

# RİSK İLETİŞİMİ PERSPEKTİFİNDEN NESNELERİN İNTERNETİ ÜZERİNE BİR İNCELEME: YENİ TEKNOLOJİLERİN YENİ RİSKLERİ

**Denizcan KABAŞ\***

## Özet

Günümüz internet araç ve teknolojileri insan yaşantısına dair çeşitli kolaylıklar sağlayabilmektedir. Özellikle son yıllarda literatüre de yerleşen Nesnelerin İnterneti (IoT-Internet of Things), pek çok farklı alanda insan müdahalesini minimum düzeye indirgeyerek gündelik yaşantının farklı alanlarındaki ‘verimliliği’ artırabilmektedir. Ancak öte yandan söz konusu kullanım biçimleri beraberinde öngörülmesi zor yeni sorunları da getirebilmektedir. Bu doğrultuda bakıldığında kitle iletişim araçları vasıtasıyla toplumsal ve/veya bireysel yaşantının çeşitli kademelerinde yaşanabilecek sorunları öngörme ve bunlara çözüm bulma amacı taşıyan risk iletişimi stratejileri, nesnelerin interneti olgusuyla da farklı perspektiflerden katkı sağlayabilmektedir. Ancak gelişen internet teknolojilerinin beraberinde yeni sorunları da gündeme getirme potansiyeli, nesnelerin internetini yeni risklerin taşıyıcısına dönüştürebilmektedir. Bu çalışmada da, risk iletişiminin klasik işleyiş paradigmalarından hareketle, nesnelerin internetinin risk olgusuna karşı taşıdığı olanaklar ile ortaya çıkabilecek ‘yeni tip riskler’ arasındaki temel çelişkiler tartışılmaktadır.

**Anahtar Kelimeler:** risk, risk iletişimi, risk toplumu, yeni teknolojiler, nesnelerin interneti.

\* Araştırma Görevlisi, Üsküdar Üniversitesi, İletişim Fakültesi, E-Posta: denizcan.kabas@uskudar.edu.tr



# AN EXAMINATION ON THE INTERNET OF THINGS FROM RISK COMMUNICATION PERSPECTIVE: NEW RISKS OF NEW TECHNOLOGIES

**Denizcan KABAŞ\***

## **Abstract**

Today's internet tools and technologies can provide various facilities for human life. Especially IoT (Internet of Things), which has been used in the literature in recent years, can increase 'productivity' in different areas of daily life by minimizing human intervention in many different areas. On the other hand, these may also bring about unpredictable new problems. In this respect, through mass media, risk communication strategies aiming to predict the problems that may be experienced in various levels of social and/or individual life and finding solutions to these, can also contribute from different perspectives with the internet of things. However, the potential of bringing new problems to the agenda along with developing internet technologies, may cause the internet of things to convey new risks. In this study, based on the classical paradigms of risk communication, the main contradictions between the possibilities of the internet of things against the phenomenon of risk and possible 'new types of risks' are discussed.

**Keywords:** *risk, risk communication, risk society, new technologies, internet of things.*

\* Research Assistant, Üsküdar University, Faculty of Communication, E-Mail: denizcan.kabas@uskudar.edu.tr



# RİSK İLETİŞİMİ PERSPEKTİFİNDEN NESNELERİN İNTERNETİ ÜZERİNE BİR İNCELEME: YENİ TEKNOLOJİLERİN YENİ RİSKLERİ

## GİRİŞ

Günümüz dünyası hem teknolojik unsurların hızlı değişimi ve gelişimi hem de buna bağlı olarak ortaya çıkan yenilikler ekseninde şekillenmektedir. Özellikle enformasyon temelli küresel ağların yaygınlaşması ile teknolojiye dair 'erişebilirlik algısı', gündelik yaşam pratiklerini değişime uğratmaktadır. Bu açıdan bakıldığında, kesintisiz bir biçimde birbirleriyle bağlantı içerisinde olan bireylerde de olduğu gibi, çeşitli elektronik cihazların da kendi aralarında bir tür iletişim gerçekleştirdiği görülmektedir. Bu iletişimin boyutları ise aşama aşama insan faktörünün bağlayıcılığını ortadan kaldırmakta, bir anlamda da, nesnelere kendi bilinç ilişkilerini ortaya çıkartmaktadır.

'Nesnelerin İnterneti' (*Internet of Things: IoT*) olarak da adlandırılan 'akıllı cihazların etkileşimi' konusu bu noktada anlam kazanmaktadır. Zira çeşitli kablosuz bağlantılar aracılığıyla pek çok elektronik cihaz birbirleriyle etkileşim kurabilmekte ve hatta internet vasıtasıyla da bu durum zaman-mekân gözetmeksizin, küresel ölçekte etkili olabilmektedir. Ev eşyalarından akıllı otoyollara, giyilebilir teknolojilerden tohum uyarı sistemlerine dek pek çok farklı alandaki nesnelere kurduğu etkileşimler, en temelde 'yaşamı kolaylaştırma' ve 'riskleri engelleme' eksenlerinde işlevlik kazanmaktadır.

Risk konusu, hem günümüz toplumsal yaşantısının ekonomi-politik çerçeveler içerisinde yeni belirsizliklerle karşılaşılması hem de teknolojik gelişmeler ile küresel ölçekteki etkileşimlerin yeni tehditleri durmaksızın üretmesi nedeniyle, dikkatle üzerinde durulması gereken bir konu olarak karşımıza çıkmaktadır. Bu açıdan nesnelere interneti olarak adlandırılan söz konusu teknolojilerin de mevcut ya da öngörülemez riskleri engelleme potansiyeline sahip olması, yeni paradigmanın geliştirilebileceği konusunda fikir vermektedir. Bu durum da; risklerin tanımlanması, bu

konuda farkındalık yaratılması, önlem alınması ve olası risk durumlarında gerçekleştirilecek faaliyetlerin belirlenmesi ile harekete geçilmesi açısından pek çok yeni olanağın tanımlanmasını sağlamaktadır.

Nesnelerin interneti, genel olarak riskleri engelleme ve olası risk durumlarında harekete geçecek akıllı sistemlerin, insan etkisinin minimum seviyede tutularak, kendiliğinden işlemesi anlamında öne çıkmaktadır. Ancak bu durum da beraberinde yeni soru işaretlerini getirmektedir. Özellikle elektronik cihazlar ve internetin kendi içerisinde getirebileceği yeni riskler meselesi ile insan etkisinin olabildiğince azaltılması konusunun yaratabileceği farklı tehlikeler de, bu kapsamda olası tehditlerin temel çerçevesini oluşturmaktadır. Öte yandan söz konusu bu sistemlerin, büyük şirketlerin tekelinde bulunması ve pazarlama süreçlerinin de küresel ölçekteki kâr marjlarının düşünülerek yapılması konuları da, ele alınabilecek diğer sorunların oluşması hakkında yeni tartışmalar başlatabilmektedir.

Risk iletişimi genel çerçeveden bakıldığında; risklerin öngörülebilmesi, kitlelerin sosyo-kültürel özelliklerine uygun bir şekilde farkındalık yaratılabilmesi, uzmanlar ile bireylerin buluşturulması gibi aşamalardan oluşturulan ve nihai olarak, risk kültürü oluşturulmasını hedefleyen bir olgu olarak değerlendirilebilmektedir. Nesnelerin interneti de, ilk etapta riskleri engelleme ve risk anında durumu bertaraf etmeye yönelik faaliyetler gösteriyor olmakla beraber aynı zamanda da, kullanıcıların olası riskler konusunda bilinçlendirilmesi ve bu konudaki farkındalıklarının arttırılması gibi kolaylıklar da sunmaktadır.

Nesnelerin interneti, özellikle son yıllarda giderek artan bir tartışma ve kullanım alanını oluşturmaktadır. Bu kapsamda yakın bir gelecekte, gündelik hayatlarımızın sıradan bir parçası haline dönüşeceği düşünülen nesnelerin internetinin risk iletişimi açısından olumlu ve olumsuz yönlerinin irdelenmesi, hem risk iletişimi alanına farklı yaklaşımların getirilmesi hem de yeni teknolojik gelişmelerin toplumsal hayat dinamiklerine olan etkilerinin öngörülmesi açısından önem taşımaktadır.

## Risk Kavramı ve Risk İletişimi

Risk sözcüğü, en temel çerçevede şu şekilde tanımlanabilmektedir: “Bir olayın belirli koşul ve ortamlarda doğurabileceği can, mal, ekonomik ve çevresel gibi değerlerin kaybının gerçekleşme olasılığı. Diğer bir deyişle; “risk=potansiyel kayıplar” veya “risk=tehlike x hasar görülebilirlik” (AFAD, 2014:128). Bu noktada dikkat çeken unsur ise, ‘olasılık’ kavramı olarak karşımıza çıkmaktadır. Zira risk kavramının mevcudiyeti ancak bir olasılık durumu ile söz konusu olabilmektedir. Bu açıdan riskin, gelecekteki olasılıklar düşünülerek kapsamlı bir çerçevede ele alınan tehlikeleri anlattığı söylenebilmektedir (Kasapoğlu, 2007:2). Öte yandan risk, bir açıdan da felaket öngörüsü anlamına gelmekte ve kitle iletişim araçları olmadan, sanal bir durum olarak, gerçekleşinceye kadar tam manasıyla anlaşılammamaktadır (Beck, 2014:357). Genel çerçeveden bakıldığında temel risk alanlarını Giddens’ın (1994) kategorileştirdiği noktalar üzerinden değerlendirmek, bütüncül bir bakış açısının geliştirilebilmesine olanak tanımaktadır:

“1. Riskin yoğunluk anlamında küreselleşmesi: Örneğin, nükleer savaş insanlığın varlığını tehdit edebilmektedir.

2. Riskin, gezegenimiz üzerindeki herkesi, en azından çok sayıda kişiyi etkileyebilecek nitelikteki rastlantısal olay sayısının çoğalması anlamında küreselleşmesi: Örnek olarak, küresel işbölümündeki değişimler.

3. Yaratılmış çevreden ya da toplumsallaşmış doğadan kaynaklanan risk: İnsan bilgisinin maddi çerçeveye girmesi.

4. Milyonların yaşam şansını etkileyen kurumsallaşmış risk ortamlarının gelişimi: Örneğin, yatırım pazarları.

5. Riskin, risk olarak bilinmesi: Riskler içindeki “bilgi boşlukları” dinsel bilgiler ya da sihir yoluyla “kesinlikler” haline çevrilemez.

6. Yaygınlaşmış risk bilgisi: Ortak olarak karşılaştığımız tehlikeler geniş kitlelerce bilinmektedir.

7. Uzmanlığın sınırlılıklarının bilinmesi: Hiçbir uzmanlık sistemi, uzmanlık ilkelerinin uygulama sonuçları açısından tümüyle uzman olamaz. (1994:113)”

Bu durumlar aslında risk kavramının tek başına ele alınamayacağını, toplumsal ve teknolojik dinamiklerin de göz önünde bulundurularak farklı olasılıkların incelenmesi gerekliliğini ortaya koymaktadır. Bu açıdan kitle iletişim unsurlarına ve temel toplumsal değişimlere yapılan vurgular, risk kavramının söz konusu iletişim alanı ile toplumsal olanın kesişimine işaret etmektedir.

Toplumsal koşulların içkin bir şekilde risk kavramını geliştirdiği söylenebilmektedir. Bu durum 'risk toplumu' olarak adlandırılan bir gerçekliği ortaya koymaktadır. Bu açıdan risk toplumunda farklı nitelikler ve etki güçleri taşıyan risklere maruz kalma ihtimali olan grup ve birey sayısının artmakta olduğu (Yakut, 2008: 16) ifade edilebilmektedir. Bu doğrultuda da toplumsal yaşantının bir diğer özelliği olarak, önceki dönemlerde karşılaşılan risklerin üzerine eklenen yeni sorunların karşımıza çıktığı söylenebilmektedir. Zira en temelde, sosyo-ekonomik belirleyiciler ve teknolojik üretim-tüketim biçimlerinde yaşanan değişimlerin, bambaşka tehlikeleri de ortaya koyduğu gözlemlenmektedir. Bu açıdan Ulrich Beck'in (2014:72) yaptığı değerlendirme de, yaşanan dönüşümün tablosunu genel hatlarıyla ortaya koymaktadır:

“Sınıflı toplumun itici gücü şöyle özetlenebilir: Açım! Öte yandan, risk toplumunun harekete geçirdiği devinim ise şöyle ifade edilir: Korkuyorum! İhtiyaç ortaklığının yerini endişe ortaklığı alır. Risk toplumu modeli, bu anlamda endişeden kaynaklanan dayanışmanın ortaya çıktığı ve siyasi güç haline geldiği toplumsal bir dönemi imler.”

Risk toplumu olarak ifade edilebilen günümüz açısından, söz konusu risklerin bir hayli geniş bir çerçevede karşımıza çıktığı ve bunların da zaman-mekân gözetmeksizin oldukça karmaşık bir şekilde oluştuğu ifade edilebilmektedir. Örneğin; “Genetiği bozulmuş meyve ve sebzeler, biyolojik silahlar, nükleer silahların kullanılması ve halen kullanılacak tehdidiyle yaşanılması, savaşların devam etmesi, sanayide kullanılan zehirli gazlar, küresel ısınma ve ozon tabakasının delinmesi...” (Kul, 2007:124-125) gibi birbirinden farklı ve bir o kadar da benzer sorunlar, günümüz toplumlarının başat riskleri konusunda fikir vermektedir. Bu açıdan söz konusu risklerin merkezinde, artık yalnızca doğanın dönüştürücü etkisinin değil; insanın doğaya ve yine insana karşı giriştiği eylemlerin de olduğu açıkça



belirtilebilmektedir. Temel bir hareket noktası olarak ise, söz konusu risklerin sınıflandırılması; “doğal (*dışsal*)” ile “imal edilmiş (*manufactured*)” veya “insan ürünü (*human-made*)” (Kasapoğlu, 2007:3) şeklinde yapılabilmektedir. Ancak günümüz risklerinin girift yapısı beraberinde çözüm konusunda bir belirsizlik getirmekte ve söz konusu riskleri yeni boyutlarda, yeniden üretebilmektedir. Bu da aslında; siyasi, ekonomik ve toplumsal hayatta artan belirsizliklere paralel olarak risklerin de artması ve dahası; risklerin de bireyler üzerinde baskılar oluşturarak, yeni türden risklerin oluşturması (Akbal, 2007:71) yönünde gerçekleşmektedir.

Her ne kadar bu ve benzeri değerlendirmeler bir tür bilinmezliği işaret ediyor gibi görünse de, hem toplumsallık içerisinde hem de bireysel potansiyeller kullanılarak gerçekleştirilebilecek değişimlerin de mevcut olduğu bilinmektedir. Bu açıdan risk iletişimi olarak adlandırılan süreçler, kullanabilecek ve yeniden üretebilecek teknolojik imkânlar vasıtasıyla, yeni önlem biçimleri ortaya koymaktadır. Özellikle vurgulamak gerekirse, risklerle mücadelenin sadece anlık bir eylem değil; bir süreç halinde, pek çok farklı bileşenin ve sosyo-ekonomik ile kültürel arka planların da düşünülerek ve dahası geçmişte yaşanılanlardan önemli dersler çıkarılarak gerçekleştirilebileceği göz önünde bulundurulmalıdır. Sonuç olarak risk iletişimi olarak adlandırılan bu süreçlerin önemi, bir kez daha ortaya çıkmaktadır.

Risk iletişimi, hem yaşanılacak sorunların ortaya konması hem de olasılığın gerçekliğe dönüşmesine engel olunması açısından önemli bir yol haritasını işaret etmektedir. Bu açıdan bakıldığında, risk iletişimi kavramı, genel hatlarıyla, şu şekilde tanımlanabilmektedir: “İnsanların tehlikeler hakkında bilgilendiği, davranış değişikliği yönünden etkilendiği ve riskler ile ilgili karar mekanizmalarına katılabildikleri sosyal süreç” (AFAD, 2014:128). Risk iletişimi olgusu biraz daha açılacak olunursa, ilgili süreçler katılımcı bir boyutta gerçekleştirilebilmektedir: “Risk iletişimi, riskin varlığı, doğası, şekli, ciddiyeti ve kabul edilebilirliğine ilişkin paydaşlar arasındaki iki yönlü iletişimidir. Ancak bu şekilde paydaşlar arasında fikir ve eylem birliği geliştirilebilir” (Kadıoğlu, 2011:100). Tehlike (olasılık), kabul edebilirlik, davranış değişikliği, etkilenme, karar alma, katılım, sosyal ve süreç gibi sözcüklerin aynı zamanda risk iletişiminin ana unsurları olduğu düşünülebilmektedir. Bu açıdan asıl önemli nokta ise, riskin ne olduğunun analiz edildiği aşama olarak karşımıza çıkmaktadır.

Risklerin ele alınması, ilk etapta risk analizi süreci ile gerçekleştirilmekte ve bu aşamada aslında risk iletişiminin de temel hareket alanı oluşturulmaktadır. Bu çerçevede risk analizinin, iletişim biliminin teori ve modellerinin üzerinde şekillendiği ve iletişim süreçlerinin asıl çalışma alanı olarak belirlediği (Yakut, 2008:9) söylenebilmektedir. Bu doğrultuda da risk analizinin 4 aşamalı bir süreç içerisinde gerçekleştiği görülmektedir. Bu aşamalar ise şu şekilde özetlenebilmektedir: “1. Zararın belirlenmesi 2. Doz-cevap değerlendirmesi 3. Etkilenim değerlendirmesi 4. Risk nitelendirmesi” (Güler ve Çobanoğlu, 1997:27). Risk iletişimi içerisinde izlenecek yolun ise, sadece riskin analiz edilmesi ile sınırlı kalmayacağı ve en genel çerçevede, ‘Çağdaş Afet Yönetimi’ olarak adlandırılan kapsamlı bir sürecin ele alınma zorunluluğunun olduğu görülmektedir. Söz konusu süreç ise; olası afet öncesi-sonrası tüm toplumsal kesimler arasındaki riske dair bilgi akışının sağlanması, zaruri önlemlerin ilgili kesimlere duyurulması, bu kapsamda uygulama etkinliklerinin hayata geçirilmesi ile ilgili tüm işbirliği faaliyetlerini kapsamaktadır (Yakut, 2008:17). Buradan da hareketle; zararların azaltılması, hazırlık, müdahale ve iyileştirme gibi farklı aşamaların bir bütün olarak, söz konusu yönetim şeması içerisinde konumlandığı (Kabasakal, 2008:13) ve bu aşamaların da önemle dikkate alınması gereken bir süreç olduğu (Kasapoğlu, 2007:55) ifade edilebilmektedir.

Tüm bu süreçlerden hareketle; risk iletişiminin konumlandığı ve asıl önem atfettiği aşama olarak ise, ‘olay öncesi’ olarak kavramsallaştırılabilecek nokta ele alınabilmektedir: “Risk iletişimi bir olay meydana gelmeden önce yapılan koruyucu/önlem alıcı çalışmaları ortaya koymaktadır. Risk iletişimi, uzun dönemli, kapsamlı kalıcı etkisi olan çalışmaları öne çıkarmaktadır.” (Yakut, 2008:23). Bu açıdan ‘Çağdaş Afet Yönetimi’ içerisinde yer alan ve koruyucu/önleyici faaliyetleri de kapsayan ‘zarar azaltma’ aşamasına bakılacak olunursa; zarar azaltmaya dair faaliyetlerin, temel amacının riski azaltmak olduğu ve bu doğrultuda da hazırlık ile müdahale aşamalarından farklılaştığı (İTÜ, 2005:6) görülmektedir. Bu çerçevede, risk yönetimi olarak adlandırılan kapsamlı çalışmalar içerisinde, söz konusu tüm süreçlerde; değerlendirme, yargı, analiz, karar verme, plan oluşturma ve eyleme geçme (Güler ve Çobanoğlu, 1997:31) faaliyetlerinin yer aldığı görülmektedir.

Sonuç olarak; risk iletişiminin bugün geldiği nokta ve erişebileceği ideali konusunda, risk iletişimi stratejilerinin oluşturmaya çalıştığı ‘risk

kültürü', önemli bir noktayı işaret etmektedir. Bu çerçevede; iletişim bilimlerinde yapılacak çok yönlü uzman çalışmalarının, profesyoneller tarafından üretilecek olan mesajlar vasıtasıyla ilgili kesimlere etkili bir şekilde ulaştırılması ve bunlardan da geri bildirimlerin sağlanması sayesinde etkileşim durumunun yaratılması, önem taşıyan bir husus (Yakut, 2008:58-59) olarak değerlendirilebilmektedir. Tüm bunlar da aslında, risk iletişimi olarak ifade edilen çalışmaların genel çerçevesini çizmektedir.

## **Nesnelerin İnterneti ve Kullanım Olanakları**

Günümüz dünyasının yarattığı koşullar, hem toplumsal hem de bireysel manada çeşitli belirsizlikleri gündeme getirmektedir. Bu belirsizliklerin tezahürü ise 'yeni riskler' olarak karşımıza çıkmaktadır. Ancak teknolojik gelişmelerle beraber, söz konusu riskler konusunda çeşitli çözüm yolları ortaya çıkmakta ve bunlar da, elektronik cihazlar vasıtasıyla, gündelik hayat içerisinde kullanılmaya başlanmaktadır. Örneğin; gündelik ev yaşantısındaki tehlikelerin önlenmesi, sağlık konusunda güncel takibin yapılabilmesi, ulaşım araçlarının kaza yapma olasılığının düşürülmesi, toprakta yapılan üretimlerde riskli kimyasalların fark edilebilmesi gibi pek çok farklı bileşen, söz konusu elektronik cihazların yeni kullanım biçimleri aracılığıyla gündelik hayatın bir parçası haline gelebilmektedir. Öte yandan tüm bu durumlar, riskin algılanış biçimlerini de değiştirmekte ve toplumsal anlamda teknolojiyi kabul derecesi arttıkça, risklere karşı rasyonel refleksler de geliştirilebilmektedir (Güler vd., 2011:24). Bu da aslında, teknolojinin hangi amaçlarla kullanıldığıyla ilişkili bir durumu ortaya koymaktadır.

Nesnelerin interneti olarak adlandırılan kavram da, bütünleşik ve küreselleşmiş bir ağ üzerinde her şeyi (elektronik cihaz), herkesle birbirine bağlamapotansiyelinesahip;insan,makine,doğalkaynak,üretimhattı,lojistik ağ, tüketim alışkanlıkları, geri dönüşüm mekanizmaları gibi çeşitli unsurları kapsayan bir bağlantı yapısını işaret etmektedir. Bu yapının önemi; gündelik hayatın her noktasının, sensörler ve yazılımlar vasıtasıyla etkileşime geçmesi, bu sayede de nesnelerin minimum düzeyde insan etkisiyle, kendi aralarında etkileşime geçmesi olarak gösterilebilmektedir (Rifkin, 2015:20). Bu açıdan, temel olarak, 4H olarak adlandırılabilen ve "her yerden, herkesle, her zaman, her nesne ile bağlantı" anlamına gelen bir süreç, nesnelerin internetinin temel hareket prensibini oluşturmaktadır (Kutup, 2011). Buradan hareketle

nesnelerin interneti hakkında, temel hatlarıyla; “her alandaki ürün ve hizmetlerin ağ üzerinden haberleşmesi ve akıllı hale getirilebilmesi” (Şeker, 2014:9) şeklinde bir tanımlama yapılabilmektedir. Nesnelerin interneti, yeniliği ve her geçen gün gelişen yapısı nedeniyle, tanımlama konusunda çeşitli zorluklara sahip bir alan olarak ele alınabilmektedir. Bu açıdan aktarılan örnekler ise daha çok, ‘inovatif’ ürünler ve firmaların yeni pazar hamleleri üzerinden verilmektedir. Ancak yine de son yıllarda karşılaşılan ürünler ve bu kapsamda gerçekleştirilen çalışmaların ortak noktasının, olası riskleri engelleme ve bu alanda bireylerin teknolojik kullanım farkındalığının arttırılması yönünde olduğu görülmektedir.

Nesnelerin interneti olarak adlandırılan ağ bağlantılı cihazların kullanımını internet araç ve teknolojilerinde yaşanan değişimler ve bunları kullanan kitlelerin deneyim ile ihtiyaçları doğrultusunda her geçen gün artış göstermektedir. Tarihsel açıdan bakıldığında, nesnelerin interneti olgusunun kilometre taşlarını; elektromanyetik telgraftan, Turing Makinesi’ne; ARPANET Projesi’nden, MIT’nin *inTouch* çalışmasına dek uzanan bir süreçteki çeşitli çalışma ve icatlar oluşturmaktadır. Söz konusu kavramın ilk defa kullanımı ise, Auto-ID Center’ın yürütücü müdürü Kevin Ashton’ın 1999 yılındaki sunumunda görülmektedir (Postcapes, 2018). Bu dönemde gelişen internet teknolojileri ve elektronik cihazlar sayesinde nesnelerinin internetinin, endüstriyel alanlarda kullanıcıya sunulmaya başlandığı ifade edilebilmektedir. 1992 yılında Carnegie Mellon Üniversitesi’nde soğuk içecek dolabının içerisindeki ürünlerin sıcaklık derecesinin anlaşılabilmesi adına ağa bağlanması neticesinde ilk örnekleri görülen *IoT* cihazları (Teicher, 2018), 2000’li yıllara gelindiğinde *LG* tarafından satışa sunulan *Internet Digital DIOS* adlı buzdolabı ile ticari alanda da karşılık bulmaya başlamıştır (Parry, 2015). Günümüzde gelinen noktaya bakıldığında ise, gelişen teknolojiler ile küresel ölçekte yaygınlaşan ve de ‘hız’ kazanan kablosuz internet bağlantıları neticesinde nesnelerin internetine dair çok daha gelişkin bir tablo çizilebilmektedir. Bu durum aynı zamanda söz konusu alanda yakın geleceği tahlil etmenin zorluğunu da beraberinde getirmektedir. Bu çerçevede bakıldığında; 2018 yılında yapılan çalışmalarda günümüzde 14.2 milyar *IoT* cihazının kullanılacağı ve bu sayının 2021 yılında 25 milyara ulaşacağı öngörülmekteydi (Gartner, 2018). Ancak günümüz perspektifinden incelendiğinde, Şubat 2019 itibariyle 25.9 milyar cihazın aktif olduğu ve her bir saniyede 127 yeni cihazın da internet ağına dahil olduğu görülmektedir.

Buradan hareketle nesnelerin interneti alanında gerçekleştirilen analizler incelendiğinde; 2020'ye kadar küresel pazarın 457 milyar dolara yükseleceği, bu alandaki yatırımların %40'nın sağlık sektöründe olacağı ve 2025 yılına gelindiğinde, dünya genelinde 75 milyar IoT cihazının aktif olarak kullanılacağı (Bera, 2019) söylenebilmektedir.

Günümüzde nesnelerin internetinin kullanım alanlarına bakıldığında; taşımacılık, depolama, sağlık, güvenlik, ekoloji, biyolojik çeşitlilik gibi pek çok farklı düzlemde söz konusu teknolojinin risk iletişimi açısından faaliyet göstermekte olduğu görülebilmektedir. Bu doğrultuda çeşitli örnekler incelendiğinde, öncelikli olarak, söz konusu alanı 'yeni bir endüstriyel çağ' olarak gören ve bunu da özellikle önümüzdeki 10 yıllık süreçte tüm dünyaya hâkim olacak bir egemen gücün varlığıyla özdeşleştiren Jeremy Rifkin'in (2015) ele aldığı çeşitli somut çalışmalar aktarılabilmektedir. İlk olarak sınai ve ticari sektörler düşünüldüğünde taşımacılık alanında faaliyet gösteren firmalar için verilen örnek dikkat çekici bir nitelik sergilemektedir:

“Şirketler, mal ve hizmetlerin akışını izlemek için ticari koridorları boyunca sensörler yerleştiriyor. Sözelimi UPS, Büyük Veriyi kullanarak ABD'deki 60 bin aracını anlık olarak takip ediyor. Lojistik devi, araçların farklı parçalarına sensörler yerleştiriyor. Böylece, arıza yapmaya aday parçalar, yolda daha ciddi bir sıkıntıya yol açmadan değiştirilebiliyor (Rifkin, 2015:20).”

Burada görüldüğü üzere, olası kaza-arıza riskleri minimum seviyeye düşürülmeye çalışılmakta ve genel anlamda da, diğer tehlikeleri bertaraf etme gayreti sergilenmektedir. Bu duruma benzer bir şekilde aşağıdaki örnek de, sensörlerin risk durumu konusundaki kullanım biçimleri hakkındaki önemli fikirler vermektedir:

“Sensörler, mevcut ham kaynakların ulaşılabilirliğini izleyip kaydederek durum bilgisi verirken ön ofise de depolardaki stokların durumunu aktarıyor. Sensörler, üretim hatlarında bir problem varsa o problemi de bulup gideriyor. Başka sensörler de evlerde ve şirketlerde cihazların elektrik kullanımındaki değişiklikleri ve dağıtım şebekesindeki elektriğin fiyatına olan etkisini anlık olarak izliyor (Rifkin, 2015:20).”

Nesnelerin internetine kaynaklık eden sensörlerin kullanımında, büyük

şirketlerin kâr hedeflerinden hane halkının gündelik yaşantı biçimlerine dek uzanan ve merkezine riskleri olabildiğince giderme anlayışı oturtan bir yapıyla karşılaşmaktadır. Bu yapılar her ne kadar insan etkisini de bir hayli azaltıyor görünse de aslında aynı zamanda, bireylerin risk algılarının gelişmesi ve her türden olasılığın göz önünde bulundurulabilmesi açısından önemli bir hareket alanı oluşturmaktadır.

Nesnelerin internetinin gündelik yaşama doğrudan etkileri ve önemli riskler konusunda farkındalık yaratma ve bunları engelleme potansiyeli ise, 'akıllı şehirler' kurulması yönündeki teknolojik gelişmeler aracılığıyla karşılık bulmaktadır. Bu kapsamda yine sensörler aracılığıyla sağlanan etkileşimli ortamlar ve kendi başlarına çalışabilen elektronik cihazlar üzerinden inşa edilen sistemler bina, yol, köprü ve diğer altyapı bileşenleri üzerinde faaliyet göstermektedir. Örneğin; bina yapılarının içerisinde meydana gelen düşük frekanslı titreşimler sensörler sayesinde saptanmakta ve bunlar da tehdit boyutlarına göre ilgili birimlere aktarılmaktadır. Bu sayede bina onarımlarının ne zaman ve ne şekilde yapılması gerektiği hesaplanmaktadır. Yine benzer biçimde; mahalleler arası gürültü kirliliğinin azaltılması, caddelerdeki trafik yoğunluğunun izlenmesi ve kaldırımlar üzerindeki yaya akışını engelleyecek unsurların saptanması gibi faaliyetler de, akıllı nesnelere ile gerçekleştirilebilen çalışmaların yalnızca bir kısmını oluşturmaktadır. Öte yandan akıllı şehirler sistemleri, gündelik yaşantı pratiklerinin olduğu kadar, şirketlerin maksimum kâr anlayışlarının bir parçası olarak da kullanılmaktadır. Örneğin; akıllı karayolları vasıtasıyla sürücüler, kazalar ile trafik sıkışıklıkları hakkında bilgilendirilmektedir. Bu durumun şirketler açısından önemi ise; özellikle sigorta firmalarının, taşıtların hangi gün nerede olduğu, nereye gittiği, belli zaman aralığında kaç kilometre yol yaptığını takip etmesi ve bu sayede de risk analizinin gerçekleştirilerek; poliçe fiyatlarını belirlemesi yönünde oluşmaktadır (Rifkin, 2015:21).

Sensörlerin kent yaşantısı içerisindeki kullanımları ve bunların da olası risk durumlarıyla olan ilişkileri bakımından bir hayli çeşitli faaliyet alanı ile karşılaşmaktadır. Özellikle olası çevre felaketlerinin önlenmesi ve kitlelerin bu durumlardan korunması yönündeki faaliyetler, yine nesnelere interneti alanının etkili olduğu kısımların içerisinde yer almaktadır. Bu konuda kentler ile kırsal alanlarda yerleştirilen sensörlerin toprak, su ve hava kaynaklarındaki

toksik etmenlerin ölçümünü yaptığı görülmektedir. Buradan elde edilen veriler uzmanların analizinden geçmekte ve kitle iletişim araçları vasıtasıyla ilgili topluluklar bilgilendirilmektedir. Bu çerçevede Pekin’de hava kirliliğine yönelik alınan önlemler ve bu doğrultuda elde edilen verilerin toplumla paylaşılmasına dair aktarılan örnek bir olay da, risk iletişim süreçlerine dair fikir verebilmektedir:

“2013 yılında Pekin’deki ABD Büyükelçiliği çatısına yerleştirile sensörler, başkentteki karbon salımı konusunda saatlik raporlar aktardılar. Bu veriler, anlık olarak internette yayınlandı ve halk, tehlike yaratan kirliliğe karşı uyarıldı. Sensörlerin verdiği bilgiler, Çin hükümetini, civardaki termik santrallerden kaynaklanan karbon salımın azaltılması yönünde ciddi tedbirler almaya sevk etti. Hatta otomobil trafiğinde ve enerjiyi yoğun kullanan fabrikalardaki üretimde bile kısıtlamaya gidildi (Rifkin, 2015:21).”

Nesnelerin internetinin, doğal afetlerin yaratabileceği tahribatların en aza indirgenebilmesi ve ilgili kitlelerin bilinçlendirilebilmesi gibi faaliyetler açısından da imkânlar taşıdığı ifade edilebilmektedir.

Nesnelerin internetinin gösterdiği olanaklar yalnızca doğrudan insan yaşantılarını değil, aynı zamanda ekosistem üzerinde gerçekleştirilen çalışmalara da katkı sağlayabilmektedir. Bu açıdan yabani hayvanların bedenlerine ‘implant’ şeklinde yerleştirilen sensörlerin, göç yolları üzerindeki çevresel ve davranışsal değişikliklerin ortaya çıkartılması ve bu doğrultuda da ekolojik belirleyicilerin olası risklerle karşılaşma ihtimalinin ortadan kaldırılmasına katkıda bulunmaktadır. Yine bu çerçevede, temiz su kaynaklarında yaşanabilecek kirlenmeler ile olası sızıntılar, kuraklıklar ve aşırı kullanımlar da nesnelerin internetinin konusu olabilmektedir. Öte yandan, bu durumlara benzer bir şekilde, gıda üretim ve sevkiyatında da söz konusu teknolojilerin kullanımı gerçekleşmektedir. Bu açıdan çiftçilerin; hava durumu, toprak nem oranı, polen dağılımı ve genel olarak verimi etkileyecek her türlü etmenin sensörlerle izleyebilmesi sağlanmakta ve bu sayede ideal yetiştirme koşullarının oluşturulmasına zemin hazırlanmaktadır. Bu koşullar otomatik bir şekilde kontrol edilmekte ve yine otomasyon sistemleri sayesinde mevcut risk durumlarına müdahale edilmektedir. Dağıtım süreçlerinde de yine nesnelerin internetinden yararlanılmakta ve sebze-

meyve taşınan kolilere takılan sensörler aracılığıyla, ürünlerin bozulma süreci hakkında bilgi alınabilmektedir (Rifkin, 2015:21-22). Bu sayede de bir ürünün toprakta yetişmesinden, sevkiyatına; satış aşamasından, tüketimine dek geçen süreçlerin tamamı, olası risklere karşı güvence altına alınmaya çalışılmakta ve insan sağlığının korunmasına yönelik çaba sarf edilmesine olanak tanınmaktadır. Tüm bu süreçler de entegre teknolojiler sayesinde bireylerin üretim-dağıtım ve satın alım aşamalarında karşılaşılabilecekleri riskler açısından bilgi sahibi olabilmelerine imkân sunmaktadır.

İnsan sağlığının karşılaşılabileceği riskler konusunda da farklı teknolojik gelişmeler aracılığıyla koruyucu önlemler alınmakta ve ani değişim durumunda doğrudan müdahale mekanizmaları işlerlik kazanmaktadır. Bu açıdan gerçekleştirilen faaliyetlerin genel çerçevesinde yine internet ağına entegre sensörler bulunmaktadır. Bu doğrultuda insan vücuduna yerleştirilen çipler kalp atışı, vücut sıcaklığı, cilt rengi gibi bilgileri takip etmekte, normal seyrin dışına çıkan bir durumda doğrudan ilgili doktorlara haber vererek önleyici tedbirler alınmasını sağlayabilmektedir (Rifkin, 2015:22). Benzer teknolojik cihazlar bireysel kullanıma da sunulmakta ve cep telefonu uygulamaları vasıtasıyla bireylerin biyolojik riskleri konusunda takipte bulunmaları ve ilgili veriler doğrultusunda uzmanlarla iletişim kurabilmelerine olanak tanınmaktadır. Bu çerçevede bakıldığında, sağlık konusundaki gelişmeler dikkat çekici bir boyutta çeşitlenmekte ve akıllı cep telefonu nabız uygulamalarından, kan şekeri ölçüm sensörlerine; kalp krizi müdahalelerinden, idrar testlerine dek uzanan geniş çerçevede kullanım olanakları gündeme gelmektedir. Bu olanaklar ise gündelik hayatın içerisine entegre edilmiş ve yine çipler, sensörler ile çeşitli kablosuz bağlantı araçlarıyla geliştirilmiştir (Steele ve Clarke, 2013). Bu bağlantı araçları, kendi aralarında kurdukları etkileşim ile bir anlamda yeni bir ekosistem oluşturmakta ve bu alan, her geçen gün katılım ile genişleme yönünden büyümektedir (Al-Dulaimi ve Cosmas, 2016).

Nesnelerin interneti konusunda özellikle gündelik yaşam pratikleri içerisinde yoğun bir şekilde kullanıldığı ve bu alanlardaki ürünlerin pazar açısından öne çıktığı bir diğer mecra ise, 'güvenlik sistemleri' olarak değerlendirilmektedir. Zira bu çerçevede, nesnelerin interneti alanının hem üretim hem de satış anlamında ilk sırada yer alan bu sektör; evler, iş yerleri, fabrikalar, mağazalar ve kamusal alanlarda, kameralar ile sensörlerin dahil



oldukları ağı kapsamaktadır. Sistemlerin en önemli çıktılarını ise, tehlike/ risk ve olay anında doğrudan kolluk güçlerini alarma geçirmesi ve hatta şüpheli görülen unsurları yaratan kişilerin etkisizleştirilmesine kadar varan bir veri kümesi oluşturmaktadır (Rifkin, 2015:22).

Tüm bu durumlar düşünüldüğünde, nesnelerin interneti meselesinin aynı zamanda 'yeni bir küresel değişimin' merkezinde konumlandığı görülmektedir. Bu durum literatürde de kullanılmaya başlanan Endüstri 4.0 kavramı ile ele alınmaktadır. Bu kavrama göre, nesnelerin interneti ile gündelik yaşamda insanın karşılaştığı zorluklar minimuma indirilecek ve dahası; küresel anlamda üretim-tüketim süreçleri baştan aşağıya değişime uğrayacaktır (Arslan, 2016). Bu durum aslında, hem teknoloji ve internetin küresel ölçekte etkin bir konumda yer almasının hem de ekonomik belirleyicilerin, tüm bu koşulları kendi egemen çıkarları doğrultusunda her geçen gün yeniden şekillendirmesinin bir sonucu olarak düşünülebilmektedir. Zira önceki dönemlere bakıldığında; 1960'lı yıllarda geliştirilen ağların, 1980'li yıllardaki neo-liberal dönüşümler ile işlerlik kazandığı ve dolayısıyla 90'lı yıllardan itibaren de küresel ölçekte işleyen kapitalizmin, bugünlerin global dünyasında egemen konumda bulunduğu görülmektedir. Bu açıdan Endüstri 4.0 kavramının, nesnelerin interneti üzerinden anlam kazanmasının, farklı iş kollarının ortadan kalkması ile fiziksel güç gerektiren sektörlerde çeşitli işten çıkarmaların yaşanması gibi küresel ölçekte yeni durumların ortaya çıkmasına yol açabileceği söylenebilmektedir. Bu açıdan Rifkin'in (2015:135) Amerikan Savunma Sanayisi ile ilgili aktardığı otomasyon süreçleri de, farklı iş kollarında yaşanması muhtemel değişimler konusunda fikir vermektedir:

“Ve şimdilerde Amerikan Savunma Bakanlığı İleri Düzey Araştırma Projeleri Ajansı (DARPA) ilgisini dikiş sürecine yoğunlaştırmış bulunuyor. İnternetin de mucidi olan DARPA, tekstil sektörünün otomasyona geçirilmesi en zor bölümü olarak düşünülen dikiş sürecini otomasyona geçirerek, yılda 4 milyar doları askeri kıyafetlere harcayan Savunma Bakanlığının üniforma üretiminde kullanılan işgücü maliyetlerini sıfıra çekmeyi hedefliyor. (...) Başarılı olurlarsa yeni otomasyon sistemi sayesinde üniforma üretiminde taşeronlarca çalıştırılan 50 bin kişinin işine son verilecek ve sıfıra yakın marjinal işgücü maliyeti seviyesine ulaşılmış olacak.”

Günümüzde pek çok farklı endüstriyel üretim ve satış sektörlerinde de, Endüstri 4.0 kapsamındaki faaliyetleri doğrultusunda, insan kullanımının azaltıldığı görülmektedir. Bu doğrultuda teknoloji ürünlerinin küresel ölçekteki üretim merkezi olan Uzak Doğu'dan da çeşitli örnekler verilebilmektedir. Otomotiv ürünlerinin ve *iPhone* cihazların üretimini gerçekleştiren fabrikalar, internet ağıyla birbirine bağlı çeşitli otomasyon sistemlerini kullanımları konusunda dikkate değer sonuçlara ulaşmaktadır. Örneğin Çin'in Dongguan şehrinde son 5 yılda üretim işgücünde yer alan 280.000 kişinin yerine 91.000 robot çalışmaya başlamıştır. Benzer biçimde, dünya genelindeki *iPhone* üretiminin yarısını gerçekleştiren Tayvan firması *Foxconn*, 2020 yılına kadar üretimlerinin %30'unu otomatik hale getirmeyi planlamaktadır (Zhou, 2019).

Nesnelerin internetinin, pek çok farklı açıdan risklere dair öngördüğü ve ortaya koyduğu faaliyet alanı, yeni olanakların ortaya çıkması ve risk kültürünün farklı bağlamlarda üretilmesi çerçevesinde 'heyecan verici' gelişmeleri işaret edebilmektedir. Ancak bu durum da beraberinde yeni belirsizlikleri getirmekte ve dahası, bu belirsizliklerin doğrudan doğruya risk durumları ile paralellik göstermesi söz konusu olabilmektedir. Bu açıdan riski engelleme yolunda atılan adımların yeni risklerin üretimine yol açıp açmayacağı sorunsalı da, ele alınması gereken bir başka konu olarak karşımıza çıkmaktadır.

### Yeni Teknolojilerin Yeni Riskleri

Nesnelerin interneti, temel perspektif olarak, günümüz gündelik yaşantı biçimlerinden; küresel açıdan egemen olan şirketlerin kâr marjlarını koruma reflekslerine dek uzanan geniş bir çerçevede risk olgusunun karşısında şekillenmektedir. Bu durum da beraberinde teknoloji odaklı gelişen ve bu bağlamda çeşitlenen yeni pratikleri, yaşam algılarını ile farklı olasılıkları getirmektedir. Bu 'yenilikler' ise aslında en temelde, nesnelerin internetinin gerçekleşebilmesi için gerekli olan teknolojik altyapılar üzerinden şekillenmektedir. Bu doğrultuda bakıldığında, riskleri engellemeye yönelik faaliyet gösteren bu yapıların; doğası, çalışma prensibi ve kuracağı etkileşimler çerçevesinde yeni riskleri gündeme getirmesi söz konusu olabilmektedir.

İletişim ağları ve teknolojik altyapıların ortaya koyduğu sistemin

küresel ölçekte de etkin olması, aynı zamanda güvenlik, mahremiyet ve ekonomik belirleyiciler yönünden farklı riskler için alan açmaktadır. Bu çerçevede nesnelerin internetinin de, benzer yönlerden çeşitli soruların ortaya çıkması bakımından incelenebileceği görülmektedir. Bu doğrultuda düşünüldüğünde öncelikli olarak, mahremiyet ve kişisel verilerin korunması meselesi gündeme gelmektedir. Bu durum ise beraberinde ekonomik ve politik süreçlerde söz konusu bilgilerin kullanımı hakkında çeşitli soru işaretlerini getirmektedir.

“Buradaki en önemli soru şu: Herkes ve her şey birbirine bağlandığında kişinin mahremiyetinin korunması için sınırlar nasıl belirlenecek? Sorun şu ki Nİ kullanan şirketler, kendi amaçları doğrultusunda sömürenin yeni yollarını aramak için küresel sinir sisteminin her katmanını delebirlirler. Siber hırsızlar, ticari kazanç sağlamak için kimlik bilgilerini çalabilir, sosyal medya siteleri, kârlarını arttırmak için verileri reklam verenlere ve pazarlamacılara satabilir, politik kampanya organizatörleri önemli bilgileri yabancı devletlere aktarabilir (Rifkin, 2015:84).”

Nesnelerin interneti üzerinden etkileşime giren cihazlar, temel olarak, kullanıcı pratikleri ile bilgilerinin de izlerini taşımaktadır. Benzer bir durum olarak ele alınabilecek olan sosyal medya kullanım meselesindeki ‘dijital ayak izi’ ya da ‘çerezler’ olarak adlandırılan unsurlar da, bu kapsamda, nesnelerin internetindeki çok daha somut ve temel pratiklerin arşivlenmesiyle paralellik göstermektedir.

Nesnelerin internetinin yaratabileceği riskler konusuna bakılırken ele alınan teknolojik altyapılar ile internet gibi kablosuz bağlantı yollarının için yapısının handikapları meselesi, bu durumu daha da anlaşılabilir kılmaktadır. Bu açıdan 3 temel riskin, nesnelerin interneti için de geçerli olduğu görülebilmektedir. Bu durumların genel çerçevesi ve olası risklerin kaynakları ile bunlara karşı gerçekleştirilebilecek refleksler van Dijk’ın (2016:305) 3 farklı noktadan tartışmaya açtığı durumlar üzerinden değerlendirilebilmektedir:

“Bu risklerin ilki onların zekâsına fazla güvenerek kişinin kendi yargılama yeteneğinin zayıf kalmasına neden olmaktadır. Sistemler daha akıllı hale gelse de kullanıcıları daha aptallaşabilir. (...) Akıllı

sistemler değişen kullanıcı tercihlerine adapte olabilmektedir. Ancak insanların standartları, değerleri ve duyguları da giderek daha hızlı değişmektedir. (...)

“İkinci bir tehlike ise sürekli bu bilgi araçlarını kullanan kişilerin kendilerini yeni ve şaşırtıcı izlenim ve kontaklardan kopartabileceğidir. (...) Kısıtlı oldukları için güvenli ve kontrol edilebilir olan ortamlara yerleşebiliriz. Prensipite olmasa da genelde pratikte dünyanın veya toplumun geri kalanına kapalı kişisel bir alt kültür yaratabiliriz. (...)”

“Son risk ise güvenli ve kontrol sistemlerine kendi tercih ve özelliklerini emanet eden kullanıcıların özel hayatlarının gizliliğiyle ilgilidir. 21’inci yüzyılda, enformasyon aracınız bağlantılarınıza sizin kim olduğunuz hakkında bilgi verecektir. Kesinlikle otoriteler ve şirketler bunlar bununla çok ilgileneyecektir. Bu yüzden de bu sistemleri ciddiyetle ve seçici bir şekilde ve sistemlerin attığı her adım ve aldığı her önemli karar üzerinde kontrol sahip olacak biçimde kullanmak gerekmektedir.”

Bu açıdan nesnelere internetinin doğası ve gelecekteki konumu hakkındaki temel endişelerin, aslında bu araçların varlık sebepleri ile çelişik bir durumu ortaya koyduğu görülmektedir.

*IoT* cihazlarının daha çok ev yaşantısı içerisinde karşılıklı bulunduğu ve bireysel kullanıcıların bu doğrultuda işlerlik gösteren ‘akıllı teknolojilerden’ yararlandığı söylenebilmektedir. Bu çerçevede de; ev aydınlatmalarının radyo sinyalleri vasıtasıyla uzaktan kontrol edilebilmesi, güvenlik kameralarının internet ya da kablo bağlantıları ile *hacklenerek* izlenebilmesi, *bluetooth* cihazlar vasıtasıyla kilitlerin açılabilmesi, oda sıcaklığının yazılım kodu manipülasyonu ile değiştirilebilmesi, ses alıcı özelliği olan cihazlar üzerinden ortam seslerinin dinlenebilmesi, internet modemlerinin şifrelerinin kırılarak tüm internet trafiğinin kaydedilebilmesi, otomobillerin güvenlik kilitlerinin kaldırılarak sürücünün devre dışı bırakılabilmesi (Brook, 2018) gibi pek çok farklı yeni risk, *IoT* cihazlarının potansiyel yeni risklerini işaret etmektedir. Söz konusu ev teknolojileri içerisinde yer alan cihazların yaratabileceği risklere karşılık, kullanıcı bazında alınabilecek bazı önlemler de bulunabilmektedir. Bu doğrultuda FBI’nın *IoT* cihazlar üzerinden doğan

risklere karşı yayımladığı ‘Tüketicinin Korunması ve Savunması Listesi’nde birtakım öneriler, bu çerçevede etkili olabilmektedir. Bu açıdan; cihazların sıklıkla yeniden başlatılması, düzenli olarak kullanıcı adı ve parolaların yenilenmesi, *IoT* cihazların diğer ağlardan yalıtılması, izinsiz IP girişlerini engellemek için güvenlik duvarlarının güncellenmesi, cihaz üreticilerinin önerilerinin takip edilmesi, kullanılmayan cihazların kapatılması, yeni cihaz alımlarında siber güvenlik alanında uzmanlaşmış firmaların tercih edilmesi, üreticilerin sunduğu güncel yamaların uygulanması, güvenilir sunucuların ve kimlik doğrulama yollarının kullanılması (FBI, 2017) gibi pek çok faaliyet, kullanıcıların olası risklere karşı farkındalık seviyelerini yükseltmeleri doğrultusunda izleyebilecekleri çeşitli yollar olarak değerlendirilebilmektedir.

Ancak asıl vurgulanan risk, ağların izlenebilme ve dışarıdan müdahale edilebilme potansiyellerinden ziyade; insanların algı ve deneyimlerinin, teknolojik belirleyiciler ekseninde şekillenmesi ve de çok daha yeni boyutların gündeme gelmesi olarak düşünülebilmektedir. Teknolojik gelişmelerin yakın gelecekte küresel anlamda gündelik yaşam pratikleri haline gelebilme potansiyeli düşünüldüğünde, nesnelerin internetinin farklı açılardan tartışmaya açılabileceği görülmektedir. Şimdiye kadar aktarılan bu yeni riskler, en temelde, insanlığın yakın geçmişinde de olduğu gibi; kademeli olarak, toplumsalı farklı bir yöne doğru evirmektedir (Şener, 2016:78). Bu değişim paradigması ise, aynı zamanda ‘düzenleme’ mantığının hayatın her alanında işlerlik kazanması anlamına gelmektedir. Düzenleme meselesine dair, nesnelerin internetinin; ‘yaşamı daha iyi hale getirme’, ‘akıllılaştırma’, ‘performansı arttırma’ ve bireyleri ‘mutlu etme’ taahhüdünü verdiği söylenebilmektedir. Bu durum da algısal olarak; korunma, istikrar ve mahremiyet sağlamayı ‘güvence’ altına almaktadır. Ancak tüm bunlar, bir ‘sterilleşme’ halini de oluşturmaktadır. Bu durum da, olumlu ya da olumsuz olarak adlandırılmamakla beraber, ilişkilerin belirleyiciliği konusunu her daim önde tutmaktadır (Şener, 2016:81-82).

Nesnelerin internetinin beraberinde getirdiği risklerin anlaşılması konusunda dikkat edilmesi gereken bir diğer unsur ise; tüm iletişim ağlarının yöndeşmesi, minyatürleşmesi ve de bu aygıtların günlük hayatın en temel parçası haline gelmesi ile her zaman, her yerde çevrimiçi erişim sağlanan geniş bant bağlantıları ile en genel çerçevede de ‘bulut bilişimin’ etkinliği (van Dijk, 2016:91) olarak dikkat çekmektedir. Bu durum aynı zamanda

yakınsama olarak adlandırılan ve farklı cihazların kullanım pratiklerinin birbirine aktarılması olarak gerçekleşen süreçlerin (Jenkins, 2016:19-21) de birer yansıması olarak ele alınabilmektedir. Bu açıdan da nesnelerin interneti, pek çok tehdiye açık konuma gelmekte ve yeni risklerin doğuşuna zemin hazırlamaktadır.

“Akıllı küresel ağ, muhtemelen, gelecekte yalnızca bizi değil, arabalardan giysilere, yiyeceklerden içeceklere yaşamlarımızdaki nesnelerin pek çoğunu bağlantılandırarak. Akıllı çipler ve merkezi veri bankaları aracılığıyla, yalnızca birbirimize değil, aynı zamanda çevremizdeki üretilmiş dünyaya, ortak kullanım alanlarına, etki ve tepki yapılarına da eşsiz bir biçimde bağlanma olanağı elde etmekteyiz (Chatfield, 2013:12).”

Giderek genişleyen ‘akıllı küresel ağ’ olgusu yeni risklerin, hangi bağlantılar aracılığıyla gündelik yaşama sirayet edebileceğini ve dahası söz konusu risklerin, geri dönüşü konusunda ulaşabileceği boyutları göstermektedir.

Nesnelerin internetinin taşıdığı yeni risk olguları, farklı perspektiflerden, örneklerinin çoğaltılabilme ve bunların da farklı bakış açılarından değerlendirilebilme imkanını işaret etmektedir. Ancak doğrudan kullanım pratikleri üzerinden farklı örneklerle değerlendirmelerde bulunmak yerine, araçların ve işleyiş yapılarının temel doğası ile dinamikleri üzerine genel bir çerçeve oluşturmak daha sağlıklı tartışmalar yürütülebilmesine olanak tanımaktadır. Bu doğrultuda risk iletişimi açısından nesnelerin internetinin risklerin öngörülmesi, buna uygun stratejilerin ve çözüm yollarının belirlenmesi, sorunun giderilmesi gibi farklı açılardan katkı sağlayabileceği düşünülmektedir. Ancak söz konusu iletişim olduğunda bu durumun kullanıcı farkındalığı, katılımcılığı, süreçlerin şeffaflığı ve bağımsızlığı gibi olguların farklı koşullarda kısıtlı kaldığı söylenebilmektedir. Bu çerçevede de risk iletişimini, nesnelerin interneti üzerinden farklı bir perspektiften inşa etmek ve bunu küresel ölçekte bağımsız üretim, uygulama ve denetim mekanizmalarının kitlelerce katılımcı bir şekilde gerçekleştirilerek hem nesnelerin internetinin risk iletişimi süreçlerine adaptasyonu hem de söz konusu teknolojilerin risk iletişimi stratejileri doğrultusunda incelenmesi vasıtasıyla yeni bir bakış açısının ortaya konması gerekliliği ön plana çıkmaktadır.

Son olarak, yeniden risk meselesine bu bağlamda dönülecek olunursa, maddeler ekseninde ele alınabileceği görülmektedir. Bu durum risk iletişiminin önemini yeniden gündeme getirerek canlı tutmakta ve dolayısıyla, nesnelerin internetinin de bu kapsamda düşünülmesinin gerekliliği, bir kez daha ortaya çıkmaktadır.

## **SONUÇ**

İçerisinde bulunduğumuz dünyanın koşulları, bir devinimim içerisinde, durmaksızın değişmekte ve farklılaşmaktadır. Bu durum sosyal, ekonomik ve kültürel bağlar açısından etkili olmaktadır. Özellikle teknolojinin kullanım alanının, zaman ve mekânın ötesine taşınarak küresel ölçekte işlerlik kazanması da beraberinde pek çok sorunu gündeme getirmektedir. Bu noktada ise her türden farklı toplumsal, ekonomik, politik ve çevresel bileşeni derinden etkileyen sorunsalların asıl olarak, 'belirsizlik' olgusunu ortaya çıkarttığı ifade edilebilmektedir. Bu açıdan söz konusu belirsizliklerin de risk kavramı üzerinden ele alınarak, bunlara uygun olarak, gerekli stratejilerin planlanması ve uygulanması aracılığıyla giderilmesinin gerekliliği dikkat çekmektedir.

Günümüz toplumsal ve ekonomik hayatının işleyiş yapıları, teknolojik belirleyicilikler içerisinde işlerlik kazanmakta ve bu çerçevede de toplumsal yaşam dinamiklerini yeniden düzenlemektedir. Özellikle küresel çaptaki ağların, gündelik yaşam pratiklerinin temel noktalarına sirayet etmesi ve bunu da teknoloji vasıtasıyla etkili kılması meselesi de, yeni belirsizleri ve de dolayısıyla yeni riskleri ortaya çıkartmaktadır. Bu doğrultuda düşünüldüğünde, özellikle nesnelerin interneti olarak adlandırılan yapılar ile işleyişlerin, hem risk iletişimi kapsamında ele alınması hem de beraberinde getirdiği yeni risk potansiyelleri çerçevesinde değerlendirilmesi, üzerinde önemle durulması gereken bir konu olarak dikkate alınabilmektedir.

Temel olarak gündelik yaşam pratikleri ve küresel çaptaki üretim-tüketim süreçlerindeki riskleri ortadan kaldırmaya yönelik geliştirilen nesnelerin interneti konusu, merkezinde teknolojik değişimleri barındırmaktadır. Bu değişimler de ev yaşantısı içerisindeki akıllı buzdolaplarından, vücuda yerleştirilen çiplere; topraktaki verimi arttıran sensörlerden, otomasyon üretim sistemlerine dek uzanan geniş bir tablo içerisinde gerçekleşmektedir. Tüm bunlar da birbirine her zaman, her yerden, her nesne ve her bağlantı aracılığıyla kurulan etkileşimler ile sağlanmakta ve asıl olarak kesintisiz

bir iletişim ortamını, insan faktörünü minimum düzeyde tutarak devam etmektedir. Bugünün koşullarında bu durum henüz gerçekleşmemiş olsa da, yakın döneme yönelik teknolojik atılım ve uygulama alanları göz önünde bulundurulduğunda, birkaç yıl içerisinde insan-nesne etkileşiminin daha çok nesne-nesne biçiminde olacağı öngörülebilmektedir.

Temel hareket alanı olarak risklerin bertaraf edilmesini amaçlayan nesnelere interneti, beraberinde yeni riskleri de ortaya çıkartabilmektedir. Bu açıdan dijital tabanlı işleyiş yapısından hareketle bireylerin gündelik yaşantıları ile kişisel verilerinin güvenlik tehdidiyle karşılaşması, otomasyon sistemleri ile iş gücünün insanlardan alınarak nesnelere devredilmesi, teknoloji üretim süreçlerinin de beraberinde getirebileceği ekonomik ve toplumsal sorunlar gibi çeşitli konular, nesnelere internetinin ortaya koymakta olduğu yeni risklerin genel çerçevesini çizmektedir. Bu durum da aslında teknolojinin ve temel küresel iletişim ağ paradigmasının doğası ile işleyişindeki yapısal açmazlarına tekabül etmektedir. Zira elektronik sistemler ve ağ iletişimi mantığına sahip olan söz konusu bu yapılar dışarıdan gelebilecek saldırıların engellenebilmesindeki yetersizlikleri ve maddi kazanım odaklı üretim biçimlerinden ötürü, çeşitli handikaplara sebep olabilmektedir. Zaman içerisinde karşılaşılacak örneklerin dikkate alınmasının yanı sıra teknolojinin içkin yapısı ve işleyişinden doğabilecek risklerin öngörülebilmeye çalışılması da, nesnelere internetinin kullanımı konusunda fikir verebilmektedir.

Sonuç olarak nesnelere interneti konusu daha çok ürün bazlı değişimlere ve gündelik yaşam pratiklerini kolaylaştırma ile şirketlerin kâr maksimizasyonunu sağlama gibi 'risk önleyici' unsurları üzerine odaklanmaktadır. Ancak işaret edildiği gibi söz konusu yapıların 'sunduğu' riskleri engelleme ve bu konudaki algıları biçimlendirme faaliyetleri, insan etkisinin azalmasına paralel olarak, daha önce karşılaşılmamış farklı türden risklerin doğuşuna ve buna bağlı olarak da öngörülmesi giderek zorlaşan 'belirsizlikler dizgesine' yol açabilmektedir. Bu çerçevede risk iletişimi olarak adlandırılan süreçlerin hedeflediği 'risk kültürü oluşturma' ve 'önleme' aşamalarının, kullanıcı bireylerin hızlı adaptasyon sağlayabilmesi, uygun kullanım becerisine sahip olabilmesi ve tüm bunlara uygun biliş seviyesine ulaşması ile mümkün olabileceği düşünülmektedir. Bu doğrultuda ayrıca; olası risklerin geniş kitlelerce tartışılması, güvenli yazılım ve cihazların



kullanıcı odaklı üretilmesi ile tüm bunları insani koşulların iyileştirilmesi adına bilimsel, toplumsal ve hukuki koşulları sağlayabilecek katılımcı ve şeffaf yönetsel/idari yapıların oluşturulması da, söz konusu risk iletişiminin sağlıklı bir şekilde hayata geçirilebilmesine olanak tanıyabilecektir. Aksi durumda ise risk iletişiminin asıl hedefi olan paydaşların katılımcılığı ve risk kültürünün oluşumu meselesi nesnelere arasındaki ilişkiye devredilerek; insan faktörü ikinci plana itilebilecektir. Bu durum da aslında; nesnelerin interneti ve risk iletişimi arasındaki süreçlerin çok daha uzun vadede değerlendirilmesini ve bu yönde de yeni paradigmalara oluşturulmasını gerekli kılmaktadır.

## **KAYNAKÇA**

AFAD. (2014). *Açıklamalı afet yönetimi terimleri sözlüğü*. Ankara: T.C. Başbakanlık.

Akbal, A. (2007). Hayatımızdaki riskler. A. Kasapoğlu (Der.) içinde, Yeni toplumsal travmalar (ss. 70-91). Ankara: Referans Yayınları.

Al-Dulaimi, J., ve Cosmas, J. (2016). Smart safety & Health care in cities. *Procedia Computer Science*, 98, 259-266.

Arslan, E. (2016). Endüstri 4.0 yolunda: Nesnelere interneti. 28 Mayıs 2019,

<http://www.endustri40.com/endustri-4-0-yolunda-nesnelere-interneti/>.

Bera, A. (2019, 25 Şubat). 80 IoT statistics (infographic). 25 Mayıs 2019, <https://safeatlast.co/blog/iot-statistics/>.

Beck, U. (2014). *Risk toplumu: Başka bir modernliğe doğru* (B. Doğan ve K. Özdoğan, Çev.). İstanbul: İthaki Yayınları.

Brook, C. (3 Ekim 2018). Smart devices: How to secure your connected family. *Digital Guardian*. 28 Haziran 2019, <https://digitalguardian.com/blog/smart-devices-how-secure-your-connected-family>.

Chatfield, T. (2013). *Dijital çağa nasıl uyum sağlarız* (L. Konca, Çev.). İstanbul: Sel Yayıncılık.

FBI. (2017, 17 Ekim). Common internet of things devices may expose consumers to cyber exploitation. 25 Mayıs 2019, <https://www.ic3.gov/media/2017/171017-1.aspx>.

Gartner. (2018, 7 Kasım). Gartner identifies top 10 strategic IoT technologies and trends. 28 Haziran 2019, <https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends>.

Giddens, A. (1994). *Modernliğin sonuçları* (E. Kuşdil, çev.). İstanbul: Ayrıntı Yayınları.

Güler, Ç., ve Çobanoğlu, Z. (1997). *Risk İletişimi ve risk yönetimi*. Ankara: T. C. Sağlık Bakanlığı Çevre Sağlığı Temel Kaynaklar Dizisi.

Güler, Ç., Çobanoğlu, Z., Vaizoğlu, S. A., ve Tekbaş, Ö. F. (2011). *Risk yönetimi ve iletişimi*. Ankara: Yazıt Yayınları.

İTÜ. (2005). *Zarar azaltma ilkeleri el kitabı* (S. Sözen, Haz., Okay N., Sözen S., Ünal Y. S., Çev.). İstanbul: İTÜ Yayınları.

Jenkins, H. (2016). *Cesur yeni medya: Teknolojiler ve hayran kültürü* (N. Yeğengil, Çev.). İstanbul: İletişim Yayınları.

Kabasakal, H. (2008). Afet yönetimine genel bakış ve Türkiye. G. O. Fişek ve H. Kabasakal (Haz.) içinde, *Afet ve İnsan: 1999 Marmara Depreminin Yansımaları*. (9-17). İstanbul: Boğaziçi Üniversitesi.

Kadıoğlu, M. (2011). *Afet yönetimi: Beklenilmeyeni beklemek kötüsünü yönetmek*. 65. İstanbul: Marmara Belediyeler Birliği.

Kasapoğlu, A. (2007). Giriş. A. Kasapoğlu (Der.) içinde, *Yeni toplumsal travmalar* (1-69). Ankara: Referans Yayınları.

Kul, M. (2007). Kapkaç mağdurları. A. Kasapoğlu (Der.) içinde, *Yeni toplumsal travmalar* (123-154). Ankara: Referans Yayınları.

Kutup, N. (2011). Nesnelerin interneti; 4h her yerden, herkesle, her zaman, her nesne ile bağlantı. 16. Türkiye'de İnternet Konferansı inet-tr'11. 30 Kasım-02 Aralık 2011. 15 Mayıs 2019, <http://www.iot.gen.tr/2016/02/13/nesnelerin-interneti-4h-her-yerden-herkesle-her-zaman-her-nesne-ile-baglanti/>.

Parry, T. (2015, 9 Haziran). The internet of things is about experience... and data. *Multichannelmerchant*. 28 Haziran 2019,

<https://multichannelmerchant.com/blog/the-internet-of-things-is-about-experience-and-data/>.

Postscapes. (2018, 20 Ağustos). Internet of things (IoT) history. 28 Haziran 2019,

<https://www.postscapes.com/internet-of-things-history/>.

Rifkin, J. (2015). *Nesnelerin interneti ve işbirliği çağı* (L. Göktem, çev.). İstanbul: Optimist Yayınları.

Steele, R., ve Clarke, A. (2013). The Internet of things and next-generation public health information systems. *Communications and Network*, 5(3), 4-9.

Şeker, S. E. (2014). Ağ etkisi, moore yasası ve dijitalleşmenin yenilik ile ilişkisi (Relation between innovation and network effect, moore law and digitalization). *YBS Ansikopedi*, 1(1), 8-12.

Şener, N. K. (2016). *İletişimin tekno-sosyolojisi*. Kocaeli: Volga Yayıncılık.

Teicher, J. (7 Şubat 2018). The Little-known story of the first IoT device. IBM Industries. 28 Haziran 2019, <https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/>.

van Dijk, J. (2016). *Ağ toplumu* (Ö. Sakin, Çev.). İstanbul: Epsilon Kafka.

Yakut, İ. (2008). *İletişim bilimi perspektifinden risk iletişimi stratejileri*. Kocaeli: Umuttepe Yayınları.

Zhou, C. (2019, 14 Şubat). Man vs machine: China's workforce starting to feel the strain from threat of robotic automation. *South China Morning Post*. 28 Haziran 2019, <https://www.scmp.com/economy/china-economy/article/2185993/man-vs-machine-chinas-workforce-starting-feel-strain-threat>.