International Journal of Social Inquiry
Cilt / Volume 14 Sayı / Issue 1 2021 ss./pp. 53-80

NESNELERİN İNTERNETİ, GÜVENLİK VE GİZLİLİK, İNSAN HAKLARI BAĞLAMINDA BİR DEĞERLENDİRME

Bora AKİNCE*

Makale Geliş Tarihi-Received: 07.12.2020
Makale Kabul Tarihi-Accepted: 15.05.2021
DOI: 10.37093/ijsi.950466

ÖZ

İnternetin yaygınlaşması ile birlikte nesnelerin internete bağlanmaya başlaması neticesinde insan hayatına yeni bir kavram girmiştir. Bu kavram nesnelerin interneti kavramıdır. Nesnelerin interneti akıllı telefonların, sensörlerin kullanımının yaygınlaşması ile hayatın ayrılmaz bir parçası olmuş ve insan hayatını kolaylaştırmıştır. Ancak nesnelerin interneti her ne kadar insan hayatını kolaylaştırsa da güvenlik ve gizlilik ile ilgili iki önemli konuda insanların kafasında soru işaretleri bırakmaktadır. Bu çalışmada nesnelerin interneti nedir, nasıl gelişmiştir, nesnelerin internetinde güvenlik ve gizlilik nasıl sağlanmaktadır? sorularına cevap verilecek, nesnelerin interneti teknolojisinin insan hayatında yerinin çok arttığı ve bunu neticesinde güvenlik ve gizlilik sorunlarına yol açtığı sorunsalından yola çıkılarak insan hakları hukuku bağlamında bir değerlendirme yapılacaktır.

Anahtar Kelimeler: Nesnelerin İnterneti, Güvenlik, Gizlilik, İnsan Hakları, Sosyal Medya.

Jel Kodu: F50, F59, K38.

* *Öğretim Görevlisi, Abdullah Gül Üniversitesi, Kayseri/Türkiye. bora.akince@agu.edu.tr, ORCID: https://orcid.org/0000-0003-4252-338X.*

AN EVALUATION IN THE CONTEXT OF THE INTERNET OF THINGS, SECURITY AND PRIVACY, HUMAN RIGHTS

ABSTRACT

As a result of the widespread use of the Internet, people started to connect to the internet and a new concept has been introduced to human life. This concept is the concept of the Internet of Things. The Internet of Things became an integral part of life with the widespread use of smartphones and sensors, making human life easier. However, although the Internet of Things simplifies human life, it leaves question marks in the minds of two important issues related to security and privacy. In this study, what is the internet of things, how has it developed, how is security and privacy ensured in the internet of things? Their questions will be answered, and an evaluation will be made in the context of human rights law, based on the problematic that Internet of Things technology has increased its place in human life and consequently leads to security and privacy problems.

Keywords: Internet of Things, Security, Privacy, Human Rights, Social Media.

Jel Code: F50, F59, K38.

GİRİŞ

Teknolojinin gelişmesi, internetin yaygınlaşması ile birlikte dünya yeni bir çağa girmiştir. Bu çağ iletişim çağı olarak adlandırılmaktadır. Bilgi çağında hız, iletişim, bilgi ve bunların transferi en önemli süreçleri oluşturmaktadır. Teknolojinin gelişmesi ile birlikte insanların hayatı sanal hayata taşınmaya başlamıştır (Kumar, Patel, 2014: 20). İletişim çağında internete erişimin bir insan hakkı olduğu tartışılmaktadır (Akyeşilmen, 2018: 286).

1990'lı yılların sonunda RFID (Radyo Frekanslı Kimlik – Radio Frequancy Identification) teknolojisinin ortaya çıkması neticesinde nesnelerden bilgiler toplanmaya başlanmış ve dünya yeni bir kavram olan nesnelerin interneti kavramı ile tanışmıştır. Bunun yanında geleceğin interneti (Future Internet) kapsamında değerlendirilen en önemli teknolojik gelişme nesnelerin internetidir (Coetzee, Eksteen, 2011: 1).

Nesnelerin interneti kavramı kısaca nesnelerin birbirine bağlanması ile oluşan bir ağ olarak tanımlanabilmektedir (Roman, vd., 2013: 2266). Peki bu ne anlama gelmektedir. Nesnelerin interneti kavramı nesnelerin birbirleri ile haberleşmesi ve birbirlerine komut vermesi anlamına gelmektedir. Bir diğer ifade ile fiziksel nesnelerin küresel bir ağda birbirlerine bağlanması anlamına gelmektedir (Kortuem, vd., 2010: 44).

2000'li yıllardan itibaren RFID teknolojisinin gelişmesi, akıllı telefonların dünyada kullanımının yaygın hale gelmesi, akıllı telefonlara bağlı olarak insan hayatını kolaylaştıran pek çok uygulamanın geliştirilmesi neticesinde nesnelerin interneti kavramı da insan hayatının çok önemli bir parçası haline gelmiş ve insan hayatını son derece kolaylaştırmıştır.

Ancak insan hayatını kolaylaştıran bu teknoloji insanların kafasında çok önemli bir soru işareti oluşturmuştur. Bu soru gizlilik ve güvenlik sorusudur. Nesnelerin internetinin güvenliği ile ilgili olarak çeşitli kaygılar bulunmaktadır. (Hayajneh vd., 2020: 1). Çünkü insanlar nesnelerin interneti teknolojisini kullandıkça veri üretmekte, kendi verilerini, kişisel bilgilerini bu cihazlarda paylaşmaktadır. Buradaki temel soru nesnelerin interneti teknolojisinin gelişmesi ve hayatımıza

girmesi sonucunda bu teknoloji ne kadar güvenlidir sorusu olmuştur. Ayrıca gizlilik bir diğer soru işaretini oluşturmaktadır. Nesnelerin interneti ile ilgili olarak güvenliği ve gizliliği sağlamak için çeşitli teknolojiler, dizayn metodolojileri, koruma ve güvenlik teknolojileri kullanılmaktadır (Sicari vd., 2015: 146). Güvenlik nesnelerin interneti teknolojisindeki en önemli konulardan bir tanesini oluşturmaktadır (Yan vd., 2014: 120).

Bu çalışmada nesnelerin interneti kavramı tanımlanacak, nasıl geliştiği, hangi alanlarda kullanıldığı analiz edildikten sonra, nesnelerin internetinde güvenlik ve gizlilik nasıl sağlanmaktadır sorusuna cevap aranacaktır. Nesnelerin internetinin insan hayatında önemli bir yer tutmaya başlaması neticesinde güvenlik ve gizlilik ihlalleri yaşandığı önermesinden yola çıkılarak insan hakları hukuku çerçevesinde Avrupa İnsan Hakları Sözleşmesi ve İnsan Hakları Evrensel Beyannamesi ışığında bir değerlendirme yapılacaktır.

1. NESNELERİN İNTERNETİ NEDİR?

Nesnelerin interneti tanımı ilk olarak Kevin Ashton tarafından kullanılmıştır. Ashton 1998 yılında nesnelerin internetini geleceğin interneti ve bilgisayarların sürekli olarak bağlanması olarak tanımlamaktaydı. Bu tanım teknolojinin gelişmesi ile birlikte gelecekte erişimin ve bağlantının önemini göstermekteydi (Aazam vd., 414). Kevin Ashton'a göre bilgisayarlar ve internet bilgi için insana bağımlı durumdadırlar. Ashton 2009 yılında internetteki tüm bilgiler insanlar tarafından oluşturduğunu belirtmiştir. Ancak Ashton'a göre ekonomi, toplum ve hayatta kalma fikirlere ve bilgilere değil nesnelere (things) bağlıdır. Özellikle RFID teknolojisi ile birlikte bilgisayarların tanıma, anlama kapasitesi gelişmiş ve böylelikle insanların veri girmesi sonucunda ortaya çıkan kısıtlılığı ortadan kaldırmıştır (Ashton, 2009).

Nesnelerin interneti, bilişim teknolojilerinin gelişmesi ile birlikte bilişim teknolojinde oluşan sanal dünyanın, nesneler ile bütünleşmesi anlamına gelmektedir (Uckelmann vd., 2011: 2). Bu tanım sonrasında nesnelerin interneti ile ilgili bir tanımlama sorunu ortaya çıkmış ve pek çok akademisyen tarafından, pek çok sanayi kuruluşu, pazarlamacı tarafından bu kavram kullanılmaya başlanmıştır. Nesnelerin interneti ile ilgili olarak kapsayıcı bir tanım Avrupa'da geliştirilen bir projede verilmektedir. Bu tanıma göre nesnelerin

interneti gelecekteki internet yapısının bir parçası olacaktır. Nesnelerin interneti birlikte çalışan iletişim protokollerinden oluşan ve dinamik bir küresel ağ alt yapısıdır. Nesnelerin internete bağlanması ile birlikte, nesnelere iletişim internet aracılığı ile mümkün olmakta ve nesnelerin yönetilmesi sağlanmaktadır (Uckelmann vd., 2011: 4).

Nesnelerin interneti teknolojik bir devrim olarak görülmektedir. Nesnelerin interneti ile geleceğin bilgisayar ve iletişim teknolojisidir (Wu vd., 2010: 484). Nesnelerin interneti ile her gün nesneler dijital kimlik almakta ve birbirlerine bağlanmaktadır (Broll vd.; 2009: 74).

Nesnelerin interneti Kevin Ashton'ın kurucusu ve genel müdürü olduğu Auto – ID merkezinin[1] 2003 yılında Chicago'da, tedarik zincirlerinde bulunan malların akışının otomatik bir şekilde tanımlanmasını ve izlenmesini sağlamak amacı ile kullanılması sonucunda dikkat çekmeye başlamıştır. Bu kavram Auto – ID merkezinin kurucuları tarafından kullanıldıktan sonra gerçek dünya ile sanal dünya arasındaki kombinasyonu tanımlamak için kullanılmıştır (Uckelmann vd., 2011: 2).

1.1. Nesnelerin İnterneti Kavramının Bileşenleri

Nesnelerin internetinin ortaya çıkmasındaki en önemli olay RFID teknolojisinin gelişmesidir. RFID teknolojisi esas olarak bir okuyucu ve bu okuyucunun karşısında bulunan nesnede bulunan bir etiketten oluşmaktadır. Etiketin okuyucu tarafından okunması RFID teknolojisi ile sağlanmaktadır. Günümüzde arabalarımızda kullandığımız Hızlı Geçiş Sistemi (HGS) etiketleri, otobüslerde kullanılan kart okuma sistemleri RFID teknolojisi ile çalışmaktadır. RFID teknolojisinin özellikle fabrikalarda tedarik zincirinde kullanılması nesnelerin internetinin de dünyada yayılmasına sebep olmuştur.

Nesnelerin internetinin gelişmesinde özellikle sensörler, RFID, NFC, wireless iletişimi, teknolojilerin de ki fiyatların düşmesi çok önemli bir etken olmuştur. Nesnelerin interneti akıllı nesneleri de içermektedir.

---

[1] Ayrıntılı bilgi için bkz. http://tr.chafontech.com/info/what-is-the-auto-id-centera-1765972.html (Erişim Tarihi: 23.04.2021).

İnsanlık ve çevre için görevler yapan tüm cihazlar nesnelerin interneti tanımı kapsamında değerlendirilmektedir. Bu sebepten dolayı nesnelerin interneti sadece yazılım ve donanımdan değil etkileşim ve sosyal yönü de içeren bir kavramdır (Aazam vd., 2014: 414).

Nesnelerin interneti 2000'li yıllarda RFID teknolojisi üzerinden ilerlerken, veri büyüklüğü milyonlar ile ifade edilmekteydi. Veri toplama bir tanımlayıcı arayıcılığı ile yapılmaktaydı. Ancak teknolojinin gelişmesi ile birlikte 2013 yılında nesnelerin interneti sensörler, telefonlar ve bulut sistemleri ile yapılmaya başlandı. Veri boyutu da yeni teknolojiler ile milyarlar olarak ifade edilmekteydi. Bağlantı aracı olarak wireless kullanılırken, veriler bizzat insanlar tarafından sağlanmaktaydı. Masaüstü uygulamaları, düğmeler, dokunmatik sistemler verileri toplamaya başlamaktaydı. 2020 yılında ise nesnelerin internetinin yeni teknolojiler gelişerek milyararlara hatta trilyonlara ulaşacağı tahmin edilmektedir (Ziegeldrof vd., 2014: 2731).

Nesnelerin internetinin gelişmesinde üç önemli adım bulunmaktadır. Bunlar gömülü zekâ (embedded intelligence), bağlantı ve etkileşimdir. Gömülü zeka hareketleri otomatik bir şekilde yapılmasıdır. Bu özellik örneğin çamaşır makinesi kontrol ünitesinde bulunmakta ve makinenin otomatik bir şekilde yıkamayı tamamlamasını sağlamaktadır. Gömülü zekanın geliştirilmesinden sonra ki adım ise bu cihazların bağlantısının yapılmasıdır. Cihazlar bağlantı ile birlikte akıllı cihazlar haline gelmektedir. Bu cihazların wireless yolu ile bağlanması nesnelerin internetinin en önemli özelliklerinden bir tanesidir. Ancak son adım da cihazların bağlı olması cihazların iletişim ve etkileşim sağladığı anlamına gelmemektedir. Cihazların bağlanması ile birlikte cihazların kendi arasında bilgi değişimi yapmasına bağlıdır. Böylelikle insandan insana olan iletişim; insandan nesneye, nesneden nesneye olarak değişmektedir (Tan, Wang, 2010: 377). Örneğin evlerde bulunan akıllı kombiler cep telefonlarında bulunan bir uygulama ile açılıp kapanabilmektedir. Böylelikle insan nesneye (akıllı telefon uygulaması) bir talimat vermekte, nesne (akıllı telefon uygulaması) ise bir diğer nesneye (kombi) talimat vermektedir.

Peki akıllı nesneler nasıl tanımlanabilecektir? Akıllı nesneler tanımlanırken aşağıdaki özellikleri kullanılabilir.

- Belirli bir fiziksel düzenlemeye ve bir dizi fiziksel özelliklere sahiptirler (biçim, boy vb.).
- Minimum düzeyde iletişim yeteneği bulunmalı ve aldığı mesajları cevaplama yeteneğine sahiptirler.
- Benzersiz bir tanımlayıcıya sahiptirler.
- Nesneler en az bir isim ve bir adres ile ilişkilendirilmektedir. İsim nesnenin okunabilir açıklaması anlamındadır. Adres ise nesne ile iletişim kurmak için kullanılmaktadır.
- Nesneler temel bir seviyede bilgi işlem yeteneğine sahiptirler. Bu seviye basitten başlayarak karmaşık hesaplamalara kadar gelişebilmektedir (Miorandi, Sicari, Pellegrini, Chlamtac, 2012: 1500).

1.2. Nesnelerin İnterneti ve Teknoloji

Akıllı nesneler tanımlandıktan sonra nesneleri sekiz başlık altında kategorileştirmek mümkündür;

1. Akıllı nesneler birbirleri arasında veri değişimi sağlamaktadır.
2. Sensörler fiziksel dünyanın dijital dünyadaki temsilcisidir.
3. Aktuatör fiziksel dünyada gerçekleşen eylemleri dijital dünyaya taşırlar.
4. Tanımlama ve kayıt için sensörler tarafından veriler toplanır.
5. Nesneler fiziksel dünyadaki insanlar ile iletişime girmektedir.
6. Veri madenciliği ve hizmetleri süreçleri nesneler tarafından yürütülmektedir.
7. Fiziksel dünyadaki yerler nesneler tarafından kayıt altına alınmaktadır.
8. Her nesnenin özel bir tanımlaması bulunmaktadır. (Mayer, 2009: 2).

Nesnelerin interneti dünyanın önem verdiği, gelişen teknolojilerden bir tanesidir. Avrupa'da nesnelerin interneti ile ilgili sayısız proje yapılmaktadır. Avrupa teknoloji Platformu (EPoSS) tarafından 2008 yılında yapılan bir çalışmada yönetim, standardizasyon ve birlikte

çalışabilirlik noktasında nesnelerin internetinin çok önemli olacağı vurgulanmaktadır (EPoss, 2008).

Nesnelerin internetinin temel hedefi interneti daha yaygın hale getirerek, bağımsız bir network oluşturulmasının sağlanmasıdır. Bunun yanında nesnelerin interneti ile birlikte ev uygulamaları, kameralar, sensörler, araçlar internete bağlanacak ve bu nesneler toplumsal hayatta fazlaca kullanılacaktır (Zanella, Vangelista, 2014: 22). 2015 yılında birbirine bağlı nesne sayısı 15 milyar iken 2020'de bu sayının 26 milyar olması beklenmektedir (Arias vd., 2015: 99).

Nesnelerin interneti teknolojisinin kullanım alanı da teknolojinin gelişmesi ile birlikte git gide artmıştır. Çok farklı dallarından nesnelerin interneti teknolojilerine talep gelmektedir (Xu vd., 2014: 2233). Nesnelerin interneti özellikle arabalarda lastik basınçlarını kontrol edip bir monitöre bildirmesi anlamında hali hazırda kullanılmaktadır. RFID teknolojisi otomotiv sektöründe fazlaca kullanmaktadır. Özellikle arabanın üretim, lojistik, kalite kontrol bölümlerinde kullanılmaktadır (Sundmaker vd., 2010: 50). Bunun yanında nesnelerin interneti telekomünikasyon teknolojilerinde de kullanılmaktadır. Özellikle NFC (Near Field Communication veya Türkçe ifadesi ile Yakın Alan İletişimi) ile kart yükleme yapılması, GPS sistemi nesnelerin internetinin telekomünikasyon alanındaki örneklerinden bir tanesidir. Akıllı binalarda nesnelerin interneti teknolojisinin kullanıldığı önemli alanlardan bir tanesidir. Özellikle ev teknolojilerinde akıllı klimalar, akıllı kombi sistemleri kullanılmaktadır.

Nesnelerin internetinin en çok kullanıldığı bir diğer alan ise sağlık alanıdır. Özellikle sağlık sektöründe telefonun ve RFID sensörlerinin kullanımı neticesinde kişilerin sağlık ile ilgili verileri ve ilaç alım sıklıkları gibi hastaların bilgileri doktorların ekranın görünmekte ve bu süreç tedavi süreçlerini kısaltmaktadır. Bunun yanında kan tahlili yapılırken dahi barkodların kullanılması bir tür RFID uygulamasıdır. Bunun yanında ilaç endüstrisinde de nesnelerin interneti kullanılmaktadır. Özellikle akıllı barkodlar ile ilaçların saklama koşulları, nereye nasıl nakledilmeleri gerektiği ile ilgili bilgiler ilaç üreticilerine büyük kolaylıklar sunmaktadır.

Nesnelerin internetinin kullanıldığı bir diğer alan ise tedarik zinciri yönetimi ve lojistiktir. RFID teknolojisi tedarik zinciri ve lojistik

sürecini oldukça kolaylaştırmaktadır. Özellikle envanter yönetimi anlamında büyük kolaylıklar sağlamaktadır.

Nesnelerin interneti teknolojileri, doğanın korunması, ulaşım sistemleri, gıda izlenebilirliği, tarım ve hayvancılık, bilet satma işlemleri, geri dönüşüm alanlarında da sıkça kullanılmaktadır.

2. NESNELERİN İNTERNETİ: GÜVENLİK, GİZLİLİK VE İNSAN HAKLARI

İnternetin gelişmesi, ucuzlaması, yaygınlaşması neticesinde internete bağlanan nesnelerin sayısı her geçen gün artmaktadır. Bu nesnelerin sayısının artması ile birlikte doğal olarak doğru orantılı bir şekilde bu nesnelerin kullanımı da artmaktadır. Kullanıldığı alanlar düşünüldüğünde nesnelerin interneti insan hayatının her yerindedir. Nesnelerin internete bağlanması ile birlikte geleneksel internet kabuk değiştirmiştir. Bunun yanında her nesne potansiyel bir şekilde internete bağlanabilir bir hale gelmiştir. Aynı zamanda bu nesneler birbirleri ile de iletişim kurmaya başlamıştır (Suo vd., 2012: 648).

İnternet sanal bir ortamdır. Ancak bu sanal ortamda yapılan tüm işlemlerin fiziksel sonuçları bulunmaktadır (Ünal, Ergen, 2018: 192). Bu sebepten dolayı nesnelerin interneti konusundaki en önemli iki nokta güvenlik ve gizliliktir. Nesnelerin internetini kullananların da en önemli kaygılarından bir tanesi güvenlik ve gizlilik olarak karşımıza çıkmaktadır (Atzori vd., 2010: 2802). Nesnelerin internetinin kullanımının yaygınlaşması için gizlilik ve güvenlik sorunlarının çözülmesi gerekmektedir (Goyal vd.; 2020: 4). Güvenlik internete bağlanan cihazlara yetkisiz girişlerin önlenmesidir. Gizlilik ise internete bağlanan cihazlarda bulunan bilginin yetkisiz erişiminin engellenmesidir (Ünal, Ergen, 2018: 193).

Ağa bağlanan nesnelerin sayısı arttıkça, bu nesnelerin insan hayatında kullanım oranı arttıkça ve nesnelerin insanların hayatını kolaylaştırması sonucunda hackerlar (internet korsanları) tarafından nesneler potansiyel saldırı araçları haline gelmektedir. Güvenlik nesnelerin interneti uygulamalarındaki en önemli hususlardan bir tanesidir. Güvenlik garanti edilmeden nesnelerin internetinin yaygınlaşması çok mümkün olmayacaktır (Miorandi vd., 2012: 1513).

Nesnelerin internetinde güvenlik ile ilgili kaygılar aslında internetteki kaygılar ile aynıdır. Bunun temelinde ise artan saldırıları yatmaktadır. Artan saldırılar siber saldırılar tanımını gündeme getirmiştir. Siber saldırılar gizliliğin ele geçirilmesi için düzenlenmektedir (Saygılı, Ünal, 2018: 246).

Nesnelerin internetinde nesnelerin kapasitelerinin küçük olması, sistemin wireless bağlantısı içermesi gibi sorunlardan dolayı güvenlik problemleri meydana gelmektedir (Stankovic, 2014: 6). Wirelesslar nesnelerin internetinde hackerlerin ve diğer üçüncü tarafların en çok saldırı yaptığı yerdir (Weber, 2015: 621). Yapılan hacklemelerden sonra Anthem, Apple, JP Morgan, Sony gibi şirketlerden özellikle kredi kartı bilgileri, kurumsal strateji gibi önemli bilgiler çalınmış ve bu kurumlara önemli ölçüde maliyet yansıması olmuştur (Weinberg vd., 2015: 6).

Nesnelerin internetine saldırıların kolay olmasının nedenleri ise aşağıda belirtilmektedir.

Öncelikle nesnelerin internetinde bileşenler genellikle zayıftır ve bunlara saldırmak kolaydır. İkincisi kablosuz yani kablosuz ağlar üzerinden iletişim kurulmaktadır ve kablosuz ağları gizli bir şekilde dinlemek oldukça kolaydır. Bunun yanında son husus ise nesnelerin internetinde hem enerji hem de hesaplama kaynakları oldukça düşük olduğundan güvenliği destekleyen karmaşık şemalar bulunmamaktadır (Atzori vd., 2010: 2802). Özellikle nesnelerin internetinde sensörlerin gelişmesi neticesinde sensörler üzerinden çeşitli siber saldırılarda yapılabilmektedir. Buna karşın nesnelerin interneti teknolojisi ile çalışan firmalar çeşitli güvenlik algoritmaları geliştirse de bu algoritmaların ne derece güvenliği sağladığı bir tartışma konusu olarak karşımıza çıkmaktadır.

Nesnelerin internetinin güvenliği ile ilgili ilk nokta veri güvenliğidir (data confidentiality). Veri güvenliği sadece izin verilen yetkililerin verilere erişebilmesi ve verileri düzeltebilmesi anlamına gelmektedir. Nesnelerin internetinde sadece kullanıcılar değil; aynı zamanda yetkilendirilmiş nesnelerde veriye erişebilmektedir. Bu da iki önemli noktayı ön plana çıkarmaktadır. Bunlardan birincisi kontrol mekanizması ile erişicilerin tanımlanması; ikincisi ise nesnenin kimliğinin doğrulanmasıdır (Miorandi vd., 2012: 1514). Bu tanımlama ve doğrulama işlemleri ile birlikte nesnelerin internetinde veri

güvenliği sağlanabilmektedir. Ancak nesnelerin internetinde kimlik doğrulaması ile ilgili sorunlar özellikle RFID etiketlerinin kimlik doğrulama sunucular ile çok fazla mesaj alışverişi yapamaması sebebi ile mümkün olmamaktadır. Ancak son dönemlerde bu konuda çözümler üretilmeye çalışılmaktadır (Atzori vd., 2010: 2802).

Nesnelerin internetin de bir diğer unsur ise gizliliktir. Gizlilik konusu internetin gelişmesi ile birlikte özellikle de nesnelerin interneti teknolojisi ile ilgili olarak gündemde olan en önemli konulardan bir tanesidir (Ziegeldrof vd., 2014: 2728). Gizlilik hangi veriye hangi bireysel kullanıcının ulaşacağının tanımlanması anlamına gelmektedir (Moirandi vd., 2012: 1519). Bunun yanında gizlilik kişisel bilgiler barındıran verilerin nerede nasıl saklanacağını da barındırmaktadır (Weber, 2010: 24).

2.1. Nesnelerin İnterneti: Gizlilik

Peki gizlilik neden önemlidir? Öncelikle belirtmek gerekir ki gizlilik kavramı dünya medeniyetinin en önemli unsurlarından bir tanesi haline gelmiştir. Ayrıca gizlilik ile ilgili endişeler nesnelerin interneti teknolojisinin yayılmasındaki en önemli handikaplardan bir tanesidir (Atzori vd. 2010: 2803). Bu sorunun cevabı nesnelerin internetinin kullanım alanında gizlidir. Nesnelerin interneti kişilerin sağlık bilgilerinden tutunda, kişisel bilgilerinin tutulduğu bir alandır. Bu sebepten dolayı gizlilik nesnelerin internetinde en önemli hususlardan bir tanesidir.

Veriler, veriler ile ilgili süreçlerin tamamı nesnelerin internetinin en önemli özelliklerindendir. Veri olmadan nesnelerin internetinden de söz etmek mümkün değildir. Dünyada üretilen ve saklanan verinin boyutu 4 zetabayttır. 2020'de bu verinin 40 zetabayt olması beklenmektedir. Bilgisayar teknolojilerinin en hızlı gelişen alanı nesnelerin interneti teknolojisi olmuştur (Garadi vd., 2020: 1646). Bu Teknoloji geliştikçe bu veriler artacak ve bu verilerin depolanması gerekecektir. Verilerin depolanması gün geçtikçe daha da uygun bir maliyet ile yapılabilmektedir. Bu verilerin kimin kullanacağı ise gizliliğin ayrı bir boyutunu oluşturmaktadır (Weinberg vd., 2015: 6).

Gizlilik ile ilgili olarak bu verilerin kim tarafından, ne zaman, nasıl toplandığı konusu en büyük kaygıyı oluşturmaktadır (Atzori, 2010:

2803). Ancak nesnelerin internetinde gizliliğin en önemli boyutunu ise verilerin kimler tarafından toplandığı oluşturmaktadır. Veriler ulusal güvenlik gerekçesi ile kamu kurumları tarafından talep edilmekte veya toplanmaya çalışmaktadır. Ayrıca çeşitli firmalar ürünlerini pazarlamak için bu verilere elde etmeye çalışmaktadır. Kişilerin tüm bilgilerinin (lokasyon vb.) nesneler tarafından toplanması da gizlilik ihlaline zemin hazırlamaktadır. Çünkü bu bilgiler gerek devletler, gerek kamu kurumları gerekse özel şirketler tarafından toplanmak ve kullanılmak istenmektedir.

2.2. Nesnelerin İnterneti: Güvenlik

Nesnelerin internetinde gizliliğin sağlanması için öncelikle sistemin saldırılara dayanıklı olması gerekmektedir. Ayrıca sistemin adres ve nesne verilerinin doğrulanması, bilgi sağlayıcıların erişim kontrolü sağlaması, müşteri gizliliğinin sağlanması gerekmektedir (Weber, 2015: 621).

Güven ise nesnelerin internetindeki güvenliği sağlamak için karşımıza çıkan bir diğer önemli noktadır. Nesnelerin internetinde güvenlik kimliklerin bilgiyi paylaşmadan değiştirilmesinin sağlanmasıdır. Bunun için çeşitli uygulamalar kullanılmaktadır (Moirandi vd., 2012: 1520).

Nesnelerin internetinde güvenlik aşağıdaki Şekil – 1'de gösterilmektedir (Miorandi vd., 2012: 1519).

Şekil 1: Nesnelerin İnternetinde Güvenlik.

Güvenlik ve gizlilik ile ilgili yapılan çalışmalardan sonra bazı gereklilikler tanımlanmıştır. Bunlar sistemin saldırılara karşı esnek olması, kimlik doğrulma, erişim kontrolü ve müşteri gizliliğidir. Sistemler saldırılara karşı esnek olmalı ve hatalardan kaçınmalıdır. Kimlik doğrulama alınan adres ve nesne bilgilerinin doğrulanması anlamına gelmektedir. Erişim kontrolü ise bilgi sağlayıcıların veriler üzerinde erişim kontrolü uygulaması anlamına gelmektedir. Müşteri gizliliği ise bilgi sağlayıcılarının spesifik bir müşteri ile ilgili olarak bilgi toplamasını ve çıkarım yapmasının zor olması anlamına gelmektedir (Weber, 2010: 24).

Peki bu özellikler nasıl sağlanmaktadır? Nesnelerin interneti teknolojisinde geleneksel koruma mekanizmaları (kriptolama, güvenli protokoller gibi) güvenliğin sağlanması için yeterli görülmemektedir (Roman vd., 2011: 51). Güvenliği sağlamak için VPN (Virtual Private Networks – Sanal Özel Ağlar), TLS (Transport Layer Security – Aktarım Katmanı Güvenliği), DNSSEC (DNS Güvenlik Uzantıları), Soğan Yönlendirme (Onion Routing) ve PIR (Private Information Retrivial – Özel Bilgi Alma) sistemleri kullanılmaktadır. VPN'lere erişim kısıntından dolayı bilgiler gizli kalmaktadır. TLS ise nesnelerin internetinin güvenliğini küresel bir güven yapısına dayanması neticesinde iyileştirebilme kapasitesine sahiptir. DNSSEC bilgilerin gönderilmesi sürecinde bilgilerin kaynağını, orijinalliğini ve bütünlüğünü sağlamak için açık anahtarlı şifreleme metodunu kullanmaktadır. Soğan yönlendirme ise internet trafiğini farklı kaynaklardan şifrelemekte ve karıştırmaktadır. PIR ise hangi müşterinin hangi bilgi ile ilgilendiğini gizlemektedir. Tüm bu teknolojilerdeki temel sorun performans sorunlarını meydana getirmesidir. Şu anda nesnelerin internetinde kullanılan en önemli sistem P2P (Peer to Peer – Eşler Arası) sistemidir ve uygulamalarda iyi bir performans gösterilerek tercih edilmektedir (Weber, 2010: 25).

P2P bluetooth teknolojisinin yerini daha büyük sistemlere bırakması ile ortaya çıkmış bir teknolojidir. P2P teknolojisi ile birçok bilgisayar birleştirilmekte ve veri paylaşımı yapılmaktadır. Bu teknoloji ile bir veri bireylere tek tek değil bir kerede milyonlarca kişiye göndermemizi sağlamaktadır. Nesnelerin internete bağlanması ile birlikte P2P iletişim hızlanmış ve güçlenmiştir (Sundmaeker vd., 2010: 51).

Nesnelerin interneti teknolojisinde güvenliği sağlayan bir diğer nokta ise kriptolama teknolojisidir (Arias, 2015: 99). Kriptolama teknolojisi büyük kaynak tüketimine ve enerjiye ihtiyaç duyduğu için nesnelerin internetinde kullanımı yeterli seviyede değildir (Atzori vd., 2010: 2803). Kriptolama teknolojisi her ne kadar nesnelerin interneti kapsamında tek başına yeterli görülmese de veri yönetimi alanında teknik olarak verileri korusa da bazı kuruluşlar bu verileri yönetecek kaynaklara sahip olmamaktadır. Nesnelerin internetine yönelik daha iyi kriptolama teknolojileri ve yöntemleri geliştirmek için çalışmalar devam etmektedir (Roman vd., 2011: 54). Kriptolama teknolojisinde de rastgele karma zincir protokolü (Randomize Hash-Lock Protokolü), karma zincir tabanlı protokoller (Hash Chain Based Protocols) kullanılmaktadır (Mayer, 2009: 8).

RFID teknolojilerinin kullanılması sırasında fiziksel olarak öldürücü kodlar (kill codes), faraday kafesi[2] (faraday cage) ve engelleyici etiketi (blocker tag) teknolojileri kullanılmaktadır. Öldürücü kod etiketi kalıcı olarak devre dışı bırakmakta ve bu şekilde izleme ve okumayı önlemektedir. Bu durum ürün müşteriler tarafından satın alındıktan sonra güvenliği ve gizliliği sağlamada oldukça kullanışlıdır. RFID etiketi faraday kafesine konulduğu zaman etiketi okumak imkansız hale gelmektedir. Böylelikle kullanıcılar ürünün ne zaman okunup okunmayacağına karar vermektedir. Engelleyici etiketi ise yetkisiz okuyucuların çok fazla RFID etiketi görmesini sağlayarak başka kişiler tarafından etiketin okunmasını önlemektedir (Mayer, 2009: 8).

Güvenlik ve gizliliğin yanında gerekli bir diğer husus ise şeffaflıktır. Bireyler hangi şirketlerin hangi verilerini nasıl kullandığını bilme hakkına sahiptirler (Roman vd., 2011: 54). Nesnelerin internetinde oluşturulan standartlar ile ilgili bilgiler tablo 1'de gösterilmektedir (Roman vd., 2011: 56).

---

[2] Faraday kafesi, iletkenler ile örülen ve iç kısımdaki elektriğin dış kısma iletilmediği bir yapıdır.

Tablo 1: Nesnelerin İnternetinde Oluşturulan Standartlar

Standart	**Amaç**	**Güvenlik**
ISO/IEC 14443	Temassız yaklaşım kartlarının mimarisi	Bilgi akışı koruması
IEC 62591	Endüstriyel kablosuz sensör ağları için protokol	Şifreleme, kimlik doğrulama, anahtar yönetimi
GS1 Keys	Tanımlama sistemi	Benzersiz tanımlayıcı tanımlama
ucode	Donanım agnostik tanımlayıcısı	Benzersiz tanımlayıcı tanımlama

2.3. Nesnelerin İnterneti: İnsan Hakları

Nesnelerin internetinde gizliliğe sahip olmak temel bir insan hakkı olarak tanımlanmaktadır. Bireyler nesnelerin internetini kullanırken verilerini siber uzayda bırakabilmektedirler. (Weber, 2010: 24). Nesnelerin internete her ne kadar insanlığa faydalı olsa da gizliliğin ihlali ile ilgili olarak sorunlar içerebilmektedir. Bu problemin çözülmesi için her nesnelerin interneti yazılımının kendine has bir gizlilik politikası bulunmalıdır (Stankovic, 2014: 6).

Dünyadaki teknolojikleşme seviyesi ve hızı arttıkça, insanlar internet aracılığı ile hem dünyaya hem de birbirine bağlı hale geldikçe gizlilik konusu daha da dikkat çeken ve kurumlar tarafından da dikkat edilen bir konu haline gelmiştir. Özellikle şirketlerin kalite yönetimi konularında bu noktaya dikkat edilmektedir. Nesnelerin internetinde gizliliğin sağlanması için mutlaka gizlilik politikalarının oluşturulması gerekmektedir. Nesnelerin internetinin kullanımı arttıkça veriler, kişisel veriler, veri transferi ve bunların insanlar üzerindeki etkisinin önemi de artmaktadır (Weinberg vd., 2015: 7). Ayrıca gizliliğin sağlanması noktasında bir diğer husus ise ülkelerin ve kurumların gizlilik ile ilgili tanımlarını kontrol etmelerinden geçmektedir. Pek çok kurum gizlilik tanımlarını nesnelerin interneti kavramına göre tanımlamamaktadır.

Gizlilik sağlanırken dikkat edilmesi gereken üç nokta bulunmaktadır. Bunlar üçüncü tarafların verilere erişimi, verilerin veri toplayıcı

tarafından kullanılması ve dağıtılması ve son olarak verilerin diğer veriler ile birleştirilmesidir (Weber, 2015: 624).

Gizlilik en temel insan haklarından bir tanesi olarak kabul edilmektedir. Dünyada bilgi gizliliği ile ilgili ilk yasa 1974 yılında Amerika Birleşik Devletleri (ABD)'nde Amerikan Gizlilik Aktı (US Privacy Act) ismi ile çıkartılmıştır. Teknolojinin gelişmesi ile birlikte bilgi gizliliği kavramı ortaya çıkmıştır. 1968 yılında bilgi gizliliği benim kişisel bilgilerimin ne kadarının başkaları tarafından bilinmesini seçme hakkı olarak tanımlanmıştır. (Ziegeldorf, 2014: 2729 – 2730).

Gizlilik konusu en temel insan haklarından bir tanesi olarak kabul edildiği ile ilgili bu husus hem İnsan Hakları Evrensel Bildirgesinde hem de Avrupa İnsan Hakları Sözleşmesi'nde vurgulanmaktadır.

İnsan Hakları Evrensel Bildirgesi'nin 12. Maddesi özel hayatın gizliliğini düzenlemektedir. Bu maddeye göre kimsenin özel yaşamına, ailesine ve konutuna karışılamayacağı belirtilmekte ve herkesin bu karşımalara karşı yasalar tarafından korunmaya hakkı olduğu belirtilmektedir.[3]

Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi ise "Özel ve Aile Hayatına Saygı Hakkı'nı" düzenlemektedir. Bu maddede herkesin özel ve aile hayatına, konutuna saygı gösterilmesi konusu vurgulanmaktadır.[4]

Nesnelerin interneti teknolojisinin özellikle akıllı cihazların kullanılması neticesinde çok yaygınlaşması, her eve girmesi, özellikle kullanılan mobil uygulamalardaki veriler ile ilgili olarak insan hakları bağlamında özel hayatın gizliliği kavramını gündeme getirmektedir.

---

3 İnsan Hakları Evrensel Bildirgesi, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf (Erişim Tarihi: 15.11.2020).

4 Avrupa İnsan Hakları Sözleşmesi, https://www.echr.coe.int/documents/convention_tur.pdf (Erişim Tarihi: 15.11.2020).

Nesnelerin interneti teknolojisinin yaygınlaşması sonucunda izinsiz dinlemeler, takipler kişisel verilerin takip edilmesi gibi olaylar ile sık sık karşılaşılmaktadır. Özellikle bazı istihbarat kuruluşlarının telefonlardan veri topladığı, bu verileri paylaştığı, konumları takip ettiği iddia edilmektedir. Örneğin ABD'de istihbarat birimleri akıllı telefonlardaki konum verilerini takip ettiği ile iddialar Amerikan basınında yer almıştır (Oktay, 2021). Bunun yanında Wikileaks belgelerinde de ABD istihbaratının akıllı televizyonlar ve video oyun konsolları ile dinlediği iddiaları yer almıştır.[5]

Dünyada nesnelerin internetinin gelişmesi ile birlikte en çok kullanılan iki hizmet olan Facebook ve Google bu verilerimizi nasıl kullanmaktadır? Bununla ilgili olarak Google ve Facebook gizlilik politikaları bulunmaktadır.

Bilindiği üzere facebook, instagram ve whatsapp uygulamalarının da sahibidir. Facebook gizliliğin sağlanması için hangi bilgilerimizin kimler tarafından görüleceğini ayarlamaya izin vermektedir. Bunun yanında Facebook en çok iletişim kurduğumuz kişileri, Facebook'ta bulunan hangi sayfalara üye olduğumuz ile ilgili bilgileri toplanmaktadır. Ayrıca izin verilmesi durumunda Facebook telefon rehberindeki kişilerimize erişmektedir. Facebook tarafından kullanıcıların, facebooku kullanırken sağladıkları içerikler toplanmaktadır. Bunun yanında fotoğrafların çekildiği konum bilgisi gibi bilgilerde toplanmaktadır. Bunun yanında kullanım sırasında kullanıcı tarafından etkileşim kurulan içerikler, etkileşime geçilen kişiler veya hesaplar ile ilgili hareketler ile ilgili bilgiler de Facebook tarafından toplanmaktadır. Facebook görüntülenen ve etkileşim kurulan içerikler ile ilgili bilgileri de toplamaktadır. Bunun yanında Facebook'ta izlenen tüm videolar, hangi içeriklerin görüntülendiği konularında bilgiler toplanmaktadır. 3. Kişiler tarafından paylaşılan kendimiz hakkındaki bilgiler de kullanılmaktadır. Facebook kullandığımız cihazın özellikleri, cihazda yapılan işlemler, cihazın sinyalleri ve hangi baz istasyonundan bağlandığı, izin verilmesi durumunda ise konum, kamera ve fotoğraflara erişim sağlanmaktadır.

---

5 *WikiLeaks: CIA, akıllı telefonlar ve televizyonlar üzerinden ortam dinleme yapıyor*, (08 Mart 2017), BBC Türkçe https://www.bbc.com/turkce/haberler-dunya-39197514 (Erişim Tarihi: 25.04.2021).

Facebook topladığı veriler ile telefon numaramızdan, kiminle iletişim kurduğumuza, hangi videoları, gönderileri takip ettiğimize, hangi bilgisayarı kullandığımıza, konumumuza kadar her alanda bilgi toplamaktadır. Peki bu veriler nasıl kullanılmaktadır? Bu veriler Facebook tarafından arkadaş önerisi, guruplara katılım önerisi sunması sağlanmaktadır. Facebook tarafından toplanan konum bilgileri, kişisel ilgi alanları özellikle ürün sunmak için kullanılmaktadır. Ayrıca facebook tarafından toplanan bu bilgiler kullanıcılara reklam göstermek şeklinde de kullanılabilmektedir.

Facebook'un belirttiği bir diğer konu ise çalıştığı üçüncü taraflar ile verilerin paylaşılmasıdır. Facebook 3. taraf geliştiricilerin kullanıcıların son 3 ayda kullanılmayan ürünlerin verilere ulaşmasını engellemektedir.

Facebook bu bilgileri yasaların bilgileri vermesine iyi niyet çerçevesinde inanması durumunda kişisel verileri vereceğini belirtmektedir. Ayrıca yasal bir talebin yerine getirilmesi için bilgiler paylaşılabilmektedir.[6]

Dünyanın en çok kullanılan sohbet uygulamalarından bir tanesi olan whatsapp ise kişilerin telefon rehberlerinde bulunan bilgileri toplamaktadır. Mesajlar uçtan uca şifreleme teknolojisi korunmasına rağmen teslim edilemeyen mesajlar 30 gün süre ile whatsapp sunucularında kalmaktadır. Bu mesajlar 30 gün sonra sunuculardan silinmektedir. Whatsapp tarafından kullanım ve kayıt bilgileri, whatsappın kullanıldığı cihaz ile ilgili olarak ip adresi, telefon numarası, işletim sistemi bilgileri, whatsappta paylaşılan durum bilgileri otomatik olarak toplanmakta, izin verilmesi durumunda konum bilgileri toplanmaktadır. Whatsapp toplanan bilgileri iyi niyet çerçevesine inanması durumunda bilgileri toplayabileceğini, saklayabileceğini ve paylaşabileceğini belirtmektedir. Bu bilgiler devlet taleplerine ve yasal işlemlere cevap verilmesi, dolandırıcılık ve diğer yasa dışı faaliyetlerin önlenmesi ve kullanıcıların, whatsapp ve

---

[6] Facebook Veri İlkesi, https://www.facebook.com/privacy/explanation (Erişim Tarihi: 25.04.2021).

facebookun haklarının korunması için toplanabilmekte, saklanabilmekte ve paylaşılabilmektedir.[7]

Verileri toplayan bir diğer uygulama ise dünyanın en çok kullanılan arama motoru Google'dur. Google hangi dili kullandığımızı, hangi youtube videolarını izlediğimizi toplamaktadır. Google tarafından hizmetler kullanılırken hangi cihazlardan erişim sağladığımız, hangi uygulamalara eriştiğimiz ile ilgili bilgiler toplanmaktadır. Google Play Store'un kullanıldığı durumlarda android cihazlar Google'a düzenli bilgi vermektedir. Bunun yanında Google üzerinden aranılan terimler, izlenilen videolar, içerik ve reklam görüntülenmeleri, iletişim kurulan kişiler ile ilgili bilgiler de toplanmaktadır. Google izin verilmesi durumunda konum bilgilerini de kullanmaktadır. Google bu verileri hizmet kalitesini arttırmak için kullanmaktadır. Google bu verileri izin vermemiz durumunda, alan adı ile yöneticileriyle ilgili durumlarda, yasal nedenlerle paylaşabilmektedir.[8]

Son olarak tartışılabilecek bir diğer konu ise bu şirketlerin verileri devlet ve kamu politikalarına karşı nasıl koruduğu ve hangi şartlarda bunun sağlandığıdır. Google ve Facebook gerektiği durumlarda, iyi niyet çerçevesinde ve mahkeme kararları doğrultusunda bu verileri paylaşacağını belirtmektedir. Bu konular ile ilgili olarak internet koalisyonu isimli bir kurum bulunmaktadır. İnternet koalisyonu siber ile ilgili olarak devlet politikası tartışmalarında internet ve e-ticaret şirketlerini temsil etmektedir. İnternet ekonomisini korumayı amaçlamaktadır. İnternet koalisyonun öncelik verdiği konulardan en önemlileri gizlilik, veri güvenliği standartları, web sitelerinin gizlilik politikalarıdır. Amazon, Expedia, Facebook, Google, Yahoo gibi şirketler bu koalisyonun üyeleri arasında yer almaktadır.[9]

---

7 Whatsapp Gizlilik Politikası, https://www.whatsapp.com/legal/privacy-policy (Erişim Tarihi: 25.04.2021).

8 Google Gizlilik İlkesi, https://policies.google.com/privacy?hl=tr#infocollect (Erişim Tarihi: 25.04.2021).

9 http://www.theinternetcoalition.com/about (Erişim Tarihi: 25.01.2019)

SONUÇ

Nesnelerin interneti teknolojisi internetin ucuzlaması, veri depolamanın maliyetinin düşmesi, internetin yaygınlaşması, akıllı telefonlar üzerinden uygulamaların kullanıcı sayısının her geçen gün artması neticesinde insan hayatının vazgeçilmezlerinden bir tanesi haline gelmiştir. Bunun yanında nesnelerin interneti insan hayatını ciddi ölçüde kolaylaştırmaktadır.

Nesnelerin internetinde gizlilik en önemli hususlardan bir tanesi olarak karşımıza çıkmaktadır. Kişinin pek çok bilgisinin internete bağlı nesnelerin içerisinde tutulması bu bilgilerin istenmeyen kişilerin eline geçmesi riskini doğurmaktadır. Bunun yanında bu kişisel bilgilere kimlerin eriştiği en önemli sorunlardan bir tanesidir.

Nesnelerin internetinde gizliliği sağlayabilecek en önemli unsur ise güvenliktir. Veri güvenliği, gizlilik ve güven kavramları güvenlik nesnelerin internetinde karşımıza çıkan en önemli unsurlardır. Güvenlik ile ilgili çalışmalar her geçen gün devam etmektedir. Ancak buna karşın güvenlik ihlalleri ile ilgili olarak pek çok sorunlar karşılaşılmaktadır. Bu gizliliği sağlayabilecek olan yegane unsur hiç şüphesiz güvenliğin sağlanması olacaktır.

Nesnelerin internetinde oluşan güvenlik açıklarından dolayı gizlilik ihlalleri bir insan hakları problemi olarak karşımıza çıkmaktadır. Gizlilik en temel insan haklarından bir tanesidir. İnsan Hakları Evrensel Bildirgesi'nde ve Avrupa İnsan Hakları Sözleşmesi'nde gizliliğin temel bir insan hakkı olduğu net bir şekilde belirtilmiştir.

Nesnelerin interneti ile ilgili olarak şirketler pazara hızlı girme ihtiyacı, düşük maliyetler ile ürün üretip düşük fiyatlar ile ürünün satılması neticesinde pazar payını ele geçirmeye çalışmaktadır. Bunun yanında piyasaya yönelik olarak hızlı çözümler sunmaya çalışmaktadır. Ancak bu durumlar ön plana çıktığında güvenlik ve gizlilik gibi konular ister istemez ikinci planda kalmaktadır. Ayrıca maliyetleri düşürmenin en önemli yollarından bir tanesi kullanılan güvenlik protokollerinin ve önlemlerinin azaltılmasından geçmektedir.

Nesnelerin internetinin hayatın her alanın girmesi, kişisel bilgilerimizi paylaşmamız neticesinde özel hayatın gizliliği konusunda ihlallerin riski de taşınmaktadır. Hem Avrupa İnsan Hakları Sözleşmesi hem de İnsan Hakları Evrensel Bildirgesi'nde belirtilen özel hayatın gizliliği nesnelerin interneti ile kullanılan nesneler veya bu nesnelerin kullandığı programlar tarafından ihlal edilmektedir. Bunun için yapılması gereken iki husus bulunmaktadır. Bunlardan birincisi şirketlerin gizlilik politikalarını güncellemesidir. Diğeri ise bireylere ciddi dijital vatandaşlık eğitimleri verilerek bu cihazların, uygulamaların doğru bir şekilde kullanılması sağlanabilecektir. Ayrıca insan hakları ile ilgili çalışan aktivistler, sivil toplum kuruluşları tarafından devletlere insan hakları çerçevesinde nesnelerin internetinde gizliliğin ve güvenliğin sağlanması için yasal düzenlemelerin yapılması için lobi çalışması yapılmalıdır.

KAYNAKÇA

Aazam, Mohammad; Khan, Imran; Aymen, Abdullah Alsaffar; Huh, Eui-Nam (2014, January). "Cloud of Things: Integrating Internet of Things and Cloud Computing and The Issues Involved". In: *Applied Sciences and Technology (IBCAST), 11th International Bhurban Conference on IEEE,* 414 – 419. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6778179&casa_token=07-iAnNSBBEAAAAA:fSsdQri5-iL8QK74JJicRGOamrKVDUCDTwk3jr33-zZN-WSkYTb1LZtPX4BcqxoN_pZo4BOXeAIonw&tag=1 (Erişim Tarihi: 01.04.2020).

Al-Garadi, Mohammed; Amr, Mohamed; Abdullah, Khalid Al-Ali; Du, Xiaojiang; Ali, Ihsan; Guizani, Mohsen (2020). "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security". *IEEE Communications Surveys & Tutorials,* 22(3), 1646 – 1685. Doi: 10.1109/COMST.2020.2988293 (Erişim Tarihi: 02.12.2020).

Al-Hayajneh, Abdullah; Bhuiyan, Zakirul Alam; McAndrew, Ian (2020). "Improving Internet of Things (IoT) Security with Software-Defined Networking (SDN)". *Computers,* 9(1), doi:10.3390/computers9010008 (Erişim Tarihi: 01.12.2020).

Akyeşilmen, Nezir (2018). *Disiplenlerarası Bir Yaklaşımla Siber Politika & Güvenlik*. Ankara: Orion Kitabevi.

Arias, Orlanda; Wurm, Jacob; Hoang, Khoa; Jin, Yier (2015). "Privacy and Security in Internet of Things and Wearable Devices". *IEEE Transactions on Multi-Scale Computing Systems,* 1(2), 99-109. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7321811&casa_token=3K13dSHpieAAAAAA:NjLNIm6kiAWtuq8kypw-kSS07ow2uxsmBSyLcjnuHZ9Fe2cVE9e6hNTzdA5lvcyGGUP3oBAv2F_b1Q&tag=1v (Erişim Tarihi: 01.11.2020).

Ashton, Kevin (22.06.2009). "That 'Internet of Things' Thing". *RFID Journal,* 22 (7), 97-114. http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (Eişim Tarihi: 01.11.2019).

Atzori, Luigi; Iera, Antonio; Morabito, Giacomo (2010). "The Internet Of Things: A Survey". *Computer Networks,* 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010 (Erişim Tarihi: 25.12.2018).

Avrupa İnsan Hakları Sözleşmesi, https://www.echr.coe.int/documents/convention_tur.pdf (Erişim Tarihi: 15.11.2020).

Broll, Gregor; Rukzio, Enrico; Paolucci, Massimo; Wagner, Matthias; Schmidt, Albercht; Hußmann, Heinrich (2009). "Perci: Pervasive Service Interaction with the Internet of Things". *IEEE Internet Computing,* 13(6), 74-81. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5262929&casa_token=au8_VVI-

qJIAAAAA:FiAdEu4rBRQNMRzQDGbH8ZMyrwQ7dJQPGF3NY_fy0d3Q1MuumNQ8nw-hsIa1rRAX9FFCcnQxv9_Vjw (Erişim Tarihi: 05.01.2020).

Coetzee, Louis; Eksteen, Johan (2011). "The Internet of Things-Promise for the Future? An Introduction". In: *IST-Africa Conference Proceedings,* 1-9. http://researchspace.csir.co.za/dspace/bitstream/handle/10204/5072/Coetzee1_2011.pdf?sequence=1&isAllowed=y (Erişim Tarihi: 11.03.2020).

Da Xu, Li; He, Wu; Li, Shancang (2014). "Internet of Things in Industries: A Survey". *IEEE Transactions on Industrial Informatics,* 10(4), 2233-2243. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6714496&casa_token=XjgpyRZH4EwAAAAA:XNlTT3FNXQBtzZptBmIHMJXFP_7Jf0duO24fTAruBPPY2Txz0_0pla399lhr74thuhbLmr9nX6jptw (Erişim Tarihi: 05.12.2019).

European Technology Platform on Smart System Integration (2008). "Internet of Things in 2020 Roadmap for the Future". https://goo.gl/DHjczG (Erişim Tarihi: 10.01.2019).

Facebook Veri İlkesi, https://www.facebook.com/privacy/explanation (Erişim Tarihi: 25.04.2021).

Google Gizlilik İlkesi, https://policies.google.com/privacy?hl=tr#infocollect (Erişim Tarihi: 25.04.2021).

Goyal, Parul; Sahoo, Ashok Kumar; Sharma, Tarun Kumar; Singh, K. Pramod (2020). "Internet of Things: Applications, Security and Privacy: A Survey". *Materials Today: Proceedings.* https://doi.org/10.1016/j.matpr.2020.04.737 (Erişim Tarihi 05.12.2020).

İnsan Hakları Evrensel Bildirgesi, https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf (Erişim Tarihi: 15.11.2020).

Kortuem, Gerd; Kawsar, Fahim; Sundramoorthy, Vasughi; Fitton, Daniel (2010). "Smart Objects as Building Blocks for the Internet of Things". *IEEE Internet Computing,* 14 (1), 44-51. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5342399&casa_token=WSV2lU2dge8AAAAA:zRMfHpSW1uJu-jV09UYwZNpaKxuH6HT2EoEVvpKpa8S7heFLtokPbW4AHTuP_bGuBBMFGi4uANTE-g (Erişim Tarihi: 01.10.2020).

Kumar, J. Sathish; Patel, Dhiren R. (2014). "A Survey on Internet of Things: Security and Privacy Issues". *International Journal of Computer Applications,* 90(11), 20-26. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.678.4896&rep=rep1&type=pdf (Erişim Tarihi: 28.09.2020).

Mayer, P. Christoph (2009). "Security and Privacy Challenges in the Internet of Things". *Electronic Communications of the EASST,* 17, 1-12. https://journal.ub.tu-berlin.de/index.php/eceasst/article/viewFile/208/205 (Erişim Tarihi: 20.09.2020).

Miorandi, Daniele; Sicari, Sabrina; De Pellegrini, Francesco; Chlamtac, Imrich (2012). "Internet of Things: Vision, Applications and Research

Challenges". *Ad Hoc Networks,* 10(7), 1497-1516. https://doi.org/10.1016/j.adhoc.2012.02.016 (Erişim Tarihi: 05.12.2019).

Oktay, Mücahit (2021). "ABD'de İstihbarat Birimlerinin Akıllı Telefonlardaki Konum Bilgilerini İzinsiz Kullandığı İddia Edildi", Anadolu Ajansı, (23.01.2021). https://www.aa.com.tr/tr/dunya/abdde-istihbarat-birimlerinin-akilli-telefonlardaki-konum-bilgilerini-izinsiz-kullandigi-iddia-edildi/2120029 (Erişim Tarihi: 25.04.2021).

Roman, Rodrigo; Najera, Pablo; Lopez, Javier, (2011). "Securing the Internet of Things". *Computer,* 44 (9), 51-58. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6017172&casa_token=MNMrzcufQ5MAAAAA:vVlSQCFiem6D-_KL5G-cHHN2N0bzEASneD4J1CDK4913uKesYcOiiDknXgAnKtZ8-71E3suysGNihQ&tag=1 (Erişim Tarihi: 01.10.2020).

Roman, Rodrigo; Zhou, Jianying; Lopez, Javier (2013). "On the Features and Challenges of Security and Privacy in Distributed Internet of Things". Computer Networks, 57(10), 2266-2279. https://doi.org/10.1016/j.comnet.2012.12.018 (Erişim Tarihi: 05.06.2020).

Saygılı, Mehmet Sıtkı; Ünal, Ahmet Naci (2018). "Cyber Terrorism Risk at Ports and Organizational Management Process in Application of Security Plan". *SETSCI Conference Indexing System,* 3, 246-251. http://set-science.com/manage/uploads/ISAS2018-Winter_0039/SETSCI_ISAS2018-Winter_0039_0045.pdf (Erişim Tarihi: 07.12.2020).

Sicari, Sabrina; Rizzardi, Alessandra; Grieco, L. Alferdo; Coen-Porisini, Alberto (2015). "Security, Privacy and Trust in Internet of Things: The Road Ahead". *Computer Networks,* 76, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008 (Erişim Tarihi: 01.03.2020).

Stankovic, A. John (2014). "Research Directions for the Internet of Things", *Internet of Things Journal,* 1(1), 3-9. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6774858&casa_token=jWzKUdoTsE4AAAAA:MEze1ktVTyhSmKXHkvNSWgm0dCRb_YQ2rY20gwMTJ2XwV73JJ7ZQs_C9z5yFqcZybTTGsF8ov7n__A (Erişim Tarihi: 02.05.2020).

Sundmaeker, Harald; Guillemin, Patrick; Friess, Peter; Woelfflé, Sylvie (2010). "Vision and Challenges for Realising the Internet of Things". *Cluster of European Research Projects on the Internet of Things, European Commision,* 3(3). doi:10.2759/26127 (Erişim Tarihi: 01.05.2020).

Suo, Hui; Wan, Jiafu; Zou, Caifeng; & Liu, Jianqi (2012). "Security in The Internet Of Things: A Review". In: *Computer Science and Electronics Engineering (ICCSEE), International Conference,* 3, 648-651. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6188257&casa_token=66wQdKXSU3gAAAAA:mbysb86tnhyTQi2JCOjC5gaDRavQr1S-dMSHxqgEemfBIa94SOyrWxxRpUlnc0M-4cA2JEd0KXWCEw (Erişim Tarihi: 15.04.2020).

Tan, L.; Wang, N. (2010). "Future Internet: The Internet of Things". In: *Advanced Computer Theory and Engineering (ICACTE)". 3rd International Conference on Advanced Computer Theory and Engineering,* 5, 376-380. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5579543&casa_token=aYE74sjJmnoAAAAA:ENWsNkHSMlX45TUjPRSMS2r3-9cq3JUgN-VCyr4qOPjuAGsUgIaZFrWbc2m4vW1739kTKsqTPhsKXw (Erişim Tarihi: 01.04.2020).

Uckelmann, Dieter; Harrison, Mark; Michahelles, Florian (2011). "An Architectural Approach towards the Future Internet of Things". *Architecting the Internet of Things,* 1-24.https://d1wqtxts1xzle7.cloudfront.net/35276741/An_Architectural_Approach_Towards_the_Future_Internet_of_Things.pdf?1414270437=&response-content-disposition=inline%3B+filename%3DAn_Architectural_Approach_Towards_the_Fu.pdf&Expires=1607347580&Signature=HjtS9PpCXAnqtanigvR01sFTUrnuSQlwOcFR2uyszMcEtyqBk9VuZHvGuOizjgcH4P~Y5PtUMcHrx2no4q6JEYz3q7NcIWD77jJ9hpfK1oLzdlMeXpyaDvLzAmFCAdO9KJoXvgy-6xmDZOeVhMEDwwhmrmDhfobbnnX0BAToJeiAwbJmmDgHjKuoTvFUdPYfNRKao44P2qnMspEYrmDgGv05PP5gDJelCGzWbIDnYnQaaDES2iya23oOyM5lBQPHkoXwdV71AdMYvat9j1xhNLiC3n5S1sCyhEOWOPjniLM-XNnVpYl9YwaNCMKajRX8Wj0ShUTUYom92rMd8G5x-Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Erişim Tarihi: 05.04.2020).

Ünal, A. Naci; Ergen, Ahu (2018). "Siber Uzayda Yeterince Güvenli Davranıyor Muyuz? İstanbul İlinde Yürütülen Nicel Bir Araştırma". *MCBÜ Sosyal Bilimler Dergisi,* 16(2), 191-216. Doi: 10.18026/cbayarsos.439489 (Erişim Tarihi: 07.12.2020).

Weber, H. Rolf (2015). "Internet of Things: Privacy Issues Revisited". *Computer Law & Security Review,* 31(5), 618-627. https://doi.org/10.1016/j.clsr.2015.07.002 (Erişim Tarihi: 10.01.2020).

Whatsapp Gizlilik Politikası, https://www.whatsapp.com/legal/privacy-policy (Erişim Tarihi: 25.04.2021).

Weber, H. Rolf (2010). "Internet of Things–New Security and Privacy Challenges". *Computer Law & Security Review,* 26(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008 (Erişim Tarihi: 10.01.2020).

WikiLeaks: CIA, akıllı telefonlar ve televizyonlar üzerinden ortam dinleme yapıyor, (08 Mart 2017), BBC Türkçe. https://www.bbc.com/turkce/haberler-dunya-39197514 (Erişim Tarihi: 25.04.2021).

Weinberg, D. Bruce; Milne, R. George; Andonova, G. Yana; Hajjat, M. Fatima (2015). "Internet of Things: Convenience vs. Privacy and Secrecy". *Business Horizons,* 58(6), 615-624. https://doi.org/10.1016/j.bushor.2015.06.005 (Erişim Tarihi: 01.02.2020).

Wu, Miao; Lu, Ting Jie; Ling, Fei Yang; Sun, Jing; Du, Hui Ying (2010). "Research on the Architecture of Internet of Things". *3rd International Conference on Advanced Computer Theory and Engineering,* 484 - 487. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5579493&casa_token=ydTt3i2cvmkAAAAA:eupZbUO5bEjztV_vvmAUQA7SNR9R_dQwZxNw0HYChSF0claomM07bkDuKl-HAs2K-mSMdFbkxtUnJA (Erişim Tarihi: 05.02.2020).

Yan, Zheng; Zhang, Peng; Vasilakos, V. Athanasios (2014). "A Survey on Trust Management for Internet of Things". *Journal of Network and Computer Applications,* 42, 120-134. https://doi.org/10.1016/j.jnca.2014.01.014 (Erişim Tarihi: 01.02.2020).

Zanella, Andrea; Bui, Nicola; Castellani, Angelo; Vangelista, Lorenzo; Zorzi, Michele; (2014). "Internet of Things for Smart Cities". *Internet of Things Journal,* 1(1), 22-32. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6740844 (Erişim Tarihi: 03.02.2020).

Ziegeldorf, Jan Henrik; Morchon, Oscar Garcia; Wehrle, Klaus (2014). "Privacy in the Internet of Things: Threats and Challenges". *Security And Communication Networks,* 7(12), 2728-2742. DOI: 10.1002/sec.795 (Erişim Tarihi: 07.06.2020).

http://www.theinternetcoalition.com (Erişim Tarihi: 25.01.2019).

SUMMARY

Communication age has begun in the world as a result of the development of technology. The most important feature of this era is that communication is very fast and communication technologies are very advanced. The most important feature of the communication age has been the widespread use of the internet. Internet usage has increased very rapidly after the 2000s. As a result of the widespread use of the internet, the concept of the internet of things, which means connecting objects to the internet in the world, was introduced. This concept was first used by Kevin Ashton. In particular, the development of RFID technology and the introduction of smart phones have been an important element that enables objects to be connected to the internet.

Internet of Things means connecting things to the internet. Thus, objects can be accessed via the internet. Especially the development of RFID technology and the cheaper technologies used in the internet of things have caused the internet of things to become widespread very quickly. With the spread of the Internet of Things, the definition of smart objects has also been developed.

Although the Internet of Things starts with RFID technology and smart phones; smart home systems, smart devices, smart televisions, cameras, and robot vacuum cleaners become more and more common and enter human life. Internet of Things technology is the fastest growing field in computer technology. As this field develops and costs decrease, the Internet of Things becomes more common.

Internet has become a very important element in human life with the connection of objects to the internet. Smart phones, smart homes, smart televisions, smart home appliances, smart devices, in short, smart objects have entered all areas of human life. The most important problem in the internet of things that enter human life so much is security and privacy. As these objects enter human life, they become targets of hackers. Security problems arise in the internet of things due to the small size of the objects and wireless connections. Hacking wireless networks, weak components, and the inability of objects to use much energy are the main reasons why they are targets of potential attacks. In addition, privacy is one of the most important issues of the Internet of Things. This is because the objects contain a lot of personal information. Various protocols and technologies are used to ensure privacy and security in the Internet of Things. However, these technologies are not secure enough.

Privacy is one of the most basic human rights. These issues have been addressed in both the Universal Declaration of Human Rights and the European Convention on Human Rights. The Universal Declaration of

Human Rights and the European Convention on Human Rights contain articles on privacy.

Especially, social media has become widespread with the internet of things and Facebook and Google, which are the most used tools in this field, have determined their privacy policies. However, despite this, they collect a lot of personal data.

For companies that want to increase their market share in the Internet of Things, developing new and cost-effective products is more important than security and privacy. In addition, programs used by objects often violate privacy of private life. In order to prevent this situation, first of all, companies update their privacy policies. In addition, by providing serious digital citizenship training to individuals, it will be possible to use these devices and applications correctly.