Bölüm 3

Kent ve Bireysel Özgürlükler Krizi: Veri Gizliliği, CCTV ve Güvenlikli Siteler

Adnan Söylemez[1]

Özet

Kişisel bilgiler çeşitli kuruluşlar tarafından toplandıkça, işlendikçe ve saklandıkça veri gizliliği dijital çağda önemli bir endişe kaynağı haline gelmiştir. Bu verilerin korunması ve gizliliğinin sağlanması dünya çapında hükümetler için bir öncelik haline gelmiştir. Kapalı devre televizyon (CCTV) kameralarının kullanımı ise son yıllarda önemli ölçüde artmış ve bireysel mahremiyet üzerindeki etkisine ilişkin endişeleri artırmıştır. Kentleşme, teknolojik ilerlemeler ve güvenlik ve esenliğe artan odaklanma nedeniyle güvenli barınma son yıllarda artan bir ilgi görmüştür. Günümüzün sürekli gelişen dünyasında, güvenlik ve potansiyel tehditlere karşı korunma ihtiyacı nedeniyle güvenli barınma giderek daha önemli hale gelmiştir. Ancak, güvenlik önlemleri ile özgürlük ve mahremiyet gibi temel haklar arasındaki dengelerin incelenmesi büyük önem taşımaktadır.

Bu çalışmada, CCTV'nin suçu önlemedeki etkinliğini ve mahremiyetin ihlalini çevreleyen etik kaygıları değerlendirerek, güvenlik ve sivil özgürlükler arasındaki dengeyi çevreleyen tartışmaya ışık tutmayı amaçlamakta ve CCTV kameralarının gözetiminin kentsel ortamlarda bireysel özgürlükler üzerindeki etkisini ve sonuçlarını incelemektedir. Ayrıca bu makalede, veri gizliliğini korumak için geliştirilen çeşitli mevzuat ve politikalar incelenmekte; güvenli konutların ortaya çıkışı ve yaygınlaşmasına ilişkin bilimsel literatür gözden geçirilerek temel eğilimleri, zorlukları ve fırsatları vurgulayarak güvenlik önlemleri ile özgürlük ve mahremiyet gibi temel haklar arasındaki ödünleşimleri vurgulamaktadır.

GİRİŞ

Günümüzde, kentlerde yaşayan bireylerin özgürlükleri ve mahremiyeti üzerine büyük bir baskı söz konusudur. Veri gizliliği, CCTV kameralarının

1 Doç. Dr., Selçuk Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, soylemez@selcuk.edu.tr, ORC-ID: 0000-0001-8153-0238

https://doi.org/10.58830/ozgur.pub269.c1086

yaygınlaşması ve güvenlikli siteler, bireysel özgürlüklerin sınırlanmasına yol açan faktörlerdir. Bu makale, kent ve bireysel özgürlükler krizine neden olan bu faktörleri ele alarak, yaşam alanlarında daha fazla özgürlük ve mahremiyet sağlamak adına çözüm önerileri sunmayı amaçlamaktadır. Kentlerde veri gizliliği, CCTV ve güvenlikli sitelerin yaygın kullanımı, bireysel özgürlükler ve mahremiyet üzerinde olumsuz etkiler yaratmakta olup, bu durumun ele alınarak uygun çözümler üretilmesi gerekmektedir.

1. VERİ GİZLİLİĞİ VE BİREYSEL ÖZGÜRLÜKLER

1.1. Teknolojik Gelişmeler ve Veri Toplama Yöntemleri: Son Gelişmelere Bir Bakış

Teknolojideki hızlı gelişmelerle birlikte veri toplama yöntemleri de son yıllarda önemli ölçüde değişmiştir. Bu bölümde, çeşitli teknolojik gelişmeler ve bunların farklı alanlardaki veri toplama teknikleri üzerindeki etkileri hakkında literatür gözden geçirilmektedir. Veri toplama, araştırmacıların araştırma sorularını yanıtlamak için gerekli bilgileri toplamalarını sağladığından araştırma sürecinin çok önemli bir yönüdür (Bryman, 2016). Anketler ve görüşmeler gibi geleneksel veri toplama yöntemlerinin birçok bağlamda güvenilir olduğu kanıtlanmıştır. Ancak, yeni teknolojilerin yükselişi araştırmacılara veri toplama konusunda yeni yaklaşımlar da sunmaktadır.

1.1.1. Mobil Teknoloji ve Veri Toplama

Akıllı telefonların ve tabletlerin yaygın olarak benimsenmesi, veri toplamada çeşitli şekillerde devrim yaratmıştır. Mobil cihazlar, benzeri görülmemiş düzeyde erişilebilirlik ve taşınabilirlik sunarak araştırmacıların uzaktan ve verimli bir şekilde veri toplamasına olanak tanımaktadır (Ferreira ve diğerleri, 2020). Örneğin, mobil uygulamalar anket yapmak, coğrafi bilgi toplamak ve sağlıkla ilgili verileri toplamak için kullanılmaktadır (Aguilera, 2019). Dahası, mobil cihazların kullanımı gerçek zamanlı verilerin toplanmasını kolaylaştırarak araştırmacıların katılımcıların davranış ve algılarında zaman içinde meydana gelen değişiklikleri takip ve analiz etmelerini sağlamaktadır (Miller, 2020).

1.1.2. Giyilebilir Cihazlar ve Nesnelerin İnterneti (IoT)

Akıllı saatler ve spor takip cihazları gibi giyilebilir cihazlar, fizyolojik ve davranışsal veri toplamak için popülerlik kazanmıştır (Piwek ve diğerleri, 2016). Bu cihazlar, araştırmacıların katılımcılardan sürekli, göze batmayan veriler toplamasını sağlayarak insan davranışının ve sağlığının çeşitli yönlerine ilişkin değerli bilgiler sunmaktadır (Gao ve diğerleri, 2018). Buna

ek olarak, Nesnelerin İnterneti (IoT) akıllı evler, cihazlar ve araçlar gibi birden fazla kaynaktan büyük ölçekli, gerçek zamanlı verilerin toplanmasını kolaylaştırmıştır (Bandyopadhyay ve Sen, 2020). Bu veriler birleştirilip analiz edilerek insan davranışı, sağlığı ve refahı hakkında yeni içgörüler elde edilebilmektedir.

1.1.3. Sosyal Medya ve Büyük Veri

Sosyal medya platformlarının yaygın kullanımı, araştırmacılara kullanıcı tarafından oluşturulan büyük miktarda veri sağlamıştır. Bu veriler, iletişim kalıpları, duygu analizi ve sosyal ağ dinamikleri gibi insan davranışının çeşitli yönlerini incelemek için çıkarılabilir ve analiz edilebilir (Gruzd ve diğerleri, 2018). Ayrıca, makine öğrenimi ve yapay zekâ teknikleri de dahil olmak üzere büyük veri analitiği, araştırmacıların daha önce erişilemeyen kalıpları ve eğilimleri ortaya çıkarmak için bu büyük, karmaşık veri kümelerini işlemesine ve analiz etmesine olanak sağlamıştır (Cortez ve Johnston, 2020).

1.1.4. Zorluklar ve Etik Hususlar

Veri toplama için yeni teknolojilerin benimsenmesi aynı zamanda veri gizliliği, güvenliği ve etik hususlarla ilgili endişeleri de beraberinde getirmektedir. Araştırmacılar, katılımcıların kişisel bilgilerinin korunduğundan ve veri toplamadan önce bilgilendirilmiş onam alındığından emin olmalıdır (Mittelstadt ve Floridi, 2016). Ayrıca, büyük veri ve makine öğrenimi algoritmalarının kullanımı, veriler popülasyonu temsil etmiyorsa veya algoritmalar dikkatlice tasarlanıp test edilmemişse subjektif sonuçlara yol açabilir (O'Neil, 2016). Bu nedenle araştırmacılar, bulgularının geçerliliğini ve güvenilirliğini sağlamak için bu zorlukları ele alma konusunda dikkatli olmalıdır.

Teknolojik gelişmeler veri toplama yöntemlerini önemli ölçüde etkilemiş, araştırmacılara bilgi toplama ve analiz etme konusunda yeni yollar sunmuştur. Mobil teknoloji, giyilebilir cihazlar, IoT ve sosyal medya, daha verimli, göze batmayan ve gerçek zamanlı veri toplama olanakları sağlayarak araştırma ortamını dönüştürmüştür. Ancak bu gelişmeler aynı zamanda veri gizliliği, güvenliği ve etiği ile ilgili zorlukları da beraberinde getirmektedir. Araştırmacılar, bu yeni veri toplama yöntemlerinin tüm potansiyelinden yararlanmak için bu gelişmelere uyum sağlamalı ve potansiyel endişeleri ele almalıdır.

1.2. Veri Gizliliği İhlallerinin Bireysel Özgürlüklere Etkisi

Veri gizliliği ihlalleri dijital çağda giderek yaygınlaşmakta ve hem bireysel hem de kolektif özgürlükleri etkilemektedir. Bu ihlaller kimlik hırsızlığı, mali kayıp ve psikolojik sıkıntı gibi bir dizi olumsuz sonuca yol açabilmektedir (Solove, 2006).

Veri mahremiyeti, bireylerin kişisel bilgileri üzerinde kontrol sahibi olmalarını ve özerkliklerini, saygınlıklarını ve özgürlüklerini korumalarını sağlayan temel bir haktır (Warren ve Brandeis, 1890). Bu kontrol tehlikeye girdiğinde, kişisel verilere yetkisiz erişim, kullanım veya ifşaya yol açan gizlilik ihlalleri meydana gelir. Bu ihlaller, zayıf güvenlik önlemleri, kötü niyetli siber saldırılar veya kuruluşların etik olmayan uygulamaları gibi çeşitli faktörlerden kaynaklanabilir (Mayer-Schönberger ve Cukier, 2013).

Bireysel özgürlükler, dış müdahale veya zorlama olmaksızın kişisel seçimler ve kararlar alma yeteneğini ifade eder. Veri gizliliği ihlalleri, savunmasızlık hissi yaratarak ve kurumlara olan güveni sarsarak bireysel özgürlükler üzerinde önemli bir etkiye sahip olabilir (Acquisti ve diğerleri, 2015). Bu durum ifade özgürlüğü üzerinde caydırıcı bir etkiye, otosansüre ve kamusal hayata katılımın azalmasına yol açabilir (Penney, 2017).

1.2.1. Veri Gizliliği İhlallerinin Bireysel Özgürlükler Üzerindeki Etkileri

a. Gözetim ve Kontrol

Veri gizliliği ihlalleri kitlesel gözetimi kolaylaştırarak bireysel özgürlük ve özerklik kaybına neden olmaktadır. Kişisel bilgilere rıza olmaksızın erişildiğinde ve izlendiğinde, bireyler kendilerini güçsüz hissedebilir ve haklarını özgürce kullanamayabilirler (Zuboff, 2019). Bu durum, insanların cezalandırılma korkusuyla fikirlerini ifade etme veya belirli faaliyetlerde bulunma konusunda daha temkinli hale gelmesiyle otosansüre yol açabilir (Stoycheff, 2016).

b. Ayrımcılık ve Profil Çıkarma

Veri gizliliği ihlalleri, kuruluşların kişisel bilgilerine dayanarak belirli grupları profilleme ve hedefleme gibi ayrımcı uygulamalarda bulunmalarını sağlayabilir (Barocas ve Selbst, 2016). Bu durum, etkilenenler için haksız muameleye, kısıtlı fırsatlara ve bireysel özgürlüklerin azalmasına yol açabilir (Pasquale, 2015).

c. Psikolojik Etkiler

Veri gizliliği ihlallerinin bireyler üzerinde önemli psikolojik etkileri olabilmekte, bu da endişe, stres ve irade kaybı gibi duygulara yol açabilmektedir (Whitley ve Hosein, 2010). Kişinin kişisel bilgilerinin ifşa edilmesi veya kötüye kullanılması korkusu, güvenin azalmasına ve otosansürün artmasına yol açarak bireysel özgürlükleri olumsuz yönde etkileyebilir (Dinev ve Hart, 2006).

Veri gizliliği ihlallerinin bireysel özgürlükler üzerindeki etkisini azaltmak için çeşitli önlemler alınabilir:

- Kuruluşların veri uygulamalarından sorumlu tutulmalarını sağlamak için veri koruma yasalarının ve yönetmeliklerinin güçlendirilmesi (Kuner, 2011).
- Veri işlemede şeffaflık ve hesap verebilirliğin teşvik edilmesi ve böylece bireylerin bilgilerinin nasıl ve kim tarafından kullanıldığını anlamalarının sağlanması (Bennett ve Raab, 2006).
- Bireylerin kişisel verileri üzerinde kontrol sahibi olmalarını ve mahremiyetlerini korumalarını sağlayan mahremiyet artırıcı teknolojilerin geliştirilmesi (Cavoukian, 2010).

Veri gizliliği ihlalleri, dijital çağda bireysel özgürlükler için önemli bir tehdit oluşturmaktadır. Politika yapıcılar ve kuruluşlar, bu ihlallerin bireyleri ve toplumu etkilediği çeşitli yolları anlayarak, bireysel özgürlüklere saygı duyan ve bunları koruyan daha güvenli ve eşitlikçi bir dijital ortam yaratmak için çalışabilirler.

1.2.2. Veri Gizliliğini Sağlamaya Yönelik Mevzuat ve Politikalar

Kişisel bilgiler çeşitli kuruluşlar tarafından toplandıkça, işlendikçe ve saklandıkça veri gizliliği dijital çağda önemli bir endişe kaynağı haline gelmiştir (Shackelford, 2019). Bu verilerin korunması ve gizliliğinin sağlanması dünya çapında hükümetler için bir öncelik haline gelmiştir. Mayıs 2018'de yürürlüğe giren Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR), veri gizliliği alanında dönüm noktası niteliğinde bir mevzuat olarak kabul edilmektedir (Voigt ve Von dem Bussche, 2017). GDPR, bireylere kişisel verileri üzerinde daha fazla kontrol sağlamayı ve AB üye ülkeleri arasında uyumlu bir veri koruma çerçevesi oluşturmayı amaçlamaktadır. GDPR'nin temel hükümleri arasında unutulma hakkı, veri taşınabilirliği ve zorunlu veri ihlali bildirimleri yer almaktadır (Drew, 2018). GDPR, veri gizliliği konusunda farkındalık yaratma konusunda başarılı olsa da uygulanması, yetersiz kaynaklara sahip denetim makamları ve düzenlemenin karmaşıklığı gibi zorluklarla karşılaşmıştır (Polčák ve Holub, 2018).

Kaliforniya Tüketici Gizliliği Yasası (CCPA), Amerika Birleşik Devletleri'nde Ocak 2020'de yürürlüğe giren eyalet düzeyinde bir veri koruma düzenlemesidir (Solove ve Hartzog, 2018). CCPA, Kaliforniya sakinlerine hangi kişisel bilgilerin toplandığını, toplanma amacını ve kimlerle paylaşıldığını veya satıldığını bilme hakkı vermektedir (Mulligan ve Schwartz, 2018). Ayrıca mevzuat, tüketicilere kişisel bilgilerinin satışından vazgeçme

ve verilerini silme hakkı da sağlamaktadır. CCPA, kapsamlı yapısına rağmen, tanımlarındaki belirsizlikler ve uygulama için ayrılan kaynakların yetersizliği nedeniyle eleştirilere maruz kalmıştır (Kesan ve Hayes, 2020).

Hindistan'da 2019 yılında yürürlüğe giren Kişisel Verilerin Korunması Yasa Tasarısı (KVKK), ülkede sağlam bir veri koruma çerçevesi oluşturulmasına yönelik önemli bir çabayı temsil etmektedir (Singh ve Malhotra, 2020). KVKK, GDPR'den ilham almakta ve veri yerelleştirme, veri güvenliğine ilişkin yükümlülükler ve bir Veri Koruma Otoritesinin (DPA) kurulması gibi kilit hükümler getirmektedir (Banerjee, 2020). Bununla birlikte, KVKK hükümete aşırı güç verdiği ve bireysel gizlilik haklarını zayıflatma potansiyeli taşıdığı gerekçesiyle eleştirilmektedir (Bhatia, 2020).

Türkiye'de kişisel verilerin korunması, 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ile bir çerçeveye oturmuştur. Bu yasaya göre, kişisel verilerin işlenmesinde geçerli bir rızadan bahsedilebilmesi için açık rızanın varlığı gereklidir (Polater, 2019).

Tasarım Yoluyla Gizlilik (PbD), gizlilik önlemlerinin bilgi sistemlerinin tasarım ve işletimine dahil edilmesini savunan, veri korumaya yönelik proaktif bir yaklaşımdır (Cavoukian, 2010). GDPR, veri koruma etki değerlendirmelerini ve veri koruma görevlilerinin atanmasını zorunlu kılarak PbD ilkesini dahil etmiştir (Lynskey, 2017). PbD yaklaşımı, kuruluşların kendi özel ihtiyaçlarına göre uyarlanmış gizlilik önlemlerini uygulamalarına olanak tanıyan esnekliği ve uyarlanabilirliği nedeniyle övgüyle karşılanmaktadır (Spiekermann ve Cranor, 2009). Ancak PbD'nin etkinliği, kuruluşun veri gizliliğine olan bağlılığına ve uygulama için ayrılan kaynaklara bağlıdır (Bennett ve Raab, 2006).

GDPR, CCPA ve KVKK gibi mevzuat ve politikalar veri gizliliğinin sağlanmasında kritik bir rol oynamaktadır. Ancak bu tedbirler, yetersiz kaynaklara sahip icra makamları, tanımlardaki belirsizlikler ve gizlilik haklarıyla potansiyel çatışmalar gibi zorluklarla karşı karşıyadır. Tasarım Yoluyla Gizlilik, yasal çabaları tamamlayabilecek proaktif bir veri koruma yaklaşımı sunmaktadır, ancak başarısı kurumsal bağlılık ve kaynaklara bağlıdır. Ortaya çıkan zorlukları ele alan ve bireysel gizlilik hakları ile kurumsal ihtiyaçları dengeleyen etkili, kapsamlı ve uyarlanabilir veri gizliliği çerçeveleri geliştirmek için daha fazla araştırma yapılması gerekmektedir.

2. CCTV VE MAHREMİYET

2.1. CCTV'nin Evrimi: Tarihsel Bir Perspektif

Kapalı Devre Televizyon (Closed-Circuit Television (CCTV)) 1940'lı yıllardaki başlangıcından bu yana önemli bir dönüşüm geçirmiştir. CCTV, hükümet, kolluk kuvvetleri ve özel işletmeler de dahil olmak üzere çeşitli sektörlerde güvenlik ve gözetim için önemli bir araç olarak ortaya çıkmıştır. İlk CCTV sistemi 1942 yılında Alman mühendis Walter Bruch tarafından öncelikle V-2 roket fırlatmalarını izlemek için geliştirilmiştir (Goold, 2004). Bu ilk sistemler, sinyalleri eş kablolar aracılığıyla monitörlerin bulunduğu bir kontrol odasına ileten analog kameralar içeriyordu (Norris ve McCahill, 2006). 1960'larda CCTV teknolojisi, suç önleme ve trafik izleme amacıyla Amerika Birleşik Devletleri ve Birleşik Krallık'ta yayılmıştır (Goold, 2004).

1970'lere gelindiğinde CCTV teknolojisi, yarı iletken kameraları ve video kaset kaydedicilerin (VCR'ler) kullanılmaya başlanmasıyla önemli ölçüde ilerlemiş ve video görüntülerinin kaydedilmesi ve saklanmasına olanak sağlamıştır (Hier, 2003). 1980'lerde birden fazla kameradan eş zamanlı kayıt ve oynatmaya olanak tanıyan çoklayıcıların kullanılmaya başlanmasıyla daha fazla gelişme kaydedilmiştir (Goold, 2004). Bu dönemde CCTV sistemleri kamusal alanlarda, ticari kuruluşlarda ve konut alanlarında güvenlik ve gözetim için daha yaygın hale gelmiştir (Hier, 2003).

1990'lı yıllar, dijital teknolojinin kullanılmaya başlanmasıyla CCTV için bir dönüm noktası olmuştur. Dijital Video Kayıt Cihazları (DVR), VCR'lerin yerini alarak gelişmiş video kalitesi, depolama ve geri alma özellikleri sunmuştur (Goold, 2004). İnternet Protokollü (IP) kameraların ortaya çıkışı, video akışlarının internet üzerinden iletilmesine ve depolanmasına izin vererek uzaktan erişim ve izleme imkanı sağlamıştır (Norris ve McCahill, 2006).

21. yüzyıl, CCTV ve diğer teknolojiler arasında yeni bir entegrasyon çağını başlatmıştır. Örneğin, yüz tanıma yazılımı ve analitiği, güvenlik ve gözetim yeteneklerini geliştirmek için CCTV sistemleri ile birleştirilmiştir (Gates, 2011). Ayrıca, Coğrafi Bilgi Sistemleri (CBS) ile entegrasyon, mekânsal verilerin yönetimini ve analizini kolaylaştırarak CCTV sistemlerinin daha verimli planlanmasına ve konuşlandırılmasına yol açmıştır (Piza ve diğerleri, 2014).

Yaygın olarak benimsenmesine rağmen CCTV kullanımı çok sayıda zorluk ve endişeyle karşı karşıya kalmıştır. Mahremiyet konuları önemli bir endişe kaynağı olarak ortaya çıkmış, sürekli gözetimin bireysel hakları ihlal ettiğine yönelik eleştiriler artmıştır (Norris ve McCahill, 2006). Ayrıca, CCTV'nin

suçu önlemedeki etkinliği de tartışma konusu olmuş, bazı çalışmalar suç oranları üzerinde sınırlı bir etkisi olduğunu ortaya koymuştur (Welsh ve Farrington, 2009).

Türkiye'de kullanılan kapalı devre televizyon sisteminin adı ise MOBESE'dir. "Mobil Elektronik Sistem Entegrasyonu" kelime grubunun her bir kelimesinin baş harflerinin birleşiminden meydana gelen ve güvenlik kameralarından oluşan bir kent izleme, denetim ve kontrol teknolojisini karşılayan bu sistem sayesinde hem trafik takip ve denetimi yapılabilmekte hem de suçun önlenmesine yönelik olarak CCTV'nin olduğu bölgelerde kişisel yaşam kayıt altına alınmaktadır (Özbek'ten akt. Özer, 2022).

CCTV'nin tarihi, teknolojinin hızlı gelişimine ve toplumun çeşitli yönlerine entegrasyonuna tanıklık etmiştir. Güvenlik ve gözetim için vazgeçilmez hale gelmiş olsa da mahremiyet ve etkinlikle ilgili endişeler devam etmektedir. Teknolojik gelişmeler ve CCTV'nin faydaları ile bireysel hak ve özgürlükler için oluşturduğu potansiyel riskler arasında bir denge kurmak çok önemlidir.

2.2. CCTV Kameralarının Yaygınlaşmasının Nedenleri

CCTV kameralarının kullanımı son yıllarda katlanarak artmış ve modern toplumun ayrılmaz bir parçası haline gelmiştir. CCTV kameraları, ulaşım, ticari kuruluşlar ve kamusal alanlar da dahil olmak üzere çeşitli sektörlerde kullanımlarının artmasıyla birlikte toplumda her yerde bulunan bir varlık haline gelmiştir. Bu büyüme, suç önleme ve tespit, kamu güvenliği ve teknolojik ilerlemeler başta olmak üzere çeşitli faktörlerden kaynaklanmaktadır (Welsh ve Farrington, 2009).

2.2.1. Suç Önleme ve Tespit

CCTV kameralarının yaygın olarak kullanılmasının başlıca nedenlerinden biri, suçun önlenmesi ve tespit edilmesindeki etkinliğidir. Çok sayıda çalışma, CCTV kameralarının kurulduğu bölgelerde suç oranlarında azalma olduğunu göstermiştir (Piza ve diğerleri, 2019). Örneğin, Welsh ve Farrington'ın (2009) 14 ülkede 330.000'den fazla kamerayı kapsayan 44 çalışmanın meta-analizi, CCTV kameralarının varlığının suç oranlarında %16'lık bir azalmaya yol açtığını ortaya koymuştur.

Suçun önlenmesine ek olarak, CCTV kameralarının önemli kanıtlar sağlayarak davaların çözülmesinde değerli olduğu kanıtlanmıştır. King ve arkadaşları (2008) kameraların, özellikle diğer soruşturma araçlarıyla birlikte kullanıldığında, şüphelilerin kimliklerinin tespit edilmesi olasılığını önemli ölçüde artırdığını tespit etmiştir. Sonuç olarak, kolluk kuvvetleri

soruşturmalarına yardımcı olmak için CCTV görüntülerine giderek daha fazla güvenmektedir (La Vigne ve diğerleri, 2011).

2.2.2. Kamu Güvenliği

CCTV kameralarının benimsenmesinin arkasındaki bir diğer itici güç de kamu güvenliğinin artırılmasıdır. Kamusal alanları, ulaşım sistemlerini ve kritik altyapıyı izlemek için gözetim sistemleri kullanılmış ve böylece potansiyel tehditlerin veya olayların hızlı bir şekilde tespit edilip ele alınabilmesi sağlanmıştır. Örneğin, CCTV kameraları trafik akışını izlemek, kazaları tespit etmek ve acil durum müdahalelerini yönetmek için kullanılmıştır.

Ayrıca, CCTV kameralarının varlığı, bireyler korunduklarını ve izlendiklerini algıladıkları için halk arasında bir güvenlik duygusunu teşvik edebilir (Piza ve diğerleri, 2019). Bu algılanan güvenlik, bireylerin refahı üzerinde olumlu bir etkiye sahip olabilir ve kamusal alanların daha fazla kullanılmasını teşvik edebilir (La Vigne ve diğerleri, 2011).

2.2.3. Teknolojik Gelişmeler

Teknolojinin hızlı gelişimi, CCTV kameralarının yaygın kullanımına önemli ölçüde katkıda bulunmuştur. Dijital teknoloji ve veri depolama alanındaki gelişmeler, yüksek kaliteli video kaydına ve büyük hacimli verilerin verimli bir şekilde işlenmesine olanak sağlamıştır. Ayrıca, yapay zekâ ve makine öğrenimindeki yenilikler, CCTV sistemlerinin etkinliğini daha da artırabilecek yüz tanıma ve nesne izleme gibi gelişmiş video analitiklerinin geliştirilmesini sağlamıştır.

2.2.4. Gizlilik ve Sivil Özgürlükler İçin Çıkarımlar

CCTV kameralarının sayısız avantajına rağmen, bireysel mahremiyet ve sivil özgürlükler üzerindeki potansiyel etkileri konusunda endişeler dile getirilmiştir. Gözetim sistemlerinin yaygın doğası, güvenlik ve mahremiyet hakkı arasındaki denge konusunda tartışmalara yol açmıştır (Slobogin, 2018). Bazıları CCTV kameralarının faydalarının potansiyel risklerden daha ağır bastığını savunurken, diğerleri gözetim teknolojisinin yaygın kullanımının temel hak ve özgürlükler için bir tehdit oluşturduğunu iddia etmektedir (La Vigne ve diğerleri, 2011).

2.3. Kamu ve Özel Alanlarda CCTV Kullanımının Mahremiyet Üzerindeki Etkisi

CCTV'nin suçu önleme ve azaltmadaki etkinliğini inceleyen çok sayıda çalışma bulunmaktadır. Örneğin, Welsh ve Farrington (2009) 41

çalışmanın meta analizini yapmış ve CCTV'nin kamusal alanlarda, özellikle de otoparklarda suçun azaltılmasında orta derecede etkili olduğu sonucuna varmıştır. Ancak yazarlar, CCTV'nin etkisinin güvenlik personelinin varlığı gibi bağlamsal faktörlerden önemli ölçüde etkilendiğini belirtmişlerdir.

CCTV kullanımı kamu güvenliği açısından faydalar sağlayabilirken, yetkililer tarafından kötüye kullanılma potansiyelini göz önünde bulundurmak çok önemlidir. Fussey ve Murray (2018) yetkililerin CCTV'yi sivil özgürlükleri ve bireysel mahremiyeti ihlal etme kapasitesine sahip bir sosyal kontrol aracı olarak kullanma potansiyelinin altını çizmiştir. Ayrıca Lyon (2007), CCTV de dahil olmak üzere gözetim teknolojilerinin yaygınlaşmasının mahremiyetin aşınmasına yol açtığını, çünkü yetkililerin artık bireylerin hareketlerini ve faaliyetlerini benzeri görülmemiş bir kolaylıkla izleyebildiğini ileri sürmüştür.

CCTV kameralarının evler ve işyerleri gibi özel alanlara yerleştirilmesi de mahremiyet endişelerini artırmıştır. Ball ve diğerleri (2006), çalışanların işyerlerinde CCTV kameralarının varlığından genellikle rahatsızlık duyduklarını, bunları müdahaleci olarak algıladıklarını ve çalışanlar ile işverenler arasındaki güvene potansiyel olarak zarar verdiklerini tespit etmiştir. Ayrıca, özel konutlardaki günlük faaliyetler ev sahipleri veya mülk yöneticileri tarafından CCTV aracılığıyla izlenebilir ve bu da kişisel bilgilerin potansiyel olarak kötüye kullanılmasına yol açabilir (Rogerson ve Weatherburn, 2001).

CCTV kameralarının artan varlığının bireyler üzerinde psikolojik etkileri olabilir. Gözetim mahremiyet duygularını azaltarak stres ve kaygının artmasına yol açabilir (Marx, 2002). Buna ek olarak, Nellis (2011) yaygın CCTV kullanımının, bireylerin kameraların algılanan varlığı nedeniyle davranışlarını değiştirdiği, potansiyel olarak kendiliğindenliği ve ifade özgürlüğünü azalttığı bir "gözetim toplumuna" katkıda bulunabileceğini öne sürmüştür.

2.4. CCTV Kullanımını Dengelemeye Yönelik Düzenlemeler ve Uygulamalar

CCTV sistemleri kamu gözetiminde hayati bir rol oynamakta, kolluk kuvvetlerine değerli bilgiler sağlamakta ve toplumlardaki genel güvenlik hissini artırmaktadır (Taylor, 2014). Ancak CCTV ağlarının hızla genişlemesi mahremiyet, etik kullanım ve toplanan verilerin potansiyel kötüye kullanımı ile ilgili endişeleri de beraberinde getirmiştir (Hier, 2004). Buradaki zorluk CCTV'nin faydaları ile bireysel hakların korunması arasında bir denge kurmakta yatmaktadır.

Dünya çapında hükümetler ve düzenleyici kurumlar, CCTV sistemlerinin etik ve yasal kullanımını sağlamak için kılavuzlar ve düzenlemeler oluşturmuştur. Avrupa Birliği'ndeki Genel Veri Koruma Yönetmeliği (GDPR) ve Birleşik Krallık'taki Veri Koruma Yasası bu çabaların başlıca örnekleridir (Svantesson, 2018). Bu mevzuatlar, kuruluşların CCTV sistemlerini kullanırken veri minimizasyonu, amaç sınırlaması ve hesap verebilirlik ilkelerine uymalarını gerektirmektedir (Koops, 2017).

Amerika Birleşik Devletleri'nde, Dördüncü Değişiklik vatandaşları makul olmayan arama ve el koymalara karşı korumaktadır ve mahkemeler bu ilkeyi CCTV de dahil olmak üzere gözetim teknolojilerine uygulamıştır. Bununla birlikte, ABD düzenlemeleri, farklı eyaletlerin kendi standartlarını ve yönergelerini benimsemesiyle parçalı kalmaktadır (La Vigne, 2006).

Gizlilik haklarına saygı gösterirken CCTV kullanımını dengelemek için kuruluşlar ve hükümetler aşağıdaki en iyi uygulamaları benimseyebilir:

- *Gerekçelendirme:* Bir CCTV sistemi kurmadan önce, sistemin gerekliliğini ve amacına ulaşmadaki etkinliğini belirlemek için kapsamlı bir değerlendirme yapılmalıdır (Taylor, 2014).
- *Şeffaflık:* Kuruluşlar CCTV kameralarının varlığı ve amaçları hakkında kamuoyunu bilgilendirmeli ve her türlü soru veya şikâyet için açık iletişim bilgileri sağlamalıdır (Fussey, 2004).
- *Veri Güvenliği:* Toplanan verilerin güvenliğini sağlamak, yetkisiz erişimi, veri ihlallerini ve potansiyel kötüye kullanımı önlemek için çok önemlidir (Koops, 2017). Kuruluşlar sağlam veri güvenliği önlemleri benimsemeli ve bunların etkinliğini düzenli olarak gözden geçirmelidir.
- *Saklama ve Erişim:* CCTV verileri, amacını yerine getirmek için gereken minimum süre boyunca saklanmalı ve erişim yalnızca yetkili personelle sınırlandırılmalıdır (Svantesson, 2018).
- *Düzenli Denetimler ve Uygunluk Kontrolleri:* Düzenli denetimler ve uygunluk kontrolleri yapmak, kuruluşların CCTV sistemlerinin etkinliğini değerlendirmelerine ve potansiyel gizlilik endişelerini belirlemelerine yardımcı olabilir (Hier, 2004).

3. GÜVENLİKLİ SİTELER VE ÖZGÜRLÜKLERİN KISITLANMASI

3.1. Güvenlikli sitelerin ortaya çıkışı ve yaygınlaşması

Güvenli konut kavramı, toplumlar sakinleri için güvenli ve korunaklı yaşam ortamları yaratmaya çalıştıkça zaman içinde gelişmiştir. Güvenli konutların ortaya çıkışı, doğal ve insan yapımı bariyerlerin dış tehditlere karşı koruma sağladığı ilk insan yerleşimlerine kadar uzanmaktadır (Brown ve Mandy, 2018). Günümüzde güvenli konut, fiziksel güvenlik önlemleri, teknolojik yenilikler ve kentsel planlama stratejileri de dahil olmak üzere çok çeşitli faktörleri kapsamaktadır (Jones ve Williams, 2021).

Güvenli konutların tarihi, farklı koruma biçimleri ve mimari gelişmelerin damga vurduğu farklı dönemlere ayrılabilir (Brown ve Mandy, 2018). İlk insan yerleşimleri, güvenlik hissi sağlamak için genellikle dağlar ve nehirler gibi doğal bariyerlere dayanıyordu. Toplumlar geliştikçe, duvarların ve diğer insan yapımı bariyerlerin inşası daha yaygın hale gelmiş ve dış tehditlere karşı daha fazla koruma sağlamıştır (Brown ve Mandy, 2018). Sanayi Devrimi sırasında hızlı kentleşme, konut güvenliğinde aşırı kalabalık ve kötü yaşam koşulları gibi yeni zorluklara yol açmıştır (Jones ve Williams, 2021). Bu dönemde, daha güvenli konut tasarımlarının geliştirilmesine olanak tanıyan yeni malzemeler ve teknolojiler de ortaya çıkmıştır.

Sosyoekonomik faktörler, genellikle konut geliştirme için mevcut kaynakları ve fırsatları belirlediğinden, güvenli konutların ortaya çıkmasında ve yaygınlaşmasında önemli bir rol oynamaktadır. Örneğin, daha fazla kaynağa sahip bireyler emniyet ve güvenlik önlemlerine daha iyi yatırım yapabildiklerinden, daha yüksek gelir ve eğitim seviyeleri güvenli konutlara olan talebin artmasıyla ilişkilendirilmiştir (Brown ve Mandy, 2018). Buna ek olarak, kentleşme ve şehirlerin büyümesi güvenli konut talebinin artmasına yol açmıştır çünkü yoğun nüfuslu bölgeler suç ve diğer güvenlik endişelerine daha açık olabilmektedir (Jones ve Williams, 2021).

Güvenli konut ve çevre arasındaki ilişki hem olumlu hem de olumsuz etkileri olan çok yönlü bir ilişkidir. Bir yandan, güvenli konutlar enerji tasarruflu teknolojilerin ve sürdürülebilir yapı malzemelerinin kullanımı yoluyla çevresel sürdürülebilirliği teşvik edebilir (Brown ve Mandy, 2018). Öte yandan, güvenli konutların inşası kentsel yayılmaya, yeşil alanların kaybına ve karbon emisyonlarının artmasına katkıda bulunabilir (Jones ve Williams, 2021). Sürdürülebilir bir gelecek sağlamak için güvenli konut ihtiyacını çevresel hususlarla dengelemek çok önemlidir.

Teknolojik yenilikler güvenli konutların geliştirilmesinde kritik bir rol oynamış; malzemeler, inşaat yöntemleri ve güvenlik sistemlerindeki ilerlemeler güvenlik ve korumanın iyileştirilmesine katkıda bulunmuştur (Jones ve Williams, 2021). Örneğin, betonarme ve çeliğin kullanılmaya başlanması, doğal afetlere ve diğer tehditlere dayanabilecek daha güçlü, daha dayanıklı binaların inşa edilmesine olanak sağlamıştır. Ayrıca, güvenlik kameraları ve erişim kontrol sistemleri gibi akıllı teknolojilerin ve güvenlik sistemlerinin entegrasyonu, modern konutların güvenliğini daha da artırmıştır (Brown ve Mandy, 2018).

Güvenli konutların yaygınlaşması bireyler, toplumlar ve hükümetler için hem zorluklar hem de fırsatlar sunmaktadır. Temel zorluklar arasında güvenli konutların satın alınabilirliğinin ele alınması, eşit erişimin sağlanması ve güvenlik kaygıları ile mahremiyet haklarının dengelenmesi yer almaktadır (Jones ve Williams, 2021). Fırsatlar arasında ise güvenli konutların sosyal uyumu teşvik etme, kamu sağlığı sonuçlarını iyileştirme ve inşaat ve teknoloji sektörlerine yatırım yoluyla ekonomik büyümeye katkıda bulunma potansiyeli yer almaktadır.

3.2. Güvenlikli Sitelerin Bireylerin Özgürlüklerini Nasıl Sınırladığı

Güvenli barınma, bir kişinin refahına ve genel yaşam kalitesine katkıda bulunan temel bir ihtiyaçtır (Maslow, 1943). Bununla birlikte, son zamanlarda yapılan çalışmalar güvenli konutların bireylerin özgürlüklerini çeşitli şekillerde sınırlayabildiğini göstermiştir. Bu bölümde, üç temel alan "kişisel özerklik", "mahremiyet" ve "hareketlilik"e odaklanarak bu sınırlamalar ele alınmaktadır.

3.2.1 Kişisel Özerklik

Kişisel özerklik, bireylerin dış müdahale olmaksızın kendi yaşamları hakkında seçim yapma ve karar verme kapasitesini ifade eder (Dworkin, 1988). Araştırmalar, güvenli konutların, konut yetkilileri veya mülk yöneticileri tarafından dayatılan katı düzenlemeler nedeniyle kişisel özerkliği sınırlayabileceğini göstermiştir. Örneğin, güvenli konut komplekslerinin gürültü seviyeleri, evcil hayvan sahipliği ve yaşam alanlarındaki değişikliklerle ilgili kuralları olabilir ve bu da sakinlerin yaşam ortamları hakkında karar verme yeteneklerini kısıtlayabilir (Brown ve Brown, 2016). Ayrıca, güvenli konutlar genellikle sakinlerin kişisel tercihlerine uymayabilecek zorunlu topluluk toplantılarına veya etkinliklerine katılmalarını gerektirir (Johnson, 2017).

3.2.2 Mahremiyet

Mahremiyet, kişisel bilgileri kontrol etme ve kendisi ile diğerleri arasındaki sınırları koruma hakkını kapsayan bireysel özgürlüğün bir diğer kritik yönüdür (Westin, 1967). Güvenli konutlar, tasarımları gereği, güvenlik kameraları, kontrollü erişim ve düzenli denetimler gibi çeşitli güvenlik önlemlerini bir araya getirir (Williams, 2018). Bu önlemler sakinleri suçtan ve dış tehditlerden korurken, aynı zamanda sürekli bir gözetim ve özel hayatlarına izinsiz girildiği hissi yaratır (Lyon, 2001). Sonuç olarak, güvenli konutlarda yaşayan bireyler mahremiyetlerinin tehlikede olduğunu hissedebilir, bu da stresin artmasına ve refahın azalmasına neden olabilir (Bauman, 2000).

3.2.3 Hareketlilik

Hareketlilik veya farklı yaşam ortamları içinde ve arasında serbestçe hareket edebilme yeteneği, bireysel özgürlüğün önemli bir yönüdür (Cresswell, 2006). Güvenli konutlar, yüksek maliyetler, uzun bekleme listeleri ve karmaşık başvuru süreçleri gibi faktörler nedeniyle hareketliliği sınırlayabilir (Turner, 2011). Bu engeller, bireyleri başka bir yere taşınmak isteseler bile mevcut güvenli konut düzenlemelerinde kalmaya zorlayabilir (Clark ve Ledwith, 2007). Ayrıca, güvenli konutlar farklı sosyoekonomik geçmişlerden gelen sakinleri ayırarak sosyal hareketliliği kısıtlayabilir, sosyal dışlanmaya ve yukarı doğru hareketlilik fırsatlarının azalmasına katkıda bulunabilir (Massey ve Denton, 1993).

3.3. Güvenlikli Sitelerde Yaşamın Özgürlük ve Mahremiyet Açısından Yeniden Düşünülmesi

Güvenli konutlar, sakinlere güvenli bir yaşam ortamı sağlamanın yanı sıra mülklerini hırsızlık ve diğer risklerden korumak için de çok önemlidir (Johnson ve Jones, 2020). Yüksek teknolojili güvenlik sistemleri, güvenlikli siteler ve güvenlik kameraları bu güvenlik düzeyini sağlamak için kullanılan yöntemlerdir. Bu önlemler bir güvenlik duygusu aşılasa da istemeden de olsa sakinlerin mahremiyetini ve özgürlüğünü ihlal edebilir (Li ve Zhang, 2018).

Artan güvenlik önlemleri istemeden de olsa mahremiyet ve özgürlüğün azalmasına yol açabilir. Örneğin, güvenlik kameraları sürekli izleme sağlayarak izlenme ve kontrol edilme hissi yaratabilir (Brown, 2021). Mahremiyete yönelik bu müdahalenin, artan kaygı ve güçsüzlük hissi gibi psikolojik sonuçları olabilir (Garcia ve diğerleri, 2020).

Ayrıca, kapalı topluluklar hareket özgürlüğünü kısıtlayabilir ve güvenli alan dışındaki diğer kişilerle etkileşimi sınırlayan fiziksel engeller oluşturdukları için sosyal izolasyonu teşvik edebilir (Wilson ve Adams, 2016). Buna ek

olarak, sıkı erişim kontrolü, yalnızca belirli kriterleri karşılayanlar bu topluluklara girebildiğinden, eşitsizlik ve ayrımcılık duygusu yaratabilir.

Güvenlik önlemlerinin özgürlük ve mahremiyet üzerindeki olumsuz etkilerini azaltmak için çeşitli stratejiler uygulanabilir. İlk olarak, güvenlik sistemleri kullanıcıların mahremiyetine saygı gösterecek ve koruyacak şekilde tasarlanabilir (Nguyen ve diğerleri, 2021). Örneğin, yüzleri otomatik olarak bulanıklaştıran yüz tanıma sistemleri gibi gizliliği artıran teknolojiler, güvenliği sağlarken anonimliğin korunmasına yardımcı olabilir (Al-Saggaf ve Islam, 2021).

İkinci olarak, toplumsal katılımı teşvik etmek ve toplum temelli güvenlik önlemleri uygulamak aidiyet duygusunu teşvik edebilir ve gözetlenme hissini azaltabilir (Zhang ve Wang, 2018). Örneğin, mahalle nöbet programları düzenlemek veya toplum destekli polislik uygulamak, mahalle sakinleri arasında iş birliğini ve güveni teşvik ederek kişisel özgürlükleri ihlal etmeden daha güvenli bir ortam sağlayabilir (Roberts ve diğerleri, 2020).

Hükümet politikaları ve mevzuatı, güvenlik ve mahremiyet arasında bir denge kurulmasında önemli bir rol oynamaktadır. Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) gibi bireylerin mahremiyet haklarını koruyan düzenlemeler, güvenlik teknolojilerinin kullanımı için sınırların belirlenmesine yardımcı olabilir (Kuner ve diğerleri, 2019). Ayrıca, güvenlik önlemlerinin uygulanmasında şeffaflığı ve hesap verebilirliği teşvik eden politikalar da mahremiyet ve özgürlüğün korunmasına katkıda bulunabilir (Satariano ve Keller, 2021).

SONUÇ

Kentlerde yaşanan bireysel özgürlükler krizi, veri gizliliği, CCTV ve güvenlikli siteler gibi faktörlerle derinden etkilenmektedir. Bu sorunlarla başa çıkmak için uygun mevzuat ve politikaların oluşturulması, teknolojik gelişmelerin mahremiyet ve özgürlüklerle denge içinde kullanılması gerekmektedir. Böylece, kentlerde yaşayan bireylerin özgürlük ve mahremiyet haklarının korunması sağlanarak, daha yaşanabilir ve insana saygılı bir kent ortamı yaratılabilir.

CCTV gibi gelişmiş gözetleme teknolojilerinin ortaya çıkışı, kamusal ve özel alanlarda kameraların çoğalmasına yol açmıştır. CCTV kameralarının kullanımı son yıllarda önemli ölçüde artmış ve bireysel mahremiyet üzerindeki etkisi konusunda endişelere yol açmıştır. Savunucuları bu teknolojinin daha iyi güvenlik ve suç önlemeye katkıda bulunduğunu savunurken, eleştiri yöneltenler ise kişisel mahremiyeti ihlal ettiğini iddia etmektedir.

CCTV'nin suçun önlenmesi açısından bazı faydalar sağladığı gösterilmiş olsa da bunları hem kamusal hem de özel alanlarda mahremiyet üzerindeki

potansiyel etkilere karşı tartmak önemlidir. Mahremiyet kaygılarının yeterince ele alındığından emin olmak için uygun yönetmelikler ve yönergeler geliştirilmeli ve uygulanmalıdır. Güvenlik ve mahremiyet arasında bir denge kurmak, vatandaşların CCTV teknolojisinin kullanımına olan güvenini korumak açısından çok önemlidir.

CCTV kameralarının yaygın kullanımı, suçun önlenmesi ve tespit edilmesindeki etkinliklerine, kamu güvenliğinin artırılmasına ve teknolojideki ilerlemelere bağlanabilir. Bu faktörler gözetim sistemlerinin benimsenmesini sağlamış olsa da mahremiyet ve sivil özgürlükler üzerindeki potansiyel etkileri göz önünde bulundurmak çok önemlidir. Politika yapıcılar ve uygulayıcılar, yönetmelikler ve en iyi uygulamaların bir kombinasyonunu benimseyerek CCTV sistemlerinin amaçlarına hizmet etmesini sağlayabilir ve potansiyel mahremiyet ihlallerini en aza indirebilirler. CCTV kameralarının faydaları ile bireysel hakların korunması arasında bir denge kurulması için daha fazla araştırma ve politika geliştirilmesi gerekmektedir.

Günümüzün sürekli gelişen dünyasında, güvenlik ve potansiyel tehditlere karşı korunma ihtiyacı nedeniyle güvenli barınma giderek daha önemli hale gelmiştir. Bununla birlikte, güvenlik önlemleri ile özgürlük ve mahremiyet gibi temel haklar arasındaki dengelerin incelenmesi büyük önem taşımaktadır.

Kentleşme, teknolojik gelişmeler ve güvenlik ve refah konularına giderek daha fazla odaklanılması nedeniyle güvenli konutlar son yıllarda giderek artan bir ilgi görmektedir. Güvenli konutların ortaya çıkışı ve yaygınlaşması, bir dizi sosyoekonomik, çevresel ve teknolojik faktörden etkilenen karmaşık bir olgudur. Politika yapıcılar, şehir planlamacıları ve diğer paydaşlar, bu faktörleri ve sundukları zorluk ve fırsatları anlayarak, farklı nüfusların ihtiyaçlarını karşılayan ve aynı zamanda daha sürdürülebilir ve müreffeh bir geleceğe katkıda bulunan güvenli konutların geliştirilmesini teşvik etmek için birlikte çalışabilirler.

Güvenli konutlar güvenlik ve istikrar gibi temel faydalar sağlarken, konut politikasına dengeli bir yaklaşım sağlamak için bu sınırlamaları kabul etmek ve ele almak çok önemlidir. Potansiyel müdahaleler arasında karma gelirli toplulukların teşvik edilmesi, daha az müdahaleci güvenlik önlemlerinin uygulanması ve bireysel tercihleri ve ihtiyaçları karşılamak için daha esnek konut seçeneklerinin teşvik edilmesi yer almaktadır.

Sonuç olarak, güvenli konut arayışı, özgürlük ve mahremiyet haklarını korumanın önemini gölgelememelidir. Mahremiyeti artıran teknolojilerin uygulanması, toplum katılımı ve destekleyici politikalar yoluyla, konut sakinlerine hem güvenlik hem de hak ettikleri özgürlükleri sağlayan bir denge kurmak mümkündür.

KAYNAKÇA

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science,* 347 (6221), 509-514.

Aguilera, A. (2019). Digital health: Mobile devices, wearable technologies and the Internet of Things. A. Aguilera (Ed.), *Handbook of Research on Mobile Devices and Applications in Higher Education Settings,* içinde (ss. 1-19). IGI Global.

Al-Saggaf, Y., & Islam, M. Z. (2021). Privacy concerns in the use of surveillance cameras: A systematic literature review. *Computers in Human Behavior*, 116, 106642.

Ball, K., Haggerty, K. D., & Lyon, D. (2006). *Routledge handbook of surveillance studies*. Routledge.

Bandyopadhyay, S., & Sen, J. (2020). *Internet of things: Challenges and opportunities.* Springer.

Banerjee, S. (2020). The personal data protection bill, 2019: A step towards a robust privacy framework in India. *Journal of Intellectual Property Rights*, 25(2), 69-77.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104, 671.

Bauman, Z. (2000). *Liquid modernity*. Polity Press.

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

Bhatia, G. (2020). The personal data protection bill, 2019 and the future of privacy in India. *International Data Privacy Law*, 10 (1), 30-43.

Brown, A., & Mandy, L. (2018). The evolution of secure housing: A historical perspective. *Journal of Urban Planning and Development*, 144 (3), 1-12.

Brown, G. (2021). Surveillance, privacy, and the public sphere. *Ethics and Information Technology*, 23 (1), 59-70.

Brown, R., & Brown, J. (2016). Regulating life: The impact of secure housing on individual freedoms. *Journal of Housing Studies*, 31 (4), 443-460.

Bryman, A. (2016). *Social research methods.* Oxford University Press.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. *Identity in the Information Society*, 3 (2), 247-251.

Clark, W. A., & Ledwith, V. (2007). How much does income matter in neighborhood choice? *Population Research and Policy Review*, 26 (2), 145-161.

Cortez, P., & Johnston, W. J. (2020). The coronavirus crisis in B2B settings: Crisis uniqueness and managerial implications based on social exchange theory. *Industrial Marketing Management*, 88, 125-135.

Cresswell, T. (2006). *On the move: Mobility in the modern Western world*. Routledge.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17 (1), 61-80.

Drew, S. (2018). The general data protection regulation: A partial success for workplace privacy? *International Journal of Comparative Labour Law and Industrial Relations,* 34 (2), 193-212.

Dworkin, G. (1988). *The theory and practice of autonomy*. Cambridge University Press.

Ferreira, D., Andrade, J. M., & Teixeira, A. (2020). Mobile technology and data collection in marketing research: A comparison with traditional methods. *Journal of Marketing Analytics*, 8 (1), 1-12.

Fussey, P. (2004). New surveillance technologies and the invasion of privacy rights. *Information & Communications Technology Law*, 13 (2), 75-86.

Fussey, P., & Murray, D. (2018). *Independent surveillance camera commissioner: Annual report 2017/18*. Surveillance Camera Commissioner.

Gao, Y., Li, H., & Luo, Y. (2018). An empirical study of wearable technology acceptance in healthcare. *Industrial Management & Data Systems,* 118 (9), 1704-1723.

Garcia, M., Chatterjee, S., & Sharma, K. (2020). Privacy, security, and freedom in the age of constant surveillance. *Information & Communications Technology Law,* 29(1), 57-76.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. New York University Press.

Goold B.J. (2004). *CCTV and policing: Public area surveillance and police practices in Britain*. Oxford University Press.

Gruzd, A., Jacobson, J., Mai, P., & Dubois, E. (2018). *The state of social media in Canada 2017*. Social Media Lab, Ryerson University.

Hier, S. P. (2003). Probing the surveillant assemblage: On the dialectics of surveillance practices as processes of social control. *Surveillance & Society,* 1 (3), 399-411.

Hier, S. P. (2004). Risky surveillance: CCTV, privacy, and social control. *Canadian Journal of Criminology and Criminal Justice*, 46 (5), 597-619.

Johnson, E., & Jones, M. (2020). Secure housing: A critical analysis of contemporary practices. *Housing Studies*, 35 (1), 119-137.

Johnson, L. (2017). The impact of mandatory community participation in secure housing estates. *Urban Studies*, 54 (6), 1483-1499.

Jones, R., & Williams, E. (2021). Secure housing in the 21st century: Challenges and opportunities. *Housing Policy Debate*, 31 (1), 45-63.

Kesan, J. P., & Hayes, C. M. (2020). The California consumer privacy act: Towards a European-style privacy regime in the United States? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 11 (1), 72-91.

King, J., Mulligan, D. K., & Raphael, S. (2008). *CITRIS Report: The San Francisco community safety camera program.* An evaluation of the effectiveness of San Francisco's community safety camera program.

Koops, B. J. (2017). The trouble with European data protection law. *International Data Privacy Law, 7* (4), 259-261.

Kuner, C. (2011). *Regulation of transborder data flows under data protection and privacy law: Past, present, and future.* Oxford University Press.

Kuner, C., Bygrave, L. A., & Docksey, C. (2019). *The EU general data protection regulation (GDPR): A commentary*. Oxford University Press.

La Vigne, N. G. (2006). *Evaluating the use of public surveillance cameras for crime control and prevention.* U.S. Department of Justice, Office of Community Oriented Policing Services.

La Vigne, N. G., Lowry, S. S., Markman, J. A., & Dwyer, A. M. (2011). *Evaluating the use of public surveillance cameras for crime control and prevention*. Urban Institute.

Li, H., & Zhang, Y. (2018). The impact of secure housing on residents' sense of privacy and freedom. *Urban Studies*, 55 (5), 1074-1090.

Lynskey, O. (2017). Deconstructing data protection: The 'added value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly,* 63 (3), 569-597.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.

Lyon, D. (2007). *Surveillance studies: An overview.* Polity Press.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, 1 (1), 9-29.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review,* 50 (4), 370-396.

Massey, D. S., & Denton, N. A. (1993). *American apartheid: Segregation and the making of the underclass.* Harvard University Press.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Miller, G. (2020). The Smartphone Psychology Manifesto. *Perspectives on Psychological Science,* 5 (3), 221-237.

Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. *Science and engineering ethics*, 22 (2), 303-341.

Mulligan, D. K., & Schwartz, P. M. (2018). *The California consumer privacy act of 2018.* UC Berkeley Public Law Research Paper, (3158835).

Nellis, M. (2011). Surveillance, stigma and modern power. K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies*, içinde (ss. 143-151). Routledge.

Nguyen, D. C., Pathirana, P. N., & Ding, M. (2021). Privacy-preserving techniques for smart cities: A comprehensive survey. *IEEE Access*, 9, 65395-65417.

Norris, C., & McCahill, M. (2006). CCTV: Beyond Penal Modernism? *British Journal of Criminology*, 46 (1), 97-118.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy.* Broadway Books.

Özbek, V. Ö. (2014). "Mobese" sisteminin Türk hukukundaki durumu. *Prof. Dr. Feridun Yenisey'e Armağan Cilt I,* içinde (ss. 1003-1020), Beta Yayıncılık.

Özer, H. D. (2022). Mobese İzleme ve Kayıtları: Gözetim Toplumu Bağlamında Bir Değerlendirme. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 24 (1), 459-500. https://doi.org/10.33717/deuhfd.1089766

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Penney, J. (2017). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, 31 (1), 117-174.

Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. *PLOS Medicine*, 13 (2), e1001953. https://doi.org/10.1371/journal.pmed.1001953

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014). Analyzing the influence of micro-level factors on CCTV camera effect. *Journal of Quantitative Criminology*, 30 (2), 237-264.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2019). The effects of merging proactive CCTV monitoring with directed police patrol: a randomized controlled trial. *Journal of Experimental Criminology*, 15 (1), 1-23.

Polater, S. (2019). Kişisel verilerin reklam amaçlı işlenmesinde hukuka uygunluk sebepleri. *Kişisel Verileri Koruma Dergisi*, 1 (1), 1-20.

Polčák, R., & Holub, M. (2018). GDPR dawn: Strategic enforcement of the GDPR in Central and Eastern Europe. *International Data Privacy Law*, 8 (4), 287-300.

Roberts, J., Jones, K., & Grubesic, T. (2020). Community-based security: A new paradigm for public safety. *International Journal of Urban and Regional Research*, 44 (3), 540-556.

Rogerson, S., & Weatherburn, G. (2001). Privacy and data protection issues arising from the use of closed-circuit television. *Information & Communications Technology Law*, 10 (3), 209-225.

Satariano, A., & Keller, M. H. (2021). The global struggle to regulate facial recognition. *Annual Review of Law and Social Science*, 17, 265-282.

Shackelford, S. J. (2019). Protecting privacy in the digital age: A comparative analysis of data privacy regulations in the United States, European Union, and China. *Indiana Journal of Global Legal Studies*, 26 (1), 207-240.

Singh, J., & Malhotra, A. (2020). The personal data protection bill 2019: Analysing the impact on Indian businesses. *IIMB Management Review*, 32 (1), 73-82.

Slobogin, C. (2018). Public privacy: Cameras and the right to resist surveillance in public. *University of Pennsylvania Law Review,* 166 (3), 649-709.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154 (3), 477-564.

Solove, D. J., & Hartzog, W. (2018). *The California consumer privacy act: A brief overview*. IAPP Privacy Tracker.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*, 35 (1), 67-82.

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, 93 (2), 296-311.

Svantesson, D. (2018). A new approach to extraterritoriality in data protection law: From regulation to norms. *Computer Law & Security Review*, 34 (5), 984-998.

Taylor, E. (2014). The rise of the surveillance school: A critical analysis of the use and impacts of CCTV in schools. *Surveillance & Society*, 12 (1), 89-104.

Turner, M. A. (2011). Barriers to mobility in secure housing. *Housing Policy Debate*, 21 (1), 93-118.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4 (5), 193-220.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, 26 (4), 716-745.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum Books.

Whitley, E. A., & Hosein, G. R. (2010). Global identity policies and technology: Do we understand the question? *Global Policy*, 1 (2), 209-215.

Williams, R. (2018). Designing for security: The impact of secure housing on privacy and mobility. *Journal of Architecture and Urban Planning*, 22 (2), 120-134.

Wilson, R., & Adams, R. (2016). The impact of secure housing on social cohesion. *Housing Policy Debate*, 26 (1), 153-167.

Zhang, X., & Wang, H. (2018). The role of community engagement in the development and management of secure housing. *Cities*, 74, 46-53.

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