Araştırma Makalesi - Gönderim Tarihi: 01.03.2019 - Kabul Tarihi: 10.05.2019

Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza"

Merih TAŞKAYA[12]
Ömür TALAY[3]

Öz

Tarih, insanlığın bilim ve teknoloji alanında atmış olduğu ilk adımları, deyim yerindeyse daha koyu harflerle yazar. Yeniliklerin başlangıç noktası olarak kabul edilen bu ilk adımlar, daha sonraki gelişmelere de dayanak olarak kabul edilir. Yaşadığımız çağdaki teknolojik gelişmeler de ileride gerçekleşecek olan daha büyük gelişmelerin başlangıç noktası olarak öngörülmektedir. Öte yandan, dijital teknolojilerde yaşanan gelişmeler için "henüz yolun başındayız" düşüncesi, pek çok uzman tarafından dile getirilmiştir. Tüm gelişmeler gibi, cesaretlendirici ve korkutucu sonuçları içinde barındıran dijital dünyaya dair gelişmeler, kişisel verilerin güvenliği söz konusu olduğunda genellikle kötümser öngörüleri gündeme getirmektedir. Pazar kurallarının geniş hakimiyeti nedeniyle, dijital gözetime konu olan "kişisel verilerin güvenliği" sorunu, konu üzerine çalışan sosyal bilimcilerin sıklıkla uyarıda bulunduğu bir alan haline gelmiştir. Pazarlama amaçlı geliştirilen yazılımlar, dijital birer göz gibi çalışmakta, kişisel verilerin pazarlama hedefleri temelinde elde edilmesinde aktif rol oynamaktadır. Özellikle çerez kullanımının aracı kılındığı bu tür uygulamalarda kişilerin açık rızasının alınması konusundaki karmaşa, hem çerez kullanımının bir hizmet sunumu için koşul haline getirilmesi noktasında, hem de yine bu kapsamda açık rıza kavramının tanımındaki bulanıklık nedeniyle sorunlu bir alan yaratmaktadır. Bu çalışmada bu sorun, yargı ve denetleme aktörlerinin görüşleri ışığında, alana ilişkin literatür ve yasal mevzuat kapsamında değerlendirilmiştir.

Anahtar Kelimeler: Dijital Gözetim, Veri Gözetimi, Dijital Pazarlama, Çerezler, Açık Rıza

Atıf: Taşkaya, M. ve Talay, Ö. (2019). Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza". Akdeniz Üniversitesi İletişim Fakültesi Dergisi, Haziran (31), s. 356-376

1 Doç. Dr., Akdeniz Üniversitesi İletişim Fakültesi, merihtaskaya@gmail.com, ORCID Numarası: 0000-0002-1907-9340.

2 Sorumlu Yazar / Corresponding Author

3 Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Mezunu, omurtalay@gmail.com, ORCID Numarası: 0000-0002-1633-6655.

Marketing Agents for Digital Surveillance: "Cookies" and "Explicit Consent" in the Use of Cookies

Abstract

History writes the first steps taken by humanity in the field of science and technology, in other words, in bold letters. These first steps, which are accepted as the starting point of the innovations, are accepted as the basis for further developments. Technological developments in the age we live are foreseen as the starting point of further developments. On the other hand, the idea that "we are at the beginning of the road" for developments in digital technologies has been mentioned by many experts. Like all developments, innovations about the digital world, which have both encouraging and frightening results, often pessimistic considerations when it comes to the security of personal data. Due to the wide dominance of the market rules, the issue of the "security of personal data" subject to digital surveillance has become an area where the social scientists working on the subject are frequently warned. The software developed for marketing purposes works as a digital eye and plays an active role in obtaining personal data on the basis of marketing objectives. Especially in cookie applications, there is a conceptual confusion about getting explicit consent of persons. In this study, in the light of the opinions of judicial and supervisory actors, this problem has been evaluated within the scope of the literature and legal regulations.

Keywords: Digital Surveillance, Dataveillance, Digital Marketing, Cookies, Explicit Consent

Giriş

Patrick Somerville'in yönettiği, başrollerini Emma Stone, Jonah Hill ve Justin Theroux'un paylaştığı 2018 Amerikan yapımı "Maniac" adlı dizinin fütüristik göndermeleri, pazarlamanın geleceğine ilişkin distopik bir noktaya işaret ediyor. Reklam izlemenin para kazanma yollarından biri haline geldiği bu evrende, Ad Buddy sistemi işliyor. Bu sistemde ödemenin gerçekleşmesi için, ödenecek meblağa karşılık gelecek reklamı okumak üzere yanınıza gelen bir insanın sunduğu reklamı dinlemek gerekiyor. Parasız kalındığı anlarda reklam izlenerek harcama yapılabilen bu ödeme biçiminin yer aldığı sahneler, geleceğin gerçekliğinin bir parçası olarak sunuluyor. Dizide pek de keyifli olmayan hatta giderek eziyet halini alan bu süreç, özellikle internet kullanıcıları için hali hazırda neredeyse her an yaşanan bir gerçekliğe denk düşmekte. Bu gerçekliği yaratan sürecin ayak izlerini geriye doğru takip ettiğimizde, internette yapılan aramaların, ziyaretlerin, beğenilerin ve benzerleri gibi eylemlerin ardından bırakılan dijital izlerden elde edilen verilere dayanan kişiselleştirilmiş reklamları doğru hedefe ulaştırmakta aktif rol alan çerezlerle karşılaşmaktayız. Çerezlerin kişilere ait izlerin takibini sağlayacak ve bu takip biçimi aracılığı ile elde ettiği en basit kişisel beğenileri bile sistematik verilere dönüştüren yazılımların pazarlama amaçlı kullanımlarının somut göstergeleriyle de sıklıkla karşılaşmaktayız. İnternette arama

motorlarında tarattığınız bir kavram, kısa süre içinde o kavramla ilgili ürünlerin sunulduğu reklam kutucukları olarak karşınıza çıkabilmekte. Pek çok kişiye gözetlendiği hissini yaşatan bu anların kuşkuya yol açan özelliği, karşılarına çıkan reklamların, internet aramalarında ilgilendikleri en son konuyla ilişkili ürünlere yönelik reklamlar oluşudur. Dijital gözetim olarak kavramsallaştırılan bu ve benzeri takip süreçleri, her şeyden önce en basit haliyle kişinin reklam izlememe tercihinin elinden alınması anlamına gelen bir kişisel irade blokasyonudur. Sürecin daha derin katmanlarında, yani çerezler aracılığı ile takibinin sağladığı kişisel verilerin toplanması aşamalarındaki manipülatif eylemlerin yarattığı durumlar da oldukça trajiktir. Kişisel verilerin toplanması çerezlerin kullanımı aracılığı ile yapılmaktadır. Ancak çerez kullanımının açık rızaya dayalı olması gerekirken, çeşitli internet sayfalarının çerez kullanım şartlarının kabul edilmemesi durumunda sayfanın kullanıcıya sunumunun sonlandırılması, hizmetin sunumunu şarta bağlamakta, çerez kullanım şartlarının kabulü ile de kişisel verilerin kullanımının sınırları çoğu zaman bulanık bırakılmaktadır. Her iki durumda da öznenin, iradesine müdahale söz konusudur; bu bir özgürlük sorunudur; dolayısıyla bu durum bir insan hakları mücadelesi konusudur.

Dijital gözetim pek çok akademik çalışmada daha geniş sorunlar etrafında, makro boyutlu bir yaklaşımla ele alınmıştır. Bu çalışmada ise dijital gözetimin pazarlama amaçlı aracıları olarak 'çerezler' sorunun merkezine oturtulmuş ve açık rıza kavramının tanımının esnek çeperlerinin yarattığı belirsizliğin bu sorunu besleyen nitelikleri masaya yatırılmıştır. Bu noktada, çalışmamız boyunca kavramsal uzlaşının sağlanabilmesi için dijital gözetim, kişisel veri, veri güvenliği gibi kavramlar birbirleriyle ve ekonomik sistemin nitelikleriyle –özellikle tüketim bağlamında- bağlantılandırılmıştır. Çalışmada, yargı süreci aktörlerinden bilişim hukuku uzmanlarının ve denetim aktörlerinden veri denetim uzmanlarının veri güvenliği ve kişisel verilerin korunması konularındaki görüşleri bu bağlamda değerlendirilmiştir.

1. Kişisel Verilerin Korunması: Veri Güvenliği Bağlamında Dijital Gözetim

2010 yılında yapılan Anayasa değişikliği ile Anayasanın özel hayatın gizliliğini düzenleyen 20. Maddesine,

> "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel verileri hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak Kanunda öngörülen hallerde veya kişinin açık rızasıyla islenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"

şeklinde bir fıkra eklenerek, kişisel verilerin korunması açıkça anayasal güvence altına alınmıştır.[4] Kişisel Verilerin Korunması Kanunu (KVKK) ise 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Uluslararası belgeler, mukayeseli hukuk uygulamaları ve ülke ihtiyaçları göz önüne

4 Kişisel Verilerin Korunması Kurumu, 2018a, s. 10.

alınmak suretiyle hazırlanan Kanun ile kişisel verilerin çağdaş standartlarda işlenmesi ve koruma altına alınması amaçlanmaktadır. Bu kapsamda, Kanunun amacı, kişisel verilerin işlenme şartlarını, kişisel verilerin işlenmesinde kişilerin temel hak ve özgürlüklerinin korunmasını ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Kişinin mahremiyetinin korunması ile veri güvenliğinin sağlanması da bu kapsamda değerlendirilmektedir.[5]

Kişisel verilerin korunması ile ilgili ülkemizde ve dünyada çeşitli düzenlemeler yapılsa da bu verilere erişmek isteyenlerin yasal olmayan yollarla veri toplama faaliyetlerine yaygın biçimde devam ettiği yönündeki şikayetler gündemden düşmemektedir. Özellikle kişisel verilerin elde edilmesinde ve bu verilerin anlamlandırılmasında kullanılan yöntemler, kişilerin dijital ortamlarda gözetlenmesine, özel hayatın gizliliği hakkının gaspına ve mahremiyet ihlallerine neden olmaktadır.

Gözetim, her şeyden önce kavramsal olarak, temelde 'izleme' ve 'koruma' biçiminde ikili bir içeriğe karşılık gelmesi nedeniyle, benzeri pek çok kavram gibi övgü-yergi ekseninde değişen anlamlandırmalara tekabül etmektedir. David Lyon, (2013, s. 14,15) gözetim pratikleri için, antropolojik bir bakış açısıyla insan toplumunun temelinde yer alan edimlere işaret etmekte ve gözetimin bir kişinin diğer kişi üzerinde ona göz kulak olduğu ya da onu incelediği izlenimi bırakmak için sergilenen ilkel bir izleme davranışı olduğunu ileri sürmektedir. Kutsal olduğuna inanılan kadim metinlerde, koruma, kollama ve denetleme anlamlarına denk düşen gözetim (Çakır, 2015, s. 195), içinde yaşadığımız dönemle bağlantılı olarak gözetimin amacına odaklı çıkarımlarla birlikte, daha özgül bir tanımlamaya kavuşmuş görünmektedir. Bu çizgide, Lyon (2006, s. 13) gözetlemeyi, "hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel veri toplanması ve işlenmesi" olarak tanımlamaktadır. Gözetimin amacının, davranışların sürdürülmesini sağlamak niyetiyle ya da bazı davranışları engellemek suretiyle davranış değişimlerini kontrol etmek olduğu noktada, toplumsal düzlemde güç ilişkilerinin yarattığı dinamiklerle karşılaşmak kaçınılmazdır. Gözetimin, belirli grupların diğer gruplar üzerinde davranış kontrolü sağlamak amacıyla veri toplama, depolama, analiz etme, değerlendirme ve amaca uygun biçimde kullanma, bunu yaparken de potansiyel olarak fiziksel, ideolojik ve/veya yapısal şiddetten kaçınmaksızın, insanları belirli davranışlara yöneltme süreci (Çakır, 2015, s. 248) olarak tanımlanmasının nedeni de buradan kaynaklanmaktadır. William Bogard'a göre de (1996) bir şeyi gözlemek, aslında onu izlemek veya korumak demektir. Özellikle devletler için gözetimi meşrulaştırmanın bir yolu da Bogard'ın vurguladığı "koruma" söylenidir.

Koruma söyleni, insanlık tarihi boyunca teslimiyeti de beraberinde getirmiştir. Teslimiyet güvenliğe ihtiyaç duyulan tüm alanlara dairdir. Güvenlik vaadi, kabile şeflerinin söylemlerinden devletlerin söylemlerine; politik iktidarla ekonomik iktidarın aynı noktaya evrildiği dönemlerde ise daha çok şirketlerin söylemlerine geçmiştir. Gözetimin koruma ile eş anlamlı kabulünü sağlayan da kabile şefinin, devletin ve giderek şirketin yayılmacı ve kapsayıcı güç alanının bekasını garanti altına alan 'tehdit'lerdir.

5 Kişisel Verilerin Korunması Kurumu, 2018a, s. 12.

Doğal tehdit unsurlarının yanı sıra inşa edilmiş tehdit unsurlarının varlığı, -güç birliği (ayaklanma, isyan vb.) yaptığı her dönemde yönetici için büyük tehdit oluşturan- tebaa yerine, sultanın çıkarlarının güvenliğinin asıl amaç olduğu gerçeğini su yüzüne çıkarır. Gözetimin bireysel düzlem yerine toplumsal düzlemin konusu olması, kitleden gelecek tehditlerle baş edilebilmesi için gereklidir.

Dijital gözetim de bireyler arasında ayrım yapmamakta, herkesi gözetim altına alarak "toplu gözetim" ya da "kitle gözetimi" durumu yaratmaktadır. Bu durum-, kitlenin tamamını potansiyel şüpheli konumunda toplamaktadır (Çakır, 2015, s. 317). Güvenlik gerekçesi dışında, devletlerin yurttaşlarını sistematik biçimde gözetlemelerindeki amaç, modern dönem paradigmalarının getirisi olan, her şeyi öngörebilir, hesaplanabilir ve okunabilir kılmaktır. Bu ilk unsur dışında, güvenlik gerekçesi ile yapılan gözetimde, devlet tüm yurttaşlarını potansiyel tehlike/suçlu olarak konumlandırmakta ve dolayısıyla ulusal güvenliği sağlamak amacıyla gözetim yapıldığı iddia edilmektedir (Arslantaş-Toktaş vd., 2012, s. 25).

Politik iktidar dışında, ekonomik iktidar tarafından yapılan gözetim, ilk bakışta disipline edici nitelik taşımıyormuş gibi görünse de, gündelik yaşamdaki eylemleri yönlendirmek amacını –örneğin tüketim alışkanlıklarını biçimlendirmek gibi- taşıdığı için rıza üretimi yoluyla disiplin niyeti gözetmektedir. Ekonomik yaşamın gözetimi, insanların seçimlerinin takibi üzerinden kişiye özel oluşturulan profilleri veri olarak değerlendiren ve üretim ve pazarlama şablonlarını bu verilere dayandırarak dizayn eden şirketler vasıtasıyla açığa çıkmaktadır (Baştürk, 2016, s. 213).

Yurttaşların, barış dönemlerinde güvenlik alanları olarak hissettikleri evler, gözetimden azade oldukları inancıyla doludur. Lyon, (2006, s. 37) bu güvenlikli yuva hayalinin, dışarıdan gelmesi muhtemel baskılara ve taleplere zemin hazırlayan elektronik cihazlar aracılığı ile evin içinden dışına ve dışından içine, çoğu zaman aile fertlerinin haberi bile olmadan veri gönderilmesi nedeniyle altüst olduğunu söylemektedir. Gözetim, son kertede kontrol amaçlıdır. Ortada herhangi bir şeyi kontrol etme niyeti varsa, -bazen bir nesneyi, bir kişiyi ya da bir kitleyi- öncelikle o şeyi iyi tanımak gerekmektedir; bunun yolu ise gözetlemekten geçmektedir (Karakehya, 2009, s. 334). Gözetimin pek çok biçimini üç temel başlık içinde toplayan Alan Westin'e göre bunlar; "Fiziksel gözetim", "psikolojik gözetim" ve "veri gözetimi" olarak kategorize edilebilir:

> Fiziksel Gözetim: Kişinin bulunduğu yerin, hareketlerinin, konuşmalarının ya da özel yazışmalarının kişinin bilgisi veya rızası dışında optik, akustik araçlarla gözetlenmesi, Psikolojik Gözetim: Yazılı, sözlü testlerin ya da araçların veya maddelerin kullanılması suretiyle, kişinin isteyerek vermediği bilgileri enformasyonu elde etme veya kişinin kendisinin özel hayatı ve kişiliği bakımından önemli olabilecek hususları farkında olmadan açığa çıkarma, Veri Gözetimi: Veri isleme araçları aracılığıyla kişi veya gruplar hakkındaki bilginin, enformasyonun toplanması, islenmesi, değişimi ve kullanımı (Ketizmen, 2008, s. 193,194'den akt. Türkiye Bilişim Derneği, 2008, s. 15)

Çalışma konumuz kapsamında, gözetimin en güncel, en sistematik ve etkin yollarından birisi olan veri gözetimi, Türkiye Bilişim Derneği'nin ifadeleriyle, gözetim içinde incelenebilecek tüm boyutlar arasındaki sınırı kaldırmaktadır. "Fiziksel gözetim

ve psikolojik gözetime ilişkin bilgi ya da enformasyonun, bilişim sistemleri aracılığıyla işlenebilmesi olanağı, veri gözetiminin sınırlarını ortadan kaldırabilecek nitelikte bir gözetim boyutu olduğunun da göstergesidir" (Türkiye Bilişim Derneği, 2008, s. 16).

Gözetim amaçlı veri toplama deneyimleri, pek çok defa veri güvenliğini tehlikeye atan vakalara yol açmıştır. Bu denli dinamik bir yapının denetiminin güçlüğü kabul edilebilir bir noktada durmaktadır. Ağ güvenliğinin ve verimliliğinin artırılması amacıyla, internet ağlarının denetimi sağlanmaya çalışılmaktadır. Ancak bu durumun kötüye kullanımı, dijital gözetime, içerik kontrolü baskılarına ve giderek de geniş –haklı haksız ayrımı gözetilmeksizin- bir sansür girişimine neden olabilmektedir.[6] Bu durum dijital ortamların güvenilirliğinin sorgulanmasına neden olmaktadır. Dijital ortamlardaki güvenlik derecesinin yükseltilmesi de ancak bu alanda yeterli bilgi ve birikime sahip kuruluşlarca ya da bu alanda çalışan kişilere verilen eğitimlerle mümkün olmaktadır. Dijital teknolojilerdeki süratli değişimler boyunca dinamizmini koruyamayan eğitim içerikleri, yasal düzenlemeler, gelişmelerin know-how'a hızla entegre edilememesi gibi nedenler yüzünden, güvenlik açıkları dijital gözetim için geniş patikalar yaratmaktadır. İnternet kullanımının yaygınlaşması ve güvenliğe ilişkin sorunların kitlesel bir hal alması nedeniyle de bu alandaki güvenlik duvarlarının kalınlaştırılması kaçınılmaz olmuş, bu amaçla çeşitli yazılımlar geliştirilmiştir:

> Bu bağlamda *Intrusion Detection* Sistemleri ortaya çıkmıştır. IDS sunucu ve ağlardaki saldırıları algılayıp engellemeyi amaçlar. Buna dönük olarak, sunucu veya ağdaki etkinlikleri sürekli izleyerek, ya bilindik zararlı yazılım imzalarıyla karşılaştırır ya da sistemdeki bozuklukları algılamaya çalışır. IDS, ağdan akan verilerin içeriğinin de incelenmesini içerdiği için net tarafsızlığı ilkesi, organizasyonel sınırlar içinde de olsa ihlal eder. İnternet'in sürekli artan önemi, kısmen IDS›ten ilham alan, *Derin Veri Analizi* (Deep Packet Inspection - DPI) adında yeni bir kavramın gelişimini hazırlamıştır. Paketlerin yalnızca adres kısmını isleyen geleneksel router donanımı ve yazılımından farklı olarak, DPI sistemleri paket içeriğinin hepsini veya çoğunu inceler. DPI süreci, bir posta idaresinin elindeki mektupları yalnızca adresine iletmek yerine, hepsini açıp içlerini okumasına benzetilebilir. Bu yüzden DPI uygulamasının özel yaşam ve bilgi güvenliği açısından ciddi sonuçları vardır. Ayrıca, belirli bir organizasyonu ilgilendiren IDS›in aksine, DPI sistemleri İnternet Servis Sağlayıcılar (Internet Service Provider - ISP) tarafından uygulanmakta ve ISP'leri kullanan nüfusların tamamını olası özel yaşam ihlallerine açık hale getirmektedir. (Kırlıdoğ ve Fidaner, 2012, s. 1015).

Çoğu ülkedeki servis sağlayıcıları yasal olarak üst veriyi depolamaya tabidir. Servis sağlayıcılar, üst veriyi depolayarak ve analiz ederek, verilerin kaynağını, varış yerini, tarihini, zamanını, süresini ve iletişim türünü tespit edebilir ve tanımlayabilmekte[7] ; bu da çeşitli güvenlik ihlallerine neden olabilmektedir.

Derin veri analizi, bir ağı kullanan tüm kullanıcıların, bunlar arasından belli bir kesimin ya da tek bir kullanıcının ağ üzerindeki davranışlarını, "ağ izleme" yöntemi ile takip edebilmektedir. Bunun yanı sıra devletler, çocuk pornografisi gibi geniş

6 Joler vd. (2015)

7 SHARE LAB (2015a)

kabul görmüş suçları engellemekten, muhalif düşüncelerin görünmez kılınması gibi baskıcı eylemlere kadar pek çok alanda yine derin veri analizi ile "gözetim ve sansür" gerçekleştirebilmektedir. Derin veri analizi, şirketlere de tüketici gözetimi için geniş olanaklar sunmaktadır. Özellikle "hedefli reklamcılık" kapsamındaki uygulamalarda, kişisel veriler ve dijital izler aracılığı ile elde edilen bilgiler, reklamın kitleye ulaştırılmasında isabetli hedefleme sağlayabilmektedir. Gönderilen reklamın isabet gücünün artırılması için gerekli verilerin toplanması, çoğunlukla kişilerin cihazlarına kaydedilen çerezler aracılığı ile yapılmaktadır. Her bir kullanıcıya atanan kimlik numaraları ile eşleşen ilgi alanlarını belirlemek için kişinin tüm etkinlikleri kaydedilmektedir. Çerez kullanım şartlarının kabulü ya da reddi ile kullanıcılar teorik olarak kişisel bilgilerinin toplanmasını engelleyebilir ya da sunulan hizmeti kullanmaktan vaz geçebilirler. Ancak daha karmaşık sistemlerin, kullanıcılar çerezleri sildiğinde bile kullanıcı hakkındaki bilgileri toplamayı sürdürdüğü de bilinmektedir (Kırlıdoğ ve Fidaner, 2012, s. 1016,1017). Gelinen noktada internet alanındaki güvenlik ihlallerini önlemek amacıyla geliştirilen yazılımların dijital gözetime hizmet ettiği, bu alanda yapılan akademik çalışmalarda sıklıkla ifade edilmekte, bu sistemlerin amacının dışında da kullanılabileceği dile getirilmekte, kişisel veri gözetimi için devletlerin ve şirketlerin amaçlarına hizmet eden bir mekanizma haline dönüştüğü vurgulanmaktadır (Talay, 2018, s. 53).

2. Kişisel Verileri Damıtılmış Bilgiye Dönüştürme Aracı Olarak Üst Veri

6698 Sayılı Kişisel Verileri Koruma Kanunu'nda tanımlandığı biçimiyle kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Bu tanım, kişinin, kişiliğinin bir parçası olarak beğenilerinden oluşturulan kişisel profilini de kapsayan pek çok bilgiye işaret edebilir. Beğeniler ve ilgi alanları, hedefli reklamlar için kıymetli bilgiler kapsamındadır. Kişisel cihazlara kaydedilen çerezler aracılığı ile kullanıcılara atanan kimlik numaraları, bu beğeni ve ilgi alanları ile eşleştirildiğinde, başlangıçta pek de kişisel gibi durmayan verilerden, kişiye ilişkin yeni bilgiler türetilebilmektedir. Bu bilgiler dijital profilleme ve kişiselleştirmenin yükselişine tanıklık ettiğimiz bu günlerde özellikle pazarlamacılar için veri sermayesi yaratmaktadır. Öte yandan bu girişimler, sonuçları ağır olabilecek sosyal ayrımları ve gizlilik sorunlarını tırmandıracak gibi görünmektedir. Pazarlamacıların yeni jargonlarıyla, insanları 'hedef' ve 'çöp' olarak sınıflandırıyor olmaları bile, bu tehlikenin göstergesi sayılmalıdır (Turow 2015, s. 21). Bu ayrımı yapabilmeleri için önemli bir aygıt haline gelen kişisel verilerin yeni bir sermaye biçimine dönüşmesi, alınıp satılan bir meta olarak kabul görmesi bu noktada pek de şaşırtıcı değildir. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Genel Sekreteri Angel Gurria "İnternet Ekonomisinin Geleceği Üzerine"[8] adlı bir toplantıda, kişisel verileri para birimi olarak lanse etmiştir. Buradan da anlaşılacağı üzere kişisel veriler artık yalnızca bir veri değil, değer taşıyan bir nesne olarak görülmektedir. Oysa kişisel veri adı üstünde kişiseldir, mümkün olan en üst düzeyde mahremiyetinin korunması gerekmektedir. Mahremiyet kişinin kendi alanıdır, bölünmemiş özerkliğine ait bölgesidir ve mahremiyetin sınırlarını gizlilik çizer (Bauman ve Lyon, 2016, s.

8 Gurria (2008)

41). Özel hayatın gizliliği, bireyin kendisini diğerlerine açıp açmayacağına ve bunu yapacaksa ne ölçüde yapacağına karar verme hakkı kapsamında anlamlandırılmıştır (Van Dijk, 2016, s. 172).
Mahremiyet Komitesi Raporu'na[9] göre mahremiyet hakkının iki yönü bulunmaktadır. Bunlardan ilki, bireyin kendisi ve çevresine izinsiz dahil olunmaması özgürlüğü, ikincisi ise bilgi mahremiyeti, yani kendisiyle ilgili bilgilerin başkalarına nasıl ve ne ölçüde aktarılacağına kendisi için karar verme hakkıdır. "Mahremiyet gözetimle birlikte kesintiye uğrar, gizliliğini ve anlamını yitirir" (Çakır, 2015, s. 11). Bauman ve Lyon'a göre (2016, s. 35) "Mahrem olan her şey artık potansiyel olarak kamusal alanda yapılıyor ve kamunun tüketimine açık halde. Bunun nedeni de insanların neyin kamusal neyin mahrem olması gerektiği konusundaki anlayışlarının değişmesidir". Öte yandan internet kullanıcıları, kişisel verilerinin kaydedilerek işlenmesi ve bunun yol açabileceği sorunlar konusunda yeterince bilgi sahibi değillerdir. Yapılan çalışmalar da bu durumu ortaya koymaktadır (bknz: Shklovski vd., 2014; Talay, 2018).

İnsanlar giderek bilgisayarlar ve algoritmalar tarafından gerçekleştirilen araştırmalar için, birer analiz nesnesi haline dönüşmüştür. Üst veriler genellikle dijital pazarlama, işletme analizi veya bilimsel araştırma alanındaki veri toplama ve analizine dayanan işletmeler için bir kaynaktır. Kullanıcılar çevrimiçi olur olmaz, her hareketi (tıklama, gönderilen veya alınan e-postalar) çok fazla ve değişen miktarlarda görünmez bir iz üretir. Bu izler toplanarak bir araya getirilmekte ve analiz edilen bu izler davranış kalıplarını, konumları, alışkanlıkları ve ilgi alanlarını ortaya çıkarmaktadır. Bu izlerin çoğu da üst verilerde gizlidir. Üst verilere erişmede serbestlik tanınan yapılar genel olarak şirketler[10], İnternet servis sağlayıcıları[11] ve Devletler[12]dir (Joler vd. 2015).[13]

Özellikle şirketler, kendi pazarlama hedeflerine uygun verileri büyük veri içerisinde yer alan üst verilerden elde etmektedir. Avrupa Dijital Haklar Örgütü'nün gözlemci üyelerinden olan Alternatif Bilişim Derneği'nin web sitesinde bulunan elektronik broşürde büyük verinin tanımı, yine bu örgütün yayınladığı European Digital Rights dokümanından çevrilerek sunulmuştur:

> "Büyük Veri" çok büyük ve karmaşık veri tabanlarını tanımlamak için kullanılan yaygın bir terimdir. Büyük Veri, tek bir sunucu veya masaüstü bilgisayarda yürütülen geleneksel "yerel" tekniklerle yönetilemeyen veya analiz edilemeyen ve milyonlarca kaynaktan gelen veri kitlelerini (bir arama motorunun deposundan, internet araştırmalarından, Wikipedia'nın veri tabanından alınan veriler gibi) ifade etmek için kullanılır (Alternatif Bilişim Derneği, 2013, s. 11).

9 Klein, 1972

10 Google veya Facebook gibi reklamcılık hizmetleri sunan şirketlerdir. Üst verilere erişmekle yetinmezler, sunucularında gerçek veri ve içeriğe sahiptirler

11 Üst veri erişimi olan ikinci grup internetin altyapısıyla ilgilidir. Bunlar İnternet servis sağlayıcıları, mobil servis sağlayıcıları, İnternet değişim noktaları ve denizaltı optik kablolarıdır ve kablolarından, yönlendiricilerinden ve sunucularından geçerken verilere erişebilirler

12 Çoğu durumda, ulusal kanunlar hükümetlere veya bazı ajanslara Üst veriler başta olmak üzere kullanıcıların verilerine meşru erişim imkânı verir. İnternet altyapı sahipleri veya hizmetleri sunan şirketler, kendi yetkileri altındaki hükümetlerle işbirliği yapmakla yükümlüdürler. Devletin taleplerine sıklıkla uygundurlar ve farklı teknik işbirliği şekillerine sahiptirler. Bununla birlikte, birçok ülkede, devlet kurumları, Üst veri toplamaya dayalı vatandaşların kitle gözetimine yönelik programlar geliştirmeye yatırım yapmıştır.

13 Joler vd. (2015)

Büyük Veri; sosyal medya paylaşımları, GSM operatörleri aracılığı ile gerçekleştirilen aramaların kayıtları, fotoğraf, video, ağ konumu, log gibi farklı kaynaklardan elde edilen verilerin anlamlı ve işlenebilir hale dönüştürülmüş biçimidir (Eyüpoğlu vd., 2017, s. 177).

Üst veri kapsam bakımından büyük veriden daha dar, ancak ilişkisellik bakımından daha özgüldür: Üst veri kısaca, belirli bir veri hakkındaki detaylı, -örneğin kaynak bilgisi, bilginin oluşturulma zamanı, konumu gibi- bilgilerdir. Üst veri, tek bir veri ya da belirli bir dijital varlık hakkında, tikel bağlamda ayrıntılı bilgi sağlarken, büyük veri, tüm verilerdeki detaylı bilgileri içermektedir. Büyük verideki kişilerin tüketim kalıpları ve eğilimlerini keşfetme olanağı, üst veri aracılığı ile daha spesifik hale getirilebilmektedir. Büyük veri, çok büyük bir veri yığını olup, standart teknoloji araçlarıyla incelenemezken; üst veriyi incelemek daha kolay olabilmektedir: "Üst veri iğne ise, büyük veri samanlıktır".[14]

> Burada Edward Snowden'ın 2014 yılında yapmış olduğu bir açıklama akıllara gelmektedir: "Üst veri, olağanüstü bir biçimde müdahalecidir. Bir analizci olarak içerik yerine üst veriye bakmayı tercih ederim, çünkü o daha hızlı ve kolay, ayrıca yalan da söylemiyor... Eğer telefon konuşmanızı dinliyorsam, öylesine konuşuyormuş gibi yapabilirsiniz, kodlar kullanabilirsiniz. Fakat eğer üst verinize bakıyorsam, hangi numaranın hangi numarayı aradığını biliyor olurum. Hangi bilgisayarın hangi bilgisayarla konuştuğunu biliyor olurum". Amerika Birleşik Devletleri Ulusal Güvenlik Teşkilatında Genel Danışman olan Start Baker da şöyle demiştir: *"Üst veri kesinlikle bir insanın yasamı hakkında her şeyi söylüyor. Eğer yeterli üst veriniz varsa, içeriğe ihtiyacınız kalmaz"* (akt. Talay, 2018, s. 33).[15]

Türkiye Bilişim Derneği, 2008'de 10. Dönem çalışma grubunun yürüttüğü çalışmalar kapsamında oluşturulan nihai rapora göre, kişisel verilerin korunması konusu salt bilişim teknolojileri kapsamında değerlendirilmemeli, 'gözetim' üst kavramı altında, sosyolojik bir düzlemde ele alınmalıdır. Çünkü kişisel verilerin korunması, salt veri koruması değil, bireyin özgürlüğünün korunmasıdır. Çalışma grubunun raporuna göre, veri korumasının güvenlik, gizlilik odağında ele alınması, özgürlük sorunsalının gözden kaçmasına neden olabilecektir. Böylelikle, gözetimin istenmeyen sonuçlarına ilişkin sorumluluk, teknolojik donanım ya da yazılım yeterliliği gibi teknik düzlem dışında, temel sorun bağlamında kurum ve kuruluşların yükümlülükleri ile bağlantılandırılabilecektir (Türkiye Bilişim Derneği, 2008, s. 5).

3. Dijital Ortamda Yeni Pazarlama Aracıları: Çerezler

Joseph Turow, (2015, s. 25) Türkçeye 'çerezler' olarak çevrilen "cookies"i tanımlarken bilgisayar kullanıcısının sabit diskinde, internette hangi siteleri ziyaret ettiğine dair verileri kaydetmenin yolunu açan yazılımları işaret etmektedir. Bu vurgu doğrultusunda, özellikle şirketlerin reklam hedef kitlelerini belirleme ve isabetli gönderi trafiği oluşturma niyetiyle, kişisel bilgisayarlardan veri topladıklarını belirtmektedir. Çerez sistematiği, web sitelerinin kullanıcının daha önce siteye girip girmediğini öğrenmek için site her ziyaret edildiğinde diski okuyarak çalışmaktadır. "Tüketiciye sağladığını iddia ettikleri

14 Martin (2016)

15 SHARE LAB (2015a)

avantaj, bireysel ihtiyaçlara göre düzenlenmiş tüketici reklamlarının sadece doğru olan hedeflere yöneltilmesidir. Şirketin avantajı ise piyasanın bireyselleşmiş bir düzeyde bilinebilmesidir" (Lyon, 2006, s. 208). Çerezlerin internet dünyasında yer alış amacı başlangıçta kullanıcı dostu niyetler taşımaktaydı. Bu minvalde, çerezlerin kullanıcıya sağladığı çeşitli avantajlardan söz edilmektedir. Örneğin, ziyaret edilen bir web sitesine ilk ziyarette yüklenen fotoğraf, resim, animasyon gibi görsel unsurlar, çerezler sayesinde bilgisayar hafızasında kalmakta ve ikinci bir ziyaret halinde kullanıcıya zaman kazandırmaktadır. Ancak günümüzde internet sitelerine erişim, internet hızlarının giderek artması ve geniş bant olanakları sayesinde neredeyse saliseler halinde gerçekleşmektedir. Böylelikle web sitelerinin yeniden ziyaretinde çerezlere ihtiyaç duyulmamaktadır. Çerezler bu durumda kullanım amaçlarını aşan bir noktada değerlendirilmektedir. Her ne kadar web sitelerinde bulunan kullanıcı ve şifrelerin çerezler aracılığı ile kaydedilmesiyle beraber kullanıcılar, bir sonraki ziyaretlerinde kullanıcı adı ve şifrelerini girmek zorunda kalmıyor olsa da, sorun kişisel verilerin güvenliği olduğunda, sağlanan bu kolaylığın bedelinin düşünülmesi gerekmektedir. Çünkü çerez uygulamaları, artık kullanıcı dostu bir tutumdan ziyade, pazarlama hedefleri doğrultusunda veri toplayan aracı davranışı sergilemektedir. Lawrence Lessig'e göre de "Web, çerezlerden önce temelde kişiseldi. Çerezlerden sonra Web, sıra dışı gözetim yeterliliği olan bir alan haline geldi". Pazarlama faaliyetleri için oldukça değerli bir araç olan veri, 21. Yüzyılın petrolü olarak nitelendirilmekte; çerezler ise bu petrolü yüzeye çıkaran sondaj aygıtı olarak çalışmaktadır.[16]

Kasım 2016 itibariyle internet sitelerinin %46.1'i çerezleri kullanmaktadır. Ancak bu çerezlerin %91.3'ü güvenli olmayan çerezlerden oluşmaktadır.[17] Sırbistan'da 2015 yılında kişiler tarafından en sık kullanılan 50 web site üzerinde yürütülmüş olan bir araştırmaya göre, çevrimiçi izleme çerezlerinin 4'te 3'ünden fazlası (%75,4), Amerika Birleşik Devleri menşeili şirketlere aittir. Google, Amerika'nın çerez diliminin yarısına sahipken geri kalanı çoğunlukla Facebook, Amazon ve Twitter arasında paylaşılmaktadır. Bu büyük Amerikan şirketleri katmanının altında, çevrimiçi davranışı izleyen, çoğunlukla reklamcılık ve veri analizi yapan yüzlerce, nispeten daha küçük şirket ağları vardır. Genel olarak, bu çerezlerin gerçekten küçük bir miktarı, bölgesel şirketler için veri toplamaktadır. Amerika, çevrimiçi davranışlarımızdan en yüksek değeri elde ettiği için, büyük bir farkla en baskın kullanıcı-izleme ekonomisine sahiptir.[18]

İnternette herhangi bir web sitesine girdiğimizde ya da mobil uygulama kullanmak istediğimizde karşımıza çıkan bir uyarıyla beraber bu hizmeti kullanmaya devam etmemiz için çerez ve gizlilik politikalarını onaylamamız istenmektedir. Bu durum, kişisel verilerin toplanmasındaki açık rıza kavramının içeriğini belirsiz kılmaktadır. Zorlama bir rıza halini alan çerez politikaları nedeniyle verileri toplanan kişiler kendileri istemedikleri halde daha sonra bu ortamlarda reklam, bildirim, mesaj veya promosyon postalarıyla karşılaşmakta, hizmetin kullanım bedelini reklama maruz kalarak ödedikleri

16 SHARE LAB (2015b)

17 W3Techs (t.y.)

18 SHARE LAB (2015b)

halde bir de verilerini teslim etmektedir (bknz: Meng vd., 2016; Talay, 2018).

4. Yöntem

Çalışmada, yargı ve denetim süreçlerinde rol alan aktörler olarak iki bilişim hukuku uzmanının ve bir veri denetim uzmanının veri güvenliği ve kişisel verilerin korunması konularındaki görüşleri, dijital gözetimin pazarlama amaçlı kullanımı bağlamında değerlendirilmiştir. Söz konusu aktörlerle 20.02.2019 ve 25.02.2019 tarihlerinde yapılan –kayıtlı izinli- yarı yapılandırılmış görüşme formları ile yapılan derinlemesine görüşmelerden elde edilen ses kaydı verileri bulgulara dönüştürülmüş, ve bu bulgular, alana ilişkin literatür ve yasal mevzuat kapsamında değerlendirilerek sunulmuştur.

5. Bulgular

Kişisel veri, internet kullanıcısı olsun olmasın pek çok kişi için kapsam ve içerik bakımından anlaşılması pek de kolay olmayan bir kavramdır. Kişisel verilerin güvenliği konusunda, kişilerin bireysel düzlemde alabilecekleri önlemlerse, çoğu zaman internet teknolojisine yeterince hakim olamamaktan, gelişmeleri yeterince takip edememekten dolayı oldukça kısıtlı kalmaktadır. Devletlerse veri güvenliğini yasalarla taahhüt altına almaya çalışmakta, ancak uygulamada karşılaşılan sorunlar gündemde kalmaya devam etmektedir. Kişisel verilerin güvenliği kurumsal bağlamda veri sorumlularının görev alanındadır. Bu noktada veri sorumlularının yetkinlik düzeyleri önemli bir alanda durmaktadır. Çeşitli yazılımlar aracılığı ile kişisel verilerin güvenliğinin riske girmesi durumunda, sıklıkla çerez yazılımları sorumlu tutulmaktadır. Bu durumda, çerez kullanımının kabulü veya reddi internet kullanıcısının iradesine bırakılmış gibi görünse de, özellikle pazarlama amaçlı veri toplama faaliyetleri söz konusu olduğunda, yasada yer alan açık rıza kavramının sınırlarının aşındırıldığı uygulamalarla karşılaşılmaktadır. Çalışmamızda, derinlemesine görüşme yapılan yargı ve denetim uzmanlarına kişisel verilerin güvenliği, veri sorumlularının yetkinlikleri ve çerez kullanımında açık rıza kavramına ilişkin sorular yönlendirilmiş ve bu üç ana konu, birbirleriyle bağlantılı biçimde değerlendirilmiştir.

5.1. Yargı ve Denetim Bağlamında Kişisel Verilerin Korunması

6698 sayılı Kişisel Verileri Koruma Kanunu kapsamında "kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması, yetkisiz kişilerin erişimine açılması, ifşası veya amaç dışı ya da kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi"[19] amacı vurgulanmakta ve kişisel verilerin korunması, temel hak ve özgürlüklerin korunmasıyla eş tutulmaktadır. Kanun'a göre bu koruma aynı zamanda, insan onurunun ve kişilik haklarının da korunması anlamına gelmektedir. Bu konuda yapılan pek çok akademik çalışmada Kanun'da yer alan istisnai durumların esnetilmesine olanak sağlayacak durumlara değinilmiş, bu durumun yaratabileceği güvenlik açıkları belirtilmiştir.

19 Kişisel Verilerin Korunması Kurumu, 2018b.

Güvenlik açıkları, Kanun'da yer alan boşluklardan, uygulayıcıların yetersizliğine, hackerların faaliyetlerinden kullanıcının bilgisizliğine veya dikkatsizliğine kadar pek çok noktadan kaynaklanabilmektedir. Ancak güvenlik açıklarını azaltma girişimlerinin, kontrol, düzenleme ve geliştirmenin en hızlı yapılabileceği noktadan başlaması gerektiği, bu noktanın da Kanun'a ve Kanun'u uygulayanlara işaret ettiği ortadadır.

Çalışmamız kapsamında yapılan derinlemesine görüşmelerde, Türkiye'de kişisel verilerin güvenliğine ilişkin sorulara alınan yanıtlar, bu konuda güvenlik açıklarının yoğunluğuna dikkat çekmektedir. Çalışma kapsamında görüşülen tüm aktörlerin konu hakkındaki ifadeleri aynı yöndedir. Bilişim Hukuku danışmanı olan Görüşmeci 1, kişisel verilerin aktarılması ve kayıt sistemlerinde sınırsız dolaşımının yarattığı güvenlik sorunlarına dikkat çekmiştir:

> …gerçekten veri güvenliği denilen kısım yok Türkiye'de. Özellikle dijital veri güvenliği. Güvenlik duvarının ne olduğunu hiç kimse bilmiyor. Dijital verinin nasıl korunması gerektiğini kimse bilmiyor. Bilseler de bunu uygulamak çok ta işlerine gelmiyor açıkçası. Bir de nerelere aktarıldığının boyutu yok. Siz bir yerde bilginizi verdiniz hastaneye gittiniz parmağınızı okutuyorsunuz, cihaz merkezine gidiyor bu bilgiler… Cihaz yabancıysa yurtdışına gidiyor, SGK'nın kaydına giriyor, hastanenin kaydına giriyor. Hastanenin ortak çalıştığı bir firma varsa onun kayıt sistemine gidiyor. Sizin genetik veriniz dünyanın her yerine aktarılıyor ve bunun bir sınırı yok (Görüşmeci 1).

Yine Bilişim Hukuku danışmanı olan Görüşmeci 2 ise, daha çok kullanıcıların kişisel verilerini paylaşırken hassasiyet geliştirmemelerinin kişisel verilerin güvenliğini tehlikeye attığını ifade etmiştir:

> Devlet bu verilerimizi ne kadar iyi koruyor? Kamu kurumlarıyla veri paylaşırken hiç kaygı duymuyoruz. Nasıl olsa kamu kurumu diye. Oysaki bilgi saklanmasının kendi eşikleri, sınırları, güvenlik duvarları var. Yani dijital anlamda var. Bazen kamu kurumlarının verileri de çok daha çalınabiliyor, paylaşılabiliyor. O nedenle hepimizin her kurumla veri paylaşırken özenli olmamız lazım. Bir de çok kolay evet diyor musun? Kabul ediyor musun? … Çünkü bakın kötü niyetli kişiler de haksız para kazanmak ya da suç işlemek bizim kişisel verilerimize, hassas verilerimize ulaşmak isteyen kişiler de bizim kadar bu alanda çalışıyorlar. Belki bizden fazla. O yüzden bizim davranışlarımızı kolaylıkla hangi hataya düşeceğimizi biliyorlar (Görüşmeci 2).

Lyon'a göre (2006, s. 23) insanlar çoğu zaman, kişisel verileri talep edildiğinde bu bilgileri, görecekleri faydanın ödeyecekleri bedelden daha fazla olduğuna inanarak, ya da yanlış bir şey yapmadıkları sürece, saklamaları ya da korkacakları bir şey olmadığını düşünerek şirketlerle memnuniyetle paylaşabilmektedir. Kişisel veriyi talep eden merciler, kamu kuruluşları olduğunda, kişiler bu bilgileri daha yüksek bir güven duygusu içerisinde, daha az kaygı duyarak paylaşabilmektedir.

Bağımsız bir denetleme kuruluşunda bilişim teknolojileri uzmanı olarak çalışan ve veri koruma denetiminde aktif rol alan Görüşmeci 3, dijital alt yapının yetersizliğinin Türkiye'de güvenlik sorunu yarattığını, buna ek olarak kurumsal düzlemde veri koruma hassasiyetinin yeterince gelişmediğini dile getirmektedir:

> Türkiye doğal olarak dijital altyapı olarak, güvenlik olarak bunlara hazır olmadığı

> bir dönemde. … [Örneğin] sağlık sektöründe, kişilerin özel verilerinin damar izine kadar toplandığı bir dönem yaşıyoruz. … Sürekli haberlerde de görüyoruz işte kanser hastalarının listesinin sızdırıldığı, ilaç firmaları tarafından ele geçirildiği gibi birçok şey görüyoruz. Devlet kurumlarında şu anda kurum bazında kişisel verilerin nasıl korunması gerektiği ile ilgili genelgeler hazırlanıyor. Bunlarla ilgili sistematiği daha yeni oturtmaya başladığı için özellikle bazı sektörler hiç ele alınmadı. Mesela turizm sektörü… Olayların senaryolaştırılması yapılmadı. Hukuki boyutta daha önce emsal teşkil etmediği için veya emsali olmadığı için nelerle nasıl kararlar verileceği daha henüz senaryolaştırılmadı (Görüşmeci 3).

Her üç görüşmecinin de kişisel verilerin güvenliği konusunda farklı boyutlara vurgu yaparak, Türkiye'de veri güvenliğine ilişkin zayıflıkları dile getirdikleri görülmektedir. Bunların yanı sıra görüşmeciler, 6698 sayılı Kanun'un içeriğinin Avrupa Birliği uyum yasaları doğrultusunda hazırlanmış olsa da, kişisel verilerin güvenliğinin yargı ve denetim düzleminde sağlanabilmesi için Türkiye'nin sosyolojik yapısının dikkate alınarak uygulanması gerektiğini belirtmişlerdir. Görüşmeciler, kişisel verilerin güvenliği konusundaki önemli sorunlardan birinin de "kişisel veri" kavramının kapsamının yeterince bilinmemesi olduğunu dile getirmişlerdir. Bu noktada, veri güvenliğini sağlamada aktif rol oynaması beklenen veri sorumlularının yetkinliklerinin önemi gündeme gelmektedir.

5.2. Veri Sorumlularının Veri Güvenliğini Sağlama Yetkinliklerine İlişkin Görüşler

Kişisel Verileri Koruma Kanunu'na göre, veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. Kişisel verilerin güvenliğinin sağlanması için kilit noktada bulunan veri sorumlularının çalışma koşulları, teknik donanım sahipliği ve kişisel veriye ilişkin kavramsal bilgisinin yeterliliği kişisel verilerin korunmasında oldukça önemlidir. Çalışmamız kapsamında, veri sorumluları ile doğrudan irtibatta olan görüşmecilerin alan gözlemlerini aktardıkları cümleler de konunun öneminin altını çizmektedir. Görüşmelerden elde edilen ifadeler, veri sorumlularının ve onların güvencesinde çalışan veri işleyicilerinin gerek kişisel verinin kavramsal boyutuna gerekse veri güvenliğini sağlayacak teknik donanıma ve bilgi birikimine yeterince sahip olmadıkları noktasında ortaklaşmaktadır.

Görüşmeci 1, kişisel verilerin oldukça basit algılandığını, özel nitelikli kişisel veriler alanına denk düşen verilere ilişkin bilgilerin kapsamına ilişkin bilgi düzeylerinin düşük olduğunu belirtmektedir:

> …kimse kişisel verinin tam olarak ne olduğunu bilmiyor Türkiye'de. Ben otellerdeki eğitimlere de katıldım, yoğun bir şekilde çalışıyoruz. Kişisel verinin korunması ile ilgili en azından üst düzey müdür ya da müdür yardımcısı pozisyonundaki personelin eğitimini birebir hukukçularımızla beraber yapıyoruz. Direktörümüz var. Onunla birlikte eğitimlere katıldık ve kişisel veri [nedir] sorusunu sorduğumuzda insanların aklına gelen şey imza ya da T.C. kimlik numarası [oluyor]… Evet, bunlarda kişisel veri ama… Özel nitelikteki kişisel verileri sorusuna [gelince]… Kişiler T.C. kimlik numarası ve imzasını özel nitelikli kişisel verisi olduğunu düşüyor (Görüşmeci 1).

Görüşmeci 2, kişisel veri kavramının kapsamının yeterince bilinmiyor oluşunu, kavramın görece yeni bir kavram olmasına bağlamaktadır:

> Kanunda tanımlanan kişisel verinin ne olduğunu bu alanda çalışanlar da bilmiyor. Türkiye'de yeni karşılaştığımız bir kavram. Avrupa'dan bir anlamda Avrupa ile birlikte ürettiğimiz bir kavram. O yüzden vekillerimiz, kurumsal müvekkillerimiz, özellikle yabancılarla çalışan kurumsal müvekkillerimiz bu alanı çok iyi biliyorlar. Diğer müvekkillerimiz ise toplumda ne kadar biliniyorsa o kadar biliyorlar (Görüşmeci 2).

Görüşmeci 2, kişisel veri kavramının bilinirlik düzeyinin, bireysel düzlemden ziyade kurumsal yapılarda arttığını ifade etmektedir. Kişisel verilerin sistematik biçimde kayıt altına alınması ihtiyacı duyan turizm, sağlık gibi sektörlerde veri sorumlularının konuya hakimiyetinin yüksek olma durumunu ise, yabancı ortaklık ya da sahiplik durumu ile ilişkilendirmektedir.

Kişisel Verileri Korumaya yönelik mevzuatta, veri sorumlusu olmasa bile, herhangi bir kurumda çalışanların hepsinin asgari düzeyde kişisel verilerle ilgili bilgi sahibi olmaları için çalışmaların sürdürülmesi gerekliliği belirtilmektedir. Görüşmeci 3'ün ifadeleri de kişisel verilerin ne olduğuna ve ne derece önemli olduğuna ilişkin bilgi yetersizliği olduğunu doğrulamaktadır. Bunun da ötesinde, görüşmecinin verdiği örnek, kurumda çalışan tüm personelin bu konuda asgari düzeyde bilgi sahibi olmama durumunun yaratacağı sorunlara işaret etmektedir:

> Kişisel verinin gerçekte ne olduğunu, bunun öneminin ne olduğunu bilmiyorlar. Kurum güvenliğiyle [ilgili] şöyle bir örnekleme yapayım: Otel diskoyu kamera kaydı altına almak zorunda, çünkü adli bir vaka, bir kaza, bir yaralanma olursa otel sorumlu ve bunu ispatlamak zorunda. Sizin bu görüntüyü alma zorunluluğunuz var ama bu görüntüyü nerde yayınlayacaksınız? Oradaki bir animatör o görüntüyü başka amaçlarla kullanırsa burada bir ihlal var. Bu nedenle neyin kişisel veri, neyin veri ve bunların nasıl işleneceği ile ilgili inanılmaz bir bilgi kirliliği var. Bunların olmaması için şu anda eğitimler düzenleniyor. Kişisel Verileri Koruma Kurumu sempozyumlar düzenliyor (Görüşmeci 3).

Veri sorumlusu bulundurma zorunluluğu olan kurumsal alanda bile, kişisel verinin içeriğine ve kapsamına hâkimiyetin düşük düzeyde olduğu, görüşmecilerin ifadelerinden anlaşılmaktadır. Söz konusu, bireysel düzlem olduğunda sorunun daha da karmaşık bir hal almış olduğunu söylemek pek de akıl dışı olmayacaktır. Kurumsal yapılardaki veri sorumlularının konuyla ilgili donanımı bu denli yetersizken, bireysel internet kullanıcılarının çoğunlukla kişisel verinin neleri kapsadığı konusunda yeterli bilgiye sahip olmalarını beklemek gerçeklikle örtüşmeyecektir. İnternet kullanıcılarına yönelik tüketici gözetimi yapan yazılımların barındırdığı çerezler aracılığı ile kullanıcının kişisel verilerinin elde edilmesi karşısında, internet kullanıcılarının neredeyse savunmasızlığı bu noktada değerlendirilmelidir.

5.3. Çerez Kullanımı Kabulünde Açık Rıza Karmaşası

Çerez kullanımının kabul edilmesi esnasında açık rızanın alındığı algısını yaratan çerez kullanım şartlarının bulunduğu dijital metnin onaylanması sonucunda elde edilen kişisel verilerin kullanım alanlarındaki belirsizlik, kişisel verilerin güvenliğini tehdit eden bir unsur olarak değerlendirilmektedir. Bu noktada açık rıza kavramının anlamsal

içeriğindeki karmaşa alanı daha sorunlu bir hale getirmektedir. Kişisel Verileri Koruma Kanunu'nda açık rıza "İlgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanıdır" biçiminde tanımlanmaktadır. Açık rızanın temelde üç unsuru içinde barındırması gerekliliği, yine aynı Kanun kapsamında yer almaktadır. Buna göre açık rızanın unsurları:

> a. Belirli bir konuya ilişkin olma: Açık rıza beyanının kapsamı genel nitelikte olmamalı, belirli bir duruma özgülenmiş olmalıdır. Örneğin; veri sorumlusu tarafından "tüm ürün ve hizmetlerimizin sunulması için kişisel verilerinizin işlenmesine açık rıza veriyor musunuz?" biçiminde rıza alınması durumunda, rıza "belirli bir konuya ilişkin" olmayacağı için geçerli bir rıza olarak kabul edilmeyecektir.
>
> b. Bilgilendirmeye dayanma: Elde edilecek kişisel verilerin hangi amaçlarla kullanılacağı açıkça belirtilmeli, kişinin anlamayacağı terimler ya da yazılı bilgilendirme yapıldığında okumakta güçlük çekeceği oranda küçük puntolar kullanılmamalıdır.
>
> c. Özgür iradeyle açıklanmış olma: Bir irade beyanı olan "rıza" beyanının kişinin özgürlüğünü etkileyecek hallerden arınmış olması gerekmektedir. Bu doğrultuda, "açık rıza" beyanını veren veri sahibinin iradesini bozacak bir durum mevcut olmamalıdır. Örneğin; veri sorumlusu tarafından veri sahiplerinin rızalarının elde edilmesi, bir ürün veya hizmetin sunulmasının ön şartı olarak ileri sürülmemelidir.[20]

Bu üç unsurun temel alındığı düzenlemede de belirtildiği gibi, "belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar 'battaniye rızalar' olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Örneğin; 'her türlü ticari işlem, her türlü bankacılık işlemi ve her türlü veri isleme faaliyeti' gibi belirli bir konu ve faaliyeti işaret etmeyen rıza beyanları battaniye rıza kapsamında değerlendirilebilecek durumlardır".[21]

Bu konuda Görüşmeci 1'in ifadeleri, kavramın kapsamına ilişkin detay vermektedir:

> Açık rıza zaten Türk Hukukuna ilk kez bu kanunla girdi. Rıza kavramı gibi bir kavramımız var ama açık rıza kavramı KVKK'da ilk kez kullanıldı. Kanun tam anlaşılamayabiliyor, kanunun bazı terimleri tam anlaşılabilir değil mesela ilgili kişi, ben ilk okuduğumda uzun süre ilgili kişiyle ne kast edildiğini düşündüm. Aslında veri sahibi çok daha dilimize oturan bir şey. Kanunda kurumunda kabul ettiği gibi tercüme hataları var. Tam bize uygun değil, hazır giyim gibi aldığımız bir kanun olmuş. O yüzden açık rızayı da kurumun bununla ilgili yayınladığı rehber kitapçıklardan verdiği örneklerden ya da eğitim ve çalışmalarındaki örneklerle anlatabiliyorlar. Daha çok böyle battaniye rıza var mesela her şeyi kabul ediyorsunuz. Hala uygulamadaki rızalar ne yazık ki tam sağlıklı rıza kavramına uymuyor.

Kişisel Verileri Koruma Kurumu tarafından hazırlanan, 100 soruda KVK (Kişisel Verileri Koruma) başlıklı dokümanda, açık rızanın bir hizmet sunumu için koşul haline getirilmesinin hukuka aykırılığından bahsetmektedir ki bu durum çerez kullanım koşullarının kabulünde alındığı iddia edilen açık rıza ile çelişki yaratmaktadır:

> Açık rızanın özgür irade ile açıklanması gerektiğinden, ilgili kişinin açık rızasının alınması,

20 Kişisel Verilerin Korunması Kurumu, 2017.

21 Kişisel Verilerin Korunması Kurumu (t.y.)

> bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir. Örneğin, bir hizmetten yararlanılmasının üyelik şartına bağlandığı yerlerde, üye olmak isteyen ilgili kişinin parmak izinin alınması ve islenmesinin üyelik sözleşmesinin kurulması için zorunluluk olarak öngörülmesi hukuka aykırı olacaktır. Çünkü bu şekilde alınan açık rıza özgür irade ile açık rıza verilmesi ilkesine ve ölçülülük ilkesine aykırı olacaktır. Açık rıza beyanı herhangi bir şekil şartına tabi değildir[22].

Görüşmecilerin ifadelerinden de anlaşılacağı gibi, açık rızanın çerez kullanımı ile ilişkisinde önemli bir karmaşa bulunmaktadır:

> Açık rıza kavramında bir hizmetin verilmesi bir şarta bağlı tutulmaması lazım. Ekstra ayrıcalıklardan yararlanmayabilir. Örnek veriyorum internet sitesinden alışveriş yapacağım beni üye olmaya zorlamaması lazım. Ben sadece bir defa alışveriş yapacağım ama bütün bilgilerimi alıyor… Evet, yasal olarak saklaması gereken verilerim olabilir. Örnek veriyorum fatura düzenleyecektir, faturayı yasal süresi içinde saklaması gerekiyordur bunu anlıyorum. Ama benim iletişim bilgimi saklıyor, telefon numaramı, adresimi, T.C. kimlik numaramı saklıyor... Kişisel Verileri Koruma Kurumu'nun geçtiğimiz dönemlerde verdiği karar var: Hiç kimse bir defa alışveriş yapacağı siteye zorla üye yapılamaz. Alışverişe devam etmek için kabul etmeniz lazım. Kabul ediyorum… Ben, herkes neredeyse kabul ediyordur muhtemelen. Bu, battaniye rıza sizin az önce söylediğiniz ve o çerez kullanımlarına da o şekilde bakılabilir. Zorunlu tutulan bir rıza sağlıklı bir rıza değil… [çerez kullanımını kabul ediyorum seçeneği kabul edilmezse hizmet kullanımı durdurulursa] bu açık rıza değil. O sayfada kalmak için mecbur bırakılıyorum. Tam bir bilişimci olmamakla birlikte bilişimcilerin aktardığı kadarıyla girdiğim internet sitesinin beni hatırlayıp sonra bana küçük hatırlatmalar göndermesi için benim bilgisayarıma bırakılan çerezler. Ben buna rıza vermek zorunda değilim aslında. Ben sadece bir defaya mahsus belki de hiç hatırlamak istemediğim bir siteye girdim... Çok alakasız yerde çok alakasız reklamlarla karşı karşıya kalıyorsun. Bunları görmek istemiyorsun ama seni o site seni mecbur bırakıyor. Bu açık rıza değil, battaniye rıza gibi mecbur bırakıyor sizi o rızayı vermeye (Görüşmeci 1).

Görüşmeci 2'nin çerez kullanım şartlarının kabulü sırasında açık rızanın alınması konusundaki görüşlerinde de benzer ifadeler yer almaktadır. Görüşmeci 2, bu benzerlik dışında, uygulamada açık rıza alınmasının uygun örneklerinde de bahsetmiştir ki bu ifadeler, hukuka uygun uygulamaların da yapılabileceğine işaret etmektedir:

> [Hizmet sunumunun çerez kullanımının kabul edilmesine bağlanması açık rıza olarak]… kabul edilemez. Çünkü çerez kullanımı artık öyle bir hale geldi ki çerez sözcüğü dışında onun açılımına girip te bakıldığını görmedim. Artı bazı yerlerde açılımı yok zaten. O yüzden bu açık rıza olarak kabul edilemez. …sizin izninizle kullanılması son derece doğal ama burada iznin öyle iyi niyetli olması lazım. İşin aslı iyi niyettir. Bazı siteler iyi niyetli değil. Bazıları da iyi niyetli. Bu çerez rızalarında, sayfanın okunabilirliği, görüntüsü, tasarımı önce sizi aydınlatmaya götürüp orda hayır gerek yok diyorsan geri döndürme gibi çok pratik yöntemleri var. Ama iyi örnekleri de var kötü örnekleri de var (Görüşmeci 2).

Tüm uygulamalarda olduğu gibi, çerez kullanım koşullarının açık rızaya uygunluk ölçüsünde sunulmasında da iyi ve kötü örneklerin varlığı kabul edilmelidir. Ancak sorun kişisel verilerin korunması olduğunda, odaklanılması gereken nokta iyi ya da kötü

22 Kişisel Verilerin Korunması Kurumu, 2018a.

niyet çerçevesinden ziyade yasal uygunluk olsa gerektir. Çünkü tüketiciler gözetim karşısında, piyasa kurallarına alıştırılmış halde davranış sergileme eğilimindedirler. Lyon'un da (1997, s. 217) belirttiği gibi "Tüketici gözetimi genellikle, doğrudan veya zorlayıcı değildir, fakat tüketici becerilerini öğretme ve tüketicileri piyasa kurallarına göre davranışı içselleştirmeye özendirme konusunda özellikle başarılı olmaktadır".

Bilişim teknolojileri uzmanı olarak veri denetimi üzerine hizmet veren Görüşmeci 3'ün konu üzerindeki görüşlerine göre, çerez kullanım şartlarının bulunduğu dokümanlar, aydınlatma metni olarak değerlendirilmektedir. Görüşmeci 3, şirketlerin, çerez kullanım şartlarını veri sahibine sunan uygulamaların ya da web sitelerinin, çerez kullanım şartlarının kabulünü açık rızayla aldıklarını düşündüklerini belirtmiştir:

> [Çerez kullanımının kabulünü, açık rıza olarak kabul ediyorlar] …tabi. Bunlar bir aydınlatma metnidir. Şu anda girerseniz birçok kurumda, otellerde KVKK politikasını artı bilgilendirmeyi yapma zorunluluğu var. Hepsinde görürsünüz… Şöyle, ben bunları böyle böyle kullanacağım, benim varlık nedenim bu, kabul etmiyorsan burayı terk edebilirsin diyor. Çünkü var oluş amacı kişisel verilerinin o kısmıyla, …harcama kalemlerinle, ne kadarlık mala baktığınla ilgileniyordur. Artık pazarlama için sen bir deneksin, teklifte bulunacak sana (Görüşmeci 3).

Görüşmeci 3, uygulamada çerez kullanımının kişiyi pazarlama için bir denek konumuna indirgediğini ifade etmektedir. Gözetleme sistemlerinin kendilerini gizleme becerilerinin gitgide arttığını, gözetimi açıktan yapsa bile her geçen gün daha sistematik ve zekice yollara başvurduğu (Lyon, 2006, s. 12) bilinmektedir. Bu duruma bir de bireylerin neredeyse her gün kullandıkları bilişim teknolojileri aracılığı ile kişisel verilerinin gönüllü dağıtıcısı haline geldikleri gerçeği eklenince, maruz kaldıkları incelikli gözetim sonucunda (Güven, 2011, s. 173), bireyler gönüllü olmasalar bile kişisel bilgilerini şirketlere sunmuş olmaktadırlar.

Sonuç

21. yüzyılın en önemli gelişmelerinden biri olan internet ve teknolojik araçlar gündelik yaşamın önemli bir parçası haline gelirken, zaman ve mekân sınırlarını ortadan kaldırarak, bilgiye erişimi hızlı ve ulaşılabilir kılmıştır. Kişiler, internetin ilk dönemlerinde yalnızca kendisine sunulan bilgiye erişebilirken, günümüzde içerik üreten kullanıcılar haline dönüşmüş ve bu alandaki etkileşime doğrudan katılır olmuştur. İnternet ağlarının yaygınlaşması ve internet ortamındaki genişlemeye paralel olarak dijital gözetim de giderek yaygınlaşmış, hızlıca ve hissettirmeden, hayatımızın pek çok alanında denetim mekanizması haline gelmiştir. Politik ve ekonomik iktidarlar, kullanıcıların internette geçirdikleri zamanlarda bıraktığı dijital izleri anlamlandırarak elde etmiş oldukları kişisel verileri, kendi çıkarları doğrultusunda kullanarak, çoğu zaman kişilerin mahremiyetini açıkça ihlal etmektedir. Dijital ortamlarda kişiler kendilerine ait mahremiyet bölgelerini koruyamamakta ve kişisel verileri üzerindeki kontrolü kaybetmektedir. Böylelikle kişisel verilerin korunması özel hayatın gizliliği bağlamında daha da önemli bir konuma gelmektedir.

Derinlemesine görüşmelerden elde edilen verilerin, mevzuatla karşılaştırmalı analizi sonucunda Türkiye'de kişisel verilerin güvenliği konusunda yaşanan sorunların, veri korumadaki bilgi eksikliğinin ve veri aktarımının kontrolsüzlüğünün yanı sıra veri sahibinin verilerini paylaşmadaki cömertliğinin de sonuçları olduğu bulgulanmıştır. Kişisel verilerin kullanımı ile ilgili olarak ülkemizdeki yasal mevzuatın henüz kişiler ve kanun uygulayıcıları tarafından yeterince bilinmemesi, bu alandaki farkındalığın da artırılmasının gerekliliğini göstermektedir.

Derinlemesine görüşmelerde, veri sorumlularının veri güvenliğini sağlama konusundaki yetkinlik düzeyleri de veri güvenliğinin sağlanmasında sorunlu alanlardan birisi olarak ifade edilmiştir. Öncelikle kişisel verinin kapsam ve içeriğinin yeterince bilinmiyor olmasının yol açtığı sorunları aktaran görüşmeciler, veri sorumlularının denetimlerindeki aksaklıkları da alan gözlemleri üzerinden aktarmışlardır. Ayrıca teknik alt yapı eksikliğinin de veri güvenliği için önemli açıklara neden olduğu da yine görüşmecilerin ifadeleri arasında yer almaktadır. Veri sorumlularının, veri işleyicilerin ve alt yapı uygunluğunun denetlenmesi için gerekli koşulların henüz oluşmadığı da görüşmeciler tarafından ifade edilmiştir.

Devletin kişisel verileri korurken, politik iktidar olarak kendisinin ve ekonomik iktidar olarak da şirketlerin çıkarlarını gözetmesi, konuyu giderek daha karmaşık hale getirmektedir. Kişisel verilerin korunması ve kişisel verilerin güvenliğinden sorumlu olan veri sorumlularının yükümlülükleri Kişisel Verileri Koruma Kanunu'nda netleşmiş gibi görünse de uluslararası düzeyde kişisel verilerin korunmasıyla ilgili yeni düzenlemeler (yönetmelik-tüzük) yapılmaya devam edilmektedir. Kişisel Verileri Koruma Kanunu'nun 4. Maddesinde yer alan kişisel verilerin işlenmesine ilişkin temel ilkeler, Avrupa Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine ve Avrupa Birliği Veri Koruma Direktifine paralel biçimde düzenlenmiştir. 04.05.2016 tarihinde Avrupa Birliği Resmi Gazetesinde yayınlanan ve 24.05.2018 tarihinde yürürlüğe giren Avrupa Birliği Veri Koruma Tüzüğü'nün 51. Maddesinin 1.fıkrası, üye devletler tarafından Tüzüğün uygulanması ve izlenmesinden sorumlu olacak bir denetim mekanizmasının oluşturulması gerektiğine işaret etmektedir. Yine aynı Tüzüğün 52. Maddesine göre de denetim makamının görevlerini yerine getirirken tamamen bağımsız olması gerektiği belirtilmiştir. Tüzük uyarınca denetim makamı herhangi bir dış etkenden bağımsız hareket etmeli ve herhangi bir kimseden talimat almamalıdır. Kişisel Verileri Koruma Kurumu 2016 yılında Başbakanlığa bağlı olarak kurulmuştur. Ancak 15 Temmuz 2018 tarihli ve 30479 sayılı Resmi Gazetede yayımlanan "Bakanlıklara Bağlı, İlgili ve İlişkili Kurum ve Kuruluşlar ile İlgili 2018/1 Sayılı Cumhurbaşkanlığı Genelgesi" uyarınca Adalet Bakanlığı'na bağlanmıştır. Avrupa Birliği Veri Koruma Tüzüğü'nde yer alan "denetim mekanizmasının bağımsız olması gerektiği" vurgusu, bu noktada tekrar hatırlanmalıdır. Adalet Bakanlığı da diğer devlet kurumları gibi kişisel veri toplayan bir kurumdur ve bu noktada veri güvenliği adına denetlenmesi gerekmektedir. Bu denetimin kendisine bağlı bir kurum tarafından yapılıyor olması, soru işaretlerine neden olmaktadır. Öte yandan, diğer kurum ve kuruluşlardaki veri sorumlularının faaliyetlerinin herhangi bir bağımsız üst kurul tarafından denetlenmemesi ya da bu bağımsız üst kurula karşı sorumlu olmaması,

bu alanda endişelere neden olmaktadır. Devlet, vatandaşları hakkında giderek daha çok bilgi istemekte iken, şirketler ise daha çok potansiyel müşteri talep etmektedir. Devletler daha çok sağlık, güvenlik ve siyasal alanda veri toplarken şirketler, pazarlama ve reklam sektörlerinde kullanılabilecek verilere iştah kabartmaktadır. Bu nedenledir ki dijital gözetim ve veri gözetimi daha önce hiç olmadığı kadar yoğunlaşacak, bitmek tükenmek bilmeyen bir veri avını da beraberinde getirecektir. Bu noktada, Avrupa Birliği uyum sürecinde olan ülkemizde de kişisel verilerin korunmasında etkin bir biçimde yer alacak, veri sorumlularının faaliyetlerini bağımsız bir şekilde denetleyecek üst bir kurulun varlığına gerek duyulmaktadır.

İnternet ortamında verilen hizmetlerin, çerez kullanımı kabulü koşuluna bağlanmış olması, Kişisel Verileri Koruma Kanunu'nda yer alan açık rıza ile çelişik durumlar yaratmaktadır. Derinlemesine görüşmelerden elde edilen ifadelerde de çerez kullanım koşullarının kabulü sonrasında, elde edilen kişisel verilerin kullanım alanındaki belirsizliğin kişisel verilerin güvenliğini tehlikeye atan sonuçlara neden olduğu görüşü hakimdir. Öte yandan hizmet sunumunun koşula bağlanmış olması durumunun da açık rızaya aykırı olduğu, çerezler aracılığı ile elde edilen kişisel verilerin çoğu zaman battaniye rızayı dayattığı da yine görüşmeciler tarafından ifade edilmiştir.

Kişisel Verileri Koruma Kanunu'na göre, internet siteleri ya da mobil uygulamalar tarafından yayınlaması zorunlu olan aydınlatma metinleri ya da çerez politikaları hizmetin kullanılacağı ortamda sade, okunabilir bir biçimde, net olarak açık rızaya mahal verecek şekilde (onaylıyorum-onaylamıyorum biçiminde) verilmelidir. 'Onaylamıyorum' seçeneğini tercih eden kişilerin de hizmeti kullanmaya devam etmesi, hizmeti kullanmayı zorlaştırıcı herhangi bir yaptırımla karşılaşmaması gerekmektedir. Herhangi bir yazılım ya da mobil uygulamanın veri toplama ayarları, kişiler o yazılımı kullanmaya başlamadan açık olmamalı, veri toplama işlemi kişinin açık rızası alınmadan devreye girmemelidir. Ülkemizde faaliyet gösteren birkaç şirket sınırlı da olsa internet sitelerinde kişisel verilerin elde edilmesinde müzakereye yer vermiştir. Ancak bu şirketler de verinin toplanmasında seçenek olarak sundukları veri kapsamının derecesini kendi lehlerine düzenlemiştir. Kişisel verilerin toplanmasında, veriyi elde etme sürecinde müzakereli bir sistem işletilmeli ve bu sistem, toplanacak kişisel verinin kapsamının arttırılmasından ziyade azaltılması yönünde çalışmalıdır. Ayrıca verilen izinlerin en üst düzeyde veri toplamayı sağlayacak biçime değil, mümkün olan en az miktarda veri toplamayı sağlayacak biçime dönüştürülmesi, çerez kullanımında açık rızaya dayanma ilkesinin uygulanabilirliğini kısmen de olsa sağlayabilecektir.

Kaynakça

Arslantaş-Toktaş, S., Binark, M., Dikmen, E. Ş., Küzeci, E., ve Özaygen, A. (2012). *Türkiye'de Dijital Gözetim: TC Kimlik Kartlarından E Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi.* İstanbul: Alternatif Bilişim Derneği.

Baştürk, E. (2016) *Gözetimin Soykütüğü: Faucault'dan Deleuze'e Postmodern Bir Arkeoloji.* İstanbul: Kalkedon Yayıncılık.

Bauman, Z. ve Lyon, D. (2016). *Akışkan Gözetim* (E. Yılmaz, Çev.). İstanbul: Ayrıntı Yayınları.

Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* UK: Cambridge University Press.

Çakır, M. (2015). *İnternette Gösteri ve Gözetim. Eleştirel Bir Okuma.* Ankara: Ütopya Yayınevi.

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H., ve Öneş. O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. *International Journal Of Informatics Technologies, 10*(2), 177-184.

Güven, S. K. (2011). Gözetimin Toplumsal Meşruiyeti. H, Köse (Der.). *Medya Mahrem Medyada Mahremiyet Olgusu ve Transparan Bir Yaşamdan Parçalar* içinde (s. 173-198). İstanbul: Ayrıntı Yayınları.

Karakehya, H. (2009). Gözetim ve Suçla Mücadele: Gözetimin Tarihsel Gelişimi İle Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 58*(2), 319-357.

Kırlıdoğ, M ve Fidaner, I. B. (2012). Derin Veri Analizi: İnternet'teki Temel Gözetim Aracı. *XIV. Akademik Bilişim Konferansı, 1-3 Şubat 2012, Uşak, Türkiye, Bildiriler* içinde (s.1015-1018).

Lyon, D. (1997). *Elektronik Göz* (D. Hattatoğlu, Çev.). İstanbul: Sarmal Yayınevi.

Lyon, D. (2006). *Gözetlenen Toplum: Günlük Hayatı Kontrol Etmek (*G. Soykan*,* Çev.). İstanbul: Kalkedon Yayıncılık.

Lyon, D. (2013). *Gözetim Çalışmaları* (A. Toprak, Çev.). İstanbul: Kalkedon Yayıncılık.

Meng, W. Ding R., Chung S. P., Han S., ve Lee W. (2016) The Price Of Free: Privacy Leakage In Personalized Mobile In-Apps Ads, 23nd Annual Network and Distributed System Security Symposium, NDSS, San Diego, California, USA, February, s.1-15.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., ve Borgthorsson, H. (2014). Leakiness And Creepiness in App Space: Perceptions Of Privacy And Mobile App Use. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, s.2347-2356.

Talay, Ö. (2018) *Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi* (Yayımlanmamış Yüksek Lisans Tezi). Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya.

Turow, J. (2015*). İzleniyoruz* (M. Benveniste, Çev.). İstanbul: Hil Yayın.

Van Dijk, J. (2016). *Ağ Toplumu* (Ö. Sakin, Çev.). İstanbul: Kafka Yayınevi.

İnternet Kaynakları

Alternatif Bilişim Derneği (2013). *Veri Korumaya Giriş* [Broşür]. 22 Aralık 2017 tarihindehttps://ekitap.alternatifbilisim.org/files/veri_korumaya_giris_edri_paper_06_tr.pdf adresinden edinilmiştir.

Gurria, A. (2008). Closing remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy. 15 Aralık 2017 tarihinde http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingoclosingremarksbyangelgurriaoec.htm adresinden erişilmiştir.

Joler, vd., (2015) Metadata Investigation: Inside Hacking Team. 15 Aralık 2017 tarihinde https://labs.rs/en/metadata adresinden edinilmiştir.

Kişisel Verilerin Korunması Kanunu. (2016, 7 Nisan). Resmi Gazete (Sayı:29677) http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf adresinden 1 Şubat 2019 tarihinde edinilmiştir.

Kişisel Verilerin Korunması Kurumu. (2017). 6698 Sayılı *Kişisel Verilerin Korunması Kanununun Uygulanmasına Yönelik Soru Cevaplar*. Ankara: KVKK Yayınları. https://kvkk.gov.tr/yayinlar/6698%20SAYILI%20K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNUNUN%20UYGULANMASINA%20Y%C3%96NEL%C4%B0K%20SORU%20VE%20CEVAPLAR.pdf adresinden 15 Şubat 2019 tarihinde edinilmiştir.

Kişisel Verilerin Korunması Kurumu. (2018a). 100 Soruda Kişisel Verilerin Korunması Kanunu. Ankara: KVKK Yayınları. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf adresinden 15 Şubat 2019 tarihinde edinilmiştir.

Kişisel Verilerin Korunması Kurumu. (2018b, Mart). *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*. Ankara: KVKK Yayınları. 1 Şubat 2019 tarihinde https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/0517c528-a43d-49f5-b1eb-33dc666cb938.pdf adresinden erişilmiştir.

Kişisel Verilerin Korunması Kurumu. (t.y.). Açık Rıza Alırken Dikkat Edilecek Hususlar. https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar adresinden 15 Şubat 2019 tarihinde edinilmiştir.

Klein, R. (1972). The Report of the Committee on Privacy. https://onlinelibrary.wiley.com/doi/full/10.1111/j.1467-923X.1972.tb02068.x adresinden 10 Nisan 2018 tarihinde edinilmiştir.

Martin T. (2016). Big Data vs. Metadata: What's the Diffrence?. 15 Aralık 2017 tarihinde https://www.linkedin.com/pulse/big-data-vs-metadata-whats-difference-toby-martin adresinden edinilmiştir.

SHARE LAB (2015a). Invisible Infrastructures: Data Flow. https://labs.rs/en/invisible-infrastructures-data-flow adresinden 15 Aralık 2017 tarihinde edinilmiştir.

SHARE LAB (2015b). Invisible Infrastructures: Online Trackers. https://labs.rs/en/invisible-infrastructures-online-trackers adresinden 15 Aralık 2017 tarihinde edinilmiştir.

TBD-Kamu-BİB, Kamu Bilişim Platformu X. "Kişisel Verilerin Korunması." (2008). II. Çalışma Gurubu 1. Bölüm "Kişisel Verilerin Korunması ya da Kişisel Verilerin İşlenmesi Karşılığında Bireyin Korunması" 22 Aralık 2017 tarihinde https://eski.tbd.org.tr/usr_img/cd/kamubib17/raporlarPDF/RP2-2008.pdf adresinden edinilmiştir.

W3Techs. (t.y.). Usage Statistics of Cookies for Websites. https://w3techs.com/technologies/details/ce-cookies/all/all adresinden 5 Şubat 2019 tarihinde edinilmiştir.