NESNELERİN İNTERNETİNİN HUKUKİ YÖNDEN İNCELENMESİ

Yrd. Doç. Dr. Armağan Ebru BOZKURT YÜKSEL *

Öz

Teknolojideki gelişmeler hayatın her alanını etkilediği gibi hukuku etkilemektedir. Teknoloji pek çok konuda kolaylık sağlamakta bununla birlikte hukuki açıdan bazı sorunları da beraberinde getirmektedir. Nesnelerin İnterneti de hayatı kolaylaştıran teknik bir gelişmedir. Burada birbiri ile veya başka bilgisayar ile bilgi alışverişi yapabilen aygıtlar söz konusudur. Ancak bu teknoloji ile ilgili olarak çeşitli sorunlar gündemdedir. Özellikle güvenlik ve mahremiyetin korunması konularındaki eksiklikler ve hukuki düzenlemelerin henüz tam olarak hazırlanmamış olması nedeni ile nesnelerin İnterneti ile ilgili birtakım endişeler söz konusudur. Avrupa Birliği ve Amerika Birleşik Devletleri'nde çeşitli çalışmalar yapılmakla birlikte nesnelerin İnterneti konusunda standartlaşma sağlanamamıştır. Konunun hukuki zemininin oluşturulması süreci de halen devam etmektedir. Bu çalışma nesnelerin İnterneti kavramını kısaca açıklamakta daha sonra konu ile ilgili hukuki problemlere ve mevcut düzenlemelere değinmektedir.

Anahtar Kelimeler

Nesnelerin İnterneti, Güvenlik, Mahremiyet, Siber Saldırı

* Dokuz Eylül Üniversitesi, İİBF, İşletme Bölümü, Ticaret Hukuku Anabilim Dalı (e-posta: armaganbozkurt@yahoo.com). Bu makale 1-3 Aralık 2015 tarihlerinde İstanbul Üniversitesi, Beyazıt İstanbul'da gerçekleşen XX. Türkiye'de İnternet Konferansında "Nesnelerin İnterneti ve Hukuk" başlığı ile sunulan tebliğin genişletilmiş halidir. (Makale Gönderim T.: 11.02.2016/Kabul T.: 12.02.2016)

EXAMINING INTERNET OF THINGS FROM A LEGAL PERSPECTIVE

Abstract

Technologic developments affect law as it does every aspect of life. Technology provides convenience in many areas. However it brings some problems from legal perspective. Internet of things is a technologic development that makes life easier. Internet of things is about the devices that can connect to each other and computers. But there are some complications on the agenda about this technology which is beneficial to human life. Especially there are some concerns about Internet of things because of deficiencies in security and protection of privacy and regulations that have not completely prepeared yet. Although there are some studies going on in European Union and United States of America, standardization has not completed yet. The formation of the legal basis of the subject is still going on as well. This paper explains the concept of Internet of things at first and then refers to the legal issues related to the subject and the existing regulations.

Keywords

Internet of things, Security, Privacy, Cyber Attack

I. NESNELERİN İNTERNETİ KAVRAMI VE TEKNOLOJİSİ

İngilizcede *Internet of things (kısaca IoT)* olarak ifade edilen kavramın karşılığı olarak nesnelerin İnterneti[1] terimi kullanılabilir. Nesnelerin İnterneti birbiri ile bağlantılı aygıtlarla ilgilidir. Bu teknolojide algılayıcısı/sensörü olan her çeşit nesnenin İnternet'e bağlanarak birbirleri ile haberleşmesi söz konusudur[2]. Nesnelerin birbirleri ile haberleşebilmesi sayesinde insan hayatını kolaylaştırıcı gelişmeler sağlanmaya çalışılmaktadır[3]. Bileğe takılabilen bileklik şeklinde egzersiz takip cihazları *(fitness tracker)*, bebeklerin soluk alıp vermelerini takip edebilen giysiler, akıllı arabalar sensörü olan nesnelere örnek olarak sayılabilir. Tam olarak üzerinde anlaşılmış bir tanımı olmamakla birlikte nesnelerin İnterneti akıllı nesnelerin oluşturduğu merkezi olmayan ağ şeklinde açıklanabilir. Bu nesneler algılayabilen, kayıt tutabilen, yorum yapabilen, bilgi iletişiminde bulunabilen ve kendi başına ya da diğer nesnelerle birlikte işleyen nesnelerdir. Bu nesneler diğer nesneler ile bilgisayarlar ile veya diğer kişiler ile bağlantı kurabilmektedir[4]. Nesnelerin İnterneti teknolojisinin en çok kullanıldığı alanlar sağlık, otomobil, evler, işyerleri ve akıllı telefonlardır[5].

Nesnelerin İnterneti *(Internet of Things)* terimi ilk defa 1999 yılında Kevin Ashton tarafından yapılan bir sunumda kullanılmıştır[6]. Günümüzde bu terimin yanında bir de her şeyin İnterneti anlamına gelen *Internet of everything (kısaca IoE)* terimi de kullanılmaktadır. Bu terimi ilk kullanan

---

1 İnternet, özel isim olduğundan ilk harfi büyük yazılmıştır. www.tdk.gov.tr (Erişim 08.10.2015).

2 **Peppet,** Scott: "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review, Vol.93:85 vd.

3 http://www.donanimhaber.com/isletim-sistemleri/haberleri/Google-Nesnelerin-interneti-icin-yeni-bir-isletim-sistemi-gelistiriyor.htm, Yayınlanma 22.05.2015 (Erişim 08.10.2015).

4 **Blum,** Philip: "Internet of Things', 101: Legal Concerns-Law 360, http://www.law360.com/articles/526266/internet-of-things-101-legal-concerns (Erişim 08.10.2015).

5 **Peppet,** s. 86 vd.

6 **Ashton,** Kevin: "That Internet of Things Thing", RFID Journal, Yayınlanma 22.06.2009, http://www.rfidjournal.com/articles/view?4986 (Erişim 16.10.2015).

kişi ise John Chambers'dır. Cisco Şirketi'nin yönetim kurulu başkanı *(CEO)* olan Chambers her şeyin İnternetini ağ bağlantılarının daha yararlı olması için tüm insanları, süreci *(process)*, verileri ve nesneleri bir araya getirmek olarak tanımlamaktadır[7]. Artan bağlantılılık her şeyi online/çevrimiçi hale getirmektedir. Böylelikle daha önce eşi görülmemiş imkânların işletmeler, bireyler ve devletler için söz konusu olacağı öngörülmektedir. Nesnelerin İnterneti fiziksel nesnelerin bir ağ üzerinde birbiri ile bağlantılı olmasını ifade etmektedir. İnsanlar ve süreç buna dâhil değildir. Her şeyin İnternetinde ise insanlar ve süreç de bileşen olarak vardır. Bu bakımdan her şeyin İnterneti, nesnelerin İnternetini de içeren bir teknolojidir[8].

Nesnelerin İnterneti sadece nesnelerin İnternet'e bağlanması olarak algılanmamalıdır. RFID yongaları/çipleri *(chip)* okuyabilen sensörlerden oluşan yeni bir ağ modeli de bu kavramın içindedir[9]. RFID, Radio Frequency Identification kelimelerinin baş harflerinden oluşan bir kısaltmadır. Radyo frekansı ile kimlik saptama şeklinde tercüme edilebilir. Burada küçük bir yonga (chip/çip) ve antenden oluşan bir aygıt söz konusudur. 2000 bayta kadar veri taşıyabilen bu yonga üzerinde bulunduğu nesne için bir kimlik belirleyici teşkil etmektedir[10]. Radyo frekansı ile kimlik saptama teknolojisi tüm ürünlerin diğerlerinden ayırt edilmesini sağlar. Barkod sistemine benzemekle birlikte ondan farklı olarak bilginin okunabilmesi için temas ya da görüş alanı içinde olması gerekmez[11]. Tüm nesneler bir etiket taşımak sureti ile bir sensörün önünden geçerken sinyaller sayesinde bilgi alışverişi

---

7 **Pearl,** Robert: "Cisco CEO John Chambers: American Health Care is At a Tipping Point", Forbes, Yayınlanma 28.08.2014, http://www.forbes.com/sites/robertpearl/2014/08/28/cisco-ceo-john-chambers-american-health-care-is-at-a-tipping-point/ (Erişim 16.10.2015).

8 **CISCO,** "The Internet of Everything-Global Public Sector Economic Analysis", Yayınlanma 2013, s. 1, https://www.cisco.com/web/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf (Erişim 16.10.2015).

9 **Yetimler,** Emrah: "Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri," http://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri (Erişim 14.10.2015).

10 http://www.technovelgy.com/ct/technology-article.asp (Erişim 13.10.2015).

11 **Peslak,** Alan R.: "An Ethical Exploration of Privacy and Radio Frequency Identification", Journal of Business Ethics, Y.2005, N.59, s. 328.

yapılabilmektedir[12]. Radyo frekansı ile kimlik saptama teknolojisinin kullanımında mahremiyetin korunması ile ilgili birtakım endişeler bulunmaktadır. Örneğin üzerine Radyo frekansı ile kimlik saptama (RFID) etiketi konulmuş bir ürünün satışından önce müşteri tarafından incelenmesi halinde bu durum izlenebilmektedir. Müşterinin elindeki ürün ile mağazadaki konumu bulunabilmektedir. Satış sürecinde satın alınan ürüne ilişkin kayıt yapılması, satın alınan ürün ile daha önce satın alınanlar arasında koordinasyon kurulması, ürünün satış bilgisinin devlet veya vergi kurumları ile ya da başka kurumlarla paylaşılması yine mahremiyet ile ilgili endişeler ortaya çıkarmaktadır. Satış sonrası ise satın alınan ürünlerin fiziksel olarak takibinin mümkün olması, radyo frekansı ile kimlik saptama (RFID) etiket okuyucuları sayesinde kişinin hareketlerinin izlenebilmesi de yine mahremiyet ile ilgilidir[13].

Nesnelerin İnterneti teknolojisinin pek çok avantaj sağlayacağı düşünülmektedir. Örneğin, beyaz eşya kullanıcılarının, bakım ve tamir konusunda beklemeleri bu teknoloji sayesinde ortadan kalkacaktır. Çünkü uzaktan aletlerdeki arıza anlaşılarak gerekli programlama yapılabilecektir. Yine açık kalan bir buzdolabı kapağı nedeni ile buzların erimesi ve suyun dışarı akması ya da yiyeceklerin bozulması, buzdolabının sahibine kapağın açık kaldığına ilişkin bilgi vermesi sayesinde ortadan kalkacaktır. Üreticiler bu teknoloji sayesinde kullanıcıların ürünleri tam olarak nasıl kullandığı bilgisine ulaşabilecek ve böylece gereksiz fonksiyonlar üzerinde çalışmak yerine gerekli olan özellikler üzerinde yoğunlaşacaklardır[14]. Nesnelerin İnterneti sayesinde bugün çok büyük miktarlarda gerçek zamanlı bilgi elde edilebilmekte ve paylaşılabilmektedir[15]. 2020 yılı itibarıyla 5 milyar aygıtın İnternet'e bağlı olacağı tahmin edilmektedir[16].

---

12 **Barbry,** Eric: "The Internet of Things, Legal Aspects What Will Change Everything", Digiworld Economic Journal, no.87, 3rd Q.2012, s. 87, http://innovation-regulation2.telecom-paristech.fr/wp-content/uploads/2012/10/CS87_BARBRY.pdf (Erişim 12.10.2015).

13 **Peslak,** s. 336.

14 **Walker,** Kim: "The Legal Considerations of the Internet of Things", Computer Weekly, http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things (Erişim 07.10.2015).

15 **Walker;** Uluslararası Veri Kuruluşu'nun *(IDC-International Data Corporation)* Dijital Evren *(Digital Universe)* araştırmalarına göre dünyadaki verilerin miktarı 2020 yılı itibarı ile 44 zetabayt olacaktır. Bu verilerin % 10'u ise nesnelerin İnternet'i sayesinde

Nesnelerin İnterneti pasif olarak sadece bilgiye ulaşmayı sağlamaktan ibaret değildir. Nesnelerin İnterneti insana karar verme konusunda yardımcı olarak bilgiyi aktif hale getirmektedir. Örneğin akıllı telefonunuz nesnelerin İnterneti sayesinde size acıktığınızda sadece çevredeki restoranların yerini göstermekle kalmayıp en son yediğiniz yemeğin ne olduğunu hatırlatarak diyetinize uygun, misafir sayınıza, onların damak tadına, restorandaki müsait yer durumuna göre ve bütçenize uygun restoranı belirtecektir[17].

Nesnelerin İnterneti sayesinde nesneler arasında bağlantı sağlanması yanında nesneler akıllı hale *(smart things)* gelmektedir. Akıllı bir nesne karar alma sürecine yardımcı olmakta veya insan yerine kararı vermektedir. Ancak bu durum bazı sorunlar doğurabilmektedir. Örneğin kendi kendine giden arabalar, akıllı nesneler ile ilgili olarak sorumluluk konusundaki sorunları ortaya çıkarmıştır. Amerika Birleşik Devletleri Nevada Eyaleti'nde 2011 yılında kendi kendine giden (insansız) arabalar için kanuni zemin oluşturulmuş, ilk izin de Google arabaları için verilmiştir *(first self driven car license)*. Burada gündemde olan sorun herhangi bir kaza olması durumunda sorumluluğun arabanın sahibine mi, arabanın üreticisine mi yoksa akıllı arabaya mı ait olacağı ile ilgilidir[18].

---

elde edilecektir. **Adshead,** Anthony: "Data Set to Grow 10-fold by 2020 as Internet of Things Takes Off", http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off, Yayınlanma 09.04.2014 (Erişim 08.10.2015); Veri ölçüleri olarak adlandırılabilecek ölçülere bakılırsa 1 zetabayt oldukça büyük bir ölçektir. 1 kilobayt *(kilobyte)*=1000 bayt *(byte);* 1 megabayt *(megabyte)*=1 milyon bayt; 1 gigabayt *(gigabyte)*=1 milyar bayt; 1 terabayt *(terabyte)*= 1 trilyon bayt; 1 petabayt *(petabyte)*=1 katrilyon bayt; 1 exabayt *(exabyte)*=1 kentilyon bayt; 1 zettabayt *(zettabyte)*=1 seksilyon bayt. Bu ölçekler *yottabyte, xenottabyte, shilentnobyte, domegemegrottebyte* şeklinde devam etmektedir. **Bunn,** Julian: "How Big Is a Petabyte, Exabyte, Zettabyte, Or a Yottabyte?" High Scalability, http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html, Yayınlanma 11.09.2012 (Erişim 08.20.2015).

16 **Vickery,** James: "Legal Tech Series: What is the Internet of Things?", https://www.youtube.com/watch?v=5bSa2QGA9Dk, Yayınlanma 21.06.2015, (Erişim 08.10.2015).

17 **Barbry,** s. 91.

18 Amerika Birleşik Devletleri'nde Kaliforniya, Arizona, Hawaii, Oklahoma eyaletleri de kendi kendine giden arabaların yasal olarak kabul edilmesi hususunda kanuni düzenlemeler üzerinde çalışmaktadır. **Barbry,** s. 91.

II. NESNELERİN İNTERNETİ İLE İLGİLİ HUKUKİ SORUNLAR

Nesnelerin İnterneti teknolojisi ile ilgili henüz yeterli ve gerekli hukuki düzenlemeler bulunmamaktadır. Buna karşılık nesnelerin İnterneti teknolojisi hızla gelişmekte ve insanların hayatında yer almaktadır. Örneğin, Fitbit[19] ve Nike+ FuelBand[20] isimli spor/sağlık takipçilerinin satışından 2013 yılında 300 milyon Amerikan Doları elde edilmiştir[21].

Nesnelerin İnterneti ile ilgili doğabilecek hukuki sorunlar ise ayrımcılık, güvenlik ve mahremiyet üzerinde yoğunlaşmaktadır.

A. Ayrımcılık

Nesnelerin İnternetinin kullanıcılar/tüketiciler ile ilgili pek çok bilgiyi ortaya çıkarması nedeni ile çeşitli açılardan ayrımcılığın söz konusu olabileceği belirtilmektedir. Örneğin bir spor/sağlık takipçisi bileklik şeklindeki ürünün onu kullananın sadece egzersiz rutinini değil, aynı zamanda tütün ürünü ya da uyuşturucu madde veya alkol kullanıp kullanmadığını da takip edeceğini ki bunların her birinin aynı zamanda kişiye özgü biyometrik[22] verilere ve hassas kişisel verilere[23] de ilişkin olduğu belirtilmektedir. Nesne-

---

19 Bir bileklik olarak hazırlanmış Fitbit isimli ürün, kullanan kişinin günboyu yaptığı aktiviteleri, kilosunu, uykusunu ve yediklerini takip etmektedir. https://www.fitbit.com/whyfitbit (Erişim 16.10.2015).

20 Bileğe takılan ve usb bağlantısı ile bilgisayara bağlanabilen bileklik şeklinde bir üründür. İnternet sitesinden uygulamanın akıllı telefonlara da indirilmesi mümkündür. İnternet bağlantısı sayesinde sosyal paylaşım sitelerinde dahi kullanıcının o gün kaç adım attığını paylaşabilmesi mümkündür. Kullanıcının gün içerisinde ne kadar adım attığını harcadığı kaloriyi, kalp atışlarını takip etmektedir. https://secure-nikeplus.nike.com/plus/products/fuelband/ (Erişim16.10.2015).

21 **Peppet,** s. 92.

22 Biyometrik veriler, bireyin belirlenebilir hale gelmesini sağlayan iris, retina, parmak izi, el geometrisi, DNA, yürüyüş tanımaya ilişkindir. **Akgül,** Aydın: "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", TBB Dergisi, 2015(118), s. 206.

23 *"…kişilerin ırksal kökenine, dini inançlarına, sağlık durumu ve siyasi görüşlerine ilişkin veriler hassas veri olarak kabul edilmektedir."* **Kaya,** Cemil: "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İÜHFM, C.LXIX, S. 1-2, s. 317.

lerin İnterneti sayesinde elde edilen verilerin kiraya verenler, işverenler, sigorta şirketleri gibi ekonomik aktörler tarafından da ekonomik ayrımcılıkta kullanılabilme ihtimalinin olduğu ifade edilmektedir. Örneğin bir kişinin araç sürüş alışkanlıklarının ya da egzersiz alışkanlıklarının veya evdeki elektriği kullanma alışkanlıklarının sigorta şirketleri, bankalar ve işverenler tarafından o kişi/tüketici hakkında karar vermelerinde kullanılabileceği belirtilmektedir[24].

B. Güvenlik ve Gizlilik/Mahremiyet

Nesnelerin İnterneti ile ilgili başka bir hukuki sorun ise güvenlik ile ilgilidir. Nesnelerin İnterneti teknolojisi kapsamındaki ürünler genellikle tüketicilere yönelik ürünlerdir. Bu nesnelerin üreticileri genellikle yazılım ya da donanım şirketleri değildir. Dolayısıyla veri güvenliğin sağlanması konusu üretimde ön planda değildir. Şifreleme ya da diğer güvenlik önlemlerinin ürünlere eklenmesi ürünlerin küçük olarak tasarlanması, az enerji ile çalışması ve kapasitesinin az olması nedeni ile zorlaşmaktadır. Bu nedenle nesneler üzerindeki sensörlerin toplandığı verilerin çalınması kolay hale gelmektedir[25].

Üzerinde sensör bulunan nesnelerin topladığı verilere ilişkin olarak tüketiciler gizlilik politikası konusunda ya hiç bilgilendirilmemekte ya da gizlilik politikasının içeriği konusunda tam olarak aydınlatılmamaktadır. Üretici tarafından bir gizlilik politikası metninin hazırlandığı durumlarda toplanan verilerin kime ait olacağı, hangi biyometrik verilerin veya tam olarak hangi verilerin sensör tarafından toplandığı, ne kadar veri toplandığı, bu verilerin nasıl kullanılacağı veya satılacağı konularında tam bir açıklık olmadığı doktrinde belirtilmektedir[26].

Güvenlik ile ilgili bir diğer endişe ise nesnelerin İnterneti sayesinde kötüniyetli kişilerin suç işlemelerinin kolaylaşabilmesidir. Örneğin, akıllı bir eve akıllı cep telefonu sayesinde bağlanılabildiğini düşünelim. Kötüniyetli bir kişi bu evin merkezi ısıtma sistemini ev sahibinin cep telefonuna ulaşmak

---

24 **Peppet,** s. 93.

25 Ayrıntılı bilgi için bkz. **Peppet,** s. 94 vd.

26 **Peppet,** s. 95.

için kullanabilir. Böylelikle de ev sahibinin kredi kartı bilgilerini çalabilir ya da ev sahibinin evde olmadığı saatleri merkezi ısıtma sisteminin kullanılmadığı saatlerden öğrenerek evde hırsızlık yapabilir[27]. Ayrıca nesnelerin İnterneti teknolojisinin gelişmesi ile gelecekte saldırıların[28] *(hacking)* artması ve savaşların artık siber savaşlara dönüşeceği öngörülmektedir[29].

Nesnelerin İnterneti teknolojisinin yapısı gereği güvenlik ile ilgili ortaya çıkabilecek sorunlar da klasik güvenlik sorunlarından farklı hale gelecektir. Artık bireylerin kimliklerine yönelik hırsızlığın yerini makinelerin kimliğine yönelik hırsızlık alacaktır. Böylece makineler arasında iletilen bilgilerin ele geçirilmeye çalışılması söz konusu olabilecektir[30].

Nesnelerin İnterneti teknolojisinde sensörlerin topladığı verilerin kimliksizleştirilmesi *(deidentification)* ve anonimize edilmesi zordur. Zira sensör içeren nesnelerin her biri kendilerine ait adeta parmak izi niteliğinde özellikler taşımaktadır. Kullanıcının kimliğini belirleyici isim, adres, telefon numarası gibi bilgiler kaldırılabilse dahi sensörlerin topladığı veriler sayesinde verilerin sahiplerinin belirlenebilmesi mümkündür. Bu nedenle saldırılara açık bir sistemdir. Mahremiyetin korunması ile ilgili mevcut hukuki düzenlemeler ise bu şekilde verilerin kolayca tekrar kimliklendirilmesi tehdidine ilişkin hükümler içermemektedir[31].

Nesnelerin İnterneti sayesinde çok fazla veri toplanabildiğinden bu teknolojinin gelişmesi için gayret gösterenlerin ilgisiz verilerin toplanmaması için gerekli önlemleri almaya çalışmaları gerektiği belirtilmektedir. Veri güvenliğinin bozulmaması için gerekli önlemlerin alınması hususu da burada üzerinde durulan konulardan bir tanesidir. Ayrıca veri öznelerinin

---

27 **Walker.**

28 Trafikte kargaşa/kaos yaratmak isteyen kişiler insansız arabalara/araçlara yönelik siber saldırıda bulunabilir/hackleyebilir. http://www.theguardian.com/technology/2014/nov/21/driverless-cars-hacking-threat-road-trials-january (Erişim 17.02.2016).

29 **Taylor,** Daniel, "NSA Cyber War Will Use Internet Connected Devices as Weapons Platform; Your Home is the Battlefield", Global Research, Yayınlanma 19.01.2015, http://www.globalresearch.ca/nsa-cyber-war-will-use-internet-of-things-as-weapons-platform-your-home-is-the-battlefield/5425526 (Erişim 21.10.2015).

30 **Barbry,** s. 96.

31 **Peppet,** s. 94.

verilerinin toplanma amacının dışında kullanılmaması hususunda da korunmaları gerekmektedir. Nesnelerin İnterneti sayesinde pek çok aygıtın birbirleri ile otomatik olarak iletişimde olmaları nedeni ile bir başka sorun veri öznesinin kendisi hakkında veri toplanmasına ilişkin tam olarak neye rıza gösterdiğinin belirlenememesinin söz konusu olmasıdır[32].

Nesnelerin İnterneti sayesinde kişilerin özel hayatını ilgilendiren veriler de toplanabilmektedir. Örneğin İnternete bağlı ve bileğe takılan saat şeklindeki bir aygıt kişinin gece kaç saat uyuduğunu veya kesintisiz uyuyup uyumadığını, kaçta kalktığını, kan basıncını, tansiyonunu ölçebilir, kaydedebilir ve İnternet sayesinde başka aygıtlara gönderebilir. Yine bir otomobil bu teknoloji sayesinde onu kullanan kişinin araba kullanma alışkanlıklarını örneğin ne kadar hız yaptığını, dönüş yaparken sinyal verip vermediğini, sürüş sırasında dışarıdaki hava durumunu, hangi zamanlarda nerelere gittiğini ve en önemlisi hangi adreste ne kadar kaldığı bilgisini kaydedebilir ve İnternet sayesinde bu veriler başka aygıtlarla paylaşılabilir[33].

Nesnelerin İnterneti sayesinde çeşitli verilerin silsile halinde kaydedilmesi mümkün olmaktadır. Örneğin sağlık parametrelerinin, okuma alışkanlıklarının, yer bilgisinin, enerji kullanımının, sürüş tarzının, yeme alışkanlıklarının kaydedilmesi sayesinde kullanıcının hayatı hakkında detaylı bir görünüm elde edilebilmektedir[34]. Bu noktada bireylerin mahremiyetinin korunması gündeme gelmektedir. 2012 yılında Londra'da "Açık nesnelerin İnterneti -*Open Internet of Things"* isimli kurultayda çeşitli çalıştaylar ve açıklamalar yapılmıştır. Kurultayın sonucunda nesnelerin İnterneti konusunda varılan ana prensipler katılımcılar tarafından imzalanmıştır. Üzerinde mutabık olunan ana prensipler şunlardır: verilerin erişilebilirliği, zamanında erişimin sağlanması, mahremiyetin korunması, sürecin şeffaf olması ve verilerin kullanılmasına ilişkin izinlere dair hükümlerdir[35]. Bu Kurultay

---

32 **Walker.**

33 **Peppet,** s. 90-91.

34 **OECD,** "Machine-to-Machine Communications: Connecting Billions of Devices", OECD Digital Economy Papers No.192, 30 Jan 2012, s. 34, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2011)4/FINAL&docLanguage=En (Erişim 14.10.2015).

35 Açıklamanın tam metni ve katılımcıların listesi için bkz. Statement of the Open Internet of Things Assembly at London, United Kingdom on the 17 th June, 2012,

öncesinde bireylerin mahremiyetinin korunması için çeşitli girişimler de söz konusu olmuştur. Örneğin 2011 yılında bir şirket "Nesnelerin İnterneti Haklar Beyannamesini-*Bill of Rights for the Internet of Things*" önermiş ve bu konuda endüstriyel anlamda standartların oluşturulması açısından bir başlangıç yapmıştır[36].

Nesnelerin İnterneti söz konusu olduğunda bireylerin kendilerine ilişkin verilerin toplanmasına ve aktarılmasına önceden izin vermeleri söz konusu olacak mıdır sorusu da gündeme gelmektedir. Bu noktada yeni bir hak ortaya çıkmaktadır. Bu hak çipi etkisiz hale getirme hakkıdır *(the right to disable chips)*. Bu bir *opt-out* (vazgeçmek, çekilmek) usulüdür. Buna göre çipler öndeğer *(default)* olarak başlangıçta aktif haldedir. Kullanıcı daha sonra çipi etkisiz hale getirebilmektedir. Bir başka usul ise *opt-in* (dâhil olmak) usulü olabilir. Bu durumda çip başlangıçta aktif değildir, kullanıcı aktif hale getirip getirmemeye kendisi karar verecektir[37].

Nesnelerin İnterneti teknolojisinde kişisel verilerin kanun dışı yollardan toplanmasının cezalandırılması ile ilgili düzenlemeler yeterli değildir. Burada kullanıcıların önceden haberi olmaksızın bağlantı elemanlarının ve diğer çiplerin yerleştirilmesinin cezalandırılmasına ilişkin düzenlemelere de ihtiyaç vardır. Unutulma hakkının[38] nesnelerin İnterneti teknolojisindeki

---

https://docs.google.com/document/d/1yZAsNaesDocqqtkFgucbFS_zE4tDP1Jsfszsvls7Yuc/edit?pli=1 (Erişim 14.10.2015).

36 Xively Şirketi'nin (eski adı Pachube and Cosm), nesnelerin İnterneti konusunda bireylerin sahip olduğu hakların sıralaması için bkz. http://postscapes.com/open-internet-of-things-assembly (Erişim 14.10.2015).

37 **Barbry,** s. 93.

38 Unutulma hakkı kavramının tartışılmaya ve kanuni düzenlemelerde yer almaya başlaması ilk defa Fransa ve Arjantin'de 2006 yılında başlamıştır. **Weber,** Rolf H.: "The Right to be Forgotten More Than a Pandora's Box?", Journal of Intellectual Property, Information Technology & E-Commerce Law, Y.2011, No:2, s. 120; **Sreeharsha,** Vinod: "Google and Yahoo Win Appeal in Argentine Case", The New York Times, Yayınlanma Tarihi 19.08.2010, http://www.nytimes.com/2010/08/20/technology/internet/20google.html?_r=0 (Erişim 22.09.2015); ROSEN, Jeffrey, "The Right to be Forgotten", Stanford Law Review, Vol.64, February 13, 2012, s. 91, http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf, (Erişim 16.09.2015); Unutulma hakkı kavramını 2012 yılında Avrupa Komisyonu Başkan yardımcısı ve Avrupa Birliği Adalet Komisyon üyesi *Viviane REDING*

karşılığı nesnelerin İnterneti yoluyla elde edilen verilerin silinmesi hakkıdır. Kullanıcıların verilerinin silinmesini isteme hakları da olmalıdır[39].

Mahremiyet ve güvenlik ile ilgili endişeler nesnelerin İnterneti konusunda ilk akla gelenler olmakla birlikte gelecekte işletmelerin rekabet gücü ve rekabet hukuku ile ilgili sorunların da gündeme geleceği öngörülmektedir[40].

III. NESNELERİN İNTERNETİNE İLİŞKİN KANUNİ DÜZENLEMELER VE DİĞER ÇALIŞMALAR

Nesnelerin İnterneti teknolojisi henüz gelişme aşamasındadır. Bununla birlikte konu ile ilgili kanuni düzenlemeler de yapılmaya çalışılmaktadır. Bu konuda Avrupa Birliği'nde yapılan çalışmalara bakıldığında, 2008 yılında bakanlıklar düzeyinde toplantılar yapılarak geleceğin İnternet'i ve özellikle nesnelerin İnterneti hakkında görüşmeler yapılmıştır[41]. Yine 2009 yılında

---

tanımlamıştır. Unutulma hakkından kişilerin verileri üzerinde kontrol sahibi olabilmelerinin bir yolu olarak söz etmiştir. Buna göre kişilerin kendilerine ait kişisel verilerin işlenmesine ilişkin rızalarını geri alabilme haklarına sahip olmaları gerekir. *REDING* ayrıca İnternet'in neredeyse sınırsız bir arama ve saklama kapasitesine sahip olduğunu, küçük bir kişisel bilginin paylaşımından yıllar sonra dahi etkisini gösterebileceğini belirtmiştir. Bu itibarla bir kişi verilerinin daha fazla işlenmesini ve saklanmasını istemiyorsa ve bunun için geçerli bir neden de yoksa verilerin sistemden silinmesi gerektiği de belirtmiştir. Bundan başka unutulma hakkının mutlak bir hak olarak anlaşılmaması gerektiği, verilerin geçerli ve hukuka uygun olarak veri tabanında saklanmasına ilişkin durumların olduğunu ifade etmiştir. Gazete arşivlerini bu duruma örnek gösteren REDING, unutulma hakkının geçmişin tamamen silinmesi anlamına gelmediğini aynı şekilde ifade özgürlüğü ve medyanın özgürlüğünden daha üstün olmadığını da belirtmiştir. **Reding,** Viviane: "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age", Innovation Conference, Digital, Life, Design, (22.01.2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (Erişim 16.09.2015).

39 **Barbry,** s. 94.

40 **Federal Trade Commission,** "The Internet of Things and the FTC: Does Innovation Require Intervention?" Remarks of Commissioner Maureen K. Ohlhausen of the Commissioner, Yayınlanma Tarihi 18.10.2013, https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internetthingsremarks.pdf (Erişim 11.10.2015); **Blum.**

41 **Barbry,** s. 85.

Avrupa Komisyonu Nesnelerin İnterneti Konusunda Avrupa İçin Hareket Planı isimli bildirimi hazırlamıştır[42].

Avrupa Komisyonu 12 Nisan 2012 ve 12 Temmuz 2012 tarihleri arasında kamuoyu araştırması yaparak Nesnelerin İnternetinin Yönetişimine İlişkin Kamuoyu Araştırması Hakkında Rapor yayınlamıştır. Rapor nesnelerin İnterneti üzerine üreticilerin, tüketicilerin, akademisyenlerin, sivil toplum örgütlerinin, devlet kurumlarının, telekomünikasyon kurumlarının katılımı ile hazırlanmıştır. Raporda nesnelerin İnternetinin Avrupa Birliği vatandaşlarının hayatını sağlık, ulaşım, çevre ve enerji gibi alanlarda kolaylaştıracağı öngörülmüş, buna karşılık bireylerin mahremiyeti ve güvenliği ile ilgili riskler taşıdığı belirtilmiştir[43].

Raporun hazırlanmasında kullanılan kamuoyu araştırmasında nesnelerin İnterneti teknolojisinde veri koruma ile ilgili tedbirlerinin alınmasına gerek olup olmadığı sorusuna üretici/sanayici katılımcılar mevcut veri koruma kurallarının yeterli olduğu bu nedenle ek koruma tedbirlerine gerek olmadığı yönünde cevap vermişlerdir. Hatta bazı üreticiler kullanıcıların her bir uygulama için açık rızasının aranmasının nesnelerin İnternetinin gelişmesi önünde bir engel oluşturacağını, nesnelerin İnterneti yoluyla elde edilmiş anonimize edilmiş verilerin üçüncü kişilerle paylaşılmasının mümkün olması gerektiğini belirtmişlerdir. Buna karşılık son kullanıcıların büyük çoğunluğu ve tüketici örgütleri mevcut veri koruma kurallarının yeterli olmadığını, nesnelerin İnterneti kapsamında mahremiyet ve veri koruma alanında daha fazla çalışma yapılması gerektiğini belirtmişlerdir. Ayrıca veri öznelerine ait verilerin yine onların kontrolünde kalması gerektiğini belirterek bazı prensiplerin olması gerektiğinden söz etmişlerdir. Buna göre, kullanıcıların rızasının alınmasından ziyade kullanıcının nesnelerin İnterneti sistemine dâhil olmayı isteme veya istememeyi seçebilmesi gerektiği

---

42 **Commission of the European Communities,** "Internet of Things – An Action Plan for Europe", Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions", Brusseles 18.06.2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF (Erişim 12.10.2015).

43 **European Commission,** "Report on the Public Consultation on IoT Governance", http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746, s. 2, Yayınlanma 16.01.2013, Erişim 08.10.2015.

belirtilmiştir. Aynı zamanda verilerin silinmesi ve unutulma hakkının da korunması gerektiği belirtilmiştir. Belirtilen bir diğer husus kullanıcının açık rızası olmadan kişisel verilerin o nesneye ilişkin uygulama programının amacının dışında kullanılamaması gerektiğine ilişkindir. Şeffaflığın sağlanması yani kullanıcıların veri toplamanın mahiyeti ve amacı hakkında bilgilendirilmesi gerektiği de son kullanıcıların cevaplarında yer almıştır. Bunlara ek olarak mahremiyetin sağlanmasının nesnelerin İnternetine ilişkin uygulamalarda öndeğer *(privacy by default and design)* olarak tasarlanması gerektiğine işaret edilmiştir. Ayrıca hukuka uygun olmayan bir şekilde verilere erişimin engellenmesi açısından sistem güvenliğinin (şifreleme dâhil olmak üzere) öncelikli olması gerektiği ifade edilmiştir. Verilerin saklanmasının zamanla sınırlı olması bununla birlikte isteyen kişilerin verilerin saklanmasına izin vermeme hakkına da sahip olması gerektiği talepler arasındadır. Ayrıca hesap verilebilirlik, dürüstlük kurallarına, etik ve hukuk kurallarına uygun kullanım sağlanmalıdır diyen katılımcılar vardır. Bazı katılımcılar veri koruma konusunda denetim yapacak bağımsız otoritelerin olması gerektiğini de belirtmiştir[44].

Raporda kamuoyu araştırmasına katılan sanayi alanında faaliyet gösteren işletmelerin henüz gelişme döneminde olan bir sektörde kamunun dâhil olmasını sorguladıkları görülmektedir. Üreticiler nesnelerin İnterneti teknolojisinin ve uygulamalarının bu konuda yapılacak kanuni düzenlemeler ile ilgili hareket tarzının belirlenmesi beklenmeden gelişmesi gerektiğini belirtmiştir. Üreticiler mevcut veri koruma ve rekabet kurallarının ve güvenlik ve çevre ile ilgili hukuki düzenlemelerin hâlihazırda son kullanıcıyı zaten koruduğunu, ayrıca nesnelerin İnterneti konusunda yapılacak uygunsuz yönetişimin bu alanda yapılacak yatırımlara ve yeniliklere engel oluşturacağını da ileri sürmüşlerdir. Buna karşılık son kullanıcılar, sivil toplum ve tüketici kuruluşlarını destekleyerek, mahremiyet, güvenlik gibi temel haklar ve etik hususlar söz konusu olduğunda ekonomik hususların geri planda olduğuna, nesnelerin İnterneti kapsamında son kullanıcıların haklarının tam olarak korunması gerektiğine işaret etmişlerdir. Raporda son kullanıcıların nesnelerin İnterneti pazarının rekabetçi bir şekilde gelişememesi ve tüketicilerin belirli teknolojiler ve/veya belirli üreticilere mahkûm olması riskinden de

---

44 **European Commission,** s. 3-4.

söz edilmektedir. Bu itibarla nesnelerin İnterneti konusunda özel düzenlemeler yapılarak bu alandaki teknolojinin ve pazarın gelişiminin kontrolünün sağlanması, bu alandaki meselelerin yönetişimi *(governance)* ile ilgili olarak sivil toplum örgütlerinin temsil edildiği çok paydaşlı platformun gerekliliğine değinilmiştir[45].

Tasarı halindeki Avrupa Birliği Veri Koruma Tüzüğü'nde getirilen yeniliklere bakıldığında kamuoyu araştırmasında katılımcıların taleplerinden bazılarının karşılandığı görülebilmektedir. Kişisel verilere en az şekilde erişimin öndeğer olarak kabul edilmesi *(privacy by design and default)* mevcut Avrupa Birliği Veri Koruma Direktifi'nde yer almazken tasarı halindeki Veri Koruma Tüzüğü'nün 23 ve 33.maddelerinde düzenlenmiştir. Buna göre veri işleme için kullanılacak sistemlerde veri kontrolörleri *(data controller)* veri öznelerinin *(data subject)* haklarının korunması için gerekli tedbirleri almak zorundadır. Bu itibarla veri işleme faaliyetlerinin gerekli amaçlar için minimum düzeyde olmasının öndeğer kabul edilmesi sağlanmalıdır (Tasarı md.23). Tüzük'te ayrıca sınırlayıcı bir sayım olmamakla birlikte mahremiyetin öndeğer olarak kabul edilmesini gerektiren faaliyetlere örnek olarak sistematik profil çıkarma; sağlık, cinsel yaşam, ırk ve etnik köken ile ilgili bilginin işlenmesi; kamuya açık alanlarda büyük ölçekli video güvenlik kaydı yapılması; çocuklara ilişkin verilerin, biyometrik verilerin veya genetik verilerin büyük ölçekli dosyalama sistemlerinde işlenmesi sayılmıştır (Tasarı md.33). Düzenlemenin devamında mahremiyetin öndeğer olarak kabul edilmesinin içeriği, veri işleme faaliyetine ilişkin açıklamanın yapılması, veri öznesi için risklerin ne olduğunun ve bu risklere karşı veri kontrolörünün alacağı önlemlerin ne olduğunun açıklanması şeklinde düzenlenmiştir[46]. Veri Koruma Tüzüğü'nde veri öznesinin rızası (Tasarı md.6, 9), veri öznesinin profilinin çıkarılması için toplanan verilerin hukuka uygun olarak kullanılması (Tasarı md.20), gizlilik politikası *(privacy policy)* (Tasarı md.11, 14) veri korumaya ilişkin yükümlülüklerin yerine getirilmemesi halinde yaptırımlara (Tasarı md.79) ilişkin düzenlemeler de yer almaktadır.

---

45 **European Commission,** s. 15.

46 **Hunton&Williams,** "The Proposed EU General Data Protection Regulation", A Guide for in-house lawyers, June 2015, s. 21, https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf (Erişim 09.10.2015).

Nesnelerin İnterneti konusunda Amerika Birleşik Devletleri'nde mahremiyet ve veri güvenliği ile ilgili düzenlemelerin yapılması gündemdedir[47]. Amerika Birleşik Devletleri'nde kişisel verilerin korunmasına ilişkin federal bir düzenleme bulunmamaktadır. Bununla birlikte sektörel bazda hazırlanmış kanunlar bulunmaktadır. Örneğin Federal Ticaret Komisyonu *(Federal Trade Commission)* Çocukların Çevrimiçi Mahremiyetinin Korunması Kanunu'nun uygulamasını yürütmektedir[48] *(Children's Online Privacy Protection Act_COPPA)*. Bu Kanun websiteleri veya online hizmet veren operatörlere on üç yaşından küçüklerin kişisel verilerinin toplanmasında sınırlandırmalar ve yükümlülükler getirmektedir. Yine Birleşik Devletler Sağlık ve İnsani Hizmetler Dairesi *(U.S.Department of Health and Human Services),* ilgili kurumlarda sağlık verilerine ilişkin mahremiyet, güvenlik ve ihlal bildirimi konusunda milli standartlar içeren Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası'nın *(HIPAA-Health Insurance Portability and Accountability Act)* uygulamasını yürütmektedir. Bu Kanun ile hastalara ilişkin hassas verilerin korunması konusunda standartlar getirilmiştir. Buna göre bu tarz veriler ile uğraşan şirketlerin, her türlü fiziksel, ağ ve işlemeye ilişkin güvenlik önlemlerini almaları gerekmektedir[49].

Eyalet kanunlarına bakıldığında öne çıkan kanunlardan bir tanesi Kaliforniya Çevrimiçi Mahremiyetin Korunması Kanunu'dur *(California Online Privacy Protection Act)*. Bir diğeri ise Masaçusets Tüzüğü'dür *(Massachusetts Regulation)*. Federal bir yasanın olmaması nedeni ile Federal Ticaret Komisyonu'nun yönlendirici bir rolü bulunmaktadır. Bu kapsamda Komisyon mahremiyet ile ilgili çerçeve niteliğinde kuralları *(privacy framework)* yayınlayarak belirli bir tüketici, bilgisayar ya da başka bir aygıt ile ilişkilendirilebilen tüketici verileri toplayan veya kullanan şirketlere bu konudaki en iyi olabilecek uygulamaları açıklamıştır. Komisyonun özellikle üzerinde durduğu temel prensipler, ürün tasarımı aşamasında mahremiyetin

---

47 **Walker.**

48 Komisyon'un çalışmaları ile ilgili detaylı bilgi için bkz. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (Erişim 10.10.2015).

49 http://www.onlinetech.com/resources/references/what-is-hipaa-compliance (Erişim 10.10.2015).

dikkate alınması *(privacy by design),* tüketicilere kolaylaştırılmış seçim imkânı tanınması *(simplified consumer choice)* ve şeffaflıktır *(transperancy)*[50].

Nesnelerin İnterneti konusunda mahremiyet ve güvenlik ile ilgili faaliyetleri olan diğer bir kuruluş ise Birleşik Devletler Enerji Dairesi'dir *(U.S.Department of Energy).* Daire akıllı sayaçlarda mahremiyet ve güvenlik ile ilgili çok taraflı katılımcıların olduğu toplantılar yapmıştır. Bir başka kurum, motorlu araçlar ile ilgili siber güvenlik araştırmalarını başlatan Birleşik Devletler Ulaştırma Dairesi Ulusal Yollar Trafik Güvenlik İdaresi'dir *(U.S. Department of Transportation's National Highway Traffic Safety Administration)*. Birleşik Devletler Yiyecek ve İlaç İdaresi *(U.S.Food and Drug Administration)* birbiri ile bağlantılı tıbbi cihazlarda siber güvenliğin sağlanması ile ilgili kılavuz yayınlamıştır. Federal İletişim Komisyonu *(Federal Comunication Commission)* kablosuz ağlar ile taşınan tüketici bilgilerinin kullanılmasında gizliliğe ilişkin kuralların uygulanmasında görevlidir[51].

Nesnelerin İnternetinde mahremiyetin korunması ile ilişkilendirilebilecek açık bir kanuni düzenlemeye örnek ise Kaliforniya'da 1 Ocak 2014 tarihinde yürürlüğe giren ve Medeni Kanun'un mahremiyet ile ilgili bölümüne eklenen akıllı sayaçlardan elde edilen verilerin korunmasına ilişkin düzenleme verilebilir. Bu düzenleme ile işletmelere müşterilere ait akıllı sayaçlar ile İnternet üzerinden iletilen elektrik ve gaz tüketim bilgilerinin açıklamasına sınırlama getirilmiştir[52].

İnsan Hakları Evrensel Beyannamesinde mahremiyetin temel bir insan hakkı olması itibarıyla Amerika Birleşik Devletleri'nde Radyo frekansı ile kimlik saptama *(RFID)* teknolojisinin kullanımı ile ilgili çalışmalar da

---

50 **Blum; Federal Trade Commission,** "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers", March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (Erişim10.10.2015).

51 **Blum.**

52 **Alston&Bird LLP,** "California's New Privacy Law Covering Utility Smart Meter Data Takes Effect on January 1, 2014", Yayınlanma 02.12.2013, http://www.lexology.com/library/detail.aspx?g=f502e9aa-af91-49ae-b997-6ace73f56069 (Erişim 11.10.2015).

yapılmıştır. Federal Ticaret Komisyonu *(Federal Trade Commission-FTC)* tarafından çevrimiçi mahremiyetin korunmasına ilişkin Dürüst Bilgi Uygulamaları'nın *(Fair Information Practices)* RFID teknolojisinin kullanımına da adapte edilmesi tavsiyesinde bulunmuştur. Buna göre ürünlerin satışından sonra takibi hakkında uygun bir şekilde mağazada uyarıların bulunması gerekmektedir. Müşterilerin satın aldıkları ürünlerde RFID teknolojisi içeren bir yonga/çip bulunduğu hususunda uyarılması ile müşterilerin isterlerse o ürünü satın almamaları mümkün olacaktır[53].

IV. TÜRK HUKUKUNDA NESNELERİN İNTERNETİ

Türk hukukunda nesnelerin İnternetine ilişkin özel bir kanuni düzenleme mevcut değildir. Bununla birlikte bazı kanunlardaki hükümler konu ile ilişkilendirilebilir. Öncelikle 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dan bahsetmek gerekir. Bu Kanun'un amacı, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir (Kanun m.1). Kanun'un 8.maddesi uyarınca İnternet ortamında yapılan ve içeriği yine Kanun'da sayılan suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir. Bu suçlar Türk Ceza Kanunu'nda yer alan intihara yönlendirme; çocukların cinsel istismarı; uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma; sağlık için tehlikeli madde temini; müstehcenlik; fuhuş; kumar oynanması için yer ve imkân sağlama suçları ve Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlardır. Nesnelerin İnterneti sayesinde toplanan verilerin söz konusu suçları oluşturacak şekilde İnternet'te yayınlanması halinde ilgili İnternet sitesine erişim engellenebilecektir. Örneğin üzerinde sensörü olan oyuncak sayesinde bir çocuğun elde edilen görüntülerinin bir İnternet sitesinde çocuğun cinsel istismarı teşkil edecek şekilde yayınlanması durumunda 5651 sayılı Kanun'da düzenlenen erişimin engellenmesi mümkün olabilecektir.

---

53 **Peslak**, Alan R.: "An Ethical Exploration of Privacy and Radio Frequency Identification", Journal of Business Ethics, Y.2005, S. 569, s. 337.

Türk Ceza Kanunu'nun 243.maddesinde bilişim sistemine girme ve kalma suçu düzenlenmiştir[54]. Bilişim sisteminin çeşitli tanımları olmakla birlikte Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in 3(1)(b) maddesindeki tanım *"bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem"* şeklindedir. Dolayısıyla nesnelerin İnterneti teknolojisi ile birbirine bağlanan nesnelerin oluşturduğu sistem Türk Ceza Kanunu anlamında bir bilişim sistemi oluşturabilir. Bu sisteme yetkisiz olarak giren ve kalan kişi suç işlemiş olacaktır. Türk Ceza Kanunu'nun 244.maddesinde ise bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçu düzenlenmiştir[55]. Buna göre birbiri ile bağlantılı nesnelerin oluşturduğu sisteme yetkisiz olarak giren, bu nesneler arasındaki veri akışını engelleyen, bozan, verileri yok eden veya değiştiren, başka bir yere aktaran kişi 244.maddedeki suçu işlemiş olacaktır.

Nesnelerin İnterneti ile ilgili olabilecek bir diğer kanun ise Tüketicinin Korunması Hakkında Kanun'dur. Bu Kanun'un 5.maddesinde tüketiciyle müzakere edilmeden sözleşmeye dâhil edilen ve tarafların sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olan sözleşme şartları haksız şart olarak düzenlenmiştir. Tüketiciyle yapılan sözleşmelerde yer alan haksız şartlar kesin olarak hükümsüzdür. Konumuz bakımından bir örnek vermek gerekirse, tüketicinin satın aldığı nesne İnternet'e bağlanmak suretiyle sensörü sayesinde topladığı kişisel verileri satıcıya iletiyorsa ve satış sözleşmesinde veya o nesneyi kullanmak için indirilen uygulamaya ilişkin sözleşmede kişisel verilerin satıcı tarafından istenilen şekilde kullanılabileceği, başkasına satılabileceği ve buna kullanıcının/tüketicinin hiçbir şekilde itiraz edemeyeceği yönünde hüküm varsa bu hüküm haksız şart teşkil edebilir. Ayrıca Türk Ticaret Kanunu'nun 55.maddesi uyarınca dürüstlük kuralına aykırı işlem şartı kullanılarak hazırlanan genel işlem şartlarını kullanmak haksız

---

54 Geniş açıklama için bkz. **Erdoğan,** Yavuz: "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 12, Özel S., 2010, s. 1363-1433.

55 Geniş açıklama için bkz. **Yılmaz,** Sacit: "5237 sayılı TCK'nın 244.Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, 2011(92), s. 62-100.

rekabet de teşkil eder. Yine Türk Borçlar Kanunu'nun 21.maddesi uyarınca "*karşı tarafın menfaatine aykırı genel işlem koşullarının sözleşmenin kapsamına girmesi, sözleşmenin yapılması sırasında düzenleyenin karşı tarafa, bu koşulların varlığı hakkında açıkça bilgi verip, bunların içeriğini öğrenme imkânı sağlamasına ve karşı tarafın da bu koşulları kabul etmesine bağlıdır. Aksi takdirde, genel işlem koşulları yazılmamış sayılır. Sözleşmenin niteliğine ve işin özelliğine yabancı olan genel işlem koşulları da yazılmamış sayılır".*

Türkiye Cumhuriyeti Anayasası'nın 20.maddesinde özel hayatın gizliliği başlığı altında *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*[56]*"* hükmü yer almaktadır. Bu itibarla nesnelerin İnterneti sayesinde kişisel verileri toplanan kişiler bu verilerin korunmasını isteme, bu verilerin nasıl kullanılacağını bilme ve silinmesini isteme hakkına sahiptir. Ayrıca nesnelerin İnterneti sayesinde toplanan kişisel veriler ile ilgili olabilecek diğer mevzuat hükümleri Kişisel Verilerin Korunması Kanunu Tasarısı'nda[57] bulunmaktadır. Kanun Tasarısı uyarınca kişisel veriler ancak kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir (m.4). Ayrıca kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez (m.5). Özel nitelikli kişisel verilerin işlenmesi yasaktır. Bu veriler ancak yeterli önlemlerin alınması şartıyla Tasarı'da belirtilen hallerde işlenebilir (m.6). Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde, resen veya ilginin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir (m.7). Kişisel veriler ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (m.8). Kişisel verilerin elde edilmesi sırasında veri sorumlusu kişisel verilerin hangi amaçla

---

56 5982 sayılı Türkiye Cumhuriyeti Anayasası'nın Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun, 2.maddesi ile Anayasanın 20.maddesine eklenen ifade. RG.,T.13.05.2010, S. 27580.

57 Tasarı metni için bkz. http://www2.tbmm.gov.tr/d26/1/1-0541.pdf (Erişim 28.02.2016).

işleneceği, kimlere ve ne amaçla aktarılabileceği hakkında ilgili kişilere bilgi vermekle yükümlüdür (m.10).

Türk Medeni Kanunu'nun 24.maddesinde ise kişiliğin saldırılara karşı korunmasına ilişkin madde bulunmaktadır. Yine Türk Ceza Kanunu'nun 135.maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi ile ilgili bir düzenleme, 136.maddesinde verileri hukuka aykırı olarak verme veya ele geçirme ile ilgili bir düzenleme, 138.maddede verileri yok etmeme başlıklı bir düzenleme yer almaktadır[58].

Bir pirinç tanesi büyüklüğünde olan radyo frekansı teknolojisi (RFID) çiplerinin günümüzde insan bedeninde deri altına yerleştirilmesi mümkündür. Amerika Birleşik Devletleri'nde ve İsveç'te bazı işyerlerinde işçilerin koluna deri altına bu küçük çipler yerleştirilmek suretiyle onların işe giriş çıkış saatleri, bulundukları yerler takip edilebilmektedir. İşçilerin taşıdığı bu çipler akıllı telefonlar ile bilgisayarlar ile bağlantı halinde olabilmektedir[59]. Bu çiplerin çıkarılması için küçük bir operasyon ile derinin kesilmesi gerekmektedir. Türk hukuku açısından bakılacak olursa böyle bir uygulama işçi kabul etse dahi etik olarak tartışılabilir. İşverenin işçiyi bu mikroçipleri takmaya zorlaması İş Kanunu madde 24 anlamında ahlak ve iyiniyet kurallarına uymayan hal sayılabilir. Ayrıca işverenin gözetim borcu kapsamında işçinin sağlığını ve güvenliğini sağlaması gerektiğinden çiplerin işçilerin vücuduna yerleştirilmesinin bu kapsamda uygun olup olmadığı tartışılabilir.

Fikir ve Sanat Eserleri Kanunu ile de nesnelerin İnterneti ilişkilendirilebilir. Özellikle telif hakkı ihlalleri ve patent ile ilgili sorunlar burada gündeme gelebilecektir. Bunun dışında nesnelerin İnternetinde en önemli hususlardan olan bilgi güvenliğinin ve haberleşme gizliliğinin korunması

---

58 Geniş bilgi için bkz. **Gürkaynak,** Gönenç/**Yılmaz,** İlay: "The International Comparative Legal Guide to: Data Protection 2015-TURKEY", 2nd Edition, www.iclg.co.uk, (Erişim 16.09.2015).

59 **Sieberg,** Daniel: "A Company Requires Employees to have an RFID Chip Implanted Under Skin", http://www.gvsu.edu/cms3/assets/2D085406-FC80-AE2E-7233BDF30DCE3642/electronicmonitoringofemployees/employees_required_to_be_rfid_chipped.pdf (Erişim 05.02.2016); **Burton,** Bonnie: "Swedish Office Gets Under Employees' Skin With RFID Microchips", CNET, yayınlanma tarihi 03.02.2015, http://www.cnet.com/news/swedish-office-gets-under-employees-skin-with-rfid-microchips/ (Erişim 05.02.2016).

Elektronik Haberleşme Kanunu'nda ilke olarak kabul edilmiştir (m.4(l)). Elektronik İmza Kanunu yine nesnelerin İnterneti ile ilişkilendirilebilecek bir başka hukuki düzenlemedir.

SONUÇ VE ÖNERİLER

Nesnelerin İnterneti teknolojisi kullanıcılara pek çok kolaylık getirmektedir. Bununla birlikte, bireylerin toplanan verilerinin (tüm bu verilerin toplamından oluşan büyük verinin de/big data) nasıl kullanılacağı konusunda açıklık yoktur. Kişisel verilerin gizliliğinin ve güvenliğinin korunması hususunda endişeler söz konusudur. Konu hakkındaki milli ve milletlerarası kanuni düzenlemeler henüz yeterli değildir. Ayrıca sensör taşıyan bir nesnenin üreticisinin kullanıcının bulunduğu ülkeden başka bir ülkede olması durumunda yargılama yetkisi ve uygulanacak hukuk ile ilgili sorunlar çıkabilecektir.

Nesnelerin İnterneti teknolojisi hakkında kullanıcıların/tüketicilerin üreticiler tarafından yeterince bilgilendirilmeleri gerekmektedir. Bunun yanısıra kullanıcılara kolaylıkla sistemden çıkabilme imkânının sağlanması ve/veya kullanıcının rızasının önceden alınması gerekmektedir[60].

Nesnelerin İnterneti teknolojisi içeren ürünleri satın alan tüketicilerin bu ürünlerin kullanımı hakkında bilinçlendirilmeleri gerekmektedir. Tüketicilerde veri mahremiyetinin/gizliliğinin korunması ve veri güvenliği konusunda farkındalık ve duyarlılığın artırılması için çalışmalar yapılmalıdır. Türk hukukunda yapılabilecek kanuni düzenlemeler bakımından nesnelerin İnternetinin mevcut Veri Koruma Kanunu tasarısı içinde yer alması veya yönetmeliklerle sektörel bazda (sağlık, otomobil, akıllı ev teknolojisi vs. için ayrı ayrı) düzenlenmesi düşünülebilir. Ayrıca Tüketicinin Korunması Hakkında Kanun ve Türk Ceza Kanunu kapsamında nesnelerin İnternetine

---

60 Kullanıcının rızasının alınamadığı durumlarda ise verilerin başlangıçtakinden başka bir amaçla kullanılmasından veya üçüncü kişilerle paylaşılmasından önce anonimize edilmesi gerektiği öneri olarak getirilmiştir. **Article 29 Data Protection Working Party,** "Opinion 8/2014 on the Recent Developments on the Internet of Things", Adopted on 16 September 2014, 14/EN WP 223, s. 20, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Erişim 12.10.2015).

ilişkin özel hükümler eklenebilir. Nesnelerin İnterneti teknolojisi içeren bir ürünü satın alan tüketicinin bu ürünü kullandığında kendisi hakkında hangi verilerin toplandığı, bu verilerin nasıl kullanılacağı konusunda bilgi sahibi olması hukuken sağlanmalıdır. Bunun dışında üreticilere standartlar getirilerek, veri mahremiyetinin ve güvenliğinin üretimde ön planda tutulması hususu şart koşulabilir. Yine yurt dışından nesnelerin İnterneti teknolojisi içeren ürünlerin ithalatının yapılması halinde ithal ürünlerde de aynı standartlara uygun olma koşulu getirilebilir.

KAYNAKLAR

Adshead, Anthony: "Data Set to Grow 10-fold by 2020 as Internet of Things Takes Off", http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off, Yayınlanma 09.04.2014 (Erişim 08.10.2015)

Akgül, Aydın: "Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı", TBB Dergisi, 2015(118), s. 199-222.

Alston&Bird LLP: "California's New Privacy Law Covering Utility Smart Meter Data Takes Effect on January 1, 2014", Yayınlanma 02.12.2013, http://www.lexology.com/library/detail.aspx?g=f502e9aa-af91-49ae-b997-6ace73f56069 (Erişim 11.10.2015).

Article 29 Data Protection Working Party: "Opinion 8/2014 on the Recent Developments on the Internet of Things", Adopted on 16 September 2014, 14/EN WP 223, s. 20, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (Erişim 12.10.2015).

Ashton, Kevin: "That Internet of Things Thing", RFID Journal, Yayınlanma 22.06.2009, http://www.rfidjournal.com/articles/view?4986 (Erişim 16.10.2015).

Barbry, Eric: "The Internet of Things, Legal Aspects What Will Change Everything", Digiworld Economic Journal, no.87, 3rd Q.2012, s. 87, http://innovation-regulation2.telecom-paristech.fr/wp-content/uploads/2012/10/CS87_BARBRY.pdf (Erişim 12.10.2015).

Blum, Philip: "Internet of Things', 101: Legal Concerns-Law 360, http://www.law360.com/articles/526266/internet-of-things-101-legal-concerns (Erişim 08.10.2015).

Bunn, Julian: "How Big Is a Petabyte, Exabyte, Zettabyte, Or a Yottabyte?" High Scalability, http://highscalability.com/blog/2012/9/11/how-big-is-a-petabyte-exabyte-zettabyte-or-a-yottabyte.html, Yayınlanma 11.09.2012 (Erişim 08.20.2015).

CİSCO: "The Internet of Everything-Global Public Sector Economic Analysis", Yayınlanma 2013, s. 1, https://www.cisco.com/web/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf (Erişim 16.10.2015).

Commission of the European Communities: "Internet of Things – An Action Plan for Europe", Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions", Brusseles 18.06.2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF (Erişim 12.10.2015).

Erdoğan, Yavuz: "Bilişim Sistemine Girme ve Kalma Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 12, Özel S., 2010, s. 1363-1433.

European Commission: "Report on the Public Consultation on IoT Governance", http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1746, s. 2, Yayınlanma 16.01.2013, Erişim 08.10.2015.

Federal Trade Commission: "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers", March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (Erişim10.10.2015).

Federal Trade Commission: "The Internet of Things and the FTC: Does Innovation Require Intervention?" Remarks of Commissioner Maureen K. Ohlhausen of the Commissioner, Yayınlanma Tarihi 18.10.2013, https://www.ftc.gov/sites/default/files/documents/public_statements/internet-things-ftc-does-innovation-require-intervention/131008internettthingsremarks.pdf (Erişim 11.10.2015).

Gürkaynak, Gönenç/**Yılmaz,** İlay: "The International Comparative Legal Guide to: Data Protection 2015-TURKEY", 2nd Edition, www.iclg.co.uk, (Erişim 16.09.2015).

Hunton&Williams: "The Proposed EU General Data Protection Regulation", A Guide for in-house lawyers, June 2015, s. 21,

https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/Hunton_Guide_to_the_EU_General_Data_Protection_Regulation.pdf (Erişim 09.10.2015).

Kaya, Cemil: "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi", İÜHFM, C.LXIX, S. 1-2, s. 317-334.

OECD: "Machine-to-Machine Communications: Connecting Billions of Devices", OECD Digital Economy Papers No.192, 30 Jan 2012, s. 34, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2011)4/FINAL&docLanguage=En (Erişim 14.10.2015).

Pearl, Robert: "Cisco CEO John Chambers: American Health Care is At a Tipping Point", Forbes, Yayınlanma 28.08.2014, http://www.forbes.com/sites/robertpearl/2014/08/28/cisco-ceo-john-chambers-american-health-care-is-at-a-tipping-point/ (Erişim 16.10.2015).

Peppet, Scott: "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review, Vol.93, s. 85-176.

Peslak, Alan R.: "An Ethical Exploration of Privacy and Radio Frequency Identification", Journal of Business Ethics, Y.2005, N.59, s. 327-345.

Taylor, Daniel: "NSA Cyber War Will Use Internet Connected Devices as Weapons Platform; Your Home is the Battlefield", Global Research, Yayınlanma 19.01.2015, http://www.globalresearch.ca/nsa-cyber-war-will-use-internet-of-things-as-weapons-platform-your-home-is-the-battlefield/5425526 (Erişim 21.10.2015).

Vickery, James: "Legal Tech Series: What is the Internet of Things?", https://www.youtube.com/watch?v=5bSa2QGA9Dk, Yayınlanma 21.06.2015, (Erişim 08.10.2015).

Walker, Kim: "The Legal Considerations of the Internet of Things", Computer Weekly, http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things (Erişim 07.10.2015).

Yetimler, Emrah: "Internet of Things (Nesnelerin İnterneti) Nedir? Cihazların Etkileşim Trendleri," http://www.karel.com.tr/blog/internet-

things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri (Erişim 14.10.2015).

Yılmaz, Sacit: "5237 sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, 2011(92), s. 62-100.

YARARLANILAN İNTERNET SİTELERİ

http://postscapes.com/open-internet-of-things-assembly (Erişim 14.10.2015).

http://www.donanimhaber.com/isletim-sistemleri/haberleri/Google-Nesnelerin-interneti-icin-yeni-bir-isletim-sistemi-gelistiriyor.htm, Yayınlanma 22.05.2015 (Erişim 08.10.2015).

http://www.onlinetech.com/resources/references/what-is-hipaa-compliance (Erişim 10.10.2015).

http://www.technovelgy.com/ct/technology-article.asp (Erişim 13.10.2015).

http://www.theguardian.com/technology/2014/nov/21/driverless-cars-hacking-threat-road-trials-january (Erişim 17.02.2016).

https://docs.google.com/document/d/1yZAsNaesDocqqtkFgucbFS_zE4tDP1Jsfszsvls7Yuc/edit?pli=1 (Erişim 14.10.2015).

https://secure-nikeplus.nike.com/plus/products/fuelband/ (Erişim16.10.2015).

https://www.fitbit.com/whyfitbit (Erişim 16.10.2015).

https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule (Erişim 10.10.2015).

www.tdk.gov.tr (Erişim 08.10.2015).