AKILLI KENTLERDE VERİNİN GİZLİLİĞİ VE GÜVENLİĞİ: İLKELER VE YAKLAŞIMLAR

Levent MEMİŞ[*], Melikali GÜÇ[**]

Öz

Teknolojik gelişmelerin dinamik ortamında ortaya çıkan yenilikler, toplumsal ve ekonomik alanlarda yeni durumları gündeme getirmektedir. Kentler, bu gelişmelerin yansıdığı önemli alanlardan biridir. Bu noktada akıllı kent ve büyük veri kavramları gündeme gelmekte, bu gelişmeler kentsel alanda sunulan hizmetlere yeni biçimler kazandırmaktadır. Fakat bu gelişmeler beraberinde bazı olumsuzlukları da getirmektedir. İfade edilenler kapsamında araştırmanın amacı; akıllı kentlerde ortaya çıkan büyük verinin gizliliğini, güvenliğini güçleştiren ve bunları tehdit eden unsurları ele alarak ortaya çıkan olumsuzlukları gidermek amacıyla gündeme gelen ilkeler ve yaklaşımları incelemektir. Temelde yanıt aranan soru: "Akıllı kentlerin önemli bir parçası olan, büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla hangi ilkeler ve yaklaşımlar öne çıkmaktadır?". Sorunun cevabı ilgili literatür, hukuki düzenlemeler ve uluslararası oluşumların aldığı kararlar üzerinden aranmaktadır. Genel sonuçlara göre bazı düzenlemeler (AB Veri Koruma Tüzüğü gibi) öne çıkmakla birlikte, veri güvenliği konusunda küresel düzeyde üzerinde uzlaşı sağlanan standartların olmadığı anlaşılmaktadır. Fakat bazı ilkelerin ve yaklaşımların önem kazanmakta olduğu tespit edilmiştir. Çalışmanın sonunda, elde edilen sonuçlara göre politika önerileri sunulmuştur.

Anahtar Kelimeler: *Akıllı Kent, Büyük Veri, Açık Veri, Veri Gizliliği ve Güvenliği.*

DATA SECURITY IN SMART CITIES: PRINCIPLES AND APPROACHES

Abstract

Innovations emerging in the dynamic environment of technological developments lead to new situations in social and economic fields. Cities are one of the important areas where these developments are reflected. Thus, smart cities and big data concepts come up and these developments cause changes in services provided in cities. However, these developments bring along some negativities, as well. The main purpose of this study is to examine the approaches and principles that have come to fore in order to ensure the privacy and security of big data in smart cities. Basically, the answer to this question is sought: what principles, approaches and practices come to the forefront in order to ensure the confidentiality and security of big data that is an important part of smart cities? The answer is sought through the relevant literature, legal regulations and international decisions. According to the general results of the study, it is understood that there are not any consensual standards on data security at global level. However, some regulations draw attention. At this point, the "General Data Protection Regulation (GDPR)" which came into force in 2018 is important. However, some principles and approaches are gaining importance. At the end of the study, some suggestions about policies are made according to the results obtained.

Keywords: *Smart City, Big Data, Open Data, Data Privacy and Security.*

[*] Dr.Öğr.Üyesi, Giresun Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü, levent_memis@hotmail.com, ORCID NO: 0000-0002-5438-691X.

[**] Öğr.Gör., Giresun Üniversitesi, Tirebolu Mehmet Bayrak Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, melikali.guc@giresun.edu.tr, ORCID NO: 0000-0003-0986-9290.

Makale Geliş Tarihi: 04.11.2019 Makale Kabul Tarihi: 22.01.2020

GİRİŞ

Son dönemlerde gündeme gelen teknolojik gelişmelerin (nesnelerin interneti, sensör, güvenlik yönetim sistemleri, coğrafi bilgi sistemleri, sanal gerçeklik gibi) kentsel alanda karşılığını bulmasıyla birçok kavram geliştirilmiş ve akıllı kent kavramı öne çıkmıştır. Adı geçen teknolojiler aynı zamanda klasik verinin ötesinde daha büyük miktarlarda verinin elde edilmesine de katkı sağlamaktadır. Bu büyük verilerden, kentlerin yönetiminde yararlandığı gibi, açık hale getirilerek (belirli sınırlılıklar dâhilinde) diğer paydaşların kullanımına da sunulduğu bilinmektedir. Bu sayede verilerin kentin karmaşık sorunlarına karşı politika geliştirmeye katkı sağlaması beklenmektedir.

İfade edilen potansiyel getirilerin yanında, büyük veriyle bağlantılı açıklar (*vulnerabilities*) ortaya çıkmaktadır. Bu bağlamda kişisel verilerin gizliliği (*privacy*) ve güvenliği (*security*) konusu öne çıkmaktadır. Verilerin dijital ortamlarda oluşması ve depolanmasıyla amacı dışında, yasa dışı erişimi kolaylaşmaktadır. Bu durum, farklı ölçeklerde (yerel, ulusal ve uluslararası) gündeme gelmekte; siber saldırı, siber savaş, siber casusluk, soygun 2.0, veri simsarlığı gibi kavramlarla nitelendirilmektedir. Bu kavramlar arasında siber saldırı öne çıkmaktadır. Farklı yöntemlerle ortaya çıkan siber saldırılar; (I) veri şifreleme ve yazılım güvenliğinin zayıflığından, (II) güvenli olmayan eski sitemlerin kullanılmasından ve bakım çalışmalarının yetersizliğinden, (III) akıllı kent bağlamında ortaya çıkan bütüncül sistemin karmaşık yapısından ve (IV) insan hatasından ve çalışanların bilinçli olarak kötüye kullanmasından kaynaklandığının altı çizilmektedir (Kitchin ve Dodge, 2019: 59-60). Diğer taraftan şu durumlarda kişisel verilerin gizliliği ve güvenliği öne çıkmaktadır: aktörler arası veri paylaşımında, veri entegrasyonu ve kullanıma hazır verilerde, verilerin depolandığı bulut alt yapısında, veri madenciliği, makine öğrenmesi ve yapay zekâ bağlamında gündeme gelen tehditler ve veriler üzerinde geliştirilen iş birliklerinde özel çıkarların öne çıkmasıdır.

İnternet ağlarının kamusal alana daha fazla entegre olması ve büyük verinin gündeme gelmesiyle oluşabilecek tehditleri durdurmaya yönelik ulusal, bölgesel ve uluslararası düzeyde çeşitli çabalar gösterilmektedir. İfade edilenler kapsamında çalışmanın temel amacı, akıllı kentlerde ortaya çıkan büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla gündeme gelen ilkeleri ve yaklaşımları incelemektir. Temelde yanıt aranan soru şudur: "Akıllı kentlerin önemli bir parçası olan büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla hangi ilkeler ve yaklaşımlar öne çıkmaktadır?". Bu inceleme ilgili literatür, hukuki düzenlemeler ve uluslararası oluşumların aldığı kararlar üzerinden gerçekleştirilmektedir.

Araştırmanın genel sonuçlarına göre, verinin gizliliği ve güvenliği konusunda küresel düzeyde üzerinde uzlaşı sağlanan standartların olmadığı anlaşılmaktadır. Fakat bazı düzenlemeler dikkat çekmektedir. Bu noktada 2018 yılında yürürlüğe giren "AB Veri Koruma Tüzüğü" (*General Data Protection Regulation, GDPR*) önem arz etmektedir. Bu düzenlemeyle birlikte; şeffaflık ve hesap verebilirlik prensibi, açık rıza, unutulma hakkı, veri koruma sorumluları, ağırlaştırılmış yaptırım, verilerin yurt dışına aktarılmasının sıkı kurallara bağlanması ve risk temelli yaklaşıma önem verilmektedir. Diğer taraftan genel olarak büyük verinin gizliliği ve güvenliğini sağlamak amacıyla; verilerin şifrelenmesi, kişisel verilerin anonimleştirilmesi, gizlilik bildirim sistemlerini kullanıcı dostu yapmak, verilerin saklama süresini kısaltmak, amaç sınırlılığı, algoritmik şeffaflık/hesap verebilirlik, veri minimizasyonu, dış inceleme ve denetimler öne çıkmaktadır.

1. AKILLI KENT VE KENTSEL ALANDA BÜYÜK VERİ

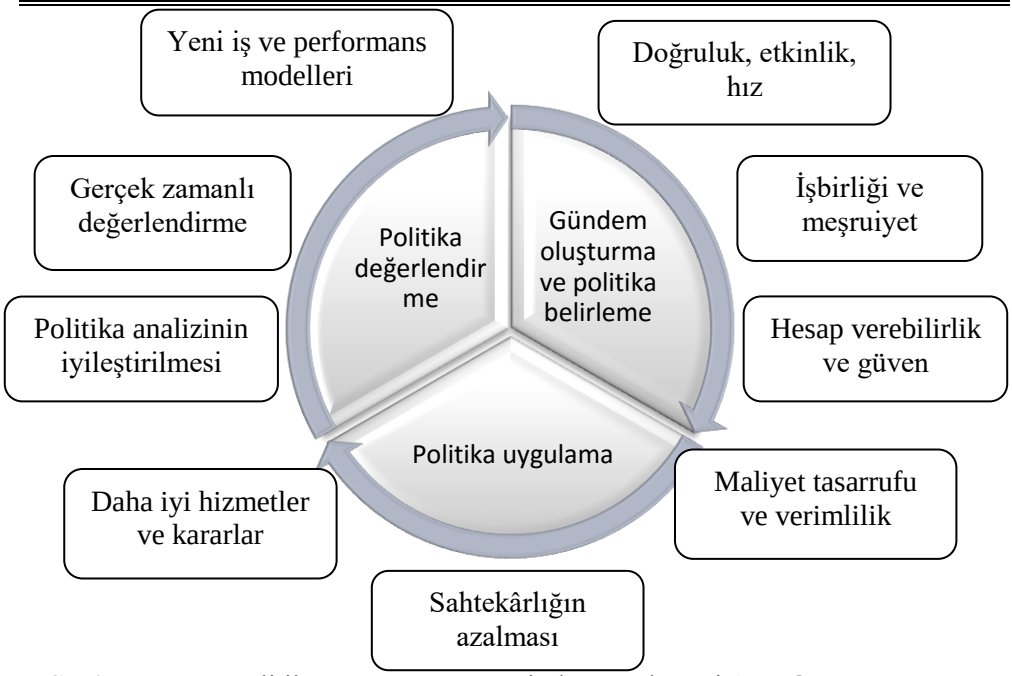
Farklı tanımlama çalışmaları olmakla birlikte genel olarak ele alındığında akıllı kent, yaşam kalitesinin artırılması amacıyla, kentin farklı fonksiyonları arasında entegrasyonu sağlayarak çözüm üreten yapıdır (Nuaimi vd., 2015: 2). Diğer bir ifadeyle yeni teknolojiler, kentin sorunlarına çözümler sunarak kent yaşamının kolaylaşmasına ve iyileşmesine katkı sağlama potansiyeli taşımaktadır. Diğer taraftan teknoloji, kentsel hizmetlere operasyonel düzeyde katkı sağladığı gibi, gerçekleştirilen faaliyetlerin verisinin oluşturulmasını ve tutulmasını da mümkün hale getirmektedir. Bu bağlamda gelişen yeni teknolojiler aracılığıyla akıllı kentlerde ortaya çıkan işlevler Lim ve Malio (2018: 168-169) tarafından 5 C (bağlantılılık/connection, biriktirme/collection, hesaplama/computation, iletişim/communications ve birlikte üretim/co-creation) şeklinde formüle edilmektedir. Bağlantılılık, özellikle nesnelerin interneti uygulamaları aracılığıyla insanlar ve nesneler arasında gerçekleşmektedir. Biriktirme, adı geçen bağlantılılık üzerinden verilere karşılık gelmektedir. Hesaplama, elde edilen verilerin makineler ve insanlar için anlaşılır hale gelmesinde, uzman bilgisine ve özel algoritmalara ihtiyaç duyulmasıdır. İletişim, insanlar ve nesneler arasında kablosuz ağlar ile gerçekleştirilen bir durumdur. Birlikte üretim, hizmet sağlayıcılar ve tüketiciler arasında değerin farklı tarafların yer almasıyla gerçekleşmesidir. Öne çıkarılan bu işlevler incelendiğinde, akıllı kentin büyük veri potansiyeline vurgu yapıldığı anlaşılmaktadır. Hatta yaşanan bu gelişmeler, veri odaklı kentleşme (*data-driven urbanism*) (Kitchin, 2016) kavramını da gündeme getirmektedir.

Temel istatistiksel teknikler üzerinden üretilen bilginin yetersiz kalması, politikalar açısından da büyük veriye yönelişi desteklemektedir. Genel olarak ele alındığında kamu sektöründe büyük verinin uygulama alanları aşağıdaki tabloda yer verildiği biçimde öne çıkmaktadır.

Tablo-1. Kamu Sektöründe Büyük Verinin Etki Alanları ve Potansiyelleri

	Büyük verinin etki alanları	**Büyük verinin taşıdığı potansiyeller**
World Bank, 2017: 2	Hizmet sunumu	Mevcut hizmetlerin iyileştirilmesi ve yeni hizmet alanlarının belirlenmesi
	Politika yapımı	Yeni ve gerçek zamanlı verilerin elde edilmesiyle politikaların belirlenmesi
	Vatandaş katılımı	Makine öğrenmesi gibi uygulamalarla vatandaşların geri bildirimine daha fazla duyarlı olunması
Maciejewski, 2017: 124; 130	Kamu denetimi	Usulsüzlüklerin, düzensizliklerin tespitinde
	Kamu düzenlemesi (politika belirleme)	Yönetilen alanların gerçek zamanlı takip edilmesini
	Kamu hizmeti sunumu	Sunulan hizmetlerin iyileştirilmesi
	Vatandaşların geri bildirimi	Kamu politikası hakkındaki düşüncelerin anlaşılması

Politika döngüsü üzerinden ele alındığında, Şekil 1'de yer verildiği gibi potansiyel katkıları barındırdığı anlaşılmaktadır. Fakat kamu örgütleri açısından; sistemsel, örgütsel ve bireysel düzeyde uyuma dikkat çekilmektedir (Pencheva, Esteve ve Mikhaylov, 2018: 6).



Şekil-1. Kamu Politikası Döngüsü Sürecinde Büyük Veri (Pencheva, Esteve ve Mikhaylov, 2018: 6).

Gelişen yeni teknolojilerin desteğiyle ortaya çıkan büyük verinin, politikaların geliştirilme sürecinde önemli bir rolünün olduğu kaçınılmaz gözükmektedir. Bu bağlamda ilgili veriler, kentin farklı politika alanlarında (ulaşım, lojistik, güvenlik, sağlık, eğitim, enerji, doğal kaynaklar, kamu yönetimi gibi) fayda sağlama potansiyeli taşımaktadır (bkz. Nuaimi vd., 2015: 7-8). İfade edilenler bağlamında Lim, Kim ve Maglio (2018: 92), akıllı kentlerde vatandaşlara, yerel yönetimlere, işletmelere ve ziyaretçilere katkı sağlamak amacıyla büyük veri kullanımını dört kategoride sınıflandırmaktadır. Birincisi (*preventive local administration*), bireysel kullanıcı aracılığıyla elde edilen veriler üzerinden sorunların ve ihtiyaçların tespit edilerek önleyici politikaların geliştirilmesine dayanmaktadır. İkincisi (*local operations management*), sunulan çeşitli hizmetler üzerinden elde edilen verilerle yerel yönetimlerin ve işletmelerin operasyonel açıdan geliştirilmesine katkı sağlamak amacıyla büyük verinin kullanımıdır. Üçüncüsü (*local network development*), kentte yaşayan tüketiciler/vatandaşların bağlantılılığı üzerinden verilerin elde edilerek hizmetlerin geliştirilmesi amacıyla verinin kullanımıdır. Dördüncüsü (*local information diffusion*), sunulan çeşitli hizmetler üzerinden elde edilen verilerin, analiz edilerek tüketicilere/vatandaşlara sunulmasıdır.

2. BÜYÜK VERİNİN İKİNCİ HALİ: AÇIK VERİ

Kentsel alanda karşılaşılan sorun ve ihtiyaçların karmaşıklığı, beraberinde farklı tarafların varlığını da önemli hale getirmektedir. Bu nedenle elde edilen verilerin farklı taraflarla paylaşımı politika geliştirme sürecinde önemli görülmekte ve açık veri kavramı söz konusu olmaktadır. Elde edilen veriler, farklı tarafların kullanımına sunulacak şekilde hazırlanan bir web portalı aracılığıyla açık hale getirilmektedir. Dünya genelinde nüfusu 1 milyonun üzerinde olan 68 yerel yönetim biriminin açık veri portalına sahip olduğu tespit edilmektedir (Erginli ve Tülek, 2019: 14). Açık veriyle birlikte; kamu hizmetlerinin iyileştirilmesi, yenilik, ekonomik büyüme ve mesleklerin ortaya çıkması, açıklığın ve hesap verebilirliğin yükselişi ve vatandaş katılımının sağlanması gibi faydalar beklenmektedir (Lee, Cyganiak ve Decker, 2014: 18). Diğer bir ifadeyle açık veri platformları sayesinde, kentleri daha iyi anlamak, bu sayede daha doğru politikalar geliştirmek ve bu süreçte vatandaşın katılımını sağlamak mümkün olabilmektedir (Erginli ve Tülek, 2019: 12). Bu noktada sürdürülebilir ve başarılı bir açık veri programının üç temel dayanağına dikkat çekilmektedir: gizlilik, veri koruma ve kamu güvenliği (EDP, 2016). Ayrıca bazı ülke uygulamaları üzerinden bazı unsurların (politika, portal, kalite ve etki) önemli olduğu tespit edilmektedir (Detaylı bilgi için bkz. EDP, 2019).

Açık verinin gündeme gelmesiyle birlikte, uluslararası düzeyde de birtakım ilkelerin, kriterlerin, düzenlemelerin ve projelerin geliştirildiği görülmektedir. Bu bağlamda 2013 yılında G8 Açık Veri Sözleşmesi (*Open Data Charter*) gerçekleştirilmiştir. Bu sözleşmeyle açık veriye yönelik şu ilkeler benimsenmiştir: Açıklığı varsayılan olarak belirleme, zamanında ve kapsamlı, erişilebilir ve kullanılabilir, karşılaştırılabilir ve birlikte çalışılabilir, yönetişimin ve vatandaş katılımının gerçekleştirilmesi, kalkınmayı ve yeniliği kapsama (https://opendatacharter.net/history/, 15. 09. 2019). Diğer taraftan akıllı kente giden süreçte kent verisi bağlamında küresel düzeyde standartlar geliştirmeye çalışan bir meclis [*The World Council on City Data* (WCCD)] oluşturulmuş ve bu oluşum kapsamında 17 farklı temada (ekonomi, eğitim, enerji, çevre, güvenlik, barınma, atık gibi) ve 100 göstergede veri standartları (ISO 37120) kabul edilmiştir (EDP, 2016b: 4). Bunların dışında bölgesel düzeyde de Avrupa Komisyonu tarafından 2003 yılında açık verinin kullanımıyla ilgili bir direktif (2003/98/EC) yayınlanmış ve çeşitli projeler [Open Cities (2011-2013), City SDK (2012-2014) ve Icity (2012-2015)] hayata geçirilmiştir (EDP, 2016b: 7-8).

3. BÜYÜK VERİYLE GÜNDEME GELEN GÜÇLÜKLER VE TEHDİTLER

Büyük verinin elde edilmesi, analitiğine/madenciliğine yönelik tekniklerin artış göstermesi, daha fazla verilerin elde edilir olması, tutulma ve işleme maliyetlerinin azalması, veri üzerinden daha fazla bir değer üretilmesi gibi gelişmeler, büyük veri üzerine ilgiyi artırmış ve dolayısıyla bu gelişmeler beraberinde kişisel düzeyde bazı ihlalleri ve endişeleri gündeme getirmeye başlamıştır (Akıncı, 2019: 33; 41; Akt. Kitchin, 2016: 6). Hatta bu gelişmeler aynı zamanda yeni bir dijital güvensizlik (*digital insecurity*) dönemi olarak da ifade edilmektedir (Joo ve Tan, 2018).

Lim, Kim ve Maglio (2018: 94) tarafından akıllı kentlerde, veriden bilgiye dönüşüm sürecinde veri kullanımının güçlükleri şu şekilde sıralanmaktadır:

- Veri kalitesinin yönetimi
- Farklı verilerin entegrasyonu
- Veri gizliliğinin sağlanması (özel hayatın gizliliği)
- Farklı tarafların (yerel yönetimler, vatandaşlar, işletmeler, ziyaretçiler gibi) ihtiyaçlarının anlaşılması
- Coğrafi bilgiyi sağlayacak yöntemlerin geliştirilmesi
- Akıllı kent hizmetlerinin tasarlanması

Nuaimi vd. (2015: 6-9) ve Morabito (2015: 33-35) ise akıllı kentlerde büyük veriyle bağlantılı olarak şu güçlüklere dikkat çekmektedir:

- Verilerin kaynağı (çeşitliliği) ve karakterleri
- Verinin sahipliği (özellikle açık verilerde)
- Veri ve bilgi paylaşımı
- Veri kalitesi
- Güvenlik ve gizlilik
- Sivil özgürlükler ve eşitlik (bir kısmının veri üretimine dahil olmaması)
- Maliyetler
- Kent nüfusunun değişkenliği
- Veri analitiğinde yetenekli kişilerin bulunmayışı

Veriyle ilişkili olarak ortaya çıkan endişeleri/riskleri Tablo 2'de yer verildiği üzere, birbirini tamamlayan gizlilik ve güvenlik başlığı altında toplamak mümkün olabilir.

Tablo-2. Verilerin Gizliliği ve Güvenliğinde Etkili Olan Unsurlar (Ijaz, Shah, Khan ve Ahmed , 2016: 615; Jansater ve Olsson, 2018: 17-18; Georgescu ve Popescul, 2016: 8-10; AlDairi ve Tawalbeh, 2017: 1089-1090).

Verilerin Güvenliği	**Teknolojik faktörler (altyapı)** • Veriyi ortaya çıkaran teknolojilerin (RFID, SCADA, GPS, Bluetooth, sensörler, mobil, vb.) güvenlik altyapı eksikliği • Güncellemelerin ve bakımların zamanında yapılmaması • Bir birine bağlı olma etkisi **Yönetim faktörler** • Bilgi eksikliğinden kaynaklı önem verilmemesi, • Gerekli insan kaynağının bulunmaması ve insan hataları • Örgütsel birimin olmayışı, • Dış kaynaklardan kaynaklanan (tedarikçilerin rekabet şartları altında güvenliğe yeterince önem vermemesi gibi) • Güvenlik sistemlerinin test edilmemesi gibi. **Sosyo-ekonomik faktörler** • Veriyi üretenlerin farkındalık eksikliği, • Maliyetlerin yüksekliği ve kaynakların kısıtlılığı
Verilerin Gizliliği	Anonimleştirilen verilerin kişilerle ilişkilendirme potansiyeli Büyük verinin amacı dışında kullanımı Verilerden çıkarımların şeffaflık ilkesi çerçevesinde yapılmaması (ayrımcılığın oluşması gibi) ve yanlış çıkarımlarda bulunma ihtimali Tüm verilerin elde edilme potansiyeli ve veri minimizasyonundan uzaklaşılması Art niyetli kullanım ve üçüncü taraflarla izinsiz paylaşımı

Tablo 2 incelendiğinde verilerin elde edilmesi, saklanması, işlenmesi ve sunulmasında yararlanılan altyapı; örgütsel yapının ve insan kaynağı ile veriyi üretenlerle ilişkili olarak sosyal bileşenlerin ve bütçenin etkili faktörler olduğu anlaşılmaktadır.

Nesnelerin, internetle bağlantılı hale gelmesi ve bu sayede üretilen verilerin bulut sisteminde depolanması, veriye yönelik uzaktan müdahaleleri kolaylaştırmakta ve akıllı kentlerde dijital sistemleri hassas hale getirmektedir (Pelton ve Singh, 2019: 7). Bu bağlamda Joo ve Tan (2018: 94) siber-fiziksel tehditler bağlamında dört kritik güvenlik açığını aşağıda yer verilen Tablo 3'de gösterildiği gibi vurgulamaktadır.

Tablo-3. Siber Alanda Güvenlik Açıkları

Güvenlik Açıkları	**Temel Özellikleri**
Endüstriyel kontrol sistemleri	Gerçekleştirilecek saldırılarla kritik alt yapının devre dışı bırakılması ve bir yerde ortaya çıkan bozulmanın diğer alanlara da yansıması.
Kaynakları kısıtlı birimler	Güvenlik konusunda gerekli önlemlerin alınmamasından dolayı saldırıların gerçekleşmesi ve saldırıların kopyalanarak devam etmesi.
Wireless iletişimi	Bağlantı kurulan cihazlara saldırıların [man in the middle (MitM)] kolaylaşması, içeriğin algılanabilir ve değiştirilebilir olması.
Bulut depolama	Verilerin sanal bir alanda toplanmasının saldırıların hedefi haline gelebilmekte ve veri güvenliğinin ilgili servis sağlayıcılara bağlı olması.

Verilerin siber ortamda dolaşıma girmesiyle siber saldırı kavramı gündeme gelmektedir. Siber saldırılar, dijital teknolojilerin barındırdığı güvenlik açıklarını (şifreleme ve yazılım güvenliğinin zayıflığı, eski sistemlerinin kullanımı, insan hataları gibi) kullanmaya çalışmaktadır (Kitchin ve Dodge, 2019: 49-51). Farklı yöntemlerle (Patel ve Doshi, 2019: 183-188) gerçekleştirilen saldırılar; nesnelerin arasında veri akışına müdahale etme (veri tabanı kontrol ve gözetleme sistemi (SCADA), RFID takip ve kontrol sistemi gibi uygulamalarda), bulut sisteminde depolanan alanlara sızarak veriyi elde etme veya zarar verme veya verilerin sunulması esnasında verilerin manipüle edilmesi, durdurulması veya elde edilmesi şeklinde ortaya çıkabilmektedir (Özdağ ve Kılıç, 2019: 11;) (2006 sonrası gerçekleşen farklı siber saldırı örnekleri için bkz. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents, 10. 09. 2019). Ayrıca aşağıda yer verilen alanlarda farklı açılardan potansiyel saldırılara dikkat çekilmektedir (Lin vd., 2017: 28).

Tablo-4. Siber Saldırı Alanları

Kritik Sektörler	Muhtemel Saldırı Alanları			
	Kamu güvenliği	**Finans**	**Operasyonlar**	**Gizlilik**
Enerji	Güç kaynağında oluşacak bozulmayla bazı fonksiyonların etkilenmesi	Fidye veya enerji hırsızlığı	Enerji yönetim sisteminin bağlantılarına zarar vermek	Sayaç verileri ve vatandaş bilgisini çalmak
Ulaşım	Kazalara sebebiyet verme	Ücretsiz ulaşım elde etmek veya araçları rehin almak	Ulaştırma hizmetlerini kesmek ve değiştirmek	Kullanıcı verilerini ele geçirmek
Çevre	Akıllı atık su sistemine zarar vermek	Sistemleri durdurmak veya cihazları rehin almak	Komutları değiştirme ve sistem bildirimlerini bozma	Faaliyetleri izlemek için sensörlerden yararlanmak
Bağlantılılık		Sistemleri durdurmak veya cihazları rehin almak	Sistemlere zarar vermek için ağ iletişimini bozmak	Bilgileri elde etmek için bağlantılara zarar vermek
Yönetişim/Yönetim		Sistemleri durdurmak veya cihazları rehin almak	Sistemleri veya cihazları rehin tutmak; bağlantılı cihazları bots'a dönüştürmek	Açık veri ve geri bildirimlerle ilgili bilgilerin elde edilmesi

Yaşanan bu gelişmeler siber güvenlik konusuna ayrıca önem vermeyi gerekli kılmaktadır. Bu bağlamda ülkelerin farklı çabaları öne çıkmakta (Detaylı bilgi için bkz. Göçoğlu, 2019: 107-158) ve ülkelerin siber güvenlik konusundaki durumlarını yansıtan indeksler yayımlanmaktadır (bkz. Özdağ ve Kılıç, 2019: 10).

4. VERİNİN GİZLİLİĞİNİ VE GÜVENLİĞİNİ SAĞLAYAN İLKELER VE YAKLAŞIMLAR

Akıllı kent uygulamalarının yaygınlığının hızlanması, beraberinde bazı sorunların etkisini de artırmaktadır. Kentlerin internet ağlarıyla daha fazla örülmesi, siber güvenliği önemli bir unsur haline getirmeye başlamıştır (Göçoğlu, 2019). Bu nedenle akıllı kentlerde güvenlikle ilgili problemler, güncelliğini ve gerçekliğini korumaktadır (AlDairi ve Tawalbeh, 2017: 1088).

Büyük verilerin önemli bir kısmı kişisel verilerden oluşmaktadır. Bu noktada veriyi üretenlerin rızası olmadan kişisel verilerin kullanılması ve taraflarla paylaşılması, hak ihlallerini gündeme getirmektedir. Kişisel veriler bağlamında özel hayatın korunması modern devletlerin kabul ettiği temel ilkelerden biridir. Veri koruma içinde yer alan "mahremiyet", insan haklarının bir bileşeni olarak uluslararası sözleşmelerin ve ulusal düzenlemelerin önemli gündem maddesine karşılık gelmektedir (Akıncı, 2019: 57; kişisel verilerin korunması hususunda gerçekleştirilen ulusal ve uluslararası düzenlemelerin detayları için bkz. Akıncı, 2019: 59-91; Yılmaz, 2019: 149-195). Ayrıca teknolojik gelişmeler büyük verinin mekansal bağlılığını ortadan kaldırmakta ve dolayısıyla veri güvenliği konusunda ülkeler arasında daha fazla iş birliklerine ihtiyaç duyulmaktadır (Akıncı, 2019: 48). Verilerin gizliliğini ve güvenliğini artırmak amacıyla farklı ilkelerin belirlendiği anlaşılmaktadır. Çalışmanın bu kısmında uluslararası ve ulusal düzeyde öne çıkan düzenlemelere ve benimsenen ilkelere yer verilmektedir.

İfade edilenler bağlamında uluslararası alanda ilk olarak OECD tarafından 1980 yılında "*Mahremiyetin ve Kişisel Verilerin Sınırlar Arası Aktarımının Korunması Hususunda Rehber İlkeler*" yayımlanmıştır. Aşağıda yer verilen Tablo 5'te görüldüğü gibi veri koruma konusunda sekiz ilkeye yer verilmiş, bunlarla birlikte bir altyapı oluşturulmaya çalışılmıştır (Akt. Yılmaz, 2019: 124). Veri korumayı odağına alan ikinci uluslararası düzenleme ise BM'nin çalışmaları kapsamında şekillenen ve ortaya çıkan, 1990 yılında yayımlanan "*Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*"dir. Buradaki düzenlemeyle veri koruma konusunda ilk kez yetkili bir organa yer verilmiştir (Akt. Yılmaz, 2019: 126).

AB düzeyinde 1995 yılında "*AB Veri Koruma Direktifi*" (95/46/EC) yayımlanmıştır. Sonrasında ise AB düzeyinde "*Veri Koruma Tüzüğü*" kabul edilmiş (2016) ve uygulanmaya (2018) başlanmıştır. Bu düzenlemenin büyük verideki gelişmeler üzerine şekillendiği anlaşılmaktadır. Tüzüğün temel amacı, verilerin işlenmesi ve farklı taraflar arasında dolaşımı sırasında gerçek kişilerin

temel hak ve özgürlüklerini korumak olarak ifade edilmektedir (Akıncı, 2019: 86). Tüzüğün şu üç önemli alanda yenilikler getirdiği anlaşılmaktadır: kişisel verilerin ve veri sahiplerinin daha etkin korunması, veri işleyenler ile veri kontrolörlerini artırılmış sorumluluğu ve mekansal anlamda daha geniş uygulama alanına sahip olunması (Akıncı, 2019: 79-86). Tüzük kapsamında Tablo 5'de yer verilen ilkeler pro-aktif bir yaklaşımla benimsenmiştir.

Tablo-5. Verilerin Korunmasına Yönelik Ulusal - Uluslararası Düzenlemeler ve Benimsenen İlkeler (Akıncı, 2019: 86-87; Yılmaz, 2019: 124-126).

Kararlar/Düzenlemeler	**İlkeler**
OECD Mahremiyetin ve Kişisel Verilerin Sınırlar Arası Aktarımının Korunması Hususunda Rehber İlkeler (1980)	Veri toplamanın sınırlı olması ilkesi Veri kalitesi ilkesi Amacın belli olması ilkesi Kullanmanın sınırlı olması ilkesi Veri güvenliği ilkesi, Açıklık ilkesi Bireysel katılım ilkesi Hesap verebilirlik ilkesi
BM Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (1990)	Kanunilik ve dürüstlük ilkesi Doğruluk ilkesi Amacın belirliliği ilkesi İlgili kişinin erişimi ilkesi Ayrımcılık yapılmaması ilkesi İstisna koyma ilkesi
6698 sayılı Kişisel Verilerin Korunması Kanunu (2016)	Hukuka ve dürüstlük kurallarına uygun olma Doğru ve gerektiğinde güncel olma Belirli, açık ve meşru amaçlar için işlenme İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme
AB Veri Koruma Tüzüğü (2018)	Hukukilik, dürüstlük ve şeffaflık Amaçla sınırlılık Veri minimizasyonu Doğruluk Veri saklamanın sınırlandırılması Bütünlük ve gizlilik Veri işleyenler ile veri kontrolünün eşit düzeyde sorumluluğu Veri koruma etki değerlendirmesi Hesap verebilirlik

Türkiye özelinde ele alındığında ise kişisel verilerin korunmasına yönelik gelişmelerin Sekizinci Kalkınma Planı'yla başladığı ve Onuncu Kalkınma Planı uygulama süreci içinde somut olarak 2016 yılında 6698 sayılı *Kişisel Verilerin korunması Kanunu*'nun yürürlüğe konulduğu anlaşılmaktadır. Bu kanunda AB'nin 95/46/EC sayılı direktifinin etkili olduğu ifade edilmektedir (Akıncı, 2019: 131-135).

Benimsenen ilkeler incelendiğinde verilerin elde edilmesinde ve kullanılmasında, veriyi üreten kişileri koruma ve bu anlamda oluşabilecek tereddütleri giderme çabasının olduğu anlaşılmaktadır.

Verinin gizliliğini ve güvenliğini iyileştirmek amacıyla farklı yaklaşımların, çabaların ortaya çıktığı anlaşılmaktadır. Bu çabalar teknik ve yönetsel açıdan gündeme gelmektedir. Teknik açıdan bazı araçlar ve yöntemler öne sürülmektedir. Araçlar bağlamında güvenilir veri depolama ve işlem logları, uç nokta giriş onaylama/filtreleme, gerçek zamanlı güvenlik görüntüleme, kriptografik zorunlu veri merkezli güvenlik, ölçeklenebilir ve birleştirilebilir gizlilik korumalı veri madenciliği ve matematiksel analiz gibi tekniklere yer verilmektedir (Akt. Eyüpoğlu vd., 2017: 178). Yöntem açısından ise desen gizleme, güvenli dağıtımlı veri madenciliği, k-anonimlik veya kimliksizleştirme, homomorfik şifreleme gibi yöntemler öne çıkarılmaktadır (Akt. Eyüpoğlu vd., 2017: 179-183).

Yönetsel açıdan ele alındığında bir yöntem olarak ayrı bir örgütsel yapılanma önem kazanmaktadır. Bu sayede ilgili konuları daha iyi yönetmek mümkün hale gelebilmektedir. Bu bağlamda Dubai örneğinde oluşturulan "E-Güvenlik Merkezi" dikkat çekmektedir. Merkez; e-güvenlikle ilgili teknik araçları, veri güvenliğini, ilgili kurumlar arasında koordinasyonu, gerçekleştirilecek düzenlemelerde ve planlara katkı sağlamak gibi çabaları göstermektedir (Efthymiopoulos, 2016: 11). İkinci bir yaklaşım, dışarıdan gözetimin güçlendirilmesi şeklindedir. Bu kapsamda Hollanda'da faaliyet gösteren *Review Committee on the Intelligence and Security Services* (CTIVD) birimi önemli bir örneği teşkil etmektedir (Broeders vd., 2017: 319-320). Bir diğer önemli yaklaşım ise risk yönetimi anlayışıyla verinin güvenliğinin ve gizliliğinin sağlanmasıdır. Risk yönetimi bir tehlike ihtimalinin öncesinde sistematik ve titizlikle değerlendirildiği ve yönetildiği bir sürece karşılık gelmektedir. Bu yaklaşımın avantajı dijital sistemlerin incelenmesinin zorunlu kılınmasından kaynaklanmaktadır. Risk temelli bu yaklaşım, akıllı kentlerdeki koruma görevini azaltacaktır. Bu yaklaşım kapsamında iki strateji öne sürülmektedir: 1. Kent yönetimlerinin, saldırılara karşı daha sıkı güvenlik

önlemlerini oluşturması ve 2. Kent yöneticilerinin, gerçekleştirilen saldırıları caydırmak için cezaların artırılmasıdır (Joo ve Tan, 2018: 100-102). OECD tarafından belirlenen mahremiyet ilkeleri arasında da risk yönetimine yer verildiği görülmektedir (Akıncı, 2019: 128).

Kitchin ve Dodge (2019: 58-59) ise akıllı kentleri güvenli hale getirmenin yöntemlerini iki başlık altında ele almaktadır. Birincisi, erişim kanalarının iyileştirildiği, güvenlik yazılımlarının iyileştirildiği ve güvenliğe yönelik ayrı bir birimin oluşturulduğu geleneksel yöntemlerdir. İkincisi ise piyasa ve devlet odaklı yasal düzenlemeler ve yaptırımlardan oluşmaktadır. Burada da iki seçenek öne çıkmaktadır: özel sektör temsilcilerinin belirlediği standartlar üzerinden güvenliğin oluşturulması ve kuralların, standartların ve yaptırımların devlet öncülüğünde gerçekleşmesidir.

SONUÇ YERİNE: HENÜZ YOLUN BAŞINDAYKEN KENTLERDE NELERİ DİKKATE ALMALIYIZ?

Gelinen bugünkü noktada kentsel alanda, temel istatistikler ve ortalama değerler üzerinden sorunları ve ihtiyaçları belirlemeye çalışarak politika üretmek etkinliğini yitirmektedir. Çünkü ortaya çıkan yeni teknolojiler, yaşanan deneyimlerin verileştirilmesini mümkün hale getirmektedir. Elde edilen bu büyük veriler üzerinden gerçekleştirilecek analitik çalışmalar, kararları daha etkin hale getirerek politikaların geçerliliğini güçlendirebilmektedir. Ayrıca deneyimlerinin verileştirilmesiyle vatandaşın katılımını dolaylı olarak sağlayabilmektedir. Fakat büyük veriler tüm bu potansiyel faydalarına rağmen verilerin gizliliği ve güvenliği konusundaki bazı endişeleri/güçlükleri/riskleri beraberinde taşımaktadır. Gündeme gelen bu olumsuzluklar dikkate alınmadığında, özellikle veriyi üreten taraflar açısından çeşitli zararlara yol açması mümkün olmaktadır. Bu olumsuzlukların azaltılması amacıyla büyük veriye yönelik gizlilik ve güvenlik önlemleri geliştirirken, büyük verinin avantajları ile bireysel haklar arasında bir uzlaşı sağlayan yaklaşımlara ihtiyaç duyulmaktadır (Akıncı, 2019: 47-48).

İfade edilenler kapsamında kentsel alanda yeni teknolojileri yaygınlaştırırken ve bunlar üzerinden büyük veriyi elde ederken, aşağıda yer verilen hususlar dikkate değer görülmektedir (Lim, Kim ve Maglio, 2018: 92; Lin vd., 2017: 30-32; Kitchin ve Dodge, 2019: 59-60):

- Büyük veri kullanımı konusunda çok fonksiyonlu bir çalışma takımı oluşturmak, ayrı bir alt örgütlenmeye gitmek, ayrı bir bütçe oluşturmak,

- Risk yönetimi yaklaşımı bağlamında büyük veriyi yönetmek,
- Kalite kontrol ve penetrasyon testlerinin zamanında yapılması,
- Hizmetlere yönelik anlaşmalarda (dışarıdan hizmet satın almalarda) güvenliğin öncelikli hale getirilmesi,
- Büyük verinin de içinde yer aldığı dijital konularla ilgili bir acil durum ekibinin oluşturulması,
- Yazılım güncellemelerinin geçerliliğini ve güvenliğini sağlamak, zamanlamasına dikkat etmek, bu noktada dış paydaşlarla etkili iş birliği içinde olmak,
- Güvenlik altyapısını uzun dönemli bir bakış açısıyla ele almak,
- Farkındalık ve bilgi düzeyini artıracak eğitimlerin gerçekleştirilmek (vatandaşlara ve çalışanlara yönelik), gizlilik bildirimlerini kullanıcı dostu tasarlamak,
- Gizliliği göz önünde bulundurarak verileri işlemek,
- Ortak iletişim kanallarının şifrelenmesi, doğrulanması ve düzenlenmesini sağlamak,
- Kimi zaman manuel olarak geçersiz kılmaya izin verilmesi, bazı sistemlerin "sağır" (ağa bağlı olmayan) ve "dilsiz" (kodla otomatikleştirilmemiş) oluşturulması,
- "Kişisel verilerin korunması"nın ötesinde büyük veriyi esas alan hukuki düzenlemelere ihtiyaç duyulması,
- İletişim kanallarında "şifreleme" yönteminin etkin kullanımının sağlanması,
- Veri güvenliği konusunda daha fazla iş birliklerin geliştirilmesi, uluslararası düzeyde belirlenen standartların hayata geçirilmesi,
- Dışarıdan gözetimin güçlendirilmesi, açıklığın artırılmasıdır.

KAYNAKÇA

Akıncı, A. Ş. (2019). *Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti*. (Yayımlanmamış Uzmanlık Tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Sektörler ve Kamu Yatırımları Genel Müdürlüğü, Ankara.

AlDairi, A. ve Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, 109C, 1086-1091.

Broeders, D., Schrijvers, E., Sloot, B., Brakel, R. Hoog, J. ve Ballin, E. (2017). Big Data and Security Policies: Towards a Framework for Regulating The Phases of Analytics and Use of Big Data. *Computer Law & Security Review*, 33, 309-329.

EDP (2019). *Analytical Report 13: Open Data Best Practices in Europe's Top Performers: Ireland, Spain and France*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/en/content/report-13-open-data-best-practices-europe%E2%80%99s-top-performers-ireland-spain-and-france.

EDP (2016): *Analytical Report 3: Open Data and Privacy*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/sites/default/files/open_ data_ and_ privacy_v1_final_clean.pdf.

EDP (2016b): *Analytical Report 4: Open Data in Cities*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/sites/default/files/edp_analytical_ report_n4_-_open_data_in_cities_v1.0_final.pdf.

Erginli, B. E. ve Tülek, M. (2019). *Kentsel Politikanın Desteklenmesi için Yeni Araçlar: Açık Veri Platformları ve Dijital Kent Panelleri*. İstanbul: TESEV Yayınları.

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H. ve Öneş, O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. *Bilişim Teknolojileri Dergisi*, 10 (2), 177-184.

Georgescu, M. ve Popescul, D. (2016). The Importance of Internet of Things Security for Smart Cities. İçinde I. N. Da Silva and R. A. Flauzino (Ed.) *Smart Cities Technologies* (3-18). InTech.

Göçoğlu, V. (2019). Akıllı Şehirlerdeki Kritik Altyapıların Siber Güvenliği. *Uluslararası Yönetim Akademisi Dergisi,* 2 (1), 51-63.

Göçoğlu, V. (2019). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*. (Yayınlanmamış Doktora Tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Ijaz, S., Shah, M. A., Khan, A. ve Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 7 (2), 612-625.

Jansater, G. ve Olsson, O. (2018). *Cyber Security in Smart Cities Not a Primary Concern*. Master thesis, Department of Informatics, Lund School of Economics and Management, Lund University.

Joo, Y.-M. ve Tan, T.-B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival*, 60 (2), 91-106. DOI: 10.1080/00396338.2018.1448577.

Kitchin, R. (2016). *Theethicsofsmartcitiesand Urbanscience*. Phil.Trans.R. Soc., 1-15, http://dx.doi.org/10.1098/rsta.2016.0115.

Kitchin, R. ve Dodge, M. (2019): The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 26 (2), 47-65. DOI: 10.1080/10630732.2017.1408002.

Lee, D., Cyganiak, R. ve Decker, S. (2014). *Open Data Ireland: Best Practice Handbook*. Erişim Tarihi: 14 Eylül 2019, https://data.gov.ie/uploads/page_images/2019-04-24-104248.848906Best-Practice-Handbook.pdf.

Lim, C., Kim, K.-J. ve Maglio, P. P. (2018). Smart Cities with Big Data: Reference Models, Challenges and Considerations. *Cities*, 82, 86-99.

Lim, C. ve Maglio, P. (2018). Data-Driven Understanding of Smart Service Systems Through Text Mining. *Service Science*, 10 (2), 154-180.

Lin, P., Swimmer, M., Urano, A., Hilt, S. ve Vosseler, R. (2017). *Securing Smart Cities Moving Toward Utopia with Security in Mind*. A TrendLabs Research Paper, Erişim Tarihi: 15 Eylül 2019, https://documents.trendmicro.com/assets/wp/wp-securing-smart-cities.pdf.

Maciejewski, M. (2017). To Do More, Better, Faster and More Cheaply: Using Big Data in Public Administration. *International Review of Administrative Sciences*, 83 (15), 120-135. DOI: 10.1177/0020852316640058.

Morabito, V. (2015). *Big Data and Analytics, Strategic and Organizational Impacts*. Switzerland: Springer.

Nuaimi, E., Al-Neyadi, H. A., Mohamed, N. ve Al-Jaroodi, J. (2015). Applications of Big Data to Smart Cities. *Journal of Internet Services and Applications*, 6 (25), 1-15.

Özdağ, H. O. ve Kılıç, G. O. (2019). Bilgi Savaşları ve Arka Plandakiler. *Bilim ve Gelecek*, Ağustos, 6-13.

Pelton, J. N. ve Singh, I. B. (2019). *Smart Cities of Today and Tomorrow Better Technology, Infrastructure and Security*. Switzerland: Springer.

Pencheva, ı., Esteve, M. ve Mikhaylov, S. J. (2018). Big Data and AI – A Transformational Shift for Government: So, What Next for Research?. *Public Policy and Administration*, 1-21. DOI: 10.1177/0952076718780537.

Yılmaz, B. (2019). *Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. (Yayınlanmamış Doktora Tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

World Bank (2017). *Big Data in Action for Government*, Erişim tarihi: 15 Eylül 2019, http://documents.worldbank.org/curated/en/176511491287380986/Big-data-in-action-for-government-big-data-innovation-in-public-services-policy-and-engagement.