Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA AKILLI ŞEHİRLER VE VERİ MAHREMİYETİ

Miraç GÜR

Yüksek Lisans Tezi

Ankara, 2024

KİŞİSEL VERİLERİN KORUNMASI BAĞLAMINDA AKILLI ŞEHİRLER VE VERİ MAHREMİYETİ

Miraç GÜR

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı

Yüksek Lisans Tezi

Ankara, 2024

KABUL VE ONAY

Miraç Gür tarafından hazırlanan "Kişisel Verilerin Korunması Bağlamında Akıllı Şehirler ve Veri Mahremiyeti" başlıklı bu çalışma, 22.11.2023 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Doç. Dr. Oytun Canyaş (Başkan)

Doç. Dr. Duygu Hatipoğlu Aydın (Danışman)

Doç. Dr. Hüseyin Can Aksoy (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof.Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren … ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

19/01/2024

Miraç GÜR

1"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"

*(1) Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

*(2) Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkânı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

*(3) Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

***** Tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu tarafından karar verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Doç. Dr. Duygu Hatipoğlu Aydın** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Miraç GÜR

Sevgili eşim Elif Nur ve biricik kızım Gülce Fatıma'ya..

ÖZET

GÜR, Miraç. ***Kişisel Verilerin Korunması Bağlamında Akıllı Şehirler ve Veri Mahremiyeti,*** **Yüksek Lisans Tezi, Ankara, 2024.**

Teknolojinin gelişmesiyle akıllı cihazların ortaya çıkması akıllı şehirler kavramını ortaya çıkarmıştır. Veriye dayalı bir dünyada şehirlerimizin de bundan mahrum kalacağı düşünülemezdi. Artan nüfusun beslenme ve barınma ihtiyacı ile birlikte sürdürülebilir bir yaşam, şehirleri bazı değişimlere zorlamıştır. Bununla birlikte akıllı şehirlerde yaşayan insanların mahremiyetinin ve kişisel verilerinin korunması önemli bir konu haline gelmiştir. Öyle ki, gözetim teknolojilerinin akıllı şehirlerdeki kameralar, sensörler vb. vasıtalarla kullanılması akıllı şehirlerin sosyal psikoloji alanında nerede durduğunu anlamamız açısından önem arz etmektedir. Bununla birlikte akıllı şehirlerin olası mahremiyet sorunları ve bu sorunlara dair çözüm önerilerinin sunulması gerekmektedir.

Anahtar Kelimeler: Akıllı Şehirler, Kişisel Veriler, Mahremiyet, Veri, Teknoloji

ABSTRACT

GUR, Mirac. *Smart Cities and Data Privacy in the Context of Personal Data Protection,* Master's Thesis, Ankara, 2024.

The emergence of smart devices with the development of technology has revealed the concept of smart cities. In a data-driven world, it was unthinkable that our cities would be deprived of it. Sustainable life, together with the need for nutrition and shelter of the increasing population, has forced cities to some changes. However, protecting the privacy and personal data of people living in smart cities has become an important issue. In fact, the use of surveillance technologies with tools such as cameras and sensors in smart cities is important for us to understand where smart cities stand in the field of social psychology. However, possible privacy problems of smart cities and solutions for these problems should be presented.

Key Words: Smart Cities, Personal Data, Privacy, Data, Technology

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AI : Artificial Intelligence (Yapay Zeka)

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme (Avrupa İnsan Hakları Sözleşmesi)

BİT : Bilgi ve İletişim Teknolojileri

bkz. : Bakınız

BM : Birleşmiş Milletler

CCTV : Closed Circuit Telelevision (Kapalı Devre Televizyon Sistemi)

Çev. : Çeviren

Ed. : Editör

GDPR : 2016/679 sayılı ve 27 Nisan 2016 Tarihli Gerçek Kişilerin Kişisel Verilerin İşlenmesine Karşı Korunmasına ve Bu Verilerin Serbest Dolaşımına İlişkin ve 95/46/EC sayılı AB Yönergesini Yürürlükten Kaldıran Avrupa Parlamentosu ve Avrupa Konseyi Tüzüğü (General Data Protection Regulation-Avrupa Birliği Genel Veri Koruma Tüzüğü-GVKT)

GPS : Global Positioning System (Küresel Konumlama Sistemi)

IoT : Internet of Things (Nesnelerin İnterneti)

KVKK : 6698 Sayılı Kişisel Verilerin Korunması Kanunu

m. : Madde

PbD : Privacy by Design (Tasarım Yoluyla Mahremiyet)

PIA : Privacy Impact Assessment (Mahremiyet Etki Değerlendirmesi)

PPP : Public Private Partnership (Kamu-Özel Ortaklığı)

s. : sayfa

vb. : ve benzeri

vd. : ve devamı

GİRİŞ

İnsanlık, tarih başladığından beri birlikte yaşama içgüdüsüne sahip olmuş ve bu gereksinim ile giderek gelişen şehirlerin/kentlerin ortaya çıkış hikâyeleri başlamıştır. Her yüzyılda başka bir boyuta erişen şehirler, 20. yüzyıla gelindiğinde ise başta köyden kente göçlerin ve diğer birçok faktörün etkisi ile kalabalık nüfusu, farklı kültürleri, iş imkânları, barınma ve gıda ihtiyacı gibi birçok faktörün kontrollü bir şekilde yönetilmesi gereken geniş bir kavram haline gelmiştir. Öyle ki, günümüze doğru gelindiğinde ekonomik açıdan bir yerleşim birimine kent unvanı verilmesinin üzerinde yaşayanların çoğunluğunun tarım dışı sektörlerde faaliyet göstermesine bağlı olacağını savunan düşünceler yaygınlık kazanmıştır.[1] Buna bağlı olarak tarım dışında kalan özellikle sanayi bölgeleri teknolojiye ulaşım bakımından şehir/kent kavramına daha uygun olmaya başlamıştır.

Sanayi sektörünün 19. yüzyıldan itibaren şehirlerde hızlı bir gelişim göstermesi sonucunda dünya genelinde her gün binlerce kişi şehirlere göç etmekte ve buna bağlı olarak göç alan bölgelerde kısıtlı doğal kaynaklarla sürdürülebilirliği sağlamak ve kentleri daha yaşanabilir kılmak, gün geçtikçe zorlaşmakta ve nihayetinde yeni çözümlere ihtiyaç duymaktadır. Bu sorunlara ek olarak, küresel ısınma, küresel salgınlar, dünya genelinde ortaya çıkan çeşitli felaketler ve "*yeni nesillerin değişen beklentileri kentlerin ihtiyaçlarını belirlemekte, kısıtlı kaynaklarla bu ihtiyaçların sürdürülebilir biçimde karşılanması yenilikçi ve akıllı çözümleri zorunlu hale getirmektedir*".[2]

Günümüzdeki şehir/kent kavramı ise bilgi ve iletişim araçlarının hızlı gelişmesi ve teknolojik ilerlemeler sonucunda tarihsel gelişim açısından yepyeni bir algı oluşturmaya başlamıştır. Sanayi Devrimi öncesi ortaya çıkan ve "Şehir 1.0" olarak adlandırılan

---

1 Aldemir, A. (2018) "Geleneksel şehir sistemlerinin akıllı şehir sistemlerine geçiş süreçlerinin yönetilmesi", Yüksek Lisans, İstanbul. s.4

2 Nair, G. (2019) "Kentsel Yaşamın Bilgi ve İletişim Teknolojilerinin Işığında Yeniden İnşası ve Anadolu'dan Bir Örnek: Sivas Belediyesi'nin Akıllı Kent Uygulamaları", Araştırma Makalesi, 8(1): 524

kentlerin ortak özelliği başkent olmaları, dini bir merkez olmaları veya ticari faaliyet olarak bir pazar yerine sahip olmaları iken "Şehir 2.0" olarak adlandırılan kentlerde sanayi süreci başlamış ancak bununla birlikte kültür, din ve üretim alışkanlıklarının geç değişim göstermesi ile sanayi devri öncesiyle de ortak özellikler gösteren bir yapı söz konusu olmuştur.[3] Aynı zamanda ilk şehirlerde genellikle su kenarları, yerleşim yerleri olarak kullanılırken "Şehir 2.0" için bunun yerine endüstri ve ekonomi merkezli yapılar kurulmaya çalışılmıştır. Endüstrinin gelişmesiyle kamu ve özel alan ayrımı giderek belirginleşen "Şehir 2.0" kavramından günümüzde belirgin hatları ile öne çıkan "Şehir 3.0" kavramına geçiş yaşanmaktadır. Söz konusu "Şehir 3.0" kavramının ortak özelliği olarak teknoloji ile birlikte ortaya çıkan, bununla birlikte ulaşım ve iletişim altyapısını tamamlayarak insan öncelikli bakış açısına ve yüksek yaşam kalitesine sahip olduğu iddia edilen "Akıllı Şehirler" olduğu söylenebilir.

Dünyanın dört bir yanındaki pek çok şehir, yönetişim ve hizmet sunumunu iyileştirmek, daha esnek kritik altyapı oluşturmak, yerel ekonomiyi büyütmek, daha güçlü hale gelmek gibi bir dizi sorunu çözmek için ağ bağlantılı, dijital teknolojileri ve kentsel büyük verileri kullanarak akıllı bir şehir olmaya çalışmaktadır.[4] Sürdürülebilir, verimli üretim, şeffaf ve hesap verebilir yönetim ile birlikte yaşam kalitesini, emniyet ve güvenliği artırmayı amaçlayan akıllı şehirler kısacası, vatandaşların yaşamlarını iyileştirmek, şehir yönetimini geliştirmek ve ekonomik kalkınma yaratmak için dijital teknolojiyi kullanma amacını taşımaktadır.

Son yıllarda kendisinden daha fazla bahsettiren bazı teknolojik kavramların (büyük veri, nesnelerin interneti, yapay zekâ, gözetim teknolojileri vb.) ortaya çıkması ve giderek gelişmesi ile akıllı şehirler, hiç bitmeyecek bir inşa sürecine başlamıştır. Söz konusu kavramlar geliştikçe elde edilen verilerin miktarı da büyümekte ve bu sayede akıllı şehirlerin inşasında en gerekli olan malzeme de sağlanmış olmaktadır. Elde edilen veri miktarındaki artış, yukarıda bahsedilen modern şehirlerin karmaşık sorunlarına çözüm aramada en önemli yardımcı halini almaktadır.

---

3 Keleş, R. (1990). Kentleşme politikası, İmge Kitabevi, S. 76

4 Kitchin, R. (2016). "Getting smarter about smart cities: Improving data privacy and data security". Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Bu bağlamda, şehir işletim sistemleri, merkezi kontrol odaları, kentsel gösterge panoları, akıllı ulaşım sistemleri, entegre seyahat biletleri, bisiklet paylaşım şemaları, gerçek zamanlı yolcu bilgi ekranları, lojistik dahil olmak üzere kentsel ortamlarda çok çeşitli akıllı şehir teknolojileri kullanılmaktadır. Yönetim sistemleri, akıllı enerji şebekeleri, kontrol edilebilir aydınlatma, akıllı sayaçlar, sensör ağları, bina yönetim sistemleri ve bir dizi akıllı telefon uygulaması ve paylaşım ekonomisi platformlarının çoğu gerçek zamanlı olarak ve oldukça ayrıntılı bir ölçekte büyük miktarlarda veri üretir. Şehirler ve vatandaşları hakkındaki bu veriler, şayet iyi uygulama alanlarında paylaşılırsa oluşturuldukları sistem ve amaçlara hizmet edeceklerdir. Nihayetinde, bu veriler şehirleri daha verimli, üretken, sürdürülebilir, şeffaf ve adil bir şekilde yönetmek için ortaya konulmuştur.

Bununla birlikte, büyük miktarda eyleme geçirilebilir verinin üretilmesi, işlenmesi, analiz edilmesi, paylaşılması ve saklanması da çeşitli endişeleri ve zorlukları beraberinde getirmektedir. Bunlar arasında önemli olan, akıllı şehirlerin temel girdisinden kaynaklanan veri gizliliği, veri koruma ve veri güvenliği sorunlarıdır. Birçok akıllı şehir teknolojisi, vatandaşlar hakkında kişisel verileri, konum ve hareketleri yakalar ve yeni türetilmiş veriler üretmek için bu verileri birbirine bağlar ve bunun sonucunda bunları insanların profillerini oluşturmak ve onlar hakkında kararlar almak için kullanır.[5] Bu nedenle, akıllı bir şehrin insanların mahremiyeti için ne anlama geldiği ve kentsel büyük verilerin paylaşılması, analizi ve kötüye kullanılmasından ne gibi mahremiyet zararlarının ortaya çıkabileceği konusunda endişeler vardır.

Verinin akıllı şehirlerde başat rol oynaması ile birlikte kişisel verinin gizliliği ile ilgili çeşitli mahremiyet (*Privacy*) ve güvenlik (*Security*) kaygıları ortaya çıkmaktadır.[6] Akıllı şehirlerde kullanılan veriye dayalı teknoloji, dijital ortamda toplanan ve depolanan verinin korunması hususunda önlem almayı gerektirmektedir. Özellikle siber saldırılar, dijital casusluk yöntemleri ve giderek çeşitlenen ihlal yolları sonucunda dijital araçlarla donatılmış olan akıllı şehirleri daha savunmasız hale getirmektedir. Bir veri ihlalinin

---

5 Lei, C., Gang, X., Youyang, L., Gao, Y. (2018). "Security and Privacy in Smart Cities: Challenges and Opportunities" *IEEE Access*, v. 6

6 Memiş, L., Güç, M. (2020). "Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar". *Güvenlik Bilimleri Dergisi*, s.96

vatandaşlar için ne gibi etkiler doğuracağı konusunda açıklanması gereken sorunlar vardır. Alınması gereken siber güvenlik önlemlerinin alınmaması, akıllı şehirlerin karmaşık yapısı, insan hatası veya kasıt gibi unsurlardan dolayı akıllı şehirlerin güvenliğinin sağlanmasında daha fazla tedbirin alınması ihtiyacını gözler önüne sermektedir. Buradaki zorluk, altyapı ve sistem güvenliğini korurken ve herhangi bir zararlı etki ve zararı sistematik olarak en aza indirirken akıllı şehir çözümlerini kullanıma sunmak ve bunların uygulanmasının faydalarını elde etmektir. İlgili birçok paydaş ve kazanılmış menfaatler, farklı amaç ve hırslar, çeşitli teknolojiler ve bunların karmaşık düzenlemeleri göz önüne alındığında akıllı şehirlerde mahremiyeti sağlamanın kolay bir iş olmayacağı açıktır.

Akıllı şehir uygulamaların oluşturulması, akıllı bir sistemin her katmanında yaygın olarak bulunan güvenlik açıkları nedeniyle çok sayıda güvenlik ve mahremiyet sorunu da doğurabilir. Yetkisiz erişim ve siber saldırılar gibi sorunlar akıllı hizmetlerin kalitesini düşürebilir. Bir örnek vermek gerekirse, 2015 yılında Ukrayna'da yaşayan yaklaşık 80 bin vatandaş, elektrik şebekesi sisteminin bilgisayar korsanları tarafından saldırıya uğraması nedeniyle uzun bir süre elektrik kesintisi yaşadı.[7] Benzer saldırılardan korunmak için akıllı şehirlere ilişkin güvenliğin iyi bir şekilde sağlanması gerekmektedir. Söz konusu saldırıların yanı sıra, hizmet sağlayıcılar ve bazı üçüncü şahıslar tarafından aşırı veri toplama konusunda mahremiyet ve güvenlik endişelerinin de ortaya çıktığı düşünülmektedir.

Şifreleme, silme, yok etme ve anonim hale getirme gibi birçok koruma yöntemi, farklı uygulama alanlarında yaygın olarak kullanılmaktadır. Ne yazık ki, bu yöntemler akıllı şehir uygulaması için yeterli değildir. Bunun ana nedeni, çoğu sensör ve gözetim teknolojileri cihazlarının sınırlı hesaplama gücüne sahip olması ve bu nedenle yalnızca basit şifre çözme yöntemlerini kullanılabilmesi ve etkisiz kalan önlemlerin tüm sistem için ciddi tehditler oluşturması problemi ortaya çıkmaktadır. Ayrıca, geleneksel bilgi işlem sistemleriyle karşılaştırıldığında, nesnelerin interneti (Internet of Things, IoT) sistemlerinin dinamik özellikleri, akıllı şehir uygulamalarını yüksek güvenlik ve gizlilik

---

[7] Webrazzi. (2016) "Ukrayna'da elektrik neden kesildi?" https://webrazzi.com/2016/01/16/ukraynada-elektrikler-neden-kesildi/ (Çevrimiçi)

risklerine maruz bırakır. Yapay zekâ, büyük veri ve açık verinin kullanılması ile devasa büyüklükte ve anlamsız veriden, anlamlı ve analitik bilgiyi ortaya çıkaran sistemler gün geçtikçe etkisini artırmaktadır. Ayrıca, makine öğrenimi ve veri madenciliği gibi bilgi teknolojilerinin hızlı gelişimi ile saldırganlar da daha akıllı hale gelerek ve mevcut saldırı tespit mekanizmalarını atlama yeteneğine de erişebildiklerini itiraf etmek zorundayız. Tüm bu zorluklar, bizi akıllı şehirlerin mahremiyetini ve gizliliğini korumak açısından hâlihazırda uygulanmış ve geliştirilmiş teknolojileri gözden geçirmeye ve potansiyel araştırma fırsatları sağlamaya teşvik etmektedir.

Akıllı şehirlerde verinin gizliliği ve güvenliği konusunda dünya çapında ortak bir kanıya varılacak standartların olmadığı ortadadır. Buna rağmen kişisel verilerin korunması ve mahremiyet alanında bazı düzenlemeler göze çarpmaktadır. 2018 yılında tüm Avrupa'yı kapsayan ve başka kıtalardan ülkelere de ilham kaynağı olarak yürürlüğe giren Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (*General Data Protection Regulation- GDPR*), kişisel verilerin korunması ve mahremiyet alanını düzenleyen başat mevzuat olarak sayılmaktadır. Söz konusu düzenleme sayesinde; "*şeffaflık ve hesap verebilirlik prensibi, açık rıza, unutulma hakkı, veri koruma sorumluları, ağırlaştırılmış yaptırım, verilerin yurt dışına aktarımının sıkı kurallara bağlanması*" ile veri sorumlularına ve ilgili kişilere çeşitli yükümlülükler de getirmiştir.[8]

Ülkemizde ise kişisel verilerin korunması hikâyesi uzun yıllar öncesinde başlamış olsa da 2016 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ve onunla birlikte 2017 yılında kurulan Kişisel Verileri Koruma Kurumu, alanını düzenleyen ve denetleyen başat bir yapı halini almıştır.

Bilişim teknolojileri insan hayatını kolaylaştırmasının yanı sıra insanlar, şirketler, şehirler ve ülkeler arasındaki rekabeti de artırmaktadır. Söz konusu rekabet olumlu bir etki oluşturduğu gibi bazen yıkıcı etkilere de sahip olabilmektedir. Ayrıca gelişen teknolojik yeniliklerle birlikte yeni beklentiler içerisine giren şehir sakinleri, küreselleşme ile birlikte sermayenin serbest dolaşımının artmasına benzer bir şekilde

---

[8] Memiş, L., Güç, M. (2020). a.g.e. s.96

akıllı şehirlerde kullanılan teknoloji ile birlikte verinin serbest dolaşımının artması sonucunda birçok olumsuz durumla karşılaşabilmektedir.[9] Bu sebeple akıllı şehirlerde özellikle özel sektör eliyle toplanan ve işlenen kişisel verilerin güvenliği hayati bir konu haline gelmektedir. Benzer şekilde devletler bakımından egemenlik anlayışları geleneksel bakış açısı olan coğrafya egemenliği konusunu aşarak günümüzde ekonomik ve siber güvenlik alanlarını da kapsamaktadır.

Teknolojinin durmaksızın geliştiği bu ortamda devletler, şirketler ve bireyler tarafından verilerinin korunması konusunda birçok yeni sorun ortaya çıktıkça yeni çözümler de geliştirilmesi gerekmektedir. Akıllı şehirlerde veri mahremiyeti ve kişisel verilerin korunması hususunda güncel sorunlar ve bu sorunlara çözüm önerileri bulmak, söz konusu sorunlara hızlı ve etkin çözümler bularak ve en önemlisi de sorunlar daha ortaya çıkmadan çözüm önerileri geliştirmek gerekmektedir.

Tüm bu hususların yanı sıra akıllı şehirlerde gözetimin ve gözetim teknolojilerinin çeşitli sonuçları olacağı şüphesizdir. Nitekim gözetim toplumunda insan davranışları ve toplumsal hareketlerin kontrol altına alınabilmesi ve otokratik yapılara zemin hazırlaması tartışmalarının yanı sıra e-devlet gibi vatandaşın verinin kullanıcısı ve sağlayıcısı olması, akıllı şehirlerin bir demokratik yönetişim toplumu olabileceğini akıllara getirmektedir. Bir diğer taraftan akıllı şehirlerin kurumsallaşmış politika ve planlamayı güçlendirdiğini iddia eden fikirler de mevcuttur.[10]

---

9 Şengün, H., Koçhan, A., Meydan, Y., Seçil, G. (2019). "Akıllı Kentler ve Dijital Siber Güvenlik". *Assam Dergisi,* 13. Uluslararası Kamu Yönetimi Sempozyumu Özel sayısı. s. 2

10 Kaygısız, Ü., Aydın, Z. (2017). "Yönetişimde Yeni Bir Ufuk Olarak Akıllı Kentler". Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi. Cilt 9, Sayı 18. s. 58

1. BÖLÜM: AKILLI ŞEHİRLER

1.1. AKILLI ŞEHİR KAVRAMI

Son yıllarda birçok şehir, akıllı şehir programlarını başlatarak ve akıllı şehir teknolojilerini uygulayarak 'akıllı şehir' olma niyetlerini ilan etmiş ve buna bağlı olarak çok sayıda şirket, akıllı şehir çözümlerini pazarlamaya başlamıştır. Akıllı şehirleri teşvik etmeye ve geliştirmeye odaklanan bir dizi hükümet ve uluslar üstü girişimlere finans, düşünce, sivil toplum kuruluşlarının yanı sıra üniversite araştırma merkezleri de dahil olmuştur. Tüm bu girişimlere rağmen teknolojiyle ilgili pek çok popüler ifadede olduğu gibi, "akıllı şehir" terimi de iyi tanımlanmış ve üzerinde anlaşmaya varılmış ortak bir tanıma sahip değildir.

Bilgi teknolojilerinin hızlı bir gelişme göstermesi sonrasında akıllı şehirlere dair birçok farklı tanım yapılmaya çalışılmıştır. Örnek vermek gerekirse akademik ve paydaşlar tarafından ifade edilen kavramlar (Dayanıklı şehirler, sürdürülebilir şehirler, güvenli şehirler, eko-şehirler)[11], şehirlere dair belirli bir amacı öncelemekten öteye gidememiş ve daha geniş bir ifade olan ve son gelişmelerle daha çok duyduğumuz “akıllı” sözcüğü ile karşılanmaya çalışılmıştır.

Akıllı şehir denildiğinde esas olarak şehirlerin kentsel altyapılarını, şehir yönetimini ve şehir hizmetlerini iyi yönde değiştirmek için dijital enstrümanların kullanılması olduğunu anlayan bir kitle bulunmaktadır. Bu bakış açısında, şehirlerin giderek artan bir şekilde veri akışları üreten, şehirlerin akıllı sayaçlar, otonom cihazlar, sensörler, çeşitli yazılım ekipmanları ve tüm bu kurgunun ağ bağlantılı dijital olarak etkinleştirilmiş cihazlardan oluştuğunu düşünülmesinin yanı sıra başka bir bakış açısına göre ise akıllı şehir; insan sermayesini, yaratıcılığı, yeniliği, eğitimi, katılımı, sürdürülebilirliği ve yönetimi yeniden yapılandırmak için teknolojik gelişmeleri kullanarak esas olarak kentsel politika, kalkınma ve yönetişimin iyileştirilmesiyle ilgilenen bir girişim olarak

---

[11] Kitchin, R. (2014) “The Real-Time City? Big Data and Smart Urbanism”. Geo Journal, 79, 1-14. (https://doi.org/10.1007/s10708-013-9516-8)

ifade edilmektedir[12]. Burada, bahsedilen teknolojik gelişmelerden kasıt, bilgi ve iletişim alanındaki yeniliklerin stratejik kullanımı sonucunda daha katılımcı ve etkin; vatandaşların, işçilerin ve kamu görevlilerinin veri üreteceği ve bunun da daha akıllı politika ve programların uygulamaya konulmasına yardım edeceği; daha iyi ürünler üretebileceği, yerli girişimciliği teşvik edeceği ve içe dönük yatırımları çekeceği bir sistem olduğu öngörülmektedir. Bu sayede akıllı bir şehir, e-devleti etkin kullanan, açık veri yayınlayan ve açık veri ekonomisini destekleyen, şehir performansı hakkında vatandaş merkezli gösterge panoları oluşturan, sorunları raporlamaya ve planlamaya vatandaş katılımını teşvik eden, kentsel test olanakları tanıyan bir şehir olarak tanımlanabilir.

"*Araçlı, birbirine bağlı bir şehir*"[13] sistemlerinin gerçek zamanlı düzenlenmesini sağlayan yönetim ve kontrolü anlık olarak sağlayan ve denetleyen güdümlü ve ağ bağlantılı veriler; etkileşim ve programlanabilir sistemlerin kullanımı yoluyla şehirleri yeni, dinamik, bilinebilir ve kontrol edilebilir hale getirmektedir. Ayrıca, üretilen veriler sonucunda gelecekteki kentsel gelişime rehberlik ederek yeni modelleri ve simülasyonları sürekli geliştirmektedir. Başka bir şekilde ifade edecek olursak, bilim kurgu filmlerindeki akıl sınırlarını zorlayan dijital şehirlere ulaşmak için bugünkü alışkanlıklarımız ve davranışlarımızdan elde edilen verilere ihtiyaç duyulmaktadır. Bu sayede akıllı şehirlerde sivil katılımı geliştiği, hesap verebilir, şeffaf yapılar oluşturmak hedeflenmektedir.[14] Akıllı şehirlerin, böylece eşit fırsatlar sağlayan, vatandaşlarına hizmet eden ve eşitsizlikleri azaltan akıllı bir toplumu teşvik edeceği öngörülmektedir.

Akıllı şehirlerin bir ihtiyaca dayalı olarak ortaya çıktığı düşünüldüğünde, yüksek kentsel yoğunluk, kaçınılmaz olarak trafik sıkışıklığı, enerji arzı ve tüketim sorunları, sera gazı emisyonlarının artması, plansız gelişme, temel hizmetlerin eksikliği, atık yönetimine dair ihtiyaçlarda dramatik artışı ile birlikte suç oranlarında oluşan artış, akıllı şehirlere

---

12 Kitchin, R. (2016) a.g.e, Data Protection Unit, Department of the Taoiseach S.11

13 Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. ve Williams, P. (2010). "Foundations for Smarter Cities". *IBM Journal of Research and Development*, 54(4), s.16.

14 Townsend, A. "Smart Cities: Big data, Civic Hackers, and the Quest for a New Utopia". (2013) New York: W.W. Norton & Co. S.18

olan ihtiyacı ortaya çıkarmaktadır.[15] Bu sorunlarla mücadele etme yönündeki politik ve sosyal ihtiyaç (özellikle iklim değişikliği endişeleri gün geçtikçe artmaktadır), dijital ve ağ bağlantılı çözümler geliştiren teknoloji ve telekomünikasyon şirketleri için kazançlı bir pazarın bariz potansiyeliyle birleşmekte ve bu amaçla ortaya atılan ve süreç içerisinde oldukça moda olan akıllı şehir kavramının ortaya çıkmasına neden olmaktadır. Öyle ki bu fikir, daha sonra ulusal ve yerel siyasi liderler, büyük küresel teknoloji şirketleri ve uluslararası kurum ve kuruluşlar tarafından büyük bir istekle benimsenmiştir. Maliyetleri azaltmak ve ekonomik büyüme yaratmak, aynı zamanda sürdürülebilirlik, katılım, kabul edilebilir bir sivil hizmet standardı ve nihayetinde yaşam kalitesi üretmek için çeşitli çözüm önerileri ortaya atılmaktadır. Buna karşılık akıllı şehir anlayışları için neo-liberal, piyasa odaklı, teknokratik bir bakış açısının hakim olma eğiliminde olduğu; akıllı şehirleri "vatandaş merkezli" olarak gören, sosyal inovasyonu, adaleti ve kendi deyimiyle katılımı teşvik eden alternatif bir paradigmanın aksine “akıllı bir toplum”un saf ekonomik kazanç perspektifinin bu şekilde hakimiyeti, hem sosyal ihtiyaçlar hem de uygun yasal düzenlemelerin dikkate alınması açısından zarar verici olabileceği endişeleri bulunmaktadır.[16]

Akıllı toplumu ekonomik kazanç olarak gören piyasa temelli neoliberal anlayışla beraber, akıllı şehirlerin ihtiyacı olan özelliklerin karşılanamadığı bir hale gelebileceği de unutulmamalıdır. Ekonomik anlamda gücü elinde bulunduran kesim, akıllı şehirleri ekonomik güçlerinin devamlılığına bir araç olarak da kullanabilir. Hatta akıllı şehirlerde oluşturulması gereken yasal düzenlemelerin de hayata geçirilmesi bahse konu güçler tarafından engellenebilir. Nitekim veriyi ve çeşitli imkânları elinde bulunduran yapılar, insanlar üzerindeki gözetim gücünü kullanarak daha zengin ve daha güçlü olmak isteyebilirler.

Yukarıda sayılan sebeplerden dolayı akıllı şehrin kabul edilmiş tek bir tanımı yoktur ve aslında bu özellikleri kimin sağladığı oldukça önemlidir; endüstri, politikacılar, sivil toplum ve vatandaşlar doğrudan ve açıkça akıllı şehirlerin birbirinden farklı paydaş

---

15 Edwards, L. (2016). "*Privacy, security and data protection in smart cities: a critical EU law perspective*". European Data Protection Law Review, Sayı: 2 (1), s.3

16 Edwards, L. (2016) a.g.e. s.4

gruplarıdır. Bu yüzden akıllı şehirleri tanımlamak yerine temel özelliklerini detaylandırmak daha kolaydır. Şehirleri "akıllı" hale getirdiğinden sıklıkla bahsedilen birbirine bağlı temel altyapı;

- Yollar, arabalar, beyaz eşyalar, elektrik sayaçlar, ev aletleri ve bu nesneleri birbirine bağlayan ağlar veya yazılımlar kullanılır,
- IoT ağları, halk dilinde "büyük veri" olarak da bilinen, büyük miktarlarda veriyi üretir,
- Birbirleriyle birleştirilebilen, daha sonra yeniden kullanılabilen gerçek zamanlı veri akışlarına olanak tanıyan dijital iletişim ağları ve sensörler kullanılır,
- Verilerin, uygulamaların, nesnelerin ve insanların bu ara bağlantısını destekleyebilen ve depolama alanı sağlayabilen, genellikle bulut tabanlı, yüksek kapasiteli altyapıya ihtiyaç duyulur.[17]

Avrupa ve Amerika Birleşik Devletleri'nde akıllı şehirlerinden maksat, esas olarak şehir hizmetlerinin verimliliğini artırmak, dayanıklılık ve sürdürülebilirlik yaratmak, güvenlik ve kontrolü güçlendirmek ve ekonomik kalkınmayı teşvik etmekle ilgilidir. Terörizmin daha çok tehdit olarak görüldüğü Birleşik Krallık ve ABD şehirlerinde daha çok öne çıkan güvenlik girişimleri olmasına karşılık; Çin, Hindistan ve Afrika'da akıllı şehir kavramından anlaşılan ise modernleşmeyi ve ulusal kalkınmayı sağlamanın, nüfus artışına ve göçe yanıt vermenin, etkin ekonomi politikaları ve kentsel geçişleri yönetmenin bir yoludur. Bu geniş coğrafi alanlar içinde, şehir yönetimlerinin ve idarelerinin önceliklerine ve yerel kültür, tarih, siyaset ve ekonomilerin etkisine bağlı olarak önemli farklılıklar vardır. Ayrıca, akıllı şehir girişimlerinin çoğu mevcut şehirlerin iyileştirilmesiyle ilgilenirken, bazı şehirler veya yeni şehir bölgeleri akıllı şehirler olarak sıfırdan oluşturulmaktadır (örneğin, Güney Kore'de Songdo, Birleşik Arap Emirlikleri'nde Masdar ve Hindistan'da planlanan 100 akıllı şehir).[18]

---

17 Edwards, L. (2016) a.g.e. s.4

18 Kitchin, R. (2016) a.g.e, Data Protection Unit, Department of the Taoiseach. s.13

1970'lerde Los Angeles gibi büyük şehirleri görmeye başlamamız ile birlikte akıllı şehir oluşum süreci hız kazanmıştır. 20. yüzyılın başından bu yana şehirlerin optimize edilmesi gereken yerlerine dair daha karmaşık analizler yapılması, şehirlerin planlanmasına ve yönetimine ilişkin bir tür veri uygulanmasını gerçekleştirebilecek ortamı hazırlamıştır. Hatta 90'ların ortalarına gelindiğinde Amsterdam gibi şehirler, Dijital Şehir Stratejisi oluşturmaya başlamış ve şehirde internet kullanımını teşvik etmeye odaklanmıştır.

Süreç içerisinde şehirlerin nüfusu artış gösterdikçe bulundukları ülkelerden ziyade metropol niteliğindeki kalabalık şehirlerin ülkelerin önüne geçtiği gözlenmektedir. Söz konusu durum yerel yönetimlerde etkisini göstermiş olup akıllı şehir kavramı ile şehirlerin, bulundukları ülkelerden farklı politika izlemesini gündeme getirmektedir.

Akıllı şehir uygulamalarındaki farklılıklara rağmen, her biri veriye dayalı, ağ bağlantılı teknolojilerin günlük yaşamı nasıl daha iyileştirileceği ve kentsel sorunların üstesinden gelmek için kullanılabileceği beklentisiyle tüm akıllı şehirlerde kullanılan uygulama alanları bulunmaktadır. Buna göre akıllı şehirler; veriye dayalı, ağ bağlantılı altyapı, ekonomik büyümeyi ve girişimciliği teşvik eden, vatandaş merkezli girişimlerin bir karışımı olmakla beraber özellikle daha verimli şehir hizmetleri, gelişmiş ulaşım sistemleri, doğal afetlerle mücadele, ticari olarak doğrudan ve dolaylı yatırımları çeken, yerli girişimleri ve KOBİ'leri teşvik etmek amacıyla açık veri ve sivil katılımlı bir yaşam biçimini olarak ortaya çıkarmaktadır. Bu bakımdan kentteki dijital uygulamaların varlığı, o kentin mutlaka akıllı şehir olacağı anlamına da gelmemektedir.

1.2. AKILLI ŞEHİRLERİN UYGULAMA ALANLARI

Akıllı şehirlerin ortaya çıkış amacı vatandaşların yaşam standartlarını yükselterek güvenli ve müreffeh bir ortam oluşturmak olmalıdır. Aynı zamanda akıllı şehirler, şehir vatandaşlarının yaşam kalitesini iyileştirme amacını taşıyan teknolojilerin ve yoğunlukla verinin kullanımına dayanan, paydaşların şehir yönetimine entegre edildiği

bir uygulamadır.[19] Bu sebeple akıllı şehirlerin enerji, çevre, atık yönetimi, yaşam alanları, hizmetler ve endüstri hizmetleri bakımından ortaya çıkaracağı yenilikler ve kolaylıklar oldukça fazla olacaktır.

Akıllı şehirler; evler, sağlık hizmetleri, ulaşım, şebekeler, araçlar ve atık yönetim sistemlerinin "akıllı" şekilde yürütülmesini içeren bir modeldir. Akıllı ev, evin iç ortamını ve hissini ayarlayabilen bir iletişim cihazları ağıdır. Örneğin, ofis denetleyicinizden bir sinyal aldıktan sonra, ev denetleyicisi musluğu sıcak bir banyo için etkinleştirebilir, daha rahat olmanıza yardımcı olmak için klimayı ayarlayabilir, TV'yi açabilir ve en sevdiğiniz programı oynatmasını sağlayabilir. Benzer şekilde, akıllı sağlık hizmetleri, kritik sağlık parametrelerini kaydeden ve buradaki herhangi bir tutarsızlığı ilgili tıbbi personele bildiren ve ilaç enjektörlerine dahi ne kadar ilaç enjekte etmeleri gerektiğini emredebilen bir ağdan oluşacaktır. Akıllı ulaşım, seyahat süresini ve trafik sıkışıklığını en aza indirgemek için mevcut kaynakları, tıkanıklığa eğilimli önemli rotaları yönlendirerek ve boşaltarak akıllı şehir trafiğini en uygun hale getirebilir. Akıllı şebekeler, Akıllı Şehirlerin çevreye ve zamana dayalı değişen taleplerini karşılamak için çeşitli enerji kaynaklarını dengeleyen, otomatik ayarlanabilir enerji kaynaklarıdır. Akıllı araç, yolculuğu önceden planlayan, karayolu trafiğini öngören ve trafik ve yol hakkında endişelenmeden en sevdiğiniz videonun keyfini çıkarmanıza yardımcı olan sürücüsüz araçtır. Büyük şehirler, doğal kaynakların en büyük tüketicisi olduğundan dolayı büyük miktarda atık üreticisidir ve şehirlerin sürdürülebilirliği açısından önem verilmesi gereken bir husustur.[20] Akıllı atık yönetimi, şehirlerin temiz ve düzenli kalmasına yardımcı olmak için çöp kutuları, çöp toplayıcılar ve atık imha sistemlerinden oluşan ağa bağlı bir sistemdir. Özetlemek gerekirse, Akıllı Şehir, makinelerin/cihazların/nesnelerin, parametrelerini genel olarak toplumun değişen taleplerini ve bireylerin kişisel gereksinimlerini karşılayacak şekilde ayarlayarak, her bir

---

19 Pehlivan, E. (2017). "Katılımcı, Sürdürülebilir Bir Akıllı Şehir Hedefliyoruz". *Fortune Dergisi*. https://www.fortuneturkey.com/yol-acin-akilli-sehirler-geliyor-45878 (Erişim Tarihi: 19.09.2023)

20 Nair, G. a.g.e. s.525

sakinin kişisel ve sosyal yaşamının iyileştirilmesi için birlikte çalıştığı bir şehrin kavramsallaştırılmasıdır.[21]

Akıllı şehirler, yenilik üreten insanlar ve bu konuda işgücünü arz eden çalışanlar için bir birleşim noktası haline gelir ve bu sayede giderek daha akıllı hale gelen bir noktaya ulaştığı gözlenir. Nihayetinde, akıllı bir şehrin en hızlı büyüme oranlarını yakalamış ve nitelikli işgücü payının da yüksek olduğu şehirler olması beklenmektedir.

Akıllı şehir bileşenleri, bir zincirin halkalarının birbirine bağlanmasıyla meydana gelmektedir. Akıllı insan olmadan akıllı çevreden, akıllı bina olmadan akıllı akıllı uygulamalardan ve hizmetlerden bahsetmek imkânsızdır. Özellikle akıllı ulaşım sistemleri, akıllı atık yönetim sistemi, akıllı afet yönetim sistemi ve akıllı ekonomi sistemi olmadan akıllı bir yaşamdan bahsetmenin mümkün olmadığını belirtmek gerekmektedir. Her şeyden önce insanlar ve şehir sakinleri eğitilmeli ve akıllı vatandaşlar haline getirilmelidir. Ancak bu sayede akıllı şehir için sağlam adımlar atılabilir. Nitekim akıllı bir şehir meydana getirebilmek için en önemli faktör olan "*veri ve bilgi iletişim teknolojileri, ancak vatandaşların bilinçlendirilmesinden sonra etkin ve verimli kullanılabilir*".[22]

1.2.1. Akıllı Devlet

Akıllı devlet kavramı akıllı şehirlerin etkinliğini sağlayacak en önemli kavramlardan biridir. Akıllı devletin temel amacı veriye dayalı akışları, beslemeleri, bilgi temelli altyapıları ve kurumları oluşturarak vatandaşlarına daha iyi hizmetler sağlamaktır. Bunlara ek olarak, akıllı yönetişim, vatandaşların kamu kararlarına ve şehir planlamasına dahil olmalarını sağlayarak bilgi şeffaflığını ve dolayısıyla verimliliği de artırmayı hedefler. Örneğin, günümüzde sıkça kullandığımız ve giderek kapsamı daha da genişleyecek olan e-devlet, fatura ödeme ve şikayet bildirme mekanizmalarının hızlı

---

21 Saini, R., Mishra, D. (2019). (Kitap Bölümü: Privacy-Aware Physical Layer Security Techniques For Smart Cities). "Smart Cities Cybersecurity And Privacy". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları. s.39

22 Akkan, M. (2019) "Akıllı Kent Uygulamaları ve Konya Örneği". Necmettin Erbakan Üniversitesi, Sosyal Bilimler Enstitüsü. Konya, Yüksek Lisans Tezi. s.24

ve veriye dayalı çalışması gibi devlet hizmetlerinden çevrimiçi olarak faydalanmasına olanak tanır.[23]

1.2.2. Akıllı Ulaşım

Akıllı ulaşım, ulaşım sistemlerinin daha "akıllı" kullanımını amaçlar. Nüfusa bağlı araç sayısındaki artıştan kaynaklı, özellikle büyük şehirlerdeki trafik sıkışıklığı; zaman, doğal kaynaklar ve maliyet israfı olarak giderek çözülmesi öncelikli bir sorun halini almıştır. Bu sorunu çözebilmek için akıllı ulaşım ağları, güvenliği ve hızı artırarak vatandaşlara daha iyi hizmet sunulabilir. Ayrıca vatandaşlar, ulaşım odaklı mobil uygulamaları kullanarak en ekonomik ve en hızlı rotaları bulurken günlük programlarını kolaylıkla planlayabilirler. Akıllı ulaşım sistemlerinde görülen diğer yaygın uygulamalar; sürücü pasaportları, ehliyet tanıma sistemleri, uygun otoparka yönlendirme vb. tahminlerdir.

Akıllı ulaşım hizmetleri ve sistemleri, verilerin kombinasyon yerlerinden biri olması bakımından önemlidir. Akıllı şehirlerde anlık olarak veri aktarımının belki de en hızlı ve yüksek miktarlarda olduğu konu akıllı ulaşım sistemleridir. Nitekim gelişen teknoloji, artan nüfus, ulaşım araçlarında ve hareketlilikteki artış sonucu vaktin önemini de artırmıştır. Bu sebeple akıllı ulaşım sistemleri akıllı şehirlerdeki en somut sonuç alınması gereken kısım olmaktadır.

Akıllı ulaşım sistemleri, akıllı şehirlerde en hızlı ilerleme kaydeden ve en çok altyapı yatırımı yapılan kısımdır. Şehirler, farklı ulaşım seçenekleri için merkezi odak noktaları oluşturarak hizmet vermekte ve fiziksel anlamda söz konusu noktalar, genellikle toplu taşıma araçlarını yönlendirmektedir. Belki de yakın gelecekte uçan arabalarla tüm ulaşım hizmetleri, verileri kullanarak en üst düzeye çıkacaktır ama aynı zamanda bu veriler, gerek bugün gerekse yakın gelecekte, toplanarak ve analiz edilerek ulaşım altyapısını planlamak ve tüm ulaşım sistemini yönetmek için de gerekli olmaktadır ve

---

[23] Leı, C., Gang, X., Youyang, L., Gao, Y. (2018). a.g.e, s.36

olacaktır. Örnek vermek gerekirse, bisikleti nereye koyacağınıza karar vermek için sizi yönlendiren şeritler ya da Coronavirüs döneminde yaşanan sokağa çıkma yasaklarında gördüğümüz gibi kuryenin nerede olduğunu internetten takip edebilme veri akışı sayesinde mümkün olabilmektedir.

Akıllı ulaşım sistemlerine veri güvenliği boyutuyla bakıldığında hem dijital hem de fiziksel alanları ve ilişkileri yönetmek için dijital hizmetlerin kullanımı gerekmektedir. Bununla birlikte akıllı ulaşım sistemleri için işlenen kişisel verilerin mahremiyeti ve korunması hususu öne çıkmaktadır. Akıllı ulaşım sistemlerinin veriler vasıtasıyla çalışabildiği ve söz konusu verilerin ciddi bir kısmını ise kişisel verilerin oluşturduğu düşünüldüğünde akıllı ulaşım sistemlerinde mahremiyeti sağlamak oldukça zorlaşacaktır.

Bununla birlikte özellikle şehirlerin sağladıkları ulaşım hizmetleri hakkında ayrıntılı bilgilerin uzun süredir muhafaza edilmeye çalışılması dolayısıyla bu şehirler hakkında çok ayrıntılı bilgiler bulunması, mahremiyet açısından çeşitli sakıncaların başlangıcı olabilmektedir. Bir örnekle açıklamak gerekirse, bulunduğumuz şehirlerinden gerçek zamanlı konum izlemeye dair verilerin kaydedilmesi giderek yaygınlaşmaya başlamıştır. Aynı zamanda bu verilerin özel şirketler eliyle yapılması kişisel verilerin korunması ve mahremiyet açısından önem arz edeceği gibi kamu açısından da çeşitli sorunlar ortaya çıkaracaktır.

Örnek vermek gerekirse, Martı gibi elektrikli bisiklet veya elektrikli scooter şirketleri tarafından işlenen ve paylaşılan verilerle sağlanan mobilite hizmetleri, meşru temellerini hizmet verdikleri ülkenin mevzuatından alabilmektedir. Söz konusu hizmetler, kamusal alanlarda yeni mahremiyet ve veri yönetimi sorularını da gündeme getirmektedir. Tüm bunlar araçların şehrin neresinde ve ne zaman hareket ettiğine dair bilgilerin aynı zamanda o aracı kullanan kişinin de ne zaman ve nerede olduğu hakkında da bilgi sağladığı gerçeğidir. Nitekim hizmeti alan gerçek kişilerin konum verilerinin işlenmesi ve hizmetin zorunlu unsuru olarak aktarılması, kişisel verilerin ihlali anlamına

gelebilecektir. 2020 yılında çıkan bir haberde Martı ile ilgili olarak şunlar ifade edilmiştir:[24]

> *"Uygulamada harita üzerinden sizlere en yakın olan Martı'yı kolayca bulabilir ve yepyeni bir scooter sürme macerasına başlayabilirsiniz. Scooter üzerinde yer alan kodu akıllı telefonunuz ile okutarak sistem üzerinden scooterı üzerinize alabilirsiniz. Böylece her geçen dakika üzerinden ücretlendirilmekte ve Martı hesabınıza işlenmektedir*."

Dolayısıyla bu durum, mahremiyeti ve kişisel veriyi korumanın zorluklarını artıran hassas durumlar olarak ortaya çıkmaktadır.

Bu tür sistemler birden fazla kaynaktan veri toplayabilmeli ve bu bilgileri analiz edebilmeli ve gerektiğinde paydaşlara sağlayabilmelidir.[25] Akıllı ulaşım sistemleri trafik sıkışıklığına ve diğer sorunlara yol açan aksilikler hakkında bir fikir vermek için büyük veri analitiğini kullanmaya odaklanır ve yoldaki aksiliklerle ilgili olarak verileri kullanarak bilgi ortaya çıkarmaya yarayan bir model geliştirmeyi amaçlar. Trafik kazaları, doğal afetler, salgın hastalıklar gibi acil durumlar için bir bilgi altyapısı oluşturmak, akıllı şehirlerin amacına uygun olmaktadır. Buna ilişkin önerilen altyapı, acil duruma neden olan sebeplerin tam olarak tespit edilerek çözüm geliştirebilmek amacıyla akıllı mobil cihazlar, sensörler vb. çeşitli kaynaklardan üretilen tüm verileri dikkate alacaktır. Bunun yanı sıra, farkındalık sağlayacak ve olay yerindeki acil durum ekiplerine de yardımcı olacaktır. Bu sayede akıllı şehirler, kaynakları etkin bir şekilde kullanmaya odaklanacak ve aynı zamanda hayat kurtarmaya ve yaralanmaları azaltmaya yardımcı olacak ve yaşam kalitesinde iyileşme sağlayacaktır.[26]

İnsanlardan akıllı telefonlarını kullanarak şehrin veri toplanması için iş birliği yapmaları istenebilir. Önerilen vizyonda, şehirdeki çeşitli veri kaynaklarına ortak bir

---

[24] Gürsoy, A. N. (2016) "Martı Nedir? Nasıl Kullanılır?" https://www.sigortaladim.com/marti-nedir-nasil-kullanilir (Erişim Tarihi: 25.09.2023)

[25] Abberley, L., Gould, N., Crockett, K., Cheng, J. (2017). "Modelling road congestion using ontologies for big data analytics in smart cities". Uluslararası Akıllı Şehirler Konferansı (ISCC). s.2

[26] Abu-Elkheir, M. Hassanein, S. Oteafy, S. (2016) "Enhancing emergency responsesystems through leveraging crowd sensing and heterogeneous data" Uluslararası Kablosuz İletişim ve Mobil Bilgi İşlem Konferansı (IWCMC). s.190

erişim mekanizması sağlayarak elde edilecek ve bu sayede, kentin veri ekosistemindeki karmaşıklığın büyük ölçüde azaltılmasına yardımcı olur.[27] Bunu yapabilmek için büyük miktarda kişisel veri kullanılması gerekmektedir. Unutmamak gerekir ki akıllı şehrin temel amacı, akıllı şehirdeki tüm paydaşların günlük yaşam kalitesini çeşitli teknolojiler ve cihazlar yardımıyla daha iyi hale getirmektir. Toplumun hem sosyal hem de ekonomik refahı, çeşitli politikalar ve iyileştirme eylem planları yoluyla olumlu sonuç elde edilecek seviyelere getirmek önemli bir husustur. Bununla birlikte, vatandaşların ve diğer paydaşların mahremiyetine de odaklanılmalıdır. Bu yüzden akıllı şehirlerde, kişisel verilerin korunması ve mahremiyet anlayışı ile iyileştirilmiş yaşam kalitesinin dengelenmesi çok önemli hale gelmektedir. Bu da mahremiyet odaklı bir kamu politikası sayesinde elde edilebilir.[28]

1.2.3. Akıllı Çevre

Kırsaldan kente göçün artmasıyla birlikte şehirlerdeki bina sayısına bağlı olarak şehirlerin yeşil alanları giderek azalmaktadır. Bunun yanı sıra, çarpık kentleşme, orman yangınları ve endüstriye ve çeşitli atıklara bağlı olarak akarsuların, yer altı sularının ve havanın kirlenmesi sorunlarıyla başa çıkabilmek için akıllı şehirlerle birlikte akıllı bir çevre oluşturulması fikri doğmuştur.

Akıllı çevre, sürdürülebilir bir toplum inşa etme açısından önemli ölçüde katkıda bulunabilir. Özellikle, teknik yönetim araçlarını benimseyen akıllı bir şehir, enerji tüketimini, hava kalitesini, binaların yapısal güvenilirliğini sağlayarak kirlilik ve atıkları verimli bir şekilde yok etme veya geri dönüştürme yeteneğine sahip olmalıdır. Bu durumun söz konusu olabilmesi için ideal olarak, çevresel sensör ağları, gelecekte doğal afetleri tahmin etme, tespit etme ve hatta engelleme yeteneğine sahip olabilirler.

---

27 Aguilera, U., Peña, O., Belmonte, O., López-de Ipiña, D. (2017) "Citizen-centric data services for smarter cities*"*. *Future Computing Systems Dergisi*. Sayı:7, s. 236

28 Kasar, S., Meghana, K. (2021). (Kitap Bölümü: Open Challenges in Smart Cities: Privacy And Security). "Security And Privacy Applications For Smart City Development". (Editörler: Sharvarı, T., Dey, N., Aboul-Ella, H.). Varşova, Polonya: Springer Yayınları s.29

1.2.4. Akıllı Uygulamalar

Enerji maliyetlerinin giderek arttığı dünyamızda enerji tasarrufunu sağlamak devletlerin ve vatandaşların politika geliştirmesi gereken önemli bir konu halini almıştır. Etkin ve verimli bir enerji kullanımı için en sağlıklı yöntem olarak veriye dayalı uygulamaların kullanılması kaçınılmazdır.

Akıllı uygulamalar, akıllı şehirlerin su ve gaz gibi kaynakların aşırı tüketimini azaltmasına ve ekonomik büyümeyi iyileştirmesine ve çevrenin korunmasına katkıda bulunmasına olanak tanır. Pratik bir akıllı kamu hizmeti uygulaması olarak akıllı ölçüm araçları, dağınık enerji kaynaklarını izlemek için akıllı şebekelerde günümüzde yaygın olarak kullanılmaktadır. Ayrıca kaynakları yönetmek ve enerji kaybını azaltmak için akıllı su sayaçları ve akıllı ışık sensörleri de kullanılmaktadır. Yeni teknoloji ile inşa edilen akıllı binalarda açık kalan ışıkların ev sahibine haber veren sistemler gibi geliştirilebilir uygulamalar karşımıza çıkmaktadır.

1.2.5. Akıllı Hizmetler

Akıllı şehirler, vatandaşlarına sağlık, eğlence, güvenlik, ulaşım vb. hizmetleri en iyi şekilde sunmayı amaçlamaktadır. Buna rağmen akıllı şehirlerin vatandaşa yansıyacak en son halkası olan hizmetlerin amacına ulaşması için verinin doğru ve güncel olması gerekmektedir. Akıllı şehirlerde akıllı hizmetlerin sağlanması bu sebeple önem arz etmektedir.

Akıllı hizmetler vatandaşlara birçok yönden fayda sağlar. Örneğin, akıllı sağlık uygulamaları, giyilebilir cihazlar ve tıbbi sensörler aracılığıyla insanların sağlık koşullarını zamanında izleyebilir ve etkin çözümler üretebilir. Ayrıca sosyal ağ, eğlence, akıllı alışveriş ve diğer akıllı hizmetler, insanların günlük yaşamlarının kolaylığını önemli ölçüde iyileştirebilmektedir.

Akıllı şehirlerin temelleri, araştırmaları, ortaya çıkan eğilimleri ve gelecekteki planlamalarındaki uygulamalara geniş kapsamlı bir bakış sunmaktadır. Ayrıca akıllı şehir uygulamaları kullanıldıkça mevcut akıllı hizmetlerin güçlü ve zayıf yönleri gözden geçirilecektir. Zaten akıllı şehirlerde en önemli bakım onarım sistemi olarak kendi kusurlarını ve eksiklerini görerek onu hızlıca kapatmaya odaklanmış bir sistem oluşturması olduğu söylenebilir. Örneğin, kanalizasyon şebekesinin gelecekteki başarılı operasyonel yönetimi için, gerçek zamanlı olarak su baskını tahmini gereklidir. Sisteme devamlı olarak veri girişi sağlanarak akıllı şehir yönetimi için gerçek zamanlı tahminler rapor edilebilir. Bu sayede, mevcut bir kanalizasyon şebekesine ait bir prototipin tasarımı anlık geliştirilme ile bizlere sunabilir.[29]

1.2.6. Akıllı Binalar

Akıllı binalarda, olağandışı aktivite ve hırsızlığı tespit etmek için tüm bina alanları gözetim altına alınır ve bina ile ilgili tüm görsel veriler oluşturulur. Bu tür bilgilerin bilgisayar korsanlarına karşı korunması gerekir, çünkü bu bilgileri kullanıcıların binalarından ayrılma ve binaya giriş zamanlarını izlemek için kullanabilirler. Algılama sırasında kişisel verilerin korunması için veri güvenliği sağlanmalıdır.

Akıllı şehir uygulamalarında kullanılan veriler bulutta depolanır. Bu veriler bulut sunucularına açık olduğu için güvenilmeyen bulut sunucularından bu verilere erişme tehdidi olabilir. Veriler düz metin olarak bulut üzerinden gönderilirse, verilerin saldırıya uğrama veya etik olmayan amaçlar için kullanılma olasılığı olabilir. Bu durumdan kaçınmanın bir yolu, Akıllı şehirlerde kişisel verilerin şifrelenmesi, depolama ve işleme amacıyla uyumlu bir şekilde bir bulut sunucusunda şifreli metin biçiminde gönderilmesidir. Kamu ve altyapı alanına ait geri bildirim ve kontrol sistemleri saldırganlar ve bilgisayar korsanları tarafından hedeflenmektedir. Söz konusu sistemlerde, bu tür verileri işlemek için yetkili erişime sahip olmak oldukça önemlidir.[30]

---

[29] Kasar, S., Meghana, K. (2021). a.g.e. s.30
[30] Kasar, S., Meghana, K. (2021). a.g.e. s 43

1.3. AKILLI ŞEHİRLERDE TEKNOLOJİK GELİŞMELER

Akıllı şehirler, vatandaşların yaşam kalitesini artırmayı hedefleyen, vatandaş ile birlikte bir uyum içerisinde şehrin farklı fonksiyonlarını entegre eden yapılar olması için yeni teknolojilerden faydalanmaktadır. Söz konusu teknolojik yenilikler, şehir hizmetlerine operasyonel düzeyde hizmet ettiği gibi gerçekleşen faaliyetlerden çeşitli verilerin alınmasına ve saklanmasına da hizmet etmektedir.[31]

Tüm bu gelişmelerin temelinde veri olduğunu, akıllı şehirlerin öncelikli girdisinin ve çıktısının veri olduğunu bizlere göstermektedir. Günümüzde özellikle yönetim sahasında temel istatistiki verilerin ve bu verilerden ortaya çıkan bilginin yetersiz kalması, daha büyük miktarda verinin elde edilerek analiz edilmesi ihtiyacını ortaya çıkarmıştır. Buna bağlı olarak 2016 yılında Rob Kitchin tarafından ortaya atılan veri odaklı kentleşme (Data Driven Urbanism), gün geçtikçe haklılığı anlaşılan bir kavram haline gelmiştir.[32]

Akıllı şehir ile birlikte sağlanan hizmet, kaynaklar ve verimlilik oranları değerlendirildiğinde, Los Angeles ve Oslo için şunlar belirtilmiştir:[33]

> *"Los Angeles'ta akıllı ulaşım sistemleri sayesinde duraklamalarda %35, kavşaklardaki beklemelerde %20, seyahat süresinde %13 azalma ve bunlara bağlı olarak yakıt tüketiminde %12,5 oranında düşüş sağlandığı görülmektedir. Akıllı sokak aydınlatması sistemiyle Oslo'da ki elektrik tüketimi tasarruf oranı %70 olarak hesaplanmıştır."*

Benzer şekilde ihaleler, sözleşmeler ve satın alma vb. hizmetleri "dijital ortama taşıyan Güney Kore'de 2010 yılında 40 milyar dolar civarında bir tasarruf gerçekleştirilmiştir".[34]

---

31 Memiş, L. Güç, M., a.g.e. s.96

32 Kitchin, R. (2016) "The ethics of smartcities and Urbanscience" Philosopical Transactions Society A 374: 20160115, S.1, http://dx.doi.org/10.1098/rsta.2016.0115.

33 Deloitte. (2016). "Akıllı Şehir Yol Haritası" https://www2.deloitte.com/tr/tr/pages/public-sector/articles/smart-cities.html (19.09.2023)

Akıllı şehirlerde özellikle nesnelerin interneti'ni (IoT) kullanarak nesnelerin kendi arasındaki ilişkiyi; nesnelerin interneti ile elde edilen veriler, büyük veriyi (Big Data) ve bununla bağlantılı olarak açık veriyi (Open Data); büyük miktarda verinin analiz edilerek mantıklı bir sonuç ortaya çıkarması ve bu sonuçlar arasında en olması gereken seçeneğin tercih edilmesi yapay zekâyı (Artifical Intelligence); ayrıca elde edilen büyük miktarda verinin depolanması amacıyla ortaya çıkan bulut bilişimi (Cloud Computing) açıklamak faydalı olacaktır.

1.3.1. Büyük Veri ve Açık Veri

Kamu kurumları açısından açık verinin toplanması ve paylaşılması da söz konusudur. Açık veri, "kullanılabilirlik ve erişim", "yeniden kullanım ve yeniden dağıtım" ile "evrensel katılım" olmak üzere üç temel özelliği ile tanımlanabilir.[35] Dolayısıyla her türlü alanda açık veri üretilebilmekte olup bu haliyle "akıllı şehirler açısından düşünüldüğünde su, enerji tüketimi, doğal afetler, hava ve iklim, emlak, ulaşım ve toplu taşıma gibi birçok veri, akıllı şehir uygulamalarına temel oluşturmaktadır".[36] Açık verinin özelliklerinden bahsedecek olursak "*kanunların kendisine vermiş olduğu yetkiler çerçevesinde vatandaşa hizmet sunan ve bunun neticesinde oluşan coğrafi veri, ulaşım ve trafik verisi, mali veri, adalet sistemi verisi ve akademik veri gibi veriyi depolayan, işleyen ve kullanan kamu kurumları ihtiyaç halinde sahip olduğu veriyi başta vatandaş olmak üzere, diğer kamu kurumları, özel sektör ve sivil toplum örgütleri ile paylaşmaktadır*" ifadesini zikretmek doğru olacaktır.[37]

Açık veri telif hakkından bağımsız olarak kamuya verilerin açıkça sunulması ve bu verilerin kullanılması ve işlenmesi suretiyle istifade edilmesi anlamını taşımaktadır. Bu sebeple açık veride üçüncü kişilerin sürece dahil olması oldukça kolay olmaktadır.

---

34 Köseoğlu, Ö., Demirci, Y. (2018). "Akıllı Şehirler ve Yerel Sorunların Çözümünde Yenilikçi Teknolojilerin Kullanımı". *Uluslararası Politik Araştırmalar Dergisi*, Cilt 4, s.2

35 Köseoğlu, Ö., Demirci, Y. (2018). a.g.e. s.2

36 Open Knowledge International. (2018). "Open Data Handbook" https://opendatahandbook.org/guide/en/ (Erişim Tarihi: 19.09.2023)

37 Türkiye Bilişim Derneği (TBD). (2016). "Büyük Veri Uygulamaları Çalışma Grubu Raporu" https://docplayer.biz.tr/35808546-Turkiye-bilisim-dernegi-kamu-bilisim-merkezleri-yoneticileri-birligi-kamu-bilisim-platformu-buyuk-veri-uygulamalari-calisma-grubu-raporu.html

Toplumun genelinde kullanılabilen açık verilerin şeffaflık ve hesap verebilirlik açısından da büyük avantajları bulunmaktadır. Nitekim söz konusu verilerin safahatına ulaşılabilme imkânı bulunmakla birlikte toplumsal katılımı teşvik etmesi bakımından da bir avantaj olarak görülebilmektedir. Açık veride işlenen ve paylaşılan veriler, genellikle anonimleştirilmiş veya kişisel veri kategorisinde olmayan veriler olmakla birlikte uygulamalarda kişisel veri işlenmesine dair örneklere rastlanmaktadır.

Açık veriler, daha önce kurumlar içinde kilitli olan veya sadece belirli kişilerle paylaşılan verilerin kamuya açık hale getirilmesidir. Açık verinin etkinliğinin sağlanabilmesi için kullanımı ücretsiz hale getirilen, bununla birlikte makine öğrenimi tekniklerine dayanan yeni veri analitiği geliştirilmeli ve veriyi tam anlamıyla yeni veri üreten, bu veriden değer elde eden ve elde ettiği değere göre hareket eden yapılar haline getirilmelidir. Açık verinin akıllı şehirlerde kullanımı amacıyla şehrin tüm fonksiyonlarının şeffaf olarak vatandaşa sunulduğu ve vatandaş tarafından beslenebildiği yapılar olması gerekmektedir. Özellikle kamu hizmeti şirketleri, ulaşım sağlayıcıları, cep telefonu operatörleri, seyahat ve konaklama siteleri, sosyal medya siteleri, yerel bilgi siteleri, hava durumu, devlet organları ve kamu idaresi, kütüphaneler, müzeler, yayıncılar, arşivler, finans kurumları ve perakende zincirleri, özel gözetim ve güvenlik firmaları, acil servisler, ve ev aletleri ve eğlence sistemleri; açık verinin oluşmasında en önemli rolü üstlenmektedir.[38] Söz konusu verilerin çoğu günümüzde kapalı ve özel varlık olarak kabul edilirken, bazıları ise üçüncü taraf satıcılarla paylaşılmaktadır.

Akıllı şehirlerde büyük veri ise şehre özgü uygulamalar, e-belediye hizmetleri gibi akıllı şehir girişimlerinin, şehir sistemlerinin daha fazla koordinasyonunu sağlamak için birden fazla akıllı şehir teknolojisini birbirine bağlamaya çalışması ile belirgin bir şekilde ortaya çıkarmaktadır. Benzer şekilde, kentsel operasyon merkezleri ve kentsel gösterge panoları, bir "şehir arayüzü" sağlamak için verilerinin çoğunu bir araya getirmeye ve birbirine bağlamaya çalışması gerekmektedir. Veriler sayesinde aynı

---

[38] Kitchin, Rob. (2016) a.g.e, Data Protection Unit, Department of the Taoiseach, s.20

zamanda kentsel süreçleri incelemek amacıyla simülasyon oluşturarak yeni iş alanların oluşturulmasına da yardımcı olmaktadır.

Günümüzde sensör ağlarının yaygınlaşması, verinin yaygın olarak karar alma mekanizmasına dahil edilmesi ve toplumun neredeyse her kesiminden veri akışının olması dolayısıyla büyük miktarda akıllı şehir verisi üretilmektedir. Bu yüzden çeşitli algoritmalar sayesinde büyük veri; şehir nüfusunun daha önce ölçülmemiş kısımları hakkında çeşitli tahminler yapma imkânı sağlayacaktır. Şehrin yapısını anlamak ve şehrin olanaklarını ölçümlemek bakımından "*büyük veri dışsal varyasyon kaynakları ile birleştirildiğinde güçlü hale gelecektir*".[39] Aynı zamanda büyük veri ile birlikte şehrin kıt kaynaklarının tahsisi iyileştirilerek gelecekteki ihtiyaçları tahmin edilebilecektir. Akıllı şehir uygulamalarına ilişkin fonksiyonlar incelendiğinde 5C kodu ile formüle edilen; bağlantılı (connection), biriktirme (collection), hesaplama (computation), iletişim (communications) ve birlikte üretim (co-creation) kavramları öne çıkmaktadır.[40]

Akıllı şehirlerin oluşturulmasının merkezinde, şehir altyapısı, hizmetleri ve vatandaşlar hakkında çok miktarda verinin üretilmesi, işlenmesi, analiz edilmesi ve paylaşılması yer alır. Aslında, akıllı şehir teknolojileri yukarıda bahsedildiği gibi şehirleri veri odaklı hale getirmekle, özellikle şehir sistemlerinin ve hizmetlerinin verilere göre hareket etmesini sağlamak ilgilidir. Bu nedenle, akıllı şehirler oluşturma dürtüsü, gelişen veri devrimi ile örtüşmektedir. Büyük verinin geniş ölçekli üretimi; geleneksel küçük verilerin veri altyapılarını oluşturması, veri kümelerinin paylaşılmasına, birleştirilmesine ve yeni yollarla analiz edilmesine olanak sağlanması; interneti bir "veri ağı"na dönüştürmeyi amaçlayan bağlantılı verilerin oluşturulması; tüm belgelerin veri olarak işlenmesi ve toplanması ve birbirine bağlanması ile ilişkilidir. Esasen "*büyük veri bir veri yığını, karmaşa ve kaostur*".[41] Bununla beraber unutulmaması gereken ise bu kaos içerisinde büyük veriyi kullanılabilir kılan unsurun işe yarar bir bilgi ortaya çıkarabilmesidir.

---

39 Hayta, Y. (2021). "Akıllı Kent Uygulamalarında Kişisel Verilerin Gizliliği ve Güvenliği". *Fırat Üniversitesi Sosyal Bilimler Dergisi*, Sayı: 31, s. 932

40 Hayta, Y. (2021). a.g.e. s.932.

41 Hayta, Y. (2021). a.g.e. s.932

"Sosyal medya, açık veri kaynakları, web siteleri, bloglar, sensörler ve çeşitli veri toplayan pek çok bilgi ve iletişim teknolojileri sayesinde sürekli olarak" devlet kurumları ya da özel sektör marifetiyle veri elde edilmekte ve işlenmektedir. İşlenen veriler kurumların faaliyet alanına yönelik olarak "*pazarlama, halkla ilişkiler, bankacılık ve güvenlik gibi pek çok alanın yanında bilimsel araştırmalara da konu edilmektedir*".[42] Bu sebeple, farklı alanlarda faaliyet gösteren kurumlar veya vatandaşlar eliyle yürütülen işlemler sonucunda sağlık, finans, ulaşım, eğitim gibi farklı sektörlere ait veriler büyük veriyi oluşturmaktadır. Kullanıcılara ait kişisel veriler barındıran mobil cihazlar, konum bilgisine dayalı hizmetler ve çeşitli içerik servisleri ile büyük veri akıllı şehir çözümlerinde etkin bir rol üstlenmekte olup özellikle belediye hizmetlerine ilişkin büyük veri kullanılarak geleceğe dönük tahminler yapılabilmektedir.[43]

Büyük veri ve açık veri sayesinde, bir kaza mahallindeki polis, şehre özel platformu kullanarak kaç ambulansın ne zaman sevk edildiğini görmek ve ek bilgi yüklemek için kullanabilir. Merkezde ise çeşitli veri analitiği yazılımları tarafından desteklenen bir analist ekibi, zaman içinde toplanan verileri ve periyodik olarak yayınlanan büyük hacimli verilerin yanı sıra canlı veri akışını işler, görselleştirir, analiz eder. Veriler gerçek zamanlı karar verme ve problem çözme için kullanılır. Ayrıca, şehir yaşamının belirli yönlerini ve zaman içinde değişimini araştırarak sel gibi afet durumları ile ilgili tahmine dayalı modeller oluşturmak için veriler bir araya getirilebilir. Bu durumda veriler acil durumlarda bir kriz yönetim merkezi haline gelebilir. Nihayetinde asıl hizmet amacı olarak kullanıcıların, günlük karar vermeye yardımcı olan ve şehir hakkında ayrıntılı, güncel bilgiler edinmelerini sağlayan platformlar oluşturmayı hedeflemektedir.

1.3.2. Nesnelerin İnterneti

Günümüzde kendisinden oldukça söz ettiren ve gelecekte etkisini daha fazla hissedeceğimiz nesnelerin interneti kavramı, evimizde, çevremizde ve hayatımızın

---

42 Doğan, K., Arslantekin, S. (2016). "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum". *DTCF Dergisi*, Cilt:56, Sayı:1.

43 Köseoğlu, Ö., Demirci, Y. (2018). a.g.e. s.6

neredeyse her alanında kullandığımız elektronik cihazlarımızın bizim kontrolümüz dışında birbirine veri akışı sağlayabilmesi olarak tanımlanabilir. Söz konusu durum ilk anda kulağa hoş gelse de bulaşık veya çamaşır makinasının aynı ağa bağlı başka cihazlara şahsımıza ait verileri paylaşması, mahremiyetimiz açısından çok ciddi sorunlar ortaya çıkarabilecektir.

İnternet ağı, akıllı telefon ağları, sosyal ağlar ve endüstriyel ağlar gibi heterojen ağların birbirine bağlı ve entegre olması oldukça karmaşık olmaktadır. İnsan faktörünün ortadan kalkarak nesnelerin kendi aralarında entegre olarak iletişim kurabilmesi hayatı kolaylaştırdığı kadar çeşitli önlemleri de alma gereğini ortaya çıkarmaktadır. Bu karmaşa ile başa çıkmak için yeni etkili teknolojilere ihtiyaç duyulmaktadır. Örneğin, IoT tabanlı altyapılarda kötü amaçlı yazılımların yayılma özellikleri, kablosuz sensör ağlarında verinin yayılma modellerine yönelik etkili önleme stratejilerinin geliştirilmesi büyük önem taşımaktadır.

1.3.3. Bulut Bilişim

Verilerin elde edilmesi, işlenmesi ve aktarılması konularının yanı sıra depolanması da önem arz etmektedir. Bulut hizmetleri, daha iyi teknoloji yönetimi, ölçeklenebilirlik, birlikte çalışabilirlik gibi etkili özellikleri nedeniyle günümüzde veri depolama amacıyla kullanılmaktadır. Veri taşınabilirliği, uzaktan kontrol ve etkin maliyet gibi avantajları nedeniyle kullanımı her geçen gün artsa da, bulut hizmetleri üzerinde artan veri tehditlerine yönelik bir endişe bulunmaktadır. Bulut hizmetlerinin operasyonel yapısının, verilere kimlerin erişebileceği ve veri erişiminin ne kadar gizlilik derecesine kadar verilebileceği gibi özellikler üzerindeki erişim kontrolleri açısından daha güçlü olması gerekmektedir. Bulut sağlayıcı, zayıf güvenlik uygulamaları, uygulama güvenlik açıkları ve diğer nedenlerle verileri koruyamazsa, vatandaşların verilerinin güvenliği tehlikeye girebilir ve dolayısıyla içeriden saldırılar, veri hırsızlığı vb. gibi veri ihlallerine yol açabilir.

Hizmet sağlayıcısı tarafında ortaya çıkan güvenlik ihlalleri/saldırıları, veri tehdidi güvenlik açıkları için en önemli endişe kaynağı olarak bilinmektedir. Bir veri gizliliği

politikasının veya gizlilik hizmeti düzeyi sözleşmesinin olmaması, genel bulutun verilerini bile tehlikeye atan veri saldırılarının kapsamlı nedenidir. Hizmetin sonunda güvenlik uygulamalarının görünür olmaması, saldırganlar için cazip bir giriş oluşturmaktadır.

1.3.4. Blok Zincir

Blockchain; işlemleri, anlaşmaları ve sözleşmeleri kaydeden, paylaşan bir defterdir. Verileri depolamak ve yönetmek için şeffaf ve güvenli bir platform sağlar. Akıllı bir şehir çerçevesinde, blockchain platformunu ağ ve veri tabanı seviyelerinde entegre edebiliriz, çünkü blockchain'in kendisi dağıtılmış bir veri tabanıdır. Zincire eklenen her blok için benzersiz bir mesajı veya veri setini temsil eden sayı atanır, bu da zinciri hacklemeyi ve izinsiz girmeyi zorlaştırır. Blockchain böylece herhangi bir güvenlik saldırısını önlemek için güvenilir, verimli ve ölçeklenebilir bir ortam sağlar. Blok zincirleri, her bir kullanıcının kendi benzersiz dijital imzasına sahip olduğu için blok içindeki gizliliği koruyabilir. Ayrıca, bilgiler yalnızca sahibi tarafından izin verildiğinde değiş tokuş edilebilir, böylece kişisel veriler yüksek düzeyde korunur.

Teknolojiyi kullanarak çeşitli tehditleri ve kimlik hırsızlığını önleyebiliriz. Özellikle akıllı bir şehirde sağlanan çeşitli tesislerle ilgili olarak, blok zinciri her bir birimde uygulanabilir. Örneğin, sağlık sektöründe, kayıtları depolamak, veri yetkilendirmesi ve veri kimliğini yönetmek için birleşik bir platform sağlamak için blockchain uygulanabilir. Akıllı yönetişimde[44] ise blockchain; verimlilik, hesap verebilirlik, güven ve şeffaflık sağlar.

1.4. AKILLI ŞEHİRLERDE GÖZETİM VE GÖZETİM FELSEFESİ

Akıllı şehirler, barındırdıkları teknik sistemler sayesinde küresel ölçekte başarı elde etmektedir. Aynı zamanda akıllı şehir, büyük ölçüde bilgi, teknoloji ve iletişim

---

[44] Hatipoğlu Aydın, D. (2023). "Kişisel Verilerin Korunmasında Hukukun Sınırları" *İzmir Barosu Dergisi* s.162

kullanımına dayanmakta olup elektronik içeriğin geliştirilmesine de bağlıdır. Şehir yaşamını sürdürülebilir kılabilmek amacıyla dijital teknolojinin şehre mümkün olduğunca maruziyetine dayanmaktadır. Dijital teknolojinin kullanımına odaklanan akıllı şehir tanımı, çoğunlukla gizli bir teknolojik determinizmdir.[45]

Akıllı şehirlerle ilgili belirsizliğin veya anlaşmazlığın ana kaynağı, bir şehir merkezinin ideali olarak giderek daha fazla görülen bir dinamiği beslemekten sorumlu paydaş türüdür. Bu yüzden "gözetim" terimi akıllı şehirlerde anlaşıldığından çok daha geniş bir anlama oturtulmalıdır. Mevcut birçok proje ve deneyin temel amacı, mevcut şehirleri daha akıllı, hatta bir anlamda bilinçli hale getirmektir. Akıllı şehir ideal olarak, dijital araçların optimizasyonunu, işleyişini ve sürdürülebilirliğini, ayrıca şehir sakinlerinin yaşam kalitesini ve birbirleriyle sürdürebilecekleri ilişkileri sağlayan bir şehirden oluşur. Akıllı şehirde öğrenme, anlama ve muhakeme için bazı mekanizmalar tanımlanmıştır.

Gözetim teknolojilerinin, modern demokratik toplulukları yönetmesi ve denetlemesi dolayısıyla devlet erkinin yükselişini tetiklediğini söylemek yanlış olmayacaktır. Nitekim, büyük miktarda veri birikimi sunan teknolojiler, gerek devlet gücü gerekse de ticari amaçla olsun taraflara sosyal, politik ve ekonomik üstünlükler sağlamaktadır. Bunun sonucu olarak akıllı şehir uygulamalarında kurumsal politika, planlama ve denetimi güçlendirme eğilimi mevcuttur.[46]

Akıllı şehirlerin günümüzdeki en belirgin ögelerinden biri olarak E-devlet hizmeti bulunmaktadır. Söz konusu olgu, merkezi ve yerel yönetimlere ait hizmetlerin dijital ortamda yapılabilmesidir. Gün geçtikçe gelişen bu sistemlerin akıllı şehirler için iyi bir başlangıç noktası olacağını kabul etmemiz gerekmektedir. Akıllı şehirlerde e-devlet, kamusal hizmetlerinin vatandaşlara daha iyi sunulması, iş dünyası ve endüstri ile geliştirilmiş etkileşimler, vatandaşların bilgiye erişiminin güçlendirilmesi dolayısıyla daha etkili devlet yönetimi gibi çeşitli amaçlara hizmet edebilmektedir. Yararları; daha

---

45 Kaygısız, Ü., Aydın, Z. a.g.e. s. 60
46 Kaygısız, Ü., Aydın, Z. a.g.e. s. 58

az yolsuzluk, daha fazla şeffaflık, daha fazla kolaylık, gelirlerin artırılması ve maliyetlerin düşürülmesi olarak ifade edilebilir. E-devlet uygulamalarının yaygınlaştırılması amacıyla yeni sunulan hizmetlerin iyileştirilmesi, çalışanların yetkinliklerinin geliştirilmesi, demokratik sürecin ve refahın artması için kamu idarelerinde BİT kullanımını desteklemek gerekmektedir.

Benzer şekilde belediyelerin de bazı hizmetlerini dijital ortamda sağlayabilmesinin yolu açılmıştır. Bu amaçla oluşturulan e-belediye platformları sayesinde şehir sakinlerinin belediye işlemlerinde dijital hizmet, denetim ve katılım durumlarını artıracak adımlar atılmıştır.[47]

Akıllı şehirleri akıllı yapma amacının altında yatan meşru sebeplerin dışında, her sistemde olabileceği gibi bazı sömürgeci faaliyetler de bulunabilmektedir. Sömürgecilik sonrası veri ve teknoloji, sömürgeciliğin boyut değiştirerek uygulanabildiği bir araç olabilmektedir. Küresel manada kişilerin verilerine egemen olmak isteyen ülkelerin ve şirketlerin gözetim teknolojilerini de kullanarak şehirlerin ve ülkelerin her çeşit kaynaklarına hakim olabileceği gerçeği günümüz dünyasında mümkündür.

Sömürgecilik hareketleri başladığında batılı ülkeler bakir kalmış ancak kaynakları zengin olan coğrafyaları silah zoruyla ele geçirerek sömürmüşlerdir. Bunu yaparken geri kalmış coğrafyaların insan, çevre, yeraltı ve yerüstü kaynaklarına ait verileri toplayarak sömürgecilik faaliyetlerini en karlı bölgelere yoğunlaştırmışlardır. Sömürgecilik akımının bitmesi sonrasında ‘demokratik’ rejimler yaygınlık kazanmış ve ülkelerin kendi kaderlerini tayin hakkı çeşitli mücadeleler ile kazanılmıştır. Günümüze gelindiğinde veri teknolojisindeki büyük ilerleme sonucunda medya iletişim araçlarının da katkısıyla ortaklıklara dayalı “çok aktörlü yönetim” anlayışını ifade etmek için veri temelli bir yönetişim sistemi ortaya çıkmaktadır.

---

[47] Nair, G. (2019) a.g.e. s.535

Akıllı şehirlerde yönetişim[48] kavramı ileri düzeyde teknolojinin kullanılmasıyla birlikte e-yönetişim kavramı etrafında şekillenmektedir. E-yönetişim kavramı vatandaş, sivil toplum, kamu ve öze sektör aktörlerinin karar alma süreçlerine dijital ortamda katılabilmesi imkânını sunmaktadır. Özetle anlatmak gerekirse, yönetişim devleti yuvarlak bir masaya oturtmaktır. Nitekim akıllı şehirlerde şehir yöneticilerinin kavramları, hedefleri ve denetimleri şehir sakinleriyle paylaşarak stratejik hareketlere tüm sakinlerin paydaş olması amaçlanmaktadır. Öyle ki bu süreç yerel yönetimlerde uygulaması daha kolay olduğu için yerelde yönetişim sonucu uygulanan politikaların temsil noktasında daha doğru çıktılar vereceği değerlendirilmektedir. Bununla birlikte yönetişimin yerelden genele, genelden küresele gidebilecek bir süreç halini de alabileceği düşünülmelidir. Bu süreç ile birlikte vatandaşlık kavramının boyut değiştireceği, bununla beraber yönetişimde veriyi kontrol eden gücün ise vatandaşları veri sayesinde 'yeni medya aracı' olarak daha kolay manipüle edebileceği de göz ardı edilmemelidir.

İnsanların karar alma süreçlerinin yukarıda zikredilen araçlar vasıtasıyla yönlendirilebildiği bir akıllı şehirde gücü elinde tutan erklerin, marjinalleştirilmiş topluluklar üzerinde tahakküm kurma olasılığını arttırmaktadır. Toplumsal meselelerle ilgili bir politika sorunu oluşturan ise kamu gücünün akıllı sözleşmelerin tarafı olmamasından kaynaklı olarak çok güçlü bir asimetrik güce sahip olmasıdır. Bu asimetrik gücü bertaraf edebilmek için ABD'de şehirlerin mahremiyet değerlerini ifade etme ve resmi mahremiyet ilkeleri oluşturmak amacıyla hizmet satın alınmaktadır. Bunun sonucunda şehirlerin bütüncül bir yaklaşım benimseyen daha resmi veri yönetişim politikaları geliştirmesine yardımcı olmuşlardır.

Şehir yönetimleri, herhangi bir gözetim teknolojisini edinmeden önce, bu belirli teknolojiler üzerinde mahremiyet denetimi yetkisi olan veri koruma otorite ve müfettişlerinin bakış açılarını ve mevzuatlarını dikkate almaları gerekmektedir. Şehirlerin bu mevzuatlar kapsamındaki yükümlülüklerinden kaçınmaması ve kamu hesap verebilirliğini atlamaması açısından şehirlerde de bir mahremiyet ve kişisel

---

[48] Hatipoğlu Aydın, D. (2023). a.g.e. *İzmir Barosu Dergisi* s.162

verileri koruma kurumunun veya daha küçük bir denetim mekanizmasının olması, değerli bir sistemi ortaya çıkaracaktır.

Günümüzde mobese kameraları şehrin işlek yerlerinde bulunan meydan, kavşak, cadde ve sokaklarında trafiği kontrol etmek ve kamusal alanların izlenmesi için kullanılmaktadır. Mobese kameraları hepimizin bildiği gibi görüntü alarak ve bu görüntüleri kaydederek çalışmaktadır. Kamusal alanda gerçekleşen ciddi bir trafik kazasında ve trafiğin olmadığı bir şehir meydanında gerçekleşen bir yaralama olayında mobese kayıtlarına başvurulmaktadır. Buradaki temel nokta ise mobese izlemelerinin kamusal alanda gerçekleşecek olmasıdır. Nitekim kamusal alanın izlenmesi, ölçüsüz işleme olmadığı sürece Kanuna aykırı bir işleme faaliyeti olmayacaktır.

Kamusal alanın izlenmesine ilişkin doktrinde farklı görüşler de bulunmaktadır. Bunlardan ilki kamusal alanlarda yapılan gözetleme faaliyetinin kişilerin kamusal eylemlerini oluşturacağı bu sebeple hukuka uygunluk şartını taşıdığı değerlendirilmektedir. Bir diğer görüşe göre ise kamusal alanda gerçekleştirilen gözetleme faaliyetinin kamu açısından bir keyfiyet oluşturacağı ve bu konuda yasal sınırlamalar getirilmesi gerektiği görüşüdür.[49] Burada aklımıza gelmesi gereken ise kaydedilen mobese kayıtlarının nerede saklandığı, nereye ve kimlere aktarıldığı ve bu faaliyetlere ilişkin yetkilendirilmiş kişi ve kurumların kimler olduğu sorularıdır.

---

[49] Hayta, Y. (2021). a.g.e. s.938

2. BÖLÜM: AKILLI ŞEHİRLERDE VERİ MAHREMİYETİNİN SAĞLANMASI

Birleşmiş Milletler'in raporlarına göre, kentsel alanlarda yaşayan insanların yüzdesi dünya nüfusunun %55'ini oluşturmakla beraber 2050 yılına kadar kentlerde yaşayanların bu oranının %68'e çıkacağı tahmin edilmektedir.[50] Son raporlardan, Çin'de kentsel yerleşimci sayısının 255 milyon, Nijerya'da ise 189 milyon olacağı ve Hindistan'daki şehirli insan sayısındaki artışın yaklaşık 416 milyon olacağı tahmin edilmektedir.[51] Bu devasa rakamlarla, sürdürülebilir kentleşme planlaması için çok çaba gerekmektedir. Bu yüzden teknoloji, hayatımızın ayrılmaz bir parçası haline gelmesinin yanı sıra bilmeden, teknolojinin kişisel yaşamlarımıza fazlasıyla dahil olmasına da izin verdiğimiz gerçeği göz ardı edilmemelidir.

Otonom bir aracın birçok veri teknolojisi vasıtasıyla bir araya gelip devreye girmesi için tek bir veri ortamının aksine birçok aktörün gerçekten karmaşık bir karışımı ile mümkün olabilmektedir. Akıllı şehirlere baktığımızda hassas bir şekilde toplanması gereken verilerin son derece hassas merkezlerden yönetilmesi gerektiği ortaya çıkmaktadır. Aynı zamanda şehirlerimizin içinde kasabalar ve köyler gibi farklı yerleşim bölgelerini de düşündüğümüzde karmaşık bir sistem karşımıza çıkmaktadır. Söz konusu sistem, sadece bir teknoloji ile açıklamaktan ziyade, verinin pek çok teknoloji ile kullanımı olarak tabir edilmesi, daha isabetli olacaktır. Öyle ki, akıllı şehirlerde teknolojinin veriyi kullanmasından daha çok verinin teknolojiyi kullanmasından bahsedebilmelidir. Ayrıca, verinin bu teknolojileri kullanmasında hem kamu hem de özel sektörden aktörler ile birlikte şehirde yaşayan her türden vatandaşın bu karmaşık sisteme bir şekilde dahil olduğunu söylemek yanlış olmayacaktır.

Modern şehirlerde artan karmaşık problemler ve bu problemleri çözmek için gerekli olan karmaşık çözümler için akıllı şehre başvurmak iyi bir yoldur. Zira ihtiyaç duyulan

---

50 Heilig, G. (2012). "World Urbanization Prospects: The 2011 Revision". United Nations, Department of Economic and Social Affairs (DESA), Population Division, Population Estimates and Projections Section. New York, s.14.

51 Heilig, G. (2012). a.g.e. s.14.

hizmetler için verimliliği artırarak daha fazla etkileşim sağlayan ve nihayetinde asıl amaç olan vatandaşlara ve diğer paydaşlara daha fazla hizmet sunumunu sağlayacak çözümler aranmaktadır. Bu sebepten dolayı akıllı şehirlerde verinin iyi kullanımı ve mahremiyetin sağlanması konusunda gerçekten caydırıcı ve iyi düşünülmüş kuralların gerekli olacağı şüphesiz önemli bir husus haline gelmektedir.

Algılayıcı sensörler ve diğer mekanizmalar, insan hakları perspektifinden veri toplamak için bazı sorunları da beraberinde getirmektedir. Vatandaşların gözetlenmesi, haklı olarak sorgulanmakta ve toplumlarda mahremiyet duyarlılığı geliştikçe çok dikkatli bir şekilde incelenmektedir. Buna karşılık tüm bu izleme ve mahremiyet arasındaki hassas dengenin korunması için çeşitli operasyonel zorluklar da karşımıza çıkmaktadır. Özellikle devletler ve yerel yönetimler, akıllı şehir uygulamalarına uyum sağlayabilecek yönetişim ve kontrollere yönelik büyük yatırımlar yapacak bir konuma henüz ulaşmış değildir. Bu sebeple, hepsi kendi akıllı şehir uygulamalarını yönetmek için kendi politika standartlarını belirleyen yerel yönetimlerden ziyade akıllı şehirlerde veri korumayı tek ve genel bir politika haline getirilmesinin çözüm yolları üzerinde çalışılması gerekmektedir. Zira akıllı bir şehir hayal ettiğimizde, dünyanın farklı noktalarında olan şehirlerden bahsediyor olsak bile birbiriyle etkileşimi olan ve dış dünyaya entegre bir şehir olacağını inkar edilemez bir gerçektir. Bu sayede Akıllı şehirlere özgü uluslararası politikaların ve standartların belirlenmesi ve bu ölçütlere uyumu kolaylaştırmak amacıyla uluslararası bir organizasyonun da kurulması önemli olacaktır.

Veri ve teknolojinin kullanımını geliştiren sektörler arasında bir iş birliğinin kurulması gerekmektedir. Toplulukların, vatandaşların ve sektörlerin iş birliği içerisinde olması ciddi bir kamu yararı açığa çıkaracaktır. Bunu sağlayabilmek amacıyla devletlerin kentsel tasarım planlama politikası üretmesi ve buna bağlı olarak yönetim süreçlerinde veri toplaması için gelişmiş veri analizini kullanmasını gerekli kılmaktadır. Bu durumda, doğal olarak daha akıllı, optimal, etkili ve verimli bir şehir sistemi ortaya çıkacağı iddia edilecektir.

Akıllı şehirlerde, sensörler içermeleri ve nesnelerden veri almalarından dolayı büyük miktarda veri; çöp tenekeleri, kaldırımlar ve sokak lambaları gibi araçlardan toplanabilmekte ve toplanan bu veriler veri merkezlerine aktarılabilmektedir. Bu sayede şehir ve çevresine dair istatistikleri ve ölçümleri sürekli olarak izleyebilmektedir. Aynı zamanda akıllı şehirler kameralar, sensörler içermesi ve şehrin içinde hareket eden insanların görüntülerini işlemesi, kaydetmesi, bu kayıtların aktarılabilmesi ve imha edilmesi dolayısıyla akıllı şehirler somut olaylara dayanan verileri içerir.

Mahremiyete yönelik tehdit, kişisel olabilecek büyük hacimli verilerin toplanması, bu toplanan verilerin iletilmesi, saklanma süresi ve elde edilebilecek verilerin çeşitli türleri üzerindeki teknolojik etkiden kaynaklanmaktadır. Teknoloji tabanlı ürünler, coğrafi mesafelerden bağımsız olarak dünya çapında kullanılmaktadır. Buna en iyi örnek akıllı telefondur. Çünkü akıllı telefon, çamaşır makinesi, kahve makinası, mikrodalga fırın gibi ürünlerin kullanımı şehirleşmeye bağlı olmasının aksine teknoloji tabanlı servislerin çoğu ücretli olduğu için daha çok kentsel alanlarda kullanılmaktadır. Kentli insanlar da zaman darlığıyla karşı karşıya kalmakta ve bu nedenle dış kaynak kullanımını ve teknoloji tabanlı hizmetleri kullanmayı daha yaygın bir şekilde tercih etmektedir.

Kentleşme, ekonomik büyümeye, gelişmeye ve sonucunda dönüşüme eşlik eder. Teknoloji tabanlı servislerin ve birbirine bağlı sistemlerin maksimum düzeyde kullanılması akıllı şehirlerin oluşmasına ve gelişmesine yol açmaktadır. Bu hizmetlerin çoğu başlangıçta günlük hayatı kolaylaştırmak için başlamış olsa da artık günlük yaşamın ayrılmaz bir parçası haline gelmiştir.

Bu konuda en çok bilinen teknolojik uygulama olarak Nesnelerin İnterneti (IoT), büyük ölçüde ağ üzerinden bağlanan fiziksel nesnelerin birbiriyle etkileşime girmesi olarak tanımlanabilir.[52] IoT tabanlı ürünler, akıllı şehirlerin ayrılmaz bir parçası olarak kabul edilmektedir.[53] IoT kullanılarak oluşturulan sistemlerden akıllı ev otomasyonu, akıllı

---

52 Gershenfeld, N., Krikorian, R., Cohen, D. (2004) "The internet of things". 291(4), s.22

53 Gershenfeld, N., Krikorian, R., Cohen, D. (2004) a.g.e. 291(4), s.78

sağlık gibi sistemler, yaşlılar ve fiziksel engelli hastalar için gerekli ve destekleyicidir. Bu sistemler, onlara günlük faaliyetlerinde yardımcı olmakta ve güvenliklerini sağlamaktadır. Bununla beraber teknoloji tabanlı ürün ve hizmetlerin kullanımından elde edilen veriler çok büyüktür ve kullanıcılar, kişisel verilerini de içeren söz konusu veri ihlallerinden ve güvenlik açıklarından genellikle habersizdir. Dolayısıyla nesnelerin interneti (IoT), akıllı şehirlerde mahremiyet düzenlemelerinin değişimindeki ihtiyacı hissettiren önemli bir kavram haline gelmiştir.[54]

Teknoloji katılımı hayatımıza memnuniyet katarken, çevrimiçi olarak mevcut verilerin güvenlik yönlerini de düşünmek bir zorunluluk haline gelmiştir. Çevrimiçi olarak mevcut olan kişisel veriler herhangi biri tarafından değiştirilebileceği veya kötüye kullanılabileceği için güvenlik endişeleri ortaya çıkmaktadır. Akıllı şehirde sağlanan verimlilik ve kolaylık, verilerin iletilmesine, geri alınmasına ve madenciliğine bağlı olduğundan, kişisel verilerin yönetilmesi akıllı şehir tasarımında önemli ve anlamlıdır.[55] Akıllı şehirde gizlilik, bütünlük ve erişilebilirlik üçlüsünün yerine getirilmesi zorunludur. Çünkü dijital olarak bağlanan altyapı ve kritik hizmetler, tüm ağı kasıtlı olarak bozma riski yüksek olan siber saldırılara karşı cezbedici olabilmektedir. Bu durum akıllı şehirlerde ve özellikle kritik hizmetlerde toplanan kişisel verilerin ve özel nitelikteki kişisel verilerin ele geçirilme riskini ortaya çıkarmaktadır.

Özellikle CCTV (Kapalı Devre Televizyon, Close Circuit TeleVision) kameraları, ulaşım sistemleri vb. gibi akıllı teknolojilerin kullanırken büyük miktarda veri üretilir. Araç miktarındaki önemli artış, şehrin ve kentsel nüfusun artan büyüklüğü ile artmaktadır. Bu, trafik akışını yönetmek için birçok zorluğa ve nihayetinde trafik sıkışıklığı, kazalar ve hava kirliliği gibi ciddi artışlara yol açmaktadır. Birçok araştırmacı, yaklaşmakta olan akıllı şehirlerdeki mevcut sorunları azaltmak için sensörler gibi farklı teknolojilerdeki gelişmeleri kullanmaya çalışmaktadır.[56] Dolayısıyla devletler, şirketler ve benzeri kuruluşlar, akıllı şehirlerde olası sorunlara çözümler üretmek için çalışmaktadır.

---

54 Hatipoğlu Aydın, D. (2023). a.g.e. *İzmir Barosu Dergisi* s.151

55 Braun, T., Fung, B., Iqbal, F., Shah, B. (2018) "Security and privacy challenges in smart cities". Sustainable Cities and Society. s.501

56 Kasar, S., Meghana, K. (2021). a.g.e. s.27-28

Bugün, teknoloji konusundaki dinamiklerde bir değişime ve daha geniş bir ağa bağlanabilecek uygulamalar ve cihazlar geliştiren şirketlerin ve kuruluşların giderek artmasına tanık olunmaktadır. Örneğin, yeni nesil otomotiv şirketleri, bir mobil uygulama aracılığıyla aracın kontrolünü sağlayacak uygulamaları geliştirmek için bütçelerinin büyük bir bölümünü ayırmaktadır. Benzer şekilde, birçok bilimsel araştırma ile gerçek zamanlı trafik kontrolü ve akıllı park etme yoluyla trafik sıkışıklığını ortadan kaldırmayı amaçlayan algoritmalar önermektedir.

Kişisel verilerin akıllı şehirlerde yüksek güvenlik düzeyinde korunması gerektiği düşünülürse, akıllı şehrin esas olarak elektrik şebekeleri, enerji ve ulaşım tesisleri gibi altyapı sistemlerinde işlenen kişisel verilerin korunması ile ilgilenilmesi gerekmektedir. Bu gelişmeler verinin güvenliği, hızı ve analizi açısından yeni gereksinimler meydana getirmektedir. Örneğin yakın zamana kadar, bir çamaşır makinesi sadece bazı temel güvenlik standartlarına uyması gereken bağımsız ve kapalı bir sistem olarak algılanırken akıllı şehir uygulamalarında bu cihaz, gerekli güvenlik tasarımı olmadan daha geniş bir ağın en zayıf halkası olabilecektir. Çamaşır makineleri, gözetim kameraları ve güvenlik açıklarına sahip navigasyon cihazları gibi elektrikli cihazları bu duruma örnek oluşturulabilmektedir. Diğerlerinin yanı sıra, IoT cihazlarının ise çoğunluğunu başıboş cihazların oluşturduğu güvenlik ve mahremiyet konusunda açıkları olan cihazlar olduğu da unutulmamalıdır.[57]

Bu konuda, kişisel verilerin depolanması ve taşınması ile ilgili olarak ortaya çıkan birçok farklı soru ortaya çıkmaktadır. Mevcut çözümler üzerinden düşünüldüğünde, akıllı şehirlerdeki birbirine bağlı düğümlerle ortaya çıkan ve çıkacak olan yeni zorluklarla yüzleşmeye hazır olup olmadığı tartışmalıdır. Bunun için blockchain teknolojisi ihtiyaç duyulan cevapları sağlayabileceği değerlendirilmektedir. Öyle ki, merkezi olmayan ve dağınık bir veri depolama modeline dayanan blockchain ve kısmen nesnelerin interneti teknolojisi, akıllı şehirler çağına geçişte güvenlik boşluklarını kapatmak için alternatif bir çözüm olarak tanıtılmıştır. Özellikle blok zinciri teknolojisi,

---

[57] Theodorou, S., Sklavos, N. (2019). (Kitap Bölümü: Blockchain-Based Security and Privacy in Smart Cities). "Smart Cities Cybersecurity And Privacy". (Editörler: RAWAT, Danda. GHAFOOR, Kayhan). Hindistan, Eysevier Yayınları. s.22

bizlere üçüncü taraflara bilgi depolamak için kullanılan mevcut teknolojileri terk etme fırsatı sunmaktadır. Öyle ki, Bilgiler çeşitli yerlerde blok şeklinde saklanabilmekte, her konum depolanan bilgilerin gerçek bir kopyasını tutmakta, üçüncü bir tarafın yokluğu gerekli kaynakları önemli ölçüde azaltmakta ve işlem hızını artırmaktadır.[58]

Akıllı sözleşmeler de blockchain teknolojisinin getireceği çığır açan değişiklikler arasında yer almaktadır. Akıllı sözleşmeler, büyük verinin kaotik ortamında hızlı ve özerk işlemler gerçekleştirmeyi amaçlamaktadır. Dahası, milyonlarca bağlı düğümün bir sonucu olarak, günlük işlemler için gereken işlem gücünü azaltacaktır. Kodları aracılığıyla, ağ aktif olur olmaz karar alma, etkileşim kurma ve bilgi depolama kapasitesine sahiptir. Çeşitli işlemler yalnızca her sözleşmenin koşulları yerine getirildiğinde gerçekleştirilir. Burada akıllı şehirler için ayrıca, akıllı sözleşmelerle birlikte e-yönetişim alanlarına yoğunlaşmak gerekmektedir.

Akıllı sözleşmeler, son kullanıcıya ilgili taraflarla karşılıklı anlaşmalar yapma fırsatı sundukları için e-yönetişim kavramını bir adım daha ileri götürmeyi amaçlamaktadır. Üzerinde anlaşmaya varılan sözleşmeler halka açık bir deftere kaydedilecektir. Bu amaçla, akıllı sözleşmeye ilgili tüm taraflarca doğrudan erişilebildiği için kullanıcılar üçüncü taraflardan kaçınmayı başarabileceklerdir. Sonuç olarak, sadece ihtiyaç duyulan kaynakların israfı önemli ölçüde azalmakla kalmayıp aynı zamanda işlem hızı da artacaktır.

Blockchain teknolojisinin ve özellikle e-yönetişimde akıllı sözleşmelerin uygulanmasının, mevcut güvenlik sorunlarına tek çözüm olamayacağının da vurgulanması gerekmektedir. Özellikle, şu anda işleyen akıllı sözleşmelerde ortaya çıkan bazı güvenlik açıkları da mevcuttur.[59] Akıllı yönetişim, akıllı şehir yönetiminde şeffaflığa ve katılıma katkı sunarak daha iyi planlama, karar verme ve denetlemeyi artırsa da geleneksel olarak hükümetlerin masa başında birkaç görevlisi tarafından erişilebilmesi ve vatandaşlara ait kişisel verilerin artık daha ulaşılabilir olması

---

58 Theodorou, S., Sklavos, N. (2019) a.g.e. s.22
59 Theodorou, S., Sklavos, N. (2019). a.g.e. s.23

dolayısıyla korunması ve ihlal edilmesi bakımından birçok zorluğu da beraberinde getirecektir.[60]

Akıllı şehirlerde uygulanan bir başka husus olarak açık veri politikaları, büyük miktarda verinin toplanmasını işlenmesini ve aktarılmasını mümkün kılmaktadır. Buna rağmen işlenen bu verilerden bazılarının kişisel veri olacağını düşündüğümüzde veri paylaşımının sınırları, paylaşılabilecek verilerin niteliği gibi meselelerin akıllı şehir teknolojilerindeki ilerlemeyi engellemeden çözülerek kişisel veri mahremiyetini sağlaması gerekmektedir. Bu bağlamda, çevre kirliliğini azaltmak, trafik ve ulaşım problemlerini çözmek, kaynak kullanımını düzenlemek, yenilenebilir enerjiye yönelmek ve enerji verimliliğinin temini gibi birçok alanda yenilikçi teknolojiler kullanılmakla beraber kişisel verilerin mahremiyetinin korunması gerektiği gözden kaçmamalıdır.

Nihayetinde, akıllı şehirler oluşturulurken kişisel veri güvenliği ile bağlantılı birtakım olumsuz yönleri genel olarak şu şekilde sınıflandırabiliriz;

- Tipik olarak şehre, kötü sorunlarla ve çatışan çıkarlarla dolu karmaşık bir sistem yerine, daha rasyonel ve yönlendirilebilir bir makine gibi davranır,
- Siyasi/sosyal çözümler ve vatandaş merkezli müzakereci demokrasi yerine, teknik çözümler yaratmaya güçlü bir vurgu yapar ve yukarıdan aşağıya teknokratik yönetişim biçimlerini teşvik eder,
- Sunulan teknolojik çözümler sıklıkla şehirleri tarih dışı ve jenerik pazarlar olarak ele alır; şehrin özelliklerine ve ihtiyaçlarına göre uyarlanmış özel çözümler ihtiyacını kabul etmek yerine, tüm teknik çözümlerin tek boyutlu olmasını teşvik eder,
- Kullanılan teknolojiler tamamen politik olmaktan ziyade nesnel, sağduyulu, pragmatik ve politik açıdan iyi huylu olarak tasvir edilir ve paydaşlarının görüş ve değerlerini yansıtır,
- Akıllı şehir teknolojileri geliştiricilerinin, şehir işlevlerini kamu yararı yerine kâr amacıyla yürütülen şirketlerin pazar fırsatları olarak ele almasıyla şehir hizmetlerinin şirketleştirilmesini ve özelleştirilmesini teşvik eder,

---

[60] Akkan, M. (2019) a.g.e. s.20

- Sosyal açıdan daha adil ve eşit bir toplum yaratmak yerine, kazanılmış çıkarların değerlerine ve yatırımlarına öncelik verir, eşitsizlikleri güçlendirir ve toplum üzerindeki gözetim ve kontrolü olumsuz yönde artırır,
- Kullanılan teknolojilerin sosyal, politik ve etik etkileri göz ardı edebilir ve mahremiyetin aşındırılarak tahmine dayalı profil oluşturma, sosyal sınıflandırmayı mümkün kılar,
- Uygulanan teknolojiler, istikrarlı, esnek ve güvenli sistemler üretmek yerine, potansiyel olarak kritik altyapılarda güvenlik açıkları oluşturan ve veri güvenliğini tehlikeye atan arızalı, kırılgan ve siber saldırılara açık kentsel sistemler üretir.[61]

Günümüzde dünya çapında birçok hükümet stratejiler geliştirir, çeşitli zorluklarla mücadele etmek amacıyla akıllı şehirleri teşvik etmeye odaklanır ve bunun için çeşitli ödüller verir. Merkezi hükümetler ve yerel yönetimler, akıllı şehir çerçevelerine dair taahhütlerini ortaya koyarak akıllı şehirlerin daha demokratik katılımı sağladığı iddiasıyla akıllı şehirleri bir tür politika haline getirmektedir. Bunu, büyük teknoloji firmaları ve profesyonel hizmet veren diğer büyük şirketler marifetiyle gerçekleştirmektedir. Hem devletlerin ve şehir yönetimlerinin hem de şirketlerin topladıkları verilerin, daha verimli ve optimize edilmiş şehirlere sahip olabilmek ve kamu hizmetlerini iyileştirebilmek için bir imkân olduğu iddia edilmektedir. Buna karşılık akıllı şehirlerin yerel ekonomilerde insanların işlerini kaybedebileceği ve bu yüzden ekonomik büyümenin önüne geçebileceğini söylenen kentsel zorluklardan bahsedilmektedir. Tüm bu iddiaların yanı sıra, akıllı şehirlerin trafik problemleri, suç ve israfı önleme gibi konularında büyük faydaları olacağı tartışma götürmez bir gerçektir.

2.1. AKILLI ŞEHİRLERDE KİŞİSEL VERİLERİN KORUNMASI HAKKI

Akıllı şehirlerde veriler, nitelikleri bakımından çeşitlilik gösterebilmektedir. Kişisel veri kategorisinde olmayan verileri kullanan akıllı şehir uygulamaları veya anonim hale getirilmiş kişisel veri kullanan akıllı şehir uygulamaları bakımından herhangi bir sorun teşkil etmemektedir. Bununla beraber akıllı şehirlerde kişisel verilere duyulan ihtiyaç da

---

[61] Kitchin, Rob. (2016). a.g.e. s.23

yadsınamayan bir gerçektir. Bu yüzden akıllı şehir uygulamalarının sağlıklı bir şekilde sürdürülebilmesi için kişisel veriler en önemli girdiyi oluşturmaktadır. Bu sebeple kişisel verilerin akıllı şehir uygulamalarında hukuka uygun bir şekilde işlenmesi, saklanması, aktarılması ve imha edilmesi konuları önem arz etmektedir.

Kişisel verilerin korunması hakkı birçok temel hak ve özgürlükle ilişkili olup bazı durumlarda birbirini destekleme, bazı durumlarda ise rekabet etme şeklinde kendini göstermektedir.[62] Özel hayatın gizliliği hakkı ise kişisel verilerin korunması hakkı bakımından söz konusu haklar arasında ilk sırada yer almaktadır. Öyle ki, bilgisayarların ve veri işleme faaliyetlerinin yoğunlaşmasıyla ortaya çıkan endişeler, devletlerin kişisel verileri kötüye kullanma olasılığı üzerinde yoğunlaşmış olup bahse konu teknolojilerin ilk kez yaygın kullanıldığı İkinci Dünya Savaşı'nda insanlar, sınırsız devlet gözetim ve kontrolünün ne gibi sonuçlar doğurabileceğini acı bir şekilde yaşamışlardır.[63] Söz konusu tecrübeler sonucu ilk ortaya çıkan veri koruma mevzuatlarında, bilgiye dayalı gücün birey aleyhine devlette yoğunlaşması hususu üzerinde durulmuş ve teknolojinin kullanımına ilişkin denetlenebilir ve şeffaf bir yapı oluşturulmaya çalışılmıştır.[64]

Bu amaçla kişisel verilerin korunmasına ilişkin 4 Kasım 1950 yılında imzalanan Avrupa İnsan Hakları Sözleşmesi'nin 8'inci maddesinde "*Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.*"[65] ifadesine yer verilmiştir. Benzer şekilde İnsan Hakları Evrensel Beyannamesi'nin 12'nci maddesinde "*Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve şöhretine karşı tecavüzlere maruz*

---

62 Küzeci, E. (2023). (Kitap Bölümü: Kişisel Verilerin Korunması Hakkı). "Kişisel Verilerin Korunmasına Akademik Bakış". (Editörler: Aksoy, H., Aksoy, P.). KVKK Yayınları. s.26

63 Küzeci, E. (2023) a.g.e. KVKK Yayınları. s.28

64 Küzeci, E. (2023) a.g.e. KVKK Yayınları. s.29

65 AİHS https://www.echr.coe.int/documents/d/echr/Convention_TUR

bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." ifadesi ile kişisel verilerin korunması hakkını ayrı bir hak olarak düzenlememesine kişisel verilerin korunması hakkı bakımından önemli bir ifade olarak karşımıza çıkmaktadır.[66]

Kişisel verilerin korunması hakkının diğer hak ve özgürlüklerle karşılaştırıldığı veya çatıştığı durumlar da mevcuttur. Örnek vermek gerekirse, kişisel veriyi bir ekonomik değer olarak gören Ekonomik Hak Yaklaşımında, kişisel veriye mülkiyet hakkı veya bir fikri mülkiyet hakkı olarak gören görüşler mevcuttur.[67] Bunun yanı sıra temel hak ve özgürlükler yönüyle; kişilik hakkı, insan onuru, ifade özgürlüğü, din-inanç özgürlüğü, haberleşme özgürlüğü ve bilgi edinme gibi haklar kapsamında değerlendiren görüşler de bulunmaktadır.[68] Ayrıca, kişisel verilerin korunması hakkı; devletlerin kabul ettiği, uzlaştığı metinler, mahkeme kararları, idari yaptırımlar gibi uygulamalara odaklanılmasına rağmen, kişisel verilerin korunması hakkında ulusal ve uluslararası çeşitli kısıtlamaları ve istisnaları içerdiği de görülecektir.[69]

Kişisel verilerin korunması hakkı ülkemizde ilk defa 2010 Anayasa değişikliği ile anayasal bir hak olarak karşımıza çıkmıştır. Anayasa'nın 20. maddesine 7/5/2010 tarihli ve 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun ile eklenen üçüncü fıkrada "*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir.*"[70] denilerek kişisel verilerin korunmasını isteme hakkı anayasal bir güvence halini almıştır.

Bunun yanı sıra kişisel verilerin korunması, sınırsız bir hak olmayıp bireyin hakları ile veri işleme faaliyetleri arasında denge kurmayı amaçlamakta ve bu bakımdan kişisel verilerin korunması hakkı, kişinin kendisine ait verileri üzerinde sınırsız bir tasarruf yetkisine sahip olduğuna değil; kişi ile verileri arasındaki bağın korunması ve veri

---

66 Dülger, M. (2019). "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması". *Yaşar Hukuk Dergisi*, 1(2) s. 75

67 Kocabıyık, O. (2023). "Kamu Hizmeti Yönüyle Akıllı Şehirlerde Kişisel Verilerin Korunması". Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi. s.64-65

68 Kocabıyık, O. (2023). a.g.e. s.109-116

69 Hatipoğlu Aydın, D. (2023). a.g.e. *İzmir Barosu Dergisi* s.145

70 Türkiye Cumhuriyeti Anayasası, T.C. Resmi Gazete, 2709, 9 Kasım 1982

işleme faaliyetini her aşamada meşru temellere dayanması anlamına gelmektedir.[71] Bu amaçlarla ülkemizde yürürlüğe konulan 6698 sayılı Kişisel Verilerin Korunması Kanunu'na göre kişisel veri "*Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanır.[72] Bu tanıma göre, gizlilik yalnızca bir bireyin ad, doğum tarihi, adres ve benzeri kişisel bilgileriyle ilgili değil, aynı zamanda o kişiyi belirlenebilir kılan herhangi bir anlatım veya görüşü de kapsamaktadır. Dolayısıyla günümüz veri çağında bir kişi ile alakalı kişisel veri sayılmayacak anlamsız verilerin bir araya getirilmesi sonucu kişisel veri ortaya çıkabilecektir. Özellikle modern teknolojiler ile verilerin toplanması ve depolanması, bilginin çıkarılması ve bilginin keşfedilmesi hızlanmıştır. Bu durumda, bir yandan akıllı şehirler gibi yeni uygulamalar uygulanabilir hale getirilirken öte yandan, bireyler için mahremiyetin aşınmasına yol açabilmektedir.

Söz konusu maddede veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi; ilgili kişi, Kişisel verisi işlenen gerçek kişi; kişisel verilerin işlenmesi ise kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem olarak tanımlanmıştır.[73]

6698 sayılı kanunda kişisel verilere ilişkin işleme şartları sayılmış ve mezkur Kanunun 4. maddesinde Türk hukuk sistemine girmiştir. Kişisel Verilerin Korunması Kanununun 4. maddesi şu şekildedir:[74]

---

[71] Küzeci, E. (2023) a.g.e. KVKK Yayınları. s.34

[72] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

[73] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

[74] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

> "*Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur: a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.*"

Bununla beraber 6698 sayılı Kanuna göre kişisel verinin işlenmesinin hukuka uygun olabilmesi için "açık rıza" şartını aramaktadır. "olumlu irade beyanından" ibaret olan ve ispat yükü veri sorumlusunda bulunan açık rızanın yazılı, sözlü ve hatta elektronik yol ile alınabileceği öngörülmüştür. Kanunun 3.maddesine göre açık rızanın unsurları, *"belirli bir konuya ilişkin olması, rızanın bilgilendirmeye dayanması ve özgür irade ile açıklanması*"[75]dır. Söz konusu unsurlar neticesinde kişisel verilerin işlenmesine ilişkin herhangi bir sakınca oluşturmayacaktır.

6698 sayılı Kanunun 5. Maddesi, kişisel verilerin yalnızca açık rıza ile işlenebileceği ve buna karşılık açık rızaya gerek olmaksızın kişisel verilerin işlenebildiği halleri düzenlemektedir:[76]

> "*Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:*
> *a) Kanunlarda açıkça öngörülmesi.*
> *b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.*
> *c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.*
> *ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.*
> *d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.*
> *e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.*
> *f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması*."

---

[75] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

[76] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

Zikredilen şartlar kişisel verilerin işlenmesinde açık rızanın aranmayacağı şartlar olup söz konusu verileri kişisel veri olmaması veya mezkur şartlara uygun olması durumunda herhangi bir açık rıza şartı aranmayacak ve kişisel veriler serbest bir şekilde işlenebilecektir.

2.2. AKILLI ŞEHİRLERDE OLASI MAHREMİYET SORUNLARI

Akıllı şehirlerin önemi, insan hayatının kolaylaştırılması adına kendisine duyulan ihtiyaçla orantılı olmasına rağmen ülkelerin teknolojiyi kullanma amaçlarına dair bakış açısında olan farklılıklar ile birlikte akademi, endüstri ve yönetim alanlarının iş faaliyetleri kapsamında akıllı şehirlerden istifade edebilecekleri amaçların farklı olması dolayısıyla akıllı şehirlere ortak bir tanım geliştirilememiştir.[77] Söz konusu durum akıllı şehirlerin ortak bir bakış açısına oturtulamaması ve dolayısıyla ortak bir mahremiyet kavramından söz edilememesine de sebep olmaktadır. Buna rağmen genel anlamda mahremiyet tartışmaları, bir kişi hakkındaki kişisel verilere ve özel nitelikli kişisel verilere erişim ve bunların ifşa edilmesine ilişkin uygulamalarla ilgilidir.

Kişisel olarak tanımlanabilir hiçbir bilgi, sahibinin izni olmaksızın işlenemez. Bu sebeple akıllı şehirlerde verilerin işlenmesinden kaynaklı birçok sorun ortaya çıkmaktadır. Buna karşılık akıllı şehirlerin, vatandaşlar için şehrinin bir dizi ölçümde nasıl performans gösterdiğini ve diğer şehirler ve bölgelerle karşılaştırıldığında nasıl olduğunu incelemek; yerel yetkililerin bütçelerini nasıl ve nerelere harcadıklarını görmek; gerçek zamanlı olarak ulaşım ve çevre ile ilgili neler olduğunu görmek; suçları bilmek gibi avantajları olacaktır. Bunların hepsinin gerçekleşebilmesi için gerçek zamanlı toplanan veriler de dahil olmak üzere şehirle ilgili neredeyse mevcut tüm veriler kullanılabilir hale getirilmelidir.

---

77 Köseoğlu, Ö., Demirci, Y. (2018). a.g.e. s.11

Akıllı şehirlerin inşası artık geleceğin bir çabası değil günümüzün bir gerekliliği haline gelmiştir.[78] Akıllı şehir uygulamaları çok büyük kolaylıklar sağlasa da gerçekçi uygulamalar farklı açılardan zorlanmaktadır. Tasarım, bakım ve uygulama maliyetleri ile birlikte en önemli sakıncalar arasında gizlilik ve güvenlik bulunmaktadır. Akıllı şehir için tanıtılan çerçeveler, vatandaşların mahremiyeti ve güvenliği ile ilgili birçok tehdidi de beraberinde getirmektedir. Akıllı şehirde iletişim için açık ağlar, akıllı telefonlar, bilgisayarlar vb. kullanılması dolayısıyla kişisel veriler saldırılara karşı daha savunmasız hale getirilmektedir. Bu nedenle, akıllı şehirde güvenliğin ve mahremiyetin sağlanması, gerekli ve açık bir meydan okumaya dönüşmektedir.

Akıllı bir şehirdeki birinin internetten yemek siparişi vermeye çalıştığını düşündüğümüzde kimlik numarası ile veya müşteri bilgileriyle; peynirli sandviç ve pizza sipariş edilmek istenir ancak sistem siparişi kabul etmeyi reddeder. Bunun sebebini araştıran kullanıcıya sistem tarafından en son yapılan kolesterol testi hakkında bilgi verilir ve raporlara göre o kişinin kolesterolünün yüksek olması nedeniyle peynir alımına izin verilmez. Ayrıca sistem, siparişi veren kişinin arkadaş listesinden kolesterol sebebiyle hastaneye kaldırılmanın sonuçlarıyla ilgili birkaç örnek vakayı da tanımlar. Buradaki endişe, peynirli sandviç yemenin uygun olmamasıyla ilgili değil, yalnızca çevrimiçi yemek siparişlerini alan sistemde mevcut olan ve kişisel tercihlerimize müdahale etmede bir araç olarak kullanılan kişisel verilerdir. Bu ve daha birçok benzer benzer senaryo, günlük faaliyetlerimizde yer alan teknolojinin bir sonucu olarak akıllı şehirlerde kolayca mümkündür.[79]

Görüldüğü üzere akıllı şehirlerde ürün ve hizmetlerin daha hızlı ve ucuz şekilde oluşması için ortaya çıkan akıllı uygulamalar, sadece teknolojik bağımlılığı artırmakla kalmayıp aynı zamanda kişisel veriye olan ihtiyacı da artıracaktır. Hatta söz konusu kişisel veriler yukarıdaki örnekten anlaşıldığı üzere özgür karar alma mekanizmasını sınırlayıcı bir etki de oluşturmaktadır. Bu nedenle özellikle kişisel verilerin korunması akıllı şehirler açısından oldukça önemli bir konu halini almıştır.

---

78 Ismagilova, E., Hughes, L., Rana, N.P. (2022). "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework". s.3

79 Kasar, S., Meghana, K. (2021). a.g.e s.29

Akıllı şehir pazarının önümüzdeki 20 yıl içinde 1,7 trilyon doları aşması beklenmektedir.[80] Buna rağmen akıllı bir şehrin çalışmasını sağlayan sanal ve fiziksel altyapı arasındaki karşılıklı bağlantı, yeni ve önemli siber güvenlik riskleri de beraberinde getirmektedir. Akıllı şehirlerde sağlanan her ek erişim noktasıyla kişisel verilerin güvenlik açıklarını genişletici etki oluşturmaktadır. Akıllı şehirler, çok sayıda siber saldırı tekniğinin yanı sıra kötü amaçlı yazılım gibi geleneksel araçlara karşı da hassas ve kırılgan olabilmektedir. Bu risklerin üstesinden gelmek için tüm tarafları (bireysel vatandaşlardan kamu ve özel kurumlara kadar) içeren kritik bir altyapı tasarlanmalıdır.[81]

Akıllı şehirlerin yaygın olarak eleştirilmesinin en büyük sebebi kuşkusuz mahremiyet ihlalleridir. Başkaca endişeler olarak verinin gücünden kaynaklı şirket-devler, şirket-vatandaş, devlet-vatandaş dengesinin bozulması söylenebilir. Kişisel olarak kimliğini belirli kılmaya yarayan verilerin akıllı şehirlerde bildirim ve rıza gibi mekanizmalara yönelik geleneksel mahremiyeti koruma araçlarının, günlük hayatın içine yerleştirilmiş, her yerde bulunan gözetim teknolojilerine karşı etkili bir şekilde sağlanıp sağlanamayacağı konusunda büyük endişeler bulunmaktadır. Nitekim bu kadar karmaşık bir sistemde geleneksel mahremiyet kurallarıyla kişisel verilerinin gizliliğinin sağlanması operasyonel açıdan oldukça zor olacaktır. Sisteme sürekli olarak veri sağlayan vatandaşlara ait kişisel verilerin ve bu verilere ilişkin rızanın nasıl çalışacağı konusu henüz açık değildir. Bir şehirde bulunan her kameradan veya enerji sarfiyatındaki akıllı takip sistemlerinin her kontrol edilmesinde açık rızanın alınabilmesi akla çok uygun gelmemektedir. Bu sebeple mahremiyetin sağlanabilmesi amacıyla kamusal alandaki akıllı sistemlere ilişkin bir çalışma yapılmalıdır. Zira akıllı şehirlerin gerek yerel ve merkezi hükümetler eliyle gerekse de kamu tüzel kişiliğinin kendi inisiyatifiyle özel hukuk tüzel kişilerine veri toplama imkânı verilmesi hususunda olsun vatandaşlar açısından büyük bir mahremiyet ihlaline sebep olabilmektedir.

---

80 Das, A., Sharma, S., Ratha, B. (2019). (Kitap Bölümü: The New Era of Smart Cities, From the Perspective of the Internet of Things). "Smart Cities Cybersecurity And Privacy". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları. s.7

81 Das, A., Sharma, S., Ratha, B. (2019). a.g.e. s.7

Mahremiyet türlerinden bahsedecek olursak; kimlik mahremiyeti (kişisel verileri korumak için), bedensel mahremiyet (gerçek kişinin beden bütünlüğünü korumak için), bölgesel mahremiyet (kişisel alanı, eşyayı ve mülkiyeti korumak için), konum ve hareket mahremiyeti (mekansal davranışın izlenmesine karşı koruma sağlamak için), iletişim mahremiyeti (konuşmaların ve yazışmaların gözetlenmesine karşı koruma sağlamak için) ve işlem mahremiyeti (genellikle çevrimiçi platformlarda yapılan sorguların/aramaların, satın almaların ve diğer alışverişlerin izlenmesine karşı koruma sağlamak için) olarak tasnif edilebilir.[82]

Yapılan tasniften de anlaşılacağı üzere akıllı şehirlerde oluşan sorunların yalnızca teknoloji yardımıyla çözülebileceği algısının hatalı olacağıdır. Nitekim teknoloji ve veri ile gün yüzüne çıkan akıllı şehirlerde şehirlerin karşılaştığı problemler ve bu problemlere bulunan kalıcı çözümlerin yerine hızlı ve kolay çözümler bulmak için teknolojiden yararlanmak pek de haksız bir yaklaşım olmayacaktır.[83] Buna rağmen akıllı şehirler ile birlikte insanların hayat tarzlarında ve yerel ve merkezi hükümetlerin yönetim ve demokrasi anlayışlarında hatırı sayılır dönüşümler yaşanabilecektir. Bunun yanı sıra, daha fazla kaynak harcamanın önüne geçmek için şehirlerin karşılaştığı büyük zorluklara karşı daha cesur politikalar ortaya koymayı kolaylaştıran daha adil çözümler bulunabilmektedir.

Bununla birlikte akıllı şehirlerin güç tüketimi, izleme ve bakım gibi kendi altyapısal zorlukları vardır. Sensörlerin çoğu enerji ile çalışır, enerjinin kesilebilme endişesinden dolayı, tüm sistemin bir anda çökebilme durumu unutulmamalıdır. Bu durumda sensörlerin ve altyapının izlenmesi, tüm ağdaki önemlerine bağlı olarak insan müdahalesini gerektirebilir. Arızalı cihazların değiştirilmesi, bozuk iletişim yollarının yeniden kurulması ve altyapının daha da yükseltilmesi için yeni donanım ve yazılım iyileştirmeleri gerekebilir. Altyapıyla ilgili tüm bu sorunların yanı sıra, akıllı cihazlar

---

82 Kitchin, Rob. (2016). a.g.e. s.25

83 Gharaibeh, A., Khalil, I., Salahuddin, M., Guizani, M. (2017). "Smart Cities: A Survey on Data Management, Security and Enabling Technologies". IEEE Communication Surveys & Tutorials. s.10

arasındaki açık kablosuz iletişim, önemli bir güvenlik açığı olan kişisel verilerin güvenliğini sağlama zorluğunu da beraberinde getirmektedir.[84]

Cihazların akıllılığı, verilerin gönderilmesine ve alınmasına dayanır. Bu bilgiler davetsiz misafirler tarafından ele geçirildiğinde, iletişim güvenliği IoT tabanlı Akıllı Şehirlerde büyük bir tehdit oluşturacaktır. Bu güvenlik ihlalinin yansımaları, evdeki veya yoldaki sensörlerden gelen bilgilerin mevcudiyeti nedeniyle kullanıcıların mahremiyetinin kaybolmasına neden olabilecektir. Bir bireyin günlük rutini ile ilgili neredeyse tüm bilgiler akıllı şehirlerde mevcut olduğundan, saldırıların kapsamı maddi kayıpların ötesine geçerek kişiselleştirilmiş saldırılara da sebep olabilecektir. Örneğin, uyuşturucu bağımlısı bir hastanın enjektör ile aldığı günlük ilacına ilişkin enjektöre giden kontrol sinyali manipüle edilirse, bu bağımlı ve tedavi edilen bir bireyin ölümüne yol açabilecektir.

Bireyin hedeflenmesinin yanı sıra, bilgisayar korsanlarının tüm altyapının kontrolünü ele geçirmesi, tahribat oluşturması ve insan hayatını tehlikeye atması vakaları görülebilecektir. Ev, ofis, ulaşım ve akıllı şebekeler de dahil olmak üzere her şeye kimlik doğrulama ile uzaktan erişebilmek mümkün olmaktadır. O yüzden kötü niyetli biri, kimlik doğrulamanın güvenlik duvarını kırabilirse, işleri istediği gibi hareket ettirecektir. Bu nedenle tüm şehir, sakinleriyle birlikte, uzaktan çalışan biri tarafından planlanan siber bir saldırı riski altında kalabilmektedir.[85]

Tüm bu sebeplerden dolayı 6698 sayılı Kanunun "*Veri güvenliğine ilişkin yükümlülükler*" başlıklı 12. maddesinin (1) numaralı fıkrasında "*Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak*

---

84 Saini, R., Mishra, D. (2019) a.g.e. s.40
85 Saini, R., Mishra, D. (2019) a.g.e. s.40

zorundadır."[86] hükmüne yer verilmiştir. Bahse konu düzenleme ile veri sorumluları tarafından alınması gereken tüm tedbirler belirtilmiştir.

Buna rağmen IoT cihazlarının bu konuda ciddi ölçüde başarısız olduğunu söylemek mümkündür. LoT'nin mahremiyet açısından daha önce de bahsedildiği gibi önemli bir sorunu, cihazlarının açıkça kullanıcı deneyimi olarak göze batmayacak ve kusursuz olacak şekilde tasarlanmış olmasıdır. Bir başka deyişle, kendilerini gündelik yaşamın dokusundan ayırt edilemez hale gelinceye kadar bir örümcek gibi ağlarını örmektedir. Oturma odasındaki akıllı ortam aydınlatması veya akıllı termostatlar gibi IoT sistemleri, genellikle kullanıcının ihtiyaç ve isteklerinin bağlamsal olarak farkında olacak, günlük uygulamaları ve rutinleri hakkında bilgi toplayacak ve aynı zamanda görünmez kalacak şekilde tasarlanmıştır. Buna karşılık, kişisel verileri çevrimiçi bir sosyal medya platformunda paylaştığımızda, söz konusu platformda kişisel verilerimizin işleneceğine ilişkin bir bilinç eşiğini geçtiğimizin farkındalığıyla ve genellikle hizmeti kullanmaya başlamadan önce en az bir kez kişisel veri işlenmesine ilişkin izin verme veya izni geri alma haklarımızın bulunduğunun bilincinde davranırız. Buna karşılık nesnelerin internetinde bu tür bir bildirim ve fırsat için çoğunlukla tasarım gereği bulunmamaktadır. Göze çarpmayan bir işlev özelliği olmadığı durumlarda bile, cihazlar genellikle küçük ve ekransız olduğundan dolayı IoT cihazları, gizlilik bildirimlerini görüntüleme veya bireyler tarafından izin verilen tercihler sağlama araçlarına sahip değildir.

Bahsedilen sorun evlerde ne kadar olumsuz olursa olsun akıllı şehirlerin halka açık yerlerinde daha da ciddi bir sıkıntı oluşturmaktadır. Zira tüketiciler en azından teorik olarak akıllı termostatlarının gizlilik politikasını okuma şansına sahip olabilirken, işe gittikleri akıllı yol veya akıllı tramvay aracılığıyla kişisel verileri toplandığında gerçek anlamda böyle bir şansa sahip olamayacaklardır. Örnek vermek gerekirse ulaşım hizmeti amacıyla akıllı şehirdeki bir otobüsün konum verileri işlendiğinde söz konusu işlemenin bir kişisel veri işleme faaliyeti olmayacağı açıktır. Buna rağmen söz konusu konum verisi işleme faaliyeti otobüsü kullanan bir kişiyi veya otobüste bulunan bir

---

[86] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

kişinin konumunu tespit etmeye yönelik ise bir kişisel veri işleme faaliyetinden söz etmek mümkün olacaktır.[87]

Akıllı şehirlerde neredeyse tüm sistemler kişisel verileri anonimleştirmeden işlemektedir. Bu sebeple IoT cihazlarının hiçbir kullanıcının rızası alınmadan ve veri akışı olduğu dahi fark edilmeden akıllı cihazlar arasında veri akışının ciddi sıkıntılara sebep olabileceği su götürmez bir husustur. Bunun yanı sıra bazı cihazların belirli özelliklerini kısıtlamak da çok olası bir seçenek olmayacaktır. Bu sebeple AB hukuku ve Türkiye'de yerleşik kişisel veri koruma mevzuatı, IoT cihazları açısından etkisiz olabileceği değerlendirilmektedir. Böyle bir durumda, her ne kadar zor olduğu kabul edilse de kullanıcıların kendi kişisel verilerini mümkün olduğu kadar korumaları ve buna uygun önlemler almaları gerektiği düşünülmektedir. Benzer önlemlerin, IoT cihazlarının yazılım ve donanım taraflarına eklenmesi gündeme geldiğinde unutulmamalıdır ki IoT cihazlarını üreten şirketlerin ana amacının karlılık olduğu ve mahremiyete önem veren bir tavır sergilemeyecekleri hususudur. Örnek vermek gerekirse, kullanıcının mahremiyetine önem veren bir buzdolabının veya kişisel verilerin aktarılmayacağını garanti eden bir çamaşır makinasının varlığını kimse duymamıştır.[88] Bu sebeple Kanunun 12'nci maddesinde sayılan veri sorumlusuna ait yükümlülükleri, IoT cihazlarına ilişkin kişisel veri işlendiği durumunda ortaya çıkacaktır.

Mahremiyet, temel bir insan ihtiyacı olması dolayısıyla bir kişi, bazı özel hayatına ilişkin bilgilerinin arkadaşları tarafından, finansal bilgilerinin bankacısı tarafından ve sağlığına ilişkin bilgilerinin ise doktorları tarafından bilindiğinin farkında olarak kendini güvende hissedebilecektir. Bununla birlikte, yukarıda bahsedilen farklı meslek gruplarından olan insanların herhangi birisi kendisi hakkındaki özel hayat, finansal ve sağlık bilgilerini aynı anda biliyorsa, kişi kendini rahat hissetmeyecektir.[89] Bunun nedeni, kişi hakkında bilgi toplanması, alışkanlıkları, inançları ve sağlığı hakkında bilgi

---

87 Kocabıyık, O. (2023). a.g.e. s.42

88 Zoonen, L. (2016). "Privacy Concerns in Smart Cities". Government Information Quarterly v. 33. s. 473

89 Magi, T. (2011). "Fourteen reasons privacy matters: a multidisciplinary review of scholarly literature", Quarterly Library. s.190.

edinilmesine izin verilmesidir. Bu durum ise kişi için dezavantajlı bir durum oluşturabilmektedir.[90] Bu sebeple kişisel verilerin bilinmesi, kişisel zararın yanı sıra kimlik hırsızlığı, şantaj ve kişiye karşı işlenen hırsızlıklar gibi yasadışı faaliyetlere yol açabilmektedir. Beş tür vatandaş gizliliği vardır ve bunlar; kimlik gizliliği, arama gizliliği, konum gizliliği, ayak izi gizliliği ve mülkiyet gizliliği olarak sıralanabilir.

Kimlik gizliliği, kullanıcıların akıllı şehir bileşenleriyle iletişim kurduklarında tanımlanabilecekleri bilgileri içerir ve kişiyi belirli kıldığı için akıllı şehirlerde açıkça bir kişisel veri olarak atfedilmektedir. Örneğin, akıllı telefona yüklenen bir uygulama yalnızca uygulamanın amacına katkıda bulunmakla kalmaz, aynı zamanda kişinin kişisel verilerini de paylaşabilir. Kimlik gizliliği, uygulamayı kullanan kişinin tanımlanmasıyla sınırlı olmayıp bazen bir kişinin uygulama için izin verdiği veriler, diğer kişilere ait kişisel verileri de içerebilmektedir. Örneğin, sosyal medya kullanıcısı olmayan bir kullanıcının, diğer kullanıcılardan, o kişi hakkında paylaşılan bilgileri kullanılarak kişisel bilgilerini, toplanan verilerden elde edilen kalıplarla karşılaştırmak için kullanılan teknik manasına gelen profilleme çıkarılabilir.[91] Benzer şekilde, multimedya verileri de diğer kişilerce paylaşılarak veya görüntüleri ifşa edilerek mahremiyet ihlaline sebebiyet verebilir.[92] Arama gizliliği, kullanıcılar tarafından sorulan sorgularla ilgili olup kişinin araştırdığı ve sorduğu sorular analiz edilerek kullanıcı kimliği tanımlanabilir veya tespit edilebilir.[93]

Konum gizliliği, kullanıcıların belirli zamanlardaki konumları hakkındaki bilgilerini içerir. Modern cep telefonları gibi cihazlar, boylam ve enlem gibi GPS tabanlı konum bilgilerini toplayabilir ve kullanıcılarının mekansal ve zamansal tercihlerini ortaya çıkarabilir. Konum tabanlı bir hizmeti, örneğin yakınındaki bir restoranı sorgulayan biri,

---

90 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). (Kitap Bölümü: Crowdsensing And Privacy İn Smart City Applications). "Smart Cities Cybersecurity And Privacy". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları. s.59

91 Aksoy, H.C., (2022). "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme" *Kişisel Verileri Koruma Dergisi*. 4(2), s.72.

92 Y. Li, Y.-S. Jeong, B.-S. Shin, J.H. Park. (2017). "Crowdsensing multimedia data: security and privacy issues", IEEE Multimedia. s.60.

93 H. Li, H. Zhu, S. Du, X. Liang, X. Shen. (2016) "Privacy leakage of location sharing in mobile social networks: attacks and defense". *IEEE Transactions on Dependable and Secure Computing Dergisi*, Sayı: 15. s.650

konumunu gösterebilir. Konum verilerinden ve zaman damgalarından, bir kişinin demografik bilgileri, ev ve iş adresleri, işe gidip gelme rotaları ve diğer alışkanlıkları hakkında bilgiler kolayca türetilebilmektedir.[94]

Ayak izi gizliliği ise bir sistemde kalan küçük bilgi parçalarının birleşimiyle ilgili risklerle ilgilidir. Örneğin, bir web sayfasına erişmek için web tarayıcısı kullanan bir kişi, cihazda ve tarayıcıda bıraktığı çerezlerden dolayı, bireyin tercihlerini ortaya çıkarabilen ayak izini oluşturmaktadır.[95] Öyle ki, günümüzde ilgili kişilerin çerezler vasıtasıyla mahremiyetlerinin ihlal edilmesi kabul görmüş bir durumdur ve ilgili kişilerin bu sayede profilleri çıkarılabilmektedir.[96] Dolayısıyla ayak izi gizliliğinde kişisel veri olma özelliğini bireyin tanımlanabilir kılınması anından itibaren kazanmış bulunmaktadır.

Akıllı şehirlerdeki veri işleme faaliyetinin denetimsiz kalması en istenilmeyen durum olacağı şüphesidir. Nitekim vatandaşların kişisel verilerinin hangi araçlarla, ne şekilde işleneceği, nerelere nasıl aktarılacağı, nerelerde ne kadar saklanacağı gibi soruların Kanun yoluyla düzenlenmesi ve şeffaf bir şekilde uygulamaların görülebilmesi gereklidir. Aynı zamanda kamu yönetimi bakımından da şeffaflık ve hesap verilebilirlik ilkelerinin kişisel veriler bakımından uygulanması elzem bir konudur.

Kişisel verilere ilişkin herhangi bir denetim mekanizmasının olmadığı varsayıldığında veri sorumluları tarafından kolaylıkla aktarılabileceği unutulmamalıdır. Söz konusu veri aktarımına dair herhangi bir merkezi denetimin olmaması durumunda akıllı şehirlerde kamu hizmeti olarak her türlü verinin işlenebileceği, saklanabileceği, aktarılabileceği ve imha edilebileceği düşüncesinin doğru olmayacağı ve bir keyfiyete sebep olabileceği değerlendirilmektedir. Ayrıca söz konusu hizmetlerin kamu tarafından özel sektör eliyle kullandırıldığı durumlarda denetim mekanizmasının önemini daha da artırmaktadır.

---

94 P. Joglekar, V. Kulkarni (2017) "Privacy Issues in Urban Computing using Mobile Crowdsensing" International Journal of Computer Applications, Volume 168, s.24

95 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). s.59

96 Aksoy, H. C. ve Halıcıoğlu, M. (2021). "AB ve Türk Hukuklarında Çerezler". *Kişisel Verileri Koruma Dergisi*. 3(1), s.62

Bu kapsamda 6698 sayılı Kanunun Kanunun "İlgili Kişinin Hakları" başlıklı 11. maddesine göre, herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

> *"a) Kişisel veri işlenip işlenmediğini öğrenme,*
> *b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,*
> *c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,*
> *ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,*
> *d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,*
> *e) 7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,*
> *f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,*
> *g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,*
> *ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme*

haklarına sahiptir." hükmü bulunmaktadır.[97] Dolayısıyla ilgili kişilerin kişisel verilerin korunması hakkında başvurabileceği yollar Türk hukukunda açıkça belirtilmiştir.

Kişisel veri mahremiyeti en az fiziksel mahremiyet kadar önemlidir. Bu sebeple gerek devlet tarafından gerekse vatandaş tarafından korunmalıdır. Vatandaşların bu konuda aydınlatılması ve kişisel verilerin korunması alanında bilinçlendirme çalışmalarının yapılması önem arz etmektedir. Nitekim Kanunlar bulundukları ülkedeki bilinç düzeyi doğrultusunda uygulanabilir olmaktadır. Bu sebeple veri mahremiyeti ve kişisel verilerin korunması bakımından insanların bilinçlenmesi ve her bireyin kendi kişisel verisini öncelikle kendisinin koruması gerekmektedir. Aynı zamanda teknolojik gelişmelerle giderek ihtiyaç haline gelen ve giderek önemi artacak olan akıllı şehirlerde hükümetler ve şehir yöneticileri tarafından bilinçlendirme faaliyetinin önemi de artmaktadır.

---

[97] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

Son yıllarda farklı akıllı uygulama senaryolarında önemli sorunlarla karşılaşılmaktadır. Örneğin, akıllı şebekelerdeki akıllı ölçüm altyapısı, konut sakinlerinin yaşam alışkanlıkları ve çalışma saatleri de dahil olmak üzere özel hayatlarını izleyebilmektedir.[98] Benzer şekilde akıllı evler ve akıllı sağlık hizmetleri bağlamında cihaz üreticileri ve hizmet sağlayıcıları da kullanıcıların özel nitelikli kişisel verilerine erişebilmektedir. Akıllı mobilite uygulamaları tarafından toplanan büyük miktardaki konum verisi, kullanıcının konumunu ve mobilite araçlarını anlamak için kullanılabilmektedir.

Bu sorunlara ek olarak, yüksek teknoloji şirketleri, trafik kazalarını azaltmayı ve daha temiz ve akıllı bir toplum inşa etmeyi amaçlayan otonom araçlar geliştirmek için milyarlarca dolar harcamasına rağmen akıllı araçların büyük bir güvenlik sorunu olarak görülebileceği de unutulmamalıdır. Nitekim bir Akıllı araç siber saldırıya uğradığında hem can güvenliği hem de kişisel veri gizliliği tehdit altına girecektir. Özellikle bilgisayar korsanları, fren yapmak, motoru kilitlemek ve direksiyonu kontrol etmek gibi uzaktan saldırılar gerçekleştirmek için güvenlik açıklarından yararlanabilirler. Ayrıca otonom bir aracın bilgisayar sistemi tarafından toplanan büyük miktarda kişisel veriler, önemli gizlilik sorunlarına neden olabilir. Benzer şekilde yapay zeka sistemleri de ticaret sistemlerinin, ev aletlerinin ve kalp pillerinin otomatik kontrolü gibi çeşitli akıllı uygulamalarda vazgeçilmez roller oynamasına rağmen yapay zekanın giderek artan kullanımı güvenlik risklerini de beraberinde getirmektedir.[99] Örneğin, hizmet sağlayıcılar ve cihaz üreticileri, kişisel verileri analiz etmek ve ilgili hizmetlerin birincil hedeflerini aşan hassas verileri işlemek amacıyla veri madenciliği teknolojilerini kullanabilmektedir. Bununla birlikte yapay zeka bilgisine sahip saldırganların da makinalar ve uygulamalar gibi giderek daha akıllı hale geldiğini unutmamak gerekmektedir.[100]

---

98 Zoonen, L. (2016). a.g.e. Government Information Quarterly v. 33. s. 475

99 Bianca W. (2022). "Artificial Intelligence in the City: Building Civic Engagement and Public Trust". (Kitap Bölümü: AI Trust, and the City: Assets and Accountability). (Editörler: Brandusescu, A., Reia, J.). Centre For Interdisciplinary Research on Montreal. s.73

100 Bianca W. (2022). a.g.e. Centre For Interdisciplinary Research on Montreal. s.74

Akıllı şehir teknolojileri, her türlü kişisel veriyi elde eder ve söz konusu verilerin hacmini ve kapsamını olağanüstü bir şekilde genişletir. Önemli olan bu verilerin elde edilmesi ve dağıtılmasıdır. Veriler dijital veri tabanlarında düzenlendiği ve saklandığı için veri analitiği kullanılarak incelenmeye oldukça uygundur. Dolayısıyla gözetimin yanı sıra, takma adlar(pseudonym), kullanıcı adları, parolalar, hesap numaraları, adresler, e-postalar, telefon numaraları, kredi kartı numaraları vb. veriye dayalı araçlar olmaksızın günlük yaşamı sürdürmeyi neredeyse imkânsız hale getirerek insanın da verileşmesine sebep olur.

Bir birey hakkında doğrudan bir veri tabanında kodlanmasa dahi kişisel verilerle alakalı profilleme yöntemiyle akıllı şehirlerde mahremiyet zararları üretilebilir. Örneğin, başkalarıyla ortak yakınlık ve ortak hareket potansiyelinden dolayı belirli gruplara üyeliği açığa çıkaracak şekilde siyasi, sosyal ve dini inanç verileriyle ilgili sonucunu çıkarmak için kullanılabilir. Benzer şekilde, sosyal medyada birkaç kişinin gönüllü olarak verdiği verilerle, sosyal ağlarda yapılan analiz yoluyla birçok kişi hakkında açıklanmayan bilgilere erişmenin kilidini açabilir. Buna da örnek vermek gerekirse sosyal medya kullanıcılarının yalnızca yüzde yirmisinin cinsel yönelimini bilmenin, neredeyse diğer tüm kullanıcıların cinsel yönelimlerine ilişkin yüksek doğrulukla çıkarım sağlanması anlamına gelebilmektedir.[101] Tahmine dayalı bir profil adına üretilen herhangi bir cinsel yönelim çıkarımı, aile evine gönderilen reklamlar veya ailede ortak kullanılan bir bilgisayarda sosyal medya aracılığıyla paylaşılırsa, bu durum aile içerisinde hasarların yanı sıra birçok kişisel ve sosyal hasara neden olabilecektir.

Bireysel mahremiyetin sağlanmasına yönelik temel stratejilerden bazıları; takma adlar, veya çeşitli anonimleştirmelerdir. Bununla birlikte büyük verinin üretilmesi, birçok durumda verilerin yeniden tanımlanmasını nispeten basit hale getirebilir. Özellikle takma adlar, bir kişiyi tanımlamak için isim yerine benzersiz bir etiketin kullanıldığı anlamına gelir ve anonim olarak değerlendirilir. Bununla birlikte, takma adlar da diğerlerinden ayırt edilebilir ve sürekli olarak tanınabilir, zaman ve mekan içinde takip

---

[101] Kitchin, R. (2016). a.g.e. s.33

edilebilir ve ayrıntılı bireysel profiller oluşturmak için kullanılabilir.[102] Kişinin kimliği net olarak belirlenemese bile takma ismin kalıcı olması, veri sorumlularının bu veriler üzerinden hareket etmesine ve bireylerle nasıl etkileşime gireceğini profillemesine olanak tanır. Ayrıca akıllı şehirlerde bir takma adın diğer hesaplara ve işlemlere bağlanması, onun potansiyel olarak yeniden tanımlanabileceği anlamına gelmektedir. Bu sebeple veriler tamamen kimliksizleştirilmedikçe, veri kümelerini tarayıp birleştirerek anonimleştirmeyi tersine çevirmenin mümkün olduğu açıktır. Bir başka boyutu olarak kişisel verilerin üçüncü taraflarla paylaşılmadan önce bunun ne ölçüde gerçekleştiği oldukça şüphelidir.

Profilleme konusunda Genel Veri Koruma Tüzüğü'nün 22'nci maddesinde bazı durumlarda ilgili kişiler hakkında otomatik yollarla karar verilmesi mümkün olmaktadır söz konusu durumlar; "*birlik veya üye devlet hukukunun izin vermesi (ilgili kişinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacıyla uygun tedbirlerin de belirtilmesi kaydıyla), ilgili kişinin açık rızasının varlığı ve ilgili kişi ve veri sorumlusu arasında bir sözleşme kurulması veya ifası için gerekli olması.*" olarak sayılabilir.[103] Dolayısıyla akıllı şehirlerde yukarıda sayılan hallerde ilgili kişiler hakkında profillemeye başvurulması meşru kabul edilmektedir. Bununla beraber 6698 sayılı Kanunun 11'inci maddesinde zikredilen "münhasıran otomatik sistemler vasıtasıyla" ifadesinin profillemeye işaret ettiği yorumu çıkarılabilecektir.[104] Dolayısıyla veri sorumlusuna başvuru mekanizması içerisinde zikredilen hususta profilleme öncesinde aydınlatmanın yapılması da gerekmektedir.

Bahsedildiği üzere kişisel veriler öngörülemeyen şekillerde paylaşılabilmekte ve yeniden kullanılabilmektedir. Bir başka deyişle, kişisel verilerin yalnızca belirli bir amaçla işlenmesi, yalnızca o amaç için gerekli olduğu sürede saklanması ve yalnızca o amaçla ilgili yerlere aktarılması ilkelerinin sekteye uğraması anlamına gelebilir. Amacı dışında işlenen, saklanan ve aktarılan kişisel veriler ise daha sonra ilgili kişilere bildirimde bulunmaya veya açık rıza almaya gerek kalmadan veri ticareti amacıyla çok

---

102 Joglekar, P., Kulkarni, V. (2017) a.g.e. International Journal of Computer Applications, Volume 168, s.24

103 Aksoy, H.C., (2022). a.g.e. *Kişisel Verileri Koruma Dergisi*. 4(2), s.78.

104 Aksoy, H.C., (2022). a.g.e. Kişisel Verileri Koruma Dergisi. 4(2), s.82.

sayıda yolla satılabilir ve yeniden kullanılabilir. Burada temel amaç; tahmine dayalı profil oluşturmak, sosyal olarak kategorileştirmek, davranışsal olarak dürtüleri harekete geçirmek, bireyleri kontrol etmek veya yönetmek olabilecektir.[105] Bu sürecin sonunda meydana gelebilecek kavram olan 'veri determinizmi', bireylerin tahmine dayalı gelecekteki olası davranışları veya olayları değerlendirmek ve uygun eylemlerini yönlendirmek için kullanıldığı ileriye dönük yönetişim biçimi olarak da ifade edilebilir. Örneğin polis birimlerinin gelecekte işlenecek suçların yerlerini tahmin etmek ve polis memurlarını bu bölgelerde devriye sayısını artırmak amacıyla yönlendirmek için tahmine dayalı analitiği kullanabilirler. Tüm bu durumlarda, kişisel verileri tahmine dayalı profiller oluşturmaya yarayan uygulamalar, ilgili kişilerin makul mahremiyet beklentilerine zarar verebilir.

Bir başka önemli husus ise kişisel verilerin ve mahremiyetinin korunmasının temel taşı olarak kabul edilen bildirim ve onay mekanizmasının akıllı şehir teknolojilerinde önemli ölçüde zayıfladığıdır. Yukarıda belirtildiği gibi bireyler günlük olarak birçok akıllı şehir teknolojisiyle etkileşime girmekte ve bunların her biri kendileri hakkında kişisel veri üretmektedir. Bu etkileşimlerin hacmi ve çeşitliliği göz önüne alındığında, bireylerin düzinelerce kuruluş genelinde mahremiyetlerini denetlemesi, verilerin şimdi ve gelecekte nasıl kullanılacağını bilmeden ilgili kişilerin önlerine sunulan çeşitli şartlar ve koşulları kabul etmenin maliyet ve faydalarını değerlendirmesi pek mümkün değildir.[106] İlgili kişiler, tüm bu sistemler ve uygulamalar genelinde kişisel veri mahremiyetini yönetmek istese bile uzun ve karmaşık yasal belgelerle karşı karşıya kalacak ve sonucunda ilgili kişi ya hizmete izin verecek ya da hizmeti reddedecektir. Sonuç olarak, bildirimde bulunmak ve rıza istemek uzun vadede yorucu ve boş bir uygulama haline gelebilecektir. Bu durumda da gizlilik politikaları, ilgili kişiler için mahremiyet güvencesi olmaktan çok veri sorumluları için sorumluluk reddi işlevi

---

105 Ünal, S., Sezgin, A. (2021). "Büyük Veri (Big Data)'nin Yapay Zekâ Uygulamalarında Toplumsal Sınıflandırmaya Yönelik Kaygılar" *Bilişim Teknolojileri Online Dergisi*. s.49

106 Ünal, S., Sezgin, A. (2021). a.g.e. *Bilişim Teknolojileri Online Dergisi*. s.49

görecektir. Söz konusu rıza yorgunluğuna bağlı olarak bilinçsiz bir şekilde ya tüm seçenekleri kabul edecek ya da hizmetten mahrum kalacaktır.[107]

Anlaşıldığı üzere, akıllı şehir uygulamaları birbiriyle ilişkili nedenlerden dolayı bir dizi potansiyel mahremiyet zararına neden olabilmekte ve bunların her biri mahremiyetin korunmasına yönelik mevcut yaklaşımlar açısından da önemli zorluklar doğurabilmektedir. Dahası, bu konular genel kamuoyunu, özel sektörü, kanun koyucuları ve uygulayıcıları önemli ölçüde ilgilendirmektedir.

2.3. AKILLI ŞEHİRLERİN ADALET VE TEMSİL YÖNÜNDEN SAKINCALARI

Şehrinizdeki yollarda bulunan çukurları coğrafi olarak etiketleyebilirsiniz ve arabanızı sürerken arabanız çukura düşmesi durumunda söz konusu çukuru belediyeye bildirerek belediyenin ilgili departmanı tarafından tamir ettirebilirsiniz. Aslında başlangıçta toplumu dahil etmenin iyi bir yolu olduğu düşünülen sonuç, daha fazla çukurun ve şehrin daha fazla teknolojiye sahip olma eğiliminde olan daha zengin bölgelerinin düzeltilmesinin bir sonucu olmasıdır. Yani teknolojiye erişim imkânı olan bölgelerde bulunan çukurların bildirilerek tamir edilmesi sağlanmakla birlikte teknolojiye erişim imkânı diğeri kadar iyi olmayan kırsaldaki vatandaşların çukurları tamir edilmeyecektir. Bu yüzden akıllı şehirlerde sadece çukurların nerede olduğu hedeflenmeye çalışılsa bile, şehrin zengin bölümlerinde katılımın artması, sorun bildirme ve karar alma süreçlerine erişim imkânı kısıtlı olan kesimlerden daha fazla kural belirlenmektedir.

Bir işletme, altyapısını ve hizmetlerini kullanan kullanıcılarının özel bilgilerinin güvenliğini sağlamaktan sorumludur. Benzer şekilde devletler de hizmetlerini verimli ve sorunsuz bir şekilde sağlamak için vatandaşlarını en iyi şekilde tanımlamaları gereken ve verilerini işleyen kuruluşlardır. Örneğin, Türkiye Cumhuriyeti vatandaşlarına verdiği kimlik numaraları üzerinden hangi hastaneden hangi hizmeti aldığını ve hangi ilaçları kullandığına ilişkin verileri işlemek zorundadır. Söz konusu

---

[107] Aksoy, H. C. ve Halıcıoğlu, M. (2021). a.g.e. *Kişisel Verileri Koruma Dergisi*. 3(1), s.73

veriler ise özel nitelikli kişisel veri olarak kabul edilmektedir. Aynı zamanda devletler, biyometrik tabanlı bir kimlik veri tabanı ve kimlik doğrulama sistemi geliştirerek günümüzün cep telefonları ve kişisel cihazları, kullanıcılarının biyometrik bilgilerini bir araya getirebildiğinden kullanıcıların akıllı şehirlerdeki kitle algılama uygulamaları için kimlik doğrulamak ve akıllı şehir uygulamalarına bağlanmak için kullanabilirler. Bunun yanı sıra söz konusu hizmetleri kullanmakta zorluk çeken vatandaşların süreç içerisinde sistemin dışına atılması ve çeşitli temsiliyet sorunları oluşmasına yol açmaktadır.

Her insan hayatı onurlu, huzurlu, sağlıklı bir çevreyle yaşamak ister. Hiç kimse, veri toplayan ve insanları gözlemleyen kameraların gözetimi altında olmak istemez. Yaşamın mücadelesi ile kaliteli yaşam arasında bir denge olmalıdır. Polise yardımcı olmak ve suçu azaltmak için kamera ve sensörlerden faydalanılabilir ancak insanların sürekli gözetim altında olduğunu bilmesi oldukça rahatsız edici bir durum olacaktır. Amacını aşacak şekilde yerleştirilen bu kamera ve sensörlerin, insanlarda korku ve paniğe sebep olacağı değerlendirilmektedir.[108]

Toplum içerisinde bazı gruplar marjinalleştiğinde de temsil noktasında bazı sorunlar ortaya çıkmakta ve kamu otoritesine dair güven ortamının oluşmasında bazı sakıncaları beraberinde getirmektedir. Marjinalleşmiş gruplar kamu otoritesinin kendilerini daha fazla gözetim altında tuttuğunu ve bu yüzden her hareketlerinin takip edildiğini düşünmektedirler. Dahası akıllı kelimesinin akıllı şehirlerden ziyade marjinalleşmiş grupları izlemeye yarayan ve algısal olarak akıllı polis içgüdüsüyle sonuçlanmaktadır. Bu sorunların üstesinden gelmenin yolları, eşitlik ve doğru temsil sistemini oturtmak olmalıdır. Bunun yanı sıra erişilebilirlik sorunlarını da ortadan kaldırarak geleneksel olarak marjinalleştirilen toplulukların da dahil olacağı bir dizi kullanıcı merkezli çözümler üretmek gerekmektedir.

İnsanlar için şehir sorunlarına makul bir çözüm sağlama beklentisi olarak akıllı şehir uygulamalarında adalet ve temsil etrafında çeşitli şikayetler ortaya çıkmaktadır. Akıllı şehirlerin daha verimli kentsel yaşama ve şehir hizmetlerine izin vermesi, tahmine

---

[108] P. Joglekar, V. Kulkarni (2017) a.g.e. Volume 168, s.34

dayalı polisliğe ve ayrımcılığa uğramış toplulukları hedef almasına sebep olabilmektedir. Tipik olarak zaten marjinalleştirilenlerin hapsedilmesine yol açan bir gözetim modelinde akıllı şehirler, adil yönetilmediği takdirde daha yüksek oranlarda suçlara ve ötekileştirilmiş grupların varlığına yol açabilecektir.

Bir diğer geçerli endişe ise sakinlerin her gün temas ettiği tüm akıllı sensörlerden toplanan verilerdir. Toplanan veriler ile verileri toplanan kullanıcının kimliği arasında bir ayrım olmalıdır. Akıllı şehir uygulaması, çözümlerine şeffaflık ve eğitim ekleyerek akıllı şehir sakinlerinin bazı endişelerini gidermelerine yardımcı olabilir. Bununla birlikte yerel yönetim yetkililerinin ve akıllı şehir sakinlerinin de topluluk kurullarına ilişkin karar verme süreçlerine dahil olmaları gerekmektedir.[109]

Türkiye'de E-Devlet uygulaması akıllı şehir uygulamasının entegrasyonu için başarılı bir örnek sayılabilir. Ayrıca bu şekilde bir uygulamayı ve dolayısıyla devasa miktarda veriyi yönetebilmenin oluşturacağı zorlukları göz ardı etmemek gerekir. Türkiye Cumhuriyeti'nin hayata geçirdiği bu uygulamayı şehirler özelinde oluşturmanın ortaya çıkaracağı farklı ve iyi yönleri de olacaktır. Bunlardan bazıları sosyal güvenlik yardımlarının doğru adrese ve ihtiyaç duyulan miktarda ulaştırılmasını sağlamaktır. Bir diğeri ise akıllı şehirde eğitim eşitsizliğinden mustarip olan mahallelere daha fazla önem vererek toplumsal tabakalaşmanın önüne geçmektir.

Bir başka boyut olarak, kamu yönetiminin klasik yaklaşımlarının giderek büyüyen nüfusu ve kentleri yönetmekte güçlük çektiği ortadadır. Bu yüzden gerek kamunun gerekse şirketlerin ve küçük işletmelerin akıllı şehir uygulamalarını benimsediklerine şahitlik edilmektedir. Bu sebeple kamunun, şirketlerin ve bireylerin güncel teknolojik gelişmelere uyum sağlaması önemli bir hale gelmektedir.[110]

---

109 Kasar, S., Meghana, K. (2021). a.g.e. s.42.
110 Hayta, Y. (2021). a.g.e. s.931

2.4. KAMUSAL GÖZETİM VE AKILLI ŞEHİRLERDE KAMUNUN ROLÜ

Akıllı şehir uygulamalarında akıllı devlet bileşeninin yanı sıra kamunun rolü ve kamusal gözetim oldukça önemlidir. Özellikle şehrin meydan, cadde, toplanma alanı vb. kamusal alanlarının kamera ve sensörler vasıtasıyla kamu tarafından gözetlenmesi ve vatandaşların kişisel verilerinin işlenmesi, kamunun akıllı şehirlerdeki rolünün tartışılmasını gerektirmektedir. Nitekim akıllı devlet kavramının yanı sıra akıllı şehirlerde diğer kamusal kurum ve kuruluşların etkisi vardır. Bu sebeple devlet, hükümet, belediye ve diğer kamu kurum ve kuruluşlarının gözetim teknolojilerini kullanarak akıllı şehirlerde yer alması akıllı şehir olma özelliği ile gözetim toplumu olma arasında bir denge kurmada bizlere yardımcı olacaktır.

Akıllı şehir dediğimizde vatandaşların/şehir sakinlerinin karar alma süreçlerine katılması, akıllı şehir uygulamalarına veri sağlayan öznesi olması, akıllı şehirlerde denetim yetkisine sahip olması ve akıllı şehrin ana amacı olarak vatandaşların hayatını kolaylaştırması hedeflenmektedir. Bu sebeple devletin akıllı şehirlerdeki rolü önem arz etmektedir. Bu hususta devlet; akıllı şehir uygulamaları hayata geçirilirken iyi bir strateji oluşturmalı ve akıllı politikaların savunucusu olmalı, devlet ve devletin ilgili kurumları yönetim anlayışı bakımından akıllı şehir fikrine açık olmalı, yasalar ve düzenlemeler ile yönlendirici ve düzenleyici bir yönetim anlayışı belirlemeli, enerji şebekeleri ve dijital altyapılar gibi akıllı şehirlerin olmazsa olmazı diyebileceğimiz noktalarda koruyucu bir yönetim oluşturmalı, akıllı şehirlerin sürekli gelişeceğini unutmadan yenilikçi çözümler üretebilmek amacıyla yenilikçi ve yatırımcı bir bakış açısına sahip olmalı, rekabeti ve yeni işletmeler için veriye erişimi kolaylaştırmak amacıyla kolaylaştırıcı ve hizmet sunucu yönetim felsefesini şiar edinmeli ve son olarak akıllı şehirlerdeki tüm tarafları bir araya getirebilmek ve çözüm üretebilmek amacıyla çözüm sağlayıcı yönetim anlayışını belirlemelidir.[111] Bir bakıma akıllı şehir sistemlerine geçiş için en önemli konulardan biri kamunun iyi bir liderlik rolü üstlenmesidir.

---

[111] Akkan, M. (2019) a.g.e. s.32

Akıllı şehir uygulamalarını hayata geçirirken altyapı temelli yenilikler oluşturulmalı ve bu durum da akıllı şehirlerin en büyük finansal kalemini oluşturmaktadır. Dolayısıyla şehir sakinlerinin, kaynakların akıllı şehir için büyük ölçekli ve yüksek maliyetli altyapı yatırımlarına ikna edebilmek gerekmektedir. Bu konuda uygulama ve uyumluluk önem teşkil etmektedir. Akıllı şehirlerde olması gereken yönetişim kavramını ortak karar alma süreçlerinde hayata geçirmek kamu tarafının yerine getirmesi gereken bir yükümlülüktür.

Benzer şekilde altyapı yatırımları hayata geçirilirken şehrin tarihi dokusu ve kültürel mirasına zarar verilmemelidir.[112] Akıllı şehirden bahsedildiğinde insanların zihnine gökdelenler ve bunlar arasında kısa mesafelerde seyahat edebilen hava araçları gelmemeli; bunun aksine mevcut şartları, şehrin tarihi, kültürü, ekonomik ve sosyal durumunu göz önünde bulundurarak şehir sakinlerinin hayatını teknolojik imkânları ve veriyi kullanarak kolaylaştıracak şartlar zihinlerde oturtulmalıdır. Nitekim şehir sakinlerinin kişisel verileri korunurken ve mahremiyeti sağlanırken şehrin kendisine ait mahrem dokusu zarar görmemelidir.

Akıllı şehirlerde büyük veri ve açık veri teknolojisi sayesinde verinin doğru bir şekilde toplanması ve yayınlanması ekonomi ile doğrudan ilişkilidir. Örnek vermek gerekirse Amerika'nın Illinois eyaletine bağlı Chicago şehrinde 2017 yılında meydana gelen ekonomik sıkıntı, hükümet ile birlikte hükümet dışı geliştiriciler, tasarımcılar ve tüm ilgili taraflarla birlikte hareket edilerek aşılmış olup Eyalette meydana gelen tüm gelişmeler veri akışı olarak paydaşlarla paylaşılmış ve ekonomik darboğaz kısmen de olsa aşılmıştır.[113] Bu konuda doğru akıllı şehir stratejisi olarak talebe bağlı bir akıllı şehir uygulamasının hayata geçirildiğinden söz edilebilecektir.

Bu sebeple, akıllı şehirlerin sadece teknolojik bir olgu olmanın yanı sıra sosyal, ekonomik ve politik bir anlam ifade etmektedir. Nitekim sadece vatandaşların katılımı, teknolojiyi üst düzeyde kullanmak, kirlilik ve verimlilik için değil, aynı zamanda akıllı

---

112 Aldemir, A. (2018). a.g.e. s.45

113 Addison, J. (2018). "Smart City Chicago". https://meetingoftheminds.org/smart-city-chicago-27152 (Erişim Tarihi: 23.10.2023)

şehirler, kamunun vatandaşlarına sağlayabileceği politika, iş fırsatları ve ihracat potansiyeli gibi imkânları olan bir pazar olarak da düşünülmelidir.

Akıllı şehirlerde finansman ayrıca önem verilmesi gereken bir konudur. Tarihsel olarak, özellikle Avrupa'da, durgunluk sonrası nakit sıkıntısı çeken kamu sektörünün ulusal veya belediye düzeyindeki mali desteği, ilgili radikal teknolojik uygulamaları finanse etmek için genellikle yeterli olmamıştır. Bunun yerine finansman, "bir kamu kurumu (federal, eyalet veya yerel) ile her sektörün belirli becerilerini ve varlıklarını kamu yararına kullanan bir özel sektör kuruluşu arasındaki anlaşmalar" olarak tanımlanabilecek Kamu-Özel Ortaklığı (PPP) yoluyla olma eğilimindedir. IBM tarafından 2014 Dünya Kupası ve 2016 Olimpiyat Oyunlarına hazırlık amacıyla inşa edilen Brezilya'nın Rio de Janeiro şehrindeki İstihbarat Operasyon Merkezi'dir. Rio dünyadaki en tehlikeli şehirlerden biri olarak kabul edilmesi sebebiyle Olimpiyatlar ve Dünya Kupası için beklenen ziyaretçi akışının bir şekilde güvence altına alınmasına ihtiyaç duyulmuştur. Şehrin her yerine yerleştirilen yüzlerce kamera ve sayısız sensörler yardımıyla sürekli merkezden izlenen şehirde canlı veri akışı sayesinde şehir operatörlerinin suça, kazalara, elektrik kesintilerine, sağanaklara, fırtınalara ve diğer olaylara anında müdahale etmesine olanak tanınmıştır.[114]

Ülkemizde bu amaçla oluşturulan 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planındaki aşağıda alıntılanan ifadeler bu konudaki yol haritasını çizmektedir:[115]

> "*Paydaş ihtiyaçlarına cevap veren, geçmiş dönem tecrübelerini önemseyerek mevcut durumu dikkate alan, uluslararası uygulamaları değerlendiren bütüncül bir strateji ile; ortak bir vizyon ve yol haritası hazırlamak, sistematik ve açık yönetişim ile izlemek ve değerlendirmek, değişen koşullara uyumu sağlamak ve şehirlerde ortak bir anlayış ile Akıllı Şehir olgunluğunu geliştirmek hedeflenmiştir. 2020-2023 Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı; merkezi yönetim kurum ve kuruluşları, yerel yönetimler, özel sektör, sivil toplum kuruluşları ve üniversitelerin dâhil olduğu ortak akıl ve bilimsel bakış açısı ile şekillenen, ulusal*

---

114 Edwards, L. (2016). a.g.e. s.6-7

115 Çevre ve Şehircilik Bakanlığı. (2019). "Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı". https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf s.6

katmanda hazırlanan Türkiye'nin ilk, dünyanın dördüncü Akıllı Şehir stratejisi ve eylem planıdır."

Eylem planından da anlaşılacağı üzere devletin başı çektiği söz konusu girişimde aynı zamanda yerel yönetimler, özel sektör, sivil toplum kuruluşları ve üniversitelerin dâhil olduğu bir ortak akıl ile süreç yürütülmektedir.

Bahse konu Eylem Planı kapsamında "*Akıllı Şehir Kapsamında Oluşturulan ve Kullanılan Kişisel Verinin Korunumu Sağlanacaktır.*" başlığı altında yapılacaklar ifade edilmiştir. Buna göre "akıllı şehircilik hizmetlerinde kullanıcı güvenliğinin sağlanması", "akıllı şehircilik hizmetlerinde kullanıcı güveni ile kullanıcı tarafından kabul görme düzeyinin artırılması", "akıllı şehircilik hizmetlerine katılım ile hizmetlerin işlerliğinin artırılması" ve "kişisel verinin millî bir değer olarak korunmasının sağlanması" hususları eylem planının ilgili başlığından beklenen faydalar arasında sayılmıştır.[116] Bunun yanı sıra, veri kirliliğinin ve işlevsiz veri yığınlarının önüne geçilebilmesi için;[117]

- *Akıllı şehir kapsamında oluşturulan ve kullanılan kişisel verinin gizlilik ve mahremiyet açısından kritiklik seviyesinin belirlenmesi ihtiyacının bulunduğu;*
- *Verinin daha güvenli bir ortamda korunabilmesi için kritiklik seviyeleri dikkate alınarak gerekli kontrol noktaları ve ilişkili önlemlerin hayata geçirilmesi ihtiyacının bulunduğu;*
- *Kullanıcıların akıllı şehir uygulamalarına güveninin sağlanabilmesi için, kimlik ve kişisel veri güvenliğinin sağlanması için kimlik doğrulama ve süreç adımlarının güvenliğinin artırılması ihtiyacının bulunduğu;*
- *Akıllı şehir uygulamalarının ulusal ve uluslararası düzeyde kişisel verinin korunmasına yönelik mevzuata uyumlu bir yapıda yapılması ve işletilmesinin, bu verinin meşru bir zeminde tutulması ve işletilmesini sağlayacağı,*

ifade edilmiştir.

---

116 Çevre ve Şehircilik Bakanlığı. (2019). a.g.e. s.630
117 Çevre ve Şehircilik Bakanlığı. (2019). a.g.e. s.632-635

Dolayısıyla ülkemizde kişisel verinin gizlilik ve mahremiyet açısından kritiklik seviyesinin akıllı şehirlerde ne olduğu, söz konusu seviyelere ilişkin ne gibi önlemler alınacağı, kişisel veri güvenliği ve mahremiyet açısından ne gibi teknik önlemlerin alınacağı ve tüm bu hususların hukuki boyutunun ve mevzuata uyumunun nasıl olacağı hususunda bir başlangıç olması açısından çok olumlu gelişmelerdir. Veri güvenliğinin sağlanması bakımından temel ilkelere uyulması ve şeffaflığın ortaya çıkarılması önem arz etmektedir.[118]

Günümüzde birçok kent, akıllı şehir olma yolunda ciddi adımlar atmasına rağmen bazı kentlerde ise birkaç teknolojik imkânın kullanılmasıyla akıllı şehir ilan edilen şehirlerimiz mevcuttur. Akıllı şehirler birçok farklı alanda teknolojik ve sosyal entegrasyon sisteminin birbiriyle etkileşim halinde kullanılması sonucu ortaya çıkmaktadır. Buna göre, söz konusu teknolojilerden bir veya birkaçını şehrin trafik sistemlerine veya ulaşım altyapısına yerleştirilmesi sonucu o şehirde akıllı şehirden bahsedilemeyecektir. Zira akıllı şehirden bahsedebilmek için; ulaşımdan sürdürülebilirliğe, şehrin atık sisteminden ekonomik ve finansal yapısına, hükümet ve belediye uygulamalarından karar alma süreçlerine katılmaya kadar birbirini etkileyen birçok etkenin bir araya gelmesi gerekmektedir.[119] Şehir sakinlerinin ve vatandaşların hayatlarını kolaylaştırmayan ve çözüm üretmeyen uygulamaların akıllı şehir uygulaması olarak değerlendirilmemesi gerekmektedir. Bu hususta dikkat edilmesi gereken nokta ise akıllı şehir uygulamalarının ihtiyaca göre oluşturulması, teknolojik kaynaklardan yararlanılması, şehir sakinlerinin sürece dahil edilmesi ve birçok farklı alanda teknolojik ve sosyal entegrasyon sisteminin birbiriyle etkileşim halinde kullanılması gerekmektedir.

Akıllı şehirlerin hayata geçirilebilmesi için kullanılan yüksek miktarda verinin tek elden yönetilmesi gereklilik olduğu kadar çeşitli zorlukları da beraberinde getirecektir. Bu amaçla kamu tarafında ve genellikle merkezi hükümetler marifetiyle tek elden yönetim için uygun birimlerin oluşturulması, verilerin tek elde toplanması, işlenmesi,

---

118 Nur, P., Canyaş, O. (2023). "Bir Norm Çatışması Örneği: Vergi Usul Kanunu ve Kişisel Verilerin Korunması Kanunu". *Türkiye Adalet Akademisi Dergisi*, Sayı:54. s.119

119 Townsend, A. (2013) a.g.e. s.26

aktarılması, depolanması, analiz edilmesi ve söz konusu veriler için uygun güvenlik ve mahremiyet önlemlerinin alınması gerekmektedir. Merkezi hükümetlerin yanı sıra yerel yönetimlerin, çeşitli kamu kurum ve kuruluşları ile birlikte kamu niteliğini haiz meslek kuruluşlarının da verileri toplama, işleme, aktarma, analiz etme ve depolama durumlarının yanı sıra uygun güvenlik ve mahremiyet önlemleri alma yükümlülükleri mevcuttur.

Merkezi hükümet ile yerel yönetimler arasında, akıllı şehir uygulamalarına geçiş ve uygulama esnasında, işbirliğinin sağlanamaması büyük bir problem meydana getirecektir.[120] Merkezi yönetimin yerel yönetimin ihtiyaçlarını görmezden gelerek yanlış politika üretmesi veya veri paylaşımına engel olması; benzer şekilde akıllı şehir uygulamaları için birçok alanda yenilik yapılması konusunda merkezi hükümetle farklı anlayışlara sahip olunması, sürece zarar vermesinin yanı sıra ciddi bir emek ve kaynak israfına da sebebiyet verecektir. Özellikle merkezi hükümet ile yerel yönetimler arasında veri paylaşımının sağlanması, akıllı şehir uygulamalarının ortak politika oluşturulması bakımından en önemli başlangıcı olduğu söylenebilir.

Akıllı şehirlerde en önemli aşamalardan biri de devlet eliyle oluşturulan yasal çerçevedir. Mevzuat, olası riskleri öngörerek çözüm önerilerini de birlikte sunmalıdır. Bunun yanı sıra akıllı şehirlerde sürekli kendini geliştirecek olan teknolojik yeniliklere ilişkin telif hakları sorununa da hakları koruyucu bir mevzuat bakış açısıyla yaklaşmalıdır.[121] Akıllı şehirlerde kişisel verilerin korunmasına ve mahremiyete ilişkin oluşturulacak mevzuatın sadece kanundan ibaret olmaması, bunun yanı sıra akıllı şehirlerde mahremiyet ve kişisel verilere ilişkin çeşitli yönetmeliklerin de oluşturulması gerekmektedir. Öyle ki akıllı şehir uygulamaları birçok sektörü birbiriyle ilişkilendirmesi dolayısıyla sektör bazında ilgili kamu kurumlarının akıllı şehirlerin kendi faaliyet alanıyla ilgili kısımlarında alt mevzuatlar oluşturması gerekmektedir.

---

120 Nam, T. Pardo, T. A. (2011). "Conceptualizing Smart City with Dimensions of Technology, People, and Institutions". Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times. s.288

121 Aldemir, A. (2018) a.g.e. s.39

Kamunun akıllı şehirlerde yerine getireceği hak ve yükümlülüklerinin tam anlamıyla sağlanabilmesi amacıyla söz konusu uygulamaların kamu-özel işbirliğinde hayata geçirilmesi gerektiği düşünülmektedir. Nitekim kamu otoritelerinin teknolojiyi ve veriyi kullanma yeteneğinin şirketler kadar hızlı ve etkin olmadığı gerçeği mevcuttur. Bu sebeple uzun vadede akıllı şehirlerde kamu, rolünü özel sektör ile birlikte yürütmektedir.

Akıllı şehirlerde kamunun oynaması gereken liderlik rolünün yanı sıra insan davranışlarının, cadde, sokak ve meydanların, çeşitli kamusal alanların kamera ve sensörler vasıtasıyla gözetlenmesiyle oluşturulmak istenilen kamusal gözetimden bahsedilmesi gerekmektedir. Öyle ki akıllı şehirlerin insan hayatını kolaylaştırma amacı taşıdığı kadar kamusal gözetimin insan hayatına tehlike oluşturabilecek tarafları mevcuttur. Sürekli izlendiğini bilen ve yaptığı her hareketin kayıt altına alınacağının farkında olan insanların davranışları bir süre sonra huzursuzluğa dönüşebilecektir. Hatta hükümetler bu yolla toplumda baskı altında tutmak istediği kişi ve grupları (dini, milli veya davranışsal farklılıklarından dolayı olabilir) bu yolla baskı altında tutabilecektir.

Buna karşılık akıllı şehirlerde suçun önlenmesi, trafik sıkışıklığının giderilmesi, vb. amacıyla kamusal gözetimin çeşitli faydalarının bulunduğu inkar edilemez. Örnek vermek gerekirse bir ada ülkesi ve şehir devleti olan Singapur'da[122] 2014 yılında başlatılan bir uygulamada, temizlikten trafik durumuna kadar her şeyi izlemek için kurulan kamera ve sensörler vasıtasıyla insanların yetkisiz alanlarda sigara içtiği, yüksek binalardan çöp attığı tespit edilerek "Sanal Singapur" adındaki çevrimiçi uygulamaya veriler aktarılmakta ve hükümet tarafından ülkenin anlık olarak takip edilmesi sağlanmaktadır.[123]

Bu yüzden kamusal gözetiminin kişisel verilerin korunması boyutu akıllı şehirlerde en önem verilmesi gereken konulardan biri olmalıdır. Özellikle bu konuda kişisel verilerin korunması ve mahremiyet ile akıllı şehirlerde uygulanacak gözetim arasında bir denge

---

122 https://tr.wikipedia.org/wiki/Singapur (Erişim Tarihi: 25.10.2023)
123 Aldemir, A. (2018). a.g.e. s.66

sağlanması gerektiği önümüzdeki dönemlerde sıkça karşılaşacağımız sorunlardan birini oluşturmaktadır.

Tarihsel olarak, bedenlerimizle başlayan, evlerimizi kucaklayan ve ardından dış dünyayla olan özel iletişimlere kadar uzanan bir mahremiyet alanımızı koruma eğilimindeyiz. Bu, aynı zamanda Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) 8. maddesinin mezkur "özel hayatımıza, aile hayatımıza, evimize ve yazışmalarımıza" saygı gösterilmesini talep ettiği hususdur. Buna karşılık, şehirler özü itibariyle mahremiyet beklentilerinin en az olduğu kamusal alanlar olarak görülmektedir. Buna rağmen bilgi toplumunda çeşitli amaçlarla kontrol edilen pek çok sanal alan, özellikle çevrimiçi uygulamalar ve arama motorları sayesinde; ifade, bilgi edinme veya toplantı haklarının geleneksel olarak kullanıldığı şehir meydanları veya halk kütüphaneleri benzeri yerler, yarı kamusal bir karakter kazanmıştır. Akıllı şehirlerde ise tam tersi bir paradigma işlemekte ve tarihsel olarak kamusal alan olan şehir meydanları, yollar, toplu taşıma araçları, sağlık sistemleri artık özel şirketler tarafından işletilmekte ya da en azından özel şirketler tarafından verileri işlenen sensörler ve kameralarla dolu olmaktadır. Dolayısıyla işlenen söz konusu veriler, özel veri tabanlarında tutulmaktadır. Bu yüzden şehirlerin bu kısımları artık "özel-kamusal-yerler" olarak adlandırılabilecek yerler haline gelmektedir.[124]

Bir zamanlar evlerde güvenli bir şekilde saklanan kişisel verilerin artık ev dışında, akıllı telefonlarda, diğer taşınabilir cihazlarda, web sunucularında veya bulut sistemlerinde tutulduğu yadsınamaz bir gerçektir. Dahası, mahrem alan içerisinde güvende olabilecek kişisel veriler artık genellikle dünya için şeffaftır. Hatta, akıllı sayaçlarla donatılmış evler, enerji tüketiminin ve elektrikli uygulamaların ince ayrıntılarını ortaya çıkarabilmekte ve bunların doluluğu ve faaliyetleri dışarıdan dakikalarca gözlemlenebilmektedir. Isı sensörleri, mikrofonlar ve küçük gözetleme hava araçları da evdeki mahremiyet duvarını kolaylıkla aşabilmektedir. Bir zamanlar insanların mahremiyetini korumak için muhtemelen yasal korumaya ihtiyaç duymadıkları kamusal alanlarda bile, akıllı CCTV sistemleri, GPS, Wi-Fi ağları ve yüz tanıma yazılımları

---

[124] Cho, K., Kim, C. (2017). "Design For Privacy In Public Space" 21st International Conference On Engineering Design, s.246

sebebiyle kamusal alanda gizliliğin neredeyse sona erdiği anlamına gelmekte ve kişisel verilerin korunması zorlaşmaktadır. Kişisel verilerinize akıllı bir şehrin kamuya açık alanlarında kolayca erişilebiliyorsa, o zaman özel bir konutta olduğu gibi aynı mahremiyet korumalarının da kamusal alanda geçerli olması tartışmalı bir husus halini almaktadır. Akıllı bir araçta veya akıllı bağlantılı bir toplu taşıma sisteminde seyahat ediyorsanız, bunlar yaşadığınız evle aynı mahremiyetin parçası olacağından söz edilmese de eskisinden daha fazla bir korumaya ihtiyaç duyulduğu su götürmez bir gerçektir. Bu gibi soruların cevaplandırılması, akıllı şehirlerde kişisel veri mahremiyetinin nasıl sağlanacağı konusunda oldukça aydınlatıcı ve iyi bir başlangıç olacaktır.

Akıllı şehirlerin kamuya açıklığında önemli bir nokta, akıllı bir şehirde yaşayanlarla ilgili veri ifşa edilmesinin kaçınılmaz olmasıdır. Çevrimiçi gezinti yapan bir vatandaşın; sosyal ağını, bir alışveriş sitesini veya bir arama motorunu seçerken akıllı şehirlerin hükümet tarafından işletilen sensörler ve gözetim teknolojilerine karşı çok az alternatifi olduğu değerlendirilmektedir. Dolayısıyla söz konusu husus, bir hükümete fazladan ve orantısız güç katabilmektedir. Bu konuda daha muhtemel tehlike ise bu tür kişisel verilerin Kamu özel ortaklığı (PPP) yoluyla özel şirketlerin eline geçmesi ve oradan da açık piyasaya düşmesi ve sigortacılara, işverenlere veya gayrimeşru yapılara ulaşması durumunda olumsuz etkiler oluşturmasıdır. Bu tür durumlarda 6698 sayılı Kanunun 18'inci maddesinde, veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler hakkında 15.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezası ile cezalandırılacağı, söz konusu kabahatin kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar tarafından gerçekleştirildiği durumlarda ise haklarında disiplin hükümlerine göre işlem yapılarak ve sonucunun Kurula bildirileceğine hükmedilmiştir.[125] Bunun yanı sıra 5237 sayılı Türk Ceza Kanununun 135 ve 140'ıncı maddeleri arasında kişisel verilerin

[125] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016.

kaydedilmesi, hukuka aykırı olarak verme ve ele geçirilmesi, verileri yok etmemeye ilişkin cezalara hükmedilmiştir.[126]

Açık sosyal medya istihbaratı ve veri madenciliği, herhangi bir mahremiyet unsurundan yoksun olarak kabul edilmekte ve dolayısıyla izlenebilmesi, işlenmesi ve veri madenciliği yapılabilmesi için genel olarak herhangi bir mahkeme emrine veya iznine ihtiyaç duyulmamaktadır. Bu tür bir izleme, profil çıkarmaya katkıda bulunabilir ve bu da bireyler üzerinde önemli bir etkiye sahip olabilmektedir. Örnek vermek gerekirse, İngiliz Yüksek Mahkemesi, isyancı olarak yasayı çiğnediği sırada CCTV kamerası sayesinde fotoğrafı çekilen bir çocuğun, polisin bu görüntüyü kamuya yaymasını engelleme hakkına sahip olmadığına karar vermiştir.[127] Buna karşılık Avrupa ve Amerika'da kişisel veri koruma mevzuatları ise, verilerin tamamen yurtiçinde işlenmesine sağladığı muafiyet dışında herhangi bir önemli özel/kamu ayrımı yapmamaktadır. Kategori ayrımları, işlemenin nerede gerçekleştiğine değil, kişisel verilerin kişiyi tanımlı veya tanımlanabilir kılan[128] bir şekilde işlenip işlenmediğine ilişkindir. Özellikle evlerimizin içinde bulunan nesnelerin birbirine veri akışı sağlaması, akıllı şehirlerde kişisel verinin kim tarafından ele geçirildiğini bulmanın zor olması dolayısıyla kamusal alan ve özel alan ayrımının tekrar yorumlanması gerektiğini bizlere göstermektedir.

Tüm bu hususların yanı sıra 6698 sayılı Kanunun 28'inci maddesinde kişisel verilerin işlenmesine ilişkin istisna hükümlere yer verilmiştir. Mezkur maddede kişisel verilerin, gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi; kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi; kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi; kişisel verilerin millî savunmayı, millî güvenliği, kamu

---

126 5237 sayılı Türk Ceza Kanunu

127 Edwards, L. (2016). a.g.e. s.15

128 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi; kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi istisna kapsamında tutulmuştur.[129]

Dolayısıyla akıllı şehirlerde işlenmesi öngörülen birçok faaliyet Kanun kapsamında istisna sayılarak akıllı şehirlerdeki kişisel veri işlemeye ilişkin denetim yetkisi sınırlandırılmıştır. Kamu marifetiyle işlenen kişisel verilerde istisna kapsamının geniş tutulması, normal şartlarda bir sorun teşkil etmezken akıllı şehirlerde işlenen kişisel verilere ilişkin veri sorumlusu kamu tüzel kişisinin, hesap verebilirliğini azaltacak bir durumu meydana getirmektedir. Buna karşılık istisnaların tahdidi olarak sayılması ise sınırsız veri işlemenin önüne geçebilecek olumlu bir işareti oluşturmaktadır.

2.5. AKILLI ŞEHİRLERDE ÖZEL SEKTÖRÜN ELİNDEKİ KİŞİSEL VERİLER

Bir şehrin nasıl akıllı şehir haline geleceğine dair uzun vadeli ve dönüştürücü planlara sahip olması gerekmektedir. Aynı zamanda bazı özel firmalarla akıllı şehirlerde bazı dijital hizmetler geliştirmek için yapılan sözleşmelerden dolayı şehrin belirli yerlerine sensörler ve kameralar yerleştirmek için girişimlerde bulunulmaktadır. Örneğin e-scooter'ların ortaya çıkması ve neredeyse her sokak başında bekleyen scooter'ların uygulama ile kullanılması akıllı şehirler için önemli bir gelişmedir. Bu durum bir akıllı şehir girişimi yapan şirket örneği olabilir ve e-scooter'lar, kullanıma bağlı olarak büyük miktarda veri üretmiştir. Akıllı sokak lambaları gibi sürekli trafikte veri akışına izin veren uygulamalar sayesinde işe gidiş gelişinize dair seyahat süreleriyle ilgili kesin bilgilerle planlamanıza olanak sağlamaktadır. Bugün belediyeler tarafından oluşturulan otobüsün nerede olduğu ve ne zaman geleceği gibi uygulamaların yaygın olduğu aşikardır.

---

[129] 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

Bu konuda ülkemizde ortaya çıkan güncel bir tartışma konusu olarak İstanbul Kart uygulamasına değinmek faydalı olacaktır. İstanbul Büyükşehir Belediyesi tarafından hayata geçirilen İstanbul Kart uygulamasında, 2022 yılı sonuna kadar tüm kartların kişiselleştirilmesini zorunlu kılınması, kişisel verilerin güvenliğine ve mahremiyete ilişkin ciddi endişeleri de beraberinde getirmiştir.[130] İstanbul'da yaşayan vatandaşların konum verilerinin kişiselleştirilmiş kart uygulamasıyla anlık takip edilebilmesi, anonim bir şekilde seyahat etme hürriyetine zarar verecektir. Bu konuda Kanunda belirtilen şartlardan yalnızca açık rıza alınması şartının uygulanması veri sorumlusu olarak İstanbul Büyükşehir Belediyesi'ni meşru bir zemine oturtabilecektir. Söz konusu uygulamaya ilişkin öğrenci, 65 yaş üstü veya diğer özel durumlara sahip olan vatandaşların kişisel verilerinin işlenmesinin Kanunun 5'inci maddesinde sayılan işleme şartlarından "*Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.*" Hükmüne uygun olabileceği, bunun dışında tüm toplu taşıma kartı kullanan İstanbullulardan açık rıza alınması gerektiği değerlendirilmektedir.

Bu konuda değinilmesi gereken bir başka önemli husus ise 5393 sayılı Belediye Kanununa 15/2/2018 tarihinde eklenen Ek Madde 3'tür. Söz konusu ek maddede belirtilen "… *e-Belediye bilgi sistemini kurmaya, işletmeye, veri saklama, veri iletimi ve veri paylaşımı ile ilgili politikaları tespit etmeye, çalışma usul ve esaslarını belirlemeye ve bu sistem ile ilgili merkezî bir hizmet standardizasyonu oluşturmaya İçişleri ile Çevre ve Şehircilik bakanlıkları müştereken yetkilidir.*"[131] ifadesinden anlaşılacağı üzere akıllı şehirlerde hayata geçirilecek olan e-belediye uygulamalarına ilişkin politika belirlenmesinde, usul ve esasların belirlenmesinde ve standartların oluşturulmasında belediyenin değil merkezi hükümetin yetkili olduğuna hükmedilmiştir. Dolayısıyla söz konusu hüküm doğrultusunda ülkemizde akıllı şehir uygulamalarının üniter devlet yapısına herhangi bir zarar vermeden hayata geçirilmesi gerektiği ile birlikte kişisel verilerin işlenmesi, saklanması, aktarılması ve paylaşılmasına ilişkin merkezi hükümetin yerel yönetimlere yol haritası çizeceği anlaşılmaktadır.

---

130 Kul, H. H., Melikoğlu, M. Y. "İBB'nin İstanbulkart'ın kişiselleştirilmesi kararı seyahat özgürlüğünün kısıtlanması olarak değerlendiriliyor". (2022) https://www.aa.com.tr/tr/gundem/ibbnin-istanbulkartin-kisisellestirilmesi-karari-seyahat-ozgurlugunun-kisitlanmasi-olarak-degerlendiriliyor/2722479 (Erişim Tarihi: 10.01.2024)

131 5393 sayılı Belediye Kanunu (https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5393.pdf)

Buna karşılık 5216 sayılı Büyükşehir Belediyesi Kanununun 8'inci maddesinde belirtilen "*... Bu amaçla, kamu kurum ve kuruluşları ile özel kuruluşlar alt yapı koordinasyon merkezinin isteyeceği coğrafi bilgi sistemleri dâhil her türlü bilgi ve belgeyi vermek zorundadırlar. ...*"[132] ifadesinden ise büyükşehir belediyelerinin akıllı şehirlerde yapacağı alt yapı yatırımlarında kişisel verilerin paylaşılmasına ve aktarılmasına ilişkin hukuki bir güvence elde ettiği belirtmek gerekmektedir. Bu kapsamda akıllı şehirler uygulamalarının merkezi hükümet ile yerel yönetimlerin bir işbirliği halinde hayata geçirilmesi önem arz edecektir.

Günümüz teknolojisinde şehirlerde bilgi iletişim araçlarının yaygınlaşmasıyla birlikte bilgiye erişim kolaylaşmış ve buna bağlı olarak rekabet olanakları gelişmiştir. Hiç şüphesiz ki şehirlerde dijital altyapı yazılımlarının kullanılması, büyük teknoloji şirketleri eliyle gerçekleşmektedir. Günümüzde kişisel veriler, bireyin devlet karşısında korunması kadar şirketlerin manipülasyonu karşısında da korunmalıdır.[133] Buna bağlı olarak akıllı şehirlerde şirketlerin elindeki verilerle şehir sakinlerinin ve idaresinin şirketlere bağımlılığı durumunu ortaya çıkarmaktadır.[134] Hatta açık verilerle birlikte özel sektör eliyle sağlanan veriler bir araya geldiğinde akıllı şehirlerde bir "Şirketlerin Beylik Dönemi" oluşacağı da söylenebilecektir.

Veri alışverişi için evrensel, açık veya özel standartların bulunmaması, verileri özel şirketlere yönlendiren bir diğer önemli sorundur. AB, akıllı şehirlerde özellikle enerji ve genel olarak IoT sistemleri gibi alanlarda faaliyet gösteren özel teknoloji tedarikçileri için birlikte çalışma protokolleri oluşturma girişimlerini finanse ederek bu durumu hafifletmeye çalışmaktadır. Aksi takdirde akıllı şehir, tekelci bir teknoloji veya telekomünikasyon sağlayıcısının özel veri derebeyliğine dönüşebilecektir. Avrupa Birliği, bu yüzden "büyük verinin" kime ait olduğu ve nasıl kontrol edileceğine ilişkin süregelen endişelere ve belirsizliklere bir çözüm bulmaya çalışmaktadır. Özellikle bu konunun hem şehirler hem de vatandaşlar için sorunlu olduğu konusunda tarafların duyarlı hale gelmesini gerektirmektedir. Sonuç olarak, toplanılan verilerle ne yapıldığı

---

132 5216 sayılı Büyükşehir Belediyesi Kanunu

133 Aksoy H.C., (2022). a.g.e. *Kişisel Verileri Koruma Dergisi*. 4(2), s.70.

134 Şengün, H., Koçhan, A., Meydan, S. (2019) a.g.e. s. 11

ve bu verilerin sahibinin kim olduğu akıllı şehirlerin karşılaştığı temel sorular olabilmektedir.[135]

Benzer şekilde söz konusu şirketlerin elindeki verilerin, özellikle kişisel verilerin korunması amacıyla yine aynı şekilde nitelikli teknoloji şirketlerinin ürünlerine ihtiyaç duyulmaktadır. Bu durumda akıllı şehirlerin özel sektöre bağımlılığını artırması söz konusu olmaktadır. Bu durumda ülkelerin teknolojiyi üreten ve aynı zamanda koruyabilen şirketlere sahip olması büyük bir avantaj oluşturacaktır.

Günümüz dünyasında savaşlar ve siyasi mücadeleler; silahların, uçakların ve diğer güç araçlarının varlığının yanı sıra verinin elde edilmesi ve kullanılması ile de gerçekleşmektedir. Hatta veriler kullanılarak bazı uluslar baskı altında tutulmakta ve gözetim teknolojileri marifetiyle egemen ülkenin çıkarlarına muhalefet oluşturacak en küçük faaliyetler dahi önceden fark edilerek ona ilişkin politikalar geliştirilmektedir. Bu sebeple teknolojiyi kullanan uluslara nispeten teknolojiyi kendisi üreten ve yukarıda bahsedildiği gibi kendisi koruyabilen ülkelerin diğer ülkelere nitelikli bir üstünlüğü söz konusu olmaktadır. Bu noktada dikkat edilmesi gereken husus ise söz konusu güç mücadelesinde şirketlerin büyük finansman sağlayarak sürece dahil olmasıdır.

Uluslararası ya da çok uluslu şirketler açısından akıllı şehirler geleceğin önemli sektörlerinden biri olarak tanımlanmaktadır. "*Bu kapsamda Siemens, BMW, Mercedes Benz, IBM, Phillips, General Electric ve Veolia gibi şirketler kentsel kaliteyi ileri boyutlara taşıyabilmek adına çalışmalar yapmaktadır.*"[136] Bu şirketler verinin ve bilgi iletişim teknolojilerinin kendilerine sağladığı pazarlama gücü sayesinde ürün ve hizmetlerini pazarlayabilmek için tüketicilere daha kolay ulaşabilme imkânı elde etmektedir. Hiç şüphesiz ki söz konusu imkânın altında kişisel veri yatmaktadır. Öyle ki otonom araçlarla piyasaya çıkan "Tesla" şirketinin veriyi kullanma gücü sayesinde piyasa değerini, kısa zaman zarfında on yıllardır otomotiv sektöründe faaliyet gösteren

---

135 Edwards, L. (2016). A.g.e. s.10
136 Akkan, M. (2019) a.g.e. s.27

dünya devi şirketlerin piyasa değerinin üzerine çıkarabilmesinin altında yatan sebep veriyi kullanabilme gücüdür.

Bunun yanı sıra büyük şirketlerin akıllı şehir uygulamalarında önemli rol oynamaları, söz konusu şirketleri akıllı şehir yönlendiricileri konumuna eriştirmektedir. Normal şartlarda hükümet ve şehrin yerel yöneticileri tarafından kontrol edilmesi gereken akıllı şehir sistemlerinin, özel sektöre devredilmesi sonucunda devletin tasarrufunda bulunan vatandaşlarına ait kişisel verilerin, veriyi kullanarak karına kar katan özel şirketlerin eline geçmektedir. Bu durumda ise vatandaşlara ait kişisel verilere erişim imkânı bulan şirketlerin belirli bir süre sonra merkezi ve yerel hükümetlerden daha fazla güce ve finansal kara erişim imkânı bulacağını söylemek yanlış olmayacaktır.

Akıllı şehir sakinleri süreç içerisinde hayatı kolaylaştırma amacı taşıyan akıllı şehirde meydana gelen iyileşmelere şahit oldukça ve sürece katılı arttıkça artık akıllı hizmetlerin vatandaşlar tarafından vazgeçilmesi mümkün olmayacaktır. Örnek vermek gerekirse akıllı telefonlar hayatımıza girmeden önce akıllı telefonun varlığından bile haberdar değilken hayatımıza girdikten sonra ve özellikle sağladığı bazı hizmetlerle hayatımızı kolaylaştırması sonrasında insanlar için vazgeçilemez bir hal almaya başlamıştır. Benzer bir durumun önümüzdeki yirmi yıl içerisinde otonom araçlarda ortaya çıkacağını tahmin etmek zor olmayacaktır. Akıllı şehirler sakinlerine de sağlanan hizmetlerin kalitesi ve boyutu toplumun geneline yayıldıkça söz konusu hizmetleri aksatmanın veya hizmetlerden vazgeçmenin mümkün olmayacağını söylemek gerekmektedir. Bu durum ise öncesinde şirketler marifetiyle ve kamu adına işlenen, aktarılan, saklanan ve imha edilen kişisel veriler sayesinde özel sektör ve hükümet arasında güç makasının açılmasına sebep olacaktır.[137]

Akıllı şehirlerde demokratik hükümetlerin kamusal alanları özelleştirmesi ile birlikte merkezi hükümetler adına veri işleyen şirketler (veri toplayan ve yönetenler), fiili olarak kamusal alanların valileri haline gelmektedirler. Bir kamu hizmeti sağlayıcısının belirli erişilebilirlik standartlarını karşılama yükümlülükleri olabilmektedir. Buna rağmen

---

[137] Cho, K., Kim, C. (2017). a.g.e. 21st International Conference On Engineering Design, s.270

akıllı şehir uygulamasında dijital hizmetler sunan özel aktörler için bu durum her zaman geçerli değildir. Özel aktörlerin bu konuda daha fazla ileriye gittiği yerlerde sistemde bazı boşluklar ortaya çıkmaktadır. Devletten daha çok veri toplayan bu özel aktörler ile birlikte vatandaşların artık şehrin dijital yüzü olan özel aktörler aracılığıyla hükümetleriyle etkileşime girdiği güçlü bir üçlü mekanizma sorunu ortaya çıkmaktadır. Uygulamadaki hizmet ile alakalı "kime şikayet edeceğim" ve "kim geri bildirimde bulunacak" gibi pratik soruların gündeme geldiği durumlarla karşılaşmak şimdiden öngörülebilmektedir. Bunun yanı sıra vatandaşların akıllı şehirlerin merkezinde yer alıyor olması da kişisel veri mahremiyetine olan ihtiyacı daha fazla ortaya çıkarmaktadır.

İnsanlar hakkındaki kişisel veriler, daha iyi kararlar almak ve kullanıcıya kişiselleştirilmiş bir deneyim sunmak için toplanır, analiz edilir ve saklanır. Şirketler bu kişisel verileri daha iyi hizmetler sunmak ve hedef ürünleri hedef tüketicilere pazarlamak için kullanır. Bilgi gizliliği, iletişim gizliliği ve veri gizliliğinin birleşimidir.[138] Bilgi gizliliği, bu iletişimler diğer kişiler veya kuruluşlar tarafından izlenmeden başkalarıyla iletişim kurma yeteneğidir. Veri gizliliği ise bu veriler ve bunların kullanımı üzerinde önemli ölçüde kontrol sahibi olmak için diğer kişi ve kuruluşlar tarafından kişisel verilere erişimi sınırlama yeteneğidir.[139] Teknolojiyi günlük faaliyetlerimizde kullanırken ad, soyad, telefon numarası, elektronik posta gibi kişisel verilerimizi kamu kurum ve kuruluşları ile şirketlere ve diğer tüzel ve gerçek kişilere teslim etmekteyiz. Verilerimizi teslim ettiğimiz bu yapılar ise ürün ve hizmetlerini pazarlamak için büyük miktarda veriyi toplamaktadır. İnternet ortamında sadece gezinsek bile, mahremiyetimizin ihlal edilmesi riski her zaman mevcuttur. Mesela çeşitli işlemler sırasında çevrimiçi toplanan kişisel verilerin üçüncü taraflara hukuka aykırı bir şekilde aktarılma riski, rahat bir şekilde internette gezinirken arka planda hep mevcuttur. Kişisel olabilecek büyük miktarda verinin toplanması, toplanan bu verilerin

---

138 Edmondson, V., Cerny, M., Lim, M., Gledson, B., Lockley, S., Woodward, J. (2018). "A smart sewer asset information model to enable an 'Internet of Things' for operational wastewater management". Autonomous Construct. s.163

139 Edmondson, V., Cerny, M., Lim, M., Gledson, B., Lockley, S., Woodward, J. (2018). a.g.e. s.200

işlenmesi, iletilmesi, saklanma süresi ve elde edilen verilerin türleri, mahremiyet açısından önemli faktörlerdir.[140]

Kabul edilmesi gerekir ki kişisel verileri elde edebilen ve onu koruyabilen şirketler, genellikle çok uluslu ve merkezi gelişmiş ülkelerde faaliyet gösteren büyük şirketler olmaktadır. Bu anlamda az gelişmiş ve gelişmekte olan ülkelerin akıllı şehir bakımından veya diğer teknolojik entegrasyon faaliyetleri bakımından merkezi (diğer bir ifadeyle ana serverları) gelişmiş ülkelerde bulunan çok uluslu şirketlerin elde ettiği verilere ve söz konusu verilerin korunmasına ihtiyacı da ortaya çıkmaktadır.

Özel sektörün elindeki kişisel verilerin ülke içerisinde kalması ve korunmasının da yine aynı ülkede yapılabilmesi için o ülkede faaliyet gösteren veriye dayalı teknoloji şirketlerinin güçlü ve rekabet edebilir durumda olmalıdır. Özellikle şirketlerin ana hizmet sağlayıcılarının ülke içerisinde bulunması kişisel verilerin yurtdışına aktarılmaması amacıyla önem arz etmektedir. Bu konuda 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 9'uncu maddesinde kişisel verilerin yurtdışına aktarılmasına ilişkin hükümleri mevcuttur. Söz konusu maddenin (1) numaralı fıkrası, "*Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz*." hükmünü amir olup mezkur maddenin (2) numaralı fıkrasında kişisel verilerin; *"... kişisel verinin aktarılacağı yabancı ülkede yeterli korumanın bulunması ya da yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki sorumluların yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabileceği*" hükme bağlanmıştır.[141] Dolayısıyla ülkemizde kişisel verilerin, ilgili kişilerin açık rızasının varlığı olmadan, yurtdışına aktarılabilmesi için yeterli korumanın bulunduğu ülke olması şartının varlığı, söz konusu şart sağlanamıyorsa ise Kişisel Verileri Koruma Kurulu izniyle ülkemizdeki ve muhatap ülkedeki veri sorumlularının yazılı taahhüt vermesi gerekmektedir.

---

140 Kasar, S., Meghana, K. (2021). a.g.e. s.31

141 6698 sayılı Kişisel Verilerin Koruması Kanunu, T.C. Resmi Gazete, 12301, 7 Nisan 2016. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

2.6. AKILLI ŞEHİRLERDE MAHREMİYET NASIL SAĞLANIR?

Akıllı şehirlerin mahremiyeti öncelikle kullanıcıların yani vatandaşların bilinç düzeylerinin artırılması yoluyla sağlanabilir. Bunu takip eden hususlar ise alınması gereken diğer idari ve teknik önlemler olarak sıralanabilir.

Öncelikle akıllı şehirlerin cazibesi arttıkça devletlerin ve yerel yönetimlerin uygulamalarında akıllı şehir standartları belirlenecek ve bu kurallara uygun davranması gerekecektir. Söz konusu standartların büyük ölçüde kanunlar, tüzükler ve yönetmeliklerle yapılması sonucu uygulama alanında daha bağlayıcı olacağı tartışma götürmezdir.

Alınması gereken bir diğer önlem ise özel sektörün elindeki kişisel verilere olan denetimi ve erişimi kontrol edebilmektir. Zira verinin ekonomik değeri arttıkça özel sektörün elindeki veriler ile birlikte şirket sermayesinde artışlar olacaktır.

Veri analitiği, günümüz karar alma süreçlerinde her alanda öne çıkmakta ve bu nedenle veri önemli bir faktör haline gelmektedir. Bireyin her aktivitesi takip edilerek bir veri analitiği oluşturulduğundan, kişisel sağlık alışkanlıklarından sosyal medyadaki düşüncelerine kadar tüm veriler kişinin önemli bir varlığını oluşturmaktadır. Söz konusu veri analitiği, elde edilen verilerden, bireyin sosyal alışkanlıklarını ve statüsünü kolayca bulmaya yardımcı olacaktır. Bu veriler, sağlık verileriyle birleştirildiğinde ise ortaya daha kırılgan bir tablo çıkmaktadır. Nitekim bireylerin sosyal medya faaliyetlerini tartışırken, hizmeti paylaşmadan veya kullanmadan önce kabul ettiği en azından dolaylı bir onay mekanizmasından bahsedilebilir. Buna rağmen IoT cihazlarından bahsederken, cihazın onay istemesi gibi bir ortam bulunmamakta ve kişinin kendisi herhangi bir faaliyete onay veya ret verememektedir. Bu durumda, insanlar için sürekli olarak daha iyi bir yaşam kalitesi veya daha yüksek kar hedefleyen hükümetler ve özel kuruluşlar; bazı gelişmeleri sağlarken kişinin mahremiyeti ve rızası dışında işlenen verilerini düşünmek zorunda kalmıştır.

Siber güvenlik, bilgi işlem sistemlerine, veri alışverişi kanallarına ve işledikleri verilere odaklanan bir güvenlik alt kümesidir.[142] Siber güvenlik, akıllı şehirlerdeki kritik sektörlere yönelik siber saldırı ve illegal faaliyetlerin artan potansiyeli nedeniyle kritik bir konu halini almıştır. Akıllı şehirlerdeki siber tehditleri düşündüğümüzde karşımıza veri ve sistem tehditleri çıkmaktadır. Bu siber risklerin üstesinden gelmek için, risk değerlendirmesi ve yönetimi için net bir yapı geliştirmek gerekmektedir. Akıllı bir şehirde siber riski azaltmaya yardımcı olmak için bazı önlemler alınmalıdır: tehditleri değerlendirmek için tehdit modellemesi yapılmalı, riskleri kabul ederek ve istisnalar belgelenmeli, risk değerlendirmesi ve yönetimi sürekli devam eden bir süreç haline getirilmeli, şehirdeki idarecilerin mahremiyet ilkelerini anlamaları ve desteklemeleri için eğitilmeli esneklik göz önünde bulundurulmalı, minimum güvenlik temelleri oluşturulmalı, bir güvenlik temelini desteklemek için net sorumluluklar tanımlanmalı, sürekli güvenlik izleme için bir sistem kurulmalı, tehdit ve güvenlik açıklarını paylaşmaya yönelik beklentiler belirlenmeli, şehirde yaşayan tüm paydaşlar arasındaki paylaşım için bir mekanizma oluşturulmalı, sistemi test etmek için siber tatbikatlar yapılmalı, şehirlerdeki aidiyet duygusu oluşturulmalı, geniş çaplı halkı bilinçlendirme kampanyaları geliştirilmeli ve sistem üzerinde çalışanlara öğrenme ve eğitim programları geliştirilmelidir.[143]

Akıllı şehirlerle ilgili iki temel güvenlik kaygısı vardır. Bunlardan ilki, akıllı şehir teknolojilerinin ve altyapı güvenliğinin bir siber saldırı yoluyla saldırıya uğramaya karşı ne ölçüde savunmasız olduğu; ikincisi ise bu tür teknolojiler ve altyapılarda işlenen, saklanan ve paylaşılan kişisel verilerin güvenliğidir.[144] Veriye dayalı şehircilik, büyük miktarlarda veri, kişisel veri ve bilgiyi üretir, işler, saklar ve paylaşır. Bu kişisel verilerin çoğu doğası gereği hassastır. Akıllı şehirlerde açık veri şeklinde yayınlanan verilerde olduğu gibi bazı veriler özgürce paylaşılabilirken, bazı veriler özel kabul edilerek güvenli bir şekilde saklanmayı ve korunmayı gerektirmektedir. Kişisel veri ihlalleri ise söz konusu sebeplerden dolayı ne kadar fazla sistem ve altyapı ağına bağlanırsa daha yaygın hale gelmekte ve saldırıya uğrama riski artmaktadır. Buna

---

142 Das, A., Sharma, S., Ratha, B. (2019). a.g.e. s.6
143 Das, A., Sharma, S., Ratha, B. (2019). a.g.e. s.8
144 Kitchin, Rob. (2016). a.g.e. s.39

karşılık çoğu şehrin siber güvenlik bütçeleri ve kaynakları sınırlıdır. Siber güvenlik departmanı, genellikle birkaç personelden ibarettir ve aldıkları eğitim buna bağlı olarak sınırlı kalmaktadır. Kişisel verilerin güvenliğini veya gizliliğini korumak için herhangi bir uygulama tasarlanırken siber güvenlik ile birlikte bazı gereksinimler de dikkate alınmalıdır. Bunlar; karşılıklı kimlik doğrulama, takip edilemezlik, oturum anahtarı, ileti gizliliği ve saldırı önleme.[145] olarak sıralanabilir.

Bilindiği gibi sensörler ve diğer işleme araçları kullanılarak özel nitelikli kişisel veriler de işlenmektedir. Bu veriler, ilgili kişiler tarafından açık rızaları alındıktan sonra şifreli metin formatında bir veri kayıt sisteminde saklanmakta ve böylece gizlilik açısından emin olunmaktadır. Gizliliği daha fazla korumak için özel nitelikli kişisel verilerinin şifresi tamamen çözülmemelidir. Bu sebeple önce veri kayıt sistemi düzeyinde kısmen şifre çözülerek ardından kullanıcı düzeyinde şifrenin çözülmesi beklenmektedir.

Elektronik ticaretin popülerlik kazanmasıyla birlikte şirketler, gizlilik gerektiren bu verileri ticari kazanç sağlamak için üçüncü kişilere aktarmaktadır. Söz konusu ticari faaliyetin kişisel verilerin korunması alanında meşru sayabilmek için anonimleştirmeyi kullanmak en doğru çözüm olacaktır. Zira akıllı şehirlerde ve akıllı ulaşım sistemlerinde kişileri belirli veya belirli kılabilir faaliyetlerin dışında işleyişi kolaylaştırmak amacıyla, aktarılacak verilerin anonimleştirerek aynı amaca hizmet edebileceği düşünülmektedir. Tüm bunların yanı sıra, akıllı bir altyapıda sıradan ve önemsiz sorunların üstesinden gelmek için günlük olarak yeni güvenlik önlemleri almak gerektiğini unutmamak gerekmektedir.[146]

Akıllı şehirlerde hiç şüphesiz siber güvenlik alanında alınması gereken önlemler önemli bir yer teşkil eder. Bu kapsamda 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12'nci maddesinde sayılan *"(1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel*

---

145 Wu, L., Wang, J., Kumar, N., He, D. (2017) "Secure public data auditing scheme for cloud storage in smart city". https://doi.org/10.1007/s00779-017-1048-7 s.35

146 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.9

verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmü gereğince teknik ve idari tedbirlerden önemli bir ayağı ise siber güvenlik alanı oluşturacaktır.

Buna göre güvenilir bir siber güvenlik yaklaşımı denildiğinde, bilgisayarlarda, ağlarda, programlarda veya güvende tutulması gereken verilerde birden fazla koruma katmanına sahip bir yapı aklımıza gelmeli ve bir örgüt yapısındaki insanlar, süreçler ve teknoloji, siber saldırılara karşı etkili bir savunma oluşturmak için iş birliği halinde olmalıdırlar.[147] Bir siber saldırısı kimlik hırsızlığından, şifrelerin ele geçirilmesine, aile fotoğrafları ve özel nitelikli kişisel verilerin kaybolmasına kadar her türlü durumla sonuçlanabilmektedir. Böyle bir durumda vatandaşlar, kişisel verilerini paylaştıkları devlet yetkilileri ve şirket yöneticileri, enerji santralleri, hastaneler ve finans şirketleri gibi kritik güvenlik duvarlarına sahip yapılara güvenmek mecburiyetindedirler.

Artık sadece bireylerin değil, "*devletlerin, kamu kurumlarının, sosyal platformların ve özel şirketlerin sunmuş oldukları ürün ve hizmetlere ilişkin iletişimler de sanal ortamlar vasıtasıyla gerçekleştirilmektedir*".[148] Bu durumda tüm veri kaynakları sanal ortamda birikmekte olup söz konusu durum, hizmetler ve kaynaklar açısından büyük bir tehlike oluşturmaktadır. Bu nedenle aygıtların ve insanların ağlar yoluyla birbirine bağlı olduğu akıllı şehirlerde amacına ulaşacak bir siber saldırının etkisi de büyük olacaktır.[149] Bunun yanı sıra, kişisel verilerin ve özel nitelikli kişisel verilerin kötü niyetli kişilerin eline geçmesiyle şehir sakinlerine sunulan günlük işlemler sekteye uğrayabilecek ve hatta durma noktasına gelebilecektir. Bu tür olumsuzluklarla karşılaşılmaması için akıllı şehirlerde siber güvenliğe önem verilmesi ve bu konuda akıllı şehir sakinlerine farkındalığının oluşturulması gereklidir.

---

147 Cisco, Annual Report. (2019) https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2019.pdf s.4

148 Şengün, H., Koçhan, A., Meydan, Y., Seçil, G. (2019). a.g.e. s. 5

149 ÇELİK, S. (2018). "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım". *Academic Review of Humanities and Social Sciences*. Cilt 1, Sayı 2, s. 112. https://dergipark.org.tr/tr/pub/arhuss/issue/40217/478931

Akıllı şehir uygulamaları şehirde üretilen ürün ve hizmetlere ilişkin verilerin, çeşitli yazılımlar vasıtasıyla işlenmesi olarak düşünüldüğüne göre, söz konusu yazılımların sürdürülebilirliği de bir güvenlik tehdidini beraberinde getirmektedir. Örneğin, şehirdeki akıllı ulaşım sistemine yapılacak bir siber saldırı, şehrin bütün ulaşım sisteminin sekteye uğramasına yol açabilecektir.[150] Benzer şekilde akıllı enerji sistemlerine yapılacak kötü niyetli bir müdahale de bütün sistemi olumsuz etkileyebilecektir. Öyle ki sadece akıllı şehirlerle sınırlı olmamakla beraber, günümüzde veriyi kullanarak devletler arasındaki güç dengesi değişmekte, kişisel verilerin iyi korunamaması sonucu hükümet seçimlerine müdahale, veri altyapılarının çalınması, askeri ve istihbari birçok bilginin önceden bilinerek çeşitli savunma mekanizmaları oluşturulması gibi birçok tehdit bulunmaktadır.[151]

Akıllı şehirlerde mahremiyet sorunlarına ilişkin kişisel veri güvenliğini sağlamanın en iyi yollarından birinin de tasarım yoluyla mahremiyet (Privacy by Design, PbD) olabileceği gerçeği ortaya çıkmaktadır.[152] Mahremiyeti tasarıma inşa etme fikrini düşünmemiz ve eğer şimdi akıllı şehirler inşa ediyorsak, PbD'nin toplum için neler yapabileceğini önceden düşünerek veya en azından bunların bir kısmını tasarlayıp inşa ederek akıllı şehirleri oluştururken çözmemiz gerekmektedir. Bu da bizlere gösteriyor ki akıllı şehirlerin de kendi içerisinde büyük problemlerinin olacağı ve bu problemleri en başta tasarlayarak ve süreç içerisinde bozulan kısımların düzeltilerek yol alınması gerektiğidir. Ayrıca akıllı şehirleri salt donanımla ilgilenen bir yapı olarak görmek yanlış olacaktır. Zira akıllı şehir özünde sistemle, insanla, doğayla ilgilenmesi dolayısıyla hayatı kolaylaştıran bir uygulamalar bütünü olarak bilinçlerde oturtulması gerekir. Dolayısıyla akıllı şehirleri tüm dertlere deva bir şehir sistemi olarak görmek hatayı en başında yapmak olacaktır.

Akıllı şehirlerde oldukça karmaşık bir yapı olacağı öngörülen akıllı şehirlerde sensörler, kablosuz ağlar, kameralar, uygulamalar ve iletişim sistemleri elektriğe bağlıdır. Bundan dolayı elektrik kesilebilir, yazılımda hata olabilir, siber saldırı gerçekleşebilir ve tüm bu

---

150 Şengün, H., Koçhan, A., Meydan, Y., Seçil, G. (2019). a.g.e.. s. 5

151 Yıldırımer, A. (2022). "Enformasyon Çağında Gözetim Toplumu: Facebook Cambridge Analytica Skandalı" *Yeni Medya Elektronik Dergisi*. Sayı:6 s.108

152 Deloitte (2021) "Privacy by Design Setting a new standard for privacy certification"

olumsuz durumlar şehrin altyapısında ciddi tahribatlar oluşturabilir. Bunun yanı sıra akıllı şehirlerde IoT kullanımı oldukça fazla olacağından dolayı[153] siber saldırı riski diğer ihtimallere göre daha yakın durmaktadır.

Avrupa Birliği veri koruma yasalarının ise akıllı şehirlerde kişisel veri mahremiyetine yönelik olası tehditleri nasıl kontrol edeceğine ilişkin iki olası çözüm olan; akıllı şehirler için zorunlu bir bütünsel mahremiyet etki değerlendirmesi (PIA, Privacy Impact Assessment) veya her bir veri grubu için açık rıza alınması ve kişisel veri işlemenin bu şekilde meşru hale getirilmesi seçenekleri uygulanabilecektir.[154] Öyle ki, mahremiyet etki değerlendirmesi, kişisel verilerin yeni kullanımlarının mahremiyet üzerindeki olası etkilerini değerlendirme süreci[155] olarak ifade edilmesi ile birlikte açık rıza alınması gereken her bir veri grubu açısından ilgili kişilerden açık rıza alınması da akıllı şehir uygulamalarında çeşitli kolaylık ve zorluklara sebep olacağı düşünülmektedir.

Mahremiyet, akıllı şehirlerde genel bir öncelik olmalıdır. Yeni teknolojiler, kendilerine sunulan hizmetleri benimseyecek olan kullanıcılara güven sağlayabilmelidir. Bu yüzden anahtar yönetimi, kimlik doğrulama işlemi sırasında gizliliğin korunmasında önemli bir role sahip olacaktır. Özellikle IoT sistemlerinde, gecikmeyi ve kişisel veri aktarımını azaltmak için hafif şifreleme şemaları gereklidir. Özellikle birbirine bağlı cihazların çoğalması, kullanıcıların kimlik doğrulamasında daha esnek çözümlerin aciliyetini artırmaktadır. Bu tür şemalar, makineden makineye kimlik doğrulamanın yanı sıra IoT'nin çeşitli yönlerinde de uygulanabilir olmaktadır.[156]

Akıllı şehirlerde mahremiyeti ve kişisel verileri koruyabilmek amacıyla akıllı şehir sistemini her yönden analiz ederek kişisel verilerin hangi noktada ihlal edilebileceği konusunda ortak bir mutabakata varılmalıdır. Bu durumda akıllı şehirlerde kişisel verilerin işlenmesine ilişkin ortak bir dil geliştirilmesi ve benzer mevzuatların çıkarılması gerekmektedir. Özellikle büyük veri ve nesnelerin interneti hususlarında

---

153 Edwards, L. (2016). a.g.e. s.3
154 Edwards, L. (2016). a.g.e. s.1
155 Metin, B., Erkan, S., Atasu, İ. ve Yılmaz, E., (2019). "Privacy Impact Assessment as a Tool for GDPR Compliance Preparation". *Kişisel Verileri Koruma Dergisi*. 1(2), s.80
156 Theodorou, S., Sklavos, N. (2019) a.g.e. s.33

anlaşma sağlanması gerekmektedir. Burada değinilmesi gereken başlıca nokta, Avrupa Veri Koruma Tüzüğü (GDPR) ile Amerika Birleşik Devletleri'nde yürürlükte olan mevzuat arasında bu konularda farkların bulunduğudur. Devamında ise; Amerika, Avrupa, Afrika ve Asya'da bulunan kişisel veri koruma mevzuatları birbiriyle uyumlu hale getirilmelidir. Nitekim kişisel verilerin işlenmesi ve yurtdışına aktarılması uluslararası ticareti ciddi derecede ilgilendiren bir konudur. Bu sebeple akıllı şehirlerde işlenen ve aktarılan kişisel verilerin yukarıda bahsedildiği gibi kim tarafından işleneceği ve nereye aktarılacağı önemli sorular haline gelmektedir.

Özellikle gözetim uygulamaları söz konusu olduğunda, bir birey hakkındaki kişisel veriler toplanabilmekte veya kişisel, sosyal ve yasal sonuçlara yol açacak şekilde işlenebilmektedir. Bu nedenle, akıllı şehirlerde kişisel verilerin korunması ve mahremiyetle ilgili yükümlülükleri ve uygulamalarının etkilerini göz önünde bulundurmak gerekecektir. Dikkatli bir şekilde değerlendirilmezse, korunması gereken veriler kamuya açıklanabilecek, sadece itibara zarar vermekle kalmaz, aynı zamanda yasal ihlallere de yol açabilecektir. Bu sebeple, kişisel verileri elinde bulunduran bir tüzel kişinin, verileri kötüye kullanım, müdahale ve kaybın yanı sıra yetkisiz erişim, değişiklik ve ifşadan korumak için gerekli tüm idari ve teknik tedbirleri alması gerekmektedir. Ayrıca, gizlilik ve güvenlikle ilgili teknolojilerin giderek gelişmesinden dolayı geçmişte makul önlemler olarak atfedilen adımlar, bugünün bağlamında makul olmaktan çıkabilecektir. Bu nedenle, tüzel kişilerin kişisel bilgilerin güvenliğiyle ilgili yaklaşımlarını düzenli olarak değerlendirmeleri gerekmektedir.[157]

Ayrıca, veri sorumlusu tüzel kişilerin kişisel bilgilerin yönetimi hakkındaki gizlilik politikasını açıkça ifade etmesi ve güncel tutması gerekmektedir. Bu nedenle, gizlilik politikasının, verilerin işlenmesinin, depolanmasının, aktarılmasını ve imha yöntemlerini içerecek şekilde belirli aralıklarla gözden geçirilmesi gereklidir. Bir tüzel kişilik, belirli bir amaç için kişisel veriler toplayabilir. Bu tür veriler, kişinin rızası olmadan farklı bir amaç için kullanılmamalı veya ifşa edilmemelidir. Gizlilik politikasında istisnai durumlar söz konusu olduğunda söz konusu tüzel kişilik, verilerin

---

[157] Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.60

ifşa edilmeden önce kimlik bilgilerinden arındırılmasını sağlamak için makul adımları atmalıdır. Bu bağlamda, akıllı şehirlerin çok sayıda sensörden veri toplaması, verileri ağ üzerinden depolama ve işleme için buluttaki sunuculara taşıması ve verileri şehrin altyapısı ve hizmetleri hakkında daha akıllı bir şekilde karar vermek için kullanması gereklidir. Dolayısıyla akıllı şehir uygulamaları geliştirilirken anlamsız ve büyük miktarda verinin kullanımı bir sorun olmasa da, bu sistem şehir ve vatandaşları için çeşitli riskler de içermektedir.[158]

6698 sayılı Kanunda belirtilen imha çeşitleri olarak silme, yok etme ve anonim hale getirme işlemleri uygulanabilmektedir. Akıllı şehirlerde kişisel verilerin açık rıza aranmadan hukuka uygun bir şekilde işlenebilmesi isteniyorsa silme, yok etme ve anonim hale getirme işlemlerinden sadece anonim hale getirmenin uygun olabileceği değerlendirilmektedir. Nitekim silme işleminde kısmen ve yok etme işleminde ise tamamen söz konusu veriyi geri getirmenin mümkün olmadığı öngörülmektedir. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 10. maddesindeki "*Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir*."[159] hükmü doğrultusunda kişisel verilere ilişkin anonimleştirmenin etkisi düzenlemiştir. Kişisel verilerin anonimleştirilmesine ilişkin işlemler de mezkur Yönetmeliğin belirttiği usulde yapılması gerekmektedir.

Anonimleştirme, verilerin gizlilik korumalı paylaşımında kullanılan yaklaşımlardan biridir. Veriler anonimleştirilip kamuya açıklandığında bile, kimliksizleştirilmiş veriler, bireylerin kimliğini çıkarmak için diğer veri kümeleriyle birleştirilebilir. Mozaik etkisi olarak da bilinen birden fazla kaynaktan gelen verileri kullanarak bilgi çıkarma yaklaşımı, bazen endişe verici olabilmektedir. Yayınlamadan önce kişisel verileri kaldırdıktan sonra bile, küçük nüfuslu konumlardan gelen veriler hala bireysel

---

158 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.60

159 Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf

kimlikleri dolaylı olarak ortaya çıkarabilmektedir.[160] Bu sebeple akıllı şehirlerde kişisel verilerin korunmasına dair tam bir taahhüt vermek neredeyse imkânsızdır.

Bir işletmenin üçüncü taraf bir uygulama kullanarak bir kişinin kimliğini doğrulaması gerekiyorsa, ne işletme ne de üçüncü taraf uygulaması, bireyin kimlik doğrulamasıyla ilgili bilgileri depolamamalıdır. Güvenlik gereksinimlerine ve ilgili tehditlere bağlı olarak, verilerin taşınması ve depolanması sırasında simetrik anahtar şifrelemesi veya ortak anahtar şifrelemesi gibi çeşitli şifreleme yöntemleri kullanılabilir. Kullanıcıların anonimleştirilmesi veya takma adların kullanılması, korumanın sağlanmasına yardımcı olabilecektir.[161] Bunun yanı sıra unutmamak gerekir ki, bir kişinin kişisel verileri imha edildiğinde bile, kaydın kalan özniteliklerinin doğru değerleri kişiyi tanımlamak için geri getirilebilir.[162]

Kimlik doğrulama, akıllı bir sistemin farklı katmanları için bir başka temel gereksinimdir ve kimlikleri kanıtlamak ve heterojen bir sistemdeki hizmetlere yalnızca yetkili kişilerin erişebilmesini sağlamak için gereklidir.[163] Bu noktada mahremiyetin amacı kişisel verinin saldırılara maruz kalmasını veya yanlış kaynağa aktarılmasını önlemektir.

IoT tabanlı uygulamalarda saldırganların iletişimi gizlice dinleme veya akıllı cihazlara erişme yeteneğine sahip olduğu varsayılır. Bu nedenle, ağ arasındaki veri aktarımının gizliliğini korumak için, güvenilir iletişim ve depolama sistemleri oluşturmak amacıyla şifreleme tabanlı teknolojiler yaygın olarak uygulanmalı ve kullanılabilirliği artırılmalıdır. Akıllı şehir sistemlerinin veya uygulamaların saldırı altında dahi etkin işleyişini sürdürebilme yeteneğine sahip olması gerekmektedir. Üstelik bu cihazlar saldırılara açık olduğundan, akıllı bir sistemin her türlü anormal durumu tespit edebilmesi ve sistemin daha fazla zarar görmesini önleyebilme yeteneğine de sahip

---

160 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.61

161 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.62

162 Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). a.g.e. s.63

163 Leı, C., Gang, X., Youyang, L., Gao, Y. (2018). a.g.e. s.139

olması gerekmektedir. Koruma mekanizmaları güçlü bir sağlamlığa sahip olmalı ve giderek daha akıllı hale gelen saldırılarla başa çıkabilmek için uyarlanabilir bir şekilde öğrenmeye devam edebilme yeteneğine sahip olmalıdır.

Hem IoT cihazlarının hem de cihazlar ile bulut arasında aktarılan verilerin bütünlüğünün sağlanması da önemlidir. Genel bir akıllı uygulamada kişisel veriler birçok cihaz arasında değiş tokuş edildiğinden, eğer iyi korunmazlarsa, iletim süreci sırasında veriler kolayca tahrif edilebilir. Gelen tehditleri önceden tahmin etmek ve bilmek, özellikle web tabanlı uygulamalar için, saldırı sonrasında tespit edip kurtarmaktan çok daha önemlidir. Bu nedenle güvenlik durumu farkındalığının sağlanması ve akıllı uygulamalara yönelik çeşitli saldırıların otomatik olarak tahmin edilebilmesi için akıllı sistemlerinin geliştirilmesi büyük önem taşımaktadır.

Şu ana kadar yapılan tartışmalardan, akıllı şehir uygulamalarıyla ortaya çıkan bir dizi kişisel veri gizliliği, koruma ve güvenlik endişesi olduğu açıkça görülmektedir. Bu sebeple akıllı şehir teknolojilerinin mümkün kıldığı gözetim teknolojileri, tahmine dayalı profil oluşturma, sosyal sınıflandırma, yönetişim, şehir altyapı ve hizmetlerinde sağlanan kolaylık ve tüm bunlara ilişkin oluşturulan mevzuat; kişisel veri gizliliği, koruma ve güvenliğinin en iyi şekilde nasıl uygulanacağıyla ilgilidir. Aynı zamanda, toplumun kitlesel gözetlenmesine ilişkin mahremiyet ile ulusal güvenlik arasında bir denge gözetilmesi gerektiğini bizlere göstermektedir. Öte yandan kişisel verilerin korunması hakkı insan hakları kavramı içerisinde vazgeçilmez bir yerde durduğu için kitlesel gözetleme tehlikesi, özgürlük gibi temel toplumsal değerlerin kaybının yerini yüksek düzeyde kontrol edilen ve otoriter toplumların almasından endişe edilmektedir.

Akıllı şehirlerde yapılan kitlesel veri üretimi, yeni ürünler, pazarlar ve karlılık ile bireysel ve kolektif haklar arasında bir denge meselesinin varlığını ortaya çıkarmaktadır. Bir tarafta, kişisel veri gizliliği ve mahremiyetinin yenilikçiliği ve bireysel verilerden ekonomik değer elde edilmesini engellememesi gerektiğini ileri sürerken diğer tarafta ise mahremiyeti ihlal etmeden ve ilgili kişileri profillemeden büyük veriden değer elde etmenin ve yeni ürünler üretmenin mümkün olduğunu ileri sürmektedir. Bu nedenle kişisel verilerin mahremiyetine ilişkin tartışmalar bazen

oldukça siyah beyaz terimlerle anlatılsa da aslında grilerin bol olduğu bir mecraya oturmaktadır. Asıl mesele, mahremiyet ile diğer çıkarlar arasındaki dengeyi korumak için doğru araçların mevcut olmasını sağlamaktır. Bu amaçla akıllı şehirlerde piyasa çözümleri, teknolojik çözümler, politika üretme ve düzenlemelere ilişkin çözümler, yasal çözümler, yönetişim ve yönetim çözümleri oluşturmak çok önemli bir alanı oluşturmaktadır.

Akıllı şehirler bağlamında kişisel verileri koruma ve veri mahremiyeti konularında endişeler mevcuttur ve bu endişeler ilerleyen yıllarda temkinli bir yaklaşıma dönüşebilecektir. Bu durumda akıllı şehirlerin potansiyel faydalarının farkına varılamaması anlamına gelmesine rağmen daha verimli, üretken, sürdürülebilir, şeffaf, adil ve hakkaniyetli şehirler üretme konusundaki potansiyel faydalarını da göz önünde bulundurmamız gerekmektedir. Yapılması gereken ise bir dizi gerçek kaygının bulunduğunu kabul etmek ve akıllı şehir teknolojilerinin faydalarından yararlanmayı da sağlayacak çözümler bulup benimsemektir.

Akıllı şehirlerde kişisel verileri ve mahremiyeti korumak için bir denge mekanizması oluşturulması gerektiği elzemdir. Akıllı şehirleri göz ardı etmek veya kasıtlı olarak bunlardan kaçınmak geçerli bir yaklaşım olmadığı gibi çeşitli zararlar doğuran ve güç dengesizliklerine sebep olan akıllı şehirler geliştirmek de doğru değildir. Bunun yerine, merkezinde bir dizi etik ilke ve değer bulunan bir akıllı şehir oluşturmak daha makul bir yaklaşım olacaktır. Şunu da belirtmek gerekir ki akıllı şehir alanında çeşitli paydaşlar ve çıkarlar göz önüne alındığında, böyle dengeli bir yaklaşımın tasarlanması veya uygulanması da kolay değildir.

Akıllı şehirleri inşa ederken insanların hayatlarını kolaylaştıracak, iyileştirecek ve geleceğe dair umutlandıracak şehirler oluşturma kaygısı güdülmelidir. Aksi takdirde gücü elinde tutan devlet, şirket ve benzeri yapılara hizmet eden; gücüne güç katan ve insanların hayatlarını kolaylaştırmanın aksine zorlaştıran yapıların kişisel verileri ve mahremiyeti hiçe saydığı bir topluma dönüşebilmemiz kaçınılmazdır. Unutulmaması gerekir ki akıllı şehirlerde kişisel verilerin ve mahremiyetin koruması için insanların akıllı şehirden daha akıllı olması gerekmektedir.

SONUÇ

İnsanlık tarihi ile birlikte insanlar gibi şehirler de dönüşümler geçirmeye maruz kalmış ve birçok gelişim aşamasından sonra teknoloji ile birlikte farklı bir boyuta geçilmiştir. Sanayi sektörünün gelişmesi sonucu şehirlerin yapıları ve sistemleri de bundan nasibini almıştır. Tarıma dayalı üretim ilişkileri olan şehirlerden büyük sanayi ve teknoloji şehirlerine doğru gelişim gösteren şehirlerde ihtiyaçlar da bununla birlikte değişmeye ve çeşitlenmeye başlamıştır. Modern şehir sisteminde ulaşım, iletişim, yönetim, altyapı, eğitim, sağlık vb. birçok konuda yeni ve teknolojiye dayalı ihtiyaçlar ortaya çıkmaktadır.

Bu amaçla ortaya çıkan akıllı şehir kavramı; vatandaşların yaşamını iyileştirmeyi, şehir yönetimi geliştirmeyi ve bunları yaparken dijital teknolojileri kullanmayı hedefleyen; içerisinde teknolojik araçların bulunduğu teknik bir sistemin yanı sıra sosyolojik ve felsefik tartışmaları da beraberinde getiren bir sistem bütünü olarak karşımıza çıkmaktadır. Akıllı şehirlerin bu hizmetleri sunabilmesi için hiç şüphesiz veriye ihtiyaç duyulmaktadır. Veriye dayalı bir temele oturan akıllı şehirlerin en önemli veri girdisini ise kişisel veriler oluşturmaktadır.

Verinin, akıllı cihazlar kullanılarak çok miktarda üretilmesi ile birlikte ortaya çıkan yığını anlamlı bir bilgiye dönüştürebilmek amacıyla büyük veri, açık veri, nesnelerin interneti, bulut teknolojisi, gözetim teknolojileri, blockchain ve yapay zeka gibi çeşitli yeni kavramlar ortaya çıkmıştır. Sayılan süreçlerde insan faktörü etkin bir rol oynarken ortaya çıkan nesnelerin interneti kavramı ile birlikte insan faktörü olmaksızın akıllı nesnelerin birbirleriyle irtibatı dolayısıyla veri aktarımının gerçekleşmesi ve otonom hareket kabiliyeti kazanması ortaya çıkmıştır.

Bununla birlikte her ne kadar teknolojinin gelişimi birçok ihtiyacı karşılayacak boyuta ulaşsa da insanların ilk yaratıldığı günden günümüze mahremiyet ihtiyacı değişmemiştir. Günümüzde insanların bir arada yaşadığı alan olan kamusal alan, yarı kamusal alan ve en mahrem alanları olan özel alan kavramlarının değişim gösterdiği yadsınamaz bir gerçektir. Özellikle gelişen teknolojinin sonucu olarak kişisel verilerin

ve şehirlerde yaşayan insanların mahremiyetinin korunması ihtiyacı önemli bir sorun haline gelmiştir. Bununla beraber günümüzde kamu hizmetlerinin ifasında kamu sektörünün yanı sıra özel sektörün de önemli bir rol oynaması kişisel verilerin korunması ve mahremiyet hususlarında endişeleri giderek artırmaktadır. Söz konusu gelişmelerin, şirketlerin güçlenmesine bir araç olacağını iddia eden görüşler mevcuttur.

Tüm bu gelişmeler akıllı şehirlerde verinin ne kadar büyük miktarlarda kullanılacağının yanı sıra vatandaşların mahremiyetinin nasıl bir tehdit altında olduğunu da gözler önüne sermektedir. Günümüzde Avrupa'da ve dünyanın başka kıtalarından ülkeler tarafından kullanılan Genel Veri Koruma Tüzüğü (GDPR) ve Türkiye'de 2016 yılından beri yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ise bu alanda farkındalığın artırılması ve bir başlangıç olması bakımından önem arz etmektedir. Bu çalışmada, ülkemizde 6698 sayılı Kanuna ve diğer mevzuata dayanarak akıllı şehirlerde kişisel verilerin ve mahremiyetin nasıl ve hangi şartlarda korunacağına ilişkin açıklık getirilmeye çalışılmıştır.

Akıllı şehirlerde kişisel veriler korunmasına olan ihtiyaç, hiç şüphesiz bir şehri akıllı yapacak araçların varlığından dolayı ortaya çıkmıştır. Şehirde bulunan sensörler ve kameralar gibi kişilerin verilerini işleyen her türlü araçlar, akıllı şehirlerde gözetleme sistemlerinin bir parçası haline gelmektedir. Gözetleme sistemleri, vatandaşlar üzerinde bazı sosyolojik ve psikolojik etkiler oluşturmaya gebedir. Vatandaşların şehir faaliyetlerine aktif katılabildiği ve haberdar olabilmesinin yanı sıra sürekli takip edildiği ve gözlendiği hissini taşımasının farklı sonuçlar doğuracağı kuşkusuzdur. Bu sebeple gözetim teknolojilerinin de hukuka uygun bir şekilde oluşturulması önemli bir husustur. Sürekli kamera, sensör ve çevrimiçi platformlarda gözetlendiğini düşünen insanların bir süre sonra teknolojik determinizm tuzağına düşebileceği, marjinalleşmiş grupların ortaya çıkabileceği, temsiliyet sorunu ve suç oranlarının artış gösterebileceği endişeleri göz ardı edilmemelidir.

Akıllı şehir yapısında insanların şehir yönetişimde aktif rol oynaması elbette olumlu karşılanan bir husustur. Mahremiyet sorunlarını çözüme kavuşturabilmek amacıyla hızlı ve etkin bir mekanizmanın kurulmasının yanı sıra akıllı şehirlerde uluslararası ortak bir

mahremiyet anlayışı ile birlikte ortak politikaların ve organizasyonların belirlenmesi gerekmektedir. Özellikle akıllı şehirlerde kişisel veri işleme, aktarım, saklama ve imha kurallarının yanı sıra aydınlatma ve açık rıza mekanizmalarına ilişkin olası sorunları irdelemek ve bunlara uygun çözümler üretebilmek için dengeli bir sistemi ortaya çıkaracak uzun bir yola ihtiyaç bulunmaktadır.

Hiç şüphesiz akıllı şehirlerde kişisel verilerin korunması ve mahremiyetin sağlanması veri güvenliğine ilişkin uygulanması gereken teknik tedbirleri hayati derecede önemli hale getirmektedir. Özellikle siber saldırılar ve sistemde bulunan açıklara karşı tedbirlerin alınması gerekmesinin yanında LoT cihazlarının fark edilmezliği ve insanların bu konularda bilinç düzeylerinin artırılması gerekmektedir.

Akıllı şehirler; hizmetleri iyileştirmek, israfı azaltmak, kaynakları etkin ve doğru yerlere kullanmak, yönetişimi geliştirmek, temsiliyeti, demokrasiyi, denetimi ve hesap verebilirliği artırmayı amaçlarken söz konusu hizmetleri veriyi ve özellikle kişisel veriyi kullanarak yerine getirecektir. Bu sebeple kişisel verilerin hukuka uygun bir şekilde işlenmesi, saklanması, aktarılması ve imha edilmesi önemli bir konu haline gelmektedir. Bununla birlikte akıllı şehirlerde kullanılan gözetim teknolojilerinin insanlar üzerinde bir baskı mekanizması olarak kullanılmasına dikkat edilmelidir. Bu sebeple akıllı şehirler tesis edilirken bu hususlar göz önünde bulundurulmalıdır ve akıllı şehirlerden daha akıllı olunmadığı sürece kişisel verilerim ve mahremiyeti korumanın mümkün olmadığını unutmamak gerekmektedir.

KAYNAKÇA

"*Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler*" (Çevrimiçi) https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler

Abberley, L., Gould, N., Crockett, K., Cheng, J. (2017). "*Modelling road congestion using ontologies for big data analytics in smart cities*". Uluslararası Akıllı Şehirler Konferansı (ISCC).

Abu-Elkheir, M. Hassanein, S. Oteafy, S. (2016) "*Enhancing emergency responsesystems through leveraging crowd sensing and heterogeneous data*" Uluslararası Kablosuz İletişim ve Mobil Bilgi İşlem Konferansı (IWCMC).

Addison, J. (2018). "*Smart City Chicago*". https://meetingoftheminds.org/smart-city-chicago-27152.

Aguilera, U., Peña, O., Belmonte, O., López-de Ipiña, D. (2017) "Citizen-centric data services for smarter cities*". Future Computing Systems Dergisi*. Sayı:7.

Akkan, M. (2019) "*Akıllı Kent Uygulamaları ve Konya Örneği*". Necmettin Erbakan Üniversitesi, Sosyal Bilimler Enstitüsü. Konya, Yüksek Lisans Tezi.

Aksoy H. C., (2022). "Kişisel Verilerin Korunması Yönüyle Algoritmik Karar Verme" *Kişisel Verileri Koruma Dergisi*. 4(2).

Aksoy, H. C. ve Halıcıoğlu, M. (2021). "AB ve Türk Hukuklarında Çerezler". *Kişisel Verileri Koruma Dergisi*. 3(1).

Aldemir, A. (2018). "*Geleneksel Şehir Sistemlerinin Akıllı Şehir Sistemlerine Geçiş Süreçlerinin Yönetilmesi*" (yüksek lisans tezi). İstanbul, 2018.

Bianca W. (2022). "*Artificial Intelligence in the City: Building Civic Engagement and Public Trust*". (Kitap Bölümü: AI Trust, and the City: Assets and Accountability). (Editörler: Brandusescu, A., Reia, J.). Centre For Interdisciplinary Research on Montreal.

Braun, T., Fung, B., Iqbal, F., Shah, B. (2018) "*Security and privacy challenges in smart cities*". Sustainable Cities and Society.

Cho, K., Kim, C. (2017) "*Design For Privacy In Public Space*" 21st International Conference On Engineering Design.

Cisco, Annual Report. (2019) https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2019.pdf .

Çelik, S. (2018). "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım". *Academic Review of Humanities and Social Sciences*. Cilt 1, Sayı 2 https://dergipark.org.tr/tr/pub/arhuss/issue/40217/478931.

Çevre ve Şehircilik Bakanlığı. (2019). "*Ulusal Akıllı Şehirler Stratejisi ve Eylem Planı*". https://www.akillisehirler.gov.tr/wp-content/uploads/EylemPlani.pdf.

Das, A., Sharma, S., Ratha, B. (2019). (Kitap Bölümü: The New Era of Smart Cities, From the Perspective of the Internet of Things). "*Smart Cities Cybersecurity And Privacy*". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları.

Deloitte. (2016). "*Akıllı Şehir Yol Haritası*" https://www2.deloitte.com/tr/tr/pages/public-sector/articles/smart-cities.html.

Doğan, K., Arslantekin, S. (2016). "Büyük Veri: Önemi, Yapısı ve Günümüzdeki Durum". *DTCF Dergisi*, Cilt:56, Sayı:1.

Durdu, M. (2019). "*Mükellef Verilerinin Korunması ve Vergi Mahremiyeti*". Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C.27.

Dülger, M. (2019). "Avrupa Birliği Genel Veri Koruma Tüzüğü Bağlamında Kişisel Verilerin Korunması". *Yaşar Hukuk Dergisi*.

Edmondson, V., Cerny, M., Lim, M., Gledson, B., Lockley, S., Woodward, J. (2018). "*A smart sewer asset information model to enable an 'Internet of Things' for operational wastewater management*". Autonomous Construct.

Edwards, L. (2016). "Privacy, security and data protection in smart cities: a critical EU law perspective". *European Data Protection Law Review*, Sayı: 2 (1)

Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., Nepal, S. (2019). (Kitap Bölümü: Crowdsensing And Privacy İn Smart City Applications). "*Smart Cities Cybersecurity And Privacy*". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları.

Gershenfeld, N., Krikorian, R., Cohen, D. (2004) "*The internet of things*". 291(4).

Gharaibeh, A., Khalil, I., Salahuddin, M., Guizani, M. (2017). "Smart Cities: A Survey on Data Management, Security and Enabling Technologies". IEEE Communication Surveys & Tutorials.

Gürsoy, A. N. (2016) "*Martı Nedir? Nasıl Kullanılır?*" https://www.sigortaladim.com/marti-nedir-nasil-kullanilir.

H. Li, H. Zhu, S. Du, X. Liang, X. Shen. (2016) "Privacy leakage of location sharing in mobile social networks: attacks and defense". *IEEE Transactions on Dependable and Secure Computing Dergisi*, Sayı: 15.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. ve Williams, P. (2010). "Foundations for Smarter Cities". *IBM Journal of Research and Development*, 54(4)

Hatipoğlu Aydın, D. (2023). "Kişisel Verilerin Korunmasında Hukukun Sınırları" İzmir Barosu Dergisi.

Hayta, Yasemin. (2021). "*Akıllı Kent Uygulamalarında Kişisel Verilerin Gizliliği ve Güvenliği*". Fırat Üniversitesi Sosyal Bilimler Dergisi, Sayı: 31.

Heilig, G. (2012). "World Urbanization Prospects: The 2011 Revision". *United Nations, Department of Economic and Social Affairs (DESA),* Population Division, Population Estimates and Projections Section. New York.

Ismagilova, E., Hughes, L., Rana, N.P. (2022). "Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework".

Kasar, S., Meghana, K. (2021). (Kitap Bölümü: Open Challenges in Smart Cities: Privacy And Security). "*Security And Privacy Applications For Smart City Development*". (Editörler: Sharvarı, T., Dey, N., Aboul-Ella, H.). Varşova, Polonya: Springer Yayınları.

Kaygısız, Ü.; Aydın, Z. (2017). "Yönetişimde Yeni Bir Ufuk Olarak Akıllı Kentler". *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. Cilt 9, Sayı 18.

Keleş, R. (1990). "*Kentleşme politikası*", İmge Kitabevi.

Kitchin, R. (2014) "The Real-Time City? Big Data and Smart Urbanism" *Geo Journal*, (Çevrimiçi) https://doi.org/10.1007/s10708-013-9516-8.

Kitchin, R. (2016) "*Getting smarter about smart cities: Improving data privacy and data security*". Data Protection Unit, Department of the Taoiseach, Dublin, Ireland.

Kitchin, R. (2016) "*The ethics of smartcities and Urbanscience*". Philosopical Transactions Society (Çevrimiçi) http://dx.doi.org/10.1098/rsta.2016.0115 .

Kocabıyık, O. (2023). "*Kamu Hizmeti Yönüyle Akıllı Şehirlerde Kişisel Verilerin Korunması*". Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi.

Köseoğlu, Ö., Demirci, Y. (2018). "Akıllı Şehirler ve Yerel Sorunların Çözümünde Yenilikçi Teknolojilerin Kullanımı". *Uluslararası Politik Araştırmalar Dergisi*, Cilt 4.

Kul, H. H., Melikoğlu, M. Y. "*İBB'nin İstanbulkart'ın kişiselleştirilmesi kararı seyahat özgürlüğünün kısıtlanması" olarak değerlendiriliyor*". (2022) https://www.aa.com.tr/tr/gundem/ibbnin-istanbulkartin-kisisellestirilmesi-karari-seyahat-ozgurlugunun-kisitlanmasi-olarak-degerlendiriliyor/2722479.

Kutlu, Ö., Kahraman, S. (2017) "Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi". *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, c.5.

Küzeci, E. (2023). (Kitap Bölümü: Kişisel Verilerin Korunması Hakkı). "Kişisel Verilerin Korunmasına Akademik Bakış". (Editörler: Aksoy, H., Aksoy, P.). KVKK Yayınları.

Leu, C., Gang, X., Youyang, L., Gao, L., Yunyun, Y. (2018) "*Security And Privacy İn Smart Cities: Challenges And Opportunities*". Ieee Access.

Magi, T. (2011). "*Fourteen reasons privacy matters: a multidisciplinary review of scholarly literature*", Quarterly Library.

Memiş, L., Güç, M. (2020) "Akıllı Kentlerde Verinin Gizliliği ve Güvenliği: İlkeler ve Yaklaşımlar". *Güvenlik Bilimleri Dergisi.*

Metin, B., Erkan, S., Atasu, İ. ve Yılmaz, E., (2019). "Privacy Impact Assessment as a Tool for GDPR Compliance Preparation". *Kişisel Verileri Koruma Dergisi*. 1(2).

Nair, G. (2019). "*Kentsel Yaşamın Bilgi ve İletişim Teknolojilerinin Işığında Yeniden İnşası ve Anadolu'dan Bir Örnek: Sivas Belediyesi'nin Akıllı Kent Uygulamaları*". Araştırma Makalesi, 8(1).

Nam, T. Pardo, T. A. (2011). "*Conceptualizing Smart City with Dimensions of Technology, People, and Institutions*". Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times.

Nur, P., Canyaş, O. (2023). "Bir Norm Çatışması Örneği: Vergi Usul Kanunu ve Kişisel Verilerin Korunması Kanunu". *Türkiye Adalet Akademisi Dergisi*.

Open Knowledge International. (2018). "*Open Data Handbook*" https://opendatahandbook.org/guide/en/.

P. Joglekar, V. Kulkarni (2017) "*Privacy Issues in Urban Computing using Mobile Crowdsensing*" International Journal of Computer Applications, Volume 168.

Pevlivan, E. (2017). "*Katılımcı, Sürdürülebilir Bir Akıllı Şehir Hedefliyoruz*". Fortune Dergisi. https://www.fortuneturkey.com/yol-acin-akilli-sehirler-geliyor-45878.

Saini, R., Mishra, D. (2019). (Kitap Bölümü: Privacy-Aware Physical Layer Security Techniques For Smart Cities). "*Smart Cities Cybersecurity And Privacy*". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları.

Şengün, H., Koçhan, A., Meydan, Y., Seçil, G. (2019) "Akıllı Kentler ve Dijital Siber Güvenlik". *Assam Dergisi*, 13. Uluslararası Kamu Yönetimi Sempozyumu.

Theodorou, S., Sklavos, N. (2019). (Kitap Bölümü: Blockchain-Based Security And Privacy İn Smart Cities). "*Smart Cities Cybersecurity And Privacy*". (Editörler: Rawat, D., Ghafoor, K.). Hindistan, Eysevier Yayınları.

Townsend, A. (2013) "*Smart Cities: Big data, Civic Hackers, and the Quest for a New Utopia*". New York: W.W. Norton & Co.

Türkiye Bilişim Derneği (TBD). (2016). "*Büyük Veri Uygulamaları Çalışma Grubu Raporu*" https://docplayer.biz.tr/35808546-Turkiye-bilisim-dernegi-kamu-bilisim-merkezleri-yoneticileri-birligi-kamu-bilisim-platformu-buyuk-veri-uygulamalari-calisma-grubu-raporu.html.

Ünal, S., Sezgin, A. (2021). "Büyük Veri (Big Data)'nin Yapay Zekâ Uygulamalarında Toplumsal Sınıflandırmaya Yönelik Kaygılar" *Bilişim Teknolojileri Online Dergisi.*

Webrazzi. (2016) "Ukrayna'da elektrik neden kesildi?" https://webrazzi.com/2016/01/16/ukraynada-elektrikler-neden-kesildi/ (Çevrimiçi).

Wikipedia. "Singapur" https://tr.wikipedia.org/wiki/Singapur.

Wu, L., Wang, J., Kumar, N., He, D. (2017) "*Secure public data auditing scheme for cloud storage in smart city*". https://doi.org/10.1007/s00779-017-1048-7.

Y. Li, Y.-S. Jeong, B.-S. Shin, J.H. Park. (2017). "*Crowdsensing multimedia data: security and privacy issues*", IEEE Multimedia.

Yıldırımer, A. (2022). "Enformasyon Çağında Gözetim Toplumu: Facebook Cambridge Analytica Skandalı" *Yeni Medya Elektronik Dergisi.*

Zoonen, L. (2016). "Privacy Concerns in Smart Cities". Government Information Quarterly v. 33.

EKLER

EK 1. ORİJİNALLİK RAPORU

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu *Form No.*	FRM-YL-15
		Yayım Tarihi *Date of Pub.*	22.11.2023
	FRM-YL-15 **Yüksek Lisans Tezi Orijinallik Raporu** *Master's Thesis Dissertation Originality Report*	Revizyon No *Rev. No.*	01
		Revizyon Tarihi *Rev.Date*	01.12.2023

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI BAŞKANLIĞINA

Tarih: 19/01/2024

Tez Başlığı: Kişisel Verilerin Korunması Bağlamında Akıllı Şehirler ve Veri Mahremiyeti
Tez Başlığı (Almanca/Fransızca)*::.....
.....

Yukarıda başlığı verilen tezimin a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 109 sayfalık kısmına ilişkin, 19/01/2014 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 20 'dir.

Uygulanan filtrelemeler*:

1. ☐ Kabul/Onay ve Bildirim sayfaları hariç
2. ☐ Kaynakça hariç
3. ☐ Alıntılar hariç
4. ☒ Alıntılar dâhil
5. ☐ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tezimin herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumlarda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

19.01.2024

Öğrenci Bilgileri			
	Ad-Soyad	Miraç GÜR	
	Öğrenci No	N18131177	
	Enstitü Anabilim Dalı	Kamu Hukuku	
	Programı	Tezli Yüksek Lisans	
	E-posta/Telefon		

DANIŞMAN ONAYI

UYGUNDUR.
Doç. Dr. Duygu HATİPOĞLU AYDIN

* Tez **Almanca** veya **Fransızca** yazılıyor ise bu kısımda tez başlığı **Tez Yazım Dilinde** yazılmalıdır.
**Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları İkinci bölüm madde (4)/3'te de belirtildiği üzere: Kaynakça hariç, Alıntılar hariç/dahil, 5 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 5 words) filtreleme yapılmalıdır.

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu *Form No.*	FRM-YL-15
		Yayım Tarihi *Date of Pub.*	22.11.2023
	FRM-YL-15 **Yüksek Lisans Tezi Orijinallik Raporu** *Master's Thesis Dissertation Originality Report*	Revizyon No *Rev. No.*	01
		Revizyon Tarihi *Rev.Date*	01.12.2023

TO HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF PUBLIC LAW

Date: 19/01/2024

Thesis Title (In English): Smart Cities and Data Privacy in the Context of Personal Data Protection

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 19/01/2024 for the total of 109 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled above, the similarity index of my thesis is 20 %.

Filtering options applied**:

1. ☐ Approval and Decleration sections excluded
2. ☐ References cited excluded
3. ☐ Quotes excluded
4. ☒ Quotes included
5. ☐ Match size up to 5 words excluded

I hereby declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

Kindly submitted for the necessary actions.

19.01.2024

Student Information			
	Name-Surname	Mirac GUR	
	Student Number	N18131177	
	Department	Public Law	
	Programme	Master's Thesis	
	E-mail/Phone Number		

SUPERVISOR'S APPROVAL

APPROVED
Assoc. Prof. Duygu HATIPOGLU AYDIN

**As mentioned in the second part [article (4)/3]of the Thesis Dissertation Originality Report's Codes of Practice of Hacettepe University Graduate School of Social Sciences, filtering should be done as following: excluding refence, quotation excluded/included, Match size up to 5 words excluded.

EK 2. ETİK KURUL/KOMİSYON İZNİ YA DA MUAFİYET FORMU

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu *Form No.*	FRM-YL-09
		Yayım Tarihi *Date of Pub.*	22.11.2023
	FRM-YL-09 **Yüksek Lisans Tezi Etik Kurul Muafiyeti Formu** *Ethics Board Form for Master's Thesis*	Revizyon No *Rev. No.*	01
		Revizyon Tarihi *Rev.Date*	01.12.2023

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI BAŞKANLIĞINA

Tarih: 19/01/2024

Tez Başlığı (Türkçe): Kişisel Verilerin Korunması Bağlamında Akıllı Şehirler ve Veri Mahremiyeti
Tez Başlığı (Almanca/Fransızca)*: .....
.....

Yukarıda başlığı verilen tez çalışmam:

1. İnsan ve hayvan üzerinde deney niteliği taşımamaktadır.
2. Biyolojik materyal (kan, idrar vb. biyolojik sıvılar ve numuneler) kullanılmasını gerektirmemektedir.
3. Beden bütünlüğüne veya ruh sağlığına müdahale içermemektedir.
4. Anket, ölçek (test), mülakat, odak grup çalışması, gözlem, deney, görüşme gibi teknikler kullanılarak katılımcılardan veri toplanmasını gerektiren nitel ya da nicel yaklaşımlarla yürütülen araştırma niteliğinde değildir.
5. Diğer kişi ve kurumlardan temin edilen veri kullanımını (kitap, belge vs.) gerektirmektedir. Ancak bu kullanım, diğer kişi ve kurumların izin verdiği ölçüde Kişisel Bilgilerin Korunması Kanuna riayet edilerek gerçekleştirilecektir.

Hacettepe Üniversitesi Etik Kurullarının Yönergelerini inceledim ve bunlara göre çalışmamın yürütülebilmesi için herhangi bir Etik Kuruldan izin alınmasına gerek olmadığını; aksi durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

19.01.2024

Öğrenci Bilgileri			
	Ad-Soyad	Miraç GÜR	
	Öğrenci No	N18131177	
	Enstitü Anabilim Dalı	Kamu Hukuku	
	Programı	Tezli Yüksek Lisans	
	E-posta/Telefon		

DANIŞMAN ONAYI

UYGUNDUR.
Doç Dr. Duygu HATİPOĞLU AYDIN

* Tez **Almanca** veya **Fransızca** yazılıyor ise bu kısımda tez başlığı **Tez Yazım Dilinde** yazılmalıdır.

	HACETTEPE ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ	Doküman Kodu *Form No.*	FRM-YL-09
		Yayım Tarihi *Date of Pub.*	22.11.2023
	FRM-YL-09 **Yüksek Lisans Tezi Etik Kurul Muafiyeti Formu** *Ethics Board Form for Master's Thesis*	Revizyon No *Rev. No.*	01
		Revizyon Tarihi *Rev.Date*	01.12.2023

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
DEPARTMENT OF PUBLIC LAW

Date: 19/01/2024

ThesisTitle (In English): Smart Cities and Data Privacy in the Context of Personal Data Protection

My thesis work with the title given above:

1. Does not perform experimentation on people or animals.
2. Does not necessitate the use of biological material (blood, urine, biological fluids and samples, etc.).
3. Does not involve any interference of the body's integrity.
4. Is not a research conducted with qualitative or quantitative approaches that require data collection from the participants by using techniques such as survey, scale (test), interview, focus group work, observation, experiment, interview.
5. Requires the use of data (books, documents, etc.) obtained from other people and institutions. However, this use will be carried out in accordance with the Personal Information Protection Law to the extent permitted by other persons and institutions.

I hereby declare that I reviewed the Directives of Ethics Boards of Hacettepe University and in regard to these directives it is not necessary to obtain permission from any Ethics Board in order to carry out my thesis study; I accept all legal responsibilities that may arise in any infrigement of the directives and that the information I have given above is correct.

I respectfully submit this for approval.

19.01.2024

Student Information			
	Name-Surname	Mirac GUR	
	Student Number	N18131177	
	Department	Public Law	
	Programme	Master's Thesis	
	E-mail/Phone Number		

SUPERVISOR'S APPROVAL

APPROVED
Assoc. Prof. Duygu HATIPOGLU AYDIN