İletişim Kuram ve Araştırma Dergisi - Sayı 55 / Güz 2021
Ankara Hacı Bayram Veli Üniversitesi
İletişim Fakültesi
Süreli Elektronik Dergi
E-ISSN: 2147-4524

Araştırma Makalesi

Dijitalleşme ve Etik Sorunlar: Nesnelerin İnterneti Teknolojisini Gözetim, Gizlilik, Güvenlik Kapsamında Değerlendirme

Digitalization and Ethical Issues: An Evaluation of Internet of Things Technology Within the Scope of Surveillance, Privacy and Security

İlknur Doğu Öztürk, Dr. Öğrt. Üyesi, Doğuş Üniversitesi Meslek Yüksekokulu, E-posta: iozturk@dogus.edu.tr
Burcu Zeybek, Doç. Dr., Doğuş Üniversitesi Meslek Yüksekokulu, E-posta: bzeybek@dogus.edu.tr

https://doi.org/10.47998/ikad.932173

Anahtar Kelimeler:

Nesnelerin İnterneti,
Gizlilik,
Güvenlik,
Etik,
Dijital İletişim.

Öz

İnternet teknolojisi üzerinden birbirleriyle haberleşebilen nesnelerin meydana getirdiği ağ olan Nesnelerin İnternet'i (IoT) önemli bir veri kaynağı olarak değerlendirilmektedir. Nesnelerin İnterneti (IoT) ile veri paylaşımı yapılabilmekte, aynı zamanda yaşam kalitesini iyileştirmek, yeni hizmetler ve uygulamalar oluşturmak için tüm cihazlara bağlanılabilmektedir. IoT, çeşitli cihazların ve nesnelerin adreslenebilir olmasını sağlamakla birlikte, bu cihazları tanıyabilmekte ve yerini belirleyebilmektedir. Nesnelerin birbirine bağlandığı bu ağın kullanımı ise etik sorunları da beraberinde getirmektedir. Dijitalleşme sürecinin bir parçası olan IoT'un yararlı kullanım alanları ile birlikte güvenlik açıkları, gizlilik ihlalleri ve mahremiyete saygısızlık, gözetim toplumunun inşa edilmesi gibi çeşitli güçlükleri ön plana çıkmaktadır. Bu güçlükleri öncelikli olarak ele almak ve IoT ürünleri ve hizmetleri için güvenlik ve gizliliğin sağlanması temel olmalıdır. Buradan hareketle çalışma, IoT teknolojilerinin etik yaklaşımla kullanımına dikkat çekmeyi ve gözetim, bilgi güvenliği, gizlilik sorunlarını tartışmayı amaçlamaktadır. Çalışma, IoT teknolojisinin kullanımı kapsamında, tehditlerin ve çözüm önerilerinin incelenmesi açısından önemlidir. Sonuç olarak mahremiyet ve şeffaflık ile gizlilik ve gözetimin aynı anda bir arada olamayacağı; bu nedenle duruma göre esnek bir biçimde karşılanması gerektiği anlaşılmıştır. Güvenlik sorunu konusunda da sorumluluğun, IoT cihazı sağlayıcıları ve kullanıcıları tarafından paylaşılmasının gerektiği görülmüştür. Diğer yandan kullanıcının gizlilik ve güvenlik konusunda bilinçli olmasını sağlamak elzemdir.

Keywords:

Internet of Things,
Privacy,
Security,
Ethics,
Digital
Communication,

Abstract

As a network, which consists of objects communicating with each other through internet technology, Internet of Things (IoT) is considered as an important data source. Through the means of Internet of Things (IoT), not only can data be shared, but also connection to all devices is possible for improving quality, of life, and creating new services and applications. IoT allows various devices and objects to be addressed, and can also recognize and locate such devices. The use of this web, on which objects are interconnected, implies certain ethical issues. Apart from the beneficial intended uses of IoT as part of the process of digitalization, such uses introduce various challenges such as privacy violations, disrespect to privacy, and construction of surveillance society. These challenges must be addressed as a priority, and IoT products and services must be built upon security and privacy. Based on this perspective, the study aims to draw attention to the use of IoT technologies with an ethical approach, and discuss issues related to surveillance, information security, and privacy. The study is important in terms of investigating the threats and solution suggestions within the scope of the use of IoT technology. As a result of the study, it was determined that a flexible approach must be adopted according to the situation since privacy and transparency, and confidentiality and surveillance cannot exist together. It was observed that the responsibilities on the security issue must be shared between providers of IoT device and the users. It was concluded that awareness of the users of IoT devices must be raised on privacy and security.

Araştırmacı Orcid ID : 1: 0000-0001-6459-0845, 2: 0000-0002-2391-5727
Geliş Tarihi : 05.05.2021
Kabul Tarihi : 24.08.2021

Giriş

Bilgi toplumunun teknolojiye dayalı yenilikleri, özel ve kamu kurumları için talepleri, beklentileri ve ihtiyaçları tespit ederek karşılama olanağı sağlamaktadır. Teknoloji, bilgi toplumunda rekabete dayalı bir sistemi körüklemektedir. Rekabet ortamında, yeniliklerin günlük yaşama yansıma ve dâhil olma gücü, toplumsal yaşamdaki pek çok pratiğin dijital ortamda gözlenmesine, bireysel ve kurumsal faaliyetlerin daha şeffaf bir görünüm kazanmasına yol açmaktadır. Nesnelerin İnterneti (IoT) teknolojisi, veri odaklı yaklaşımı ile günlük yaşam pratiklerini dönüştüren ve kolaylaştıran, şeffaflık sağlayan ve gözetim olanağı sunan dijital araçlar arasındadır.

IoT, sensörler tarafından yakalanan veriler ile iletişim ve yerelleştirme için kullanılan donanım yardımıyla fiziksel ve sanal nesneleri benzersiz bir şekilde birbirine bağlayan küresel bir altyapı ağına dayanmaktadır (Popescul ve Georgescu, 2013:209). Nesneler kablosuz internet ile başka fiziksel nesnelere bağlanmaktadır. İnsanların hayatını kolaylaştırmak için nesneler arasında iletişim kurulmasına dayanan bu teknoloji; otomotiv, sağlık, lojistik, bilişim, inşaat ve tarım gibi çeşitli alanlarda enerji kaynaklarının sürdürülebilirliğini sağlamada, imalat ve üretim süreçlerini geliştirmede, akıllı evler ve akıllı şehirler inşa edilmesinde kullanılmaktadır (Roman v.d., 2013: 2266; Beechamresearch. "IoT Sector Map", 2016). Makinelerin kendi aralarında iletişimini ve bu makineleri kullanan insanlara ilişkin veri toplamayı mümkün kılan bu yeni teknoloji, makine-makine ve makine-insan işbirliğine olanak sağlamaktadır. Günümüzde kişiler arası iletişim sürecinin makinelerle ve makineler arası iletişime doğru genişlediği, sanal ile gerçek arasındaki sınırın bulanıklaştığı düşünüldüğünde etik sorunların tartışılması gerektiği görülmektedir. 2025 yılında dünyada 75,4 milyar cihazın ağa bağlı hâle gelmesi beklenmektedir (Evans, 2011).

IoT gibi yeni teknolojilerin yarattığı değişim ortamında erişilebilirlik, gizlilik, mülkiyet ve bilgi bütünlüğü gibi konularda kaygılar ortaya çıkmaktadır. Etik bir davranış, bilgi üzerinde mülkiyet haklarını uygulamayı, bilgiye erişimi ve bilginin bütünlüğünü sağlamayı, özel yaşam hakkını uygulamayı gerektirmektedir (Valacich ve Schneider, 2010: 484). Bu doğrultuda çalışmanın amacı, IoT teknolojisinin mevcut kullanım durumunu ve geleceğini, gözetim, mahremiyet, şeffaflık, gizlilik, veri güvenliği gibi hem birbiriyle çelişen hem de her biri önemli bir ihtiyaç olarak kabul gören konular kapsamında etik davranışa uygunluk çerçevesiyle incelemektir. Çalışma ile kullanıcılarının yeni dijital araçların etik sorun yaratma potansiyelini göz önünde bulundurmadığı varsayımından hareket edilmiştir. Bu bağlamda konu, IoT kullanımı kapsamında karşılaşılan gözetim, gizlilik ve güvenlik konuları ile ilgili kapsamlı bir literatür taraması yapılarak ele alınmıştır. IoT teknolojisinin kurumlar ve bireysel kullanıcılar için faydaları aktarılırken yol açtığı tehditler tartışılmıştır.

Nesnelerin İnterneti Teknolojisinin Kapsamı ve Özellikleri

Modern kablosuz iletişim teknolojilerinin gelişimi ile birlikte ortaya çıkan nesnelerin birbiriyle iletişimine imkân sağlayan yapılara Nesnelerin İnterneti- IoT (Internet

of Things) adı verilmektedir (Atzori v.d., 2010). Bir başka deyişle akıllı cihazların, birbirlerini algılayarak iletişime geçebilen nesnelerin internet aracılığıyla akıllı bağlantı kurması şeklinde tanımlanmaktadır (Ercan ve Kutay, 2016). Her yerden, her zaman, her şeyin birbirine bağlanabildiği bir dönemi başlatan (Tan ve Wang, 2010) ve birbirleriyle iletişim hâlinde olan milyonlarca akıllı nesneden meydana gelen nesnelerin interneti, aynı zamanda internetin geleceği olarak da görülmektedir. Nesnelerin internetinin amaçladığı insanların yaşam tarzını etkileyecek temel değişiklik, günlük hayatlarındaki her bir cihazın (ses, görüntü algılayıcıları, duman detektörleri, ev aletleri, iklimlendirme sistemleri, vb.) internet aracılığıyla ulaşılabilir (çevrim içi) olmasıdır (Doyduk ve Tiftik, 2017). Bu açıdan nesnelerin internetinin, insanların günlük faaliyetlerini kolaylaştıran yeni uygulamalar geliştirerek yaşam kalitesini yükseltmeyi amaçlayan, gelecek vadeden bir teknoloji olduğunu söylemek mümkündür.

Nesnelerin İnterneti cihazları, milyarlara varacak ölçekte artmaktadır. Bu geniş ölçekli cihazlar ağı, birbirleri ile iletişim içerisinde olabilmeleri için, kontrol edilmelidir. Bu ağ ayrıca, yorumlama ve analiz ile ilgili olarak kritik konuların öne çıkmasına neden olan ciddi miktarda veri üretimine yol açmaktadır. Sofistike yazılım algoritmalarının donanım ile birleştirildiği IoT cihazlarının zekâ becerileri, akıllı kararlar almalarına ve iletişim hâlinde oldukları diğer cihazlarla akıllıca etkileşim kurmalarına imkân sağlamaktadır. Nesnelerin İnterneti ortamında, çevre ortamı algılayan, gerekli bilgileri toplayan ve depolayan bu sensörler, elde edilen veriler doğrultusunda kararlar alarak bağlam farkındalığı sağlamaktadır. Sensörler, çevre ortamdaki değişiklikleri algılamak ve durumlarını ortaya koyan veriler oluşturmak için kullanılan IoT sisteminin, temel bir parçasını oluşturmaktadır (Guillemin ve Friess, 2009). Aynı zamanda özellikle bellek, enerji ve zamanla ilgili kısıtları aşma noktasında yönetim sürecini güç hâle getiren farklı donanım ve yazılım özelliklerine sahip milyarlarca heterojen nesneden oluşmaktadır.

Nesnelerin İnterneti teknolojisinin diğer özelliklerinden biri de, farklı özelliklere sahip cihazları birleştirerek, bu cihazlar aracılığıyla elde edilen bilgiler vasıtasıyla yeni uygulama ve hizmetler yaratmaktır. Nesnelerin İnterneti ağında, IP adresi gibi benzersiz bir tanımlayıcıdan yararlanılarak her bir nesne tanımlanır ve tanınır. Bu kimlikler, cihazları uygun platformlara göre yükselmek için Nesnelerin İnterneti üreticileri tarafından sunulur. Ayrıca bu cihazlar, kullanıcıların gerekli bilgileri cihazlardan toplamalarına, durumlarını kaydetmelerine ve bunları uzaktan yönetmelerine imkân sağlayan ara yüzlere sahiptir.

Günümüz bilgi toplumunda rekabet içerisindeki kurumlar, müşterilerinin ya da hedef kitlelerinin değişen taleplerini, ihtiyaçlarını öğrenmek, yükümlülüklerini doğru biçimde yerine getirmek için çabalasa da bu amaçların gerçekleşemediği durumlar da olabilmektedir. Bu noktada yeni bir bilgi teknolojisi olan nesnelerin haberleşmesi, iletişim kurması olan Nesnelerin İnterneti, veri yönetiminde sahip olduğu avantajlarla ön plana çıkmaktadır. Toplanan veriler sürekli ve eş zamanlı erişime açık olup veri elde etme ve paylaşma işlemleri güçlü ve verimli bir şekilde gerçekleşmektedir (Yang v.d., 2013: 1858). Gözlemleme ve kontrol, büyük veri ve iş analitiği, bilgi paylaşımı ve işbirliği alanları kapsamında uygulanan Nesnelerin İnterneti, müşteri değerinin iyileştirilmesine önemli katkı sağlamaktadır. Elde edilen bilgiler, potansiyel iyileştirme alanlarının açığa çıkmasına, ürün ve hizmetlerin maliyetlerini düşürmesine ve verimliliklerini artırmak

yoluyla optimize edilmesine olanak sağlamaktadır. Nesnelerin interneti teknolojisi ile gerçekleştirilen gözlem ve kontrol fonksiyonu, müşterilere farklı değer önermeleri sunmayı mümkün kılmaktadır. Örneğin, akıllı ev uygulamaları konseptinde enerji tasarrufu ve güvenlik müşteri değer önermeleri olarak belirtilebilir (Lee ve Lee, 2015).

Etik çerçevede, her yerde bulunma, görünmezlik, belirsizlik, tanımlama güçlüğü, özerk ve öngörülemeyen davranış, nesnelerin sosyal yaşamın ikamesi olarak görülmesini sağlayan birleşik zekâ, kontrol güçlüğü gibi dezavantajları bulunmaktadır (Popescul ve Georgescu 2013: 210-211). Bu dezavantajlar çerçevesinde gizlilik ve güvenlik konularında sorunlar yaşanmaktadır. En büyük endişe ürünün kullanımı ile ilgili verilere kötü niyetli kişiler tarafından erişilmesi konusunda gözlenmektedir (Roman vd., 2013: 2271).

Gizliliği de içinde barından güvenlik kavramı olarak; veri gizliliği, hizmet sürekliliği ve bütünlüğü, kötü yazılımlara karşı koruma, bilgi bütünlüğü gizlilik koruması ve erişim kontrolü gibi çok sayıda görevi kapsamaktadır (Alan vd., 2018: 308). Ayrıca nesnelerin interneti teknik olduğu kadar sosyal anlamda da zorlukları kapsamaktadır. Bu zorluklara etkili çözümler üretebilmek için gizlilik ve güvenlik sorunlarının çözülmesi gereklidir (Zeybek, 2020: 422).

Nesnelerin İnterneti için Olası Gizlilik Tehditleri

Nesnelerin İnternetinin büyümesine bağlı olarak internete milyarlarca yeni sensör ve cihaz dâhil olmakta, bu da insanlar hakkında, onların onayıyla ya da onayları olmaksızın, bağlantı içerisinde oldukları kişi ya da kurumlar, alışveriş kayıtları, mali işlemleri, fotoğrafları, ses kayıtları, sohbetleri, sağlık durumları da dâhil olmak üzere çok fazla bilgi üretimine zemin hazırlamaktır. Bu aşırı miktarda bilgi, gizliliği yönetilmesi güç bir konu hâline getirmektedir (Atlam v.d., 2018).

IoT sisteminde gizlilik, farklı biçimlerde ortaya çıkabilir. Ama öncelikle gizliliğin ne anlama geldiğini tanımlamak gerekmektedir. Westin (1967)'e göre gizlilik, 'Bireyler, topluluklar ya da kurumların kendileri hakkındaki bilgilerin ne zaman, nasıl ve ne ölçüde başkalarına iletilebileceğini belirleme hakkıdır'. Gizlilik, dört ana unsurla ilişkili bir kavramdır: bilgi, iletişim, beden ve bölge. Bilgi gizliliği, bir kuruluş tarafından toplanan, finansal ve tıbbi bilgiler gibi çeşitli kişisel veri türleri ile ilgiliyken, iletişimin gizliliği, herhangi bir iletişim ortamını kullanan iki iletişim noktası arasında gönderilen verilerin korunması ile ilgilidir. Bedenin gizliliği, dışarıdan gelen herhangi bir zararın yanı sıra insanların fiziksel güvenliği ile ilgiliyken, bölgesel gizlilik ev, iş yeri ve umumi yerler gibi fiziksel mekânlar üzerindeki yapı sınırları ile ilgilidir.

Byung-Chul Han (2017: 59), Platon'un mağara metaforunda bahsettiği hakikat dünyasının aksine içinde bulunduğumuz toplumu şeffaflık toplumu olarak adlandırır. Şeffaflık toplumu, hakikat ışığı olmadan içini gösteren toplumdur. Bu ışıksız toplumda ışınım her şeyi görünebilir kılar. Müdahaleci ve ayrıca hiyerarşiler ile farklılıklar yaratarak düzeni ve yön bulmayı sağlayan bu ışınım homojenleştirir ve düzleştirir. Han (2017: 60)'a göre, şeffaflık toplumu enformasyon toplumudur. Enformasyon, her tür olumsuzluktan yoksun olduğu ölçüde bir şeffaflık fenomenidir. Şeffaflık toplumu bireyleri de şeffaflığın

bir parçası olmaya zorlar. Gizliliği tercih eden birey yalnızlaştırılır. Fuchs (2020: 276) ise modern toplumda tam gizliliğin olmasının mümkün olmadığını ifade eder. Çünkü yabancılar, mübadeleyi sağlayan veya güven gerektiren sosyal ilişkilere girerler. Güveni kurmak özellikle kapitalist piyasa ilişkilerinde, diğer kişilere dair belirli verileri bilmeyi gerektirir. Bu nedenle bir yabancıya güvenilip güvenilmeyeceği, gözetim yöntemlerinin yardımıyla kontrol edilebilir. Böylece gizlilik, güven kazanmayı engellediği gibi doğası gereği gözetime karşı gelmeyi sağlamaktadır.

Bireylerin tercih/düşünce ve eylemleri -yani onlara ait her tür bilgi- gittikçe 'şeffaflaşırken'; egemen güçlerin varlıkları da, bu teknolojiler sonrasında alabildiğine 'gizli' kalmaktadır. İnternet bu bağlamda panoptik bir aygıta dönüşür. Kullanıcıları ise nesne hâlini alır (Dolgun, 2004: 61). Bu durumda gizlilik karşısında şeffaflık bir ihtiyaç olarak öne çıkmaktadır. Kişisel bilgilerin mutlaka sır olarak saklanması yerine kişisel enformasyonu paylaşma ve saklamanın bireyin kararına bırakılmasının önemli olduğu vurgulanır (Fuchs, 2020: 273).

İnsanların gizliliğinin korunması, Nesnelerin İnterneti bağlamında üstesinden gelinmesi oldukça zor bir konu hâline gelmiştir. Bunun nedeni, veri toplama sürecinin daha pasif, yaygın ve daha az müdahaleci olması, buna bağlı olarak kullanıcıların takip edildikleri konusunda daha az farkındalığa sahip olmasıdır. Kişisel bilgiler üzerindeki kontrolün kaybedilmesi potansiyel riski, bir gizlilik tehdidi olarak tanımlanır. Bu tehdit genellikle kullanıcıların temel kaygılarından biridir ve herhangi bir yeni teknolojinin ne derecede benimseneceği üzerinde önemli bir etkiye sahiptir (Atlam vd., 2018: 256). Nesnelerin İnternetinin en önemli özelliklerinden biri, nesnelerin ortamı algılama kapasitesidir. Ama bu kapasite aynı zamanda kullanıcıların eylem ve faaliyetlerinin takip edilip izlenmesine yol açar, bu da kullanıcı gizliliğinin ihlal edilmesine bağlı olarak, insanların yaşamlarını kaybetmesine kadar varan çok sayıda tehdide neden olmaktadır. Bu tehditler:

Kimlik Saptama:

Nesnelerin İnterneti sistemi, doğası itibariyle nüfuz edici niteliktedir ve bu özelliği, kullanıcılar ve onların çevre ile etkileşimleri hakkında çeşitli veri türlerinin algılanmasını ve toplanmasını mümkün hâle getirmektedir. Bu veriler genellikle kullanıcının kontrolü dışında konumlanmış hizmet sağlayıcılarında işlenir. Kimlik saptama, bir tanımlayıcının (örn. isim, adres) bir birey ile ilgili özel verilerle ilişkilendirilmesi ile bağlantılı bir tehdittir. Nesnelerin İnternetinde yeni teknolojiler ve çeşitli tekniklerin bağlantısallığı, kimlik saptama tehdidinin kapsamını genişletir (Ziegeldorf v.d., 2014). Gözetleme kameralarının güvenli olmayan bağlamlarda kullanılması, tüketicilerin davranışlarının analiz ve pazarlama amaçlarıyla incelendiği bu gibi tekniklere bir örnektir. Bu sorunun çözümü için, bir cihazın Nesnelerin İnternetinde toplayabileceği verileri minimize etmek ve verilerin üçüncü kişilerle paylaşılması üzerinde denetim sağlamak üzere öznitelik tabanlı kimlik doğrulama uygulamalarının kullanılması önerilmektedir.

Konum Saptama ve İzleme:

Konum saptama ve izleme, cep telefonu konumu, internet trafiği veya GPS verileri

gibi farklı araçlar üzerinden, zaman ve mekân vasıtasıyla bir kişinin konumunu belirleme ve kayıt alma tehditleridir (Ziegeldorf v.d., 2014). Yoğun miktarda ve kapsamlı mekânsal ve mekânsal-zamansal verilerin kullanılabilirliği, coğrafi verilerin kullanılmasına ve mekânsal bilgi analizlerine dâhil edilmesine olan ilginin artmasına yol açmıştır. Nesnelerin İnterneti sisteminin gelişimiyle birlikte, konum farkındalığına sahip uygulamaların kullanım alanlarının ve doğruluk performanslarının artması, veri toplama teknolojisinin mekân sınırlarını aşıp aynı anda pek çok yerde mevcut olabilmesi ve kullanıcının kimliği, konumu ve faaliyetlerini kaydeden Nesnelerin İnterneti cihazları ile etkileşim olanakları gibi yerelleştirme tehditlerinin boyutunu artırır gibi görünmektedir.

Profil Oluşturma:

Bireylerin faaliyet ve eylemleri hakkındaki verileri uzun süre toplayıp işleyerek bu verileri bazı özelliklere göre sınıflandırma işlemidir. Bilgiler genellikle kullanıcıların izni olmadan toplanır ve daha eksiksiz bir profil oluşturmak üzere başka kişisel verilerle entegre edilir. Profil oluşturma günümüzde e-ticaret, hedeflenmiş reklamcılık ve kredi derecelendirmesi gibi çok çeşitli alanlarda kullanılmaktadır (Toch v.d., 2012). Profil oluşturma ile bağlantılı risklerden biri, aynı bilgisayarı ve tarayıcıyı kullanan diğer kullanıcıların bir kimsenin kişisel bilgilerine maruz kalabilecek olmasıdır. Dahası, sadece izleniyor ve takip ediliyor olma farkındalığı bile çok sayıda kullanıcıda rahatsızlık duygusu oluşturmaktadır.

Nesnelerin İnternetinin yükselişi ile birlikte, veri kaynaklarının ve bağlı cihazlarının olağanüstü artışına bağlı olarak veri toplama da nicel anlamda inanılmaz derecede artış göstermektedir. Veriler artık insanların özel hayatlarının daha önce erişilir olmayan bölümlerinden toplandıkça - örneğin kıyafetlerden ve evdeki farklı cihazlardan toplanan veriler - veri, nitel olarak da değişime uğrayacaktır (Ziegeldorf v.d., 2014).

Yaşam Döngüsü Geçişleri:

Bu tür gizlilik tehdidi, bir tüketim ürününün sahibinin, ürünün yaşam döngüsü içerisinde değişmesi durumunda kişisel bilgilerin ifşa edilmesi ile ilgilidir. Akıllı telefonlar, kameralar ve dizüstü bilgisayarlar gibi kişisel bilgileri içeren tüketici ürünleri, yaşam döngüleri boyunca çoğunlukla aynı kullanıcının kontrolünde olduğu için, bu sorun çok sık gözlenmez. Fakat günlük yaşamda kullanılan nesnelerin birbirine gittikçe daha fazla bağlanmasına ve daha fazla kişisel veriyi içermesine bağlı olarak, ürün sahibinin değişmesi ile bağlantılı gizlilik ihlalleri riski de artmaktadır (Aleisa ve Reaud, 2016: 7).

Envanter Saldırısı:

Belli bir yerdeki şeylerin varlığı ve özellikleri ile ilgili bilgilerin yasadışı yollarla toplanması ile ilgilidir. Envanter saldırıları genellikle Nesnelerin İnterneti cihazlarının iletişim hızı, reaksiyon süresi vb. gibi parmak izi bilgileri kullanılarak gerçekleştirilebilir. Nesnelerin İnternetinin geleceğe dönük hedefleri tamamen gerçeğe dönüşürse tüm akıllı cihazlar İnternet üzerinden adreslenebilir hale gelecek, bu da yetkisiz kişi ve kurumların bu durumdan yararlanarak hedefe ait olan şeylerin bir envanter listesini oluşturmasına fırsat oluşturacaktır. Özel nesnelere sahip olmak, bu nesnelerin sahibi ile ilgili kişisel bilgilerin ifşasına zemin hazırladığı için, bir envanter saldırısı, bireylerin profilini çıkarmak amacıyla kullanılabilir (Ziegeldorf v.d., 2014).

Bağlantı:

Bağlantı tehdidi, birbirinden ayrı veri kaynakları ve farklı sistemlerin birleştirilmesi dolayısıyla bilgilerin kontrolsüz bir şekilde ifşası ile ilgilidir. Bireyle ilgili çeşitli türlerde bilgilerin entegre edilmesi, ürün sahibinin dahi beklemediği nitelikte bilgilerin açığa çıkarılmasını sağlar. Ortaya çıkarılan bu bilgiler, bir gizlilik ihlali olarak değerlendirilir (Toch v.d., 2012). Daha heterojen ve dağıtımlı bir sistem oluşturan farklı organizasyonların entegrasyonu ile sistemin karmaşıklığı artacağı ve veri toplama sürecini daha az şeffaf hâle getireceği için, bağlantı tehdidinin Nesnelerin İnterneti bağlamında gelecekte artması beklenmektedir (Ziegeldorf v.d., 2014).

Nesnelerin İnterneti sisteminin başarılı bir şekilde uyarlanabilmesi ve geliştirilebilmesi için, Nesnelerin İnterneti cihazlarında gizliliğin korunması temel önceliklerden biri olmalıdır. Bu ortamda gizliliği korumanın temel anahtarlarından biri, tasarım yoluyla gizliliğin koruma altına alınmasıdır. Nesnelerin İnterneti müşterileri, kendi bilgilerini kontrol edebilmeleri ve bu bilgilere kimlerin erişebileceğini tanımlayabilmeleri için gerekli özelliklere sahip olmalıdır. Günümüzde bazı şirketler, verilere istenen şekilde erişilebilmesine imkân sağlayan belli hizmetleri sunmaya yönelik bir tür anlaşmadan yararlanmaktadır. Dolayısıyla her türlü ürünün bir parçası olarak, kullanıcının gizliliğini korumaya yönelik yerleşik araçlar oluşturulmalı ve sunulmalıdır. Gizlilik ihlali ile bağlantılı temel sorunlardan biri, gizlilik konusundaki farkındalık eksikliğidir. Nesnelerin İnterneti kullanıcılarının, her türlü gizlilik ihlaline karşı kendilerini nasıl koruyabilecekleri konusunda tam farkındalığa sahip olması elzemdir (Atlam v.d., 2013). Nesnelerin İnterneti hizmet sağlayıcıları, kişisel verilerin toplanmasının kapsamını sadece sundukları hizmetlerle sınırlandırarak, veri minimizasyonu kavramını hizmet süreçlerine dâhil ederek, verileri yalnızca hizmet için gerektiği sürece tutmaları gerekmektedir (Singh v.d., 2016). Verilerin toplanmasından sonra, bireylerin kimliklerinin veri tabanlarında tutulmaması için, sosyal güvenlik numarası, plaka numarası gibi kişiye özel benzersiz tanımlayıcıların veri kayıtlarından çıkarılması gizliliği koruyacak önlemler arasında gösterilebilir. Akıllı nesnelerin ayrıntılı faktörler doğrusunda doğru kararlar verebilmesi için etkili bir erişim kontrol modelinin sunulması, Nesnelerin İnterneti kullanıcılarının gizliliğini korumaya yönelik çözümlerden biridir.

Nesnelerin İnterneti Teknolojisinde Güvenlik Sorunları

Teknolojik dönüşüm, veri odaklı bir anlayışı yaygınlaştırmıştır. Bilgi toplumu, günlük yaşam pratiklerinin bir parçası olan teknoloji yardımıyla nesneleşerek gözetlenen bir toplum hâlini almıştır (Lyon, 2006). Toplumsal hareketler, protestolar, ayaklanmalar, salgınlar ve etkili yerel yönetim gibi çeşitli gerekçeler ile gözetim bir ihtiyaç olarak kabul görmektedir. Örneğin, 2019 yılı Aralık ayında ortaya çıkan ve yeni bir dünya düzeni yaratan küresel pandemi ile mücadele amacı, hükümetleri ve yerel yönetimleri, internet teknolojisi yardımıyla daha fazla gözetim yapma için istekli hale getirmiştir. Ayrıca, bireysel internet kullanıcılarının da salgının zararını en aza indirebilme amacıyla bu gözetime daha fazla istekli olması etkisini yaratmıştır. Bu istek doğrultusunda sağlık, yerinde ve etkili yönetim, iki yönlü iletişim, verimlilik gibi çeşitli açıklamalarla gözetim pratiklerine dayanaklar dillendirilmiştir. Gözetim pratiklerine ilişkin itirazlar cılız

bir sesle dile getirilmiş ve büyük oranda bir kabulleniş gerçekleştiği görülmüştür. Bu doğrultuda, gözetim, toplumsal yaşam pratikleri içerisinde etik sınırların çizilebilmesi amacına yönelik olarak önemli bir tartışma konusunu da oluşturmaktadır. Gözetim pratiklerine yönelik kullanılabilme kapasitesi nedeniyle nesnelerin interneti teknolojisi de bu tartışmanın bir parçası olmaktadır.

Rekabet mantığına dayanan gözetim, insanlar hakkındaki veriyi toplama, depolama, işleme, yayma, değerlendirme ve kullanma yoluyla; grupların veya bireylerin belirli davranışlarını korumaya ve gerçekleştirmeye çalışır. Böylece potansiyel veya fiili fiziksel, ideolojik veya yapısal şiddet, insanların davranışlarını etki altına almak için insanlara doğrultulabilir (Fuchs, 2020: 275). Gözetim, aynı anda hem kontrolü hem de korumayı içermektedir (Lyon, 2006: 14). Fuchs (2020: 289), Lyon'un kontrol olarak ifade ettiği gözetim pratiği açıklamasını eleştirir. Gözetimin tahakküm, sömürü, sınıf, ataerkil, ırkçılık ve benzer olumsuz fenomenlerin bir boyutunu oluşturan özel bir denetim biçimi ve olumsuz bir kavram olduğunu vurgular.

Güven (2014:81), insanın gündelik yaşam pratiğinde çevresine bakarak bilgi edindiğini belirterek gözetim kavramının bugüne ait bir kavram olmadığını ve ilk toplumsal yaşam pratiklerine kadar götürülebileceğini belirtir. Bugünün gözetim kavramının, davranışların sistematik bir biçimde takip edilmesi olduğunu ve geçmişteki birbirinden haberdar olma amacının dışında çıkıldığını vurgular. Bireylerin kontrol altında tutulmasına, sistemlerin sorunsuz işlemesine ve denetimin sürdürülmesine yönelik gözetim, konuşma ve yazışmaları kayıt altına almak, anket ve görüşmeler yoluyla kişisel bilgileri elde etmek ve sosyal ağlar gibi çeşitli dijital araçların kullanımı sırasında veri edilerek gerçekleştirilir (Ketizmen, 2008: 193-194'ten akt. Çakmak ve Dinçer, 2018: 553).

Kullanıcıları, sosyal ağların ilk dönemlerinde tüm görüş, yorum, fotoğraf, kişisel bilgiyi sorgusuz sualsiz paylaşıyordu. Zaman içinde sosyal ağlarda paylaşılan bilginin güvenliğini sağlamanın önemli bir sorun olduğu görüşü oluşmaya başladı. Burada sosyal ağın kullanımı için bir ücret ödememenin karşılığı olarak kullanıcıların kendisinin ürün hâline geldiği bir ortamın inşa edilmesi, bu ortamda gizlilik ihlallerinin mahremiyet ve güvenlik konularında tartışılması gerektiği anlaşılmaktadır. Bu noktada güvenlik için, sokaklarda suç işlenmesini önlemek için yüz tanıma teknolojisinin kullanılması kabul görebileceği gibi polis devleti sonucunu yaratma korkusunu da beraberinde getirebilir. Bu etik zorlukların üstesinden gelmek için yönetişime yatırım yapmak, önceliği gizliliğe vermek, faydalar ve riskler konusunda dürüst olmak, etik konulara ticari ortakları da dâhil etmek, algoritmaları sorumlu bir şekilde kullanmak gerekmektedir (Doody, t.y.). Yönetişim ise istikrar, siyasi kararlar için destek, ortak çerçeveler ve birlikte çalışabilirlik mekanizmaları tanımlama imkânı sunar. Öte yandan, yönetişim kolayca aşırı hâle gelebilir ve aşırı kontrollü bir ortamı teşvik edebilir. (Roman vd., 2013: 2271). IoT kapsamında yönetişimin dikkatli uygulanması gerektiği anlaşılmaktadır.

Nesnelerin İnterneti sistemi ve öğelerinin fiziksel zararlar ve/veya istenmeyen tehditler oluşturmasını engellemek ve çevreyi bu zararlardan korumak için en büyük önceliklerden biri, nesnelerin güvenliğini sağlamaktır. Bunun sağlanması ve sürdürülmesi

için, güvenlik açısından kritik önem taşıyan işlemler koruma altına alınmalıdır. Güvenlik ve emniyet, birbirini etkileyen unsurlardır. Güvenlik, Nesnelerin İnterneti cihazları ile içinde bulundukları ortam üzerinde oluşabilecek fiziksel hasarlarla ilgilidir. Bir bilgisayar sistemine bağlı bir fiziksel sistemin, tek başına bir bilgisayar sisteminden daha geniş çaplı bir yüzey saldırısı oluşturacağı açıktır. Ayrıca, davetsiz misafirlerin bilgisayar sistemini algılamasını ve değiştirmesini sağlayan yan kanal saldırıları imkânı sağlayabilir. Dolayısıyla bu tür güvenlik sorunları ayrıca geleneksel güvenlik saldırılarının büyüklüğünü artırabilmektedir (Wolf ve Serpanos, 2017).

Güvenlik ve emniyet, ürünün yaşam döngüsünün tasarım aşamasında birbirine entegre edilir ve işletim aşamasında fiziksel sistemin ya da bilgisayar sisteminin kontrolünü sağlar. Nesnelerin İnterneti Cihazları internete bağlı olduğu ve gün be gün yeni tehditler ortaya çıkıp değerlendirildiği için, çalışma süresi kontrolü, yeni tehditlerin tanımlanması ve bu tehditlere bağlı risklerin en aza indirilmesine yönelik en iyi yöntemin belirlenmesi açısından daha da önem kazanmaktadır. Bu nedenle çeşitli tehditlerin tespit edilebilmesi için, sistemin işletim sırasında izlenmesi gereklidir (Wolf ve Serpanos, 2017). Cihaz, normal kullanımda güvenli bir şekilde çalışabilir, fakat cihazın hacklenmesi durumunda saldırıyı gerçekleştiren kişi, cihazın işlevselliğini manipüle ederek cihaz tarafından kontrol edilen nesnelere zarar verecek ya da cihaz aracılığıyla sistemle bağlantıya giren kişilerin güvenliğini olumsuz yönde etkileyecektir. Bu nedenle Nesnelerin İnterneti sisteminde güvenlik, titizlikle göz önünde bulundurulması gereken bir konudur (Atlam vd., 2017:256).

Nesnelerin İnterneti cihazlarının açık ve kullanılmayan portları ile bağlantılı ciddi güvenlik sorunları söz konusu olabilmektedir. Çünkü saldırıyı gerçekleştiren (hackleyen) kişiler, bu portlardan yararlanarak, başta güvenlik açısından kritik önem taşıyan cihazlar olmak üzere çeşitli cihazlara zarar verebilmektedir. Bu durumda Nesnelerin interneti cihazlarının fiziksel güvenliği ve emniyetinin sağlanması için gelecekteki ürün tasarımlarında bu konu göz önünde bulundurulmalıdır.

Nesnelerin İnterneti ile İlgili Etik Sorunlara Yönelik bir Çözüm Önerisi

Etik, felsefenin ahlaki değerle ilgili olan alt dalına karşılık gelir. İnsanın, pek çoklarına göre en temel yönü ya da özelliği, değerle doğrudan ilişkili olmak, değer yaratmak, değerin taşıyıcısı olmak olduğu için etik, temel ve önemli bir disiplindir. Etik bireyin veya ahlaki failin alıcı değil de bütünüyle kurucu ya da etkin olduğu bir alanı ya da tutumu ifade eder (Cevizci, 2012: 219-220). Etik, rasyonel yordamlamalar ile ahlaki olarak neyin doğru neyin yanlış, neyin adil neyin adaletsiz olduğunu değerlendirmektedir. Nesnelerin İnterneti bağlamında etik, insanların kendilerine ve başkalarına yönelik faaliyetlere ilişkin doğru düzenlemelerin tanımlanması ile ilgilenir; dolayısıyla neyin iyi ve kötü, doğru ve yanlış olduğunu tanımlamanın bir yolu olarak kabul edilebilmektedir. Nesnelerin İnternetinin gelişmesine, özellikle de yönetmelik ve politikaların teknolojik gelişmelerin hızına yetişememesine bağlı olarak ahlaki ikilemlerin ortaya çıkması muhtemeldir.

Nesnelerin İnterneti sisteminin günümüz toplumlarında geniş ölçekte kabul görmesine ve hâlihazırda milyarlarca cihazın bulunmasına rağmen, Nesnelerin İnterneti bağlamında etik ilkelerin uygulamaya koyulması ile bağlantılı çok sayıda sorun vardır. Tipik bir Nesnelerin İnterneti sisteminde toplanan verilerin sahibinin doğru şekilde tanımlanması güçtür. Kullanıcının rızası veya izni olmadan çeşitli veri türlerinin toplanması, Nesnelerin İnterneti sisteminde ele alınması gereken kritik bir konudur. Bir diğer konu ise Nesnelerin İnterneti sisteminin hem kamuya açık hem de kişisel verileri toplayan çeşitli sensörleri bünyesinde barındırmasıdır. Kullanıcıların bilgilerine ilişkin doğru tanımlanmış sınırların yokluğunda, kişisel ve kamuya açık bilgiler arasındaki ayrım, çeşitli Nesnelerin İnterneti uygulamalarında açıkça ortaya koyulmalı ve tanımlanmalıdır. Son olarak tek başına bir bilgisayar sisteminde güvenlik ihlali, veri kaybına ya da bilgisayar sisteminin fiziksel olarak hasar görmesine yol açabilir. Nesnelerin İnterneti sisteminde ise evler, arabalar, akıllı ölçüm cihazlarının da dâhil olduğu tüm ortamlar Nesnelerin İnterneti ağı dâhilinde birbirine bağlı olduğu için, meydana gelebilecek bir ihlal, insanların yaşamını doğrudan etkileyebilir. Örneğin bir saldırgan, ev enerjisini kontrol ederek, o evde yaşayan insanlara ciddi zararlar verebilir (Zanelle vd., 2014).

Nesnelerin İnternetinin, toplumun işleyişi ile ilgili pek çok şeyi değiştireceği açıktır. Bu nedenle, Nesnelerin İnternetinin insanlığın iyiliği için kullanılmasını sağlamaya yardımcı olacak bir etik standardın geliştirilmesi gerekmektedir. Çünkü bu sistemin kullanıldığı cihazların sayısı milyarları bulmuşken, bu cihazların ürettiği verilerin miktarı, öngörülmesi olanaksız bir seviyeye ulaşacaktır. Bu yüksek miktarda verinin verimli ve etkili büyük veri analitiği araçları ile entegre edilmesi, insanların Nesnelerin İnternetine bakışını değiştirecek ve bu verilerin kullanılması yoluyla önemli ekonomik atılımlar sağlanacaktır. Diğer yandan insanların gizliliği ihlal edilmeden bu verilerin nasıl toplanabileceğini düzenleyen uygun bir etik standart hâlâ bulunmamaktadır. Dolayısıyla gelecekte Nesnelerin İnterneti cihaz ve hizmetlerinde, dijital platformdaki kullanıcılara çeşitli etik seçenekler sunan ve kullanıcıların yararlanmak istemeleri durumunda ücret karşılığında katma değer sağlayabilecekleri bir etik tasarım geliştirilmelidir. Nesnelerin İnterneti ürünlerinde geliştirilebilecek bu etik tasarım, tüketicilerin kişisel verileri ile ilgili diğer verileri yönetip korumalarına imkân sağlayacak bir araç olarak kullanılabilecektir. Başka bir ifadeyle, Nesnelerin İnterneti kullanıcıları, Nesnelerin İnterneti cihazları ile etkileşime girerken kendi etik seçimlerini tanımlama konusunda tam bir özgürlüğe sahip olacaktır. Tüm etik seçimler ve seçenekler, programcılar ve geliştiriciler tarafından oluşturulan algoritmalara gömülü olacaktır. Bu seçimler, kullanıcıların amaçlarına en uygun olanı seçebilmeleri için farklı gizlilik ve veri koruma derecelerini içerecektir (Baldini v.d., 2018). Bu yeni özelliklerin sunulması ücretsiz olmayacağı için, etik bir Nesnelerin İnterneti Cihazı, etik çerçevenin uygulanması ve kullanıcılara daha yüksek bir özgürlük seviyesi sağlamak üzere ilave maliyetleri beraberinde getirecektir. Kullanıcılar, bu yeni etik özellikleri kullanıp kullanmama kararını verebilecektir (Atlam vd., 2018).

IoT teknolojisi ile çalışan cihazların mülkiyet hakkı bu cihazın veri tespit ettiği sensörlerin ve topladığı verinin mülkiyet hakkını da sorgulamayı gerektirir. W. Pollard (2015: 27)'a göre etik tasarıma dayalı IoT cihazları, şu özelliklere sahip olmalıdır:

- Kişisel verilerin toplanması ve dağıtımı ile hizmetleri yönetme ve kontrol etme

kabiliyeti.
- Zaman ve mekândan bağımsız olarak farklı kural ve politikaları uygulama kabiliyeti.
- Ev ve ofis gibi farklı dinamik bağlamları destekleme kabiliyeti.
- Etik seçenekleri gerekli kılan ilişkileri gözlemleme, tanıma ve destekleme kabiliyeti.

Nesnelerin İnterneti konusunda ortaya çıkan etik sorunlar, temel olarak Nesnelerin İnterneti teknolojilerinin yaygın hâle gelmesinden kaynaklanmaktadır. Nesnelerin İnterneti Sisteminin karmaşıklığı, heterojenliği ve geniş ölçekliliği dolayısıyla, bu karmaşık ortam için uygun yönetmelik ve politikaların tanımlanabilmesi adına yeni görüş ve fikirler ortaya koyulmalıdır. Ayrıca toplum, Nesnelerin İnternetine bağlı sistemlerle ilişkili risk ve fırsatları keşfetmeye devam ettikçe, bu sistemlerin kullanımı ve davranışına ilişkin şeffaflık ve etik konularının temel tartışma konularından biri olması gerekliliği daha da öne çıkmaktadır. Bunların yanı sıra, neyin uygun neyin uygunsuz, neyin iyi ve kötü olduğunun anlaşılmasına yardımcı olmak için etik çerçeveler geliştirilmesi gerekmektedir. Nesnelerin İnternetine ilişkin etik standart /tasarım mekanizmaları insan yaşamını, otonom ve öz belirlenimci sistemleri, cihazları, sanal ve fiziksel ortamları göz önünde bulunduran bir ekosistem yaklaşımını benimsemelidir (Baldini vd., 2018). Güçlü bir etik standardın şirketleri, yerel ve küresel ölçeklerde daha akıllı ve kapsayıcı tasarımlar geliştirmeye motive etmesi beklenmektedir.

Londra'da 2012 yılında "Açık nesnelerin İnterneti -Open Internet of Things" isimli kurultayda bu konuda ilk denilebilecek bir adım atılmıştır. Kurultayın sonucunda Nesnelerin İnterneti konusunda verilerin erişilebilirliği, zamanında erişimin sağlanması, mahremiyetin korunması, sürecin şeffaf olması ve verilerin kullanılmasına ilişkin konularda bir protokol imzalanmıştır (Bozkurt Yüksel, 2015: 122). Kurumsal boyutta teknolojinin etik sorun yaratma potansiyeline yönelik ilk ciddi önleyici adım atılmıştır. Bu iyi niyetli ilk adımın kapsamının genişletilmesi ve etik ilkelerin standartlaşmasının sağlanması önerilmektedir. Bu noktada her şirket, Nesnelerin İnterneti bağlamında bir etik emele sahip olmakla sorumludur; aksi takdirde tüketiciler, kişisel bilgilerinin erişime açılmasına izin vermeyecek, bu da şirketler adına veri açıklarına yol açacaktır. Şirket liderleri, bu konuyu doğru şekilde yönetebilmek için Nesnelerin İnterneti teknolojilerinin kapasitesini ve tüm dünyada erişim olanaklarının nasıl kolaylaştırılabileceğini uygun şekilde değerlendirmelidir.

Sonuç

Rekabet üstünlüğü mücadelesinde ayırt edici bir teknoloji olan Nesnelerin İnternetinin alt yapısı ve uygulamaları, etik konularla çerçevelenerek gizlilik ve güvenlik sorunları bağlamında avantajları ve dezavantajları ile incelenmiştir. İnceleme sonucunda insanlara hizmet amacıyla makinalar arasında iletişim kurulmasının ürettiği veri yoğunluğu ile bu verileri gizleme ve verilerin mahremiyetini sağlamanın önünde çok ciddi bir risk potansiyeli taşımaktadır. Ayrıca mahremiyet ve şeffaflık ile gizlilik ve gözetimin aynı anda karşılanması güç ihtiyaçlar oldukları duruma ve olaya göre esnek bir biçimde gözetilmeleri gerektiği anlaşılmıştır.

Nesnelerin İnterneti teknolojisinde sensörlerin topladığı veriler sayesinde verilerin sahipleri belirlenebilmektedir. Bu cihazların kullanıcılarına, neye rıza verdiğini bilmek ve kimlik bilgilerini erişime açmamak gibi sorumluluklar yüklenmiştir. IoT uyumlu cihazların güvenlik ve gizlilik konularının sorumluluğunu kullanıcı odaklı bir etik anlayışla üstlenmesi gerekmektedir. Nesnelerin interneti teknolojisine uyumlu cihazların üreticilerinden etik konulara yönelik standartlara uyum anlamında sınırlar beklenmediği, bu cihazların kullanıcılarının, bilinçli birer tüketici olmalarını sağlamanın gerektiği görülmüştür. Söz konusu teknolojiye uyumlu cihaz kullanmaya başlayacak kişilere, ürünün teknik özellikleri ile birlikte cihaz üzerinden hangi verilerinin toplanabileceği, bu verilerin paylaşılmasının önlenmesi için neler yapılması gerektiği gibi gizlilik ve güvenlik haklarına ilişkin bilgilendirme yapılmasının önemi anlaşılmıştır. Farkındalık kazanan bilinçli kullanıcılar, mahremiyetlerini koruma ve verilerinin güvenliğini sağlama konularında hem yasal haklarını öğrenecek hem de dijital becerilerini geliştirebilecektir. Verilerinin işlenmesini önleyemese de bu verilerin daha anonim özellik kazandırıldıktan sonra üçüncü kişilerle paylaşılmasını talep edebilmelerini sağlayacak bir iletişim etiği ve dijital okuryazarlık düzeyi için bilinç ve farkındalık en önemli koşul olarak dikkat çekmektedir.

Hak odaklı bir anlayışın temel olması şartıyla iletişim etiğine yönelik toplumun eğitilmesi gerekmektedir. Böylece haklarını gözeterek etik davranan bireyler söz konusu etik sorunlarla mücadele edebilecektir. Bu noktada, Nesnelerin İnterneti teknolojisi gibi dijital iletişim araçlarının kullanılmaları sırasında oluşan verilerin nasıl kullanılacağı konusunda, o cihazın sahibi olanların bilgilendirilmesi gerektiği de dikkat çekmektedir. Bu teknolojiye uyumlu cihaz topladığı veriyi faaliyet alanı ile ilgili bir kuruma iletiyor ve bu veri ile o cihazın sahibi ve kullanıcısı potansiyel müşteri görünümü kazanıyorsa burada vurgulanması gereken kullanıcının ürettiği verinin kimlerle paylaşılabileceğidir. Bu paylaşım fark edildiğinde yasal olarak yapılabilecekler ve ürünü kullanmayı bırakabilme durumu ile ilgili olarak daha kullanmaya başlamadan bilgilendirilme yapılması gerekmektedir.

IoT ile elde edilen verilerin filtrelenmeden dağıtılmasının önüne geçmek gerekmektedir. Verilerin toplanmasından sonra, bireylerin kimliklerinin veri tabanlarında tutulmaması için, sosyal güvenlik numarası, plaka numarası gibi kişiye özel benzersiz tanımlayıcıların veri kayıtlarından çıkarılması gizliliği koruyacak önemler arasında gösterilebilir. Akıllı nesnelerin ayrıntılı faktörler doğrusunda doğru kararlar verebilmesi için etkili bir erişim kontrol modelinin sunulması, Nesnelerin İnterneti kullanıcılarının gizliliğini korumaya yönelik çözümlerden biridir.

Nesnelerin İnterneti teknolojisinin kullanım pratiği çerçevesinde tartışılan gizlilik ve güvenlik sorunları, devletlerin gelecekte önemli bir mücadele alanı olma potansiyeline sahiptir. Bu doğrultuda söz konusu sorunlara yönelik proaktif olmak gerekmektedir. Gizliliği kontrol altında tutmayı sağlayan etik ilkelerin gözetilmesi sorumluluğu sadece kullanıcılara yüklenmemeli kurumların sorumluluk üstlenmeleri sağlanmalıdır.

Kaynaklar

Alan, A.K., Kabadayı, E.T. ve Cavdar, N. (2018). Yeni nesil "bağlantı", Yeni Nesil "İletişim: Nesnelerin İnterneti Üzerine Bir İnceleme". İşletme Araştırma Dergisi, 10(1), 294-320.

Aleisa, N., ve Reaud, K. (2016). Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion). arXiv e-prints, 1-10.

Atlam, H.F., Attiya,G ve El-Fishawy, N. (2013). Comparative Study on CBIR based on Color Feature. International Journal of Computer Applications, 78(16), 9-15.

Atlam, H, F., Alenezi, A., Walters, R. ve Wills, G.B. (2017). An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things. 2nd International Conference on Internet of Things, Big Data and Security. INSTICC. 254-260.

Atlam, H.F, Walters, R.J., ve Wills, G.B. (2018). Internet of nano things: security issues and applications. 2nd International conference on cloud and big data computing, October, 71-77.

Atzori L.,Iera A. ve Morabito G., (2010). The Internet of Things: A Survey. Comput. Networks, c. 54, sayı 15, 2787–2805.

Baldini, G., Botterman, M., Neisse, R. ve Tallacchini, M. (2018). Ethical Design in The Internet of Things, Sci Eng Ethics. 24(3). 905-925.

Beechamresearch. "IoT Sector Map". Erişim adresi: http://www.beechamresearch.com/article.aspx?id=4 (04.08.2016).

Bozkurt Yüksel, A. (2015). Nesnelerin İnternetinin Hukuki Yönden İncelenmesi. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 17(2), 113-140.

Chul Han, B. (2017). Şeffaflık Toplumu. İstanbul: Metis Yayınları.

Cevizci, A. (2012). Felsefeye Giriş. İstanbul: Say Yayınları.

Çakmak, T. F., ve Dinçer, F. İ. (2018). Gözetim Toplumu Yönetimi ve Turizm Endüstrisi Açısından Değerlendirilmesi. Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi, 6(4), 551-558.

Dolgun, U. (2004). Gözetim Toplumunun Yükselişi: Enformasyon Toplumundan Gözetim Toplumuna. Yönetim Bilimleri Dergisi, 2(1), 55-74.

Doody, L. (t.y.). Can the Smart City Be Ethical with Its Data? Erişim adresi: https://www.arup.com/perspectives/can-the-smart-city-be-ethical-with-its-data

Doyduk, H.B.B. ve Tiftik, C. (2017). Nesnelerin İnterneti: Kapsamı, Gelecek Yönelimi Ve İş Fırsatları. Üçüncü Sektör Sosyal Ekonomi. 52(3): 127-147. doi:10.15659/3.sektor-sosyal-ekonomi.17.12.767.

Ercan, T. ve Kutay, M . (2016). Endüstride Nesnelerin Interneti (IoT) Uygulamaları. Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi , 16 (3) , 599-607.

Evans, Dave. (2011). "The Internet of Things: How the Next Evolution of The Internet is Changing Everything." CISCO White Paper 1.2011 1-11. Erişim adresi: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Fuchs, C. (2020). Sosyal Medya: Eleştirel Bir Giriş, Çev. Diyar Saraçoğlu, Çev. İlker Kalaycı Ankara: NotaBene Yayınları.

Guillemin , P.,ve Friess, P. (2009). Internet of Things Strategic Research Roadmap, Lüksemburg, Erişim adresi: https://sintef.brage.unit.no/sintefxmlui/bitstream/handle/11250/2430372/SINTEF%2BS13363.pdf?sequence=2

Güven, O. Ö. (2014). Gözetim Tekniklerinin Güç İlişkileri Bağlamında Dönüşümü Ve Toplumsal Denetim. Atatürk İletişim Dergisi, (7), 79-112.

Lee, I. ve Lee, K. (2015). The Internet of Things (IoT): Applications, Investments and Challenges for Enterprise, Business Horizons, 53, 431-440.

Lyon, D. (2006). Gözetlenen Toplum. G. Soykan (Çev.) İstanbul: Kalkedon Yayınları.

Pollard, W. (2015). IoT Governance, Privacy and Security Issues, Eur. Res. Clust Internet of Things, 23-31).

Popescul, D., ve Georgescu, M. (2013). Internet of Things–Some Ethical issues. The USV Annals of Economics and Public Administration, 13(2 (18)), 208-214.

Roman, R., Zhou, J., ve Lopez, J. (2013). On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks, 57(10), 2266-2279.

Singh, J., Pasquier, T., Bacon, J., Ko, H., Eyers, D. (2016). Twenty security considerations for cloud-supported internet of things. IEEE Internet Things J. 3(3), 269–284.

Tan, L., ve Wang, N. (2010). Future internet: The Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 5, V5-376-V5-380.

Toch, E., Wang, Y. ve Cranor, L.F. (2012). Personalization and Privacy: A Survey of Privacy Risks and Remedies in Personalization-Based Systems. User Modeling and User-Adapted Interaction. 22(1-2). 203-220.

Valacich, J., ve Schneider, C. (2010). Information Systems Today: Managing in The Digital World. Prentice Hall.

Westin, A.F. (1967). Privacy and Freedom, Atheneum, New York.

Wolf, M.ve Serpanos, D. (2017). Safety and Security of Cyber Physical and internet of Things Systems. Proceedings of the IEEE. 105(6). 983-984.

Yang, L.,Yang, S. H. ve Plotnick, L. (2013). How the Internet of Things Technology Enhances Emergency Response Operations. Technological Forecasting and Social Change. 80(9), 1854-1867.

Zanelle, A., Bui, N., Castellani, A., Vangelista, L. ve Zorzi, M. (2014). Internet of Things for Smart Cities. IEEE Internet Things, 1(1). 22-32.

Zeybek, B. (2020). "Nesnelerin İnterneti Uygulama Alanı Olarak Akıllı Şehirler: Geleceğin Marka Şehirleri. Edit. P. E. Yayınoğlu, B. Küçüksaraç, İletişim Çalışmalarında Yaratıcı Ve Yenilikçi Uygulamalar. Konya: Literatürk academia.

Ziegeldorf, J.H., Morchon, O.G. ve Wehrle, K. (2014). Privacy in the Internet of Things: Threats and Challenges, Security and Communication Network. 7(12). 2728-2742.

Araştırmacı Katkı Oranı: *Araştırmacılar çalışmaya eşit oranda katkı sunmuştur.*

Destekleyen Kurum/Kuruluşlar: *Herhangi bir kurum/kuruluştan destek alınmamıştır.*

Çıkar Çatışması: *Herhangi bir çıkar çatışması bulunmamaktadır*