsizlik, kadın dostu kullanıcı tasarımının eksikliği, sosyal platformlarda istismarın çokluğu, kadınlara yönelik kırılğan algı ve sosyal platformların yoğun kullanımı nedeniyle aile üyeleri tarafından eleştirilme riski, katkıda bulunan faktörler arasında sayılmaktadır.

Farklı sosyoekonomik ve coğrafi geçmişlerden gelen kadınlar arasında daha önce bahsedilen faktörlerin katkı düzeylerini belirlemek için kapsamlı veriye dayalı araştırmalar şiddetle tavsiye edilmektedir, böylece gerekli politikalar özel bir şekilde uygulanabilecektir.



Dezenformasyon için:

Dezenformasyon ve onun yıkıcı etkileriyle mücadele etmek isteyen hükümetler için temel mesele, bir yandan dezenformasyonu önlemeye çalışmak, diğer yandan da toplumların dezenformasyona karşı daha dirençli olmalarını sağlayacak çözümler üretmek olarak tanımlanabilir. Yalan haber ve dezenformasyonla mücadelede demokratik ülkelerin benimsediği yaklaşım yol göstericidir. Bu ülkelerde dezenformasyon veya yalan haber kaynaklarına yönelik cezai yaptırımlar çok sınırlıdır ve sadece aşırı (terör) vakalar için geçerlidir. Öte yandan haberleri taşıyan platformlara da yükümlülükler getirilmesi tercih edilmiştir. Örneğin, Almanya'nın NetZ yasasında, platformların 24 saat içinde açıkça yalan haberleri kaldırma yükümlülüğü vardır. Aynı şekilde şikayet durumunda da bir haftalık süreleri vardır. Bu yükümlülüğe uymadıkları takdirde idari para cezaları öngörülmektedir. Erişim kısıtlaması gibi önlemler de bulunmaktadır. Fransa'da yalan haberlere yönelik yaptırımlar sadece seçim dönemlerinde yürürlüğe girmektedir. Seçimlerden 3 ay önce başlayan bu kısıtlamalar doğrultusunda platformlara sorumluluklar getirilmektedir.

Benzer bir yaklaşım, dezenformasyonla mücadelede Avrupa çapında kural koyucu olarak hareket eden Avrupa Komisyonu tarafından da benimsenmektedir. Komisyon'un girişimleri sonucunda büyük dijital platformlar, bu alandaki öz denetim ilkelerini belirleyen "Dezenformasyona İlişkin Uygulama Kuralları (Code of Practice on Disinformation) adlı mutabakat zaptına taraf olmuştur. Ayrıca bu yıl Avrupa Parlamentosu tarafından onaylanan "Dijital Hizmetler Yasası" ile de dezenformasyonla mücadele adına büyük dijital platformlara getirilen sorumluluklar tüm AB ülkeleri düzeyinde geçerli hale gelmiştir. Komisyon bu sorumlulukların denetleyicisi ve gerektiğinde yaptırım uygulayıcı makamı haline gelmiştir.

Bilgi ekosisteminin güçlendirilmesi, Batı demokrasilerinde dezenformasyonla mücadele için kamu düzeyinde alınan tedbirlerin bir diğer ayağını oluşturmaktadır. Bu çerçevede dijital okuryazarlığın güçlendirilmesi, "doğrulama yapan kişilerin (fact checker)" desteklenmesi ve yalan haberlerin tespit edilmesine yönelik çalışmaların yapılması, medyada çoğulculuğun sağlanması ve ifade özgürlüğünün korunması gibi hedefler ön plana çıkmaktadır. Örneğin İsveç ve Finlandiya gibi ülkelerde dijital okuryazarlık konusu büyük önem taşıyan siyasi bir hedef haline getirilmiştir. Finlandiya'da medya okuryazarlığının geliştirilmesi için bir müfredat oluşturulmuş, İsveç'te ise Temmuz 2018'den itibaren "dijital beceriler" teması okullarda zorunlu ders olarak okutulmaya başlanmıştır.

Sonuç olarak, bilgi ekosistemini korumak için yeni kurallara ve mekanizmalara ihtiyaç olduğu artık açıktır. Bu bağlamda yasa koyucunun da bir tercih yapması gerekmektedir. Nitekim yalan haberle mücadelede demokratik ülkeler ile otoriter sistemler arasında net bir ayrım ortaya çıkmıştır. Otoriter sistemlerde yasalar, kamunun ön planda olduğu, zorlayıcı ve polislin hakim olduğu,

basın ve ifade özgürlüğüne zarar veren tedbirlere ağırlık verirken, demokratik ülkeler ise tam tersine devletin yol göstericiliği ilkesine dayanmakta ve bilginin bu şekilde manipüle edilmesine esasen karşı çıkmaktadır. Sivil toplumun, gazetecilerin, doğrulama yapan kişilerin ve platformların daha fazla sorumluluk taşıdığı çözümleri benimsemişlerdir. Bu kritik tercih, demokrasilerin özünde yer alan toplumsal sözleşmedeki güvenlik ve özgürlük dengesini korumak için yapılmıştır.

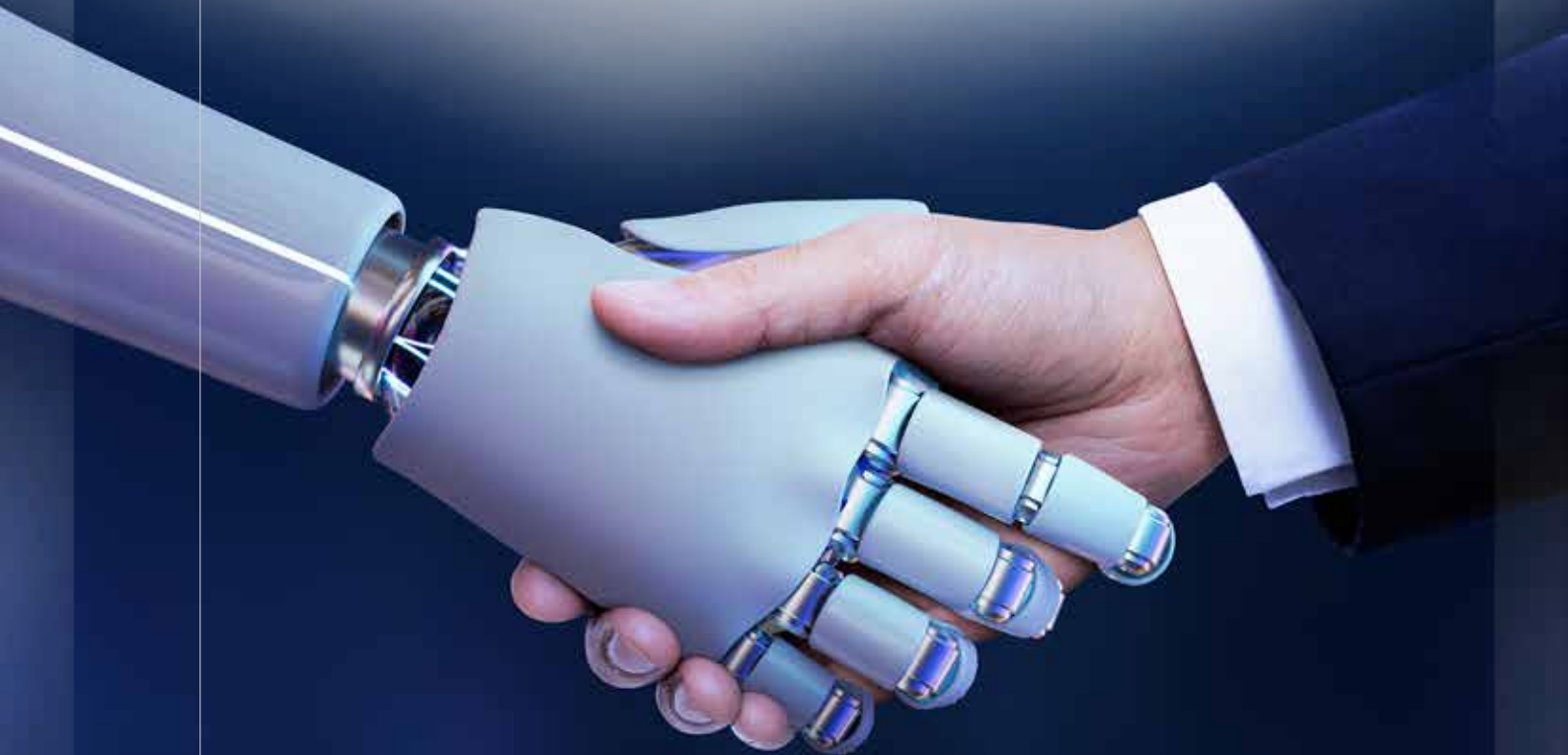
Politika önerilerimiz özünde, dezenformasyonun kriminalize edilmesinin gerçekçi ya da arzu edilen bir çözüm olmadığına dair temel inanca dayanmaktadır. Terör propagandası ve çocuk istismarı gibi halihazırda suç sayılan yasadışı içerikleri dezenformasyonla bir tutmak, ifade özgürlüğüne yönelik siyasi amaçlı sınırlamalara kapı açmaktadır. Hangi içeriğin yalan olduğunu, ulusal güvenlik için tehlikeli olduğunu, kamu düzenini ve genel sağlığı bozacak şekilde panik yaratmak amacıyla yayıldığını belirleme yetkisi, gerçeğe ulaşmanın bilimsel ve rasyonel yöntemlerini siyasileştirmek için kullanılabilir. Bu da, siyasi ve hukuki otoritelerin yalnızca neyin doğru neyin yalan olduğunu belirlemekle kalmayıp, aynı zamanda (yanlış) bilgiyi yayınlayanlara kasıt atfetmesi nedeniyle devletin aşırı müdahalesi anlamına gelir. Dahası, daha önce de belirtildiği gibi, insanları çevrimiçi katılımdan caydırmak dijital kamusal alanı daha da daraltarak dezenformatif aktörlerin ulaşmak istediği "siyasetten geri çekilmeyi" dolaylı olarak güçlendirir. Bu nedenle, sorunun kısıtlama ve yasaklar yerine yapıcı politikalarla çözülebilmesi için dezenformasyonun yasal değil politik bir tanımı olmalıdır.

Son olarak, sorunun semptomlarını hedef alan çözümlere ek olarak, dezenformasyonu etkili kılan nedenleri ele alan daha genel önlemler alınmalıdır. Bu noktada, bu raporun başlangıç noktasına geri dönüyoruz; eleştirel düşünme yoluyla dijital okuryazarlık, ister doğru ister dezenformatif olsun, tüm çevrimiçi bilgilere karşı bilinç oluşturma anahtarıdır⁴⁶.

46 Friedersdorf, Conor. "How 'Big Disinformation' Can Overcome Its Skeptics." The Atlantic, Nisan 21, 2022. <https://www.theatlantic.com/ideas/archive/2022/04/anti-disinformation-laws-social-media/629612/>.

Nesnel gerçekleri duygusal tepkileri hedefleyen içerikten ayırmak, tartışmacı akıl yürütmeyi analiz etmek ve bilgiyi değerlendirirken kanıt aramak, hem dijital içeriğe hem de genel olarak bilgiye yanıt vermek için temel becerilerdir. Bu aynı zamanda siyasi/hukuki yanıtların kaçınılmaz olarak karar verici makamın kültürel ve değer yargılarına dayandığı için uygunsuz olmasının bir başka nedenidir. Dijital okuryazarlık ve eleştirel düşünceye odaklanarak, dezenformasyona karşı en savunmasız olduğumu gördüğümüz genç nesiller, yalan bilginin yaygın olduğu bir dünyaya daha iyi yanıt verebilecek şekilde eğitilebilir. Devlet bu tür bir eğitim için ana kanal olsa da, sivil toplum ve platformlar da bu konuda farkındalık yaratmaya odaklanmalıdır.

Sonuçta, şok edici bilgilere verilen doğal duygusal tepki ve bundan kaynaklanan marjinal içerik yayınlamaya yönelik finansal teşvik, dezenformasyonun üstesinden gelmeyi nihai olarak zorlaştırmaktadır. Belki de bazı hükümetlerin kısıtlama ve suç haline getirme yolunu seçmelerinin bir nedeni de budur. Ancak bu gibi tepeden inme tepkiler en iyi ihtimalle dezenformasyonun semptomlarını hedef alabilir. Dezenformasyonun gerçekten ortadan kalkması için, kitlelerin talep özellikleri ve bilgi tedarikçilerinin politika çizgisinin sol kenarında kalmaya yönelik ekonomik teşvikleri değişmelidir. Dijital okuryazarlığın geliştirilmesinin talep tarafında oynayacağı bir rol vardır, ancak sorunun tam çözümü için özellikle dezenformasyonu hedefleyen önlemlerin haricinde başka politika önlemlerine ihtiyaç vardır. Türkiye'de yeni kabul edilen dezenformasyon yasasının uygulanması bağlamında bu genel çerçeveyi hatırlamak faydalı olacaktır.





01 // 2023

SİBER POLİTİKALAR & DEMOKRASİ 2023/01/TR

TÜRKİYE'DE DİJİTAL OKURYAZARLIK: EKONOMİK, GÜVENLİK VE DEZENFORMATİF HUSUSLARA İLİŞKİN PERSPEKTİFLER



Ekonomi ve Dış Politika
Araştırmalar Merkezi

edam

Hare sokak No.16 Akatlar / İstanbul

T. +90 (212) 352 18 54
F. +90 (212) 351 54 65

info@edam.org.tr

   // edam.org