KVKK KİŞİSEL VERİLERİ KORUMA KURUMU
www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt:4 Sayı:2

Geliş: 18.05.2022
Kabul:07.12.2022

Nesnelerin İnternetinin Kişisel Verilerin Korunması Kapsamında İncelenmesi

Alpkaan, ERTAN
Ticaret Bakanlığı Uzman Yardımcısı, Ankara, Türkiye, alpkaan.matematikci@gmail.com
ORCID ID: 0000-0002-3654-9463

ÖZ
IPv6 gibi yeni ağ teknolojilerinin kullanımı ve nesnelerin adreslenebilmesini sağlayan tanımlama teknolojilerinin gelişmesiyle nesnelerin interneti teknolojisinin kullanımı her geçen gün artmıştır.
Bu çalışma kapsamında öncelikle nesnelerin internetinin tanımı, amacı, tarihçesi, uygulama alanları, bileşenleri, mimarisine değinilmiş olup nesnelerin interneti teknolojisine ilişkin olarak kişisel verilerin korunması kapsamında dile getirilen endişeler ile 29 Çalışma Grubu tarafından nesnelerin interneti paydaşlarına verilen çözüm önerilerine yer verilerek IoT paydaşlarının veri sorumlusu niteliği değerlendirilmiştir. Son olarak ise nesnelerin internetinin Türk hukukundaki yerine değinilerek 6698 sayılı Kişisel Verilerin Korunması Kanununun mehazı niteliğinde olan 95/46/EC sayılı Avrupa Birliği Direktifinin yerini alan Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında nesnelerin interneti kullanımına ilişkin değerlendirmelere yer verilmiştir.
Anahtar Sözcükler: Nesnelerin İnterneti, Kişisel Verilerin Korunması, Avrupa Birliği Genel Veri Koruma Tüzüğü.

Examination of the Internet of Things within the Scope of Personal Data Protection

ABSTRACT
The use of internet of things technology (IoT) has increased day by day with the use of new network technologies such as IPv6 and the development of identification technologies that allow objects to be addressed. In the scope of this study, first of all; the definition, purpose, history, application areas, components, architecture of the Internet of things are discussed. Then, the concerns expressed within the scope of personal data protection regarding the IoT technology and the solution proposals given by the 29 Working Group to the IoT stakeholders are provided, and whether IoT stakeholders are qualified as data controllers is evaluated. Finally, the place of the Internet of things in Turkish law has been mentioned and within the scope of the General Data Protection Regulation, which replaces the 95/46/EC Directive of the European Union that is taken as an example of the Law No. 6698 on Protection of Personal Data, evaluations related to the use of IoT have been included.
Keywords: Internet of Things, Protection of Personal Data, EU General Data Protection Regulation.

Atıf Gösterme	Ertan, A., (2022). Nesnelerin İnternetinin Kişisel Verilerin Korunması Kapsamında İncelenmesi, *Kişisel Verileri Koruma Dergisi. 4*(2), 48-68. DOI:

GİRİŞ

Günümüzde ağların ağı (network of networks) olarak da ifade edilen internetin iletişim kapasitesi ve hızının, ortaya çıktığı 1960'lı yıllar ile kıyaslandığında olağanüstü seviyelere ulaştığı görülmektedir. 1969 yılında ortaya çıkan ve sınırlı sayıda cihazın birbiri ile iletişime geçmesini sağlayan ve internetin temelini oluşturan (Abbate 1994: 2) ARPAnet ("Advanced Research Projects Agency Network") ile temelleri atılan ağ sistemi olan internete, 75.44 milyar nesnenin bağlı olacağı öngörülmektedir (Alam 2018: 450; Greengard 2021:10). Gelişen internet teknolojileri ise her türlü nesnenin internet ile bağlantı kurmasına imkân sağlamaktadır. Bu bağlamda "her yerden, herkesle, her nesneyle ve her zaman bağlantı" ilkesiyle gelişmekte olan nesnelerin interneti ("Internet of Things", "IoT") internet teknolojilerinde önemli bir yere sahiptir (Daş-Gündüz 2018: 334).

Bu çalışma kapsamında öncelikle nesnelerin internetinin tanımı, amacı, tarihçesi, uygulama alanları, bileşenleri ve mimarisine değinilecek olup nesnelerin interneti teknolojisine ilişkin olarak kişisel verilerin korunması kapsamında dile getirilen endişeler ile 29 Çalışma Grubu tarafından nesnelerin interneti paydaşlarına verilen çözüm önerilerine yer verilerek IoT paydaşlarının veri sorumlusu niteliği değerlendirilecektir. Son olarak ise nesnelerin internetinin Türk hukukundaki yerine değinilerek 6698 sayılı Kişisel Verilerin Korunması Kanununun mehazı niteliğinde olan 95/46/EC sayılı Avrupa Birliği Direktifinin yerini alan Avrupa Birliği Genel Veri Koruma Tüzüğü kapsamında nesnelerin interneti kullanımına ilişkin değerlendirmelere yer verilecektir.

NESNELERİN İNTERNETİNİN (INTERNET OF THINGS – IOT) TANIMI

Bazı kaynaklarda "Her Şeyin İnterneti" ("Internet of Everything", "IEO") olarak da ifade edilen nesnelerin interneti, fiziksel nesnelerin veri toplamasına ve değiş tokuş etmesine izin veren siber-fiziksel sistemler için yeni bir ağ paradigması olarak ifade edilmektedir (Chen-Chen 2016: 1). Aynı zamanda IoT, sensörleri, bilgi işlem aygıtlarını, algoritmaları ve benzersiz olarak tanımlanabilen şeyler olarak bilinen fiziksel nesneleri birleştiren, dağıtılmış bir bilgi işlem teknolojisi sistemidir. Bu nesneler, herhangi bir insan müdahalesi olmadan bağlı sistemler üzerinden veri toplama ve aktarma yeteneğine sahip olup özerk veri işleme yeteneğini haizdir. Çok sayıda sensör, aktüatör, cihaz ve veri deposu arasında bilgi akışına izin veren bir iletişim ağı, bir IoT sisteminin temel unsurlarından biridir (Khan, Yüce 2019: 1).

Nesnelerin interneti, veri depolama maliyetlerinin düşmesi, düşük maliyetli sensörler ile geliştirilmiş adresleme etiketleri, büyük veri analitiği yapabilen yazılımlarının geliştirilmesi ve IPv6 gibi internet adreslerinin yeni geliştirilen cihazlara bağlanmasını sağlayan teknolojiler sayesinde geliştirilmiştir (Gülşen 2019: 108). Düşük maliyetli sensör ve iletişim cihazlarının mevcudiyetinin yanı sıra karmaşık algoritmaların maliyet etkin bir şekilde uygulanmasını sağlayan akıllı yazılım tekniklerinin geliştirilmesiyle IoT'nin gelişimi de körüklenmiştir (Khan, Yüce 2019: 2).

Nesnelerin interneti kısaca adreslenebilme özelliğine sahip olan ve standart iletişim protokolleri üzerine kurulu nesnelerin, internet vasıtası ile haberleşebilmesi olarak tanımlanmaktadır (Daş-Gündüz 2018: 327).

Adreslenebilme özelliği; otomatikleşme üzerine kurulmuş olan verimliliğin artmasını sağlayan tanımlama teknolojilerinin bir başlığı olan AUTO-ID ("Automatic Identification", "Otomatik Tanımlama") teknolojileri ile sağlanır. AUTO-ID teknolojileri geniş bir yelpazeye sahip olsa da esas olarak RFID ("Radio-frequency Identification", "Radyo Frekansı Tanımlama") olduğu söylenebilir. Yine bu kapsamda ses tanıma teknolojisinden, biyometrik tanıma teknolojisine, akıllı kartlardan, sensörlere kadar kapsamlı bir yelpazenin olduğu belirtilmelidir. Bir çeşit ürün tanımlama standardı olan

EPC'nin ("Electronic Product Code", "Elektronik Ürün Kodu) (RFID etiketleri üzerine kodlanan benzersiz numaralar) tanıtılması ile birlikte ehemmiyet kazanan nesneler arasındaki iletişim, RFID teknolojisinin kullanılması ile beraber önem kazanmıştır (Sundmaeker-Guillemin, Friess-Woelffle 2010: 12).

Herhangi bir verinin elle girilmesine veya insan müdahalesine ihtiyaç olmaksızın nesnelerin veya makinelerin birbiri ile veri iletişiminde bulunduğu, bilgi topladığı ve toplanan bilgiler sayesinde karar verdiği bir ağ yapısı olarak tanımlanan (Aktaş-Çeken-Erdemli 2014: 300) nesnelerin interneti; denklemi, insan tabanlı veri girişinden hem insan hem de makine tabanlı veri girişine değiştirmiştir (Greengard 2015: 16).

"Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunmasına ve Serbest Veri Akışının Sağlanmasına İlişkin 95/46/EC sayılı Direktifin" ("Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data", "95/46/EC Sayılı Direktif") 29 uncu maddesi uyarınca kurulan "Kişisel Verilerin İşlenmesine Dair Bireylerin Korunması Hakkında Çalışma Grubu" ("Article 29 Working Party", "29 Çalışma Grubu", "WP29") danışma statüsüne sahip olup Direktifin nasıl uygulanacağına ışık tutan raporlar hazırlamıştır. IoT kavramı 29 Çalışma Grubu tarafından ortak, günlük cihazlara gömülü milyarlarca sensörün – "nesnelerin" veya diğer nesnelere veya bireylere bağlı şeylerin – verilerin işlenmesi, kaydedilmesi, depolanması ve aktarılması için tasarlandığı bir altyapı olarak tanımlanmıştır. Benzersiz tanımlayıcılarla donatılan nesneler, ağ yeteneklerini kullanarak diğer cihazlarla veya sistemlerle etkileşime girmektedirler. IoT, göze batmayan bir şekilde iletişim kurmak ve sorunsuz bir biçimde veri aktarımı yapmak için tasarlanmış olan sensörler aracılığıyla verilerin kapsamlı bir şekilde işlenmesi ilkesine dayandığından, "yaygın" ve "her yerde" bilgi işlem kavramlarıyla yakından bağlantılıdır (WP29 2014: 3).

NESNELERİN İNTERNETİNİN AMACI

Nesnelerin ağ yapısına dahil olması ve gerektiğinde birbiri ile iletişim kurması ile günlük hayatta kullanılan nesnelerin/cihazların da bu ağ yapısına dahil edilerek insan yaşamına katkı sağlanması amaçlanmaktadır. Örnek olarak bebek monitörleri, televizyonlar, panjur sistemleri, ev sunucu ve depoları vb. cihazların çevrimiçi olarak kontrolü verilmektedir (Daş-Gündüz 2018: 328).

Nesnelerin interneti kavramının amacı nesnelerin kendi arasında haberleşmesini sağlayarak ve bu veri akışı sayesinde anlamlı bilgi üreterek ve hatta kararlar alarak insan hayatını kolaylaştıran uygulamaların geliştirilmesidir. (Daş-Gündüz 2018: 327).

Örneğin; IoT sayesinde internet üzerinden web tabanlı bir hava durumu servisi ve nesne sahibi ile iletişime giren küçük bir gömülü cihaz içeren bir şemsiye yapılarak nesne sahibinin hayatı kolaylaştırılabilir. Şemsiyeye bilgi işlem ve iletişim amacıyla gömülü bir devre içeren şemsiye, internete bağlanır. Şemsiye düzenli olarak hava durumu raporunu yayınlayan bir web sitesi üzerinden her sabah bu raporları alır, verileri analiz eder ve işe gitme saatinde aralıklarla sahibine hatırlatıcılar verir. Hatırlatıcılar sayesinde nesne, sıcak ve güneşli günler için kırmızı, yağmurlu günler için sarı yanıp sönerek farklı renkli ledlerle iki durum birbirinden ayırt edilmesini sağlar. Şemsiye, NFC ("Near Field Communication" "Yakın alan iletişimi")[i], Bluetooth[ii] veya SMS teknolojilerini kullanarak sahibi işe gitmeden önce önceden belirlenmiş bir zamanda sahibinin cep telefonuna bir hatırlatıcı gönderir. Mesaj ise şu şekilde olabilir: (i) Kendinizi yağmurdan koruyun. Yağmur yağacak. Şemsiyeyi taşımayı unutmayın; (ii) Kendinizi güneşten koruyun. Sıcak ve güneşli olacak. Şemsiyeyi taşımayı unutmayın. Nesne sahibi, böylece şemsiyeyi taşımaya veya taşımamaya karar verebilir (Kamal 2017: 3).

Söz konusu şemsiye örneği nesnelerin internetinin kullanımına küçük bir örnek olsa da bu akıllı nesnelerin hayatımızın her alanına yayıldığını ve giderek daha da yaygınlaşacağını söylemek mümkündür. Tüm bu nesnelerin geliştirilme amacı ise insan hayatını kolaylaştırmaktır.

NESNELERİN İNTERNETİNİN TARİHÇESİ

İlk nesnelerin interneti uygulamasının, Cambridge Üniversitesinde bulunan bir grup akademisyenin, 1991 yılında bir kahve makinesinin görüntülerinin kameralı bir sistem ile internet üzerinden paylaşılması şeklinde olduğu ifade edilmekle (Gülşen 2019: 108) birlikte nesnelerin interneti kavramını terim olarak ilk kez 1999 senesinde MIT Auto-ID laboratuvarlarının kurucularından biri olan Kevin Ashton ileri sürmüştür (Sundmaeker-Guillemin, Friess-Woelffle 2010: 12; Aktaş-Çeken-Erdemli 2014: 300; Greengard 2021:9). Ashton çeşitli cihazları ve nesneleri birbirine bağlamak için RFID teknolojisini kullanmıştır (Greengard 2021:9).

Bilgisayar ağları ile RFID etiketleri sayesinde nesneleri birbirine bağlayan IoT'nin, terim olarak kullanılması ise Uluslararası Telekomünikasyon Birliğinin ("International Telecomunication Union", "ITU") 2005 yılındaki raporu sayesinde olmuştur (Sundmaeker-Guillemin, Friess-Woelffle 2010: 13).

1950'li yıllardan itibaren ilk kez akademik ve askeri iletişim sistemi olarak kullanılmaya başlanılan internet, 1960'lı yıllarda ARPANET ağının kurulması ile birlikte modern internet haline evrilmeye başlamıştır. 1980'li yılların sonunda Tim Berners-Lee, günümüzün interneti olarak da bilinen World Wide Web (WWW) üzerinde çalışarak modern internetin ortaya çıkmasına öncülük etmiştir. 1990'lı yıllarda ise internet akademik ya da askeri bir ağ olmaktan çıkarak sivil hale gelmiş ve forum ve blogların oluşturulabildiği, elektronik posta gönderilebildiği ve anlık mesajlaşmaların yapılabildiği bir platform olarak dönüşmüştür (Erdoğan 2018: 2).

Her ne kadar internetin kronolojik gelişimi önemli olsa da nesnelerin interneti bakımından gelişim aşamalarına göre sınıflandırılması daha önemlidir. İçeriğin sadece yer sağlayıcı tarafından üretildiği dönem olan Web 1.0, basit web olarak da ifade edilmektedir. İçeriğin yalnızca yer sağlayıcı tarafından üretilmesi nedeniyle bu dönemde internet siteleri yalnızca tek yönlü olarak bilgi aktarımında kullanılmakta; kullanıcılar sadece üretilen içerikleri görüntüleyebilmektedir. İçeriğin kullanıcılar tarafından da üretilebildiği dönem ise Web 2.0 olarak sınıflandırılmaktadır. Sosyal medya ve forum sitelerinin hayatımıza girdiği bu döneme sosyal web adı verilmektedir. İçeriğin yer sağlayıcı ve kullanıcı dışında bir yazılım tarafından üretileceği internet ise semantik web olarak da isimlendirilen Web 3.0'dır. Son olarak simbiyotik web olarak da isimlendirilen Web 4.0 ise nesneler arasında iletişim ağının bulunduğu dönemdir (Erdoğan 2018: 3; Raj-C.Raman 2017: 8).

İnternetin gelişim sürecinde nesnelerin dijital olarak internete bağlanması sonucunda içinde bulunduğumuz evrede nesnelerin çevrimiçi olarak birbirileri ile etkileşimleri sağlanmaktadır (Daş-Gündüz 2018: 327).

Nesnelerin interneti herhangi bir şirket veya kuruluş tarafından icat edilmediği gibi, hiç kimse nesnelerin internetini veya onun çalışma şeklini de tasarlamamıştır. Nesnelerin interneti sadece birbirine ve bilgisayar veri tabanlarına veri sağlayan, birbirine bağlı "şeyler"in oluşturduğu geniş bir ağıdır. Böylece, nasıl çalıştığı veya ne yaptığı konusunda basit bir standart yoktur. Esasında, IoT, küresel olarak birbirine bağlı bir ağ kuran protokollerin, standartların, platformların ve daha fazlasının bir konfederasyonudur (Greengard 2021: 15).

NESNELERİN İNTERNETİNİN UYGULAMA ALANLARI

Nesnelerin interneti pek çok alanda kullanılabilmektedir. Bu alanlar arasında akıllı ev, akıllı şehir (Samih 2019), bilimsel çalışma, enerji, endüstri, servis sağlayıcı, günlük kullanım (Sönmez-Çakır-Aytekin-Tüminçin 2018), güvenlik, imalat/üretim, kamu sektörü uygulamaları, tarımsal üretim (Dayıoğlu-Uğur-Türker 2016), taşımacılık (Koşunalp-Arucu 2018), çevre, ticaret uygulamaları (Chen-Chen 2016:1; Serpanos-Wolf 2018: 2-3), sağlık ve inşaat sayılabilir.

Ev ve binalarda; doğalgaz ve yangın algılayıcı sensörler, gözetleme ve alarm sistemleri, endüstride; optimizasyon, otomasyon, kalite kontrol ve test, enerji sektöründe; akıllı şebekelerin kullanımı, akıllı sayaçların kullanımı, ulaşımda; trafik izleme, sürücü ile araç arasındaki etkileşimin artırılması, otomasyon, akıllı park, çevre; bulut tabanlı hava izleme sistemleri, doğal afetlere karşı erken uyarı ve tedbir sistemleri vb. ve tarım sektöründe; tarımsal sulamada su tüketiminin azaltılması amacıyla su dağıtımının kontrollü yapılmasının sağlanması gibi uygulamalar örnek verilebilir.

Görüldüğü üzere, nesnelerin interneti teknolojisi pek çok alanda kullanılabilmekte olup hem kamu hem özel sektör bakımından hayati öneme sahip operasyonel bir değer haline gelmektedir.

NESNELERİN İNTERNETİNİN BİLEŞENLERİ

Nesne, veri, insan ve süreç bileşenlerinden oluşan nesnelerin interneti, bu bileşenleri bir arada değerlendirerek ülkelere, bireylere ve kurumlara pek çok hizmet bakımından farklı uygulama olanakları sağlamaktadır.

Nesne Bileşeni

Nesnelerin internetinin amacı internet aracılığıyla nesneleri birbiri ile haberleştirmek olduğundan her türlü nesne bu kapsamda değerlendirilebilir. Bu kapsamda nesnenin dahili bir sunucu ve harici bir çevre ile iletişimini sağlayacak gömülü bir sisteminin olması yeterlidir (Daş-Gündüz 2018: 329).

Veri Bileşeni

Veri ortamdaki herhangi bir şeye tayin edilen değer olarak tanımlanmaktadır (Daş-Gündüz 2018: 330). Veri aynı zamanda "bilgi, data (bilişim açısından) olgu, kavram ve komutların iletişim, yorum ve işlem için elverişli biçimli gösterimi" olarak da tanımlanmaktadır (Küzeci 2021: 13). Ancak verinin bazen tek başına bir anlam ifade etmeyebilecek olması nedeniyle ilişkilendirildiğinde, yorumlandığında, herhangi bir işleme tabi tutulduğunda veya başka bir şey ile kıyaslandığında daha anlamlı hale gelecektir. Anlamlandırılmış olan veri ise, bilgi (information/enformasyon) haline dönüşecektir. Bilgi anlaşıldığında veya uygulandığında ise "özbilgi (knowledge)" haline gelecektir (Daş-Gündüz 2018: 330).

Günümüzde, son on yılda, bir yılda üretilen verinin hacminin, bir hafta içerisinde üretildiği, IoT sayesinde internete bağlı durumda olmayan cihazların internete bağlanması nedeniyle bu veri miktarının daha da artacağı belirtilmektedir (Evans 2011: 3). Dijital ortamdaki tüm veriler ve bu verilerin analizi ise Büyük Veri (Big Data) olarak adlandırılmakta olup bu veriler log kayıtlarından, çevrimiçi sistemlerden, sosyal ağ etkileşimlerinden, sağlık kayıtlarından, arama sorgularından, mobil cihaz ve uygulamalardan, bilimsel verilerden elde edilmektedir (Daş-Gündüz 2018: 331).

İnsan Bileşeni

Kimsenin ulaşamadığı kadar çok miktardaki verinin tek başına bir anlam ifade etmeyecek olması nedeniyle uygun olan eylemin gerçekleştirilebilmesi için kararların alınıp bu verilerin insanlar tarafından kullanılabilecek faydalı bilgiler haline dönüştürülmesi gerekmekte olup verilerin insanlar tarafından kullanılabilmesi için verinin ortaya çıkarılması üç farklı etkileşim ile mümkün olmaktadır. Bunlar ise M2M (machine to machine) olarak da ifade edilen nesneler arası iletişim, M2P (machine to people) olarak ifade edilen nesne-insan etkileşimi ve P2P (people to people) olarak ifade edilen insan-insan etkileşimidir. (Daş-Gündüz 2018: 331).

Nesnelerin interneti uygulamaları kapsamında internetten elde edilen verilerden çıkarılan bilgilerden faydalanılıp insanların faydası için insan davranışlarını değiştirebilecek doğru ve zamanlı bilgi sağlanarak bir eylem gerçekleştirilir (Daş-Gündüz 2018: 331).

Süreç bileşeni

Nesnelerin internetindeki insan, veri ve nesne bileşenlerinin uyumlu çalışmasını ifade eden süreç bileşeni, bilginin doğru şeye / kişiye ve uygun şekilde ve doğru zamanda ulaştırılmasını sağlamaktadır. Süreç bileşeni sayesinde insan, veri ve nesne bileşenleri üç şekilde bir araya gelmektedir (Daş-Gündüz 2018: 331).

İlk olarak M2M Bağlantı olarak da ifade edilen ağ sistemindeki bir verinin bir nesneden/makineden diğer bir nesneye iletildiğinde gerçekleşen bağlantı şeklidir. Örnek olarak eve varmak üzere olan otomobil nesnesinin, ağında bulunan klima nesnesine komut yollayarak ev sıcaklığının sağlanmasıdır. Bilginin bir nesne ile insan arasındaki iletimini ifade eden bağlantı şekli ise M2P Bağlantı olarak ifade edilen bu bağlantıya akıllı park sistemleri örneği verilmektedir. Son olarak ise bağlantı bir kimseden diğer bir kimseye veri aktarımının gerçekleştiği bağlantı şekli olan P2P Bağlantıdır. Bu bağlantı şekline ise sosyal medya örneği verilmektedir (Daş-Gündüz 2018: 332).

NESNELERİN İNTERNETİNİN MİMARİSİ

Nesnelerin internetinin tanımı bölümünde de bahsedildiği üzere; nesnelerin interneti sadece birbirine ve bilgisayar veri tabanlarına veri sağlayan, birbirine bağlı “şeyler/nesneler"in oluşturduğu geniş bir ağ olup nasıl çalıştığı veya ne yaptığı konusunda basit bir standart bulunmamaktadır (Greengard 2021: 15). Bu sebeple her ne kadar söz konusu nesneler standart olarak birbirinin aynısı olmasa da hepsinde ortak olan bu nesnelerin her birinin, onu benzersiz bir tanımlayıcı (“Unique Identifier”, “UID”) ve bir IP adresi aracılığıyla diğer aygıtlara bağlayan bir yongaya sahip olmasıdır (Greegard 2021: 15).

Bu nesneler uydular, hücresel ağlar, Wi-Fi ve Bluetooth dahil olmak üzere kablolar ve kablosuz teknoloji aracılığıyla birbirine bağlanırlar. Yerleşik elektronik devrelerin yanı sıra çipler ve etiketler aracılığıyla gömülü veya daha sonra eklenen RFID veya yakın alan iletişimi (NFC) yeteneklerini kullanırlar.

Milyarlarca adreslenebilir nesnenin meydana getirdiği IoT, mevcut internet ağı üstünde çalışmaktadır. Bazı kaynaklarda IoT’nin mimari modellemesinin algılama, ağ ve uygulama katmanı olmak üzere üç katmandan oluştuğu ifade edilmektedir (Erdoğan 2018: 4) Bununla birlikte, nesnelerin internetinin tek tip bir çerçeveden yoksun olduğu, hala evrimleşerek son şeklini bulmaya çalıştığı, sürekli değişim ve gelişme içinde olan nesnelerin internetinin, üç, dört veya beş katmandan oluşan birkaç geçici etki alanına sahip olduğu; fakat, bu yapıların ortak bazı benzer özelliklerinin bulunduğu belirtilmektedir. En popüler IoT yapısının ise algılama katmanı, ağ katmanı ve uygulama katmanından oluştuğu ifade edilmektedir.

Bu çalışma kapsamında ise nesnelerin internetinin mimari modellemesi "aygıt/algılama/sensör katmanı", "ağ geçidi ve ağ katmanı", "servis ve uygulama destek katmanı/hizmet yönetimi katmanı" ve "uygulama katmanı" olarak dört katman olmak üzere dört başlık altında ele alınacaktır (Serpanos-Wolf 2018: 44). Nitekim Uluslararası Telekomünikasyon Birliği'nin nesnelerin interneti için belirlemiş olduğu referans modele göre de IoT'nin dört katmanı bulunmaktadır (Serpanos-Wolf 2018: 44).

Aygıt Katmanı (Device Layer), Algılama Katmanı (Perception Layer), Sensör Katmanı (Sensor Layer)

Sensör katmanı, aygıt katmanı veya algılama katmanı olarak adlandırılan ilk katmandır. Bu katman çevreyi algılayan, yararlı bilgiler elde etmek için işlenmek üzere bilgi toplayan sensörler ve aktüatörlerden oluşmaktadır. Bu katmana sıcaklık, hareket, nem, algılama olayları vb. gibi farklı türde sensörler yerleştirilebilir. Algılama katmanında veri dijitalleştirilir, güvenli kanal oluşturur ve bir sonraki katmana aktarılır. Bu katman, sonraki katmanlar tarafından işlenecek verilerin ana kaynağıdır (Agarwal, Alam 2020: 44-45).

IoT, fiziksel ortamın dijital ortam ile birbirine geçtiği ve fiziksel dünyadaki verilerin elde edilip dijital ortamda kullanıldığı bir teknoloji olup nesnelerin fiziksel ortamdan elde ettiği; nem, sıcaklık, kan basıncı, hız ve diğer her türlü durum değişiklikleri algılama katmanı yardımıyla sağlanmaktadır (Erdoğan 2018: 5; Gülşen 2019: 109; Greengard 2015: 14).

Ağ Geçidi ve Ağ Katmanı (Gateway and Network Layer)

Algılama katmanı olarak da ifade edilen aygıt katmanından temin edilen verilerin güvenilir bir şekilde iletilmesi, ağ katmanı sayesinde gerçekleştirilmektedir. Bunun gerçekleştirilmesi amacıyla fiziksel ortamda her bir nesnenin/cihazın adreslenmesi ve adreslenen nesnelerin/cihazların da dijital ortamda bir ağa bağlanması gerekmektedir (Erdoğan 2018: 6; Gülşen 2019: 109). Ağ katmanı, verilerin kapsüllenmesini ve ilgili protokollerin ağ katmanı protokollerine dönüştürülmesini sağlamaktadır (Serpanos-Wolf 2018: 45).

Ağ geçidi ve ağ katmanı, sensör katmanı tarafından güvenli kanallar aracılığıyla oluşturulan verileri yukarıdaki katmana aktarmaktadır. Zigbee, RFID, Wi-Fi vb. gibi çeşitli kablosuz teknolojiler bu katmanda veri iletmek için kullanılmaktadır. Ayrıca, verilerin depolanması ve işlenmesi bu katmanda gerçekleştirilir (Agarwal - Alam 2020: 45).

Servis ve Uygulama Destek Katmanı (Service Support and Application Support Layer), Hizmet Yönetimi Katmanı (Service Management Layer)

Hizmet yönetimi katmanı olarak da ifade edilen (Agarwal - Alam 2020: 45) servis ve uygulama destek katmanı, IoT uygulamalarını ve hizmetlerini etkinleştiren hem genel hem de hizmete/uygulamaya özgü işlevleri (yetenekleri) içermektedir. IoT servis ve uygulamalarının dağıtık yapısı göz önüne alındığında, verileri işleme ve depolama gibi genel bir işlevi olduğu gibi her servis ve uygulama bakımından özelleştirilmiş işlevleri de bulunmaktadır (Serpanos-Wolf 2018: 45).

Bu katman, IoT uygulaması programcılarının, temel donanımla ilgili herhangi bir endişe duymadan sorunsuz bir şekilde çalışmasını sağlayan özellikler sağlar. Ayrıca, bu katman alınan verileri işler, akıllı kararlar alır ve bu kararlara dayanarak hizmetleri protokoller aracılığıyla ağ üzerinden sunar. Akıllı kararlar vermek için bu katmanda çeşitli analitik çözümler uygulanabilmektedir (Agarwal-Alam 2020: 45- 46).

Uygulama Katmanı (Application Layer), Ara Yüz Katmanı, (Interface Layer)

Uygulama katmanı; algılama katmanı ve ağ katmanı üzerine kuruludur. Uygulama katmanı, büyük veri yönetiminin sağlandığı ve bunun için Peer-to-peer (P2P) ve Bulut Bilişim gibi teknolojiler kullanılarak makineler arası iletişimin (M2M), cihazlar arası iletişimin (D2D), cihaz-bulut arası iletişimin ve cihaz-ağ geçidi arası iletişimin gerçekleştirildiği katmandır (Erdoğan 2018: 6-7). Uygulama katmanı aynı zamanda ara yüz katmanı olarak da ifade edilmektedir (Gülşen 2019:109). Uygulama katmanı en üst hiyerarşik katman olarak kabul edilmektedir (Serpanos-Wolf 2018: 45).

Uygulama katmanı, kullanıcılarına istenen hizmetleri sağlar. Örneğin, uygulama katmanı, hastaya tıbbi bakım sağlayan kişiye, hastanın hızlanma ve kalp atışı değerlerini sağlayabilir. Bu katman, kullanıcının ihtiyacını karşılamak için üstün hizmetler sunma yeteneğine sahiptir. (Agarwal-Alam 2020: 46).

NESNELERİN İNTERNETİ VE KİŞİSEL VERİLERİN KORUNMASI

Nesnelerin İnternetinin Kişisel Verilerin Korunması Alanında Yarattığı Endişeler

Nesnelerin interneti teknolojisinin gelişmesi ile akıllı nesneler, insanların hayatlarını kolaylaştırma ve hayat standartlarını yükseltme amacıyla özel nitelikli ve kişisel pek çok veriyi kaydetmeye, işlemeye başlamıştır (Daş-Gündüz 2018: 333).

Mahremiyete ilişkin risk, sistemler, cihazlar ve veriler bağlantılı ve birbirine daha bağlı hale geldikçe artmaktadır. Kişisel bilgilerin veya görüntülerin istenmeyen bir şekilde kamuya maruz kalması, işletmeler ve hükümet tarafından yapılan dinlemeler ve verilerin nereye gittiğini veya nasıl kullanıldığını veya kötüye kullanıldığını bilememe bu risklerden belli başlılarıdır. Nesnelerin internetinin – ve içinde bulunan verilerin – karmaşıklığı ise verilerin açığa çıkabileceği veya sızabileceği birçok olası nokta yaratmaktadır (Greengard 2021: 191).

Bazı devlet kurumları bu endişeleri kabul etmeye ve ele almaya başlamıştır. En belirgin örnek, Avrupa Birliği'nin 2018 yılında yürürlüğe giren Genel Veri Koruma Tüzüğüdür (“European Union General Data Protection Regulation”, “GDPR”). GDPR, Avrupa Birliği vatandaşlarının kişisel verilerini işleyen kuruluşlar için katı kurallar, düzenlemeler ve cezalar getirmiştir. Kaliforniya’da ise 2020 yılında, IoT güvenliği ve gizliliğini doğrudan hedefleyen Kaliforniya Tüketici Gizliliği Yasası'nı (“California Consumer Privacy Act”, “CCPA”) yürürlüğe konulmuştur. CCPA, üreticilerin IoT cihazlarına “makul” güvenlik özellikleri eklemesini, Kaliforniya'da iş yapan şirketler için standartlar, ihlaller ve veri ihlalleri için cezalar eklemelerini şart koşmuştur. Büyük bir ihlal, ihlal başına 2.500 ila 7.500 ABD Doları para cezasına ve Kaliforniya Başsavcılığının eylemine neden olabilecektir (Greengard 2021: 192).

Yine de sensörler, makineler, kameralar, depolama ve veri işleme sistemlerinden gelen yeni veri kaynakları tarafından sıklıkla beslenen verilerin hacmi, çeşitliliği ve hızı arttıkça ihmal veya kötüye kullanım riskleri de artmaktadır. Sonuç olarak, veri işleyen kuruluşların veri kişiselleştirilmesi, verilerin tanımlanması ve verilerin yeniden tanımlanması ve nasıl depolandığı/saklandığı da dahil olmak üzere veri kalıcılığı gibi önemli sorunları ele almaları gerekmektedir (Greengard 2021: 192).

Aynı zamanda söz konusu riskler soyut değildir. Örneğin kişinin hareketini, kalp atış hızını ve diğer faktörlerini izleyen bir akıllı saat takan bir kişinin, doğru algoritmayla bir sağlık sorunu belirtileri gösterdiği tespit edilebilir. Bir işverenin bu verileri bir şekilde elde etmesi durumunda şirket bu kişiyi işten çıkarabilir. Yine söz konusu verileri elde edenin bir sigorta sağlayıcı olduğu varsayımında sigorta şirketi poliçeyi iptal edebilir veya kapsamını değiştirebilir. Belirli bir noktadan veya cihazdan iletilen veriler zararsız olabilir ve gizlilik konusunda çok az endişe kaynağı olabilir veya hiç endişe kaynağı

olmayabilir ancak birden fazla noktadan ve kaynaktan toplanan veriler kişi hakkında derin bilgiler sağlayabilir ve hassas bilgiler verebilir (Greengard 2021: 193).

İşaretçiler, sensörler, kameralar ve akıllı gözlükler her yerde bulunduğunda ve topladıkları veriler ağa bağlı bir dünyaya aktarıldığında, bir kişinin anında nerede olduğunu ve herhangi bir anda ne yaptığını belirlenmesi; davranış kalıplarının ve tüketim alışkanlıklarının kamusal bilgi haline gelmesi mümkündür (Greengard 2021: 193).

Nesnelerin interneti paydaşları (cihaz üreticileri, uygulama geliştiricileri, sosyal platformlar, diğer veri alıcıları, veri platformları ve standardizasyon kuruluşları), bireyler hakkındaki bu verilerin toplanması ve daha fazla birleştirilmesi yoluyla yeni uygulamalar ve hizmetler sunmayı amaçlamaktadır – ister kullanıcının çevreye özgü verilerini "sadece" ölçmek, ister alışkanlıklarını özel olarak gözlemlemek ve analiz etmek için olsun–. Başka bir deyişle, nesnelerin interneti genellikle tanımlanmış veya tanımlanabilir gerçek kişilerle ilgili verilerin işlenmesini ifade eder ve bu nedenle 95/46/EC sayılı Direktifin 2 nci maddesi anlamında kişisel veri işlenmesi olarak nitelendirilir (WP29 2014: 4). Ayrıca bu tür verilerin işlenmesi, önemli sayıda paydaşın koordineli müdahalesine dayanmaktadır (örneğin, cihaz üreticileri – bazen veri platformları olarak da işlev gören veri toplayıcıları veya brokerleri, uygulama geliştiricileri, sosyal platformlar vb.). Bu eylem zincirinin bir sonucu olarak IoT, cihaz üreticilerini ve ticari ortaklarını çok ayrıntılı kullanıcı profilleri oluşturmasına veya bunlara erişmesine imkân sağlayan bir konuma getirebilmektedir (WP29 2014: 4).

Tüm bunlar değerlendirilerek nesnelerin internetinin gelişiminin açıkça yeni ve önemli kişisel veri koruma ve gizlilik zorlukları gündeme getirdiği belirtilmektedir. IoT, güvenlik ihlalleri, verileri bu bağlamlarda işlenen bireyler için önemli gizlilik riskleri doğurabileceğinden önemli güvenlik kaygılarını da beraberinde getirmektedir. Bu nedenle 29 Çalışma Grubu, Avrupa Birliği vatandaşlarının temel haklarının söz konusu olduğu faaliyetlerden kaynaklanan risklerin belirlenmesine ve izlenmesine katkıda bulunmak için 16.09.2014 tarihli ve 2014/8 sayılı Görüşünü yayınlamıştır. Bu görüşte doğrudan kullanıcı ile etkileşime giren ve pazarda gelişmekte olan üç özel IoT gelişimine Giyilebilir Bilgisayar (Wearable Computing), Ölçülen Benlik (Quantified Self) ve Ev Otomasyonuna (Domotics) odaklanılmıştır.

29 Çalışma Grubu IoT ile ortaya çıkan gizlilik sorunlarını kontrol eksikliği ve bilgi asimetrisi, Kullanıcı Rızasının Kalitesi, Verilerden Elde Edilen Çıkarımlar ve Orijinal Verinin Yeniden Kullanılması, davranış kalıplarının ortaya çıkarılması ve profilleme, hizmetleri kullanırken anonim kalma olasılığının azalması olarak ifade edilmiştir. Bu kapsamda aşağıda, 29 Çalışma Grubu tarafından IoT ile ortaya çıktığı ifade edilen gizlilik sorunlarına değinilmeye çalışılacaktır.

Kontrol Eksikliği ve Bilgi Asimetrisi

Nesnelerin internetinin yaygın hizmetleri göze batmayan bir şekilde sunma özelliğinin bir sonucu olarak, kullanıcıların pratikte kendilerini üçüncü taraf izleme altında bulmakla kalmayıp kullanıcının verilerinin toplanması ve işlenmesinin şeffaf bir şekilde yapılıp yapılmayacağına bağlı olarak kişilerin verilerinin aktarılması üzerindeki tüm kontrolünü kaybetmesine yol açabileceği belirtilmiştir. Nesneler arasındaki etkileşimin kullanılan klasik araçlarla yönetilemeyen veri akışlarının oluşturulmasına neden olacağı ve nesnelerin nasıl etkileşimde bulunduğunu etkili bir şekilde kontrol etme veya belirli nesneler için aktif veya aktif olmayan bölgeleri tanımlayarak "sanal sınırları tanımlama olasılığının zorluğu"nun, oluşturulan veri akışını kontrol etmeyi olağanüstü derecede zorlaştıracağı, kişisel verilerin sonraki kullanımını kontrol etmenin daha da zor olacağı belirtilmiştir. Aynı zamanda bulut bilişim veya büyük veri gibi diğer teknik gelişmeleri de ilgilendiren bu kontrol eksikliği sorununun, ortaya çıkan bu farklı

teknolojilerin bir arada kullanılabilmesinin mümkün olduğu düşünüldüğünde daha da zorlayıcı olacağı öngörülmüştür (WP29 2014: 6).

Kullanıcı Rızasının Kalitesi

Nesnelerin interneti uygulamalarında çoğu durumda kullanıcı, nesnenin gerçekleştirdiği veri işleme faaliyetinden haberdar olmayabilecektir. Nitekim IoT'nin çalışma prensibi bunun üzerine kuruludur. Bu tür farkında olmama hali ve bilgi eksikliği, ilgili kişinin bilgilendirilmesi gerektiğinden, ilgili kişinin geçerli rızanın gösterebilmesinin önünde önemli bir engel oluşturmaktadır. Böylece bu durumun, ilgili kişilerin rızasını elde etmek için kullanılan klasik mekanizmaların IoT'de uygulanmasının, bilgi eksikliğine veya bireyler tarafından ifade edilen tercihlere uygun olarak spesifik (ince ayarlı) rıza sağlamanın gerçek imkansızlığı nedeniyle "düşük kaliteli" bir rıza ile sonuçlanabileceği öngörülmüştür. Bu kapsamda kullanıcının geçerli rızasını elde etmenin yeni yollarının – cihazların kendileri aracılığıyla rıza alma mekanizmalarının uygulanması da dahil olmak üzere – IoT paydaşları tarafından dikkate alınması gerektiği bildirilmiştir (WP29 2014: 7).

Verilerden Elde Edilen Çıkarımlar ve Orijinal Verinin Yeniden Kullanılması

Başlangıçta bir cihaz aracılığıyla toplanan görünüşte önemsiz verilerin (ör: ivmeölçer ve bir akıllı telefonun jiroskopu) daha sonra tamamen farklı bir veri (örneğin bireyin sürüş alışkanlıkları) üretilmesi için kullanılabilecektir. Nesnelerin interneti tarafından üretilen veri miktarının, veri analizi ve çapraz eşleştirme ile ilgili modern tekniklerle birlikte artmasının, kişisel verilerin orijinal işleme amacı ile ilgili olsun veya olmasın ikincil kullanımlarına yol açabilmesi mümkündür (WP29 2014: 7).

Ölçülebilen Benlik, veri toplama ve gelişmiş analiz yoluyla hareket sensörlerinden ne kadar bilgi çıkarılabileceğini de örnek oluşturmaktadır. Bu cihazlar genellikle ham verileri (örn. İlgili kişi kullanıcının hareketleri) yakalamak için temel sensörler kullanır ve mantıklı bilgileri (örn. adım sayısı) çıkarmak ve son kullanıcılara gösterilecek potansiyel olarak hassas bilgileri (örn. fiziksel durumu) çıkarmak için karmaşık algoritmalara sahiptir (WP29 2014: 7).

Kullanıcının orijinal bilgileri belirli bir amaç için paylaşmakta iradesi olsa da tamamen farklı amaçlar için kullanılabilecek bu ikincil bilgileri paylaşmak istemeyebileceği ve bu nedenle her seviyede (ham, ayıklanmış veya görüntülenen veriler), IoT paydaşlarının verilerin, işlemin orijinal amacı ile uyumlu amaçlar için kullanıldığından ve bu amaçların kullanıcı tarafından bilindiğinden emin olmalarının önemli olduğu belirtilmektedir (WP29 2014: 8).

Davranış Kalıplarının Ortaya Çıkarılması ve Profilleme

Farklı nesneler ayrı ayrı izole edilmiş bilgi parçalarını ayrı ayrı toplayacak olsa da toplanan ve daha fazla analiz edilen yeterli miktarda verinin, bireyin alışkanlıklarının, davranışlarının ve tercihlerinin belirli yönlerini ortaya çıkarabileceği; önemsiz ve hatta anonim verilerden bilgi üretmenin, sensörlerin çoğalmasıyla kolaylaşacağı ve nesnelerin profil oluşturma yeteneklerini geliştireceği belirtilmiştir. Bunun ötesinde, bir IoT ortamında yakalanan bilgilere dayanan analizlerin, ilgili kişi son kullanıcının yaşam ve davranış kalıplarının daha ayrıntılı tespit edilmesini sağlayabilecektir. Bu ise ilgili kişi kullanıcının gerçekte nasıl davrandığı üzerinde bir etki yaratabileceği belirtilerek video kameraların yoğun kullanımının vatandaşların kamusal alanlardaki davranışlarını etkilemesi örnek gösterilmiştir (WP29 2014: 8).

IoT ile, bu tür potansiyel gözetlemenin artık evler de dahil olmak üzere bireylerin yaşamının en özel alanına ulaşabileceği, bunun bireyin anormallik olarak algılanabilecek şeylerin tespit edilmesini

önlemek için olağan dışı davranışlardan kaçınma yönünde baskı altında hissedebileceği ve böyle bir eğilimin bireylerin özel hayatı üzerinde çok müdahaleci olacağı ifade edilmiştir (WP29 2014: 8).

29 Çalışma Grubunun 2014/8 sayılı görüşünü verdiği sırada yürürlükte olan 95/46/EC sayılı Direktifin 15 inci maddesinde doğrudan profilleme kavramına yer verilmese de GDPR'da buna yer verilmiştir.

Profil çıkarma GDPR'ın "Tanımlar" başlıklı 4 üncü maddesinin dördüncü fıkrasında bir gerçek kişinin işteki performansı, ekonomik durumu, sağlığı, kişisel tercihleri, ilgi alanları, güvenilirliği, davranışları, konumu veya hareketlerine ilişkin hususların analiz edilmesi veya tahmin edilmesi başta olmak üzere söz konusu gerçek kişiye ilişkin belirli kişisel özelliklerin değerlendirilmesi için kişisel verilerin kullanımını ihtiva eden her türlü otomatik kişisel veri işleme biçimi olarak tanımlanmıştır.

GDPR'ın 22 inci maddesine göre ise ilgili kişinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunmaktadır. 22 nci maddenin ikinci fıkrasında ise ilgili kişi ile veri sorumlusu arasında bir sözleşme yapılması veya yerine getirilmesi için gerekli olma, veri sorumlusunun tabi olduğu ve ilgili kişinin hak ve özgürlüklerini ve meşru çıkarlarını korumak için uygun önlemleri de belirleyen Avrupa Birliği veya Birliğe Üye Devletlerin hukuku tarafından yetkilendirilmesi veya ilgili kişinin açık rızası olması durumları bundan istisna tutulmuştur. Bu durumda kullanıcı rızasının kalitesi konusunda 29 Çalışma Grubunun belirttiği endişeler varlığını sürdürse de GDPR'ın 22 inci maddesinin ikinci fıkrasında düzenlenen diğer istisna durumlar bakımından otomatik işleme faaliyeti veya profilleme amacına dayalı kişisel veri işleme faaliyeti gerçekleştirilerek kişi hakkında otomatik bir karar verilebilecektir.

Hizmetleri Kullanırken Anonim Kalma Olasılığının Azalması

IoT'nin yeteneklerinin tam olarak geliştirilmesi, hizmetlerin anonim kullanımı olanağı üzerinde bir yük oluşturmasına ve ilgili kişilerin söz konusu hizmetleri kullanırken fark edilmeden kalma olasılığının sınırlanmasına neden olabileceği, anonim kalmanın ve kişinin IoT'deki gizliliğini korumanın giderek zorlaşacağı, nesnelerin internetinin gelişiminin, bu konuda önemli veri koruma ve gizlilik kaygıları doğurduğu belirtilmektedir (WP29 2014: 8).

IoT Paydaşlarının Veri Sorumlusu Niteliği ve İlgili Kişi

IoT'nin gelişiminde cihaz üreticilerinden uygulama geliştiricilere kadar pek çok paydaş yer almaktadır. Her ne kadar nesnelerin internetinin karmaşık yapısı nedeniyle ilgili kişinin mahremiyetinin ve kişisel verilerinin korunmasını sağlamanın mümkün olamayabileceğine hem halihazırdaki endişelere yer verilip hem de geleceğe yönelik endişelere değinilse de GDPR'ın 3 üncü bölümünde düzenlenen ilgili kişinin haklarının korunabilmesi için kişisel veri işleme faaliyetini gerçekleştiren veri sorumlularının tespiti gerekmektedir. Nitekim ilgili kişinin söz konusu haklarını yöneltebileceği veri sorumlusunu tespit edebilmesi önemlidir.

IoT paydaşların karmaşık ağı, bireyin kişisel verilerinin işlenmesiyle ilgili olarak, kendi müdahalelerinin özelliklerine dayanarak, aralarında yasal sorumlulukların kesin bir şekilde tahsis edilmesini gerektirmektedir. Bu çerçevede cihaz üreticileri, sosyal platformlar, üçüncü taraf uygulama geliştiricileri, cihaz üreticileri ve üçüncü taraf uygulama geliştiricileri dışındaki üçüncü taraflar ve IoT veri platformlarının niteliği değerlendirilecektir.

Cihaz Üreticileri

Nesnelerin internetinde cihaz üreticileri, yalnızca fiziksel ürünleri müşterilerine veya beyaz etiketli ürünleri diğer kuruluşlara satmaktan fazlasını yaparlar. Ayrıca, "nesnenin" işletim sistemini geliştirmiş veya değiştirmiş veya verilerin ne zaman ve kime hangi amaçlarla iletileceği, veri toplama sıklığı dahil olmak üzere genel işlevselliğini belirleyen bir yazılım yüklemiş olabilirler. Cihaz üreticilerinin çoğu, cihaz tarafından oluşturulan kişisel verileri, tamamen kendi belirledikleri amaçlar için kendi belirledikleri araçlar ile toplar ve işler. Bu nedenle cihaz üreticileri veri sorumlusu olarak nitelendirilebilecektir (WP29 2014: 11).

Sosyal Platformlar (Sosyal Ağlar)

İlgili kişilerin IoT'deki verileri kamuya açık olarak veya diğer kullanıcılar paylaşabilmesi olasıdır. Özellikle, Ölçülebilir Benlik cihazlarının kullanıcıları, grup içinde bir tür olumlu rekabeti teşvik etmek için bu tür verileri sosyal ağlarda başkalarıyla paylaşma eğilimindedir (WP29 2014: 11).

Sosyal ağlarda "nesneler" tarafından toplanan verilerin bu şekilde paylaşılması, kullanıcı uygulamayı bu anlamda yapılandırmasından sonra genellikle otomatik olarak gerçekleşmektedir. Sonrasında ise paylaşım özelliği genellikle üretici tarafından sağlanan uygulamaların standart varsayılan ayarlarına göre değişir (WP29 2014: 11).

Bu kişisel verilerin sosyal platformlarda toplanması, belirli kişisel verilerin korunmasına ilişkin bazı sorumluluklarının artık onlar için geçerli olduğu anlamına gelecektir. Bu veriler kullanıcı tarafından sosyal platformlara aktarıldığından, sosyal platform tarafından kendi belirledikleri farklı amaçlar için işlendiklerinde sosyal platformlar da veri sorumlusu olarak nitelendirilecektir. Örneğin, bir sosyal ağ, belirli bir kullanıcının düzenli bir koşucu olduğu ve koşu ayakkabılarıyla ilgili reklamlarını gösterdiği sonucuna varmak için bir adımsayar tarafından toplanan bilgileri kullanabilir. Bu durumda sosyal ağ bu kişisel veri işleme amacı doğrultusunda söz konusu veriler bakımından veri sorumlusu niteliğini haiz olacaktır (WP29 2014: 11-12).

Üçüncü Taraf Uygulama Geliştiricileri

Birçok sensör, uygulama geliştirmeyi kolaylaştırmak amacıyla API'leri[iii] ("Application programming interface", "Uygulama programlama arayüzü") kullanır. İlgili kişilerin bu uygulamaları kullanmak için, cihaz üreticisi tarafından depolandığı şekilde, verilerine erişmelerini sağlayan üçüncü taraf uygulamaları da yüklemeleri gerekmektedir. Bu uygulamaları yüklemek genellikle uygulama geliştiricisine API aracılığıyla verilere erişim sağlamak anlamına gelmektedir. Bazı uygulama geliştiricileri belirli nesnelerin interneti kullanıcılarını ödüllendirebilir. Örneğin bir ev sigortası şirketi müşterilerinin yangın alarmlarının doğru şekilde yapılandırıldığından emin olmak için belirli bir uygulama geliştirebilir. Bu veriler uygun şekilde anonimleştirilmediği sürece, bu erişim hem yürürlükten kaldırılan 95/46/EC Sayılı Direktifin 2 nci hem de GDPR'ın 2 nci maddesi kapsamında bir kişisel veri işleme faaliyeti sayılır. Bu nedenle söz konusu verilere erişim sağlayan uygulama geliştiricisi, veri sorumlusu niteliğini haiz olur. Bu tür uygulamalar genellikle isteğe bağlı olarak yüklenir ve kullanıcının rızasının alınması gerekir. Bu durumda ise bu rızanın ilgili kişinin tarafından açıkça verilmesi, spesifik olması ve ilgili kişinin rızası hakkında veri sorumlusu tarafından bilgilendirilmesi gerekir (WP29 2014: 12).

Diğer Üçüncü Taraflar

Cihaz üreticileri ve üçüncü taraf uygulama geliştiricileri dışındaki üçüncü tarafların da bireyler hakkında bilgi toplamak ve işlemek için IoT nesnelerini kullanabilmesi mümkündür. Örneğin, sağlık sigortala

şirketleri müşterilerinin ne sıklıkta egzersiz yaptığını izlemek ve sigorta primlerini buna göre uyarlamak için müşterilerine pedometre vermek isteyebilirler. Cihaz üreticilerinin aksine, bu tür üçüncü tarafların nesne tarafından toplanan veri üzerinden hiçbir kontrolü olmamakla birlikte, bu tür IoT cihazları tarafından üretilen verileri kendi belirledikleri belirli amaçlar için toplayıp depoladıkları durumda söz konusu kişisel veri işleme faaliyeti bakımından veri sorumlusu sıfatını haiz olurlar (WP29 2014: 12).

IoT Veri Platformları

Standardizasyon ve birlikte çalışabilirlik eksikliği nedeniyle, nesnelerin interneti bazen her üreticinin kendi arayüz ve veri formatı kümesini tanımladığı bir "Nesnelerin İntraneti" olarak görülmektedir (WP29 2014: 12). Nitekim tek kullanıcı tarafından farklı üreticilerin ürettiği IoT nesnelerinin kullanılabilmesi mümkündür.

Bu durum kullanıcıların verilerini bir cihazdan diğerine aktarmalarını (hatta birleştirmelerini) etkili bir şekilde önlemektedir. Bununla birlikte, akıllı telefonlar ve tabletler, birçok IoT cihazı aracılığıyla internete toplanan verilerin doğal ağ geçitleri haline gelmiştir. Sonuç olarak, üreticiler, yönetimlerini merkezileştirmek ve basitleştirmek için bu tür farklı cihazlar aracılığıyla toplanan verileri barındırmayı amaçlayan platformlar geliştirmişlerdir. Bu tür platformlar ise kullanıcıların kişisel verilerini kendi amaçları için işlediklerinde ise veri sorumlusu olarak nitelendirilebilmeleri mümkündür (WP29 2014: 13). Bu platformlara IBM Watson IoT Platformu örnek olarak verilebilir. IBM Watson IoT Platformu, nesnelerin interneti aygıtlarından değer elde etmeyi kolaylaştıran, tamamen yönetilen, bulutta barındırılan bir hizmettir (IBM).

İlgili Kişi Olarak Bireyler: Aboneler, Kullanıcılar ve Kullanıcı Olmayanlar

Aboneler ve daha genel olarak IoT kullanıcıları ise nesnelerin interneti uygulamaları bakımından ilgili kişi olarak nitelendirilecektir. İlgili kişilerin topladığı ve muhafaza ettiği veriler münhasıran kendi kişisel veya evsel amaçları için kullanıldığı takdirde, söz konusu veri işleme faaliyeti mülga 95/46/EC Sayılı Direktif ve GDPR'da "Hanehalkı Muafiyeti" olarak isimlendirilen muafiyet kapsamına girecektir (WP29 2014: 13).

Bununla birlikte, uygulamada, IoT'nin iş modeli, kullanıcının verilerinin sistematik olarak cihaz üreticilerine, uygulama geliştiricilerine ve veri sorumlusu olarak nitelendirilen diğer üçüncü taraflara aktarılmasını beraberinde getirmektedir. Bu nedenle, "Hanehalkı Muafiyeti", nesnelerin interneti bağlamında sınırlı bir uygulamaya sahip olacaktır. Nesnelerin internetindeki verilerin işlenmesi, Nesnelerin internetinin abonesi ya da gerçek kullanıcısı olmayan ilgilendirebilmesi mümkündür. Örneğin, akıllı gözlükler gibi giyilebilir cihazlar tarafından, cihazın sahibi dışındaki diğer ilgili kişiler hakkında veri toplaması muhtemeldir. Bu durumda her ne kadar kişi nesnenin sahibi veya kullanıcısı olmasa da söz konusu nesne tarafından toplanılan veriler bakımından ilgili kişi niteliğini haiz olacaktır (WP29 2014: 13).

Kişisel Verilerin Korunması Bakımından IoT Paydaşlarına Öneriler

29 Çalışma Grubunun 2014/8 sayılı Görüşünde tüm IoT paydaşlarına kişisel verilerin korunması bakımından belli ortak öneriler sıralanmıştır. Bunlar: IoT'de yeni uygulamalar başlatılmadan önce Mahremiyet Etki Analizi[iv] ("Privacy Impact Assesment") yapılması, kişisel veri işleme faaliyeti sırasında elde edilen ham verilerden gerekli veriler çıkarıldıktan sonra ham verilerin silinmesi, tasarım gereği gizlilik ("privacy by design") ve varsayılan olarak gizlilik ("privacy by default") ilkelerinin uygulanması, ilgili kişilerin kendi verilerinin kontrolüne sahip olmasının sağlanması, bilgi verme, reddetme hakkı sunma ve rıza isteme yöntemlerinin mümkün olduğunca kullanıcı dostu hale getirilmesi

ve cihazlar ve uygulamaların kullanıcı ve kullanıcı olmayan ilgili kişileri bilgilendirecek şekilde – örneğin cihazın fiziksel arabirimi üzerinden veya kablosuz bir kanalda bir sinyal yayınlayarak – tasarlanmasıdır. Aynı zamanda söz konusu görüşte işletim sistemi ve cihaz üreticileri, uygulama geliştiricileri, sosyal platformlar, IoT cihaz sahipleri, standardizasyon kuruluşları ve veri platformları bakımından da özel nitelikte öneriler sıralanmıştır (WP29 2014: 21-24). Ancak söz konusu önerilere çalışmanın kapsamını genişletecek olması nedeniyle yer verilmemiştir.

NESNELERİN İNTERNETİNİN TÜRK HUKUKUNDAKİ YERİ

Stratejik Planlar

Her ne kadar IoT gibi ilerlemeye açık bir teknolojinin uluslararası toplumda dahi yönetişim ve düzenleme bakımından tam olarak yerleşememiş olması ve nesnelerin interneti teknolojisinin henüz Türkiye'de yaygınlaşmamış olması bu konuda Türkiye'de herhangi bir düzenlemenin mevcut olmaması sonucunu doğurmuş (Erdoğan 2018: 126) olsa da pek çok kamu kurumu tarafından yayımlanan stratejik planda nesnelerin internetinin yaygınlaştırılmasına dair hedefler konulmaktadır. Bu kapsamda Bilgi Teknolojileri ve İletişim Kurumunun "2019-2023 Stratejik Planı"nda (BTK 2017), Çevre, Şehircilik ve İklim Değişikliği Bakanlığı'nın "Nesnelerin İnterneti – Akıllı Şehirler Kapasite Geliştirme ve Rehberlik Projesi" (Çevre, Şehircilik ve İklim Değişikliği Bakanlığı 2020) ve Sanayi ve Teknoloji Bakanlığı'nın "2023 Sanayi ve Teknoloji Stratejisi"nde nesnelerin internetinin yaygınlaştırılmasına ilişkin hedeflere yer verildiği görülmektedir (Sanayi ve Teknoloji Bakanlığı 2019).

Aynı zamanda 04.11.2019 tarih ve 30938 (Mükerrer) sayılı Resmî Gazetede yayımlanan 2020 Yılı Cumhurbaşkanlığı Yıllık Programının Onaylanması Hakkında Kararda (Karar Sayısı: 1733) nesnelerin internetinin yaygınlaştırılması amacıyla teşvik programlarının düzenlenmesine ilişkin kararlara yer verilmiştir. Bunlar; Rekabetçi Üretim ve Verimlilik başlığı altında yer alan Sanayi Politikalarına ilişkindir. Buna göre KOSGEB tarafından KOBİ Gelişim Destek Programı kapsamında 2019'da "İmalat Sanayinde Dijitalleşme" temalı iki proje teklif çağrısı ilan edildiği belirtilerek imalat sanayii özelinde, büyük veri, nesnelerin interneti, otonom robot teknolojileri, akıllı sensör teknolojileri, yapay zekâya dayalı siber fiziksel akıllı fabrika sistem ve bileşenleri ile siber güvenlik olmak üzere altı akıllı dijital teknoloji konusu bu proje teklif çağrılarının kapsamına dâhil edilmiştir. Aynı zamanda nesnelerin interneti "Kritik Teknolojiler"den biri olarak sayılmış ve bu kapsamda politikalar belirlenmiştir. Yine aynı şekilde Kamu Hizmetlerinde e-Devlet Uygulamaları başlığında ise belirlenen tedbirlerden birini diğer teknolojik gelişmelerin yanı sıra nesnelerin interneti teknolojilerinden yararlanılabilmesi için süreç ve teknolojik altyapı iyileştirmelerinin yapılması oluşturmaktadır.

Üniversiteler Bünyesinde Gerçekleştirilmesi Planlanan Bilimsel Çalışmalar

Ayrıca, 27.06.2021 tarih ve 31524 sayılı Resmi Gazetede yayımlanan Kahramanmaraş Sütçü İmam Üniversitesi Bilgisayar Uygulama ve Araştırma Merkezi Yönetmeliği'nin 6 ncı maddesinin birinci fıkrasının (c) bendinde; 12.04.2021 tarih ve 31452 sayılı Resmi Gazetede yayımlanan İzmir Kâtip Çelebi Üniversitesi Akıllı Fabrika Sistemleri Uygulama ve Araştırma Merkezi Yönetmeliği'nin 5 inci, 6 ncı ve 14 üncü maddelerinde; 07.03.2021 tarih ve 31416 sayılı Resmi Gazetede yayımlanan İzmir Kâtip Çelebi Üniversitesi Yapay Zeka ve Veri Bilimi Uygulama ve Araştırma Merkezi Yönetmeliğinin 14 üncü maddesinde; 06.02.2021 tarih ve 31387 sayılı Resmi Gazetede yayımlanan Kütahya Dumlupınar Üniversitesi Akıllı Sistemler Tasarım Uygulama ve Araştırma Merkezi Yönetmeliği'nin 5 ve 6 ncı maddelerinde; 20.05.2019 tarih ve 30779 sayılı Eskişehir Osmangazi Üniversitesi Tasarruf Ekonomisi ve Sürdürülebilirlik Uygulama ve Araştırma Merkezi Yönetmeliği'nin 5 inci maddesinde ve 18.03.2019 tarih ve 30718 sayılı Resmi Gazetede yayımlanan Düzce Üniversitesi Elektrikli Araçlar ve Dijital

Dönüşüm Uygulama ve Araştırma Merkezi Yönetmeliği'nin 6 ncı maddesinde nesnelerin interneti uygulamalarının geliştirilmesine yönelik amaçlar konulduğu görülmektedir.

Nesnelerin İnternetine İlişkin Yasal Düzenlemeler

Anılan stratejik planlar ve kalkınma planlarında belirlenen hedefler yönünden nesnelerin interneti teknolojisinin kullanımının yaygınlaşması asıl önemini, nesnelerin internetine yönelik ne tür yasal düzenlemelerin gerçekleştirileceği ve bu ilgili düzenlemelerin hangi metoda dayanarak oluşturulacağı noktasında göstermektedir. Nitekim teknolojinin her geçen gün gelişmesi karşısında hukuk düzeninin bu gelişmelerin doğurduğu ihtiyaçlara cevap verebilecek konumda olmak zorunda olması kanun koyucunun ise bu kapsamda tam bir ikilem içinde kalmasına neden olacaktır.

Kanun koyucu yeni teknolojilerin bütün sonuçlarını analiz etmeden hızlı bir biçimde hukuki düzenleme çıkartırsa bu düzenlemenin inovasyonun önünü kesebileceği ve toplumun refahına katkı sağlayacak bir gelişimin önüne geçebileceği gibi, öte yandan tamamen hareketsiz kalması durumunda ise bireyleri koruma yükümlülüğünü gereği gibi yerine ifa edememe riski ile karşılaşılabilir. Collingridge ikilemi olarak ifade edilen bu durum David Collingridge tarafından kontrol ikilemi olarak tanımlanmaktadır (Çekin 2021: 30-31).

Yeni gelişen teknolojilere yönelik olarak üç ayrı düzenleme modelinin ele alınması gerektiği ve bunların "Öz Düzenleme" (Self-Regulation), uluslararası yasal çerçevenin çizilmesi ve devlet mevzuatının belirlenmesi olduğu belirtilmektedir (Erdoğan 2018: 80). Nesnelerin interneti teknolojisine yönelik olarak ise kişisel verilerin korunması kapsamında ulusal düzenlemelerle söz konusu alan regüle edilmeye çalışılmaktadır.

Avrupa Birliğinde gelişen ve giderek yaygınlaşan bir teknoloji olan nesnelerin internetine ilişkin yasal düzenleme halihazırda kişisel verilerin korunması bakımından tüm Avrupa Birliği üye ülkelerinde doğrudan yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğüdür. Nitekim "Nesnelerin İnterneti ve Kişisel Verilerin Korunması" bölümünde de ifade edildiği üzere söz konusu nesneleri kullanan ilgili kişilerin profilleme ve davranış kalıplarının çıkarılması gibi özel hayatın gizliliğini ihlaline kadar ihtimaller söz konusu olabilmektedir. Her ne kadar kişisel verilerin korunmasına ilişkin endişelerin çok fazla olduğu görülse de doğrudan söz konusu gelişimin önünün kesilmeye çalışılmadığı görülmekle birlikte gelişen teknoloji karşısında kişisel verilerin korunması suretiyle bireylerin korunmaya çalışıldığı görülmektedir.

Türkiye'de ise her ne kadar Avrupa Birliği üye ülkelerindeki kadar olmasa da nesnelerin interneti kullanımının yaygınlaşmaya başladığı görülmektedir. Avrupa Birliğinde de görüldüğü üzere nesnelerin internetinin yaygınlaşması karşısında bireylerin korunabilmesi kişisel verilerin korunması yoluyla olabilecektir. Bu kapsamda 07.04.2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanununa ("6698 sayılı Kanun") değinilmesinde fayda görülmektedir. 6698 sayılı Kanunun "Tanımlar" başlıklı 3 üncü maddesinin birinci fıkrasının (ç) bendinde ilgili kişi; kişisel verisi işlenen gerçek kişiyi, (d) bendinde kişisel veri; kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi, (e) bendinde kişisel verilerin işlenmesi; 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 işlemi, (ı) bendinde veri sorumlusu; kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişi olarak tanımlanmıştır.

Bu kapsamda GPDR çerçevesinde veri sorumlusu olarak tasnif edilen IoT paydaşları 6698 sayılı Kanun kapsamında da veri sorumlusu niteliğini haizdir. Her ne kadar 6698 sayılı Kanunda, GDPR'ın 22 nci maddesinde yer verilen profillemeye ilişkin düzenleme yer almasa da 6698 sayılı Kanunun "İlgili kişinin hakları" başlıklı 11 inci maddesinin birinci fıkrasının (g) bendinden ilgili kişinin işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme hakkı düzenlenmiştir.

GDPR KAPSAMINDA IOT KULLANIMINA İLİŞKİN YAPILAN DEĞERLENDİRMELER

IoT, hızla büyüyen bir teknoloji sektörü olup Avrupa Birliği'ndeki gelişimi benimsenmesi sağlık, kamu hizmetleri, şehir planlama ve yönetim, lojistik ve tedarik zinciri yönetimi, tarım ve ticaret gibi alanlarda görülebilir. IoT nesneleri ve hizmetleri tarafından büyük miktarda kişisel veri ile kullanım verileri toplanmakta ve paylaşılmaktadır (Wachter 2018: 266-267). Çok sayıda gizlilik riski oluşturan IoT'nin gerçekleştirdiği kişisel veri işleme faaliyeti, "kusursuz" bir deneyim sağlamak için sıklıkla kullanıcılar tarafından fark edilmeyecek şekilde gerçekleştirilmektedir. Nesnelerin internetinin çıkarımsal analitik kişiselleştirmeye yönlendirilebilmesi nedeniyle potansiyel olarak ayrımcı kararlar verilmesine sebep olabilecektir. IoT'nin kesintisiz ve şeffaf olmayan doğası ile gizlilik tehditlerine karşı koruma sağlamak için kullanıcıların bilgilendirilmesi ile kişisel verilerinin toplanması ve işlenmesinin kontrol altında tutulması arasında temel bir gerilim bulunmaktadır (Wachter 2018: 267). GDPR, tanımlama teknolojilerinin oluşturduğu risklerle ilgili çok sayıda hüküm içermekle birlikte, GDPR'daki yasal gereklilikler, kullanıcıların gizlilik konusundaki çıkarları ile IoT geliştiricilerinin ve veri sorumlularının çıkarları arasında adil bir denge kurulmasını sağlamak için yetersiz olabilecektir (Wachter 2018: 268).

IoT'de tanımlamayı sağlamak için kişisel verilerin kapsamlı bir şekilde toplanması ve kesintisiz bağlanmasının gerekliliği göz önüne alındığında, veri koruma yasaları özellikle önem arz etmektedir. IoT'deki tanımlama teknolojilerinin getirdiği gizlilik riskleri bağlamında, GDPR, kişisel verilerin işlendiği tüm sektörlerdeki uygulanabilirliği ve geniş coğrafi etkisi nedeniyle özellikle ilgili bir yasal çerçeve olmakla birlikte, IoT profili oluşturma ve tanımlama teknolojilerinin kullanıcı gizliliği üzerindeki etkisini en aza indirmek için IoT teknolojilerinin tasarımı ve dağıtımına ilişkin daha fazla hukuki düzenlemenin yürürlüğe konulmasının uygun olacağı, ayrıca, GDPR kapsamında anahtar kavramların belirsiz veya tanımsız bırakıldığı, bu doğrultuda, ilgili kişilerin gizlilikle ilgili çıkarlarının ve IoT hizmetlerinin belirlenmesi ve sağlanmasında veri sorumlularının çıkarlarının nasıl dengeleneceği konusunda belirsizlik oluşabileceğine yönelik görüşler belirtilmiştir. Veri sorumluları IoT'de arka planda çalışmak üzere tasarlanmış işletim sistemleri ile kullanıcıların veri koruma standartlarına göre bilgilendirilmesi ve ilgili kişilerin verilerinin kontrolünü ellerinde tutması konularında zorluklar yaşamaktadır (Wachter 2018: 270).

İlk olarak, IoT olabildiğince çok veri elde edilmesine yönelik olup, veri koruma hukukunda yer alan veri minimizasyonu ilkesi ile çatışmaktadır. İkinci olarak, kullanıcıların profilini çıkarmak ve kişiselleştirilmiş hizmetler sağlamak için kullanılan karmaşık çıkarımsal analizler, ilgili kişiler hakkında öngörülemeyen korelasyonları ve bilgileri ortaya çıkarabilir. Üçüncü olarak ise, veri sorumlularına dayatılan aydınlatma yükümlülüğü, şeffaflık sağlamak için yetersiz olabilmektedir (Wachter 2018: 271). IoT'nin gizlilik riskleri ile GDPR'ın IoT ile ilgili temel hükümlerindeki netliğin eksikliği göz önüne alındığında, ileriye dönük olarak "gizlilik" ve "tanımlanabilirlik" arasında yasal açıdan uyumlu olan ancak ilgili kişiler için etik açıdan istenmeyen bir durum sağlayan cihazlara ve hizmetlere maruz kalınabilir (Wachter 2018: 272). Bu kapsamda, GDPR'ın yasal veri işlemeye ilişkin ilkeleri, IoT'de "gizlilik" ve "tanımlanabilirlik" arasındaki gerilimleri çözmek için bir temel sağlayabilecektir.

Hukuka uygun, adil ve şeffaf olma ilkesi veri sorumlularının kişisel verilerin işlenmesi için meşru gerekçelere sahip olma yükümlülüklerini açıklamaktadır. Adillik ilkesi tanımlanmamış olsa da 29

Çalışma Grubu ve akademisyenler, adilliğin farkındalıkla bağlantılı olduğunu, yani ilgili kişilerin veri işlemeden haberdar edilmesi gerektiğini düşünmektedir. Bu, özellikle IoT geliştiricileri için önemlidir çünkü nesneler genellikle büyük miktarda kişisel veri toplar ve bunlardan bazıları hassas kabul edilebilir. Ayrıca, kusursuz veri toplama, ilgili kişilere kişisel verilerinin toplandığını unutturabilir.

Amaçla sınırlı olma ilkesi, veri sorumlularının toplanan verileri yalnızca belirli ve iyi tanımlanmış amaçlar için kullanma yükümlülüğüne atıfta bulunur. Toplanan verilerin başka amaçlarla kullanılması ilkiyle uyumlu olmalıdır. Bu ilke, IoT için zorluklar oluşturabilir. Çoğu zaman, belirsiz veya geniş tanımlanmış amaçlar için büyük miktarda veri toplanmaktadır. Veri sorumlularının yalnızca "yeterli, ilgili ve işlendikleri amaçlarla ilgili olarak gerekli olanlarla sınırlı" verileri kullanmaları gerekmektedir.

Veri sorumlularının doğru verileri depolaması ve kullanması gerekir. Doğruluk, verilerin "işlendikleri amaçlarla" ilgili olarak doğru ve eksiksiz olması ihtiyacını ifade eder. Sonuç olarak, IoT geliştiricileri bu gereksinimi karşılamak için veri kümelerini seçmek ve güncellemek konusunda önemli bir zorlukla karşı karşıyadır. Dolayısıyla, kullanıcı kimliğinin doğrulanması, özellikle birden fazla kişi potansiyel olarak aynı cihazı kullanabildiği durumda çok önemlidir. Doğrulama olmadan, birden çok kullanıcıdan gelen kullanım verilerinin yanlışlıkla tek bir kullanıcının profili altında kaydedilebilmesi hatalı işlemeye yol açabilecektir (Wachter 2018: 273-274).

Saklama sınırlaması ilkesi, veri sorumlularını kişisel verileri "kişisel verilerin işlendiği amaçlar için gerekenden daha uzun süre" saklamamakla yükümlü kılmaktadır. IoT'de, belirli bir ürün veya hizmetin amacı için depolanan verilerin faydasının periyodik olarak yeniden değerlendirilmesi gerekecektir. Veriler "yalnızca kamu yararına arşivleme amacıyla, bilimsel veya tarihsel araştırma amaçları veya istatistiksel amaçlarla işlenecekse", belirli bir işleme amacına bağlantı olmadan da depolamaya izin verilir. Bu ilke, ilgili kişilerin hakları ile çatışabilir.

Hesap verebilirlik ilkesi gereği veri sorumluları kişisel veri işleme faaliyetlerinin kayıtlarını tutmakla yükümlüdürler. Bu hususlar, veri sorumlularının tüm temel ilkelere saygı gösterme yükümlülüklerini ciddiye almalarını sağlamayı amaçlamaktadır. Veri sorumlularının, yasadışı erişim, veri ihlalleri, veri kayıpları veya sızıntılarına karşı koruma sağlamak için uygun güvenlik mekanizmaları uygulaması gerekir. IoT geliştiricileri tarafından nesnelerin ve hizmetlerin tasarımına uygun (siber) güvenlik standartları ve mekanizmaları yerleştirilmelidir (Wachter 2018: 274-275).

GDPR'ın yedi temel ilkesi IoT'de gizlilik, güven ve tanımlanabilirliği dengelemek için kritik öneme sahip olmakla birlikte gizliliğin korunması ve sistemlerin siber saldırılara karşı dayanıklılığı her zaman garanti edilemeyecektir. Ancak, olası riskler konusunda açıklık ve dürüstlük, kullanıcıları her durumda çıkarlarının korunacağına ikna etmeye yönlendirecektir (Wachter 2018: 276).

Öte yandan, GDPR öncelikle Avrupa'da bulunan veri sorumluları ve veri işleyenler için geçerlidir. Kişisel verilerin, Avrupa dışına aktarılması halinde kişisel verilerinin korumasını kaybetme riski vardır. Bu nedenle GDPR, veri alıcısının verilerin korunacağını garanti etmemesi durumunda takma ad verme ve şifreleme gibi uygun güvenlik önlemleri ile sağlanmadıkça Avrupa dışına veri aktarımlarını kısıtlamaktadır (Barati-Rana-Petri-Theodorakopoulos 2020: 119).

Diğer taraftan, GDPR, geliştirilen herhangi bir ürün veya hizmet için "privacy by design/tasarım yoluyla gizlilik" yaklaşımının benimsenmesini gerektirir. (Lodge-Crabtree 2021: 181-182) Ayrıca, nesnelerin işlediği kişisel verileri korumak için uygun teknik önlemler alınmalıdır. Nitekim siber güvenlik ile kişisel verilerin korunması ayrılmaz bir şekilde bağlantılıdır.

SONUÇ

Nesnelerin interneti uygulamaları insan hayatını kolaylaştırmakla birlikte, bilgisayarların ve internetin ortaya çıktığı ve bunların yaygınlaşması ile daha da önemli hale gelen kişinin mahremiyetine ilişkin endişeleri artırmıştır. Nitekim tek bir veri sorumlusu tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinde, ilgili kişinin bu faaliyetlerin tespitini yapması ve bu çerçevede veri sorumlusuna başvurarak kişisel verilerinin korunmasına ilişkin haklarını kullanabilmesi, nesnelerin interneti gibi pek çok paydaşın kişisel veri işleme faaliyetinde bulunduğu durumlar karşısında daha kolaydır.

Wachter tarafından işaret edildiği üzere, nesnelerin internetindeki tanımlama teknolojilerinin getirdiği gizlilik riskleri bağlamında, GDPR, kişisel verilerin işlendiği tüm sektörlerdeki uygulanabilirliği ve geniş coğrafi etkisi nedeniyle özellikle ilgili bir yasal çerçeve olmakla birlikte, IoT profili oluşturma ve tanımlama teknolojilerinin kullanıcı gizliliği üzerindeki etkisini en aza indirmek için IoT teknolojilerinin tasarımı ve dağıtımına ilişkin daha fazla hukuki düzenlemenin yürürlüğe konulmasının uygun olacağı değerlendirilmektedir. Nitekim, nesnelerin internetinde cihaz üreticileri, veri toplayıcıları veya brokerleri, uygulama geliştiricileri gibi paydaşlar tarafından kişisel veri işleme faaliyeti gerçekleştirilse de söz konusu paydaşlar nesnelerin interneti uygulamalarının yalnızca bir kısmına dahil olabilmektedir. Bu da 29 Çalışma Grubunun da işaret ettiği üzere kişisel verisi işlenen ilgili kişilerin verileri üzerindeki kontrolünü kaybetmesine yol açabilmektedir. Özellikle nesnelerin interneti uygulamaları özelinde "veri sahipliği" konusu yeni tartışmalara yol açmıştır (Janecek 2018).

Nesnelerin internetinin mimarisi, uygulama alanları, bileşenleri ve beraberinde getirdiği gizlilik sorunları birlikte değerlendirildiğinde veri sorumlusu statüsünü haiz cihaz üreticileri, sosyal platformlar, üçüncü taraf uygulama geliştiricileri, cihaz üreticileri ve üçüncü taraf uygulama geliştiricileri dışındaki üçüncü taraflar ve IoT veri platformlarının kişisel verisi işlenen kullanıcının rızasının öncelikle cihazlar aracılığıyla alınması gerektiği, kişisel verilerin işlenme amacının nesneden beklenen amaçla uyumlu olması gerektiği ve kullanıcıya mümkün olduğunca anonim kalma olasılığının tanınması gerektiği değerlendirilmektedir. Nitekim nesnelerin interneti uygulamaları kapsamında kişisel verilerin işlenmeye başlandığı ilk andan itibaren veri akışlarının kontrol edilememesi, verilerden çıkarımlar elde edilmesi, davranış kalıplarının ortaya çıkarılması ve profilleme gibi tüm aşamalarda ilgili kişinin verileri üzerinde kontrolünü kaybetme olasılığını artırmaktadır. Bu da kullanıcıyı nesnelerin interneti uygulamalarından beklenen fayda ile kişisel veriler üzerinde azalan kontrol nedeniyle meydana gelebilecek zararın kıyaslanarak söz konusu nesnelerin kullanıp kullanılmama yönünde karar vermeye zorlamaktadır.

Sonuç olarak, gizliliğe ilişkin problemlerin öncelikle veri sorumluları tarafından tespit edilmesi, privacy by design [tasarımdan itibaren gizlilik, veri koruma ilkelerine (şeffaflık, veri minimizasyonu, ölçülülük vb.) yeni uygulamaya geçirilecek sistemlerin oluşturulma sürecinden başlayarak uygun şekilde tasarlanması] ve privacy by default (kullanıcılarının gizliliğinin korunması için her türlü seçeneğin varsayılan olarak önceden aktif edilmesi) ilkeleri temel alınarak gizlilik sorunlarının en aza indirilmesi gerekmektedir. Nitekim yeni gelişen teknolojilere yönelik genel hukuki yaklaşım, teknoloji ürünü henüz piyasaya sürülmeden hukuki düzenleme yapılıp söz konusu teknolojik gelişimin engellenmesi yönünde değildir. Bu sebeple söz konusu ürünlere gizlilik sorunlarının öncelikle veri sorumluları tarafından tespiti ve engellenmesi gerekmektedir.

KAYNAKLAR

Abbate, Janet Ellen (1994) From ARPANET to Internet: A History of ARPA-sponsored Computer Networks, Pennsylvania University, Doctoral Thesis.

Aktaş, Faruk; Çeken, Celal; Erdemli, Yunus Emre (2014) Biyomedikal uygulamaları için nesnelerin interneti tabanlı veri toplama ve analiz sistemi". Tıp Teknolojileri Ulusal Kongresi, Kapadokya, Nevşehir, 25-27 Eylül 2014.

Alam, Tanweer (2018) A Reliable Communication Framework and Its Use in Internet of Things (IoT) Islamic University of Medina.

Alam, Mansaf; Kashish Ara, Shakil; Khan, Samiya (2020) Internet of Things (IoT) Concepts and Applications, *"Open Service Platforms for IoT"* Agarwal, Preeti; Alam, Mansaf, Springer Nature Switzerland.

Chen, Min; Chen, Shigang (2016) RFID Technologies for Internet of Things, Springer International Publishing, Switzerland.

Crabtree, Andrew; Haddadi, Hamed; Mortier, Richard (2021) Privacy by Design for the Internet of Things – Building Accountability and Security, "Data Protection by Design and Default: IoT App Development", Lodge, Tom; Crabtree, Andrew, The Instution of Engineering and Technology.

Daş, Resul; Gündüz, Muhammed Zekeriya (2018) Nesnelerin İnterneti: Gelişimi, Bileşenleri ve Uygulama Alanları, Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, Sayı 24(2).

Dayıoğlu, Mehmet Ali; Uğur, Furkan; Türker, Ufuk (2016) : Seralarda Nesnelerin İnterneti Teknolojisinin Uygulanması: Tasarım ve Prototip Geliştirme, Gaziosmanpaşa Üniversitesi Ziraat Fakültesi Dergisi, Sayı:33

Erdoğan, Can (2018) Nesnelerin İnternetinin Kamu Hizmetlerine İnovatif Etkileri ve Büyük Veri Yönetimi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul.

Evans, Dave (2011) The Internet of Things- How the Next Evolution of the Internet Is Changing Everything, Cisco Internet Business Solutions Group (IBSG).

Greengard, Samuel (2015) The Internet of Things, MIT, ABD.

Greengard, Samuel (2021) The Internet of Things – Revised and Updated Edition, The MIT Press Essential Knowledge Series, ABD.

Gülşen, İzzet (2019) Nesnelerin İnterneti: Vaatleri ve Faydaları, Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD), Cilt:6, Sayı:8.

Kamal, Raj (2017) Internet of Things: Architecture and Design Principles, McGraw Hill Education (India) Private Limited.

Khan, Jamil Y.; Yüce, Mehmet R. (2019) Internet of Things (IoT): Systems and Applications, Jenny Stanford Publishing Pte. Ltd.

Kosunalp, Selahattin; Arucu, Muhammet (2018) Nesnelerin İnterneti ve Akıllı Ulaşım, Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi, Cilt:1, Sayı:1.

Küzeci, Elif (2021) Kişisel Verilerin Korunması, On İki Levha Yayıncılık, İstanbul.

Janecek, Vaclav (2018) Ownership of Personal Data in the Internet of Things, Computer Law & Security Review, Sayı:34, s. 1039-1052.

Baratı, Masoud; Rana, Omer; Petrı, Ioan; Theodorakopoulos, George (2020) GDPR Compliance Verification in Internet of Things, Specıal Section On Blockchaın-Enabled Trustworthy Systems, Volume 8.

Çekin, Mesut Serdar (2021) Yapay Zekâ Teknolojilerinin Hukuki İşlem Teorisine Etkileri, On İki Levha Yayıncılık, İstanbul, 1.Baskı.

Sundmaeker, Herald; Guillemin, Patrick; Friess, Peter; Woelffle, Sylvie (2010) Vision and Challenges for Realising the Internet of Things, Cluster of European Research Projects on the Internet of Things, European Commission.

Raj, Pethuru; C. Raman, Anupama (2017) The Internet of Things, Enabling Technologies, Platforms and Use Cases, CRC Press.

Samih, Haitham (2019) Smart Cities and Internet of Things, Journal of Information Technology Case and Application Research, Sayı: 21 (1).

Serpanos, Dimitrios; Wolf, Marilyn (2018) Internet of Things – IoT Systems Architectures, Algorithms, Methodologies, Springer International Publishing.

Sönmez Çakır, Fatma; Aytekin, Alper; Tüminçin, Alper Fatma (2018) Nesnelerin İnterneti ve Giyilebilir Teknolojiler, Sosyal Araştırmalar ve Davranış Bilimleri Dergisi, Cilt:4, Sayı:5.

Wachter, Sandra (2018) The GDPR and the Internet of Things: A Three-Step Transparency Model, Law, Innovatıon And Technology 2018, VOL. 10, NO. 2.

ELEKTRONİK KAYNAKLAR

Article 29 Data Protection Working Party, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", Erişim Adresi: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, Erişim Tarihi: 13.07.2022

Bilgi Teknolojileri ve İletişim Kurumu, "2019-2023 Stratejik Planı", Erişim Adresi: https://www.btk.gov.tr/uploads/pages/yayinlar-stratejik-planlar/btk-2019-2023-stratejik-plani.pdf, Erişim Tarihi: 13.07.2022

Cisco. "Internet of Things". Erişim Adresi: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, Erişim Tarihi: 13.07.2022

Çevre, Şehircilik ve İklim Değişikliği Bakanlığı'nın "Nesnelerin İnterneti – Akıllı Şehirler Kapasite Geliştirme ve Rehberlik Projesi", Erişim Adresi: https://www.akillisehirler.gov.tr/wp-content/uploads/KapasiteGelistirme/Egitim_Pdf/Nesnelerin_Interneti.pdf, Erişim Tarihi: 13.07.2022

International Communication Union, "About International Communication Union" Erişim Adresi: https://www.itu.int/en/about/Pages/default.aspx, Erişim Tarihi: 13.07.2022

Sanayi ve Teknoloji Bakanlığı'nın "2023 Sanayi ve Teknoloji Stratejisi", Erişim Adresi: https://www.sanayi.gov.tr/assets/pdf/SanayiStratejiBelgesi2023.pdf, Erişim Tarihi: 13.07.2022

IBM, "About IBM Watson IoT Platform", Erişim Adresi: https://cloud.ibm.com/docs/IoT?topic=IoT-about_iotplatform#:~:text=IBM%20Watson%E2%84%A2%20IoT%20Platform%20is%20a%20fully%20managed%2C%20cloud,of%20Things%20(IoT)%20devices. Erişim Tarihi: 13.07.2022

[i] NFC teknolojisi onlarca yıldır var olan RFID teknolojisinin bir evrimidir. NFC, ilkel eşleşme prensibine göre çalışır. Bu, esasen, bir bobinden bir elektrik akımı geçirerek bir manyetik alan üreten okuyucu cihaz içerir. Bir etiket (kendi bobini ile) yakınına getirildiğinde, alan etiket içinde herhangi bir kablo veya hatta fiziksel temas olmadan bir elektrik akımı başlatır. Ardından, ilk sinyal alışverişi tamamlandığında, etikette depolanan veriler kablosuz olarak okuyucuya iletilir.

[ii] Bluetooth, farklı cihazlar arasında veri alışverişini sağlayan kablosuz bir radyo teknolojisidir. Bluetooth bilgi iletmek için dalga boyunu kullanırken, cihazların bağlı kalması için genellikle yalnızca kısa bir mesafede çalışır.

[iii] Geliştiriciler tarafından aynı ortamda çalışan programlar arasında birlikte çalışabilirlik oluşturmak için kullanılan protokoller, biçimler, standartlar, araçlar ve diğer kaynakları ifade eden uygulama programlama arayüzü esasında bir yazılım aracısıdır. (Greengard 2021: 233)

[iv] Mahremiyet Etki Analizi (PIA), bir programın veya sistemin geliştirme yaşam döngüsü boyunca gizlilik risklerini belirlemek ve değerlendirmek için kullanılan bir araçtır. Bir Mahremiyet Etki Analizi, hangi kişisel tanımlayıcı bilgilerin toplandığını belirtir ve bu bilgilerin nasıl korunacağını, nasıl korunacağını ve nasıl paylaşılacağını açıklar.