

Nesnelerin İnterneti ve Hukuk

Armağan Ebru BOZKURT YÜKSEL

Dokuz Eylül Üniversitesi İİBF İşletme Bölümü Ticaret Hukuku ABD armagan.bozkurt@deu.edu.tr

Özet

Nesnelerin İnterneti birbiri ile bağlantılı aygıtlarla ilgilidir. Pek çok kolaylık sağlayan bu teknoloji ile ilgili çeşitli hukuki sorunlar gündemdedir. Konu ile ilgili hukuki düzenlemeler henüz tam olarak hazırlanmadığı için de 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 Sözcükler: Nesnelerin İnterneti, Radyo Frekansı ile Kimlik Saptama, Güvenlik, Mahremiyet, Kişisel Verilerin Korunması

Abstract

Internet of things is about the devices that can connect to each other. There are many legal issues on the agenda about this technology. There are also concerns about this technology since the legal regulations have not prepared. 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, Radio Frequency Identification, Security, Privacy, Personal Data Protection

1. Giriş

Birbiriyle bağlantılı nesneleri ilgilendiren nesnelerin İnterneti teknolojisi insan hayatını kolaylaştırıcı bir gelişmedir. Bununla birlikte özellikle hukuki açıdan pek çok sorunu da beraberinde getirmektedir. Nesnelerin İnterneti teknolojisi sayesinde pek çok veri gerçek zamanlı olarak toplanabildiğinden bunların işlenmesi, güvenliği ile ilgili endişeler gündemdedir.

2. Genel Olarak Nesnelerin İnterneti

Nesnelerin İnterneti teknolojisinde algılayıcısı/sensörü olan her çeşit nesnenin İnternet'e bağlanarak birbirleri ile haberleşmesi söz konusudur.[1] Nesnelerin İnterneti akıllı nesnelerin oluşturduğu merkezi olmayan ağ şeklinde tanımlanabilir. Bu nesnelere algılayabilen, kayıt tutabilen, yorum yapabilen, bilgi iletişiminde bulunabilen ve kendi başına ya da diğer nesnelere birlikte işleyen nesnelere denir. Bu teknolojiye nesnelere diğer nesnelere ile bilgisayarlar ile veya diğer kişiler ile bağlantı kurulabilmektedir. [2]

Nesnelerin İnterneti (*Internet of Things*) terimi ilk defa 1999 yılında Kevin Ashton tarafından yapılan bir sunumda kullanılmıştır. [3]

Nesnelerin İnterneti teknolojisinin pek çok avantaj sağlayacağı düşünülmektedir. Bunlardan bir tanesi uzaktan özellikle beyaz eşyalardaki arızaların anlaşılabilir ve gerekli programlamanın servisler tarafından yapılabilmesidir. Başka bir avantajı üreticilerin bu teknoloji sayesinde kullanıcıların ürünleri tam olarak nasıl kullandığı bilgisine ulaşabilmeleri ve böylece gereksiz fonksiyonlar üzerinde çalışmak yerine gerekli olan özellikler üzerinde yoğunlaşabilmeleridir. [4] Nesnelerin İnterneti sayesinde bugün çok büyük miktarlarda

gerçek zamanlı bilgi elde edilebilmekte ve paylaşılabilir. [5] 2020 yılı itibarıyla 5 milyar aygıtın İnternet'e bağlı olacağı tahmin edilmektedir. [6]

Nesnelerin İnterneti sadece nesnelerin İnternet'e bağlanması olarak algılanmamalıdır. RFID yongaları/çipleri okuyabilen sensörlerden oluşan yeni bir ağ modeli de bu kavramın içindedir. [7] RFID (Radio Frequency Identification-Radyo frekansı ile kimlik saptama) teknolojisinde 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. [8] RFID sisteminde tüm nesnelere bir etiket taşımak suretiyle bir sensörün önünden geçerken bilgi alışverişi yapılabilir. [9]

3. Hukuki Sorunlar

Nesnelerin İnterneti ile ilgili hukuki sorunlardan ilki ayrımcılık ile ilgilidir. Bu teknolojiyi kullanan kişiler hakkında toplanan verilerden o kişiler ile ilgili pek çok bilginin elde edilebilir olması çeşitli açılardan ayrımcılığı gündeme getirebilir. Örneğin nesnelerin İnterneti sayesinde bir spor/sağlık takipçisi bileklik şeklindeki ürün onu kullananın egzersiz rutinini, tansiyonunu takip edebilir. Nesnelerin İnterneti sayesinde bileklik ile elde edilen veriler sayesinde kiraya verenler, işverenler, sigorta şirketleri gibi ekonomik aktörler kullanıcılar arasında ekonomik ayrımcılık yapabilir. Yine kişinin araç sürüş alışkanlıkları ya da egzersiz alışkanlıkları veya evdeki elektriği kullanma alışkanlıkları sigorta şirketleri, bankalar ve işverenler tarafından o kişi/tüketici hakkında karar vermede kullanılabilir. [10]

Nesnelerin İnterneti ile ilgili başka bir hukuki sorun ise veri güvenliğinin ihlalidir. Nesnelerin İnterneti teknolojisinde nesnelerin üzerindeki sensörlerin toplandığı verilerin çalınması mümkündür. [11]

Nesnelerin İnterneti teknolojisini taşıyan ürünleri kullanan tüketiciler bu ürünleri kullanmaları durumunda kendileri hakkında toplanacak verilere ilişkin olarak gizlilik politikası konusunda ya hiç bilgilendirilmemekte ya da gizlilik politikasının içeriği konusunda yeterince aydınlatılmamaktadırlar. Üreticiler bir gizlilik politikası metni hazırlasalar dahi kullanıcıların toplanan verilerinin kime ait olacağı, tam olarak hangi verilerin sensör tarafından toplandığı, ne kadar veri toplandığı, bu verilerin nasıl kullanılacağı veya satılacağı konularında tam bir açıklık olmadığı da görülmektedir. [12]

Güvenlik ile ilgili bir diğer endişe ise nesnelerin İnterneti sayesinde kötünietli kişilerin suç işlemelerinin kolaylaşabilmesidir. Örneğin, akıllı bir eve akıllı cep telefonu sayesinde bağlanılabildiği durumda kötünietli bir kişi bu evin merkezi ısıtma sistemini ev sahibinin cep telefonuna ulaşmak 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. [13] Ayrıca nesnelerin İnterneti teknolojisinin gelişmesi ile gelecekte saldırıların (*hacking*) artması ve savaşların artık siber savaşlara dönüşeceği öngörülmektedir. [14]

Nesnelerin İnterneti sayesinde çok fazla veri toplanabildiğinden bu teknolojinin gelişmesi için gayret gösterenlerin ilgisiz verilerin toplanmaması, veri güvenliğinin sağlanması ve verilerin toplanma amacının dışında kullanılmaması gerekmektedir. [15]

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 profili çıkarılabilir. [16] Bu itibarla kişilerin mahremiyetinin korunması gerekmektedir.

Nesnelerin İnterneti teknolojisinde kişisel verilerin kanun dışı yollardan toplanmasının cezalandırılması ile ilgili düzenlemeler de yeterli değildir. Bu teknolojiye kullanıcıların önceden haberi olmaksızın bağlantı elemanlarının ve diğer çiplerin yerleştirilmesinin cezalandırılmasına ilişkin düzenlemelere ihtiyaç vardır. Unutulma hakkının nesnelerin İnterneti teknolojisindeki karşılığı nesnelerin İnterneti yoluyla elde edilen verilerin silinmesi hakkıdır. Kullanıcıların nesnelerin İnterneti sayesinde toplanan verilerinin silinmesini isteme hakları da olmalıdır. [17]

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. [18]

4. Kanuni Düzenleme Çalışmaları

Nesnelerin İnterneti teknolojisi ile ilgili Avrupa Birliği'nde yapılan çalışmalara bakıldığında, 2008 yılında bakanlıklar düzeyinde toplantılar yapılarak geleceğin İnternet'i ve özellikle nesnelerin İnterneti hakkında görüşmeler yapıldığı görülmektedir. [19] 2009 yılında Avrupa Komisyonu Nesnelerin İnterneti Konusunda Avrupa İçin Hareket Planı isimli bildirimini hazırlamıştır. [20]

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. [21]

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. 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. 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 saklanması zamanla sınırlı olması bununla birlikte isteyen kişilerin verilerin saklanmasına izin vermeme hakkına da sahip olması gerektiği talepler arasındadır. Bunlara ek olarak 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.[22]

Raporda üreticiler nesnelerin İnterneti teknolojisinin ve uygulamalarının bu konuda yapılacak kanuni düzenlemeler ile ilgili hareket tarzının belirlenmesi beklenmeden gelişmesi gerektiğini belirtmiştir. Mevcut veri koruma ve rekabet kurallarının ve güvenlik ve çevre ile ilgili hukuki düzenlemelerin hâlihazırda son kullanıcıyı koruduğunu belirtmişlerdir.

Ayrıca nesnelerin İnterneti konusunda yapılacak uygunsuz yönetişimin bu alanda yapılacak yatırımlara ve yeniliklere engel oluşturacağını belirtmişlerdir. 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 olduğunu belirtmişlerdir. Nesnelerin İnterneti kapsamında son kullanıcıların haklarının tam olarak korunması gerektiğine işaret etmişlerdir. Raporda son kullanıcıların nesnelerin İnterneti pazarının rekabetçi bir şekilde gelişmemesi ve tüketicilerin belirli teknolojiler ve/veya belirli üreticilere mahkûm olması riskinden de 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. [23]

Avrupa Birliği'nde Genel 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 2018 yılında yürürlüğe girecek olan Genel Veri Koruma Tüzüğü'nde düzenlenmiştir. Buna göre veri işleme için kullanılacak sistemlerde veri kontrolörleri (*data controller*) veri öznelinin (*data subject*) haklarının korunması için gerekli tedbirleri almak zorundadır. Bu itibarla veri işleme faaliyetlerinin gerekli amaçlar için minimum düzeyde olmasının öndeğer kabul edilmesi sağlanmalıdır.

Nesnelerin İnterneti konusunda Amerika Birleşik Devletleri'nde mahremiyet ve veri güvenliği ile ilgili düzenlemelerin yapılması gündemdedir. [23] Örneğin, Birleşik Devletler Sağlık ve İnsani Hizmetler Dairesi (*U.S. Department of Health and Human Services*), ilgili kurumlarda sağlık verilerine ilişkin mahremiyet, güvenlik ve ihlal bildirimini 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. [24]

Amerika Birleşik Devletleri'nde Federal Ticaret Komisyonu mahremiyet ile ilgili çerçeve niteliğinde kuralları (*privacy framework*) yayınlamak 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 dikkate alınması (*privacy by design*), tüketicilere kolaylaştırılmış seçim imkânı tanınması (*simplified consumer choice*) ve şeffaflıktır (*transparency*). [25]

Kaliforniya'da 1 Ocak 2014 tarihinde yürürlüğe giren ve Medeni Kanun'un mahremiyet ile ilgili bölümüne akıllı sayaçlardan elde edilen verilerin korunmasına ilişkin düzenleme eklenmiştir. Buna göre işletmelere müşterilere ait akıllı sayaçlar ile İnternet üzerinden iletilen elektrik ve gaz tüketim bilgilerinin açıklanmasına sınırlama getirilmiştir. [26]

5. Türk Hukukunda Nesnelerin İnterneti

Türk hukukunda bazı kanunlardaki hükümler konu ile ilişkilendirilebilir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında 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. Buna göre nesnelerin İnterneti sayesinde toplanan verilerin söz konusu suçları oluşturacak şekilde İnternet'te yayınlanması halinde ilgili İnternet sitesine erişim engellenebilecektir.

Türk Ceza Kanunu'nun 243.maddesinde bilişim sistemine girme ve kalma suçu düzenlenmiştir. [27] 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. Buna göre birbiri ile bağlantılı nesnelerin oluşturduğu sisteme yetkisiz olarak giren, bu nesnelere arasındaki veri akışını engelleyen, bozan, verileri yok eden veya değiştiren, başka bir yere aktaran kişi 244.maddedeki suçu işlemiş olacaktır.

Tüketicinin Korunması Hakkında Kanun'un 5.maddesindeki tüketiciyle müzakere edilmeden sözleşmeye dâhil edilen ve tarafların sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olan haksız sözleşme şartları da nesnelerin İnterneti teknolojisi içeren ürünlerin kullanıcılarını ilgilendirmektedir.

Türk Ticaret Kanunu'ndaki dürüstlük kuralına aykırı işlem şartı kullanılarak hazırlanan genel işlem şartlarını kullanmanın haksız rekabet teşkil edeceğine ilişkin düzenleme de konu ile ilgilidir (m.55). Türkiye Cumhuriyeti Anayasası'nın 20.maddesinde özel hayatın gizliliği ile ilgili düzenleme vardır. 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 hükümler Kişisel Verilerin Korunması Kanunu'nda bulunmaktadır.

Türk Medeni Kanunu'nun kişiliğin saldırılara karşı korunmasına ilişkin (m.24), Türk Ceza Kanunu'nun kişisel verilerin hukuka aykırı olarak kaydedilmesine ilişkin (m.135), verileri hukuka aykırı olarak verme veya ele geçirmeye ilişkin (m.136), verileri yok etmemeye ilişkin (m.138) düzenlemeleri ve Fikir ve Sanat Eserleri Kanunu, Elektronik Haberleşme Kanunu ve İş Kanunu da nesnelerin İnterneti ile ilişkilendirilebilir.

6. Sonuç ve Öneriler

Nesnelerin İnterneti teknolojisi kullanıcılara pek çok kolaylık getirmektedir. Bununla birlikte, bireylerin toplanan verilerinin (tüm bu verilerin toplamından oluşan büyük verinin de) nasıl kullanılacağı konusunda açıklık yoktur. Güvenlik konusunda da tehlikeler söz konusudur. Konu hakkındaki kanuni düzenlemeler henüz yeterli değildir.

Nesnelerin İnterneti teknolojisi içeren ürünleri satın alan tüketicilerin/kullanıcıların bu ürünlerin kullanımı hakkında bilinçlendirilmeleri gerekmektedir. Tüketicilerde mahremiyetin korunması ve veri güvenliği konusunda farkındalık ve duyarlılığın artırılması için çalışmalar yapılmalıdır. Ayrıca nesnelerin İnterneti teknolojisi içeren ürünlerin üretiminde ve ithalatında veri güvenliğinin ve mahremiyetin korunması için standartlar oluşturulmalıdır.

7. Kaynaklar

- [1] PEPPET, S., "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", Texas Law Review, Vol.93:85 vd.
- [2] BLUM, P., "Internet of Things", 101: Legal Concerns-Law 360, <http://www.law360.com/articles/526266/internet-of-things-101-legal-concerns> (Erişim 08.10.2015).
- [3] ASHTON, K., "That Internet of Things Thing", RFID Journal, Yayınlanma 22.06.2009, <http://www.rfidjournal.com/articles/view?4986> (Erişim 16.10.2015).
- [4] WALKER, K., "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).
- [5] WALKER; ADSHEAD, A., "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).
- [6] VICKERY, J., "Legal Tech Series: What is the Internet of Things?",

<https://www.youtube.com/watch?v=5bSa2QGA9Dk>, Yayınlanma 21.06.2015, (Erişim 08.10.2015).

- [7] YETİMLER, E., "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).
- [8] <http://www.technovelgy.com/ct/technology-article.asp> (Erişim 13.10.2015).
- [9] BARBRY, E., "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).
- [10] PEPPET, s.93.
- [11] Ayrıntılı bilgi için bkz. PEPPET, s.94 vd.
- [12] PEPPET, s.95.
- [13] WALKER.
- [14] TAYLOR, D., "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).
- [15] WALKER.
- [16] 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/publicdisplay_documentpdf/?cote=DSTI/ICCP/CISP\(2011\)4/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplay_documentpdf/?cote=DSTI/ICCP/CISP(2011)4/FINAL&docLanguage=En) (Erişim 14.10.2015).
- [17] BARBRY, s.94; Unutulma hakkı ile ilgili geniş bilgi için bkz. BOZKURT YÜKSEL, A.E., "İnternet ve Unutulma Hakkı", İzmir 4.Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir 2016, s.23-43.
- [18] 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.
- [19] BARBRY, s.85.
- [20] 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", Bruxelles 18.06.2009, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF> (Erişim 12.10.2015).
- [21] 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.

[22] EUROPEAN COMMISSION, s.3-4.

[23] EUROPEAN COMMISSION, s.15.

[24] WALKER.

[25]<http://www.onlinetech.com/resources/references/what-is-hipaa-compliance> (Erişim 10.10.2015).

[26] 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/repo>

[rts/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf](#) (Erişim10.10.2015).

[27] 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).
