**DEĞİŞEN GÜVENLİK ANLAYIŞINDA GELECEĞİN AKILLI KENTLERİ**

***İlke Bezen TOZKOPARAN*[[1]](#footnote-1)**

**Öz**

Güvenlik, insanlık tarihi kadar eski bir olgudur. Huzur ve güven arayışının insanoğlunun ilk var oluşundan bugüne kadar geçerliliğini koruyan bir ihtiyaç olduğu bilinen bir gerçektir. Dünya tarihinde, insanların ilk yerleşik düzene geçmesiyle emniyet, asayiş, huzur ve düzen ihtiyacı ortaya çıkmıştır. Güvenlik ihtiyacı, Maslow’a göre insan bedeninin canlı kalması için gereken fizyolojik ihtiyaçlarından sonra ikinci sırada gelmektedir. Günümüzde geleneksel güvenlik anlayışı, küreselleşmenin yarattığı dinamik ortamın da etkisiyle değişmiştir. Ulusal ve uluslararası güvenliğe yönelik tehditler farklılaşmıştır. Böylece, güvenlik; küreselleşme, teknolojinin gelişmesi ve yeni tehditler sayesinde yeniden tanımlanmayı gerektirmiştir. Değişen ve dönüşen güvenlik kavramının etkisiyle, dünya daha önceden öngörülemeyen, hiçbir sınır tanımayan tehdit ve risklerle karşı karşıyadır.

Yine insanlık tarihinin başlangıcında nüfusun yarısından çoğunun kentlerde yaşadığı varsayılmaktadır. 2030 yılına kadar da dünya nüfusunun üçte ikisinin kentlerde yaşayacağı düşünülmektedir. Artan bu nüfus yoğunluğu kentsel altyapılarda, kaynaklarda ve hizmetlerde de bir artışa yol açacaktır. Bu yüzden, kentsel altyapıların ve kaynakların yönetiminde ve vatandaşların bugünkü ve gelecekteki ihtiyaçlarının etkin ve verimli bir şekilde karşılanmasında, kentlerin akıllı hale gelmesine ihtiyaç duyulmaktadır. Ancak literatürde herkes tarafından kabul gören bir “akıllı kent” tanımı bulunmamaktadır. Akıllı kentin zeki kent, bilgi kenti, dijital kent, teknolojik kent, sürdürülebilir kent ve yeşil kent gibi farklı anlamları bulunduğu ifade edilmektedir. Akıllı kent tanımlamalarında teknoloji, altyapı, bilgi yönetimi, bağlantılılık, sürdürülebilirlik, yaşam kalitesi, katılımcı yönetişim gibi kavramların öne çıktığı da görülmektedir. Bir kentin, kullanılan ifadelerdeki gibi bir kent olabilmesi için, kentte ortaya çıkabilecek sorunların çözümünde bilgi ve iletişim teknolojileri kullanılarak çözümlerin geliştirilmesi ve kentte yaşayanların da bu çözümleri bir yaşam biçimi olarak benimseyip kullanmaları gerekmektedir. Bu bağlamda bir kentin değişip dönüşmesi, üst nesil teknolojik sistemlerin kullanılmasını gerektirmekte ve bu durum da ancak yenilikçi adımlar atılarak gerçekleştirilebilmektedir. Ancak bu teknolojik sistemler yeni nesil güvenlik tehditlerini de beraberinde getirmektedir.

Buradan yola çıkılarak, zeki kent, bilgi kenti, dijital kent, teknolojik kent, sürdürülebilir kent ve yeşil kent gibi farklı anlamları bulunan; genel olarak, bilgi ve iletişim teknolojilerinin katkısıyla yönetişim, hareketlilik, çevre ve yaşam bileşenleri bütününde oluşan ve pek çok boyutu bir araya getiren akıllı kentlerin, değişen güvenlik kapsamındaki durumu bu çalışmanın ana konusunu oluşturacaktır. Çalışmada, kent, akıllı kent ve güvenlik kavramsal çerçevesinden sonra bilgi ve teknolojinin kentsel hizmetlerde daha fazla kullanılmaya başlanmasıyla kentlerde meydana gelen değişim ve dönüşümler yeni güvenlik anlayışı kapsamında ele alınacaktır. Türkiye’den ve dünyadan uygulamalar ile bu değişimin ve dönüşümün yeni güvenlik anlayışında nasıl yer aldığı ve gelecekte nasıl yer alacağı incelenecektir.

**Anahtar Kelimeler:** Kent, Akıllı Kent, Güvenlik, Yeni Güvenlik, Teknoloji

**SMART CITIES OF FUTURE IN THE CONCEPT OF CHANGING SECURITY**

**Abstract**

Security is as old as human history. It is a well-known fact that the search for peace and confidence has been a necessity since the first existence of mankind. In the history of the world, the need for security, order, peace and order has emerged with the first settling of people. According to Maslow, the need for safety comes second after the physiological needs of the human body. Today, the concept of traditional security has changed with the effect of the dynamic environment created by globalization. The threats to national and international security have varied. Thus, security; has necessitated to redefine because of the globalization, development of the technology and new threats. As a result of the changing and transforming security concept, the world is faced with unpredictable threats and risks.

At the beginning of human history, it is assumed that more than half of thepopulation lives in cities. By 2030, two thirds of the world’s population is expected to live in cities. This increasing population density will lead to an increase in urban infrastructure, resources and services. Therefore, cities need to become intelligent in the management of urban infrastructures and resources and to meet the present and future needs of citizens effectively and efficiently. However, there is no definition of “smart city” accepted by everyone in the literature. It is stated that the smart city has different meanings such as smart city, information city, digital city, technological city, sustainable city and green city. It is seen that concepts such as technology, infrastructure, knowledge management, connectedness, sustainability, quality of life, participatory governance are prominent in smart city definitions. In order for a city to be a city like expressions used, it is necessary to develop solutions by using information and communication technologies in solving the problems that may arise in the city and those who live in the city should adopt and use these solutions as a way of life. In this context, changing and transforming a city requires the use of high-end technological systems and this can only be achieved by taking innovative steps. However, these technological systems bring new generation security threats.

From this point of view, it has different meanings such as intelligent city, information city, digital city, technological city, sustainable city and gren city; in general, the status of smart cities, which are formed in the whole of governance, mobility, environment and life components with the contribution of information and communication technologies and which bring together many dimensions, will be the main subject of this study. In this study, after the city, smart city and security conceptual framework, the changes and transformations in cities will be discussed within the scope of new security concept. With applications from Turkey and the World, these changes and the transformation how takes place at the new security concept and how the future will take place will be investigated.

**Keywords**: City, Smart City, Security, New Security, Technology

**GİRİŞ**

Son zamanlarda bilim ve teknoloji alanındaki gelişmelerin ve yeni buluşların toplumların sosyokültürel değerleriyle birlikte zaman ve mekân algılarını da değiştirdiği bilinen bir gerçektir. Aynı anda birçok olanak ve problem oluşturan bu gelişmeler, 21. yüzyılda yaşam tarzlarını biçimlendirmeye ve düzenlemeye yönelmiştir. Geçmiş ve şimdi arasındaki bağlantı kopmuş, birbiriyle ilişkisi olmayan bir dizi deneyim eşzamanlı olarak yaşanmaya başlanmıştır. Türk dil kurumuna göre zaman, “bir işin, bir oluşun içinden geçtiği, geçeceği ve geçmekte olduğu süre, vakit, bir sürenin belirli bir parçası, belirlenmiş bir an, çağ, mevsim, bir işe ayrılmış, veya bir iş için alışılmış saatler, dönem devir, bir süre ile ilgili durum, şartlar, olayların oluş ve akış sırasını belirleyen düzenli ve dönemli gök olaylarını birim olarak kullanan sanal bir kavram” olarak tanımlanmıştır. Zamanın “geçmiş” olarak geriye doğru sonsuza değin uzandığı, “gelecek” olarak da ileriye doğru akıp gittiği belirtilmektedir. (Kaçar, 2007: 58)

Zamanın değişmesi, bilgi ve teknolojinin ilerlemesi; mekânları, toplumu, güvenlik anlayışını ve kentleri değiştirmiştir. İnsanlık tarihi kadar eski bir olgu olan güvenlik anlayışı, küreselleşmenin yarattığı dinamik ortamın da etkisiyle geleneksel anlayışından farklı bir boyuta geçmiştir. Ulusal ve uluslararası güvenliğe yönelik tehditler farklılaşmıştır. Böylece, güvenlik; küreselleşme, teknolojinin gelişmesi ve yeni tehditler sayesinde yeniden tanımlanmayı gerektirmiştir. Değişen ve dönüşen güvenlik kavramının etkisiyle, dünya daha önceden öngörülemeyen, hiçbir sınır tanımayan tehdit ve risklerle karşı karşıya kalmaktadır.

Bu değişim ile birlikte artan nüfus yoğunluğunun kentsel altyapılarda, kaynaklarda ve hizmetlerde de bir artışa yol açacağı düşünülmektedir. Kentlerin yerleşik ve gelişmiş bir toplumsal durum olduğu belirtilebilir.(Kayan, 2015: 277) Bu yüzden, kentsel altyapıların ve kaynakların yönetiminde ve vatandaşların ihtiyaçlarının karşılanmasında, kentlerin akıllanması gerekmektedir. Ancak literatürde herkes tarafından kabul gören bir “akıllı kent” tanımı bulunmamaktadır. Bir kentin, akıllı bir kent olabilmesi için, kentte ortaya çıkabilecek sorunların çözümünde bilgi ve iletişim teknolojileri kullanılarak çözümlerin geliştirilmesi ve kentte yaşayanların da bu çözümleri bir yaşam biçimi olarak benimseyip kullanmaları gerekmektedir. Bu bağlamda bir kentin değişip dönüşmesi, üst nesil teknolojik sistemlerin kullanılmasını gerektirmekte ve bu durum da ancak yenilikçi adımlar atılarak gerçekleştirilebilmektedir. Ancak bu teknolojik sistemlerin yeni nesil güvenlik tehditlerini de beraberinde getirdiği bilinmektedir.

1. **BİLGİDEN AKILLI KENTLERE BİR KAVRAMSAL ÇERÇEVE**

Çalışmanın akışında kullanılan kavramlar bu bölümde kısa bir şekilde ele alınmaya çalışılacaktır. Bilgi, bilgi güvenliği özellikle çalışmada üzerinde durulmaya çalışılan veri güvenliği; kent, kent güvenliği ve akıllı kentler şeklinde kavramsal çerçeve verilecektir.

Bilgi, günümüzde temel ekonomik kaynak olarak ele alınmakla birlikte yeniçağın bir özelliği olarak ortaya çıkmaktadır. Bilgi ve teknoloji birlikte sadece küresel ekonomik başarıyı sağlamamakta, aynı zamanda demokrasiyi de yeniden canlandırmaktadır. (Aydoğdu, 2011: 1776) Bilgi çağı, öğrenmeyi herkes için olanaklı kılan yeni eğitim teknolojilerinin gelişmesine yol açtığı için, Sanayi Devrimi’nden sonra insanlığın bugüne dek tanık olduğu en önemli olay olarak nitelendirilmektedir. (Aydoğdu, 2013: 18)

Bilgi güvenliğiyle ilgili kullanılan terminoloji ulusal güvenlik söylemlerinde kullanılan terminoloji ile uyum içindedir. Tehditler, başarısızlıklar, kazalar ve saldırılar olarak ayrılmaktadır. Başarısızlıklar yazılım tasarımındaki hatalar, insani hatalar, virüsler; kazalar doğal afetler gibi rastgele çıkan olaylar; saldırılar ise düşmanlar tarafından tasarlanan zarar verici olaylardır. (Collins, 2017: 363) Bilgi güvenliği, bilgiye sürekli olarak erişilebilen bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkalarının eline geçmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci olarak tanımlanmaktadır. Bilgi güvenliğinin temel unsurları; gizlilik, bütünlük ve erişilebilirlik olarak ifade edilmektedir. (Yılmaz, 2015: 1-2) Bilgi altyapısının teknik boyutları sürekli değişikliğe uğradığı için siber güvenlik söylemi hiçbir zaman durağan olmamıştır. Güvenlik çalışmaları alanında en son yaygınlaşan konulardan biri siber güvenliktir. Bilgi ile birlikte onun üretimi, yönetimi ve manipülasyonu her zaman önemli bir olgu olmuştur. Bilgi, inanç ve fikirleri kontrol etmek, askeri güç ve hammaddeler gibi somut kaynaklarla güvenlik elde etmek kadar önemlidir. (Collins, 2017: 8) Günümüzde bilgi güvenliği konusunda dijital veri güvenliği kavramı ön plana çıkmaktadır. Dijital veri güvenliğini de, “elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür” (Yılmaz, 2015: 3) biçiminde tanımlamıştır. Kişilerin ve kurumların, bilişim teknolojilerini kullanırken kendilerini bekleyen tehdit ve tehlikeleri daha önceden analiz ederek gerekli önlemleri aldıklarında dijital veri güvenliğini sağlamış olacağı da düşünülmektedir. (Yılmaz, 2015: 3)

Kent “Sürekli toplumsal gelişme içinde bulunan ve toplumun, yerleşme, barınma, gidişgeliş, çalışma, dinlenme, eğlenme gibi gereksinmelerinin karşılandığı, pek az kimsenin tarımsal uğraşılarda bulunduğu, köylere bakarak nüfus yönünden daha yoğun olan ve küçük komşuluk birimlerinden oluşan yerleşme birimi” (Keleş, 1998: 75) olarak tanımlanmıştır. Yine kent, “toplumsal bakımdan benzerlik göstermeyen bireylerin oluşturduğu, göreceli olarak geniş, yoğun nüfuslu ve mekânda süreklilik niteliği olan yerleşme” (Keleş, 2004: 107) olarak da tanımlanabilir.

Kent güvenliği; kent sınırları içerisinde yaşayan insanların, gerek sosyal gerekse iş yaşamında can ve mal güvenliğinin sağlanmasıdır. Devletlerin sınırları içerisinde çatışmaların artması, uluslararası toplumu toplumsal şiddet, göç hareketleri, yoksulluk ve işsizlik, örgütlü suç ve terörizm gibi konularda daha fazla meşgul etmekte ve bu konularla daha fazla ilgilenmeye zorlamaktadır. (Kılıç, 2019: 50-51) Kentlerde güvenliğin olmamasının işsizlik, yoksulluk, eğitimsizlik gibi nedenlerinin bulunduğu bilinmektedir. Kentle bütünleşemeyen birey topluma yabancılık çekmekte ve bir anlamda suça yönelmektedir. Burada bireyin yaşam kalitesi kentin yaşam kalitesi ile birlikte hareket etmektedir. Hem bireyin toplumda refah içinde yaşaması hem de kentin yaşam kalitesinin sağlanması kent güvenliği için en temel olgu olarak ifade edilmektedir. (Kılıç, 2019: 50-51) Bununla birlikte, güvenli kentin bileşenleri, kentin yaşam kalitesinin yükselmesi, yaşanılan mekândan memnun olunması ve yaşanılan mekânla ilgili olarak bireylerin olumlu bir algıya sahip olması, kentte çöküntü alanları, terk edilmiş mekânlar ve suçluları suç işlemeye yönelten mekânların olmaması, kentte ışıklandırmanın yeterli olması, kentte işsizliğin düşük düzeylerde olması ve kente sosyal, ekonomik ve çevresel yatırımların yapılması olarak belirtilmektedir. (Kılıç, 2019: 53)

Kent ve kent güvenliği tanımlarının yanında, genel olarak akıllı kent tanımında tam bir kabule ulaşamadığı ifade edilmektedir. (Akbulut, 2009: 38) Akıllı kent kavramının ise üzerinde aynı fikirde olunan bir tanımının olmadığı belirtilmektedir. (Bilici ve Babahanoğlu, 2018: 127) Bir anlamda, akıllı kentler, kentlerde yaşam kalitesinin iyileştirilmesi için dijital teknolojilerin ve verinin günümüzde yoğunlaşan kullanımı ile birlikte kent yönetiminin bütünleştirilmesi olarak ifade edilmektedir. Yükselen büyük veri ve veri madenciliği uygulamaları, açık veri ve açık kodlu yazılımlar ile Web 2.0 ve sosyal medya uygulamalarının yaygınlaşması 1990’ların sonundan itibaren gündeme gelen e-belediyecilik kavramını da dönüşüme yönlendirmiş ve artık e-belediyeciliği aşan “akıllı kent” aşamasına geçildiği söylenmektedir. (Köseoğlu ve Demirci, 2018: 42) Akıllı kentin öğeleri akıllı ekonomi, akıllı toplum, akıllı ulaşım, akıllı çevre, akıllı yaşam, akıllı teknoloji ve akıllı şebeke olarak tasnif edilebilir. (Gül ve Atak Çobanoğlu, 2017: 1549) Akıllı kentler, sunduğu kentsel hizmetler bakımından kullanıcıların tercihlerini ve ihtiyaçlarını dikkate alan, farklı araçlarla her yerden erişilebilen, çok sayıda ve farklı uygulamalardan veri ve hizmetlerin bütünleşmesine dayanan kentler olarak ifade edilebilir. (Akbaş, 2018: 141) Akıllı kentlere ulaşabilmek için akıllı süreçler geliştirmek, mevcut süreçlerin etkinliğini ve verimini arttırmak için veri odaklı yönetim yaklaşımı benimsemek gerekmektedir. (Akdamar, 2017: 204) Bunun yanında, akıllı kentler bir ağ yönetimi olarak, nesnelerin interneti, bulut bilişim ve farklı araçlar sayesinde birbirine bağlıdır. Söz konusu ağın yönetimi insan müdahalesinden bağımsız olarak çalışmaktadır. Akıllı kentler, yeşil uygulamaların temel gerekliliklerini karşılamak için verimli kaynak kullanımına dayanmaktadır. (Köseoğlu, 2019: 34) Akıllı kentler içerdiği teknik altyapı sayesinde küresel ölçekte başarı kazanmaktadır. Akıllı kent yoğun bilgi, teknoloji ve iletişim kullanımına dayanmaktadır. Elektronik içeriğin geliştirilmesini esas almaktadır. Çoğunlukla ”güçlendirilmiş gerçeklik” olarak tanımlanmaktadır. (Kaygısız ve Aydın, 2017: 60) Nesnelerin interneti (IoT) akıllı kentlerin yapılandırılmasına yönelik erişilebilir açık veriye açık sistemler sayesinde ulaşmaktadır. (Memiş, 2018: 70) Bilgi teknolojisinin kentler üzerindeki etkisine ilişkin yapılan varsayımlar, online alışverişte, online bankacılıkta, online uzaktan öğrenimde büyük bir artışın olacağıdır. Bu bağlamda e-iş, e-devlet, e-hizmet olaylarının gelişeceği üzerinde durulabilir. (Castells, 2008:526-529-531) Akıllı kentleri oluşturan veri toplanmasına ilişkin hukuki altyapının sağlanması ve idari düzenlemelerin yapılması gerekmektedir. Ticari sır, devlet sırrı, özel hayatın gizliliği gibi konularda veri toplanması ve paylaşılmasına ilişkin esasların güvence altına alınması vurgulanmaktadır. (Köseoğlu, 2019: 37)

1. **AKILLI KENTLERİN GÜVENLİĞİ**

Kamusal güvenliğin sağlanması, devletlerin en eski fonksiyonlarından birisidir. Ulusal güvenlik politikalarının yanında, 1980’lerden itibaren kent güvenliği kavramı da politika gündeminin bir parçası haline gelmiştir. Bu dönemde hem kentleri ilgilendiren güvenlik problemleri artmış hem de nitelik bakımından farklılaşmıştır. Yine 1980’lerden itibaren kamu sektörünün büyük kısmının özelleştirilmesi ve kısıtlamalardan arındırılması ve 1990’lardan itibaren küreselleşmenin hızlanması, önemli altyapıların birçoğunun özel (ulus-ötesi) girişimcilere geçmesiyle sonuçlanınca, önemli altyapıları koruma daha önemli hale gelmiştir. Bu gelişme, piyasa güçlerinin belli önemli altyapı sektörlerinde arzu edilen güvenlik düzeyinin sağlanmasında yeterli olmadığı bir durum ortaya çıkarmıştır. En fazla dile getirilen örnekler, bankacılık ve finans, devlet hizmetleri, telekomünikasyon, bilgi ve iletişim teknolojileri, acil durum ve kurtarma hizmetleri, enerji ve elektrik, sağlık hizmetleri, ulaştırma, lojistik ve dağıtım, su sağlanması’dır. (Collins, 2017: 373) Kent güvenliği, 1987’de düzenlenen Kentsel Güvenlik İçin Avrupa Forumu’nda tartışılmış, 1992’de Avrupa Konseyi tarafından duyurulan Avrupa Kentsel Şartı’nda kent sakinlerinin sahip oldukları haklar arasında sayılmıştır. Şarta göre Avrupa kentlerinin yurttaşları imkânlar el verdiği ölçüde emin ve güvenli bir kentte yaşama hakkına sahiptir. 1996’da Afrikalı belediye başkanlarının kentsel suç ve şiddetle mücadele konusundaki talepleri üzerine BM-HABİTAT tarafından “Daha Güvenli Kentler Programı” başlatılmıştır. Böylece kent güvenliği konusu, yerel ve ulusal sınırların ötesinde küresel siyaset gündemine eklemlenmiştir. (Köseoğlu, 2019: 25)

Kent güvenliğini tehdit eden unsurlar arasında suç ve şiddet öne çıkmaktadır. Kolektif şiddet, kadına yönelik şiddet, nefret suçları, organize suçlar, uyuşturucu ve insan kaçakçılığı ve terörizm bu kapsamda değerlendirilebilir. (Caragliu ve Del Bo, 2019: 375) Kentte yaşayanların suç ve şiddete karşı kişisel güvenliğinin sağlanmasının yanında dijitalleşmeyle birlikte bilgi güvenliği ve siber güvenlik; iklim değişikliği ve doğal afetlerin etkileriyle güvenli kentsel altyapı ve planlama sistemlerinin kurulması; salgın hastalıklarla mücadele, su, orman alanları ve tarım arazilerinin korunması ve gıda güvenliği gibi konular ise sağlık güvenliğinin günümüzde önem kazanmasına neden olmaktadır. (Zygiaris, 2013: 221-224)

Kişisel güvenlik, günümüzde halen kent güvenliğinin en önemli boyutunu oluşturmaktadır. Son yıllarda metropol kentlerde yaşanan terör saldırıları insanlarda kişisel ve toplumsal huzur ve güven açısından derin izler bırakmaktadır. Özellikle genç işsizliğin yüksek olduğu kentlerde gençlerin şiddet eğilimlerinde artışlar gözlenebilmektedir. Öte yandan akıllı kentler kapsamında kullanılan sensörler, drone ve kamera sistemleri gibi akıllı teknolojiler kentsel hizmetlerin etkin ve verimli yürütülmesine katkı sağlamaktadır. Ancak akıllı kent uygulamalarına yapılan yatırımlar, siber güvenlik yatırımlarıyla birlikte gerçekleşmediği takdirde güvenlik sorunlarını artırıcı bir etkiye sahip olmaktadır. Güvenli kentlerin önemli unsurlarından biri de sağlık güvenliğidir. Kentte yeterli yürüyüş yolu ve yeşil alanların bulunması, trafik kazalarının önlenmesi ve hava kirliliğinin kontrol altına alınması, sağlıklı gıda temini ve gıda denetimlerinin yapılması gibi faaliyetler sağlıklı kentlerin inşasında önemli role sahiptir. (Köseoğlu, 2019: 26)

İstenilen güvenlik seviyesini sağlayamadıkça, akıllı kentler akıllı sayılmazlar. Genel güvenlik ve mahremiyet bütünlük, gizlilik, erişim kontrolü, gizlilik ve reddedilme şartlarını içermektedir. Akıllı kentler, bu ortamlarda yaşayan insanlar hakkında ayrıntılı bilgiler içeren fiziksel alanlardan algılanan verileri kullanmaktadır. Bu verilerin yolculuğu bir sensör düğümünde başlar ve kullanıcı uygulamasında sona ermektedir. Bu nedenle, akıllı kent benzersiz güvenlik gereksinimleri ortaya koymaktadır, çünkü verileri birbiriyle paylaşan birbirine bağlı sistemler sistemidir. Bu, akıllı kent hizmetlerinin yaygın kullanımını engelleyen temel argümandır. (Butt ve Afzaal, 2017: 2)

Akıllı bir kentin güvenlik gereksinimleri iki kategoriye ayrılabilir: Operasyonel güvenlik gereksinimi; kullanılan teknolojinin ve altyapının güvenli olmasını ve siber saldırılara karşı bağışıklığa sahip olmasını sağlamaktır. İkinci; veri ile ilgilidir. Altyapı içerisinde farklı teknolojiler kullanılarak üretilmekte ve iletilmektedir. Bununla birlikte, veri güvenliği ve koruması, işletim güvenliğine bağlıdır. (Butt ve Afzaal, 2017: 7)

Güvenliğin yanında önemli bir konu olarak karşılaşılan gizlilik kavramı, istenmeyen ilgiden ve korunmadan uzak durma halidir. Ancak, gizlilik kavramı, farklı kültürlere, bağlamlara ve bilgi türüne göre farklılık gösterir. Gizlilik çeşitli boyutlara sahiptir: (Martinez-Ballesté, Pérez-Martinez, Solanas, 2013: 115) Kimlik gizliliği, bir bireye ilişkin kişisel verilerin korunması ile ilgilidir. Bedensel mahremiyet, fiziksel yönlerin korunmasına odaklanmaktadır. Bölgesel gizlilik, bir bireyin kişisel mülkünü ve alanını korumaktadır. Mobilite gizliliği, konum koordinatlarını ve izleme ile ilgilidir. İletişim gizliliği, gizlice dinlenmeye karşı iletişim kanallarının korunması ile ilgilidir. Bu kanallar arasında donanım aygıtları bulunur, veri aktarımını kolaylaştıran iletişim, kablolu ya da kablosuz iletişim araçlarıdır ancak bunlarla sınırlı değildir. İşlem gizliliği sorguları ve yanıtları izlemeye karşı korumaya odaklanmaktadır.

Bununla birlikte kurumlara ve bireylere yapılan ya da yapılacak olan siber saldırılar genellikle aşağıdaki üç saldırının birinde kategorize edilmektedir. (Martinez-Ballesté, Pérez-Martinez, Solanas, 2013: 116-117):

1. Uygunluk saldırıları: Bu sınıflandırma, bazı hizmetleri reddeden saldırılar veya sistemi tamamen yıkanlar içindir.

2. Gizlilik saldırıları: Bu saldırılar yetkisiz izleme ve bilgi erişimi ile ilgilidir.

3. Bütünlük saldırıları: Bu saldırılar, saklanmış bilgiyi birleştirmek veya değiştirmek için sisteme girmeyi amaçlamaktadır. Ayrıca, bu saldırılar kritik hizmetleri durdurmak, sistemi virüslere bulaştırmak veya sistemi etkin kılmamak gibi konfigürasyonları değiştirmektedir.

**3. AKILLI KENTLERDEKİ GÜVENLİK AÇIKLARI VE SORUNLARI**

Akıllı kentlerde unutulmaması gereken kamusal güvenliğin sağlanması ile birlikte bireyin güvenliğinin ve gizliliğinin de sağlanması, birey mahremiyetinin de korunmasıdır. Bu bağlamda, bir sistemin güvenlik açığı, zayıf şifreleme, insan hatası gibi sorunların neden olabileceği güvenlik açıkları şeklinde ifade edilmektedir. Akıllı bir kentte sistemlerin kullanımını siber saldırılara karşı savunmasız bırakan çok yönlü bileşenler mevcuttur. Bu bileşenler karmaşık ve karşılıklı olarak birbirine bağımlıdır. Bununla birlikte, bu karmaşıklık ve birbirine bağımlılık kamusal alanlarda fiziksel olarak dağılmış sensörlerle daha da ağırlaştırılmıştır. Bunlar şu şekilde sıralanabilir: (Butt ve Afzaal, 2017: 7-9)

Algılama Katmanında Sınırlandırılmış Cihazlar: Nesnelerin interneti, tüm radyo frekansı ile tanımlama ve sensör cihazlarını internete bağlamaktadır. Radyo frekanslı tabanlı nesneler, ulaşım sistemleri için kullanılan akıllı kartlar, internete bağlanmak için bir okuyucu ve bir ağ geçidi gerektirdiği için pasiftir. Öte yandan, sensör aygıtları sensörler, aktüatörler ve mikro denetleyicileri içermektedir. Günümüzde, sıcaklık, nem, konum, hız, yakınlık gibi farklı fenomenleri algılamak için mevcut çeşitli sensörler bulunmaktadır. Dahası, geleneksel olarak cihazlar; elektronik cihazlar, kapılar ve ışıklar bile kullanıcılar tarafından uyarılmakta ve uzaktan kontrol edilmektedir. Bu sensör cihazlarının çoğu kaynaklarla sınırlıdır ve etkili bir güvenlik veya gizlilik mekanizmasına sahip değildir. Böylece, bu cihazlar saldırıya açık hale gelmekte ve güvenliği tehdit eden riskler için her türlü bağlantı portalı açılmaktadır.

Zayıf Şifreleme: Ağa bağlı bir yazılım aygıtını güvenceye almanın geleneksel yollarından biri, şifreleme kullanmaktır. Şifreli kanalın, sistemi saldırganlara karşı koruma sağladığına inanılmaktadır. Mevcut akıllı kent girişimleri, sistemleri test etmeden dağıtmaktadır. Siber güvenlik tehditleri için akıllı kentlerde IoT cihazlarının çoğunun kısıtlamaları bulunmakta ve uygun şifreli bağlantıları destekleyememektedir. Şifreli bağlantılar bile diğer güvenlik sorunlarına eğilimlidir, çünkü saldırganlar hala yan kanal ve soğuk önyükleme saldırıları kullanarak şifreli sistemlere girmektedir. Bu sorunlar akıllı kent sistemlerinin geniş kabul görmesinin önündeki en büyük engellerdendir.

Entegrasyon Katmanında İletişim Teknolojileri: Yeteneklerine bağlı olarak farklı IoT cihazları tarafından kullanılan çeşitli iletişim teknolojileri bulunmaktadır. Bu teknolojiler arasında RFID, NFC, Bluetooth, WiFi, 3G ve 4G mobil teknolojilerine dayalı 6LoWPAN sayılabilir. Bütün bu teknolojilerin güvenliği bulunmaktadır. Bu, en gelişmiş teknolojilerin bile altyapısında zayıflıkları vardır.

Bulut Katmanı: Bulut katmanı, akıllı kentlerde ölçeklenebilirliği desteklemek için gereken esnekliği sağlamaktadır. Ancak, bulut sistemlerinin dış kaynak kullanımı, çok kiracılık ve yoğun hesaplama gerektiren büyük veri gibi güvenlik sorunları da bulunmaktadır. Veriler üzerinde daha az kontrol sağlayan ve sonunda güvensizliğe neden olan uzaktan erişim gizlilik ihlalleri dış kaynak sağlamak gerektirir. Bu, bulut sağlayıcısının güvenilir olduğundan ve dış kaynaklı verilerin güvenlik ve gizlilik perspektifinden doğrulandığından emin olarak ele alınabilir. Çok kiracılık, birden çok kullanıcının bulut platformunu kullanmasını sağlamaktadır. Bu nedenle, çok kiracılık çeşitli güvenlik açıkları ortaya çıkarmaktadır. Bir diğeri, bulut bilişim ile ilgili husus, geleneksel güvenlik tekniklerini çok fazla gerektirdiğidir. Bulutun muazzam miktarda veriyle başa çıkmak için iletişim veya hesaplama yükü bulunmaktadır. Bu ek yük, örneğin; uzaktan saklanan tüm veri kümesinin karma olması durumundadır.

Sistemlerin Karmaşıklığı ve Cascade Etkisi (Öngörülmeyen Olaylar Zinciri): Akıllı kent sistemleri, heterojen cihazlar ve ağlar içeren büyük ölçekli ve karmaşık sistemlerdir. Akıllı kent mimarisinin birden fazla katmanı bulunmaktadır. Her katman cihaz ve teknolojilerin bolluğundan oluşmaktadır. Birçok paydaşın varlığında riski ölçmek ve azaltmak bileşenleri ile diğer sistemler arasındaki karşılıklı bağımlılık ağı bulunmaktadır. Çoklu bağlantılar sistem bileşenleri, her sistem bağımsız olsa bile onları güvenlik risklerine maruz bırakmaktadır. Ayrıca, bu karşılıklı bağımlılıklar bir sistem bileşeninin ara yüzünü korurken veya yükseltirken bir sorun haline gelmektedir. Yüksek derecede birbirine bağlı bileşenler ayrıca, örneğin bir sisteme yapılan bir saldırı; diğer sistemleri de ciddi şekilde etkileyebilir. Bu güvenlik riski, başarılı bir saldırının bir sistemin tüm sistemlerini yıkabileceği akıllı bir şehrin yönetiminin gerçekleştirilmesini büyük ölçüde zorlamaktadır.

Yazılım Hataları: Yazılım tabanlı bir cihaz, saldırganların sisteme gizlice girmesi için delikler açan böcek yazılımı nedeniyle siber saldırılara açık hale gelebilmektedir. Bu faktör daha çok, bu hataların bulunduğu milyonlarca kod satırı içeren karmaşık sistemlerde yoğunlaşmaktadır. Saldırganlar için bir arka kapı açabilmektedir. Bir saldırgan akıllı şehir sistemine girdiğinde sistemin kontrolünü ele geçirebilir ve mevcut verileri kullanabilir.

Kullanıcı Ekipmanı: Akıllı bir kentin farklı kullanıcıları kalabalıkta, güvenliği tehdit edici risklere açık olan mobil cihazlarını kullanarak, katma değerli servisler tüketebilir ve katılabilir. İlk olarak, her cep telefonu kendi IMEI’si tarafından benzersiz bir şekilde tanımlanabilir. Bu IMEI kişisel bilgileri ve mobil cihazları izlemek için kullanılabilir. Ayrıca, birçok kullanıcı kötü niyetli uygulamalara yanlışlıkla erişim izni de verebilmektedir. Bu tür bir uygulama izin aldığında, kullanıcının bilgilerine ve cihazın kontrolüne erişebilmektedir.

İnsan Faktörü: Akıllı kent sistemlerinin tamamen özerk bir şekilde çalışmasına izin verilmemektedir. Bu nedenle, insan her zaman akıllı kent sistemleri ile etkileşimin karar verme döngüsünde yer almaktadır. Yanlışlıkla veya kasıtlı olarak insan hatası veri sızıntısına veya sistem arızasına neden olabilmektedir. Akıllı bir kent kullanıcısı, örneğin belediyenin çalışanı sistemi sabote edebilir.

Eski Sistemler: Eski sistemler kentin her alanında bulunmaktadır. Bu sistemlerinin yetkilerinin çoğu mevcut altyapının akıllı bir kente entegre edilmesini gerektirir. Eski sistemlerin çoğu güvensiz ve çoğunlukla bugünün güvenlik zorlukları göz önünde bulundurulmadan on yıllar önce oluşturulmuştur. Bu sistemler düzenli olarak güncellenmemekte ve saldırganlara giden çevre yolu doğal güvenlik açıklarına sahiptir. Akıllı bir kentteki yeni sistemlerin bile herhangi bir kesinti olmadan, düzenli olarak güncellenmesi gerekmektedir.

1. **AKILLI KENT ÖRNEKLERİ**

Bu bölümde bazı kentlerdeki akıllı uygulamalar ile Türkiye’deki durum kısaca verilmeye çalışılmıştır.

* 1. Melbourne

Belirli güvenlik konuları doğrudan belediyelerin görev alanına girse de genelde suç ve şiddetle mücadele, uyuşturucu veya iklim değişikliğine karşı tedbir alınması gibi politik konular kentteki resmi ve hükümet dışı aktörlerin birlikte çalışmasını gerektirmektedir. Bu nedenle metropoliten kentlerde farklı güvenlik konularına ilişkin kapsamlı stratejiler ve eylem planlarının geliştirilmesine ihtiyaç bulunmaktadır. Melbourne Belediyesi 2014-2017 Güvenli Kent Stratejisi buna örnek verilmektedir.“Melbourne kenti insanların güvenli, birbirine bağlı, gündüz ve gecenin herhangi bir saatinde kent yaşamına katılabileceği bir yer” olma vizyonu doğrultusunda beş konuya odaklanan bir eylem planı geliştirmiştir. Bu konular; müreﬀeh ve yaratıcı 24 saat canlı bir kent, güvenli ve kapsayıcı kent, dayanıklı çocuklar ve gençler, uyuşturucu ve alkol kullanımıyla ilgili zararların azaltılması, güvenli ve memnuniyet oluşturucu bir ortamın inşası olarak sayılmaktadır. (Beyond the Safe City: Strategy 2014-2017, Melbourne, 2019)

* 1. Atina

Atina’da 1982’de araç trafiğini sınırlandırmak amacıyla geliştirilen alternatif sistemde plakasının sonu tek ve çift rakamla biten araçlara farklı günlerde kent merkezine giriş izni verilmiştir. Ancak bu politika etkili olmamıştır. Çünkü ailelerin farklı bir rakamla biten ikinci bir araç satın alma, taksi ve motosiklet kullanma oranlarının hızlıca artmasına neden olmuştur. Bu nedenle, sistem karbon emisyon oranlarına göre çevreyi daha az kirleten araçlara öncelik verme şeklinde değiştirilmiştir. (Köseoğlu, 2019: 27)

* 1. Daejeon

Daejeon’da (Güney Kore) hususi araç kullanımını azaltmak için 2012’de “Arabasız Bir Gün” adı verilen bir kampanya yürütülmüştür. Kampanyaya katılanlara haftanın bir günü 07:00’dan 22:00’a kadar hususi araçlarını kullanmazsa otomobil vergisinden yüzde 10 kesinti, park ücretinde yüzde 30 indirim, araç sigorta primlerinde yüzde 8,7 indirim, araç muayene ücretinde yüzde 10 indirim ve toplu taşımada ücretsiz sigorta hizmeti gibi faydalar sağlanmıştır. (Köseoğlu, 2019: 27)

* 1. San Francisco

San Francisco’da koruyucu aile, çocuklar için göz hapsi ve akıl sağlığı departmanları bölge başsavcısı ile vaka bilgilerinin kurumlara verilmesi ve kurumlar arasında sınırlı paylaşımı konusunda uzlaşmıştır. Böylece kurumlar hizmetlerden yararlanmadaki çakışmaların farkına varmışlardır. Ayrıca hizmetleri kullanan iki bin çocuğun departmanların kaynaklarının yarısını tükettiğini ve çoğunun da kurumlara yürüme mesafesinde olduğunu görmüşlerdir. Veri paylaşımı sayesinde İnsan Hizmetleri Kurumu (Human ServiceAgency) hizmet sunumunu en ihtiyacı olan kullanıcılara yönlendirmiş, hizmetlerini güncellemiş ve vaka koordinasyonunu geliştirmiştir.(Köseoğlu, 2019: 36)

* 1. Helsinki, Espoo, Vantaa ve Kauniainen

2010’da Helsinki, Espoo, Vantaa ve Kauniainen kentleri bölgesel bilgiye hızlı ve kolay bir şekilde erişilmesini amaçlayan bir web hizmeti olarak Helsinki Region Infoshare (HRI) kurmuştur. “https://hri.fi/en\_gb/” adresinden ulaşılabilen açık veri platformunda 1.000 civarında veri seti ücretsiz olarak kullanıma açılmış ve bir süre sonra rutin belediye faaliyetlerinin bir parçası haline gelmiştir. Web sitesinde paylaşılan veri temelde istatistikî bilgi olup genelde CBS tabanlıdır. Zaman içinde paylaşılan veri kategorileri artarak 12’ye ulaşmıştır (konut, yerel yönetim, haritalar, kültür ve rekreasyon, trafik ve turizm, eğitim, imar, ekonomi ve vergileme, sağlık ve sosyal hizmetler, nüfus, çevre ve doğa). Paylaşılan veri AR-GE faaliyetleri, karar verme, görselleştirme, veri gazeteciliği ve metropoliten alanda sunulan kamu hizmetleri için uygulama geliştirilmesi gibi alanlarda kullanılmaktadır.(Köseoğlu, 2019: 36)

* 1. Barcelona

Barcelona’da çöp kutularına yerleştirilen sensörler çöp seviyesini izlemekte ve çöp toplama hizmetleri düzenlenmektedir. Kentin yeşil alanlarında sulamayı yönetmek için akıllı su sistemlerinin kullanılmaktadır. Sokak lambalarındaki sensörler gün ışığına göre ışık yoğunluğunu ayarlamaktadır.(Gül ve Atak Çobanoğlu, 2017: 1553)

Bu kentler özelinden çıkılıp Türkiye’ye bakılacak olursa; Türkiye’de hem merkezi idarede ilgili bakanlık ve kurumlar bünyesinde hem de bu konuda politikalar geliştiren belediyelerde akıllı şehirlere ilişkin idari birimler bulunmaktadır. Ayrıca ulusal düzeyde Bilgi Toplumu Stratejisi ve Eylem Planı ve E-Devlet Stratejisi ve Eylem Planı gibi politika ve strateji belgelerinde akıllı şehirlere ilişkin altyapının ve uygulamaların geliştirilmesi konusunda amaç ve hedefler belirlenmiştir. Yerel ölçekte bakıldığında, belediyeler kendi stratejik planlarında ve politikalarında konut ve yerleşim, ulaşım ve trafik, acil yardım ve afet yönetimi gibi alanlarda akıllı şehir uygulamalarını kullanmaktadır. Cumhurbaşkanlığı Hükümet Sisteminde çıkan kararnamelerde ise, Cumhurbaşkanlığı teşkilatında teknoloji politikalarını belirlemek ve uygulamaları takip etmek üzere bir başkanlık ofisi ve politika kurulunun oluşturulması ifade edilmektedir. Çevre ve Şehircilik Bakanlığı ise 2019-2022 Ulusal Akıllı Kentler Stratejisi ve Eylem Planı hazırlık çalışmalarını sürdürmektedir. (Köseoğlu ve Demirci, 2018: 45)

**SONUÇ ve TARTIŞMA**

Kentte bir silah sesi duyulduğunda, onun nereden geldiğini bulmak, emniyet güçlerinin işlerini kolaylaştırır mı? Ya da dar bir sokaktaki evde çıkan yangına en kısa sürede ulaşma ve müdahale etmenin en iyi yöntemi ne olabilir? Bu sorular kentlerin akıllı ve güvenli olma yollarında önemli sorulardır. Zaten bir kentte yaşayan insanlarda, kameraların, sensörlerin, veri ağlarının yaşama, çalışma ve seyahat etme biçimini nasıl değiştirdiğini fark etmektedirler.

Kentler hem sürekli büyümekte ve genişlemekte hem de küresel olarak erişilebilir duruma gelmektedir. Kentlere yönelik insan merkezli tehditler de artmaktadır. Kent yönetimlerinin, büyüme ve genişleme ile meydana gelen sorunlara çözüm bulmaları için kamu güvenliğine öncelik vermeleri gerekmektedir. Ulaşım, atık yönetimi, aydınlatma gibi sorunlara büyük oranda çözümler getiren akıllı kentler; kamu güvenliği ve afetler için de çözümler sunabilmektedir.

Akıllı kentler, sahip oldukları konforun yanı sıra güvenli kentlerdir. Akıllı kentte ulaşım, altyapı, aydınlatma gibi unsurlar ve kamu güvenliği oldukça önemlidir. Kamu güvenliğine yönelik olarak geliştirilen tüm akıllı uygulamalar, bu sayede devlet ve yerel hükümetlerin işlerini kolaylaştırmaktadır.

Ayrıca siber güvenlik zamanla ve mekânla değişmektedir, hatta yeri geldiğinde teknoloji güvenliğidir. Değişen güvenlik politikası alanında dikkat çekmektedir. Önemli altyapılara yönelik büyük çaplı, sistematik ve yıkıcı olayların gerçekleşmesi ihtimali bulunmaktadır. Yapılan çalışmalardan bu tür olaylara karşı alınacak tedbirler olduğu ve bunlar alındığı takdirde kentlerde istenilen düzeyde hem güvenlik hem de kişi gizliliğinin sağlanabileceği üzerinde durulmaktadır. Bununla birlikte, akıllı kentlere olan ya da olacak güvenlik tehditlerini kavramlaştırma ve onlara tepkiler verme konusunda temel aktörlerin sübjektif bir şekilde ortak bir anlayışa ulaşma süreçlerini belirleyen bağlamlara ve şartlara kaymalıdır, politikalar üretilmelidir, varolan politikalar uygulanmaya çalışılmalıdır.

Yine de akıllarda kentlerin geleceği ile ilgili sorular ucu açık bir şekilde yer alabilmektedir. Örneğin, Hindistan gelecek birkaç on yılda 100 yeni kent kurmayı planlamaktadır. Suudi Arabistan ve Malezya yeni ve canlı ekonomik merkezlere ihtiyaç duymaktadır. Bunların yanında, gelişmiş ülkeler de dijital küresel hayatta ya da ekonomide geride kalmamak için geçmişten miras aldıkları kentleri yeniden canlandırmak durumundadırlar. Bu canlandırmayı yaparken de güvenlik ve gizlilik açıklarını düzenleyerek ve kurumların ve kişilerin güvenliğini ve gizliliğini sağlayarak yol almaları gerekmektedir.

**KAYNAKÇA**

Akbaş, İ. (2018). “Akıllı Kentler: AB ve Türkiye Analizi.”*Sosyal Bilimler Dergisi*, 26, 139-163.

Akdamar, E. (2017). “Akıllı Kent İdealine Ulaşmada Büyük Verinin Rolü.”*Kent Kültürü ve Yönetimi Hakemli Elektronik Dergi*, 10(2), 200-218.

Akbulut, M. R. (2009). “21. Yüzyıl Kentleri İçin Teknolojik Kurgular.”*Tasarım+Kuram*, 7, 36-53.

Aydoğdu, İ. B. (2011). “Bilgi Toplumunda İnsani Güvenlik ve İnsan Hakları Sorunlarının Etik Bağlamında İncelenmesi”, *Uluslararası 9. Bilgi, Ekonomi ve Yönetim Kongresi Bildirileri*, Saraybosna, Bosna-Hersek, 1770-1783.

Aydoğdu, İ. B. (2013). “Bilgi Kenti: Bir Değişimin Anatomisi”, *Bilgi Ekonomisi ve Yönetimi Dergisi*, VIII, II, 15-26.

Beyond the Safe City: Strategy 2014-2017”, Melbourne, https://www.melbourne.vic.gov.au/SiteCollectionDocuments/beyond-safe-city-strategy-2014.pdf, (Erişim tarihi: 11.05.2019)

Bilici, Z. ve Babahanoğlu, V. (2018). “Akıllı Kent Uygulamaları ve Konya Örneği.”*Akademik Yaklaşımlar Dergisi*, 9(2), 124-139.

Butt, T. and Afzaal, M. (2017). Security and Privacy in Smart Cities: Issues and Current Solutions, [www.researchgate.net](http://www.researchgate.net), 1-15.

Caragliu, A. Del Bo, C. F. (2019). “Smart Innovative Cities: The Impact of Smart City Policies on Urban Innovation.”*Technological Forecasting&Social Change*. 142, 373-383.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür*, Birinci Cilt, Ağ Toplumunun Yükselişi, Çev., Ebru Kılıç, 2. Baskı, İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Collins, A. (2017). *Çağdaş Güvenlik Çalışmaları*. Çev., Nasuh Uslu, İstanbul: Uluslararası İlişkiler Kütüphanesi.

Gül, A. ve Atak Çobanoğlu, Ş., (2017). “Avrupa’da Akıllı Kent Uygulamalarının Değerlendirilmesi ve Çanakkale’nin Akıllı Kente Dönüşümünün Analizi.”*Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Kayfor15 Özel Sayısı*, C.22, 1543-1565.

Kaçar, D. (2007). “Kentsel Mekâna Alternatif Bir Bakış: Kentin Zamanı, Zamanın Kenti.”*Anadolu Sanat*, 18, 57-63.

Kayan, A. (2015). “Küreselleşmenin Kentler Üzerindeki Etkileri ve Küresel Kentlerin Özellikleriyle İlgili Bir Değerlendirme.”*Girişimcilik ve Kalkınma Dergisi*, 10 (1), 271-295.

Kaygısız, Ü., Aydın, S. Z., (2017). “Yönetişimde Yeni Bir Ufuk Olarak Akıllı Kentler.”*Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 9(18), 56-81.

Keleş, R. (1998). *Kentbilim Terimleri Sözlüğü*, Ankara: İmge Kitabevi.

Keleş, R. (2004). *Kentleşme Politikası*, 8. Baskı, Ankara: İmge Kitabevi.

Kılıç, E. (2019). *Yoksulluk, Kent Güvenliği ve Suç İlişkisinin Kentsel Yaşam Kalitesine Etkileri: İzmir Örneği.* Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

Köseoğlu, Ö. ve Demirci, Y. (2018). “Akıllı Şehirler ve Yerel Sorunların Çözümünde Yenilikçi Teknolojilerin Kullanımı.”*Uluslararası Politik Araştırmalar Dergisi*, 4(2), 40-57.

Köseoğlu, Ö. (2019). *Metropoliten Kentlerin Geleceği, Yeni Yaklaşım, Model ve Uygulamalar*. İstanbul: Seta Yayınları.

Martinez-Ballesté, A.,Pérez-Martinez, P. A. And Solanas, A., (2013) *The pursuit of citizens' privacy: a privacy-aware smart city is possible,* vol. 51, IEEE, 136-141. **DOI** [10.1109/MCOM.2013.6525606](https://doi.org/10.1109/MCOM.2013.6525606)

Memiş, L. (2018). “Akıllı Teknolojiler, Akıllı Kentler ve Belediye Örgütlenmesinde Dönüşüm.”*Yasama Dergisi*, 36, 66-92.

Yılmaz, E. (2015). *Öğretmenlerin Dijital Veri Güvenliği Farkındalığı.* Yayınlanmamış Doktora Tezi, Eskişehir Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.

Zygiaris, S. (2013). “Smart City Refence Model: Assisting Planners to Conceptualize the Building of Smart City Innovation Ecosystems.”*J KnowlEcon*, 4, 217-231. DOI 10.1007/s13132-012-0089-4

1. **Dr. Öğretim Üyesi, Fırat Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, Elazığ,** **ilke@firat.edu.tr****, tlfn:05339573449** [↑](#footnote-ref-1)