

GÖZETLENEN TOPLUM: SİBER GÜVENLİK SÖYLEMLERİNDE GÜVEN, KORKU VE TEKİNSİZLİK

Aynur TEKKE*

Atfı: Tekke, Aynur. "Gözetlenen Toplum: Siber Güvenlik Söylemlerinde Güven, Korku ve Tekinsizlik", *Sosyologca*, Sayı 30 (2025), s. 167-184.

ÖZ: Dijitalleşmenin hızla ilerlemesiyle güven, teknik bir olgu olmaktan çıkarak toplumsal ve duygusal bir deneyime dönüşmüştür. Bireyler dijital platformlarda güvenliklerini sağlamak için çeşitli önlemler alırken aynı zamanda gözetim, veri denetimi ve dijital tehditler aracılığıyla korku ve tekinsizlik duygularını da deneyimlemektedir. Bu çalışma, dijital güvenlik söylemlerinin bireylerde güven, korku ve tekinsizlik duygularını nasıl şekillendirdiğini sosyolojik bir perspektiften incelemektedir. 2015-2025 yılları arasında yayımlanmış akademik çalışmalar temel alınarak yapılan derlemede Giddens, Bauman, Lyon ve Zuboff'un yaklaşımlarından yararlanılmıştır. Bulgular, dijital güvenlik söylemlerinin yalnızca güven duygusunu artırmakla kalmayıp bireylerde kolektif korku, tekinsizlik ve paranoyak davranışları da güçlendirdiğini ortaya koymuştur. Sonuç olarak, siber güvenliğin teknik bir alanın ötesine geçerek dijital çağın duygusal ve kültürel bir meselesine dönüştüğü vurgulanmıştır.

Anahtar Kelimeler: Dijitalleşme, Dijital Güvenlik, Toplumsal Korku, Tekinsizlik, Gözetim Kültürü

The Surveilled Society: Trust, Fear, and Uneasiness In Cyber Security Discourses

ABSTRACT: With the rapid advancement of digitalization, trust has evolved from a technical phenomenon into a social and emotional experience. While individuals take various measures to ensure their security on digital platforms, they also experience feelings of fear and unease through surveillance, data control, and digital threats. This study examines, from a sociological perspective, how digital security discourses shape feelings of trust, fear, and unease in individuals. The compilation, based on academic studies published between 2015 and 2025, draws on the approaches of Giddens, Bauman, Lyon, and Zuboff. The findings reveal that digital security discourses not only increase feelings of trust but also reinforce collective fear, unease, and paranoid behavior in individuals. Consequently, it is emphasized that cybersecurity has transcended the realm of a technical field and has become an emotional and cultural issue of the digital age.

Keywords: Digitalization, Digital Security, Social Fear, Uneasiness, Surveillance Culture

Makale Türü : Araştırma Makalesi

Geliş Tarihi : 07.09.2025

Kabul Tarihi : 17.10.2025

* Bilim Uzmanı, aynurtekke61@gmail.com, ORCID: 0000-0002-5280-3169.

Giriş

Dijitalleşmenin hızla ilerlemesiyle beraber, bireyler ve toplumlar siber güvenlik söylemlerinin etkisi altında yeni bir güvenlik paradigmasıyla karşı karşıya kalmaktadır. Bu yeni paradigmada güvenlik sadece teknik bir mesele olarak değerlendirilememektedir. Bunun yanında toplumsal ve duygusal bir deneyime de dönüştüğü görülmektedir. Siber güvenlik uygulamaları, bireylerin dijital ortamda korunmasını hedeflerken öte yandan güven, korku ve tekinsizlik gibi duygusal durumları da şekillendirmektedir.¹

Güven, modern toplumların temel yapı taşlarından biri olarak kabul edilmektedir. Anthony Giddens,² güveni, bireylerin soyut sistemlere güven duymalarını sağlayan bir mekanizma olarak tanımlamaktadır. Bu güvenin, bireylerin günlük yaşamlarını düzenleyen bir temel oluşturduğunu belirtmektedir. Fakat dijitalleşme ile beraber güvenin doğası değişmiş ve bireyler, dijital platformlarda güvenliklerini sağlamak adına çeşitli önlemler almak zorunda kalmıştır. Bu durum, güvenin yeniden inşa edilmesi gerektiğini ve bu sürecinde toplumsal dinamiklerle şekillendiğini göstermektedir.

Bu bağlamda çalışma, dijital güvenlik söylemlerinin bireylerde güven, korku ve tekinsizlik duygularını nasıl şekillendirdiğini anlamayı amaçlamaktadır. Çalışmanın temel problemi, siber güvenlik söylemlerinin bireylerde güven duygusunu artırmak yerine korku ve tekinsizlik duygularını pekiştirip pekiştirmediği hususlarına odaklanmaktadır. Bu sorunsal, dijital çağın güvenlik algısındaki dönüşümü anlamlandırmak açısından önemlidir. Bu problemten hareketle çalışma şu alt sorulara yanıt aramaktadır:

- Dijital güvenlik söylemleri bireylerin günlük yaşamlarında nasıl bir korku ve tehdit algısı oluşturmaktadır?
- Siber gözetim ve veri denetimi uygulamaları, bireylerin toplumsal ilişkilerini ve dijital kimliklerini nasıl etkilemektedir?
- Mevcut literatürde dijital güvenlik ve tekinsizlik olgusu hangi sosyolojik çerçevelerle ele alınmıştır?
- Dijital güvenlik söylemleri bireylerin duygusal ve davranışsal tepkilerini nasıl yönlendirmektedir?

İlgili problem cümleleri, dijital güvenlik olgusunun sadece teknolojik değil aynı zamanda toplumsal bir mesele olarak da ele alınması gerektiğini göstermektedir. Bauman'ın³ (2007) "akışkan korku" kavramsallaştırması, dijital dünyada var olan belirsizliğin sürekliliğini vurgularken; Lyon,⁴ gözetim toplumunun bireylerde kalıcı bir tehdit hissi oluşturduğunu belirtmektedir. Zuboff⁵ ise dijital platformların ekonomik çıkarlar doğrultusunda gözetimi kurumsallaştırarak "gözetim kapitalizmi" düzeni oluşturduğunu ifade etmektedir. Tüm bu çalışmalar, dijital güvenlik söylemlerinin bireylerde güven kadar korku ve tekinsizlik duygularını da beslediğini göstermektedir.

Bu çalışma, derleme (literatür incelemesi) yöntemiyle yürütülmüştür. 2015-2025 yılları arasında yayımlanmış akademik makaleler, kitaplar ve raporlar sistematik biçimde taranmıştır. Scopus, Web of Science, MDPI ve Google Scholar gibi veri tabanlarında yapılan taramalar ile ulaşılan çalışmalar üç ana tema etrafında değerlendirilmiştir: güven ve dijital

¹ Volosevici, Dana. "Surveillance as a Socio-Technical System: Behavioral and Psychological Impacts", Social Sciences, 13(7), (2025): 614.

² Giddens, Anthony. The Consequences of Modernity. Stanford University Press, 1990.

³ Bauman, Zygmunt. Liquid Times: Living in an Age of Uncertainty. Polity Press, 2007.

⁴ Lyon, David. State, Digital Surveillance, and Society – A Scoping Review. Dinasti Publishing, 2023.

⁵ Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.

güvenlik, korku ve tekinsizlik kültürü, toplumsal ve duygusal etkiler. Analiz sürecinde özellikle Giddens, Bauman, Lyon ve Zuboff'un sosyolojik yaklaşımlarından yararlanılmış, dijital güvenlik söylemlerinin bireysel ve toplumsal düzeydeki yansımaları da karşılaştırmalı biçimde tartışılmıştır.

Teorik Çerçeve: Güven, Korku ve Tekinsizliğin Sosyolojisi

Güven, modern toplumların sürekliliğini sağlayan temel bir toplumsal olgu olarak bireylerin kurumlara ve birbirlerine yönelik kurdukları ilişkilerin merkezinde yer almaktadır. Giddens,⁶ güveni modern toplumların soyut sistemler üzerindeki bağımlılığının bir sonucu olarak açıklamakta ve bu noktada dijital teknolojilerin ürettiği karmaşık sistemlerin, bireylerin gündelik yaşamlarında yeni bir güven biçimi oluşturduğunu ileri sürmektedir. Ancak bu güven, çoğunlukla bilinmezlik olgusuyla iç içe geçerek hem ontolojik bir güvensizlik hem de tekinsizlik duygusunu tetiklemektedir.

Siber güvenlik, bu noktada sadece teknik bir koruma alanını ifade etmemektedir. Bunun yanında güven, korku ve tekinsizlik gibi duyguların üretildiği bir sosyo-duygusal alana dönüşmektedir. Beck'in⁷ *Risk Toplumu* yaklaşımında belirtildiği gibi modern toplum artık doğal değil üretilmiş risklerle karşı karşıyadır. Bu risklerin önemli bir bölümü teknolojik altyapılardan kaynaklanmaktadır. Dijital dünyada yaşanan güvenlik ihlalleri, kimlik hırsızlıkları, veri sızıntıları ve gözetim pratikleri bireylerin güvenlik algısını kökten değiştirmektedir. Söz konusu durum, bireylerde "dijital korku" olarak tanımlanabilecek bir duygusal atmosfer yaratmakta ve güvenliğe dair söylemlerin toplumsal düzeyde yeniden üretilmesini sağlamaktadır.⁸

Tekinsizlik, Freud'un⁹ klasik tanımıyla "tanıdık olanın yabancılaşması"dır. Dijital toplum bağlamında ise bu duygu, bireylerin sürekli olarak izlendikleri, izlendiklerini bildikleri ama bunu denetleyemedikleri bir ortamda var olmalarından kaynaklanmaktadır. Siber güvenlik teknolojileri görünürde güvenliği sağlarken diğer yandan bireyin özel alanına nüfuz eden bir denetim aracına dönüşmektedir.¹⁰ Bu sebeple dijital güvenlik deneyimi, hem koruyucu hem de tehdit edici diyalektik bir yapı sergilemektedir. Birey kendini güvende hissederken aynı zamanda gözetim altında olmanın oluşturduğu tekinsizlik duygusuyla yüzleşmektedir.

Duygu sosyolojisi literatürü, bu tür duygusal tecrübelerin bireysel olmasının yanında kolektif olduğunu da vurgulamaktadır. Ahmed,¹¹ duyguların toplumsal ilişkiler ağında dolaşıma girerek "duygusal atmosferler" yarattığını ileri sürmektedir. Bu noktada siber güvenlik söylemleri bilgi güvenliği veya veri koruma politikaları ile ilişkili olmasının yanında güvenliğe ilişkin duygusal normlarla da alakalıdır. Toplum, korku ve güven duyguları aracılığıyla düzenlenmektedir. Bireyler ise bu duygulara uyum sağlayarak dijital dünyada "güvenlik öznesi" haline gelmektedir.¹²

Güvenin Modern Toplumdaki Rolü

Güven, modern toplumun sürekliliğini sağlayan en temel toplumsal mekanizmalardan biridir. Giddens'a¹³ göre güven, modernliğin soyut sistemlere dayalı yapısında bireylerin belirsizlikle başa çıkabilmesini mümkün kılan bir ontolojik güven biçimidir. Geleneksel

⁶ Giddens, *The Consequences of Modernity*.

⁷ Beck, Ulrich. *Risk Society: Towards a New Modernity*. Sage Publications, 1992.

⁸ Bauman, Zygmunt ve Lyon, David. *Liquid Surveillance: A Conversation*. Polity Press, 2013.

⁹ Freud, Sigmund. *The Uncanny*. Penguin Books, 2003.

¹⁰ Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power".

¹¹ Ahmed, Sara. *The Cultural Politics of Emotion*. Edinburgh University Press, 2014.

¹² Lupton, Deborah. *The Quantified Self: A Sociology of Self-Tracking*. Polity Press, 2021.

¹³ Giddens, *The Consequences of Modernity*.

toplumlarda güven, yüz yüze ilişkiler ve doğrudan deneyimler üzerinden sağlanırken, modern toplumlarda bu güven, teknik uzmanlık, soyut sistemler ve kurumlar vasıtasıyla sürdürülmektedir. İlgili durum, bireyin kendi deneyimiyle doğrulayamadığı fakat inanmak zorunda olduğu güven biçimini ortaya çıkarmıştır.

Dijitalleşme süreçleriyle beraber bireylerin yaşamındaki güven biçimi yeni bir boyut kazanmıştır. Fakat güven, sadece devlet kurumlarına ya da ekonomik yapılara değil bunun yanında algoritmalara, dijital platformlara ve görünmez teknik altyapılara da yönelmiştir.¹⁴ Bireyler çevrimiçi platformlarda sürekli olarak kişisel verilerini paylaşmakta, kimlik doğrulama sistemlerine, bankacılık uygulamalarına ve yapay zeka destekli karar süreçlerine güven duymak zorunda kalmaktadır. Söz konusu güven ilişkisi, modern toplumun dijital uzantısı olan veri toplumunda var olmanın ön koşulu haline gelmiştir.¹⁵ Fakat bu güven, tek yönlü ve istikrarlı bir olgu değildir. Dijital alt yapılara duyulan güven aynı anda hem bağımlılık hem de kırılganlık hissedilmesine yol açmaktadır. Bir yandan bireyler dijital sistemler olmadan yaşamlarını sürdüremez hale gelmekteyken diğer yandan bu sistemlerin kontrolsüz hale gelen doğası onları belirsizlik ve korku ile karşı karşıya bırakmaktadır. Bu sebeple güven, modern toplumda “kontrollü bir risk alma davranışı” olarak da tanımlanabilmektedir.¹⁶ Beck’in risk toplumu teorisi, bireylerin modernleşme süreçleriyle beraber üretilmiş risklerle bir arada yaşadığını dolayısıyla güvenin artık doğallıktan ziyade bir zorunlu strateji haline geldiğini vurgulamaktadır.

Siber güvenlik, stratejik güvenin en belirgin görünümlerinden birini teşkil etmektedir. Bireyler güvenlik uygulamalarına, parola sistemlerine, antivirüslere ya da devletin dijital koruma mekanizmalarına duydukları güven aracılığıyla riskleri yönetmeye çalışmaktadır. Fakat bu güven çoğu zaman “bilinmez bir alana teslimiyet” anlamına gelir. Çünkü birey, teknik sistemlerin işleyişini tam anlamıyla denetleyemediği bir dünyaya karşı güven hissetmek zorunda kalmaktadır. Bu durum da Giddens’in¹⁷ belirttiği ontolojik güven kavramını dijital çağ özelinde aldığı kırılgan görünümünden biri olarak değerlendirilebilmektedir. Bu noktada siber güvenlik ile dijital güvenlik arasındaki ayrımın netleştirilmesi önem arz etmektedir. Siber güvenlik, temelde ağların, kritik altyapıların, ulusal bilgi sistemlerinin ve çevrim içi ağ bütünlüğünün korunmasını kapsayan teknik ve stratejik bir alandır.¹⁸ Kavram büyük oranda devlet politikaları, ulusal tehdit algıları ve kurumsal güvenlik yapıları ile ilişkilidir. Buna karşılık dijital güvenlik ise bireyin dijital ortamdaki varlığını korumaya odaklanmaktadır. Mahremiyet ihlalleri, kimlik hırsızlığı, kişisel veri sızıntıları, algoritmik manipülasyon, çevrim içi taciz ve gözetim teknolojileri bireysel odakta tecrübe edilen güvenlik risklerini içermektedir.¹⁹ Bu çerçevede modern birey, dijital araçlar aracılığıyla sürekli bir güvenlik arayışı içine girmenin yanında güveni mümkün hale getiren alt yapıların karşılıklılığı karşısında güçsüzlük, belirsizlik ve kontrol kaybını da tecrübe etmektedir. Dolayısıyla dijital çağda güven, sadece teknik altyapıların değil bunun yanında mahremiyet endişelerinin, gözetim pratiklerinin ve algoritmik risk algısının şekillendirdiği duygusal bir sürecin odağına yerleşmektedir. Söz konusu çelişkili durum, siber güvenlik söylemlerinin hem teknik hem de ideolojik ve duygusal bir zeminde kurulduğunu göstermektedir.

¹⁴ Lupton, *The Quantified Self: A Sociology of Self-Tracking*.

¹⁵ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”.

¹⁶ Beck, *Risk Society: Towards a New Modernity*.

¹⁷ Giddens, *The Consequences of Modernity*.

¹⁸ Singer, Allan, Singer, P. W., *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.

¹⁹ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, ss. 201-206.

Korku ve Belirsizlik: Bauman'ın "Korku Kültürü" Yaklaşımı

Modern toplumda korku bireysel bir duygu olmasının yanı sıra politik, ekonomik ve kültürel alanlarda düzenleyici bir güç olarak rol üstlenmektedir. Beck'in²⁰ belirttiği gibi risk toplumu "gelecekteki olası felaketlerin bugünü belirlediği" bir yapıya sahiptir. Bu noktada korku, modernliğin en görünür olduğu duygulardan biri haline gelmiştir. Korkunun üretimi ve yönetimi, günümüzde özellikle dijital güvenlik politikalarının ve medya söylemlerinin odak noktasında yer almaktadır.²¹ Dijital çağda korku, bilgi akışının hızına ve medyanın sürekli alarm durumuna göre yeniden üretilmektedir. Siber saldırılar, veri sızıntıları, yapay zeka tehditleri ve dezenformasyon gibi olgular yalnızca teknik problemler değil bunun yanında duygusal mobilizasyon araçlarıdır. Bu tehditlerin sürekli olarak vurgulanması, bireylerin kendilerini potansiyel mağdurlar olarak hissetmelerine ve güvenlik teknolojilerine, devlet politikalarına ya da özel platformlara daha fazla bağımlı hale gelmelerine yol açmaktadır.²² Böylelikle korku, siber güvenliğin toplumsal kabulünü sağlayan duygusal bir ekonomi üretmektedir. Söz konusu duygu ekonomisi, bireyleri pasifleştirmeye değil, belirli davranış kalıplarına yönelmeye teşvik etmektedir. Lyon,²³ gözetim toplumunda korkunun hem bir baskı mekanizması hem de rıza üretiminde işlevsel bir araç olduğunu belirtmektedir. Bireyler güvenli hissetmek adına kişisel verilerini paylaşmakta, konumlarını açmakta, çevrim içi etkinliklerini izlenmeye açmaktadır. Bu süreçte korku, bir tür güvenlik alışkanlığına dönüşmekte, bireyler korkularını yönetmek adına gözetlenmeyi gönüllü olarak kabul etmektedir.²⁴

Duygu sosyolojisi açısından değerlendirildiğinde bu tür korkular bireysel olmaktan çok kolektif nitelik taşımaktadır. Ahmed'in²⁵ *duyguların dolaşımı* kavramı, dijital ortamlarda korkunun toplumsal olarak nasıl yayıldığını anlamak açısından açıklayıcıdır. Korku, medya aracılığıyla dolaşmakta, politik söylemlerle pekiştirilmekte ve gündelik dijital etkileşimlerde içselleştirilmektedir. Böylelikle korku hem bireysel davranışları hem de toplumsal normları biçimlendiren bir duygusal atmosfer oluşturmaktadır. Siber güvenlik söylemleri, bu atmosferi sürekli olarak canlı tutmaktadır. Her yeni veri ihlali, yapay zeka tehdidi veya kimlik hırsızlığı vakası, güvenliğe olan bağımlılığı pekiştirmektedir. Bu süreç içinde korku, bir tür duygusal sermayeye dönüşmektedir. Devletler, teknoloji şirketleri ve medya kuruluşları bu duygusal sermayeyi yönetmekte, yeniden üretmekte ve yönlendirmektedir.²⁶ Dolayısıyla dijital çağın korku dinamikleri psikolojik bir konu olmasının yanında iktidarın duygusal bir stratejisi olarak karşımıza çıkmaktadır.

Tekinsizlik (Unheimlich) Kavramının Dijital Dönüşümü

Tekinsizlik, Freud'un²⁷ çalışmasında "tanıdık olanın yabancılaşması" şeklinde tanımladığı bir duygudur. Başka bir ifadeyle yabancılaşmış tanıdıklığın bireyde oluşturduğu huzursuz duygu hâli, belirsizliğin taşıdığı ürkütücü etkidir. Dijital gözetim bağlamında bu duygu, bireyin bilinen kimlik unsurlarıyla (veri, kimlik, özel alan) kurulan etkileşimin sürekli izlenme ve denetim koşullarında dönüşmesiyle yeniden üretilmektedir. Siber güvenlik teknolojileri, gözetim uygulamalarıyla beraber bireylerin güvende olma beklentisini karşılamaya

²⁰ Beck, Risk Society: Towards a New Modernity, ss. 21-24.

²¹ Furedi, Frank. How Fear Works: Culture of Fear in the Twenty-First Century. Bloomsbury, 2018, ss. 11-14.

²² Massumi, Brian. The Politics of Affect. Polity Press, 2015, ss. 6-8.

²³ Lyon, David. The Culture of Surveillance: Watching as a Way of Life. Polity Press, 2018.

²⁴ Bauman ve Lyon, Liquid Surveillance: A Conversation, ss. 57-60.

²⁵ Ahmed, The Cultural Politics of Emotion, ss. 11-14.

²⁶ Massumi, The Politics of Affect, ss. 14-17.

²⁷ Freud, The Uncanny, ss. 237-238.

çabalarken bir yandan da bu teknolojilerin öznelliğe nüfuz etmesi, bireyde sürekli bir “ne olduğunun tam olarak farkında olmama” haline yol açmaktadır. Bu da klasik anlamıyla tekinsizlik duygusunu yeniden çağırmaktadır.

Gözetim pratikleri, toplumsal ilişkileri ve kamusal alan deneyimini sınırlarken tekinsizlik duygusunu derinleştirmektedir. Lyon’un analizlerinde gözetim hem görünür izleme hem de sosyal sınıflandırma ve profil oluşturma süreçleriyle yaşam süreçlerinin yeniden düzenlenmesi anlamına gelmektedir.²⁸ Bu tür sınıflandırma süreçleri, bireylerin davranışlarının -farkında olsun olmasın- gözetim aygıtları tarafından kodlanması üzerinden yürümektedir. Böylece birey, gözetim sisteminin kendisinde taşıdığı kategoriye göre değerlendirilen ve sınırlanan bir nesne haline gelmekte, bu da güvenin aşındığı bir özne konumu doğurmaktadır.

Dijital gözetim teknolojilerinin yaygın hale gelmesiyle birlikte tekinsizlik sadece psikolojik duygu durumuyla sınırlandırılmamaktadır. Bunun yanında davranışsal ve toplumsal düzenlemelere dönüştüğü görülmektedir. Gözetim aygıtlarının sürekli görünürlüğü ve akışkanlığı (surveillance creep) bireylerde bir “varsayılan izlenmişlik” hissi oluşturmaktadır.²⁹ Söz konusu his, bireyin kendisini sürekli olarak gözetleme sistemlerine uyumlama refleksiyle davranmasına ve ifade, iletişim ve etkileşim biçimlerinde oto-sansür uygulamasına yol açmaktadır. Tekinsizlik, bu bağlamda bireyin içsel dünyasını etkilemesinin yanında kamusal ve politik düzeyde de etkili bir stratejik araç rolü üstlenmektedir. Gözetim uygulamalarının meşruiyeti sıklıkla tehdit algısı söylemlerine dayanmaktadır. Güvenlik tehditleri dilinin sürekli olarak vurgulanması, belirli risklerin olağanüstü önlemlerle de ele alınmasını meşrulaştırmaktadır. Böylelikle söz konusu önlemlere toplumsal rıza üretilmesini kolaylaştırmaktadır.³⁰ Bu iklimde bireyler, kendilerini koruma kaygısıyla gözetim sistemlerine razı olma eğilimi göstermektedir. Dijital platformların ve devletin koruma vaatleri, kullanıcıların mahremiyet fedakarlıklarını normalleştirir ve ticari/kurumsal gözetimi görünmez kılar.³¹ Bu şekilde tekinsizlik duygusu bir iktidar teknolojisi olarak işlev kazanmaktadır. Gözetim pratikleri yalnızca dışsal bir kontrol mekanizması olmayıp buna ek olarak bireyin davranışlarını, güvenlik tercihlerini ve itaat/uyum eğilimlerini şekillendiren bir içselleştirme sürecine dönüşmektedir.³²

Siber Güvenlik Söyleminin Toplumsal İnşası

Dijital çağda güven, korku ve tekinsizlik duygularının toplumsal alanda inşa edilmesi sadece bireylerin duygusal dünyasını etkileyen süreçler değildir. İlgili duygular aynı zamanda kamu söylemleri, medya temsilleri ve iktidar stratejileri aracılığıyla yeniden üretilmektedir. Bu bağlamda siber güvenlik söyleminin toplumsal inşası, teknik güvenlik anlatıları ile duygusal rejimlerin birbiriyle nasıl iç içe geçtiğini gösteren bir analiz alanıdır. Siber güvenlik söylemi, devlet kurumları, medya kuruluşları, teknoloji şirketleri ve uzman aktörler arasında kurulan bir disiplinlerarası alan üzerinden şekillenmektedir. Bu aktörler, siber tehdidi öncelikli bir güven konusu olarak konumlandırmakta ve kamuoyunda bu tehdide dair bir farkındalık oluşturma sorumluluğu üstlenmektedir.³³ Böylelikle dijital güvenlik bir uzmanlık alanı olarak meşruiyet kazanmaktadır. Bu söylemsel üretim biçimi, uluslararası ilişkiler ve güvenlik çalışmaları kapsamında “güvenlikleştirme (securitization) olarak adlandırılan

²⁸ Lyon, *The Culture of Surveillance: Watching as a Way of Life*.

²⁹ Monahan, Torin. *Surveillance in a Time of Insecurity*. Rutgers University Press, 2010.

³⁰ Wæver, Ole. “Securitization and Desecuritization”, *On Security*. Ed., R. D. Lipschutz (Ed.), (ss. 46–86). Columbia University Press, 1995.

³¹ Lyon, *The Culture of Surveillance: Watching as a Way of Life*.

³² Foucault, Michel. *Security, Territory, Population: Lectures at the Collège de France, 1977–78*. Palgrave Macmillan, 2007.

³³ Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977–78*, ss. 108–110.

sürecin tipik bir örneğini oluşturmaktadır. Söz konusu olgu aslında güvenlik alanına dahil olmayan bir konunun siyasi aktörler tarafından varoluşsal bir tehdit olarak sunulması ve bu söylem vasıtasıyla olağanüstü önlemlerin meşrulaştırılmasıdır.³⁴ Siber tehditlerin medya, devlet ve teknoloji şirketleri tarafından kriz diliyle beraber sunulması da dijital alanın güvenlikleştirilmesi anlamına gelmektedir. Bu çerçevenin toplumsal etkisi, medya ideolojileri üzerinden yansımaktadır. Haberlerde, siber saldırılar ve veri sızıntıları “acil durum” söylemleriyle sunulmaktadır. Her yeni olay, teknik olmayan okurlarda da bir kriz hali algısı oluşturmaktadır. Söz konusu kriz anlatıları, halkın güvenlik algısını tetikleyerek rıza üretiminde etkili olmaktadır.³⁵ Bu içeriklerde kullanılan “siber savaşlar”, “veri ihlali” ya da “hack tehdidi” gibi kavramlar tehdit söylemlerini gündelik dile taşımakta ve bu söylemler aracılığıyla güvenlik adı altında gözetim teknolojilerini doğallaştırmaktadır. Bunun yanı sıra teknoloji şirketleri ve platformlar da bu söylem içinde önemli bir rol oynamaktadır. Şirketler, kullanıcılarına veri koruma, şifreleme, gizlilik modları gibi özellikler sunarak kendilerini koruyucu aktör olarak konumlandırmaktadır.³⁶ Bu tür kampanyalar, kullanıcıların gözetim sistemlerine karşı şüphe barındırmasını sınırlayan bir güven atmosferi üretmektedir. Aynı zamanda bu söylemler, kullanıcıların mahremiyet tercihlerini teknolojik rasyonelitelere (örneğin; “güçlü şifre kullan”, “iki faktörlü doğrulama yap”) indirgemekte, kişisel ve kamusal sorumluluk cephesinde bireyleri konumlandırmaktadır.

Siber Güvenlik Söylemi Nedir?

Siber güvenlik söylemi, dijital çağın güvenlik anlayışının hem teknik hem de toplumsal boyutlarını bir araya getiren çok katmanlı bir söylemdir. Bu söylem, sadece “veri koruma” ya da “tehdit önleme” gibi teknik konularla sınırlı değildir. Aynı zamanda bireylerin, kurumların ve devletlerin dijital güvenlik algılarını şekillendiren kültürel, duygusal ve politik bir anlam dünyası kurgulamaktadır. Bu anlamda siber güvenlik söylemi güven, korku ve tekinsizlik duygularının belirleyici olduğu bir toplumsal düzenleme biçimi olarak değerlendirilebilmektedir.³⁷

Söylem kavramı, Foucault’nun literatüre kazandırdığı bilgi-iktidar ilişkisine dayanan analizlerinde, toplumsal gerçekliğin sadece dil aracılığıyla temsil edilmediğini, bunun yanında söylem aracılığıyla üretilip yönetildiğini vurgulamaktadır.³⁸ Siber güvenlik çerçevesinde söylem, hangi risklerin tehdit olarak tanımlandığını, hangi aktörlerin bu tehditlere karşı koruyucu bir konumda bulunduğunu ve hangi davranış türlerinin güvenli olarak nitelendirildiğini belirleyen bir bilgi rejimi oluşturmaktadır. Bu sebeple siber güvenlik söylemi, güvenlik politikalarının meşrulaştırılmasında ve gözetim pratiklerinin normalleştirilmesinde merkezi bir rol üstlenmektedir.³⁹ Siber güvenlik söyleminin arka planında risk ve tehdit kavramlarının taşıdığı toplumsal anlam yer almaktadır. Beck’in⁴⁰ risk toplumu yaklaşımı, modern toplumların giderek daha fazla üretilmiş belirsizlikler etrafında yapılandığını vurgulamaktadır. Bu perspektiften bakıldığında dijital alanlarda sürekli yeniden tanımlanan tehditler -örneğin; kimlik hırsızlığı, siber savaş, veri sızıntısı- güvenlik söylemini dinamik ve genişleyen bir olguya dönüştürmektedir. Böylece siber güvenlik hem teknik bir koruma pratiği hem de sürekli tehdit altında olma hissiyle yaşayan bireylerin

³⁴ Buzan, Barry, Wæver, Ole ve de Wilde, Jaap de. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998, ss. 24-29.

³⁵ Buzan, Wæver, Wilde, *Security: A New Framework for Analysis*. 1998, ss. 96-99.

³⁶ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, ss. 345-348.

³⁷ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, ss. 343-349.

³⁸ Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977-78*, ss. 108-110.

³⁹ Buzan vd., *Security: A New Framework for Analysis*, ss. 95-99.

⁴⁰ Beck, *Risk Society: Towards a New Modernity*, ss. 21-24.

duygusal düzenini de biçimlendirmektedir.⁴¹ Bu söylemin toplumsal boyutu, bireylerin davranış örüntülerinde ve kültürel temsillerinde açık bir şekilde görülmektedir. “Güvenli bağlantı kur”, “şüpheli bağlantılara tıklama” ya da “kişisel verilerini koru” gibi uyarılar, hem bireysel dikkati hem de devletin güvenlik çağrılarını benimsemeyi öğütleyen normatif söylemlerdir. Bu tür mesajlar, siber güvenlik söylemini gündelik yaşamın duygusal ve davranışsal dokusuna işlemektedir. Böylece birey, güvenlik sistemlerinin pasif bir öznesi değil aktif bir katılımcısı haline gelmektedir.⁴² Dolayısıyla siber güvenlik söylemi teknik bir kavram olmaktan çok daha fazlasını temsil etmektedir. Hem bilgi üretiminin hem de duygusal düzenin bir aracıdır. Güveni, korkuyu ve tekinsizliği aynı anda üretmekte ve yönetmektedir. Bu söylem, dijital toplumun en temel duygusal alt yapılardan biri haline gelmiş, modern iktidar biçimlerinin duygusal meşruiyetini sağlamlaştırmıştır.⁴³

Korku Politikaları: Tehdit Söylemleri ve Kolektif Güvensizlik

Siber güvenlik söyleminin dayandığı temel duygusal olgulardan biri korkudur. Korku, modern toplumlarda sadece bireysel bir duygu değil bunun yanında politik bir araç işlevi görmektedir. Furedi’nin⁴⁴ ifade ettiği gibi, çağdaş toplumlarda korku bir yönetim biçimine dönüşmüştür. Bireylerin belirsizlikler karşısındaki kaygıları, siyasi ve ekonomik aktörler tarafından yönlendirilmekte ve biçimlendirilmektedir. Bu noktada siber tehditler, hem teknik riskler hem de kültürel ve ideolojik inşalar olarak da değerlendirilmelidir.⁴⁵ Korkunun bu şekilde politik hale getirilmesi, kolektif güvensizlik duygusunu sürekli olarak canlı tutmaktadır. Toplumsal düzeyde tehdit algısı, medyada ve siyasal söylemlerde sıkça vurgulanan “siber saldırı”, “veri sızıntısı” veya “dijital sabotaj” gibi temalarla yeniden üretilmektedir. Bu süreç içinde korku, toplumsal dayanışmayı değil aksine bireysel güvenlik arayışını teşvik etmektedir.⁴⁶ Bireyler kendi güvenliklerini sağlamak için veri paylaşımına, gözetim teknolojilerine ve algoritmik izleme sistemlerine gönüllü olarak katılmaktadır. Böylece korku bireysel ve yapısal düzeyde rıza üretiminin bir aracı haline gelmektedir.⁴⁷ Söz konusu durum, tekinsizlik kavramının siber toplumda kazanmış olduğu yeni anlamları da açıklamaktadır. Freud’un⁴⁸ tanımladığı haliyle tekinsizlik, tanıdık olanın bir anda yabancılaşması halidir. Dijital çağda bu durum, gündelik yaşamın sıradan araçlarının - telefonlar, akıllı cihazlar, sosyal medya platformları- birer gözetim nesnesi haline dönüşmesiyle ortaya çıkmaktadır. Birey, kendi verilerinin nerede, kimler tarafından ve hangi amaçlar doğrultusunda kullanıldığını bilmediğinde sürekli bir dijital tedirginlik hâli içinde yaşamaktadır.⁴⁹

Korku politikaları iktidarın sürekliliğini sağlayan bir strateji olarak da işlemektedir. Foucault’nun⁵⁰ biyopolitika kavramında açıkladığı üzere modern iktidar, bireylerin bedenlerini değil yaşam biçimlerini düzenleyerek işlemektedir. Siber güvenlik söylemi de bu biyopolitik yönetim tarzının dijital bir uzantısıdır. Bireyler güvende kalmak için davranışlarını, iletişim biçimlerini ve düşüncelerini denetlemektedir. Buradan hareketle korku, iktidarın meşruiyetini pekiştiren bir duygusal düzenleyiciye dönüştüğü söylenebilmektedir. Dolayısıyla siber güvenlik çağında korku sadece bir duygusal tepki

⁴¹ Monahan, *Surveillance in a Time of Insecurity*, ss. 55-57.

⁴² Lyon, *The Culture of Surveillance: Watching as a Way of Life*, ss. 45-48.

⁴³ Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977-78*, s. 109.

⁴⁴ Furedi, *How Fear Works: Culture of Fear in the Twenty-First Century*, s. 63.

⁴⁵ Beck, *Risk Society: Towards a New Modernity*, s. 81.

⁴⁶ Bauman, Zygmunt. *Liquid Fear*. Polity Press, 2006, s. 21.

⁴⁷ Zuboff, Shoshana. “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, s. 210.

⁴⁸ Freud, *The Uncanny*, s. 148.

⁴⁹ Lyon, *The Culture of Surveillance: Watching as a Way of Life*, s. 71.

⁵⁰ Foucault, Michel. *Security, Territory, Population: Lectures at the Collège de France, 1977-78*, s. 110.

değildir bunun yanında bir siyasal ekonomi unsurudur. Tehdit söylemleri, hem devletler hem de teknoloji şirketleri için yeni kontrol alanları oluşturmaktadır. Kolektif güvensizlik duygusu ise toplumsal düzeyde gözetim sistemlerinin kabulünü kolaylaştırmaktadır. Bireyler, korkularını bastırmak için mahremiyetlerinden fedakarlık etmeye razı olmaktadır. Böylece modern toplum, güvende hissetme uğruna özgürlüğünden feragat eden bir yapıya evrilmiştir.⁵¹

Güvenlik Olarak Gözetim: Dijital Panoptikonun Sosyolojisi

Modern toplumda güvenlik söylemi sadece devletin ya da kurumların üretmiş olduğu bir söylem niteliği taşımamaktadır. Medya ve dijital kültür aracılığıyla gündelik hayatın dokusuna nüfuz eden bir olgu olarak da değerlendirilmesi gerekmektedir. Siber tehditlerin haberlerde, sosyal medya platformlarında ve popüler kültürde sürekli olarak vurgulanması, bireylerin sürekli tehdit altında oldukları algısını pekiştirmektedir.⁵² Söz konusu durum, Beck'in⁵³ risk toplumu kavramıyla açıklanabilir. Risk, artık doğrudan yaşanan bir olgu değil medyatik söylemler aracılığıyla dolaşıma giren sembolik bir gerçektir. Medya, güvenlik politikalarını meşrulaştıran en etkili ideolojik araçlardan biridir. Özellikle dijital güvenlik alanında siber saldırılar ya da veri ihlalleri haberleri olağanüstü hâl duygusunu sürekli olarak canlı tutmaktadır. Bu süreç içinde medya gözetimin kaçınılmaz bir gereklilik olduğunu ima etmekte, bireylerin de güvenlik teknolojilerine rıza göstermesi normalleştirilmektedir.⁵⁴ Bu noktada, Zuboff'un⁵⁵ vurgulamış olduğu gözetim kapitalizmi dinamiği devreye girmektedir. Dijital platformlar, kullanıcı verilerini ekonomik değere dönüştürürken bunu güvenlik söylemiyle meşrulaştırmaktadır.

Sosyal medya platformları, hem bilgi aktaran hem de duygusal yönelimleri şekillendiren yapılar hâline gelmiştir. "Dijital duygulanım ekonomisi" olarak adlandırılan bu süreçte,⁵⁶ korku, endişe ve belirsizlik gibi duygular çevrim içi etkileşimlerin bir parçasına dönüşmektedir. Her siber tehdit haberi, kullanıcıların güvende olma arzusunu tetiklemektedir. Bu ise güvenlik şirketleri, devlet kurumları ve medya arasındaki çıkar ilişkilerini görünmez şekilde güçlendirmektedir.⁵⁷ Bu çerçevede dijital kültür, güvenliğin estetikleştirildiği bir sahneye dönüşmektedir. Film, dizi ve reklamlar; siber saldırı, veri hırsızlığı veya yapay zeka isyanı gibi temalar üzerinden kontrolün kaybı korkusunu yeniden üretmektedir. Böylece birey, hem dijital güvenlik politikalarını hem de gözetim teknolojilerinin kültürel hegemonyasını da içselleştirmektedir.⁵⁸ Dolayısıyla medya ve dijital kültür, siber güvenlik söyleminin yayılımını ve meşruiyetini sağlayan duygusal-ekonomik bir ekosistem oluşturmaktadır. Tehdit söylemleri, haber dilinde dramatize edilmekte, görseller, istatistikler ve aciliyet vurgusu aracılığıyla "güvende kalmak" toplumsal bir norm haline getirilmektedir. Bu süreç içinde birey, korkunun estetik hale getirildiği bir medyatik evren içinde sürekli tetikte olan bir özneye dönüşmektedir. Tekinsiz olan, artık dışsal bir tehdit değil bireyin kendi dijital varlığıyla kurmuş olduğu ilişkide içkinleşmiş bir duygudur.⁵⁹

Gözetlenen Birey: Duygusal ve Kültürel Boyutlar

⁵¹ Bauman ve Lyon, *Liquid Surveillance: A Conversation*, s. 97.

⁵² Altheide, David L. *Terrorism and the Politics of Fear*. Rowman & Littlefield, 2013, s. 16.

⁵³ Beck, *Risk Society: Towards a New Modernity*, s. 97.

⁵⁴ Couldry, Nick ve Hepp, Andreas. *The Mediated Construction of Reality*. Polity Press, 2017, s. 129.

⁵⁵ Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", s. 211.

⁵⁶ Papacharissi, Zizi. *Affective Publics: Sentiment, Technology, and Politics*. Oxford University Press, 2015, s. 127.

⁵⁷ Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Signal, 2013, s. 48.

⁵⁸ Bauman ve Lyon, *Liquid Surveillance: A Conversation*. Polity Press, s. 114.

⁵⁹ Lyon, *The Culture of Surveillance: Watching as a Way of Life*, s. 92.

Dijital çağda gözetim, teknik bir izleme pratiği olmaktan çıkıp bireylerin duygusal ve kültürel yaşamlarının odak noktasına yerleşmiştir. Artık gözetim, bireylerin gündelik davranışlarını, ilişkilerini ve kimlik inşa süreçlerini şekillendiren bir duygusal rejim haline gelmiştir.⁶⁰ Gözetim altında olma hissi, bireyde hem güvenlik beklentisini hem de korku, utanç, huzursuzluk ve tekinsizlik gibi duygusal tepkileri de tetiklemektedir. İlgili duygular, gözetimin kültürel kabulünü kolaylaştırarak bireyin kendi davranışlarını denetlemesine zemin hazırlamaktadır.⁶¹

Foucault'nun,⁶² öznenin yönetimi yaklaşımından hareketle dijital gözetim pratikleri bireylerin dışsal bir baskıyla değil, kendi kendilerini denetleme biçimleriyle işlediği bir düzen üretmektedir. Bu durumda gözetim, bireyin kimliğini şekillendiren bir içsel disipline dönüşmektedir. Artık birey, gözetlenen olmaktan çok kendisini gözetten bir özneye evrilmektedir. Dijital kimlikler, sosyal medya görünürlükleri ve veri temelli profil oluşturma süreçleri bu yeni öz-düzenleme biçimlerinin güncel örneklerini oluşturmaktadır.⁶³ Duygusal düzeyde gözetim bireyin güvenlik algısını da karmaşık bir hale getirmektedir. Ahmed'in⁶⁴ ifade ettiği gibi, duygular toplumsal ilişkiler aracılığıyla dolaşmakta ve politik anlamlar kazanmaktadır. Gözetim altında olma duygusu, bireylerin sadece devlete ya da kuruma değil birbirine karşı da güvensizlik geliştirmesine yol açmaktadır. Böylelikle güven, bir toplumsal bağ değil, risk yönetimi biçimine dönüşmektedir.⁶⁵

Kültürel açıdan gözetim, mahremiyet anlayışını da dönüştürmektedir. Dijital çağın bireyi, mahremiyetini gönüllü biçimde ifşa ederken aynı anda kontrol edilme riskini kabullenmektedir. Söz konusu durum, gözetim kapitalizminin duygusal ekonomisini oluşturmakta, bireyler aidiyet ve görünürlük duygusu uğruna veri üretmekte ve paylaşmaktadır.⁶⁶ Böylelikle gözetim, hem bir güvenlik pratiği hem de bir kimlik performansına dönüşmektedir. Gözetim çağında bireyin duygusal dünyasıyla kültürel kimliği birbirine içkin bir hale gelmektedir. Güvende olma isteği, gözetlenmeyi meşrulaştıran bir duyguya; görünür olma arzusu ise mahremiyetin çözülmesine zemin hazırlamaktadır. Bu dikotomik yapı, tekinsizlik duygusunu sürekli canlı tutmaktadır. Birey ne tamamen özgürdür ne de tamamen güvendedir. Dijital toplumun yeni öznesi, güvenlik ve özgürlük arasındaki belirsizlikte var olan gözetlenen bireydir.⁶⁷ Örneğin, Çin'in Sosyal Kredi Sistemi, vatandaşların davranışlarını izleyen, gözlemleyen ve puanlayan bir mekanizma olarak toplumsal kontrolün yeni bir görünümünü temsil etmektedir. Bu sistem, yüz tanıma kameraları ve büyük veri analizleri gibi teknolojiler aracılığıyla bireylerin toplumsal ve ekonomik faaliyetlerini izlemesiyle eleştirilmiştir.⁶⁸

Güvenlikten Paranoaya: Duygusal Rejimlerin Dönüşümü

Dijital çağda güvenlik söylemlerinin sürekli tekrarı ve tehdit vurgusu, toplumsal duygulanım üzerinde kalıcı etkiler bırakmaktadır. Bireysel düzeydeki güven arayışını, kolektif düzeyde ise yaygın bir tedirginlik ve hatta paranoyak bir bekleyiş haline getirmiştir. Bu dönüşüm, hem bireysel kaygı artışı olarak hem de davranışsal ve kültürel pratiklerin

⁶⁰ Lyon, *The Culture of Surveillance: Watching as a Way of Life*, s. 74.

⁶¹ Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", s. 211.

⁶² Foucault, *Security, Territory, Population: Lectures at the Collège de France, 1977-78*, ss. 108-112.

⁶³ Couldry ve Hepp, *The Mediated Construction of Reality*, s. 136.

⁶⁴ Ahmed, *The Cultural Politics of Emotion*, ss. 13-14.

⁶⁵ Beck, *Risk Society: Towards a New Modernity*, s. 98.

⁶⁶ Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", s. 233.

⁶⁷ Bauman ve Lyon, *Liquid Surveillance: A Conversation*, s. 102.

⁶⁸ Şahin, Mustafa, "Gözetim Toplumu ve Çin Sosyal Kredi Sistemi: Toplumsal Kontrolün Yeni Yüzü", *Journal of Suleyman Demirel University Institute of Social Sciences*, 49, (2024): 66-84.

dönüştüğü bir duygusal rejim değişimi olarak değerlendirilmelidir. Ahmed'in duyguların dolaşımı yaklaşımı, bu süreci anlamlandırmak adına yararlıdır. Korku ve tedirginlik medya, kurumlar ve sosyal etkileşimler aracılığıyla dolaşıma dahil edilmekte ve böylece kolektif bir duygusal atmosfer oluşturmaktadır.⁶⁹

Güvenlik söylemlerinin tekrarı, bireyleri risk yönetmeye zorlayan pratiklere yönlendirmektedir. Bununla beraber "her an saldırıya uğrama" ihtimali üzerinden bir tetikte olma durumu inşa etmektedir. Bu Lyon'un gözetim kültürü (surveillance culture/culture of surveillance) tanımıyla uyumludur. Gözetim gündelik yaşamın bir parçası haline gelmekte ve insanların davranışlarında sürekli bir uyum ya da refleks üretmektedir.⁷⁰ Böyle bir ortamda güvende kalma davranışı, teknik çözümlere (iki faktörlü doğrulama, VPN vb.) ya da kurumsal/platform teminatlarına yönelme şeklinde ortaya çıkarken aynı pratikler bireyde aynı zamanda kimin izlediği, verilerin nasıl kullanıldığı gibi konularda sürekli bir kuşku oluşturmaktadır. Bundan ötürü de güvenin yerini belirsizlik ve paranoya olma riski doğmaktadır.⁷¹ Siyasi etki konusunda yapılan çalışmalar, bu duygusal dönüşümü yalnızca psikolojik bir sonuç olarak görmemektedir. Massumi gibi araştırmacılar duygunun politik etkisini vurgulayarak özellikle güvenlik söylemlerinin bedensel ve önbilinçli tepkileri tetiklediğini belirtmektedir. Bu önbilinçli tetiklenme, bireyin sürekli olarak alarm durumunda kalmasına ve dolayısıyla hem öznelleşmiş gözetim pratiklerine razı olmasına yol açabilmektedir.⁷² Nitekim pandemi döneminde dijital gözetim uygulamalarının medyada nasıl haberleştirildiğine dair çalışmalar, tekrarlanan tehdit vurgusunun kamuoyunda kaygı ve kabul ürettiğini göstermiştir. Haber dili sık sık aciliyet ve risk vurgusuna dayandığı için izleme/izlenme pratikleri meşrulaştırmıştır.⁷³

Sosyal medya ve ağıl kamusal alanlar da bu süreç içinde merkezi bir rol üstlenmektedir. Marwick ile boyd'un ağıl gizlilik (networked privacy) analizleri, görünürlük, itibar ve veri paylaşımı dinamiklerinin bireylerde hem dikkatli bir öz-gözetim hem de bir endişe kültürü oluşturduğunu ortaya koymaktadır. Kullanıcılar görünür olma ile gizlilik kaygısı arasında sürekli bir denge kurma mecburiyetiyle karşı karşıyadır.⁷⁴ Bu dinamizm, güvenlik söylemleriyle birleştiğinde paranoyak bir pratik üretmektedir. İnsanlar sadece korunmak adına değil aynı zamanda olası tehditlerden kaçınmak için de sürekli strateji geliştirmektedir. Bu stratejiler -örneğin; aşırı şifreleme, çevrim içi anonimlik arayışları ya da platformlara aşırı güven- toplumsal normlara dönüşebilmektedir.⁷⁵ Siber güvenlik söyleminden kaynaklanan duygusal rejim değişimi, güvenden paranoyaya doğru bir kayış potansiyeli taşımaktadır. Güven arayışı bireyi teknik çözümlere ve kurumsal teminatlara bağlarken aynı zamanda bu bağlılık yeni kuşklar, öznellik kırılmaları ve kolektif güvensizlik üretmektedir. İlgili durum, hem politik açıdan rıza üretimi için elverişli bir zemin hazırlamakta hem de toplumsal bağları aşındırarak tekil güven yöntemlerini (self-governance) ön plana çıkarmaktadır. Başka bir ifadeyle ortak toplumsal çözümler yerine bireysel emniyet stratejileriyle meşgul olmaktadır.⁷⁶

⁶⁹ Ahmed, *The Cultural Politics of Emotion*, ss. 13-14.

⁷⁰ Lyon, David. "Surveillance Culture: Engagement, Exposure and Ethics in Digital Modernity", *International Journal of Communication*, 11, (2017): 824-842, 829.

⁷¹ Marwick, Alice E. ve boyd, danah. "Networked Privacy: How Teenagers Negotiate Context in Social Media", *New Media & Society*, 16(7), (2014): 1051-1067.

⁷² Massumi, *The Politics of Affect*, ss. 33-36.

⁷³ Comer, Leigha, Donelle, Lorie, Ngole, Marionette, Shelley, Jacob J., Kothari, Anita, Smith, Maxwell, Shelley, James M., Stranges, Saverio, Hiebert, Brad, Gilliland, Jason, Burkell, Jacquelyn, Cooke, Tommy, Hall, Jodi ve Long, Jed. "An investigation of media reports of digital surveillance during COVID-19", *Frontiers in Digital Health*, 5, 2023, ss. 4-7.

⁷⁴ Marwick ve boyd, "Networked Privacy: How Teenagers Negotiate Context in Social Media".

⁷⁵ Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power" ss. 233-236.

⁷⁶ Beck, *Risk Society: Towards a New Modernity*, ss. 21-24.

Dijital Mahremiyetin Erozyonu ve Tekinsiz Yakınlıklar

Dijitalleşme, mahremiyetin sınırlarını yeniden kurgularken aynı zamanda “yakınlık” ve “erişilebilirlik” kavramlarını da dönüşüme uğratmıştır. Platformlar ve hizmet sağlayıcılar, kullanıcı ilişkilerini ekonomik değere dönüştürürken mahremiyetin krizine yol açmakta, bireyler yakınlık ve görünürlük elde etme uğruna kişisel verilerini paylaşmaya teşvik edilmektedir.⁷⁷ Bu paylaşım/izleme döngüsü, mahremiyetin aşınmasıyla beraber tekinsiz yakınlıklar denilebilecek bir sosyal ortam üretmektedir. Tanıdık araçlar (akıllı telefon, sosyal medya platformları vs.) hem ilişki kurmayı kolaylaştırmakta hem de izlenmiş olma duygusunu evcilleştirmektedir.⁷⁸ Mahremiyetin erozyonu veri sızıntıları ya da hukuksal boşluklarla açıklanmanın yanında mahremiyet normlarının bağlama göre değiştiği gerçeğiyle de ilişkilidir. Nissenbaum’ın bağlamsal bütünlük (contextual integrity) yaklaşımı hangi bilgi akışlarının hangi sosyal bağlamlarda uygun olduğuna dair normların ihlal edildiğinde mahremiyetin zedelendiğini göstermektedir.⁷⁹ Dijital platformların veri toplama ve yeniden kullanma pratikleri, sık sık bu bağlamlar normları aşmaktadır. Sonuç olarak da kullanıcılar, beklemedikleri biçimlerde verilerinin kullanıldığını fark ettiklerinde yoğun bir rahatsızlık ve tekinsizlik hissi yaşamaktadır.⁸⁰

Hukuk ve politika literatürü, mahremiyet ihlallerinin yalnızca bireysel zararlar üretmediğini, sosyal bağları zedeleyip güven ilişkilerini de aşındırdığını vurgulamaktadır. Solove’un mahremiyet taksonomisi, mahremiyet ihlallerinin farklılığını ortaya koyarak, basit veri sızıntısının bile kimlik, itibar ve ilişki güveni üzerinde geniş etkiler oluşturabileceğini göstermektedir.⁸¹ Söz konusu etki, tekinsiz yakınlıkların şekillenmesinde merkezidir. Bireyler daha önce özel saydıkları alanların izlenme ihtimaliyle yüzleşince ilişkilerde mesafe, otosansür ya da performatif açıklık (performative self-disclosure) gibi yeni davranış örüntüleri geliştirmektedir.⁸² Dijital teknolojilerin yakınlığı estetikleştirilmesi de bu noktada önemlidir. Akıllı ev asistanları, sağlık uygulamaları ya da ilişki uygulamaları, kullanıcıya yakınlık duygusu verirken aynı anda davranışlarının kaydedildiği ve analiz edildiği bir veri alt yapısı çalıştırmaktadır. Levy’in samimi gözetim (intimate surveillance) çalışması, gözetimin en içsel alanlara (ilişkiler, cinsellik, bakım pratikleri vs.) nasıl nüfuz ettiğini göstermektedir. Böylelikle mahremiyetin sınırları bulanıklaşmakta ve yakınlık ile tehlike iç içe geçmektedir.⁸³ Ek olarak hukuki ve kurumsal düzenlemelerin yetersizliği, kullanıcıların mahremiyet kaygılarını artırmaktadır. Cohen’in ağırlıklı benlik/ağ-bağlantılı benlik (networked self) eleştirisi, teknik ve hukuki düzenlemelerin bilgi akışlarını çoğunlukla denetleyemediğini, bu durumun bireylerde sürekli olarak bir belirsizlik ve korunmasızlık hissi oluşturduğunu belirtmektedir.⁸⁴ Dolayısıyla tekinsiz yakınlıklar, hem bir duygusal tepki hem de düzenleyici boşlukların ve güç asimetrisinin bir yansımasıdır.

Dijital mahremiyetin erozyonu ile tekinsiz yakınlıklar arasında çok yönlü bir ilişki bulunmaktadır. Mahremiyet kuralları bağlamsal olarak zarar görürken yakınlık araçları izlenmişlik halini normalleştirmektedir. Bu durum bireylerde bir yandan duygusal bir rahatsızlık (tekinsizlik) diğer yandan da yeni davranış biçimleri (performatif mahremiyet, otosansür, platformlara bağımlılık) üretmektedir. Bilimsel ve politik açıdan mahremiyetin

⁷⁷ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”, ss. 8-12.

⁷⁸ Levy, Karen. “Intimate Surveillance”, Idaho Law Review, 51, (2015): 679-693, ss. 679-682.

⁷⁹ Nissenbaum, Helen. “Privacy as Contextual Integrity”, Washington Law Review, 79(1), (2004): 119-158, ss. 7-9.

⁸⁰ Nissenbaum, “Privacy as Contextual Integrity”, ss. 12-15.

⁸¹ Solove, Daniel J. “A Taxonomy of Privacy”, University of Pennsylvania Law Review, 154(3), (2006): 477-560, ss. 48-486.

⁸² Marwick ve boyd, “Networked Privacy: How Teenagers Negotiate Context in Social Media”, ss. 1054-1057.

⁸³ Levy, “Intimate Surveillance”, ss. 681-686.

⁸⁴ Cohen, Julie E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press, 2012, ss. 42-48.

korunması sadece teknik önlemler değil, bağlamsal normların gözetilmesi, şeffaflık ve kurumsal sorumluluk gerektirmektedir.⁸⁵

Güvenin Yeniden İnşası: Dijital Güvenlik Kültürü

Dijital güvenlik kültürü, organizasyonlardan ulus devletlere ve bireysel kullanıcılara kadar geniş bir yelpazede güvenin yeniden inşa edildiği ve normalleştirildiği sosyal bir süreçtir. Söz konusu süreç, teknik önlemlerin (şifreleme, antivirüsler, çok faktörlü kimlik doğrulama) ötesinde normlar, pratikler, eğitim programları, kurum içi davranış modelleri ve iletişim stratejileri aracılığıyla yürütülmektedir. ENISA ve benzeri kurumların raporları, siber güvenlik performansının büyük ölçüde teknik olmayan insan ve kültür faktörlerine bağlı olduğunu vurgulayarak kültür oluşturma için merkezi olduğunu ortaya koymaktadır.⁸⁶

Güvenin yeniden inşası iki temel ekseninde ilerlemektedir. Birincisi, kurumların ve platformların kullanıcılarla kurduğu iletişim ve şeffaflık pratikleri vasıtasıyla güven tesis etme çabasıdır. Şeffaflık, risklerin açık biçimde paylaşılması, saldırı sonrası iletişim politikaları ve kullanım politikalarının anlaşılır hale getirilmesiyle sağlanmaktadır. Bu tür uygulamalar, kullanıcıların sisteme duyduğu güveni artırırken aynı zamanda algoritmik karar süreçlerine ilişkin belirsizlikleri de azaltmaktadır.⁸⁷ İkincisi, bireysel düzeyde güven pratiklerinin geliştirilmesidir. Farkındalık eğitimleri, güvenlik davranışlarının içselleştirilmesi, düzenli tatbikatlar ve ödüllendirici geri bildirim mekanizmaları gibi unsurlar, kullanıcıların güvenli davranışları rutin haline getirmesini sağlamaktadır.⁸⁸ İlgili yeniden inşa süreci aynı zamanda bir iktidar teknolojisi niteliği taşımaktadır. Hangi davranışların “güvenli” sayılacağı, hangi risklerin öncelikli hale getirileceği ve hangi aktörlerin güven sağlayıcı olarak konumlayacağı toplumsal aktörler tarafından tanımlanmaktadır. Bu tanımlama sürecinde teknoloji şirketleri sıklıkla “koruyucu” rolü üstlenirken kullanıcılara sunulan güvenlik ürünleri ve hizmetler aynı zamanda verilerin toplanması ve yönetimi adına yeni imkanlar oluşturmaktadır.⁸⁹ Dolayısıyla dijital güvenlik kültürü, hem güven üretmekte hem de gözetim alt yapılarını meşrulaştırma riskini barındırmaktadır. Güven ile kontrol arasındaki sınır da bu noktada tartışmalı bir hale gelmektedir.⁹⁰

Uygulamalı literatür, etkin bir siber güvenlik kültürü için bütüncül yaklaşımlar önermektedir. Bu yaklaşımlar;

- Üst yönetimin taahhüdü ve liderliği
- Sürekli ve bağlama özgü eğitim-farkındalık programları
- Çalışan davranışlarını izleyen ve olumlu davranışları pekiştiren geri bildirim mekanizmaları
- Teknik çözümlerle insan odaklı uygulamaların uyumu
- Düzenli tatbikatlar ile değerlendirme bileşenlerini içermektedir.⁹¹

⁸⁵ Nissenbaum, “Privacy as Contextual Integrity”, ss. 20-24.

⁸⁶ ENISA. ENISA Threat Landscape 2021. European Union Agency for Cybersecurity, 2021.

⁸⁷ ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. European Union Agency for Cybersecurity, 2019.

⁸⁸ Hadlington, Lee. The “Human Factor” in Cybersecurity: Exploring the Accidental Insider. IGI Global, 2018.

⁸⁹ Zuboff, “The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power”.

⁹⁰ Lupton, The Quantified Self: A Sociology of Self-Tracking.

⁹¹ Alshaikh, Moneer. “Developing Cybersecurity Culture to Influence Employee Behaviour: A Practice Perspective”, Computers & Security, 98 (2020): 102003.

Araştırmalar, hem eğitim vermenin yeterli olmadığını hem de davranış değişiminin ancak kurumsal yapı, ödüllendirme ve uygun teknolojik destekle sürdürülebilir olduğunu kanıtlamaktadır.⁹² Dolayısıyla dijital güvenlik kültürü güvenin yeniden inşası adına fırsat ve meydan okuma niteliği taşımaktadır. Doğru kurgulanmış kültürel müdahaleler kullanıcı güvenliğini artırıp siber risklere karşı toplu direnç oluşturabilmektedir. Diğer yandan şeffaf olmayan ve rızaya dayanmayan uygulamalar güvenin aşınmasına, tekinsizliğin yeniden üretilmesine ve mahremiyet kaybına yol açabilmektedir. Bu sebeple politika yapımcılar, teknoloji firmaları ve araştırmacılar güven tesisinde teknik çözümlerle beraber etik, şeffaflık ve katılımcılığı odak noktasına alan yaklaşımlar geliştirilmelidir.⁹³

Tartışma: Güvenli Olmayan Güvenlik-Tekinsizliğin Kurumsallaşması

Dijital güvenlik söylemleri ve gözetim uygulamaları, teknik önlemlerle başlayıp bireylerin davranışlarına ve duygularına kadar uzanan bir yayılım göstermektedir. Ancak bu yayılan güvenlik mekanizmaları aynı zamanda bir paradoks üretmektedir. Güvenlik arayışı, kendisini sürekli tehdit altında hissetme haline çevrilmekte ve böylelikle “güvenli olmayan güvenlik” modeli gündeme gelmektedir. Söz konusu durum, güven ortamının değil aksine tekinsizliğin kurumsallaşmasının bir göstergesidir. Kurumsallaşma süreçleri, güvenlik söylemlerinin rutin ve normalleştirilmiş biçimlerine dönüşmesini içermektedir. Örneğin, devletlerin ve teknoloji kurumlarının gözetim ve veri takibi politikaları “acil önlem”, “risk yönetimi” vb. söylemlerle kurumsal yapılara entegre edilmektedir. Bu bağlamda, kurumsallaşmış tekinsizlik denen duruma geçilmektedir. birey, sürekli izlenmişlik, veri akışı, profil oluşturma gibi süreçlerle karşı karşıya kalmakta, bu süreçler kurumsal normlara dönüşmekte ve artık sıradanlaştırılmaktadır.⁹⁴ Böylece tehdit algıları, güvenlik kurumlarının meşruiyetini pekiştirirken, birey için güvenlik sağlama değil, sürekli riski yönetme haline gelmektedir.

Söylemsel düzeyde güvenlik kurumları sorunları güvenlik çerçevesi içinde tanımlamakta ve modelleyerek kendi varlık biçimlerini meşrulaştırmaktadır. Bu süreç içinde güvensizlik normalleşmekte, kurumsal sistemler sadece tehditlerle mücadele eden araçlar değil aynı zamanda riskin sürekli tekrarlandığı ve yönetildiği sistemler haline gelmektedir.⁹⁵ Bu yapısal dönüşüm, bireylerin güvenlik hizmetlerine yönelmesini sağlarken aynı anda sistemlere karşı duyulan güveni de erozyona uğratabilmektedir. Çünkü kontrol mekanizmaları sıklıkla şeffaf değildir, izleme süreçleri görünmez haldedir ve bireyler gözetim altında olduklarını hissetmektedir. Toplumsal düzeyde ise güvenin yeniden inşası yerine gözetim yükünün yayılması gözlemlenmektedir. Gözetim teknolojilerinin yaygınlaşması, mahremiyetin sınırlarını esnetirken aynı zamanda bireylerin öznel güvenlik talebini artırmaktadır. Söz konusu talep, kurumsal güvenlik çözümlerine olan bağımlılığı pekiştirmektedir. Fakat bu bağımlılık beraberinde yeni belirsizlikler ortaya çıkarmaktadır: “Kimi izliyor?”, “Hangi veriler kullanılıyor?”, “Benim hakkımda oluşturulan profil ne?” gibi sorularla karşılaşmaktadır. Böylelikle güvenlik sistemi bir avantajdan çok varoluşsal risk üreticisi haline gelebilmektedir.⁹⁶ Bu kapsamda tekinsizliğin kurumsallaşması kavramı anlamlı hale gelmektedir. Kurumlar ve teknoloji aktörleri, güvenlik söylemlerini rutin hale getirerek ve normalleştirerek bireylerin gözetim ve veri izleme süreçlerini olağanlaştırmaktadır. Bu olağanlaşma, tekinsizlik hissini bireysel düzeyden sistematik düzeye taşımaktadır. Başka bir

⁹² Sasse, M. Angela, Brostoff, Sacha ve Weirich, Dirk. “Transforming The 'Weakest Link' — A Human/Computer Interaction Approach To Usable And Effective Security”, BT Technology Journal, 19(3), (2001).

⁹³ ENISA. “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity”.

⁹⁴ Çelikpala, Mitat ve Öztürk, Duygu. “The Only Thing We Have To Fear: Post 9/11 Institutionalization of In-Security”, Uluslararası İlişkiler Dergisi, 9(35), (2012): 5-24.

⁹⁵ Coles-Kemp, Lizzie, Ashenden, Debi ve O'Hara, Kieron. “Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen”, Politics & Governance, 6(2) (2018): 109-118, s. 112.

⁹⁶ Sheehy, Bonnie. “Algorithmic Paranoia: The Temporal Governmentality of Predictive Policing”, Ethics and Information Technology, 21(1), (2019): 49-58, ss. 51-58.

ifadeyle birey sadece “izleniyor olma” duygusu yaşamamakta, bu duygu sistem tarafından üretilmiş hale gelmektedir. Söz konusu durum, güvenliğin dışsal bir garanti değil, yönetilmesi gereken sürekli bir risk olarak algılanmasına yol açmaktadır.

Sonuç

Dijital çağın hızla dönüşen yapısı, güvenliği sadece teknik bir konu olarak ele alınamayacağını açık bir şekilde göstermektedir. Artık güvenlik, bireylerin sadece verilerini koruma çabasıyla sınırlı değildir. Bunun yanında duygusal, kültürel ve toplumsal düzeyde tecrübe edinilen bir olguya dönüşmüştür. İnsanların “güvende hissetme” arzusu, dijital teknolojilerle iç içe geçmiş bir yaşam biçiminde yeniden tanımlanmaktadır. Bu durum, güvenliğin nesnel bir durumdan çok öznel bir duygu haline geldiğini göstermektedir. Bahsi geçen yönüyle dijital çağda güvenlik, hem bireyin psikolojik yapısına hem de toplumun kültürel kodlarına nüfuz eden bir duygusal deneyim olarak karşımıza çıkmaktadır. Teknolojik gelişmelerin vaat ettiği koruma duygusu, paradoksal şekilde bireylerde sürekli bir tehdit algısını da canlı tutmaktadır. Gözetim sistemlerinin yaygın hale gelmesi, algoritmik tahmin mekanizmalarının gündelik yaşamın bir parçası haline gelmesi ve siber güvenlik söylemlerinin medya aracılığıyla sürekli yeniden üretilmesi, bireylerde “her an tehdit altında olma” hissini beslemektedir. Bu durum, güvenliğin sağlama çabasının kendisini tekinsiz bir zemine taşımaktadır. Güvenliğin sağlanması adına geliştirilen araçlar, bireyin özgürlüğünü ve mahremiyetini tehdit eden yeni kaygı alanları oluşturmaktadır. Böylelikle güvenli olmayan güvenlik biçimleri kurumsal bir hale gelmektedir. Bu çerçevede siber güvenliğin sadece teknik alt yapıların, algoritmaların ya da yazılım sistemlerinin konusu olmadığı bunun yanında derin bir sosyolojik ve kültürel mesele olduğu açıktır. Güvenlik, toplumun hangi değerlere öncelik verdiğini, bireylerin teknolojiye ne ölçüde güvendiğini ve mahremiyet algılarının nasıl şekillendiğini yansıtan çok katmanlı bir olgudur. Bu nedenle siber güvenliğe dair tartışmalar, teknik yeterlilik kadar duygusal iklimi, kültürel anlam dünyalarını ve toplumsal ilişkileri de hesaba katmalıdır.

Bu çalışma kapsamında ulaşılan bulgular, giriş başlığında yöneltlen temel araştırma sorularına dair bazı soruların belirgin hale geldiğini göstermektedir. İlk olarak, dijital güvenlik söylemlerinin bireylerin günlük yaşamlarında yoğun bir “sürekli tehdit” ve “potansiyel risk” algısı oluşturduğu görülmektedir. İlgili söylemler, güvenliği koruyan bir mekanizma olmaktan ziyade bir korku üretim sürecine dönüşmekte ve bireylerin duygusal dünyasında devamlılığını koruyan bir tetikte olma hali oluşturmaktadır. İkinci olarak, siber gözetim ve veri denetimi uygulamalarının toplumsal ilişkiler üzerinde dönüştürücü bir rolü olduğu saptanmıştır. Özellikle dijital kimliklerin algoritmik şekilde sınıflandırılması ve izlenmesi, bireylerin kendilerini sunma biçimlerini değiştirmekte ve pratikler tarafından da şekillendirilmektedir. Bu yönüyle çalışma, siber gözetimin hem devlet-birey ilişkisini hem de bireyler arası ilişkileri de yeniden kurduğunu göstermektedir. Üçüncü olarak, mevcut literatürde dijital güvenlik ve tekinsizlik kavramlarının sıklıkla risk toplumu, duyguların siyaseti, gözetim toplumu, neoliberal özne, teknolojik determinizm gibi sosyolojik olgular ekseninde değerlendirildiği görülmüştür. Bu çalışma, literatürde yer alan bu tartışmalara duygusal rejimler ve kültürel güvenlik kodları üzerinden yeniden bir okuma getirmeyi hedeflemiştir. Yine dijital güvenlik söylemlerinin bireyin duygusal ve davranışsal tepkilerini güçlü bir şekilde yönlendirdiği görülmektedir. Güvenlik söylemi, bireylerde çoğunlukla rıza üretmekte, kişisel verilerin paylaşılması, gözetim uygulamalarının normalleşmesi ve mahremiyetin törpülenmesi gibi davranışları da tetiklemektedir. Bu bağlamda güvenlik söylemi, bireyin özgürlük alanını daraltırken aynı zamanda yeni bir dijital uyumluluk kültürü de oluşturmaktadır.

Güvenlik teknolojilerinin toplumla kurmuş olduğu ilişki, duygusal rejimlerin yeniden yapılanmasına da yol açmaktadır. Dijital ortamlarda bireylerin güven, korku, kuşku ve

tekinsizlik gibi duyguları sürekli tetiklenmektedir. Bu duygular, politik ve ekonomik düzenin işleyişinde stratejik araçlara dönüşmektedir. Birey, güvende kalmak için gözetim sistemlerine rıza göstermekte, kişisel verilerini paylaşmakta, mahremiyetinden ödün vermekte ve böylelikle kendi güvensizliğinin üretim sürecine bilinçsiz bir şekilde katılmaktadır. Bu döngü, dijital çağın en belirgin çelişkilerinden birini temsil etmektedir. Güvenliğin bedeli, kimi zaman özgürlüğün ve mahremiyetin kısıtlanması olmaktadır.

Bu çalışmadan hareketle gelecekteki araştırmalar için bazı yeni yönelimlerin belirginleştiği söylenebilmektedir. Öncelikle “dijital güven kültürü” kavramı, bireylerin ve kurumların güvenlik konusundaki algılarını, iletişim pratiklerini ve davranış biçimlerini anlamak açısından önemli bir araştırma alanı sunmaktadır. Güvenin dijital ortamda nasıl üretildiği, paylaşıldığı ve yeniden müzakere edildiği incelenmelidir. İkinci olarak “siber panik” olgusunun, toplumsal korkuların ve kriz anlatılarının nasıl dolaşıma dahil edildiğini anlamak açısından önem taşıdığı görülmektedir. Dijital medya ve haber platformları, siber saldırılar veya veri ihlalleri üzerinden kolektif korku üretme potansiyeline sahiptir. Bu sebeple bu tür panik anlatılarının sosyolojik analizi, duyguların yönetimi ve siyasal kontrol mekanizmalarının incelenmesi açısından zengin bir zemin sunmaktadır. Üçüncü olarak “algoritmik korku” kavramı gün geçtikçe önem kazanmaktadır. Yapay zeka ve algoritmaların karar süreçlerinde görünmez bir otoriteye dönüşmesi, bireylerin bilinçdışı düzeyde yeni bir güvensizlik biçimi geliştirmesine yol açmaktadır. Söz konusu durum, teknolojik şeffaflık, etik denetim ve dijital özerklik gibi alanlarda yeni teorik yaklaşımları zorunlu kılmaktadır. Son olarak “mahremiyet sosyolojisi” dijital çağın en kritik noktalarından biridir. Mahremiyetin kişisel sınır olmaktan çıkıp algoritmik sistemler tarafından yeniden tanımlandığı günümüzde bireylerin kendilerini koruma, gizleme veya paylaşma biçimleri değişmiştir. Mahremiyetin bu dönüşümü, kimlik, aidiyet ve toplumsal güven ilişkilerini yeniden biçimlendirmektedir.

Sonuç olarak dijital çağ, güvenliğin anlamını, kapsamını ve deneyimlenme biçimini kökten değiştirmiştir. Güvenlik artış yalnızca fiziksel ya da teknik bir korunma, yani emniyet ile eş anlamlı değildir. Çok daha geniş bir kavram olma niteliğine sahiptir ve bireyin psikolojik, duygusal ve toplumsal deneyimlerini de kapsamaktadır. Bu süreç içinde birey, hem güvenliğin öznesi hem de nesnesi haline gelmiştir. Bu sebeple geleceğin güvenlik anlayışı teknik kapasitenin yanında etik duyarlılığa, toplumsal katılıma ve duygusal farkındalığa dayalı olmalıdır. Güvenliği yeniden tanımlamak, aslında dijital çağda insanın kendini, ilişkilerini ve dünyayla kurmuş olduğu bağı yeniden düşünmek anlamına gelmektedir.

Kaynakça

- Ahmed, Sara. *The Cultural Politics of Emotion*. Edinburgh University Press, 2014.
- Alshaikh, Moneer. “Developing Cybersecurity Culture to Influence Employee Behaviour: A Practice Perspective”, *Computers & Security*, 98 (2020): 102003.
- Altheide, David L. *Terrorism and the Politics of Fear*. Rowman & Littlefield, 2013.
- Bauman, Zygmunt. *Liquid Fear*. Polity Press, 2006.
- Bauman, Zygmunt. *Liquid Times: Living in an Age of Uncertainty*. Polity Press, 2007.
- Bauman, Zygmunt ve Lyon, David. *Liquid Surveillance: A Conversation*. Polity Press, 2013.
- Beck, Ulrich. *Risk Society: Towards a New Modernity*. Sage Publications, 1992.
- Buzan, Barry, Wæver, Ole ve de Wilde, Jaap de. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, 1998.
- Cohen, Julie E. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press, 2012.

- Coles-Kemp, Lizzie, Ashenden, Debi ve O'Hara, Kieron. "Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen", *Politics & Governance*, 6(2) (2018): 109-118.
- Comer, Leigha, Donelle, Lorie, Ngole, Marionette, Shelley, Jacob J., Kothari, Anita, Smith, Maxwell, Shelley, James M., Stranges, Saverio, Hiebert, Brad, Gilliland, Jason, Burkell, Jacquelyn, Cooke, Tommy, Hall, Jodi ve Long, Jed. "An investigation of media reports of digital surveillance during COVID-19", *Frontiers in Digital Health*, 5, 2023.
- Couldry, Nick ve Hepp, Andreas. *The Mediated Construction of Reality*. Polity Press, 2017.
- Çelikpala, Mitat ve Öztürk, Duygu. "The Only Thing We Have To Fear: Post 9/11 Institutionalization of In-Security", *Uluslararası İlişkiler Dergisi*, 9(35), (2012): 5-24.
- Deibert, Ronald J. *Black Code: Inside the Battle for Cyberspace*. Signal, 2013.
- ENISA. "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity". European Union Agency for Cybersecurity, 2019.
- ENISA. "ENISA Threat Landscape 2021". European Union Agency for Cybersecurity, 2021.
- Foucault, Michel. *Security, Territory, Population: Lectures at the Collège de France, 1977-78*. Palgrave Macmillan, 2007.
- Freidman, A. ve Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, 2014.
- Freud, Sigmund. *The Uncanny*. Penguin Books, 2003.
- Furedi, Frank. *How Fear Works: Culture of Fear in the Twenty-First Century*. Bloomsbury, 2018.
- Giddens, Anthony. *The Consequences of Modernity*. Stanford University Press, 1990.
- Hadlington, Lee. *The "Human Factor" in Cybersecurity: Exploring the Accidental Insider*. IGI Global, 2018.
- Levy, Karen. "Intimate Surveillance", *Idaho Law Review*, 51, (2015): 679-693.
- Lupton, Deborah. *The Quantified Self: A Sociology of Self-Tracking*. Polity Press, 2021.
- Lyon, David. "Surveillance Culture: Engagement, Exposure and Ethics in Digital Modernity", *International Journal of Communication*, 11, (2017): 824-842.
- Lyon, David. *The Culture of Surveillance: Watching as a Way of Life*. Polity Press, 2018.
- Lyon, David. *State, Digital Surveillance, and Society – A Scoping Review*. Dinasti Publishing, 2023.
- Marwick, Alice E. ve boyd, danah. "Networked Privacy: How Teenagers Negotiate Context in Social Media", *New Media & Society*, 16(7), (2014): 1051-1067.
- Massumi, Brian. *The Politics of Affect*. Polity Press, 2015.
- Monahan, Torin. *Surveillance in a Time of Insecurity*. Rutgers University Press, 2010.
- Nissenbaum, Helen. "Privacy as Contextual Integrity", *Washington Law Review*, 79(1), (2004): 119-158.
- Padden, Michaela. "The Transformation of Surveillance in the Digitalisation Discourse". *Internet Policy Review*, 12(3), (2023).
- Papacharissi, Zizi. *Affective Publics: Sentiment, Technology, and Politics*. Oxford University Press, 2015.

- Sasse, M. Angela, Brostoff, Sacha ve Weirich, Dirk. "Transforming The 'Weakest Link' – A Human/Computer Interaction Approach To Usable And Effective Security", BT Technology Journal, 19(3), (2001).
- Sheehey, Bonnie. "Algorithmic Paranoia: The Temporal Governmentality of Predictive Policing", Ethics and Information Technology, 21(1), (2019): 49-58.
- Solove, Daniel J. "A Taxonomy of Privacy", University of Pennsylvania Law Review, 154(3), (2006): 477-560.
- Şahin, Mustafa, "Gözetim Toplumu ve Çin Sosyal Kredi Sistemi: Toplumsal Kontrolün Yeni Yüzü", Journal of Suleyman Demirel University Institute of Social Sciences, 49, (2024): 66-84.
- Volosevici, Dana. "Surveillance as a Socio-Technical System: Behavioral and Psychological Impacts", Social Sciences, 13(7), (2025): 614.
- Wæver, Ole. "Securitization and Desecuritization", On Security. Ed., R. D. Lipschutz (Ed.), (ss. 46-86). Columbia University Press, 1995.
- Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.

Etik Kurul Raporu: Bu çalışma için etik kurul raporu gerekliliği bulunmamaktadır.
--

Katkı oranı beyanı: %100.

Çatışma beyanı: Makalede, herhangi bir kurum, kuruluş ve kişi ile çıkar çatışması yoktur.
--