T. C.
B A H Ç E Ş E H İ R Ü N İ V E R S İ T E S İ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÜKSEK LİSANS PROGRAMI

SOSYAL MEDYA PAZARLAMA FAALİYETLERİNİN ARTIŞI VE VERİ TABANINDA TUTULAN KİŞİSEL VERİLERİN KULLANICIYA ETKİLERİ

Yüksek Lisans Tezi

EFE ÇETİNTAŞ

İSTANBUL, 2019

T. C.
B A H Ç E Ş E H İ R Ü N İ V E R S İ T E S İ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÜKSEK LİSANS PROGRAMI

SOSYAL MEDYA PAZARLAMA FAALİYETLERİNİN ARTIŞI VE VERİ TABANINDA TUTULAN KİŞİSEL VERİLERİN KULLANICIYA ETKİLERİ

Yüksek Lisans Tezi

EFE ÇETİNTAŞ

Tez Danışmanı: DR. SABA GAMZE ORAL

İSTANBUL, 2019

T.C.

BAHÇEŞEHİR ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

.....MBA (Tr)..... YÜKSEK LİSANS PROGRAMI

Tezin Adı: Sosyal Medya Pazarlama Faaliyetlerinin Artışı ve Veri Tabanında Tutulan Kişisel Verilerin Kullanıcıya Etkiler

Öğrencinin Adı Soyadı: Efe GETİNTAŞ

Tez Savunma Tarihi: 29.05.2019

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğu Sosyal Bilimler Enstitüsü tarafından onaylanmıştır.

Doç. Dr. Burak KÜNTAY
Enstitü Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları yerine getirmiş olduğunu onaylarım.

Program Koordinatörü

Bu Tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

	Ünvan/Ad	İmza
Tez Danışmanı	Dr. Saba Gamze Oral	
Üye	Dr. Öğr. Görevlisi Kazım Selçuk Tuzcuoğlu	
Üye	Doç. Dr. Ceyda Aysuna Türkyılmaz	

ÖZET

SOSYAL MEDYA PAZARLAMA FAALİYETLERİNİN ARTIŞI VE VERİ TABANINDA TUTULAN KİŞİSEL VERİLERİN KULLANICIYA ETKİLERİ

Efe Çetintaş

SOSYAL BİLİMLER ENSTİTÜSÜ İŞLETME YÜKSEK LİSANSI

Tez Danışmanı: DR.SABA GAMZE ORAL

Mayıs 2019, 83 sayfa

Günümüzde üretilen dijital veri dünyanın her yerinde üstel bir artış göstermektedir. Veri büyük miktarda, hızlı ve çok çeşitli üretilmektedir. Bu tip veriler büyük veri olarak adlandırılır ve bunların işlenmesi için spesifik büyük veri uygulamalarının geliştirilmesi zorunlu hale gelmiştir. Büyük veri teknolojilerinin etkin kullanımı iş süreçlerini iyileştirebilir, daha verimli çalışılmasını sağlar ve hizmet kalitesine olumlu etki eder. Büyük veri hem ekonomik hem sosyolojik açıdan büyük yararlar sağlama potansiyeline sahiptir. Büyük veri her bir birey hakkında daha önce hayal dahi edilemeyen bilgilerin elde edilmesini sağlamıştır. Ancak bu durum verilerin mahremiyeti konusundaki kurallar konusunda bazı sorunlar ortaya çıkarmaktadır. Büyük veri eğer gelişecek ve yaygınlaşacaksa mahremiyet konusundaki kaygıları gidermek mecburiyetindedir. Bu doğrultuda, 2012 yılından itibaren çoğu ülke hem güttüğü politikalarda hem de yasalarında büyük verinin gelişiminin gerekli kıldığı düzenlemeler yapmıştır. Bunun sebebi de büyük verinin adil veri işleme ilkeleri üzerinde gösterdiği büyük etkilerdir. Modern mahremiyet düzenlemeleri de bu ilkeler çerçevesinde şekillenmektedir.

Anahtar kelimeler: sosyal medya pazarlaması, veri tabanı, kişisel veri

ABSTRACT

THE INCREASE OF SOCIAL MEDIA MARKETING ACTIVITIES AND THE EFFECTS OF PERSONAL DATA IN DATABASE ON THE USER

Efe Çetintaş

SOCIAL SCIENCES INSTITUTE MBA

Thesis Supervisor: DR.SABA GAMZE ORAL

May 2019, 83 pages

Nowadays, digital data is exponentially increasing all over the world. Data is produced in big amounts, in a fast manner and in various forms. Such data is called big data and it has become mandatory to develop specific big data applications for processing them. The efficient use of big data technologies can improve business processes, ensure more efficient work and have a positive impact on service quality. Big data has the potential to provide great benefits both economically and sociologically. The big data provides information about each individual in a way that could not be imagined before. But this raises some problems in terms of the rules on the privacy of the data. For the development and dissemination of big data, concerns about privacy must be addressed. Accordingly most countries have made arrangements in the policies and laws required by the development of big data since 2012. This is due to effects of big data on fair data processing. Modern privacy regulations are created within the framework of these principles.

Keywords: social media marketing, database, personal data

İÇİNDEKİLER

KISALTMALAR

ABD	: Amerika Birleşik Devletleri
BTK	: Bilgi Teknolojileri ve İletişimi Kurumu
CCDP	: Communications Capabilities Development Programme
CDT	: Democracy and Technology Center - Demokrasi ve Teknoloji Merkezi
FPC	: First Party Cookie – Birinci Parti Çerez
GCHQ	: Government Communication Headquarters - Hükümet İletişim Merkezi
IMP	: Interception Modernisation Programme
KVKK	: Kişisel Verilerin Korunması Kanunu
NSA	: National Security Agency - Ulusal Güvenlik Dairesi
OECD	: Ekonomik Kalkınma ve İşbirliği Örgütü
RF	: Radyo frekansları
TCK	: Türk Ceza Kanunu
TPC	: Third Party Cookies - Üçüncü Taraf Çerezler
UWB:	Ultra geniş bant

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

1. GİRİŞ

İnsanlık tarihine bakıldığında, ne zaman bir yenilik ortaya çıkarıldıysa bu yeniliğin tartışmalara konu olduğu görülür. Örneğin matbaa icat edildiğinde daha sonraki nesillerin ezber yeteneklerini kaybedecekleri ve çok bilmeye gerek duymayacakları tartışılmıştır. İkinci Dünya Savaşı sonrası dönemde ise nükleer teknolojiler ve bunların ileriki dönemlerdeki etkileri ile nükleer silahlar konusundaki etik kaygılar tartışma konusu olmuştur. Bertrand Russell bu durumun bilgelikteki ilerlemenin bilgideki büyümenin gerisinde kaldığı için yaşandığını öne sürmüştür. Bu doğrultuda, bilgi geliştiğinde ancak insan iradesi ve duygu durumu aynı gelişmişliğe gelemediğinde bu ilerlemeler tehlikeli addedilebilir. Ancak duyulan bu kaygılar gelişmeyi ve yeniliği yok saymak anlamına gelmemelidir. Zaten bilgi ve iletişim teknolojilerine (BİT) bakıldığında, bunların halihazırda gündelik yaşamda yer aldığı ve etik kaygıların bunların yayılımını etkilemediği görülmektedir.

Bu teknolojilerdeki gelişmeler iletişimi son derece hızlandırmış ve hayatı da kolaylaştırmıştır. Gittikçe daha rafine hale gelen bu yenilikler gün geçtikçe daha değerli hale gelmektedirler. Ancak, bu güçlü teknolojik gelişmeler kötü amaçlarla kullanıldıklarında çok önemli olumsuz sonuçlar getirebileceklerdir. Günümüzde her şey dijitalleşmekte, veriler son derece yüksek hızlarda akmakta, toplam veri daha önce hayal edilemeyecek miktarlara ulaşmakta ve bu veri çok çeşitli olmaktadır. Büyük veri teknolojileri bu verileri üretildikleri hızda analiz edebilmektedirler. Geliştirilen algoritmalar yapılacak çıkarımları daha isabetli hale getirmekte, alınacak kararlara yardımcı olmakta, göz önünde olmayan ayrıntıları yakalamakta ve iş süreçlerinde otomasyonu mümkün kılmaktadır. Bu gelişmeler işlerin daha düşük maliyet ile yürütülmesini, ürün ve hizmetlerin müşteriye daha kaliteli şekilde ulaşmasını ve büyük ölçekte de ekonomide büyümeyi mümkün kılmaktadır.

Büyük veri hem sosyal hem ekonomik açıdan önemli getirilere sahiptir. Bu faydalara ne devletler ne de şirketler seyirci kalabilmektedir. Hem şirketlerin verilerinin hem de kamu verilerinin büyük veri ile işlenmesi dolayısıyla popüler bir konudur. Bu tarz uygulamalar Amerika Birleşik Devletleri (ABD) ve Avrupa Birliği'nde (AB) giderek

yayılmaktadır. ABD'nin en büyük BİT firmalarına ev sahipliği yaptığı, AB'nin ise çok büyük bir kişisel veri pazarı olduğu düşünüldüğünde bu durum son derece normal görülebilir. Özel sektör büyük veri kullanımına geçerken rekabette öne çıkmak ve genel olarak ticari fayda sağlamak amacı gütmektedir. Kamu ise bu uygulamaları benimserken siyasi hedefleri esas almaktadır. Hem kamu unsurları hem de özel unsurlar farklı amaçlarla da olsa büyük verinin kullanımına ve geliştirilmesine eğilmişlerdir. Ancak, çok faydalı olduğu su getirmez bir gerçek olan büyük veri, içerdiği çok miktarda kişisel veri sebebiyle veri mahremiyeti kaygılarına yol açmaktadır. Bu kaygı ile hareket eden İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD), AB ve ABD gibi tepe kurumlar, büyük verinin kullanımı düzenlemek istemişlerdir. Hızla geliştirilen bu çalışmalar ile çeşitli düzenlemeler öngörülmüştür. Büyük veri henüz yeni bir kavram olmakla birlikte, yaratmakta olduğu mahremiyet kaygıları son derece ciddi görülmektedir. Dolayısıyla bunlara hızla çözümler önerilmesi önemlidir.

Kişisel veri kavramının tanımı 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3/1. maddesinde yapılmıştır ve "kimliği belirli veya belirlenebilir gerçek kişiye dair her çeşitten bilgi" olarak gösterilmiştir. Avrupa İnsan Hakları Sözleşmesi ile Avrupa İnsan Hakları Mahkemesi'nin yapmış oldukları tanımlarda bakıldığında bu tanımların da benzer şekillerde ortaya konmuş oldukları görülebilir (Başalp, 2004: 22). Kişisel veri olarak kabul edilen bilgiler kişilerin resmi kimlik bilgilerini, eğitim ve sağlık konusundaki kayıtlarını, güvenlik konusundaki bürokratik kayıtları, kişilerin yapmış oldukları harcamaları, sosyal medyada paylaştıkları resim ve fotoğrafları ve siyasi veya dini özel bilgileri kapsamaktadır. Bu kapsamdaki veriler hassas olan ve olmayan olarak iki başlıkta incelenmektedir. Bu konuyu ele alan Avrupa Birliği Veri Koruma Direktifi 8. maddesine göre hassas bilgiler etkin köken, sağlık verileri, cinsel yaşam, inanç, fikir gibi öğelerdir ve bunların işlenmesi yasaktır.

Hassas verilerin tanımı farklı ülkelerde farklı şekillerde yapılabilir. Örneğin Polonya'da sendika üyelikleri ve genetik veriler hassas veridir, İzlanda'da ten rengi, cinsel konular, alkol veya uyuşturucu madde kullanımı, Finlandiya'da sosyal refah ve cinsel kimlik, İngiltere'de ise mahkûmiyet kararları hassas veri olarak ele alınmaktadır. Buna ek olarak, biometrik verilerin önemli hassas verilerden olduğu söylenebilir. Bu konu hakkındaki Slovenya Kişisel Veri Koruma Kanunu'nun 2004'te biometrik özellikleri insanların tamamının fiziksel, fizyolojik ve davranışsal özellikleri olarak tanıdığı

görülmektedir. Biometrik verileri ilgilendiren aktiviteler olarak ise parmak izlerinin kullanımı, parmak çizgilerinin kaydı, iris taraması, retina taraması, yüz ile alakalı özelliklerin kaydı, bir kulağın kaydı, DNA taraması ve yürüme tipi gibi özellikler verilmiştir (m. 6/21) (Kaya, 2011: 319). Yukarıdaki bilgiler ışığında, kişisel verinin kişinin belirlenmesini sağlayan her türlü veri olarak özetlenmesi uygun olacaktır (Kılınç, 2012: 1095).

2. SOSYAL MEDYADA PAZARLAMA

Çalışmanın bu bölümünde sosyal medya pazarlaması ele alınacaktır. Sosyal medyanın tanımı yapılacak, sosyal medya ve geleneksel medya arasındaki farklar ortaya konmaya çalışılacak, sosyal medya pazarlaması süreci, sosyal medya pazarlamasının faydaları ve sosyal medya pazarlaması uygulamaları açıklanmaya çalışılacaktır.

2.1 SOSYAL MEDYANIN TANIMI

Sosyal medya kavramını anlayabilmek için kavramın içinde yer alan iki kelimeyi dikkatli bir şekilde incelemek gerekmektedir. Medya kavramı çeşitli iletişim teknolojileri sayesinde fikir ve bilginin farklı kaynaklardan insanlara ulaşması şeklinde özetlenebilecek bir alanı göstermektedir. Sosyal kavramı ise insanlar arasındaki ilişki temelinde ortaya çıkan etkileşim alanıyla yakından ilgilidir. Sosyal medya ise bireylerin çeşitli araçlarla her zaman etkileşim olanağına sahip oldukları iletişim alanıdır (Neti, 2011: 2).

Sosyal medya alanına dahil olan kullanıcılar bulundukları alanda içerik üretebilmekte ve olanaklar ölçüsünde değişiklik yapabilmektedir. Bu durum Web 2.0 adı verilen internet tabanlı teknoloji sayesinde mümkün olabilmektedir. 2014 yılında ortaya çıkan Web 2.0 adı verilen bu kavram dünyada bulunan bütün internet kullanıcılarına Web'i bir platform olarak kullanabilme olanağı tanımıştır. Platformu ortaklaşa bir alan olarak kullanan kullanıcılar içerik oluşturabilmekte ve çeşitli değişiklikler yapabilmektedir. Platformlarda yer alan içeriğin büyük bir kısmını kullanıcılar üretmektedir. Sosyal medyanın ortaya çıkması ve gelişimi açısından Web 2.0 önemli bir konumda bulunmaktadır. Ancak sosyal medya ile Web 2.0'ın farklı kavramlar olduğu unutulmamalıdır (Kaplan ve Haenlein, 2010: 61).

Web 2.0'ın üç adet işlevi bulunmaktadır (Kaplan ve Haenlein, 2010: 61):

a - Adobeflash (Etkileşimi ortaya çıkartan yöntem)

b - RSS (Çok Basit Birleştirme-Yapılan paylaşımlardan hemen haberdar olma olanağı)

c - Ajax (Asenkron-Eşzamana sahip olmayan javascript)

Sosyal medya söz, yazı, görsel içerikler, video ve ses olanakları gibi uygulamaları kullanarak içerik oluşturmayı, paylaşabilmeyi, iletişim kurabilmeyi sağlayan etkileşim olanağına sahip medya türüdür. Sosyal medyanın en önemli hedeflerinden biri insanların katılımını sağlayabilmektir. İnsanların katılımını teşvik etmek için dört yol bulunmaktadır (Safko ve Brake, 2009: 3):

d - İletişim, mesajlaşma, sohbet edebilme olanağının olması (Örneğin, Twitter),

e - İşbirliklerine açık olması (Örneğin, Wikipedia),

f - Eğitim gibi faydalı olanaklara sahip olması (Örneğin, ses kayıtlarından oluşan podcastler),

g - Eğlence (Örneğin, Youtube).

Kullanıcı tarafından oluşturulan içerikler (UGC-User Generated Content) sosyal medyanın çıkış noktasını oluşturmaktadır. Oluşturulan içerikleri genellikle gönüllülük esasıyla, ücret almadan yapan kullanıcılar sosyal medyanın merkezindedir. Onların ürettiği bütün içerikler sosyal medyayı anlamlı hale getirmektedir. Atılan tweetler, üretilen görseller, sesler, videolar ve çeşitli içeriğe sahip yazılar içerik kapsamında değerlendirilmektedir Sosyal medya Web 2.0 teknolojisi temelinde kurulmuş, içeriğin kullanıcılar tarafından oluşturulmasına izin veren, yine kullanıcılar tarafından belirli kurallar çerçevesinde değişime olanak tanıyan, etkileşime izin veren medya kurallarına sahip olan; talepleri, beklentileri ve müşterileri bir araya getiren internet uygulamaları bütünüdür (Neti, 2011: 5).

İşletmelerin sosyal medya kullanımları neredeyse sosyal medyanın ortaya çıkmasıyla başlamıştır. İşletmeler kendi tanıtımları, pazar araştırması, müşteriyle etkileşim gibi birçok olanağa sahip olmak için sosyal medya kullanmaktadır. Bunu yaparken çok büyük iletişim harcamalarından kaçınabilmektedir. Çünkü sosyal medya kendine özgü bir pratiklik sağlamaktadır. Sosyal medya müşterileri dinleme açısından gerekli ortamı sunar, ancak bu olanağı iyi bir şekilde kullanan işletmeler verimli sonuçlara ulaşabilmektedir. Yaptığı faaliyetlerle ilgili en hızlı geri dönüşler sosyal medya üzerinden olmaktadır. Bir ürün üreten işletme, müşteri deneyimiyle ilgili önemli sonuçları ilk olarak sosyal medyadan elde edecektir (Safko ve Brake, 2009: 7).

Sosyal bir varlık olan insan, iletişim kurarak varlığını sürdürmüştür. Geçmişte çok sayıda iletişim yöntemi ve aracı kullanılmıştır. Sosyal medyanın ortaya çıkmasıyla birlikte iletişim konusunda insanlık yeni bir döneme giriş yapmıştır. Milyonlarca insanın aynı platform üzerinde yer alarak her gün iletişim amaçlı olarak kullandığı bu internet uygulamalar bütünü, kendine özgü iletişim sistemiyle insanların sosyal hayatlarını doğrudan etkilemektedir. Sosyal medya sadece Facebook'a fotoğraf yükleme etkinliği olarak kabul edilmemelidir. Sosyal medya kişisel bir kullanım alanı olma durumundan çıkalı çok olmuştur. Kurallarıyla, kurumsal dünyasıyla kendine özgün yapısını insanlara dayatır hale gelmiştir. Bireylerin ve işletmelerin bir arada olduğu sosyal medya mecralarını sadece içerik paylaşma araçları olarak görmek yanlış bir yaklaşım olacaktır. Çok yüksek sayılara ulaşan sosyal medya kullanıcılarının varlığı sayesinde işletmeler ve kurumlar da bu alanlara yüksek ilgi duymak zorunda kalmışlardır. Artık birçok oluşum paydaşlarıyla iletişim kurabilmek için sosyal medya araçlarını kullanmaktadır (Şahin, Çağlıyan ve Başer, 2017: 68).

2.2 GELENEKSEL MEDYA VE SOSYAL MEDYANIN FARKI

Geleneksel medya araçları belirli kurallarla oluşturulmuş, genel olarak etkileşime olanak vermeyen, tek yönlü iletişim ve haberleşme olanağının olduğu medya platformlarının oluşturduğu ağdır. Artık bu araçlar eskisi gibi etkin değildir. Geleneksel medya araçları ticari kaygılardan ötürü insanları memnun etmeyecek konumlara yerleşmiş durumdadır. Sosyal medya ise aksine etkileşime izin veren yapısı ve şeffaf niteliğiyle insanları bir araya getirme amacı gütmektedir. Sosyal medya ile yapılan pazarlama çalışmalarının temelinde birilerine bir şeyler anlatmak yoktur. Karşıdakini dinleme ve ona göre bir cevap oluşturma hedeflenenler arasındadır. Pazarlama söz konusu olduğunda işletme kendi özgün niteliklerini göz önünde bulundurarak sosyal veya geleneksel medyada en gerekli araçlara yönelmelidir. Ürünün tanıtımı ve işletme imajını güçlendirmede en uygun medya araçlarına başvurmak çok önemlidir (Yayla, 2010: 61).

İşletmeler varlıklarını sürdürmek için en iyi pazarlama stratejisini seçmek zorundadır. Bazı işletmeler çağı yakalayamadıkları için geleneksel pazarlama anlayışıyla kendisini sınırlamaktadır. Ancak var olduğu pazarın içinde bulunan tüketiciler geleneksel pazarlama alanının dışında yer alıyorsa o tüketici kitlesine ulaşabilmek çok zor

olacaktır. Bu da müşteri kaybı anlamına gelmektedir. Sosyal medya araçlarını ekin bir şekilde kullanarak sosyal medya pazarlaması yapmak tüketicinin sınırsız bilgiye ulaşımını sağlamaktadır. Tüketici kullandığı, satın aldığı ürün ve hizmetle ilgili yaşadığı deneyimleri sosyal medya araçlarında paylaşarak işletmenin ihtiyaç duyduğu değerli bilgileri üretmektedir. Tüketici aynı zamanda fikir ve düşünceler üreterek diğer insanlarla iletişime girdiği için bireysel tatminler de elde etmektedir. Tatmin ve ihtiyaçlar var olduğu sürece bu döngü devem edecektir. Tüketiciden gelen cevapları ve talepleri sosyal medya araçlarını etkin bir şekilde kullanan bir işletme doğru ve hızlı bir şekilde değerlendirebilmektedir. Sunduğu hizmetlerde gerekli değişikliklere gidebilmek için sosyal medyadan gelen bilgileri kullanmaktadır. Çeşitli iyileştirmeler yapan işletmeler müşterilerine daha iyi bir hizmet sunarak pazarda daha güçlü bir konuma gelebilmektedir. Tüketici doğrudan bir ilginin var olduğunu hissederek markaya bağlanacaktır.

Sosyal medya pazarlamasında kullanılan içerikler kısa, basit, anlaşılır nitelikte olmalıdır. Bu içeriklerin bireyler tarafından da üretilebileceği unutulmamalıdır. Geleneksel pazarlama alanında kullanılacak olan bütün içerikler ise konusunda uzman olan kişiler tarafından profesyonel bir şekilde hazırlanmakta ve bizzat kurum tarafından yayınlanmaktadır. Sosyal medya ise üretilen içeriklerin ağda çok hızlı bir şekilde yaygınlaştırılmasını sağlamaktadır. Dijital çağın getirdikleri sayesinde artık nitelik niceliğin önüne geçmiştir. Bu durumda hızlı niteliğe sahip olan işletmeler öne çıkmaktadır. Sosyal medya pazarlaması ile oluşturulan içerikler çok kolay bir şekilde güncellenebilmekte ve tüketiciler nezdinde satın alma güdüsü çok daha kolay bir şekilde oluşturulmaktadır.

Tablo 2.1'de geleneksel pazarlama ile sosyal medya pazarlaması arasındaki farklar çeşitli faaliyet alanlarına göre belirtilmiştir. Buna göre yapısal ve iş yapış teknikleri açısından büyük farklılıklar görülmektedir. Kullanılan iletişim kanallarının çeşitliliği, bilgiye erişim olanakları, odaklanılan alanlar, pazarlama karmasına ait öğelerin kullanılma biçimleri, bilgiye ulaşım olanakları, yatırım türleri, bütçe oluşturma ve geri bildirim elde etme şekilleriyle birçok alanda farklılıkların bulunduğu gözlenmiştir.

Tablo 2. 1: Geleneksel Pazarlama ile Sosyal Medya Pazarlaması Farklılıkları

Faaliyet	**Geleneksel Pazarlama**	**Sosyal Medya Pazarlama**
Bilgiye Erişim	Ürün/hizmet bilgilerine erişim sınırlıdır.	Ürün\hizmet bilgilerine erişim kolaylıkla sağlanabilir. Bilgiye erişim hızlıdır.
Etkileşim ve İletişim	Alıcılar ve satıcılar arasındaki iletişim ve etkileşim zayıftır. İletişim daha çok tek yönlü olmaktadır	Alıcılar ve satıcılar birbiriyle etkileşim halindedir. Daha çok çift yönlü iletişim söz konusudur.
Maliyet	İşletmelerin pazarlama maliyetleri (reklam vb.) yüksektir	İşletme maliyetlerini (Örneğin; personel ve reklam faaliyetlerinin maliyetleri) azaltmaktadır.
Güncellik	Pazarlama karması kapsamında faaliyetler durağandır, değiştirilmesi güçtür.	Pazarlama karması kapsamında güncellenebilir faaliyetler mevcuttur. Faaliyetlerin esnekliği fazladır.
Kıyaslama	Ürünlerin/hizmetlerin kıyaslanması güçtür.	Kıyaslama imkanı vardır ve kıyaslama yapmak kolaydır.
Satın alma Kararı	Satın alma süreci ve karar verme karmaşıklığı mevcuttur.	Teknolojik gelişmeler sayesinde satın alma kararını verme karmaşıklığı azalmıştır. Süreçler daha yalın hale dönüşmüştür.
Kaynağa Erişim	Arşivlere erişim oldukça sınırlıdır.	Arşivlere çok kısa sürede kolayca ve etkin erişim sağlanır.
Medya Kullanımı	Tüm medya karma bir şekilde kullanılmaz.	Tüm medya karma olarak kullanılabilmektedir.
İçerik	Bir komite tarafından yayınlanan	Bireyler tarafından yayılan

	içerikler vardır.	içerikler vardır.
Katılım	Paylaşımlar desteklenmez.	Paylaşım ve katılımlar desteklenmektedir.
Kontrol	Kontrol vardır	Özgürlük vardır

Kaynak: Şahin, E., Çağlıyan, V.ve Başer, H. H. (2017). Sosyal Medya Pazarlamasının Tüketici Satınalma Davranışına Etkisi: Selçuk Üniversitesi İibf Örneği. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 10*(4), 67.

Sosyal medya pazarlamasının tüketici davranışları üzerindeki etkisi çok sayıda araştırmaya konu olmuştur (Şahin, Çağlıyan ve Başer, 2017: 71). Bu araştırmalarda sosyal medyanın tüketici üzerindeki etkisi farklı birçok yönü ile mercek altına alınmıştır. İşletmeye ait markanın tanınır hale gelmesi, tüketici davranışlarını doğru bir şekilde analiz etme, yeni pazarlama stratejileri için olanakları araştırma, işletmenin dijital alanda var olan platformların etkin bir şekilde kullanılması, pazarlamanın ürettiği belirgin mesajları doğru kişilere ulaştırma, işletmeye ait internet sitesine olan trafiği artırma, markaya ait mesajların sosyal medyada görünürlük süresini uzun tutma, sosyal alanda yapılan aramaların sınıflandırılmasını sağlama, markanın verdiği mesajların tüketici tarafından içselleştirilmesini sağlama ve ürünün satış miktarını artırma gibi birçok amaç için sosyal medya pazarlamasını kullanmak mümkündür (Weinberg, 2009: 6).

2.3 SOSYAL MEDYA PAZARLAMASI SÜRECİ

Sosyal medya pazarlaması dinleme yapma, hesaplama, bağlılık oluşturma ve pazarlamaya ait birçok faaliyeti optimize etme gibi eylemlere sahip bir süreçtir (Akgün ve Ergün, 2017: 17).

Sosyal medya pazarlamasının nasıl bir süreç içerisinde gerçekleştirileceği ile ilgili yapılmış olan bir çalışmada sosyal medya pazarlamasına ait süreç "L-I-S-T-E-N" olarak yapılandırılmıştır. Bu formülde her bir harf bir süreci işaret etmektedir. Listen kelimesi İngilizcede dinlemek anlamına gelmektedir. Bu formülün ilk harfi olan L harfi sürecin ilk aşamasını oluşturmakta ve karşı tarafı dinlemeyi önermektedir. Diğer harfler ise sırayla şu anlamlara gelmektedir: I tanımlamak (identify), S çözmek (solve), T test

etmek (test), E bağlanmak (engage), N büyütmek (nurture). Bu aşamaları şu şekilde açıklamak mümkündür (İşlek, 2012: 73):

Dinleme: İlk aşama olan dinlemede işletmeler sosyal medya dünyasına ait çeşitli profesyonel dijital araçları kullanarak kelimelerle ve aramalarla ilgili analizlere ulaşmakta ve sosyal medyada işletmeyle ilgili üretilen bütün içerikleri takip edebilmektedir.

Tanımlama: Sosyal medya araçlarından elde edilen veriler çeşitli süreçlerden ve işlemlerden geçerek kategorilere ayrılır. İşletmeler kategoriler sayesinde yaptığı tanımlama çalışmasıyla stratejik pazarlama çalışmalarına yön verebilmektedir.

Çözme: İşletme ürettiği verileri bilgiye çevirip bunları pazarlama alanında kullanmaktadır. Bu aşamalarda ortaya çıkan bilgiye göre üretilecek cevaplar çözüm aşamasında gerçekleştirilmektedir. Çözüm aşamasında iletişim kurulmakta ve müşteri memnuniyetinin öne çıkacağı şekilde çeşitli çalışmalar yapılmaktadır.

Test Etme: Müşteri ile iletişim kurulduktan sonra çözüm olanakları için çeşitli aksiyonlar yapılandırılmıştır. Bu aşamadan sonra çözümün sonuçlarıyla ilgili müşteriden çeşitli geri bildirimler alınmaktadır. Geri bildirimler sayesinde elde edilen bilgiler üretilen çözümlerle karşılaştırılmaktadır. Müşteri talebinin ne oranda karşılandığı bu aşamada ölçülmektedir. Bu aşamada beklenen sonuç müşteri tatmini sağlamaktır.

Bağlanma: İşletme çeşitli çözümler üreterek müşterinin taleplerini karşılamış ve müşteri tatmini ortaya çıkmıştır. Müşteri artık bu aşamada işletmenin veya markanın varlığını içselleştirmiştir. Bu noktadan sonra müşteri işletmeyi ve markayı temsil ederek müşteri adaylarına karşı onu savunmaktadır.

Büyütme: İşletme pazarlama stratejisi sayesinde ve sosyal medya araçları ile çeşitli kategoriler üretmiş ve önemli tanımlamalara sahip olmuştur. Bu şekilde bir iletişim süreci başlamaktadır. Geri bildirimler ile yapılan iyileştirmeler sayesinde müşteri bağlılık seviyesi en üst seviyeye çıkarılmaktadır. Bu aşamadan sonra işletme müşterinin sadakatini ödüllendirerek müşteriyle işletme arasındaki bağın boyutunu güçlendirmektedir. Bu şekilde gittikçe büyüyen bir kitleye ulaşmaktadır. Sosyal medya pazarlama sürecini doğru bir şekilde yürüten işletmeler sosyal olma durumunun avantajını kullanarak sadakati yüksek bir müşteri kitlesine ulaşabilmektedir. Müşteriden

aldığı cevaplar ve talepleri doğru bir şekilde değerlendiren işletme marka değerini de üst düzey bir konuma taşıyabilmektedir.

2.4 SOSYAL MEDYA PAZARLAMASININ FAYDALARI

İşletmeler ve müşteriler sosyal medya pazarlamasına başvururken kendi faydalarını göz önünde bulundurmaktadırlar. Tüketici açısında olan faydalar hedonik, sosyal, psikolojik, fonksiyonel ve maddi faydalar olabilmektedir. Bu faydaları şu şekilde incelemek mümkündür (Kang, 2011: 27):

Hedonik Fayda: Hedonist niteliğe sahip tüketiciler satın alma davranışlarında farklı nitelikler ortaya koymaktadır. Satın alınan ürün veya hizmetin bir ihtiyacı karşılaması hedonistler için çok önemli değildir. Satın alma eyleminin verdiği haz veya ürün ve hizmetin beş duyuya hitap etmesi onlar için çok daha önemlidir. Geleneksel pazarlamada ve sosyal medya pazarlamasında hedonist tüketicilere aynı sebeplerle rastlamak mümkündür. Geleneksel pazarlama alanında tüketicinin aldığı bireysel haz sosyal medya pazarlamasında da ortaya çıkmaktadır Hedonist tüketici ihtiyacının karşılanması yanında haz ve zevklere de önem vermektedir. Sosyal medya pazarlaması ile amacına ulaşan hedonist tüketici sahip olmak istediği ürün veya hizmete çok kolay bir şekilde ulaşabilmektedir. Dijital araçları çok etkin bir şekilde kullanan sosyal medya pazarlaması çok kolay bir şekilde hedonist tüketicilere ulaşabilmektedir. Zaman veya mekân kısıtlaması olmadan arzu ettiği her şeye ulaşabilen hedonist tüketici zaman tasarrufunda bulunmakta ve nitelikli eylemlerine çok daha fazla vakit ayırabilmektedir (Torlak, Altunışık, Özdemir ve Sarıkaya, 2007: 54)..

Sosyal Fayda: İşletmelerin sosyal medya pazarlamasını kullanması yeni tüketici tiplerini de ortaya çıkarmaktadır. Bu tüketici tipine sosyal tüketici adı verilmiştir. Sosyal tüketiciler ürün ve hizmetler hakkında detaylı bilgilere çok hızlı bir şekilde ulaşma arzusuna sahiptirler. Bu tip tüketiciler aynı zamanda kullandıkları ürün ve hizmet hakkında yorum yapmayı ve bunu sosyal medya hesapları üzerinden anlatmayı tercih etmektedirler. Bu şekilde müşteri adaylarını olumlu veya olumsuz anlamda etkileme gücüne sahiptirler. Bununla birlikte sosyal medya alanını etkin bir şekilde kullanan işletme müşterileriyle bir etkileşim olanağına sahip olmaktadır. Tüketiciler ilgi duydukları markaların en güncel haberlerine sosyal medya aracılığıyla ulaşmaktadır (Tosun, 2017: 647).

Fonksiyonel Fayda: Geleneksel pazarlama alanında bulunan işletmeler tüketici ihtiyacını tespit ederek belli başlı ürünler ve hizmetler üretmişlerdir. Tek boyutlu bir iletişim ortamına sahip olan bu pazarlama türünde kontrol genellikle işletmenin elinde olmuştur. Dijital olanakların ortaya çıkması ile gelişen sosyal medya pazarlaması sayesinde işletmeler kontrol gücünü tüketiciler nezdinde kaybetmiştir. Sosyal medya pazarlaması ile işletmelerin müşterileri çok hızlı bir şekilde davranış değişikliğine yönlendirmesi zorlaşmıştır. Dijital olanaklar ile çok sayıda bilgiye kolay bir şekilde ulaşabilen tüketici artık bilgileri toplamakta, karşılaştırma yapmakta ve nesnel kullanıcı görüşlerini dikkate almaktadır. Sosyal medya pazarlamasının bu niteliği sayesinde tüketici fonksiyonel bir fayda sağlamaktadır (Kang, 2011: 29).

Psikolojik Fayda: Sosyal medya pazarlaması çok yönlü bir iletişime olanak sağlamaktadır. Tüketicilerin sosyal medya aracılığı ile kurdukları iletişim ürün ve hizmet hakkından bilgi edinme eylemi ile sınırlı kalmamaktadır. Sosyal, kültürel, ekonomik ve demografik açıdan çok farklı niteliklere sahip olan tüketici grupları ürün, hizmet, işletme, marka gibi konularda ortak bir platformda buluşma olanağına sahip olmaktadır. Sosyal ağlar aracılığıyla tüketime yönlendirilen müşteriler işletmeye tam anlamıyla güvenmek istemektedir. Tüketici dijital platformda satın alma eylemi gerçekleştirirken birçok kişisel bilgisini paylaşmaktadır. İşletmenin dijital alandaki uygulamalarında ortaya çıkabilecek zayıf güvenlikten dolayı müşteri bilgileri üçüncü kişilerin eline geçerse müşteri maddi açıdan zarara uğrayabilmektedir. Bu yüzden işletme dijital yapısını oluştururken güvenlik özelliği yüksek uygulamaları satın almak zorundadır. Bu durum işletme ile müşteri arasındaki güven duygusunu en yüksek seviyeye çıkaracaktır.

Maddi Fayda: Tüketici satın alma eylemini gerçekleştirirken birçok durumda rasyonel bir şekilde hareket etmektedir. Ürün veya hizmetten aldığı hazzın yanında maddi açıdan da tatmin olması çok önemlidir. Sosyal medya pazarlaması ile elde edilen maddi fayda müşteri için önemli bir kriter olabilmektedir. Geleneksel pazarlamada müşteri belirli sayıda satıcı ile karşı karşıya kalmakta ve ek bir indirim talep etmek satıcının inisiyatifinde gerçekleşmektedir. Ancak sosyal medya pazarlamasında müşteri bütün satıcıların bütün bilgilerini şeffaf bir şekilde görmekte ve maddi açıdan kendisine en uygun seçeneği kolay bir şekilde seçebilmektedir.

2.5. SOSYAL MEDYA PAZARLAMASI UYGULAMALARI

Dijital teknolojinin gelişmesiyle birlikte Web 2.0 tabanlı uygulamalar ortaya çıkmış ve sosyal medyanın ilk örneklerini oluşturmuşlardır. Bloglar ve mikrobloglar, sosyal işaretleme siteleri, wikiler, podcast kanalları, sosyal ağlar ve sosyal dünyalar sosyal medya aracı olarak kabul edilmektedir (Akar, 2010: 109). Bu sosyal medya araçları aşağıda detaylı bir şekilde ele alınmıştır:

Bloglar: Belirli alanlarda kişisel sayfalar oluşturarak birçok konuda yazılı ve görsel içerikler oluşturup diğer kullanıcılarla paylaşma olanağına sahip alanlardır. Genellikle orta veya uzun uzunluğa sahip yazılardan oluşmaktadır. Wordpress ve Blogger en bilinen blog uygulamaları arasında yer almaktadır.

Mikrobloglar: Mikrobloglar kısa mesaj içeriklerine sahip, çok sık bir şekilde güncellenebilen ve genel olarak basit ara yüzlere sahip sosyal medya uygulamalarıdır. Anlık, kısa paylaşımlar için uygun olmaktadır. Kullanıcılar bilgi ve duygu aktarımında, doğrudan iletişimde bu uygulamaları kullanabilmekte veya başka dijital uygulamalara yönlendirmeler yapabilmektedir. Kullanıcılar bu alanları gizleyerek tamamen kişisel alan haline getirebilmekte ve sadece belirli kullanıcılar için yazı, fotoğraf ve video paylaşabilmektedir. Akıllı telefonların mikroblog uygulamaları için uygun cihazlar haline gelmesiyle bu sitelerin popülerlik seviyeleri çok hızlı bir şekilde artmış ve kullanıcılar kişisel paylaşımlarını çok daha yoğun bir şekilde yapmaya başlamışlardır. Twitter en ünlü mikroblog uygulamasıdır (Uygun, 2010: 7).

Medya Paylaşım Siteleri: En önemli medya unsurlarından biri olan videolar medya paylaşım sitelerinden paylaşılmaktadır. Videolar için yapılan dağıtım maliyetinin düşük olması bu siteleri çok popüler hale getirmiştir. Yazı ve görsel gibi araçlarla yetinmek istemeyen birçok kullanıcı video paylaşım sitelerine başvurmaktadır. 2005 yılında kurulan Youtube şu anda en popüler video paylaşım sitesidir. Basit kullanıcı ara yüzüne sahip olması, kolay video paylaşım olanağı ve çok sayıda kullanıcının buluştuğu bir platform olması nedeniyle bu popülerlik düzeyi gittikçe artmıştır (Tosun, 2017: 647).

Wikiler: Dijital alanda bir ansiklopedi görevi gören wikiler bilgi paylaşım siteleridir. Bu sitelere üye olan kullanıcılar istedikleri sayfalar için içerik ekleyebilmekte ve çeşitli güncellemeler yapabilmektedir. Birçok kullanıcı ise araştırdığı veya merak

ettiği konuda gerekli bilgiye bu sayfalar aracılığıyla ulaşabilmektedir. Tek bir platform altında toplanan bilgiler burada depolanmakta ve herkesin kullanımına açık olmaktadır. Kullanıcılar hem okur hem yazar görevini üstlenebilmektedir. En ünlü wiki uygulaması Wikipedia'dır.

Sosyal İşaretlemeler: Sosyal işaretleme siteleri sayesinde kullanıcılar beğendikleri internet sitelerini işaretleyebilmekte ve kayıt altına alabilmektedir. Bu internet sitelerini sosyal ağı ile paylaşabilen kullanıcılar birçok internet sitesinin yaygınlaşmasını sağlamaktadır. Bu uygulamayı kullanan kullanıcılar yer imleri oluşturmakta, arşivleme yapmakta ve başvurduğu birçok internet sitesini kategorilere ayırmaktadır. En bilindik sosyal işaretleme uygulamalarından biri Delicious'tır.

Podcasting: Ses veya video kayıtlarının internet ortamından kullanıcının sahip olduğu medya aracına indirilmesi ve daha sonra istenilen zamanda izlenebilmesi veya dinlenebilmesine podcasting denir. Farklı tipteki birçok akıllı cihaza podcast indirmek mümkündür. Kullanıcı bu sayede internet bağlantısı olmadan bile indirmiş olduğu içeriğe istediği zaman ulaşabilmektedir. Televizyon ve radyo gibi medya araçlarında yayınlanan çeşitli yayınlar bu cihazlara indirilebilmektedir. Bu sayede herhangi bir yayını kaçırmak söz konusu olmamaktadır. Podcast özelliği sayesinde ses ve video özelliğine sahip içerikler geniş kitlelere yayılabilmektedir.

Sosyal Ağ Siteleri: Sosyal ağ sitelerinde yer alan kullanıcılar birbirleriyle etkileşim olanağına sahip olmaktadır. Kullanıcılara ait kişisel sanal sayfalarda yazılar, fotoğraflar ve videolar paylaşmak mümkündür. Kullanıcıların kullanabileceği bir mesaj uygulaması da vardır. Bu da iletişimin bir diğer yönünü göstermektedir. Kullanıcı paylaşımlarını farklı kişi gruplarına özel olarak açabilmekte, arkadaşlarının paylaşımları için yorumlar yapabilmektedir. En popüler sosyal ağ sitelerinden biri Facebook'tur.

Sanal Dünyalar: Kullanıcı medya aracına oyun gibi bir yazılım veya uygulama indirerek ve bu platformda bir üyelik oluşturarak sanal dünyaya katılmaktadır. Oluşturduğu üyelik kullanıcının kendisini yansıttığı sanal bir kişilik olarak kabul edilmektedir. Kullanıcı bu uygulama içinde hem oyun oynamakta hem de diğer kullanıcılarla etkileşim olanağına sahip olmaktadır. Kullanıcı kendi isteğine göre oluşturduğu sanal karakter üzerinde çeşitli simülasyonlar uygulayabilmektedir. Second Life sanal dünya uygulamasına bir örnektir.

Çevrimiçi Topluluklar: Dünyanın herhangi bir noktasında bulunan ortak ilgi ve hobi ağlarına sahip kullanıcıları sanal ortamda bir araya getiren gruplardır. Birçok insanın internette çok zaman geçirmesi insanların ilgi alanlarını sanal ortama taşımasıyla sonuçlanmıştır. Bu yüzden insanlar çevrimiçi topluluklar oluşturarak kendi ilgi alanlarına yakın insanları aynı platform üzerinde toplamayı bir uğraş haline getirmişlerdir. Benzer ilgi alanlarına sahip insanların bilgi alışverişinde bulunması, çeşitli paylaşımlarda bulunması ve yorumlar yapması grup içi etkileşim olanağını ortaya çıkarmıştır. Bu sayede kullanıcılar kendi alanlarına ilişkin yeni bilgiler öğrenmekte ve oluşturulan bağ sayesinde duygusal tatmin yaşamaktadır.

3. KİŞİSEL VERİLERİN KORUNMASI

Kişisel verilerin korunmasını tam olarak kavrayabilmek için ilk olarak kişisel veri (personal data) kavramını tam olarak anlamak gerekmektedir. Kişisel veri kavramının uluslararası geçerliliği olabilecek bir tanımı bulunmaktadır. Buna göre kişisel veri doğrudan veya dolaylı olarak gerçek kişiyle ilgili olabilecek veya onu belirlenebilir yapacak her çeşit bilgidir (Christopher ve Kuan, 2012: 66). Çalışmanın bu bölümü kişisel verilerin korunması kavramını içermektedir.

3.1 KİŞİSEL VERİNİN TANIMI

Kişisel Verilerin Korunması Kanunu (KVKK) 3. maddesine göre kişisel veri kimliği belirli veya belirlenebilir kişiye ait olan bütün bilgilerdir. Kişisel veri kapsamında kabul edilecek bilgiler kişinin kimliği, fiziksel özellikleri, sağlığı, kökeni, öğrenim ve istihdam durumuna ait birçok bilgiyi kapsamaktadır. Bununla birlikte kişiye ait sosyal yaşantı bilgileri de kişisel veri olarak kabul edilmektedir. Bu bakımdan kişinin başkalarıyla kurduğu iletişimden elde edilen haberleşme bilgileri de yine kişisel veri olarak kabul edilmektedir. Kişinin adres bilgileri, finansal bilgileri, adli ve hukuki duruma ait bilgiler, düşünce ve inanç dünyasına ait bilgilerin hepsi kişisel veridir. Hatta bireyin alışveriş alışkanlıkları bile kişisel veri olarak kabul edilmektedir (Aksoy, 2010: 1).

Nilgün Başalp kişisel veriyi şöyle tanımlamıştır: Bir kişiyi belirlenebilir hale getiren veri kişisel veridir. İlgili veri doğrudan veya dolaylı bir şekilde gerçek kişiyi ortaya çıkartıyorsa kişisel bir veriden söz edilebilmektedir (Başalp, 2004: 16). Verinin bir kimlik numarasını işaret etmesi ya da kişiye ait öznel bilgiler olan psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal durumunu ortaya çıkartan bilgiler kişisel veri olarak kabul edilmektedir. Bireyin genetik, sağlık, siyasi, etnik, dini bilgilerini açık eden veriler kişisel verilerdir. Başka bir deyişle kişiye özel olarak verilmiş olan kimlik numarası, vergi numarası, pasaport numarası, telefon numarası, motorlu araç bilgileri, ad, soyad, çeşitli görseller, ses kayıtları, özgeçmiş bilgileri, genetik bilgiler ve parmak izleri bireyi ortaya çıkartan doğrudan kişisel verilerdir. Bununla birlikte bireyin dolaylı bir şekilde belirlenebilir olmasını sağlayan yaş, meslek, adres gibi bilgiler de kişisel veri kapsamında ele alınabilmektedir (Uygun, 2010: 4).

Ketizmen'e göre kişisel veri kişinin bilinebilmesini sağlayan her türlü bilgi ve enformasyondur. Kişinin kendisi veya yaşantısı hakkındaki bilgiler ve enformasyonlar kişisel veri alanına dahil olmaktadır. Kişisel veriyi elde etme aracı olarak kullanılabilecek bilgiler ve çeşitli yöntemler özel hayat kavramı ile yakından ilişkili olmaktadır. Bu yüzden bu konuyu özel hayat kapsamında değerlendirmek çok önemlidir (Ketizmen, 2008: 192).

Kişisel verilerin düzenlenmesine ve korunmasına yönelik atılan bütün adımlar birçok kişiyi doğrudan ilgilendirmektedir. Ulusal ve uluslararası alanda yapılan çalışmalar kişisel verinin korunması ve özel hayatın gizliliği bakımından oldukça önem kazanmaktadır. Bilişim teknolojilerinin yoğun bir şekilde kullanılması ile birlikte kişisel verilerin işleme olanaklarının artması veri gözetimi kavramını ortaya çıkarmaktadır. Verilerin internet alanında kullanılması verilerin korunması konusunu çok acil bir noktaya taşımıştır. Bu konu özel hayatın gizliliği ile kesişmektedir (Benneth, 1992: 332).

OECD tarafından yayınlanan 108 sayılı sözleşmenin 2/(a) maddesinde kişisel veri, kim olduğu belirlenebilir olan bireylerle ilgili her türlü enformasyon olarak tanımlanmıştır. Bu maddenin devamında kim olduğu belirlenebilir olan kişi, bir kimlik numarasına sahip olan kişi veya belirgin fiziksel, psikolojik, ekonomik, kültürel ve sosyal niteliklerle belirlenebilecek kişi olarak tanımlanmıştır. Kişinin ve kişiye ait bilgilerin bu kadar geniş bir çerçevede ele alınmasının yanında kişiye ait ses ve görüntü kayıtları da kişisel veri kapsamına alınmıştır (Korff, 2001: 15).

1992 tarihli İsviçre Kişisel Verilerin Korunması Hakkında Federal Kanunu'nun 3/a maddesine göre kişisel veri daha önceki tanımlarda da belirtildiği gibi belirlenebilir bir kişiye ait bütün bilgilerdir (Döner, 2006: 1). Türkiye'de telekomünikasyon alanında yapılan kişisel verilerin korunması çalışmaları için üretilen yönetmelikte (Telekomünikasyon Sektöründe Kişisel Verilerin ve Gizliliğin Korunması yönetmeliği, 2004) tanımlar bölümünde kişisel veriler şu şekilde tanımlanmıştır: Doğrudan veya dolaylı olmak üzere kişiye ait kimlik numarası, fiziksel, psikolojik, ekonomik, kültürel, sağlık, etnik, dini, siyasi bilgilere ait birçok unsurun kullanılması ile bireyi tanımlı hale getirebilecek gerçek veya tüzel kişilere ait herhangi bir bilgi kişisel veridir (Özdemir, 2009: 285).

Kimliği belirleyebilecek çok sayıda bilginin kişisel veri olarak kabul edilmesi kişisel veri kavramının alanını oldukça geniş tutmaktadır. Doğrudan bireye ait olan, bireyin kim olduğunu ortaya çıkartabilecek, onu ima edebilecek birçok kişisel bilgi kişisel bilgi kapsamına alınmıştır. Bireyin fiziksel özelliklerine ait bilgiler, kan grubu gibi sağlık bilgileri, adres ve telefon bilgileri, sosyal faaliyetleriyle ilgili bütün bilgi ve unsurlar kişisel veri olarak kabul edilmiştir (Şen, 2009/3: 1197). Kanun'da tüzel kişiliklere ait veriler dahil edilmemiş, bu verilerle ilgili korumalar diğer kanunların kapsamına bırakılmıştır. Türk Ceza Kanunu (TCK) 135. madde ve bununla ilgili diğer maddeler incelendiğinde kişisel veri kavramından bahsedilse de bu kavramla ilgili tanımlamalar oluşturulmamıştır (Güney, Özdemir, Özdemir ve Solmaz, 2004: 415). Maddenin gerekçesi incelendiğinde kişiyle ilgili kayıt altına alınmış birçok bilgi kişisel veri kapsamında değerlendirilirken, kişiyle ilintili olabilecek ses ve görüntü kayıtları kişisel veri kapsamının dışında tutulmuştur (Soyaslan, 2005: 273). Bu gerekçeye göre kişiye ait olan ve kişinin doğrudan tasarrufta bulunabileceği bilgi ve enformasyon kişisel veri olarak kabul edilmektedir. Örneğin; bir işletmeye ait olan ticari sırlar gibi bazı önemli bilgiler veri olarak kabul edilse bile kişisel olmaktan çok kurumsal olarak değerlendirilmektedir. Bununla birlikte kişinin ses ve görüntü kayıtları dahil olmak üzere kişiyi fiziksel olarak belirlenebilir kılan bilgiler kişisel veri olarak kabul edilebilmektedir (Ketizmen, 2008: 230). TCK 239. madde ile ticari sır ile bankacılık ve müşteri sırrı gibi bilgiler veya çeşitli keşifler, buluşlar, sınai bilgiler farklı düzlemde ele alınmıştır. Bu yüzden 135. madde ve sonrasındaki hükümlerde yer alan suçların konusunu bu bilgi türleri oluşturmamaktadır. Bu veriler özel hayatın gizliliğinin korunmasından çok toplumsal bilginin korunması amacına yöneliktir. Amaç sanayi, ticaret ve ekonomiyle ilgili genel veya kurumsal bilgilerin güvenliğini sağlamaktır. Bu amaçla TCK 239. madde "Topluma Karşı Suçlar" kısmında "Ekonomi, Sanayi ve Ticarete İlişkin Suçlar" bölümü altında ele almıştır (Özbek, 2005: 73).

3.2 KİŞİSEL VERİLERİN İŞLENMESİ

Kişisel verilerin elde edilmesi ve kullanılması kişisel verilerin işlenmesi anlamına gelmektedir. Çok sayıda eylemi işleme olarak kabul etmek mümkündür. Kişisel verilerin farklı yöntemlerle elde edilip kayıt altına alınması, kategoriler haline getirilip ayrıştırılması, çeşitli işlemlerden geçirilip uyarlanması, düzenlenerek birleştirilmesi, birçok kişinin erişebileceği hale gelmesi, okunması, başkalarına gönderilmesi, sanal

dünyada yaygınlaştırılması, çeşitli kombinasyonlarla bazı bilgilerle ilişkilendirilebilir hale gelmesi, bloke edilmesi ve silinmesi gibi birçok eylem ve durum kişisel verilerin işlenmesi kapsamında değerlendirilmektedir (Başalp, 2004: 16). Verilerin işlenmesi elektronik veya elektronik olmayan farklı birçok ortam ve düzlemde gerçekleştirilebilmektedir (Ersoy, 2009: 20).

Kişisel verilerin işlenmesi aşamasında özellikle bilgisayarla ilintili bir yöntem kullanılmışsa verilerin otomasyon sürecinden geçtiği söylenmektedir. Kişisel verilerin korunması kapsamında bütün eylemler göz önünde bulundurulmaktadır. Verilerin elde edilmesinden başlayarak gerçekleştirilen bütün eylemler koruma altında olmaktadır (Ersoy, 2009: 18). Kişisel verinin işlenmesi konusunda bazı durumlar kapsam dışında tutulmaktadır. Kişinin kişisel araçlarında kayıt altına almış olduğu kişisel veriler bu kapsamın dışındadır. Örneğin, kişisel bir cihazın içinde yer alan fotoğraflar, adres bilgileri, telefon kayıtları veya çeşitli ilişkilenmeler sonucunda ortaya çıkabilecek kişisel kayıtlar kişisel verinin işlenmesinin kapsamının dışında kabul edilmektedir. Bunun dışında kişinin mesleki veya ticari faaliyetleriyle ilgili veriler özel bir veri olarak ele alınmasa da kişi bu verileri herkese açık bir şekilde düzenlemediği sürece bunlar kişisel veri kapsamında değerlendirilebilmektedir100. Kişisel verilerin işlenmesine yönelik uyulması gereken ilkeler şunlardır (Küzeci, 2010: 195):

I. Kişisel veriler hukuka uygun bir şekilde toplanmalı ve işlenmeli (dürüst toplama ilkesi),

II. Kişisel veriler, veri toplama amacına uygun bir şekilde, gereken miktar ölçüsünde toplanmalı (asgarilik ilkesi),

III. Kişisel veriler hukuka uygun bir şekilde önceden belirlenmiş nesnel kurallar ve amaçlar çerçevesinde toplanmalı (amaca bağlılık ilkesi),

IV. Kişinin veri toplama konusunda verdiği yetki çerçevesinde sadece belirlenmiş amaçlar için veriler toplanmalı (kullanımın sınırlandırılması ilkesi);

V. Kişisel veriler amaca uygun şekilde doğru ve tam olarak elde edilmeli (amaca uygunluk ilkesi),

VI. Kişisel verilerin haber verilmeden ilgisiz kişiler tarafından elde edilmesi, veriye zarar verilmesi, istek dışı değiştirilerek kullanılması gibi olumsuz durumların

önüne geçebilmek için gerekli güvenlik önlemleri alınmalı (koruma/güvenlik ilkesi),

VII. Kişisel verinin sahipleri verileri elde tutan kişi veya kurumlar tarafından sürekli olarak bilgilendirilmeli, ilgili verilere ulaşabilmeli ve gerekli değişiklikleri ve düzenlemeleri yapabilmeli (bireysel katılım ilkesi),

VIII. Kişisel veriye erişim sağlayabilen yetkili kişiler veri işleme konusunda çeşitli açılardan sorumluluklara sahip olmalı (sorumluluk ilkesi) (Wacks, 1989: 210).

KVKK 4. maddede kişisel verilerin işlenmesi konusunda çeşitli ilkelere yer verilmiştir. Bunlar; dürüstlük ve hukuk kurallarına uygun olma, doğru ve güncel bilgiyi oluşturma, belirli ve açık amaçlar çerçevesinde bilgiyi kullanma, amaca uygun bir şekilde işleme, amaç çerçevesinde sınırlı bir şekilde veriye sahip olmadır. Bu genel ilkeler dışında verilerin işlenmesi konusunda veri sahibinin rızasının olması ve gerekli hallerde kamu yararının gözetilmesi gibi ilkeler de bulunmaktadır. Verinin işlenmesinin amacı net bir şekilde veri sahibine iletilmelidir. Amacın meşru bir niteliğe sahip olması çok önemlidir. Belirlenen amaçlar ve sınırlar dışında verilerin üçüncü kişiler tarafından kullanılması dolayısıyla veri kullanıcıları sorumlu olacaklardır. Ayrıca amacı dışında toplanan kişisel verilerin veri işleme süreci dışında tutulması da bir diğer dikkat edilmesi konu olarak öne çıkmaktadır (Ersoy, 2009: 104).

3.3 KİŞİSEL VERİLERİN KORUNMASI HAKKI

Kişisel verilerin korunmasıyla ilgili hukuki düzenlemelerin ortaya çıkışında temel olarak üç etkenin var olduğu belirlenmiştir. Bunlar; çeşitli kuruluşların çeşitli sebeplerle kişisel veriye ihtiyaç duyması, teknolojide yaşanan değişimler ve gözetim teknolojisinde yaşanan dönüşümlerin neden olduğu endişelerdir (Küzeci, Kişisel Verilerin Korunması, 2010: 18). Bununla birlikte kişisel verilerin korunmasına ilişkin olaylar tarihsel olarak düşünüldüğünde erken dönemler ve bilgi toplumu dönemi olarak iki dönem şeklinde incelemek gerekmektedir.

3.3.1 Tarihi Gelişim

Kişisel verilerin korunması hakkındaki tartışmalar yoğun bir şekilde bilişim teknolojisinin ortaya çıkmasıyla ve kişisel verilerin otomatik bir şekilde kayıt altına alınmasıyla ortaya çıkmış olsa da tarihi çok daha eskilere dayanmaktadır. Örneğin, bir

hekimin hastalarıyla ilgili öğrendiği bilgileri saklama zorunda olmasına ilişkin oluşturulan Hipokrat Yemini kişisel verilerin saklanması konusunda en eski kayıtlardan biridir. Farklı meslek gruplarının sahip olduğu bilgiler kişiler için büyük bir önem arz etmeye başlayınca farklı yükümlülük tipleri oluşturulmuştur. Din adamının günah çıkartma gibi durumlarda öğrendiği kişisel sırları saklama yükümlülüğü, memurun sahip olduğu görevlerle ilgili öğrendiği bilgileri saklama yükümlülüğü, bankaların veya hukuk bürolarının müşterileriyle ilgili olan özel bilgileri saklama yükümlülüğü gibi yükümlülükler bulunmaktadır (Şimşek, 2008: 5-6).

İkinci Dünya Savaşı döneminde totaliter niteliklere sahip rejimlerin insanlar hakkında hukuka ve insan haklarına aykırı olacak şekilde veri toplaması, sınıflaması ve bu bilgilerde bazı kişi gruplarını tehlikeli ve düşman olarak nitelemesi çok büyük sorunların ortaya çıkmasına neden olmuştur. İkinci Dünya Savaşı sonrasında 1960'lı yıllarla birlikte bilgi toplumu kendini göstermeye başlamıştır. Toprak, sermaye ve işgücü gibi klasik üretim ögelerinden çok bilgi ve bilgiyi kullanma becerisi öne çıkmıştır (Aksoy, 2010: 3). 1960'lı yılların sonuyla birlikte bilişim dünyasında yaşanan gelişmeler gözetim ortamının ortaya çıkmasına neden olmuş ve özel hayatın gizliliğine yönelik yeni tehditler kendini göstermiştir. Kişisel verilerin artık çok kolay bir şekilde elde edilmesi, kaydedilmesi ve işlenmesi nedeniyle kişisel verilerin korunması konusunda yeni düzenlemelerin yapılması zorunluluğu ortaya çıkmıştır (Kılınç, 2015: 197).

Modern anlamda kişisel verilerin korunması konusundaki ilk tartışmalar ABD'de görülmüştür. Dönemin yönetim sistemi ülkede bulunan bütün vatandaşların kişisel verilerini tek bir merkez elinde toplamak isteyince verilerin gizliliği ve korunması konusunda yoğun tartışmalar yaşanmıştır. 1974 yılında özel yaşamın gizliliğinin korunması konusunda yönetime çeşitli yükümlülükler yükleyen Özel Yaşamı Koruma Kanunu kabul edilmiştir (Şimşek, 2008: 7). İnsanların özel yaşamlarının gizlilik çerçevesinde ele alınması yönündeki hukuki çerçeve köken olarak Amerika'dan yayılmış olsa da bu konuyla ilgili ilk düzenlemelere Avrupa'da rastlanılmıştır. Bu konuyla ilgili ilk kanun 1970 yılında Almanya'da bölgesel düzeyde kabul edilmiştir (Kılınç, 2015: 197). Daha sonra 1973 yılında İsveç Veri Koruma Kanunu; 1974 yılında ABD Özel Yaşamın Gizliliği Kanunu; 1977 yılında Federal Almanya Veri Koruma Kanunu ve 1978 yılında Fransa Elektronik Veri İşlemesi, Veriler ve Özgürlük Haklarına

İlişkin Kanun kabul edilmiştir (Küzeci, Kişisel Verilerin Korunması, 2010: 109). 1980'li yıllarda teknolojinin gelişmesiyle birlikte kişisel verileri elde etmek, depolamak ve çeşitli süreçlere tabi tutmak çok daha kolay hale gelmiştir. Bu yüzden kişisel verilerin gizliliği ve özel yaşamın korunması konusundaki hukuki düzenlemeler ulusal ve uluslararası seviyede genişletilmiştir. Örneğin; 1948 yılındaki BM İnsan Hakları Evrensel Bildirisi (İnsan Hakları Evrensel Bildirisi , 2019), 1950 yılındaki AİHS ve Medeni ve Siyasi Haklar Sözleşmesi bu hukuki düzenlemelere örnek olarak gösterilmektedir (Kılınç, 2015: 197). 1980 yılında OECD Rehber İlkeleri Sözleşmesi'ne imza atmış olsa da burada kabul edilen temel ilkeler bağlayıcı bir niteliğe sahip olmamıştır. Ardından 1981 yılında kabul edilen 108 sayılı Avrupa Konseyi Sözleşmesi, imza veren ülkeleri ulusal hukuki düzenlemeleri açısından bir yükümlülük altına sokmuştur. 1990 yılında BM Genel Kurulu, Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Düzenlenmesine İlişkin Rehber İlkeleri'ni yürürlüğe sokarak üye olan ülkelerin kişisel verilerin korunması konusunda asgari bir standarda sahip olmasını amaçlamıştır (Ersoy, 2009: 49). 1995 yılında Avrupa Birliği'nin ortaya koyduğu 95/46/EC sayılı Veri Koruma Direktifi kişisel verilerin korunması konusunda önemli bir ilerlemeyi göstermektedir. Oluşturulan bu direktifle üye ülkelerin uyması gereken genel esaslar belirlenmiştir. Ülkeler bu direktife uyabilmek için iç hukuklarında çeşitli değişikliklere gitmişlerdir (Korkmaz, 2017: 74).

Verilerin korunması konusunda yaşanan bu gelişmeler neticesinde Türkiye iç hukuku da bu durumdan doğrudan etkilenmiştir. Türkiye'nin de kabul etiği Avrupa İnsan Hakları Sözleşmesi (AİHS) kişisel verilerin korunması konusunda ülkelerin iç hukuklarını yükümlü kılmıştır (Hacıoğlu, 2004: 93). 6698 sayılı KVKK ise 95/46/EC sayılı Veri Koruma Direktifi temel olarak kabul edilerek oluşturulmuştur. Yeni teknolojilerin ortaya çıkmasıyla birlikte Avrupa kişisel verilerin korunması kapsamında çeşitli güncellemelere ihtiyaç duymuş, 2016 yılında 2016/79 sayılı Genel Veri Koruma Tüzüğünü kabul etmiştir. Türkiye, 108 sayılı Avrupa Konseyi Sözleşmesi'ni 1981 yılında kabul etmiştir. Sözleşmenin iç hukuka dahil edilmesi 2016 yılında gerçekleştirilmiştir. Türkiye, 108 sayılı Avrupa Konseyi Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin 181 sayılı Protokol'ü ise 2001 yılında kabul etmiştir. Bu protokolle birlikte ülkeler kişisel verilerin korunması konusunda tam

bağımsızlığa sahip denetleyici bir kurum kuracağını taahhüt etmiştir. İlgili protokolün Türkiye'de iç hukuka dahil edilmesi 2016 yılında gerçekleşmiştir.

3.3.2 Hakkın Dayanağı

Kişisel verilerin korunması hakkında oluşturulan çeşitli hakların dayanaklarını mülkiyet hakkı, fikrî mülkiyet hakkı, enformasyonel self determinasyon hakkı ve kişilik hakkı kapsamında yer alan yükümlülükler çerçevesinde çeşitli görüşlerle birlikte ele almak mümkündür (Küzeci, Kişisel Verilerin Korunması, 2010: 67).

3.3.2.1 Mülkiyet hakkı

Kişisel verilerin korunması hakkındaki ilk görüşlerin temelinde Amerika hukuku ile ortaya çıkan mülkiyet hakkıyla ilgili görüşler yatmaktadır. Buna göre kişisel veriler hem kişiliğin bir uzantısıdır hem de kişiliğe ait bir üründür. Veri sahibi olan bir kişi aynı zamanda kendi kişisel verilerinin sahibidir. Bu yüzden bu veriler üzerinde tam bir denetim hakkına sahiptir. Bununla birlikte mülkiyet hakkının kişiye tanımış olduğu geniş yetkileri kişisel veriye sahip olma durumuyla ilişkilendirmek mümkündür (Küzeci, Kişisel Verilerin Korunması, 2010: 62).

Bilgi çağında bilgiye sahip olma ile güce sahip olma eş anlama gelmektedir. Kişisel verileri toplayıp işlemenin ticari bir yönü mevcuttur. Bu yüzden kişisel verileri kullanarak değerler elde eden kişi veya kurumlar veri sahibine belirli miktarlarda ödeme yapmak zorunadır156. Mülkiyet hakkı düşüncesine göre veri sahibi kişi verilerinin kötüye kullanıldığı sonucuna varırsa uğradığı zararlardan ötürü dava açma yetkisine sahip olmaktadır (Akgül, 2016: 76). Bununla birlikte mülkiyet hakkı kavramı tam olarak kişisel veriye sahip olma durumuyla uyumlu olmamaktadır. Kişisel verinin sahibi olan kişiden rıza alındığı takdirde kişisel veri kullanıcısı olan kişi veya kurumlar bu veriyi üçüncü kişilerle paylaşabilecek ve gerekli gördüğü şekilde işleyebilecektir. Sonuç olarak veri kişiden tamamen soyutlanacak bir duruma bürünecek ve insanın onuruyla uyumlu olmayan olumsuz bir durum ortaya çıkacaktır (Ayözger, 2016: 15). Mülkiyet hakkı doğada sınırlı bir şekilde bulunan kaynakların doğru dağılımını hedeflerken, herhangi bir kıtlıkla bağdaştırılamayacak kişisel veriler için mülkiyet hakkını devreye sokmak sonuç olarak anlamsız bir çabaya neden olacaktır (Aksoy, 2010: 66).

3.3.2.2 Fikri mülkiyet hakkı

Kişisel verilerin korunması yönündeki ikinci görüş verileri fikri mülkiyet hakkı kapsamında değerlendirmektir. Hem kişisel verileri hem de fikri mülkiyetin korunmasındaki temel amaç bilginin korunması ve veri sahibinin zarara uğratılmamasıdır. Amaç olarak benzerlikler görüldüğü için iki hakkı aynı kapsam içinde değerlendirmek olumlu bir durum olarak görülmektedir. Buna göre fikri mülkiyete sahip olan eser sahibinin ilgili eser üzerindeki sahiplik hakkı ile kişisel veriye sahip kişilerin veriler üzerindeki sahip olma hakkı benzerdir (Aksoy, 2010: 60). Kişisel veriye sahip olan kişi telif haklarına sahipmiş gibi korunmalıdır (Küzeci, Kişisel Verilerin Korunması, 2010: 64).

Fikri mülkiyetin oluşturulması esnasında eser sahibi kişi bilinçli olarak bir üretim yapmaktadır. Ancak kişisel veriler bilinçli bir çaba sonucunda ortaya çıkmamaktadır. Kişinin yaşamı boyunca sahip olmak zorunda olduğu bilgiler ve değerler kişisel veri olarak kabul edilmektedir. Eser sahibi fikri mülkiyet hakkını kullanarak ekonomik bir amaç güdebilmektedir. Fikri mülkiyet hakkının aynı zamanda kamusal yarar gibi bir tarafı vardır. Ancak kişisel verilerin korunması konusunda ekonomik veya kamusal bir yarardan bahsetmek zordur. Kişiden izin almadan bilgilerin toplanması ve işlenmesi verilerin korunması kapsamına girmektedir (Ayözger, 2016: 16).

3.3.2.3 Enformasyonel self determinasyon hakkı

Alman Anayasa Mahkemesi'nin nüfus sayımı ile ilgili verdiği 80'li yıllara ait bir karar kişisel verilerin korunması hakkında yeni bir görüşün ortaya çıkmasına neden olmuştur. 1983 yılındaki nüfus sayımı kararına göre vatandaşlar kendilerine ait birçok önemli bilgiyi yetkili kişilerle paylaşmak zorunda kalmıştır. Bilgiyi paylaşmayan kişiler için yaptırımlar söz konusu olmuştur (Küzeci, 2014: 53). Alman Anayasa Mahkemesi bu konuda bir karara vararak insan kişiliğinin doğru bir şekilde geliştirilmesi hakkı ile birlikte enformasyonel self determinasyon hakkını kabul etmiştir. Buna göre kişi kendi geleceğini belirleme konusunda bir hakka sahiptir (Küzeci, 2014: 53). Enformasyonel self determinasyon hakkı bireye kişisel verilerin hangilerinin kimler tarafından hangi şartlar altında işlenebileceğini belirleme hakkı vermektedir (Aksoy, 2010: 71). Açık bir hukuki yükümlülük veya rıza olmadan bireylerin kişisel verilerinin toplanması, kaydedilmesi ve işlenmesi bireyi zor durumda bırakmaktadır. Bireyin devlete karşı

korunması zorunlu bir durum haline gelmiştir. Verilerin korunması noktasında herhangi bir veriye öncelik verilmemiştir. Hassas olan veya olmayan herhangi bir veri aynı hükümlere tabi olmuştur. Eğer gerçekten bir kamu yararı varsa devlet kişisel verilere müdahalede bulunabilmektedir. Otomatik bir şekilde yapılan veri işleme faaliyetlerinde de sadece verilerin toplanma amacı göz önünde bulundurulmalıdır (Şimşek, 2008: 116).

İlgili karar üç ana unsura sahiptir. Bunlardan ilki veri kaydı yapılırken belirli bir amaç göz önünde bulundurulmalı ve amaca ulaşıldıktan sonra da veri yok edilmelidir. İkincisi belirli amaçlar için toplanan veriler gelecekte belirli olmayan amaçlar için kullanılmamalıdır. Üçüncüsü ise veriyi kaydeden veya işleyen kişi veya kuruluş veriyle ilgili ortaya çıkan olağanüstü durumları veri sahibine iletmelidir (Küzeci, 2014: 59). Enformasyonel self determinasyon hakkı kişisel veri üzerinde tam bir koruma sağlamaktadır. Bununla birlikte bu hak verinin serbestçe dolaşımını sağlamaktadır (Aksoy, 2010: 71).

3.3.2.4 Kişilik hakkı

Kişisel verilerin korunması hakkıyla ilgili oluşturulan dayanaklarla ilgili bir diğer görüş kişilik hakkı ile ilgilidir. Bir kişiyi kişi yapan bütün etmenleri kişilik hakkı kapsamında değerlendirmek mümkündür. Kişiyi bir insan haline getiren bütün maddi ve manevi değerlerdir. Onur sahibi olma, sağlıklı olma, beden bütünlüğüne sahip olma, saygınlığa sahip olma, bir ada sahip olma veya ekonomik serbestliğe sahip olma gibi değerleri saymak mümkündür (Serozan, 1994: 93). Kişisel hakkın korunması sayesinde insana manevi yönden bir değer atfedilmektedir (Sancakdar, 2017: 40). Yaşamın değişen bütün nitelikleri karşısında insanları olası tehlikelerden koruyabilmek için kişilik hakkına ihtiyaç duyulmaktadır (Kanadoğlu, 2009: 70). Kişilik hakkı kişinin kendine özgü bir özel alan oluşturmasını sağlamaktadır. Kişi bu özel alan içinde yalnız kalabilmekte, sadece istediği kişilerle iletişim kurabilmekte ve kendini geliştirebilmektedir (Şimşek, 2008: 133).

Avrupa'da kabul edilen görüş kişisel verilerin kişilik hakkının bir parçası olduğu yönündedir. Kişilik hakkı var olduğu için kişisel verileri korumak zorunlu bir durum olarak ortaya çıkmaktadır. Bu görüşü destekleyenler özellikle özel hayat ve mahremiyet konularından bahsetmektedir (Aksoy, 2010: 47). Türkiye hukukuna bakıldığında ve KVKK incelendiğinde kişisel verilerin işlenmesi konusunda özel hayatın gizliliğini

korumak konusundan bahsedilmektedir. Buna göre temel hak ve özgürlükler korunmalı, kişisel veriyi işleyecek kişi ve kurumlar yükümlülüklerine uymalıdır. Temel hak ve hürriyetleri en başta özel hayatla birlikte korumanın belirtilmesi kişilik hakkı görüşünü desteklemektedir. 95/46/EC sayılı Veri Koruma Direktifi amacını belirtirken başta mahremiyet hakkı olmak üzere bütün temel hak ve özgürlükleri korumak olduğunu kayda geçirmiştir. Bu belgenin yerini alan Genel Veri Koruma Tüzüğü temel hak ve özgürlüklerle birlikte özellikle kişisel verileri de koruyacağını belirtmiştir. Buna göre kişisel verilerin korunmasını kişilik hakkı çerçevesinde ele almak mümkündür.

3.3.3 Hakkın Sınırları

Bir hakka ait norm alanının sınırlandırılması hakkın sınırlandırılması anlamına gelmektedir. Bu öğreti Anayasa Hukuku içinde ele alınmaktadır. Buna göre hakla ilgili bazı etkinlikler koruma alanı dışında bırakılabilmektedir (Gören, 1999: 369). Kişisel verileri sınırsız bir şekilde korumaktan bahsetmek mümkün değildir. Kamu yararı gibi bir durum ortaya çıkmışsa kanunlara uygun bir şekilde oluşturulan sınırlandırmalara uyulmalıdır (Şimşek, 2008: 124). Kişisel verilerin korunması konusunda ortaya çıkabilecek sınırlandırmalar kişisel verilerin işlenmesinin hangi durumlarda doğru olacağının belirlenmesi açısından önemlidir. Kişisel verinin işlenmesine izin veren bir kanun Anayasa'da yer alan sınırlandırmalarla uyumlu olmalıdır (Akdağ, 2013: 84). Hukuki açıdan yetkiye sahip olan ve meşru amaçlarla hareket eden kişi ve kurumlar veri işleme yetkisine sahip olabilmektedir. Meşru amaçlar; kamu güvenliği, genel ekonomik durum, suç oranlarının azaltılması, toplumsal sağlığın korunması ve insanların hak ve özgürlüklerinin korunmasıdır. Veri işleme yapılırken belirlenmiş yöntemlerle, belirli sınırlar içinde, özel hayata en az müdahale edecek şekilde gerçekleştirilmelidir. Müdahale AİHS'de 8. madde 2. fıkrada bulunan istisnalar gözetilerek yapılmalıdır (Bignami, 2007: 242).

Anayasa'ya göre temel hak ve hürriyetlerin sınırlandırılması sadece belirli sebeplere bağlı olarak kanunla mümkün olmaktadır. Sınırlamalar Anayasa'nın özüne, demokratik sistemin gerekliliklerine aykırı olmamalıdır. Anayasa'nın 20. maddesinde özel hayatın gizliliği hakkı düzenlenmiştir. Buna göre her kişi özel hayatına saygı gösterilmesini isteme hakkına sahiptir. Bu gizliliğe dokunulmayacağı Anayasa'da özellikle belirtilmiştir. Kişinin üstünü arama, eşyalarına el koyma kim tarafından hangi

koşullarda yapılacağı Anayasa'da düzenlenmiştir. Aynı maddenin 3. fıkrasında bireyin kişisel verilerinin korunması hakkında talep hakkı olduğu yer almaktadır. Birey, verilerinin hangi amaçlarla kullanıldığını bilmeli ve gerekli değişiklikleri talep edebilmelidir. Kişisel veriler sadece kanunda belirtilen durumlarda kişinin rızası ile işlenebilmektedir.

Anayasa'nın 13. maddesinde genel bir sınırlama nedeninden yola çıkarak temel hak ve hürriyetlerle ilgili yapılacak sınırlamalar engellenmiştir (Küzeci, 2010: 266). Temel hak ve özgürlükler için özel bir sınırlandırma belirtilmediğinden Anayasa'nın temel hak ve özgürlükleri sınırlamalar karşısında korumak istediği görüşleri ortaya çıkmıştır (Sağlam, 2002: 8). Kişiyi arama ve eşyalarına el koyma işlemleri için koşullar belirtildiği için özel hayatın gizliliğine dair birçok konunun kapsam dışı olduğu yorumları yapılmıştır (Ketizmen, 2008: 211). Anayasa'nın 20. madde 2. fıkrasına göre özel hayatın gizliliği hakkında dair bazı sınırlamalar getirilmiştir (Küzeci, 2010: 266). Özel sınırlama sebepleri ne özel hayatın gizliliğine dokunulmayacağı hükmüne ne de kişisel verilerin düzenlemesiyle ilgili hükümlere uymaktadır. Sınırlama sebeplerini 1. fıkranın birinci cümlesi yönünden uygulamak mümkündür. Çünkü bu cümleye göre kişi özel hayatının gizliliğine saygı gösterilmesini isteme hakkına sahiptir. 3. fıkrada belirtilen hususlar ise 1. ve 2. fıkranın hükümleri yönünden uygulama alanı bulmamaktadır. Kişisel verilerin korunması konusunda ortaya çıkabilecek sınırlandırmalarda Anayasa'nın 13. maddesi dikkate alınmalıdır. Özel bir sınırlandırma sebebi olmadığı sürece temel hak ve hürriyeti kanun ile sınırlandırmak mümkün değildir (Şen ve Yurttaş, 2010: 29). Kişisel verilerin korunmasıyla ilgili yapılacak sınırlandırmalar bu maddedeki ilkelere aykırı olmamalıdır (Anayasa Mahkemesi, 2014). KVKK'nın 28. maddesinde kişisel verilerin korunması hakkının sınırlandırılabileceği durumlar yer almaktadır. Bu maddenin gerekçesinde yetkili kişilerin özellikle milli güvenlik sebebiyle veri işlemesi istisna kapsamında olduğu belirtilmiştir. Suç ile elde edilen gelirlerin aklanması, terör faaliyetlerinin finansmanının yapılması ve mali suçların araştırılması gibi amaç ve durumlar istisna kapsamındadır (Kanun Tasarısı, 2016). İlgili maddede ekonomik güvenlik kavramından bahsedilmiştir. Ekonomik güvenlik kamu düzenini sağlamak için yapılan bazı faaliyetleri kapsamaktadır. Serbest piyasa sisteminin gereklerini yerine getirmeyi sağlamak ve aykırı davranışlarda bulunanları cezalandırmak ekonomik güvenlik kavramının kapsamına girmektedir (Özkan, 2009: 83).

Kişisel verinin korunması hakkını sınırlandırabilecek durumlar araştırılırken ölçülülük esası da göz önünde bulundurulmalıdır. Buna göre sınırlama çerçevesinde yapılacak eylemler amaca ulaştıracak şekilde olmalı ve hakka en az müdahaleyi gerçekleştirecek nitelikte olmalıdır (Akgül, 2016: 117). Bu konuyla ilgili diğer ilke ise normların açıklığı ilkesidir. Buna göre düzenlemeler herkes tarafından anlaşılabilir olmalıdır (Şimşek, 2008: 125).

Kişisel verilerin korunması hakkının sınırlandırılmasına ilişkin düzenlemeler sadece kanun ile olmalıdır. Bu durum özellikle KVKK'da belirtilmiştir. KVKK kanunla sınırlandırma konusunda yasal bir güvence getirmiştir (Akgül, 2016: 121). Buna göre özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin düzenlemeler kanun hükmünde kararname ile yapılamamaktadır. Örneğin, Anayasa Mahkemesi 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'de yer alan kişisel verilerin toplanmasını ve işlenmesini onaylayan ilgili maddeyi iptal etmiştir (Anayasa Mahkemesi, 2013). Sınırlandırma yapılırken hakkın özü ölçütü göz önünde bulundurulmalıdır. Hakkın özü o hakkın önemini belirten esas unsurdur (Özbudun, 2012: 105). Temel hakkın sınırlandırılması söz konusuysa, hakkın özü için her hak ayrı bir şekilde değerlendirilmelidir (Gören, 1999: 376).

3.4 KİŞİSEL VERİLERİN KORUNMASINDA VERİ GÜVENLİĞİ

KVKK'nın 12. maddesinde veri güvenliği ilkesi ele alınmış ve kişisel veriyi kullanacak kişi veya kurumun verinin korunması konusundaki yükümlülükleri belirlenmiştir. Buna göre veri sorumlusu kişisel verinin hukuka aykırı bir şekilde işlenmesini önlemek zorundadır. Verinin koruma altında olması için gerekli bütün güvenlik önlemlerini almak zorundadır. Veri sorumlusu başkası adına hareket ediyorsa ilgili kişi veya kurum ile müştereken sorumludur. Veri sorumlusu verilerin korunması konusunda kendi kurum veya kuruluşunda denetim faaliyetini de yapmak zorundadır.

2016/679 sayılı Genel Veri Koruma Tüzüğü 30. maddesinde veri sorumlusunun veriyi korurken uygulama maliyeti hesaplaması gerektiği ile ilgili düzenlemelere yer verilmiştir (eur-lex, 2016). Buna göre ilgili verinin türü, çerçevesi ve kapsamı göz önünde bulundurulmalı, hak ve hürriyetlerin hangi riskler altında olduğu belirlenmeli ve buna uygun güvenlik önlemleri alınmalıdır. Kişisel verilerin korunması konusunda

alınabilecek diğer önlemler ise şunlardır: Kişisel veriler farklı takım adlar altında işlenmeli ve çeşitli şifreleme sistemleri kullanılmalıdır. Veriyi işleyen ve kullanan sistem sürekli olarak güncel tutulmalıdır. Program için gerekli esneklikler tanınmalı ve çeşitli hallerde bu esneklik niteliği kullanılmalıdır. Uygulamalar her zaman kullanıma hazır olmalı ve gerekli uyumlaştırma çalışmaları yapılmalıdır. Verilere hangi aralıklarla ulaşılabileceği önceden belirlenmelidir. Veri işleme güvenliğini sağlayacak tedbirler sürekli test edilmelidir (Bloux ve Desfougeres, 2011: 5).

Veri güvenliği ilkesi verilerin korunmasına ilişkin alınması gereken bütün tedbirlerle ilgilidir. Veri güvenliği ilkesi ile verilerin kaybedilmemesi, verilerin üçüncü kişilerin eline geçmemesi, verilerin tahrip edilmemesi ve herkese açık hale gelmemesi amaçlanmaktadır. Kişisel verilerin korunması ile veri güvenliği farklı kavramlardır. Kişisel verilerin korunması ile kastedilen kişisel verinin işlenmesi sürecinde bireyin bütün hak ve özgürlüklerini korumaktır (Şimşek, 2008: 94). Yasal düzenlemelerle kişisel verilerin doğru bir şekilde korunduğu güvence altına alınmaktadır. Verilerin yanlış ellere geçmesi, kanun dışı olacak şekilde kullanılması, kaybolması ve değiştirilmesi gibi olumsuz durumların önüne geçmek için teknik önlemler alınmalıdır (Kalabalık, 2009: 199). Veri güvenliği ile verilere olan yetkisiz erişimler ortadan kaldırılmaktadır. Bu sayede sadece yetkili kişilerin verilere erişimi sağlanmaktadır. Verinin herkese açık gelmesi, bozulması ve kullanılabilirliğine zarar gelmesi gibi olumsuz durumları engellemek için veri güvenliği sistemi oluşturulmalıdır (Henkoğlu, 2015: 33).

Veri güvenliği ilkesinin bir başka boyutunu veri gizliliği oluşturmaktadır. Verilerin güvenliği konusunda gerekli kontrolleri sağlayan kişi hem kendi sisteminin güvenliğinden hem de verileri kendi adına işleyen kişi veya kurumların sistemlerinin güvenliğinden sorumlu durumdadır (Akdağ, 2013: 83). Kişisel veri konusundaki çeşitli işlemler de gizlilik sebebiyle kontrol altında tutulmaktadır. Kişisel verilere ulaşma konusunda yetkiye sahip olan bütün çalışanlar ve ilgili görevliler işlem gizliliği konusuna tabi olarak çalışmalarını yürütmektedir. İç hukuka göre bilgi verme konusunda bir yükümlülük ortaya çıkmışsa bu gizlilik uygulanmamaktadır. Bir ceza kovuşturması konusu nedeniyle ihtiyaç duyulan bir bilgi yetkili makamlar tarafından istenmişse ve bilgi sağlanmışsa, bu gizlilik ilkesi ihlal edilmemiştir (Solove, 2008: 111-136). Veri kontrolünü gerçekleştiren kişi bütün sistemin güvenliğinden sorumluysa

teknik anlamda bütün güncel önlemleri almak zorundadır. Sorumlu kişi güncel gelişmeleri takip etmeli, değişen teknolojik durumlara göre sistemini her zaman güncel güvenlik önlemleriyle donatmalıdır. Eğer veriler elektronik olmayan bir ortamda ise verilerin kilit alında olması ve yangında zarar görmeyecek bir ortamda bulundurulması gibi koşullar göz önünde bulundurulmalıdır (Carey, 2009: 60).

4. ÇEVRİMİÇİ İZLEME VE KULLANICI

Sanal dünyaya dahil olan insanlar çevrimiçi olarak yaptıkları her eylemde bir iz bırakmakta ve bu iz kişisel cihaza kaydolmaktadır. Yapılan eylemin durumuna göre kişisel bilgiler, sağlık bilgileri, kredi kart bilgileri, sosyal güvenlikle ilgili bilgiler ve şifreler kullanılmaktadır. Kullanıcılar bu bilgilerin tamamen güvende olduğundan tam olarak emin olamamaktadırlar. Üçüncü kişiler kullanıcıların bilgisi ve isteği dışında bu bilgilere erişim potansiyeline sahiptir (Arrington, 2013: 13).

4.1 İZLEME ARAÇLARI

Çevrimiçi izleme amacı taşıyan bir çok araç bulunmaktadır. Bu araçlar aşağıda detaylı olarak ele alınmıştır.

4.1.1 Çerezler

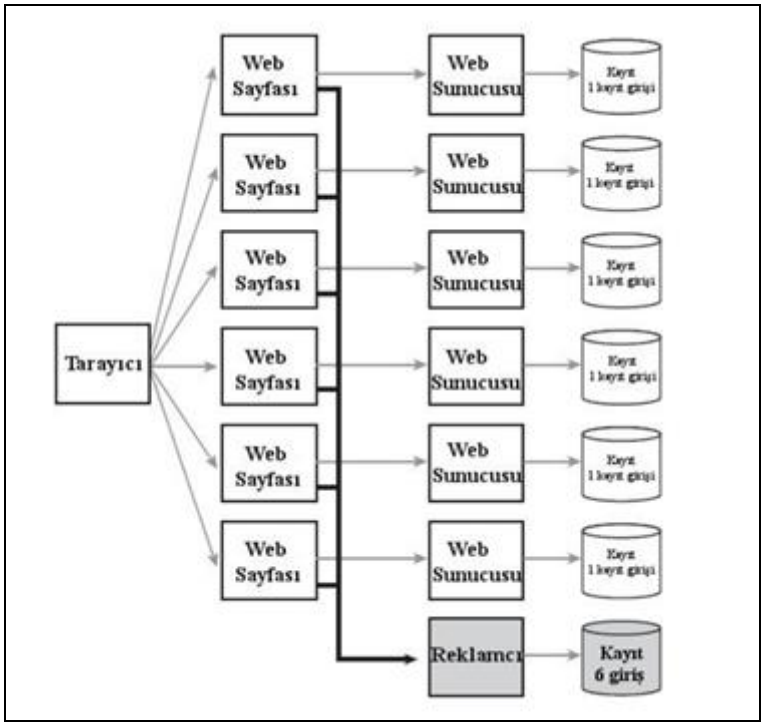
İnternet siteleri daha hızlı ve kolay bir iletişim sistemi kurmak için kullanıcıların cihazlarına çok küçük boyutlu çerez adı verilen dosyalar yükleyebilmektedir. Bu dosyalar aslında kullanıcının internet sitesi üzerindeki alışkanlıklarıyla ilgili değerli bilgiler vermektedir. Bu durum da bir sonraki aşamada kişiye özel reklam gösterme gibi bir sonucu ortaya çıkarmaktadır. Greg Conti "Googling Security: How Much Does Google Know About You" adlı kitabında çerezleri doğa bilimcilerinin hayvanlara yerleştirdikleri takip cihazına benzetmiştir. Davranışsal reklamcılık gibi alanlarda çerez kullanımlarına rastlamak mümkündür. Genel olarak kalıcı ve oturum çerezleri olmak üzere iki tür çerez kullanılmaktadır. Kısa süre için kullanılan oturum çerezleri o anki işlemin gereği için oluşturulmuştur. İnternet bankacılığı gibi işlemlerde görülmektedir. Kullanıcı internet bankacılığı hesabını her açtığında bir oturum çerezi kullanmaktadır. Etkileşimi hızlandıran çerez uygulaması olmasaydı kullanıcı göndereceği her talep için oturumunu tekrar açmak zorunda kalacaktır. Uzun süre olarak varlığını koruyan çerezler ise kalıcı çerezler olarak adlandırılmıştır. Bu çerez kullanıcının takip edilmesini sağlamaktadır. Kullanıcı çerezle ilişkili olan internet sitesine giriş yaptığında aslında o sitesinin sunucusuna giriş yapmaktadır. Kullanıcı reklam ağında yer alan bir internet sitesine ulaşmak gibi bir amacının olmadığı olaylar dışında reklam ağları da benzer bir çerez sistemini kullanmaktadır. Bu tip çerezler ise genellikle TPC (Third Party Cookies

- Üçüncü Taraf Çerezler) olarak adlandırılmaktadır. İnternet siteleri reklam işletmelerinin gömülü içeriğini yayınlamak için bu çerez sistemini kullanmaktadırlar.

Herhangi bir çerezin yapısını açıklamak için kullanılan çalışmada DoubleClick sistemi göz önünde bulundurulmuştur (Bebber, 2011: 24).

Çerezler genel olarak benzer yapılara sahiptir. Her çerezin adı, alan adı, içeriği, yolu ve bitiş tarih alanı bulunmaktadır. Davranışsal reklamcılık söz konusu olduğunda içerik alanı ögesi öne çıkmaktadır. Çünkü bu öge aynı zamanda bir tamamlayıcı içermektedir. Greg Conti, Google'a ait çerezlerin 2 yıl sonra tamamlandığını belirtirken Yahoo çerezlerinin 29 yıl sonra tamamlandığını belirtmektedir. Ancak Google'a ait çerezler Google'a her giriş yapıldığında otomatik olarak tekrar uzatılmaktadır. Kullanıcıların bu süre içinde defalarca Google'ı ziyaret ettiği düşünüldüğünde çerezlerin sistemde her zaman kayıtlı olarak kalacağı sonucuna ulaşmak mümkündür.66 Gömülü durumda olan içerik ile reklamcının sebep olduğu çerez nedeniyle bir kullanıcı birden çok internet sitesini ziyaret ettiğinde reklamcı kullanıcının tercihleri hakkında değerli bilgiler edinebilmektedir. Aşağıda yer alan şekilde reklamcının kullandığı çapraz site takibi yer almaktadır (Bebber, 2011: 25).

Şekil 4. 1 Bir reklamcının çapraz site takibi



Kaynak**:** Bebber, P. V. (2011). Informed Consent in Behavioral Advertising. *Master Thesis Information Science*. Radboud University Nijmegen, s. 26

Şekle göre farklı internet sitelerinin 6 kez ziyaret edilmesi durumunda reklam ağının sunucusunda 6 adet kayıt girişi oluşturulmaktadır. Doğrudan ziyaret edilen internet siteleri reklam ağında bulunan gömülü içerikleri kendi bünyesinde taşımaktadır (Bebber, 2011: 24). Cihazın içinde yüksek dereceli bir güvenlik ayarı yapsa bile işletmeler çerez dosyalarını kullanarak bütün kullanıcıları tespit etme olanağına sahiptir. Tespitlerin temelinde ise kullanıcıların internet tarama geçmişleri bulunmaktadır. Yüksek dereceli güvenlik seviyesine sahip olan kullanıcılar nedeniyle işletmeler daha yoğun araştırma çalışmaları yapmak zorunda kalmaktadırlar. Buna rağmen işletmeler çevrimiçi reklam faaliyeti yapma konusunda çok sayıda olanağa sahiptir (Bloux ve Desfougeres, 2011: 44). Üçüncü kişilerin tarayıcı geçmişi bilgilerine ulaşmasını engellemek isteyen bir kullanıcı çerezleri silebilmektedir. Ancak kullanıcının haberi olmadan sisteme yüklenen bir flash çerez, silinen çerezden bir tane daha oluşturabilmektedir (Arrington, 2013: 16).

4.1.2 Web İşaretçileri

Web işaretçisi, bir elektronik posta iletisine veya internet sayfasına kimin ulaştığını takip etmek için oluşturulmuş iletide veya sayfada yer alan çok küçük bir grafiktir. Genellikle görünmez niteliğe sahip, renge sahip olmayan, 1x1 büyüklüğünde grafiklerdir. Bu grafikler genel olarak Java Script'te yazılmaktadırlar. Bu işaretçiler sayfanın daha hızlı bir şekilde yüklenmesi için tarayıcının önbelleğinde yer almaktadır. Java Script'in kullanımı sayesinde sunucuya kullanıcının ekran boyutu gibi ek bilgiler gönderebilmektedir (Bebber, 2011: 27). Kullanıcı elektronik posta iletisini okurken 1x1 boyutundaki görüntü eklenmektedir. Bir web işaretçisi kullanılarak çok sayıda kullanıcıyı takip etmek istiyorsa ad alanı bölümüne benzeri olmayan bir tanımlayıcı ekleyebilmektedir (Bebber, 2011: 26).

4.1.3 Facebook

Body ve Ellison (2007: 210) sosyal iletişim sitelerini şu şekilde tanımlamışlardır: Kullanıcı olarak belirli kurallara ve sınırlara sahip bir sistem içinde halka tamamen veya gizli bir şekilde oluşturulan profillerle kurulan internet temelli iletişim faaliyetleridir. Oluşturulan listelerde bulunan arkadaş profilleri birbiriyle çok sayıda içerik

paylaşabilmekte, içeriklerle ilgili ayrıntılara ulaşılabilmekte ve bağlantı kurulan kullanıcıların iletişim kurdukları diğer kullanıcılarla iletişime geçilebilmektedir. Yapılan paylaşımların yapısı ve sistemi her sosyal ağda farklılaşmaktadır. Sosyal ağın bir diğer özelliği ise tanıdığımız kişilerle etkileşime girmenin yanı sıra tanımadığımız insanlarla da etkileşime girme olanağı sunmasıdır (Martinez, 2011).

Kullanıcı sosyal ağ üzerinde kendisine bir profil oluşturarak kayıt işlemini gerçekleştirmektedir. Kullanıcı isim, yaş, ilgi alanları, meslek gibi bilgilerini girerek ve bir profil resmi seçerek ilgili siteye kaydolmaktadır. Profil oluşturma işlemi bittikten sonra kullanıcı başka profilleri ziyaret edebilmekte ve çeşitli grupların içine katılabilmektedir. Kendi ağına profilleri ekleyen kullanıcı farklı profilleri farklı gruplar altında toplayabilmektedir. Bunlar genellikle arkadaşlar, bağlantılar, takipçiler gibi isimler almaktadırlar (Tene ve Polonetsky, 2012: 281).

Pazarlama konusunda araştırma yapanlar sosyal medyanın önemine varmış olacaklar ki sosyal medya kullanıcı sayısıyla ilgili çok sayıda istatistik üretmişlerdir. 2004 yılında kullanıma açılan Facebook 2014 itibariyle 600 milyondan fazla kullanıcıya ulaşmıştır (newsroom, 2019). Kullanıcıların birbirlerini sosyal ağlara davet etmesi ile büyümüş ve küresel bir platform ortaya çıkmıştır. İnsanlar bu alanlarda yoğun bir şekilde fotoğraf, yazı paylaşımı yapmış ve birbirlerini arkadaş olarak eklemişlerdir. Sosyal iletişim ağında kullanıcılar ilgi alanıyla ilgili bir gruba katılabilmekte ve ilgilendikleri bir haber üzerinden tartışma gerçekleştirebilmektedirler (Bloux ve Desfougeres, 2011: 2).

Facebook platformu önemli bir pazarlama platformudur. Ağ bağlantılı bir iletişim sistemine sahiptir. İşletmeler hem görünürlük kazanmak hem iyi pazarlama çalışmalarına ulaşmak için bu platformda yapılan iletişim çalışmalarını bütünleştirmişlerdir. Facebook, markaların incelenmesi konusunda yeni yöntemler keşfetmiş ve bunları uygulamaya geçirmiştir. Bu yöntemle araştırma ve satın alma gibi önemli olayları başka bir boyuta geçirmiştir. Ayrıca kullanıcılar alışveriş yaptıkları markaları platform üzerinden duyurmaya başlamıştır. Herhangi bir ürüne ait olumlu veya olumsuz bilgiyi ağda herkes görebilmektedir (Bloux ve Desfougeres, 2011: 3).

Facebook uygulamaları kullanıcıların kimlik bilgilerini herhangi bir bildirimde bulunmadan reklamcılıkla ilgili faaliyet yürüten işletmelere gönderebilmektedir. Bu durum milyonlarca kullanıcıyı ilgilendirmektedir. Kullanıcı kendi bilgilerini en yüksek

gizlilik seviyesinde saklıyor olsa bile bilgi sızıntısı gerçekleşmektedir. Çok büyük bir bilgi birikiminin olduğu Facebook'ta gizlilik seçeneklerinin zayıf olması şaşırtıcıdır (Martinez, 2011).

Facebook'ta kullanılan davranışsal reklamcılık faaliyetinin bir başka avantajı öne çıkmaktadır. "Like" (beğen) tuşunun kullanılmasıyla birlikte aslında tüketici ile işletme arasındaki bağ derinleşmekte ve bunun var olduğuna dair bir taahhüt oluşturulmaktadır. Sonuç olarak ortaya bir topluluk çıkmaktadır (facebook, 2019). Kullanıcı ilgili oluşumu beğendikten sonra hesapla ilgili bütün paylaşımları ana sayfasında öncelikli olarak görmeye başlamaktadır. Aktarılan reklamlarla birlikte kullanıcı, kullanıcının arkadaş çevresi ve diğer beğenilerle birlikte oldukça zengin profillerin oluşturulacağı açıktır. Birçok Facebook kullanıcısı siteye kayıt yaparken gerçek ismini kullanmakta ve kendisiyle ilgili gerçek bilgileri sisteme girmektedir. Facebook'un kişiye özel reklam oluşturma çalışmalarında kullanıcının sisteme verdiği bilgileri kullanıp kullanmadığı tartışılmalıdır (developers.facebook, 2019).

Reklama tıklayan kullanıcı doğrudan işletmeye ait Facebook hayran sayfasın ulaşmaktadır. Bu sayfanın içeriği işletmenin resmi internet sitesinden birçok yönden farklılıklara sahiptir. Kullanıcı bu sayfaya yönlendirilerek beğenme beyanıyla ilgili sonuçlara ulaşmaktadır. Buna göre kullanıcı artık beğendiği işletmenin bütün reklam faaliyetlerinden haberdar olacaktır. İşletme özelleştirmiş olduğu Facebook duvarında uçuşlarla ilgili fiyat bilgilerini veya insanların KLM uçaklarıyla ilgili çizmiş olduğu görselleri yayınlamaktadır (Bloux ve Desfougeres, 2011: 34).

İşletme yaptığı özel paylaşımlarla işletme ile tüketici arasındaki iletişimi etkin bir hale getirmektedir. Kullanıcılar da aslında duygularını ifade edebildikleri bir alan elde edebildikleri için markaya bağlanma gibi davranışların görülmesi kaçınılmaz olmaktadır. İşletme ile tüketici tartışma alanının açık olduğu özgün bir platform oluşturma olanağına sahip olmaktadır. İnternet ağları ile insanları bir araya getirme olanağını etkin bir şekilde kullanmak çok önemlidir. Bu şekilde reklamla ilgili mesajları çok daha fazla insana dağıtmak mümkün olabilmektedir. İşletmenin Facebook sayfasında işletmeyle ilgili çok sayıda bilgi yer almaktadır. Kullanıcı burada yer alan bilgilerle birlikte işletmenin ana sayfasına ulaşabileceği bir bağlantıyı da kullanabilmektedir. Bu örneklerle birlikte bir veya daha fazla tıklamayla yoluna devam

etme olarak tanımlanabilecek tıklama teorisi arasında bazı bağlantılar bulmak mümkündür. İşletmeler buradan yola çıkarak sayfalarını beğenen kullanıcıların tıklama davranışından yola çıkarak çeşitli faydalar elde edebileceğini düşünmüştür (Bloux ve Desfougeres, 2011: 35). Beğenme tuşunun var olmasıyla birlikte kullanıcıların aslında nelerle ilgilendiğini tam olarak belirlemek mümkün olabilmiştir. Hangi yönde yapılacak uçuşların, hangi hizmetlerin ilgi çektiğini beğeni sayısından belirlemek mümkündür. Beğenme ve tıklama haricinde kullanıcının hayran sitesinde hangi bölümlere ziyaret gerçekleştirdiklerini belirlemek mümkün olabilmektedir. Ayrıca kullanıcının nelerden etkilendiğine yönelik çıkarımlar yapmak mümkündür (Bloux ve Desfougeres, 2011: 35).

Gizlilik Konusu: Çevrimiçi gizlilik olarak bilinen E-Gizlilik, bireyin çevrimiçi olarak kimse tarafından takip edilmemesini ve izlenmemesini garanti altına almaktadır. Birey buna göre herhangi bir kısıtlama altında olmadan özgürce hareket edebilmektedir. Kişisel bilgiler kişinin rızası olmadan kayıt altına alınıp toplanamamaktadır. Kullanıcı kendi ilgi alanına doğrudan uyan bir ürün veya hizmetle ilgili reklamla karşılaştığında kişisel bilgilerinin kullanıldığını hissetmektedir. Bu sorunun önüne geçebilmek için Facebook gibi sitelerde gizlilikle ilgili özel bir alan oluşturulmuştur (Bloux ve Desfougeres, 2011: 15). Gizlilik ayarı yüksek bir seviyede belirlendiğinde birey paylaştığı bütün bilgilerin ve paylaşımların sadece kendi seçtiği kullanıcılarla sınırlı kaldığını düşünmektedir. Bu şekilde herhangi bir özel reklam uygulamasının gerçekleştirilmeyeceği varsayılmaktadır. Gizlilik ayarının kullanıcılar tarafından kullanılmamasının birçok sebebi vardır. İnternet sitesinin kullanıcıya yeterli bilgi vermemesi bu sebepler arasında sayılabilmektedir. Kullanıcı internet sitesinin sunduğu hükümler ve koşullar gibi belgeleri okumadan kabul tuşuna bastığı için aslında farkında olmadan birçok bilgisini kullanıma açmaktadır. Bunu yaparak üçüncü kişilerin bilgi kullanımına da olanak tanınmaktadır (Bloux ve Desfougeres, 2011: 16).

Davranışsal reklamcılık faaliyetlerine yönelik tam güvenin oluşturulması için kullanıcılara birtakım yetkinlikler tanınmıştır. İlgili reklam ağları opt-out (opted out for receving - reddetme hakkı - herhangi bir ürün veya hizmet bilgisi alma seçeneğinin dışında kalmak) adı verilen bir uygulamayı devreye sokmuştur. Kullanıcılar bu aracı kullanarak internet üzerinde kimlerin kendi davranışlarını takip ettiğini görebilmektedir. Kullanıcı bu belirleme sürecini tamamlamak isterse “opt-out” tuşunu

kullanabilmektedir. Bu uygulama bir anda bütün çevrimiçi reklamları ortadan kaldırmamaktadır. Ancak kullanıcılar davranışsal reklamcılık konusunda bilinçlendikleri için bu reklamcılık alanına ilgi göstermeye başlamışlardır. Kullanıcıların bu uygulamada kendilerini rahat hissetmeleri için iletişim ve eğitim çok önemlidir. Kullanıcılardan alınacak olan geri dönüşler uygulamanın performans düzeyini de en yukarıya çekecektir. Sonuç olarak davranışsal reklamcılığın temel amacı reklamcılığa olumlu anlamlar katmaktır (Bloux ve Desfougeres, 2011: 32). Bu durum daha sonra kullanıcılara da yansıyacaktır.

Yapılan analiz çalışmalarına göre birçok kullanıcı Facebook'ta yer alan davranışsal reklam konusunda kendisini tam olarak güvende hissetmemektedir. Buna göre birçok kullanıcı ya bilgilerini tamamen gizlemekte ya da bilgilerini herkese açmaktadır. Bu da profil gizleme veya açma ile gerçekleştirilmektedir (Bloux ve Desfougeres, 2011: 35). Bilgilerin etkin bir şekilde aktarılması ile bir güven ortamının oluşturulması sağlanmalıdır. Reklam kampanyaları oluşturulurken kullanıcıların geri dönüşleri göz önünde bulundurulmalıdır. Davranışsal reklamcılık konusunda kullanılan opt-out fonksiyonu ise reklamları doğrudan devre dışı bırakan bir seçenek olarak kullanılmaktadır. Bu seçenek kullanıcılara davranışsal reklamları engelleme seçeneği verdiği için insanlar gizlilik konusunda kendisini biraz daha rahat hissetmeye başlamışlardır (Bloux ve Desfougeres, 2011: 38). Ancak araştırmalara göre en üst düzey gizlilik ayarı kullanılsa bile işletmeler çerezleri veya diğer yöntemleri kullanarak kullanıcının ilgilendiği alanları tespit edebilmektedir. Çok sayıda gizlilik seçeneğini etkin bir şekilde kullanan kullanıcı ise işletmenin hedef tespitinin dışında kalacaktır. Ancak işletmenin davranışsal reklam konusunda tahminler yaparak hedef kitleye ulaşma konusunda çalışmalar yapabileceği unutulmamalıdır (Bloux ve Desfougeres, 2011: 38).

4.1.4 Tarayıcı Parmak İzleri

Diğer adı cihaz parmak izi olan tarayıcı parmak izi cihaza ait donanım ve yazılımla ilgili bilgilerden oluşmaktadır. Çözünürlük gibi konfigürasyona ait bilgileri de bu kapsamda değerlendirmek mümkündür (Bebber, 2011: 29).

4.1.5 Derin Veri Analizi

İnternet sayesinde kullanıcılardan detaylı şekilde bilgi edinmek mümkündür. Buna göre oluşturulan reklamlar kişiye özel olabilmektedir. Bu sayede davranışsal reklamlar

amacına uygun olacak şekilde kullanılmaktadır. Kullanıcıya sağlanan yararlar dışında çeşitli endişeler de kendini göstermektedir. Toplanan bilgiler neticesinde tahmini gelir aralığı için özel bir hedef fiyat belirlemesi olasılığı artmaktadır. Bu durum çevrimiçi pazarlama sistemine zarar verecek bir konumdadır. Sonuç olarak bu alan kendi potansiyelinin altında bir gelişim göstermektedir (Trading, 2010).

Belirli bir profil oluşturmak için elde edilen verinin ana kaynağında çevrimiçi izleme yer almaktadır. Bu yöntem sayesinde kullanıcıların hangi sayfayı ziyaret ettikleri, ne kadar ziyarette kaldıkları hesaplanabilmektedir. Veriler elde edilmekte ve belirli bir sıraya konmaktadır. Çevrimiçi izleme işlemi çerezlerle IP'lerin takip edilmesiyle gerçekleştirilmektedir. İzleme işlemi yapılırken genel olarak Javascript, Süper Çerezler, Tarayıcı Parmak İzleri ve Derin Veri Analizi adı verilen uygulamalar kullanılmaktadır.

Derin Veri Analizi internet servis sağlayıcıları tarafından kullanılmaktadır. Bu uygulamanın çok sayıda tartışmaya neden olduğu bilinmektedir. Özellikle akıllı telefonların ortaya çıkmasıyla birlikte karmaşık donanımların ve sistemlerin kullanılmasıyla kullanıcının ne zaman, nerede olduğu gibi çok değerli sonuçlar da elde edilmiştir. Bu sayede kullanıcı için daha detaylı bir profil oluşturma olanağı ortaya çıkmaktadır (Castelluccia ve Arvind, 2012: 6). Bu noktada kullanılan bir diğer izleme uygulamasının adı üçüncü taraf izleme uygulamasıdır. Genel olarak kullanıcıların alışık olmadığı bir uygulamadır. Bu izleme türünde kullanıcıya ait tarayıcıdaki internet faaliyeti kullanılmaktadır. Kullanıcının sürekli olarak kullandığı internet siteleri esas olarak alınmakta ve bireysel profiller oluşturulmaktadır. Bu sayede reklamlar hedefine ulaşmaktadır. Ele edilen ve tasnif edilen verilerle profil oluşturma çalışması yapılmaktadır. İnsanları endişeye sürükleyen bu uygulamanın adı "Çevrimiçi Davranışsal İzlemedir (Tene ve Polonetsky, 2012: 283)".

İnternet üzerinden oluşturulan mesajlaşma sisteminde tarafsız bir iletişim sisteminin var olması gerektiği düşünülmüştür. Bu ilkeye net tarafsızlığı adı verilmiştir. Buna göre ilgili paketler adres bölümünü görmekte, içeriğe ulaşamamaktadır. Bu unsurların adı routerdır. Askeri ve akademik amaçlarla kurulan internet sisteminde uzun süre boyunca net tarafsızlığı egemen olmuştur. Web sisteminin dünyaya yayılmasıyla birlikte bireysel ve ticari kullanıcılar bu ağa katılım göstermiş ve iletişim sistemi başka bit boyuta taşınmıştır (Kırlıdoğ ve Fidaner, 2012: 967). Küresel bir kullanım seviyesine ulaşan

internet sisteminde çok sayıda güvenlik sorunu ortaya çıktığı için güvenlik yazılımları devreye girmiştir. Bu bağlamda IDS (Intrusion Detection System - Saldırı Sezme Sistemi) adı verilen sistem oluşturulmuştur. IDS sunucu ve ağlarda bulunan saldırıları belirlemekte ve engellemektedir. Sunucuda veya ağda yer alan bütün faaliyetleri izleyen bu sistem bilinen güvenlik sorunlarıyla bir karşılaştırma yapmaktadır. Çeşitli yazlım imzalarıyla ile karşılaştırma yapılır. Herhangi bir sistem bozukluğu tespit edilmişse bunlar algılanmaktadır. IDS, ağdan geçmekte olan verilerin bütün içeriğini de incelediği için belirli sınırlar içinde de olsa net tarafsızlık ilkesini ihlal etmektedir (Kırlıdoğ ve Fidaner, 2012: 967). İnternet zamanla daha önemli bir kavram haline gelmiştir. Bu yüzden IDS'ten ilham alan, DPI (Deep Packet Inspection - Derin Veri Analizi) isimli yeni bir teknik oluşturulmuştur. Paket içeriğinin belirli bölümlerini inceleyen geleneksel router sisteminde farklı olarak DPI sistemleri var olan paketin bütün unsurlarını inceleyebilmektedir. 7 katmanlı OSI (Open Systems Interconnection - Açık Sistemler Arabağlaşımı) modelinde ise adreslemenin yapıldığı fiziki birinci katmandan itibaren bütün katmanlar inceleme altında olmaktadır. Bu sayede bütün içerikler detaylı bir şekilde analiz edilmektedir. DPI sistemi iletişimde yer alan bütün içerikleri algılayıp tasnif yapmayla birlikte bütün içerikler başka bir ortama kaydedilebilmektedir. Bununla birlikte birinci ile dördüncü katmanları inceleyen analiz Sığ Veri Analizi (Shallow Packet Inspection) adı verilen sistemlerle veya benzeri yöntemlerle yapılmaktadır. DPI aslen bir posta servisinin ilettiği bütün mektupları okumasına benzer bir sürece sahip görünmektedir. DPI sisteminin özel hayatın gizliliği konusunda ciddi endişelere neden olduğu açıktır (Kırlıdoğ ve Fidaner, 2012: 967). DPI sistemleri ISP'ler tarafından uygulanmaktadır. ISP kullanıcıları özel hayatın gizliliği konusunda ciddi risklerle karşı karşıya kalmaktadır (Kırlıdoğ ve Fidaner, 2012: 967).

Çevrimiçi olarak yapılan izleme teknikleri zamanla büyük bir gelişim göstermiştir. Çerezler, süper çerezler, tarayıcı parmak izleyici ve aygıt kimlikleyici gibi yöntem ve teknikler genel olarak kullanılmaktadır. Yoğun bir bilgi birikiminin oluşması ile izleme teknolojileri çok daha etkin hale gelmiştir. İzleme teknolojileri kendisi için önemli olan bilgileri kullanarak kendisini daha etkin bir konuma getirmektedir. Bununla birlikte verilerin toplanıp kayıt altına alınması kolay hale gelmiştir. Sonuç olarak düşük bir maliyet ortaya çıkmıştır. İşletmeler elde toplanmış olan verilerin yönetilebilmesi için iş süreçleri oluşturarak yenilikçi yollara yönelmenin yollarını araştırmıştır (Tene ve

Polonetsky, 2012: 288). DPI kurumsal seviyede veya ulusal düzeyde olabilmektedir. Tek bir ağa ait akışlar için kullanıldığında ağ güvenliği, yük dengeleme, internet kullanımına kısıtlama getirilmesi veya izlenmesi gibi kurumsal etkinlikleri gerçekleştirmek mümkün olabilmektedir. Eğer bir DPI bir ISP tarafından ulusal seviyede kullanılacaksa izlemenin derinlik seviyesi yükselmektedir (Kırlıdoğ ve Fidaner, 2012: 967). Örneğin, ISP'ler, DPI sistemine başvurarak yoğun bir ağ trafiğine neden olan BitTorrent dosya paylaşımı sistemini sık bir şekilde kullanan aboneleri tespit edebilmektedir. Benzer şekilde ISP zararlı olarak gördüğü birçok içeriğe engel koyabilmekte, belirlediği kısıtlama politikalarına başvurabilmektedir. Çeşitli ticari amaçlar için de izleme politikası uygulamak mümkündür. DPI istatistiksel çıkarımlar yapmak için kullanıcıların ağ kullanım değerlerini ciro ile karşılaştırarak işletmenin nasıl bir kâr oranına ulaştığını belirleyebilmektedir (Kırlıdoğ ve Fidaner, 2012: 698).

Devlet DPI aracılığıyla yasadışı olarak kabul edilebilecek birçok içeriğe ve internet sitesine erişim yasağı getirebilmektedir. Bunların gözetim ve sansür amaçlı olarak kullanımı görülebilmektedir. Genel olarak kabul görmüş suçların engellenmesi konusunda bu izleme sistemlerinin kullanılmasını birçok kişi doğal karşılamaktadır. Ancak muhalif hareketleri izlemek veya insanları kontrol altında tutmak gibi yasaya uygun olmayan izleme uygulamalarının görülmesi olumsuz bir durum olarak ortaya çıkmaktadır. Birçok uygulama incelendiğinde devletin kontrol amaçlı olarak bu uygulamalara yöneldiği görülmektedir. DPI gözetimini gerçekleştirmek için devlet ISP ile iş birliği yapmak zorundadır. Bu iş birliğini yasal bir gerekçeye dayandırmak da mümkündür. Devletin iznine ihtiyacı olan ISP'nin iş birliği yapacağı ise kesin gibidir. Sonuç olarak DPI sistemi sayesinde yetkili kişi ve kurumlar sınırsız bir izleme sistemine sahip olabilmektedir. Bu durum kullanıcının özel yaşamının gizliliğinin ihlali anlamına gelmektedir (Kırlıdoğ ve Fidaner, 2012: 968). Devletler internet iletişim sisteminde yer alan bütün verileri kayıt altına almak isterken yasal, teknik ve toplumsal engellerle karşı karşıya kalmaktadır. Akan veri o kadar yüksek bir seviyede olmaktadır ki teknik açıdan zorlukların var olması kaçınılmaz hale gelmektedir. Veriler eksiksiz bir şekilde kayıt altına alınsa dahi analiz edilmesi çok sayıda zorluğa sahiptir. Elektrik süpürgesi adı verilen bu yöntemde bir kanaldan geçen bütün verilerin tam olarak analiz edilebilmesi DPI için mümkün olamamaktadır. Ancak ISP'lerde mevcut bulunan özel DPI "kutuları"

sayesinde bireyleri teknik olarak takip etmenin yolları bulunmaktadır (Kırlıdoğ ve Fidaner, 2012: 968).

Derin veri analiz teknolojisi sayesinde izleme sistemlerinde yeni bir dönemin başlaması sağlanmıştır. Bu yöntemin varlığı ile heyecan ve endişe birbirini izlemiştir. Daha önceleri internet servis sağlayıcıları bu yöntemi güvenlik amacıyla kullanmıştır. Daha sonra reklamcılık işletmeleri çalıştıkları internet sitelerinde kategorilere ayırma ve kişiye özel banner şeklinde reklamlar oluşturma gibi uygulamalarla bu yöntemi kullanmaya başlamışlardır. CDT Başkanı (Democracy and Technology Center - Demokrasi ve Teknoloji Merkezi) Lesie Harris'e göre bu durum bir posta hizmeti veren işletmenin ilettiği bütün mektupları açıp okuması durumuyla eş değer olarak görülmelidir (Tene ve Polonetsky, 2012: 298). Derin veri analizi ile reklamcılar çevrimiçi olarak faaliyet gösteren bütün faaliyetleri detaylı bir şekilde analiz etmekte ve buna göre oluşturulan profillere özel olacak şekilde reklam hizmetleri sunulmaktadır. İnternet servis sağlayıcılarla ortaklık şeklinde çalışan reklam ağları bireylerin sahip olduğu çevrimiçi trafikleri sayesinde oluşturulan özel profillere uygun reklamlar üretebilmektedir. Bu, çevrimiçi trafik internet servis sağlayıcısının kendi sistemi içinde yürümektedir (Tene ve Polonetsky, 2012: 298). Derin veri analizi ile hedefe yönelik yapılan reklamcılık çalışması için yoğun tepkiler ortaya çıkmıştır. Bu yüzden ABD (Amerika Birleşik Devletleri)'de bulunan internet servis sağlayıcıları böylesi bir reklamcılık modelinin kullanımının ancak kullanıcı rızasıyla mümkün olabileceğini taahhüt etmişlerdir. Derin veri analizi ile faaliyetlerini sürdüren NebuAd bu açıklamalardan ve tepkilerden sonra kapanmak zorunda kalmıştır. İngiltere'de benzer faaliyetler yapan Phorm isimli işletme de benzer şekilde faaliyetlerini sonlandırmak zorunda kalmıştır. Phorm şimdilerde sadece Kore ve Brezilya'da faaliyetlerini sürdürmektedir. ABD'de Opt-In modeline yönelmiş olsa da başarılı olamamıştır (Tene ve Polonetsky, 2012: 299).

İnternet sitelerinin ve servis sağlayıcılarının sistemleri içinden geçen bütün hareketleri kayıt altına alırken çeşitli sebepler öne sürülmektedir: Hizmeti engelleme, virüsler ve istenmeyen elektronik postalar gibi olumsuz olayları engelleme, çevrimiçi olarak gerçekleştirilen trafik akışına bir kontrol getirme ve telif hakkı korumadır (Tene ve Polonetsky, 2012: 304). Devletler yasal bir nedene bağlı olarak dinleme ve izleme yapabilmek için internet servis sağlayıcılarından derin veri analizi yönteminin

uygulanmasını talep etmişlerdir. Birçok yönetim belirlenmiş bazı politikalar ve uygulamalar çerçevesinde derin veri analizinin uygulanmasında herhangi bir sakınca görmemektedir. Bununla birlikte derin veri analizinin davranışsal reklamcılık alanında uygulandığı görülmektedir. Phorm, Front Porch ve NebuAd gibi işletmeler derin veri analizi yöntemini kullanarak bilgisayarlar aracılığıyla kullanıcının çevrimiçi hareketlerini izlemenin yöntemini bulmuşlardır. Hareketleri izleyerek ayrıntılı profillere ulaşmak mümkündür. Bunlar davranışsal profillerdir. Derin veri analizi yöntemi sayesinde bütün trafiği izlemek mümkün olabilmektedir. Kullanıcı da daha sonra kendisine hedeflenmiş reklamlarla karşı karşıya kalmaktadır. Mevcut bulunan reklamların yerini bu reklamlar almıştır (Butler, Teddy ve Waugh, 2006: 3).

Derin veri analizi ile kullanıcının internet trafiğinde yer alan bütün detaylara ulaşmak mümkündür. Analiz aşamasında başka verilerin katılımı ile yapılacak veri madenciliği çalışması çok önemli bilgilerin elde edilmesini sağlamaktadır. Verilerin işlenmesiyle detaylı profillere ulaşılmaktadır. Derin veri analizinde izleme tekniği ISP tabanlı kullanıldığı için kullanıcının bütün internet verileri kolay bir şekilde tasnif edilebilmektedir. Bu da çerezlerden elde edilecek bilgiden çok daha büyük bir bilgi kaynağına neden olmaktadır. Yoğun bir bilgi içeriğine sahip olan trafiğe ait veriler ISP'lerde yer alan detaylı üyelik bilgileri ile eşleştirilmektedir. Buralardan elde edilen bilgilerle yapılan DPI tabanlı davranışsal reklamcılık faaliyetleri çerezler kullanılarak yapılan davranışsal reklamcılık faaliyetinden çok daha yüksek bir katma değere neden olmaktadır. Gözetim amacıyla yapılan DPI uygulamalarıyla ilgili çok sayıda örneğe rastlanmaktadır (Berber, 2013: 26).

ABD'de DPI bir gözetim aracı olarak kullanılmaktadır. James Bamford The Shadow Factory adlı kitabında bu kullanımla ilgili detaylı bilgilere yer vermiştir. Ülkedeki internet pazarını kontrol altında tutan AT&T ve Verizon isimli işletmeler DPI konusunda uzmanlaşmış olan Narus ve Verint adlı işletmelerle ortaklık kurmuşlardır. Bu işletmeler internet trafiğinin geçtiği özel tesislerde bulunan ve diğer insanların erişiminin olmadığı özel odalarda faaliyetlerini sürdürmektedir. Internet trafiğinde gerçekleşen olayların kayıtları bu tesisten geçerek bir kopya olarak NSA (National Security Agency - Ulusal Güvenlik Dairesi) bilgisayarlarına iletilmektedir (Kırlıdoğ ve Fidaner, 2012: 969). Bamford bir ülkenin neredeyse bütün internet trafiğinin iki işletmenin donanımından geçtiğini belirtmektedir. Bu trafiği uzaktan kolay bir şekilde

yönetmek mümkündür. ABD vatandaşı olmayan insanların da endişelenmesi gerekmektedir. Çünkü dünyada gerçekleşen internet trafiğinin önemli bir bölümü ABD üzerinden gerçekleşmektedir. Herhangi verinin bu noktalarda yer alan bir cihaza verisini kopyalaması mümkündür (Kırlıdoğ ve Fidaner, 2012: 969).

İngiltere Avrupa'da kendi vatandaşlarını dinleme konusunda büyük bir üne sahip olan ülke olarak öne çıkmaktadır. Ülkenin elektronik casusluk teşkilatı GCHQ (Government Communication Headquarters - Hükümet İletişim Merkezi) internet üzerinden yoğun bir iletişim faaliyetinin oluşması üzerine 2008 yılında IMP (Interception Modernisation Programme) adı verilen bir projeye başlamıştır. İki milyar sterlinlik bütçeye sahip olan bu proje internet ağırlıklı olsa da genel olarak telefon dinlemelerini kapsamıştır. Buna göre ülkede bulunan bütün ISP işletmelerini DPI donanımı yüklenecektir. Projenin duyurulmasıyla birlikte büyük bir tepki dalgası ortaya çıkmıştır. Saygın bir kurum olan London School of Economics bir rapor hazırlayarak projenin neden uygulanmaması gerektiğini ayrıntılı bir şekilde anlatmıştır. Tepkiler nedeniyle projeyi geri çeken İngiltere hükümeti kısa süre sonra benzer bir içeriğe sahip olan CCDP (Communications Capabilities Development Programme) adlı başka bir proje için çalışmalara başlamıştır (Kırlıdoğ ve Fidaner, 2012: 969).

Türkiye'de bütün içeriğiyle birlikte bilinen tek DPI tekniği faaliyeti 2012 yılında TTNET-Phorm ortaklığı ile oluşturulan davranışsal reklamcılık girişimidir. Özel hayatın gizliliğini ihlal edecek bir sistemin varlığı birçok ülkede tepkilerle karşılanmıştır. Benzeri tepkiler Türkiye'de de ortaya çıkmıştır. Sonuç olarak BTK (Bilgi Teknolojileri ve İletişimi Kurumu) 2012 yılında bir açıklama yayınlamıştır. Açıklamada bir internet sağlayıcısının Phorm Solutions isimli işletme ile ortak faaliyetler sürdürdüğü ve bu faaliyetlerin kişisel bilgi güvenliğini ihlal ettiği yönünde tespitlerin yapıldığına dair medyada haberlerin olduğuna vurgu yapılmıştır. Kişisel bilgilerin gizliliği ve güvenliğe ilişkin birçok konu doğrudan BTK tarafından düzenlenmektedir. Kurum bu çerçevede gerekli önemler almakta ve denetleme çalışmaları yapılmaktadır. Kamuoyunda çeşitli iddiaların dolaşması üzerine BTK tarafından detaylı bir şekilde inceleme yapılmıştır. İlgili işletmenin ülke içi ve dışında yapığı faaliyetler ve diğer ülkelerin işletmeyle ilgili aldığı kararlar ile çok yönlü bir çalışma gerçekleştirilmiştir. Elde edilecek sonuçlara göre gerekli yaptırımların uygulanacağına dair taahhüt BTK tarafından verilmiştir. Sonuç olarak BTK, TTNET'in Phorm isimli işletme aracılığıyla kişisel veri konusunda

ihlali yaptığı iddiasını değerlendirerek Tüketici Hakları Dairesi'nin hazırladığı takriri incelemiştir. 14.12.2012 tarih ve 2012/DK-14/623 sayı ile, kişisel verilerin işlenmesi konusunda Gezinti.com hizmeti kapsamında kullanıcılardan herhangi bir onay almadan kullanıcılara ait bilgiler ne amaçla ne kadar sürede işleyebileceğine dair herhangi açıklama yapmadığı için Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin "Telekomünikasyonun Gizliliği" başlıklı 8. maddesini ve aynı Yönetmeliğin "İzin ve Süre" başlıklı 9. maddesi ve Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin "Şeffaflık ve bilgilendirme" başlıklı 6. maddesini ihlal ettiği için TTNET hakkında soruşturma başlatılmıştır. TTNET, Gezinti.com hizmeti için hiçbir bilgi vermeden otomatik bir şekilde hizmet vermeye başladığı bütün aboneleri bu hizmet kapsamının dışında tutmak zorunda kalmıştır. Gezinti.com hizmeti kapsamında elde edilecek kişisel verilerin ne şekilde, nasıl ve ne sürede işleneceğine dair detaylı bilgilendirme yapılması da bir diğer zorunluluk olarak öne çıkmıştır. İşletme bu detaylı bilgilendirmeyi yaptıktan sonra abonenin veya kullanıcının onayını almak zorundadır. Bu aşamadan sonra abonenin siteye kaydı gerçekleştirilecektir. Gezinti.com'dan ayrılmak isteyen kullanıcının açılır pencerelere yönelmek zorunda kalmasını uygulamasına son verilmiştir. Siteyi terk etmek isteyen kullanıcı kapat tuşuna basarak siteyi terk edebilecektir. Bu hizmetten yararlanmak istemeyen kullanıcının bu isteği bir bilgi olarak kayıt altına alınacaktır. Sitenin ilgili sayfasında hizmet almayı kabul eden kullanıcının siteye kaydı yapılabilecektir (BTK 2012 DK-14/623, 2014).

4.2. İZLEME TEKNİKLERİ

İzleme teknikleri birinci taraf, üçüncü taraf, çevrimiçi sosyal ağ izlemesi, mobil cihaz tabanlı izleme, konum izleme, yeniden özdeşleştirme olarak altı başlık altında incelenebilir.

4.2.1 Birinci Taraf İzleme

İnternet sitesindeki hizmetler genel olarak "birinci taraf" tarafından işletilmektedir. İçerikle birlikte gelen hizmetler internet sayfalarında yer almaktadır. İçerik sunucusuna ait çok sayıda sayfa bulunmaktadır. İnternet sayfalarını ziyaret edenler bu sayfaları kendi bilgisayarlarında kayıt altına alabilmektedir. Bu uygulama bir bilgisayarın herhangi bir program çalıştırmasına benzemektedir. Ziyaretçinin bilgisayarına yüklemiş

olduğu sayfalar sunulan birçok faaliyetle ilgili bilgileri içermektedir. Genellikle birinci tarafın işlettiği sunucularda sunucu ürünün internet sitesi aracılığıyla satılmasına olanak tanımaktadır (Butler, Teddy ve Waugh, 2006).

FPC (First Party Cookie – Birinci Parti Çerez)'yi birçok amaç için kullanmak mümkündür. Örneğin, kullanıcıya tarama yapma esnasında bu çerezler yardımcı olmaktadır. Çerez, alışveriş sepetine ait bilgileri, tercihlerle ilgili ayarları, otomatik bir şekilde gerçekleşecek kullanıcı giriş bilgisi gibi bilgileri içerebilmektedir. Kullanıcıların bildiğine göre TPC (Third Party Cookie - Üçüncü Parti Çerez)'ler gereksizken FPC'ler ise kullanışlı ve gerkelidir (Butler, Teddy ve Waugh, 2006: 1). Bu yüzden kullanıcının FPC'yi silme olasılığı TPC'yi silme olasılığına göre daha düşüktür. Kullanıcı FPC'nin kendisine yardımcı olacağını düşünmektedir. FPC bir kullanıcının ziyaret ettiği internet sitesinin yayıncısı tarafından oluşturulmaktadır. TCP ise ziyareti yapılan bütün internet siteleri için üçüncü kişiler tarafından oluşturulmakta ve yerleştirilmektedir. Kullanıcının bilgisayarına çerezi yerleştiren kişi aslında yasal bir yükümlülük altındadır. Çerezi yerleştiren üçüncü taraf bunu bir internet sitesi aracılığıyla yapıyorsa sorumluluğu paylaşan yayıncı ile kişi arasında sözleşme imzalanmalıdır. Yayıncının çerez kullanımında kullanıcıyı bilgilendirmesi yayıncı için daha pratik bir sonucu ortaya çıkaracaktır (Butler, Teddy ve Waugh, 2006: 1).

Çerezlerin kimler tarafından hangi yollarla yerleştirildiğinin bilinmesi önemlidir. İşletme kendi internet sitesine çerezler yerleştiriyorsa birinci taraf olarak adlandırılmaktadır. Bu esnada çok sayıda üçüncü tarafın işin içine girdiği görülmektedir. Üçüncü taraflar hem kendi internet sitelerine hem de başkalarının internet sitelerine başka birileri için çerezler yerleştirebilmektedir. Bazı çerezleri veya kişileri birinci veya üçüncü parti olarak hareket ederken görmek mümkündür. Davranışsal reklam kullanım sisteminin kullanıcılar dışında ayrıca birçok aktör için de ne kadar zorlayıcı olduğu anlaşılmaktadır. Bu sistemin kullanımı için gerekli olan verilerin önemli bir kısmı çerezler aracılığıyla üçüncü parti üzerinden toplanmaktadır. İnternet sitesi sahipleri veya yayıncılar birinci parti işlevini üstelenerek çerezleri kendi internet siteleri aracılığıyla yerleştirmektedirler. Reklam ağı içinde yer alan aktörler üçüncü parti işlevi görerek başka unsurların kendileri adına çerez sistemini kullanmasına izin vermektedirler. Sonuç olarak TPC'ler internet sayfasının işleyişi

konusunda reklamcılık gibi alanlarda yoğun bir şekilde kullanılmaktadır (Mayer ve Mitchell, 2012: 420).

4.2.2. Üçüncü Taraf İzleme

İnternet sayfaları genel olarak üçüncü taraflardan gelen veriler için hizmet sunmaktadır. Hizmet kapsamında sunulan içeriğin çok sayıda amacı bulunmaktadır. İçerik çeşitli amaçlara sahip olmaktadır. Bunlardan bir reklamcılık olmaktadır. Üçüncü taraf izlemede reklamların ücretsiz hizmetleri desteklemesiyle reklamlar, hedefleme konusunda çeşitli amaçlara sahip olmak istemiştir. Bu da kullanıcıların izlenmesine neden olmuştur. İzleme etkinliğinin farkında olan kullanıcılar bunu engellemek için bazı araçlar kullanabilmektedir (Ajdari ve Hofnagle, 2013: 1)

Üçüncü tarafın izleme faaliyetinde bulunmasıyla ilgili çok geniş bir politikalar zinciri bulunmaktadır. Fayda sahibi bütün kullanıcılar internet ortamındaki izleme faaliyetlerinde bir kontrol mekanizmasının bulunması gerektiğini belirtmişlerdir. Bu konunun bazı ayrıntılarında anlaşmazlıklar görülmektedir (Mayer ve Mitchell, 2012: 417):

1. Kullanıcılar tam olarak hangi noktalarda kontrol sahibi olacaktır? İnternet kullanımı üzerine çeşitli politikalar üretenler kullanıcıların internet üzerinde izleme sonucu veri toplama konusunda kontrole sahip olması gerektiği görüşüne sahiptirler. Reklamcılıkla uğraşan çevrimiçi unsurlar ise kontrol sisteminin daha da genişletilmesini ve verinin sadece belirli kullanım alanları için kullanılması gerektiğini belirtmişlerdir.
2. Saptanmış ve varsayılan değerlerin belirlenmesi bir diğer soru olarak öne çıkmaktadır. Avrupa Birliği politikasını destekleyenler genel olarak izlemenin yapılmaması durumunu varsayılan değer olarak kabul etmişlerdir. Mali gruplar ise bu durumu tartışmaya açmışlardır.
3. Tercih mekanizmasıyla ilgili tasarım kimler tarafından gerçekleştirilmelidir? Reklamcılık faaliyetlerini gerçekleştiren mali gruplar tasarımla ilgili kontrolün kendilerinde olması gerektiğini söylemişlerdir. Politikaya yön verenler ise tasarımla ilgili sorumluluğun tarayıcıyı sağlayanların kontrolünde olması gerektiği belirtmişlerdir (Mayer ve Mitchell, 2012: 417).

Kullanıcılar ve genel olarak Avrupa Birliği politikalarına yön verenler, çevrimiçi gizliliğini bir insan hakkı olarak değerlendirmektedirler. Bazı araştırmacılar ve Amerikan politikasına yön verenler ise, gizlilik konusundaki risklerin kullanıcının inisiyatifine bırakılmasını toplumsal refah açısında bir araç olarak görmektedirler. Bir tarayıcı uygulaması olan Mozilla, bir taraf seçerek kullanıcının izleme konusunda seçeneğe sahip olması gerektiğini önemli bir hedef olarak belirlemiştir. Üçüncü parti internet siteleri ve reklamcılık konusunda ticari çıkarları olan gruplar şu anda devam etmekte olan uygulamaları savunmaktadırlar. Bu gruplar bu uygulamaların toplumun refahı için olduğunu söylemektedirler. Bu hususta da çeşitli parametreleri ortaya koymaktadır. Kullanıcının risk konusunda rızaya sahip olmasının ötesinde ekonomik çıkarlar daha ağır basmaktadır (Mayer ve Mitchell, 2012: 417). Kullanıcıların internet ortamındaki üçüncü taraf izleme etkinliklerini engellemek için üç adet çözüm geliştirilmiştir: Opt-out Çerezleri, Engelleme ve DNT Mekanizması (Mayer ve Mitchell, 2012: 422).

1. Opt-Out Çerezleri: Davranışsal reklamcılık faaliyetinde görülen çevrimiçi düzenlemelerde kullanılan opt-out çerezler kullanıcıya yardımcı olmaktadır. Ancak bu yaklaşımla ilgili çeşitli sorunlar ortaya çıkmıştır (Mayer ve Mitchell, 2012: 422). Öncelikle opt-out çerezleri hakkında gerekli güncellemeler kullanıcı tarafından yapılmalıdır. Ancak bu çerezlerin süresi bir süre sonra sona erdiği için kullanıcı düzenli olarak güncelleme yapmak zorundadır. Bunun dışında kullanıcı bir çerezi sildiğinde farkında olmadan opt-out tercihini de silebilmektedir. Opt-out çerezleri hassas bir niteliğe sahip olduğu için bu çerezleri belirli bir kurala dahil olmadan silmek veya değiştirmek mümkün olabilmektedir. Çevrimiçi olarak reklam faaliyeti gösteren işletmeler davranışsal reklamcılık kapsamında hedef açısından bir sonuç oluşturmak ve özdenetim ile gerçekleştirilen bir seçim mekanizması oluşturabilmek için AdChoice simgesi eklemektedirler. Kullanıcı simgeye tıkladığında reklamla ilgili hedefleme çalışmasının reklam için nasıl uygulandığına dair detaylı bilgi alabilmektedir. Böylece kullanıcı opt-out çereziyle ilgili ayarlar için de belirli bir sayfaya ulaşabilmektedir. Bu konuda yapılan araştırmalarda özdenetim ile oluşturulmuş opt-out modelinin kullanılabilirlik seviyesinin doğruluğu sorgulanmıştır (Mayer ve Mitchell, 2012: 422)

2. Engelleme: Konu hakkında etkili bir şekilde bilgi sahibi olanlar engelleme yöntemini kullanabilmektedir. Popüler engelleme araçlarından; Ghostery, Adblock Plus ve Internet Explorer Tracking Protection List adlı araçları bu kapsamda saymak mümkündür.

3. DNT (Do Not Track) Mekanizması: Kullanıcılar DNT uygulamasını kullanarak reklamlar, analiz hizmetleri, sosyal platformlar gibi hiçbir zaman ziyaret etmedikleri internet sayfalarının kendilerini izlemelerini engelleyebilmektedir. Güncel olarak kullanılan çerez sistemine göre çok daha basit yöntemlerle kullanıcı izlenme durumu engelleyebilmektedir. Reddetme işlemine izin veren çok sayıda çerez yoktur. Bu durum farklı yorumlamalara yol açabilmektedir. DNT ise bu kısıtlamalardan uzaklaşmak için gerekli olanakları sağlamaktadır. Gelecek dönemlerde de kullanılacağına kesin gözüyle bakılmaktadır. Çünkü yeni reklam ağları izleme konusunda kullanıcının herhangi bir girişimini beklememektedir (Mayer ve Mitchell, 2012: 424).

4.2.3 Çevrimiçi Sosyal Ağ İzlemesi

Sosyal ağ oluşturma ile katılımcılar sanal bir ağda bilgi paylaşabilmekte, iletişime geçebilmekte ve etkileşim olanağına kavuşabilmektedir. Oluşturulan sosyal ağlarla çevrimiçi hizmetleri çok daha etkin bir konuma taşımak mümkündür. Bir eğlence olanağı sunan bu ağlar bireysel ve kurumsal kullanıcılara çok sayıda fayda sunmaktadır. Bireysel kullanıcılar birçok amaç için sosyal ağlara dahil olmaktadır. Eski okul arkadaşıyla tekrardan iletişime geçmek, benzer ilgi alanlarına sahip insanlarla bir araya gelmek, sanatsal niteliğe sahip içerikler üretmek, yeni ilişkiler kurmak gibi birçok amaç bulunmaktadır. Sosyal ağları kurumsal bir kullanıcı olan işletmeler de etkin bir şekilde kullanabilmektedir. İşletme sahip olduğu markalar için konumlandırma çalışması yapma, geribildirim alma, doğrudan müşteriyle iletişime geçme, ortaya çıkan sorunlara anında müdahale etme gibi faaliyetler yürütebilmektedir. Çevrimiçi sosyal ağ sitelerinin dikkatsiz bir şekilde kullanımı sonuç olarak önemli sorunlara neden olabilmektedir. Kişisel bilgilerin sızdırılması veya kötü amaçlı yazılımlarla çıkar elde edilmesi gibi amaçlara sahip olan çok sayıda kötü niyetli kişi sosyal ağ sitelerinde yer almaktadır (Ahmand ve Aljumah, 2013: 140). Kullanıcıya ait önemli bilgilerin başka insanların eline geçmesi, kimlik bilgilerinin çalınması, sanal taciz gibi tehdit ve tehlikeler

bulunmaktadır. Kişisel bilgilerin yoğun bir şekilde bu sitelerde yer alıyor olması ve kolay ulaşılması çıkarlara sahip kötü niyetli kişilerin dikkatini çekmiştir. Kullanıcının gizliliği ve güvenliğe dair çok sayıda soru işareti sosyal ağ sitelerinin yoğunlaşmasıyla artmıştır (Ahmand ve Aljumah, 2013: 140).

Çevrimiçi sosyal ağlarda kullanılan çeşitli uygulamalar ve platformun kendisi gizlilik ve güvenlik konusunda çeşitli endişelere neden olmaktadır. Kullanıcı sisteme girdiği kişisel bilgilerinin tam olarak kimlere açık olduğunu bilmemektedir. Bu sitelerde oluşturulan gizlilikle ilgili ayarlarda çok büyük oranda değişiklik yapılamaması olumsuz bir durum olarak değerlendirilmiştir. Herkesin birbirine kolay bir şekilde ulaşabilmesi taciz gibi olumsuz durumların yaşanma olasılığını arttırmaktadır. Kimlik bilgilerinin tamamen ele geçirilmesi, elektronik dolandırıcılık ve sosyal mühendislik gibi olumsuz durumlar ve sanal suçlar çevrimiçi sosyal ağ sitelerinde yoğun bir şekilde yaşanmaktadır. Bununla birlikte kullanıcıların çevrimiçi ağlarda paylaştığı bütün içerikler uzun süreli olarak sistemde kalmaktadır. Kişisel alanla ilgili içeriklerin bu sitelerde yer alması özel hayatın gizliliğine dair olumsuz sonuçların yaşanmasına neden olmaktadır. Tatile çıkma gibi kişisel yaşama ait olayların paylaşılması bireyin özel yaşamına dair bazı tehlikelere sebep olabilmektedir. Uygulamada yer alan sağlayıcılar kullanıcıların bilgilerine sahip olarak üçüncü kişilere maddi kazanç için satabilmektedir. Kötü niyetli kişiler sosyal ağ sitelerinde yer alan yoğun bilgi birikimini kullanmaktadırlar. Bu kişiler solucan adı verilen uygulamaların yardımıyla büyük zombi bilgisayar ağları adı verilen yapılara ulaşabilmektedir. Kötü amaçla oluşturulmuş yazılımlar sosyal ağlar üzerinden yayılarak profillere etki edebilmektedir. Kişisel bilgilerin sosyal ağlarda yer alıyor olması saldırganlar için çok kullanışlı bir durumdur. Kişiye ait olan kimlik bilgileri, banka şifreleri, sosyal güvenlik numarası gibi bilgileri ele geçirmek bazı durumlarda kötü niyetli kişiler için çok kolay olabilmektedir. Bilgileri ele geçiren saldırganlar çok sayıda suçu işleme potansiyeline sahip olmaktadır. Saldırganlar genellikle sahte hesaplar kullanarak ve karşısındaki kullanıcıda bir güven duygusu uyandırarak eylemlerini gerçekleştirmektedir. Sosyal mühendislik tekniklerini uygulayan kullanıcılar bilinçli bir şekilde oluşturulmuş örnek kaynak konumlama tıklamalarına neden olarak bilgileri çalabilmektedir. Kullanıcının sosyal ağ sitelerinde paylaşmış olduğu bütün içerikler tek bir sisteme ait belirli sunucularda toplandığı için merkezileştirmenin sebep olabileceği sorunlar burada da ortaya çıkmaktadır. Bu durum

gizlilik ve güvenlik konusunda bazı sorunların daha yoğun bir şekilde ortaya çıkmasına neden olmaktadır (Ahmand ve Aljumah, 2013: 142).

Çevrimiçi sosyal ağ sitelerinde yer alan paylaşma seçeneği sayesinde sosyal ağ sitelerinde yer alan bir içeriği başka bir internet sitesinde paylaşma olanağının var olması bu siteleri gittikçe daha popüler hale getirmiştir. Çevrimiçi sosyal ağlar sayesinde kullanıcının site üzerinde yapığı etkinlikleri izlemek mümkün hale gelmiştir. Elde edilen çeşitli raporlara göre kullanıcı sosyal ağ sitesini terk etse bile kullanıcıyı izleme faaliyeti çeşitli izleme teknikleriyle devam edebilmektedir. İlgili raporlarda izleme faaliyeti nedeniyle ortaya çıkabilecek riskler detaylandırılmıştır. Kullanıcılara ait profil oluşturma işlemi bu izleme faaliyetiyle gerçekleştirilebilmektedir. Twitter isimli sitede oturum açan bir kullanıcı 15 farklı çerezi depolayabilmektedir. "Twitter'da Paylaş" butonunun olduğu bir internet sitesine giren kullanıcı aynı zamanda Twitter'ın oluşturduğu bir çerezi farkında olmadan bilgisayarında depolamaktadır. Twitter hiç ziyaret edilmese de izleme faaliyeti başlamıştır. Bu kendine özgü davranış şekli sosyal ağ sitelerinde yaygın değildir (Chaabane, Kaafar ve Boreli, 2012: 2).

Yapılan araştırmalara göre çevrimiçi sosyal ağ siteleri ağda bulunan kullanıcıların kimlik tanıtıcı bilgilerini üçüncü taraf kaynaklara sızdırmaktadır. Böylesi durumlarda sosyal ağ sitesinin teknik bir sorunu bulunmamaktadır. Ayrıca kullanıcılar dış kaynaklı uygulamalar nedeniyle oluşan bilgi sızıntısından haberdar değildirler. Facebook gibi sosyal ağlarda da dış kaynaklı uygulamalar nedeniyle sızıntıların olduğuna dair bilgiler mevcuttur (Chaabane, Kaafar ve Boreli, 2012: 4). Kullanıcılar opt-out mekanizmaları ile engelleme konusunda başarısız oldukları zamanlarda da kişisel bilgiler sızabilmektedir. Ancak bilgi sızıntıları sadece tek bir kanal tarafından gerçekleşmemektedir. Çevrimiçi sosyal ağ sitelerinde kullanıcılara ait özel kişisel bilgiler ücret karşılığı üçüncü kişilere sızdırılmaktadır.

4.2.4 Mobil Cihaz Tabanlı İzleme

Mobil uygulamaların ve faaliyetlerin artmasıyla birlikte konum tabanlı olarak gerçekleştirilen izleme çalışması yoğunlaştırılmıştır. Mobil telefonlar için ortaya çıkan GSM ve GPS sistemleri sayesinde kullanıcıları izlemek ve onlara daha verimli hizmetler sunmak önemli bir konu haline gelmiştir. Konum tabanlı hizmetler sunma insanların her zaman nerede olduğunun bilinmesi sonucunu ortaya çıkardığı için

gizlilikle ilgili tartışmalar da beraberinde gelmiştir (Barkuus ve Dey, 2003: 2). Mobil cihazların çoğunlukla kullanıcının yanında olması, çeşitli ayarlara ve uygulamalara göre sinyaller üretmesi işletmeler için etkin bir reklam alanı olarak düşünülmüştür. Mobil cihazların ezici bir şekilde popüler bir kullanım seviyesine yükselmesiyle teknik olarak yeterlilik düzeyi gittikçe bilgisayarlara yaklaşmaktadır. Bu yüzden mobil izleme tekniklerinin daha da genişleyeceği düşünülmektedir. Mobil aygıtlara odaklanmış olan az sayıda üçüncü taraf bulunmaktadır. Yeni bir pazar olarak gördükleri için üçüncü partiler bu pazara girmekte geç kalmışlardır. Ancak bu pazardaki gelişmeleri takip ettikleri açıktır. Mobil uygulama izleme sistemlerinin yoğun bir dönüşüm geçireceği düşünülmektedir (Barkuus ve Dey, 2003: 2).

4.2.5 Konum İzleme

Konum tabanlı teknolojiler diğer geleneksel teknolojilere göre yenidir. İnsanların veya nesnelerin konumunu belirlemek için kullanılan bir sistemdir. Kullanıcının hangi lokasyonda bulunduğu bu teknolojinin en önemli uygulama alanlarından birini oluşturmaktadır. Konum tabanlı teknolojinin gerçekleştirilmesinde radyo frekansları (RF), kızılötesi ışınlar, sesüstü dalgalar ve ultra geniş bant (UWB) gibi unsurlar kullanılmaktadır (Yun ve Kim, 2006: 210). Bazı kullanıcılar konumlarının bilinmesinden memnun olarak çeşitli hizmetler alıyor olsa da bazı kullanıcılar bu durumdan endişelidir. Araştırmacılar kullanıcıların konum bilgileri konusunda bazı kontrollere sahip olması için çeşitli algoritmalar üzerinde çalışmaktadırlar (Grutese-Liu ve Liu, 2004: 128).

Telsizler konum belirleme konusunda sunduğu olanaklarla eşsiz bir konuma yükselmiş görünmektedir. Bu noktada yaşanan gelişim sunulan hizmetlerin kalitesini arttırsa da bireylerin özel hayat gizliliği konusunda endişeleri bulunmaktadır (Grutese-Liu ve Liu, 2004: 28). Kullanıcının farklı gizlilik seviyesine yönelerek farklı seçenekleri istemesi, konum izleme uygulamasının gizlilik konusuna yaklaşımında başka sorunları ortaya çıkartmaktadır. Cep telefonunda gerçekleştirilecek her konum izleme faaliyetinde kullanıcıdan izin talep edilmesi bir süre sonra zaman maliyetine yol açan bir sorun olabilmektedir. Bilinçli bir şekilde oluşturulan gizlilik politikalarındaki uygulamaların içeriğini saptamak bazen karmaşıktır (Grutese-Liu ve Liu, 2004: 28). Kullanıcılar genellikle dış hizmetlerden gelen talepleri onaylamaktadırlar. Çünkü uygulamanın

kullanıcı yararına bir hizmet sunacağını düşünmektedirler. Ancak her ne olursa olsun kullanıcı gizlilik talep edecektir. Hizmeti sunanlar buna uygun olacak şekilde bir politika belirlemek zorundadır. Örneğin, oluşturulan bir politikaya göre kişi kamusal alandayken konum izlemesine maruz kalırken özel alanlarda konum izlemesi pasif hale gelmektedir. Bu politikalar genişletilerek binaların durumuna göre çeşitlendirilebilmektedir (Grutese-Liu ve Liu, 2004: 29).

4.2.6 Yeniden Özdeşleştirme

Yeniden özdeşleştirme, anonim olarak görünen verinin ilgili kişinin kimlik bilgileriyle eşleştirilmesiyle ortaya çıkmasını ifade etmektedir (Malin B. , 2006: 4). Bireyler çeşitli veri tabanlarında kendilerine ait bilgi parçaları bırakmaktadır. Bireyler kendileri hakkında veri toplandığına dair tam bir kontrole sahip değildirler. Hatta bireyler sanal dünyada bir bilgi parçası bıraktıklarını dahi bilmezler (Malin B. , 2006: 5). Yeniden özdeşleştirmede anonim olarak görülen veriler arasında ilişki kurulmaktadır. Aslında bu yöntemle veri toplama konusunda gizlilik kapsamında bir saldırı yapılmaktadır (Malin B. , 2006: 1).

Bireyler iş veya özel hayatlarında isteyerek veya istemeyerek çok sayıda kimlik kullanmaktadır. Bu bilgilerin bazıları değişirken bazıları sabit kalmaktadır. Kullanıcı bir internet sitesini ziyaret ettiğinde IP adresi ilgili internet sayfasında kayıt altına alınmaktadır. Eğer çevrimiçi bir satın alma işlemi gerçekleştiriliyorsa kullanıcıdan genel olarak kimlik bilgileri istenmektedir. Bununla birlikte bir internet sitesi kendisini ziyaret eden kullanıcıların IP adreslerine ait kayıtları paylaşabilmektedir. İnternet sitesi üçüncü bir tarafa bilgi satışı yaparken kendi internet sitesine kimlik bilgilerini veren müşterilerin bilgilerini de satmaktadır. Bu çerçevede kişinin kimlik bilgileri ile IP adresleri arasında bağlantı kurmak mümkün olabilmektedir. Kişinin ad soyadının yanında adres bilgilerinin yer almasıyla konum açısından da bağlantı kurulabilmektedir. Yeniden özdeşleştirilmiş verilerle kullanıcının nerelerde daha yoğun ve daha az satın alma işlemi yaptığına dair değerli bilgiler edinilmektedir. Ayrıca böylesi bir duruma ulaşılmadan önce kullanıcılar kimliksizleştirilmiş IP adreslerinden oluşan bilgilerin yeniden özdeşleştirmeden geçmeyeceğini düşünmektedir (Malin, Sweeney ve Newton, 2003: 2).

İnternet sayfaları kişisel bilgilerin yer aldığı listeleri ticari bir eşya olarak kabul etmektedir. Toplanmış olan veriler çevrimiçi politikalar kapsamında farklı amaçlar için yasaya uygun olacak şekilde satılabilmektedir. Elektronik ticaretle ilgili uygulamalarda düzenli olarak üçüncü taraflara bilgi iletildiği düşünülmektedir. İnternet ortamında toplanan birçok bilgi hassastır. Birçok internet sitesi gizlilik politikasında tanımlanmamış verilerin bazı verilerle bağlantı kurularak yeniden özdeşleştirme için kullanılmayacağına dair taahhüt vermektedir. Bunu garanti altına almak için tanımlanmış ve tanımlanmamış veri iki ayrı küme altında toplanmaktadır. Özellikle ABD'de çevrimiçi gizlilik politikalarının oluşturulmasına büyük önem verilmektedir. İnternet sayfası gizlilik politikasına aykırı bir faaliyette bulunursa yasal yaptırımlarla karşı karşıya kalabilmektedir (Malin B. , 2006: 10).

4.3 İZLEMENİN RİSKLERİ

İzlemenin bireysel kullanımdan başlayarak giderek genişlemesiyle birlikte küresel bir sorun ortaya çıkmıştır. Yapılan gözetimin siyasi, ticari ve güvenlikle ilgili boyutları bulunmaktadır. Pazarlama uzmanları tüketicinin alışkanlıklarını belirleme ve alışkanlıklara göre hareket etme konusunda uzmanlaşmışlardır. Davranışlarda gerçekleşen ciddi değişimleri kavramak müşterinin başka ürünlere yönelme olasılığını arttırmaktadır. Buna benzer izleme faaliyetleri müşteri bağlılık kartları gibi araçlarla yapılmıştır. İnternet ise çok daha güçlü bir araç olarak öne çıkmaktadır.

İzleme ile büyük ekonomik faydalar elde edilse de çok sayıda sakıncanın ve tehlikenin var olduğu gözden kaçmamalıdır. Özel hayatın gizliliğinin ihlal edildiğine dair çok sayıda açıklama mevcuttur. Birçok kuruluş ise gizlenmesi gereken herhangi bir unsurun var olmadığını öne sürerek herkesin şeffaf bir şekilde hareket etmesi gerektiğini öne sürmüştür. Solove bu görüşe gizlilik konusunda dar kapsamlı bir bakış açısını ortaya çıkarttığı için karşı çıkmaktadır. Gizlilik konusunda tek kriter ortaya bir zararın çıkması olmamalıdır. Toplanan bilgilerin elde edilmesi ve sonrasında işlenmesi ile yanlış kararlara ulaşmak olasıdır. İnsanları yanlış kararlara sürükleyecek bazı sorunların başlangıç noktasını veri toplamak oluşturabilmektedir.

Hizmet sunumunda izleme faaliyeti yürüterek belirli profiller oluşturmanın sonucu hizmette ayrımcılık veya dışlama olabilmektedir. Yapılan profilleme çalışmasıyla kullanıcının bir hastalığa sahip olduğu düşüncesi ortaya çıkabilmektedir. Bu bilgiyi

kullanan bir sigorta işletmesi ilgili bireyi sigorta kapsamı dışında tutabilir veya kişiden çok yüksek prim ödemesi talep edebilir. Bu duruma fiyat ayrımcılığı adı verilmektedir. Bu konunun uygulanması oldukça eskidir. Alıcının yaşı veya cinsiyeti gibi özellikleri fiyat ayrımcılığı sonucunu doğurabilmektedir.

Kişiye özel profilleme yaparak hizmet sunma bazı riskleri ortaya çıkarmaktadır. İçeriğin kişiye özel bir şekilde sunulması profillemedir. Bir haber sitesinde kişinin ilgi alanına göre haber türlerini öne çıkarma kişiselleştirme için bir örnektir. Satış yapan bir site kişinin önceki alışverişlerine göre bazı ürünleri öne çıkarabilmektedir. Çevrimiçi reklamları da kişiselleştirmek mümkündür. Bu durumda birey sadece kendi tercihlerine göre belirli bir çerçevenin içinde sıkışıp kalmaktadır. Bazı haberlerin kullanıcılar için özelleştirilerek gösterilmesi sansürle ilgili konuları yeniden tartışmaya açmıştır. Kişiselleştirmeyle bilgi sızdırma yapmak da mümkündür. Tüketicinin nasıl bir ilgi alanına sahip olduğu bilgisi izlemeyle belirlenebilmektedir. Kullanıcının arama motoru geçmişine göre bir profil oluşturulmakta ve gösterilen reklamlar buna göre yeniden yapılandırılmaktadır (Castelluccia ve Arvind, 2012: 13).

4. YÖNTEM

Çalışmanın bu bölümünde araştırma yöntemine ilişkin bilgilere yer verilmiştir.

5.1 ARAŞTIRMA KONUSU

Yaşanan gelişmelerle dünya küresel bir köy haline gelirken, gizlilik, mahremiyet kavramı sınırları da kolay aşılır hale getirmiştir. Bu hızlı gelişim beraberinde ekonomiye farklı ve önemli bir katkı sağlarken diğer yandan teknolojinin sağladığı imkânlarla tüketici bireylerin özel yaşam alanlarına kendi rızaları olmadan erişimini de mümkün kılmaktadır. Sosyal ağlarda paylaşılan kişisel bilgiler kötü niyetli kişilerin ulaşım kolaylığı ile kimlik hırsızlığı, çevrimiçi taciz ve bilgi sızması gibi riskler oluşturmaktadır. Yapılan çalışmalarda çevrimiçi sosyal ağlardaki (Facebook, Twitter, Instagram) oturumların kapatıldıktan sonra dahi kullanıcıların izlenebilmesi ve elde edilen bilgilerle kullanıcı profillerinin oluşturulabilmesi sonucunda doğabilecek risklere vurgu yapılmıştır. Türkiye'de İstanbul'da bilişim sektöründe çalışan (her meslek grubu) baz alınarak kişisel verilerinin izlenmesi konusunda ne kadar bilinçli ve farkında oldukları incelenmiştir.

5.2 ARAŞTIRMANIN AMACI

Teknolojik gelişmeler ve yaygınlaşan internet kullanımı, işletmelerin hedef müşterilerine dijital medya gibi yeni ve yenilikçi yollar ile ulaşmasına neden olmaktadır. Tüketicilerin dijital pazarlama faaliyetlerini kullanımının artmasıyla beraber, dijital pazarlama işletmeler için stratejik önem taşıyan bir araç haline gelmiştir. İşletmeler dijital pazarlama sayesinde müşterilerine herhangi bir yerde, zamanda ve durumda ulaşabilmektedirler.

Sosyal medya üzerinden kullanıcıların yaptığı paylaşımların kendi iradeleri ile siteye yüklenmesi sonucu daha sonra bu kişisel verilerin başka hesaplarca kişilik hakkına saldırı niteliğinde ele geçirilmesi, saklanması ve transferi halinde, bu işlemleri hukuka uygun kılan kişisel veri sahibinin rızasının geçerli olup olmadığının tespiti önem kazanmıştır. Ayrıca internet sitelerinde kişisel verilerin işlenmesi için ziyaretçinin rızasını elde etme yöntemleri tartışmalı bir konudur.

Bu çalışmanın amacı sosyal medya pazarlama faaliyetlerinin artışı ve bunun sonucunda veri tabanında tutulan kişisel verilerin kullanıcıya etkilerinin tespit edilmesidir.

5.3 ARAŞTIRMANIN ÖNEMİ (AKADEMİK VE TİCARİ)

Sosyal medya pazarlaması günümüzde giderek büyüyen bir sektör haline gelmiştir. Sosyal medya pazarlaması nedeniyle veri tabanında tutulan kişisel verilerin hangi amaçla, kimler tarafından kullanılacağı tüketiciyi doğrudan etkilemektedir. Dolayısıyla bu veriler tüketicilerin sosyal medya pazarlamasına bakışını değiştirmektedir. Bu çalışma tüketicilerin bu durumdan nasıl etkilendiğinin belirlenmesi sosyal medya pazarlamasın yapan firmalara da yol haritası oluşturması konusunda önem taşımaktadır. Buna ek olarak literatüre de bu alanda yapılan ulusal bir çalışma olarak katkı sağlaması planlanmaktadır.

5.4 ARAŞTIRMA SORULARI VEYA HİPOTEZLER

H1: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H2: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri yaşlarına göre farklılaşmaktadır.

H3: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri eğitim durumlarına göre farklılaşmaktadır.

H4: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri sosyal medya kullanma durumlarına göre farklılaşmaktadır.

H5: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri sosyal medyada vakit geçirme sürelerine göre farklılaşmaktadır.

H6: Katılımcıların kişisel verilerin korunmasına ilişkin bilgi düzeyleri en çok kullandıkları sosyal ağa göre farklılaşmaktadır.

5.5 ARAŞTIRMA KÜMESİ: EVREN VE ÖRNEKLEM

Bu çalışmanın evrenini sosyal medya kullanan kişiler oluşturmaktadır. Örneklem ise 20-30 yaş aralığında İstanbul'da yaşayan ve telekomünikasyon sektöründe çalışan kişilerdir.

5.6 VERİLERİN TOPLANMA TEKNİĞİ VE AÇIKLAMASI/SAVUNMASI

Araştırmada veri toplama tekniği olarak anket yöntemi kullanılmıştır. Araştırma için oluşturulan anket formu iki bölümden oluşmaktadır. Anket formunun ilk bölümü demografik bilgi formu şeklinde olup katılımcıların cinsiyetleri, yaşları, eğitim durumları, sosyal medya kullanma durumları, sosyal medya kullanma süreleri ve en çok kullandıkları sosyal ağı ölçmeye yönelik sorulardan oluşmaktadır. Anket formunun ikinci bölümü ise kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyini ölçmeye yönelik olarak hazırlanmış bir ölçekten oluşmaktadır. Bu ölçek, Aydın'ın (2018) (2018) çalışmasından alınarak, sosyal medyaya yönelik olarak uyarlanmıştır. Ölçek, 1=Doğru, 5=Hayır şeklinde 5'li likert tipinde 20 maddeden oluşmakta olup, katılımcıların sosyal medyadaki kişisel verilerinin korunmasına ilişkin ne derecede bilgi sahibi olduklarını ölçmektedir. Ölçeğin geliştirildiği çalışmada güvenilirlik katsayısı (Cronbach's alpha) 0,719 olarak bulunmuştur.

5.7 VERİLERİN ANALİZİ

Araştırmada toplanan veriler IBM SPSS programı ile analiz edilecektir. Analizde öncelikle katılımcıların demografik bilgilerine ilişkin bulgular gösterilecektir. Sonrasında katılımcıların sosyal medyadaki kişisel verilerinin korunmasına ilişkin bilgi düzeylerine yönelik cevapladıkları sorulara yönelik elde edilen bulgular tanımlayıcı istatistikler ile gösterilecektir. Daha sonrasında araştırma hipotezlerini test etmek amacıyla katılımcıların kişisel verilerinin korunmasına ilişkin bilgi düzeylerinin demografik bilgilerine göre farklılık gösterip göstermediği bağımsız örneklem t testi veya tek yönlü varyans analizi ile incelenecektir.

6. BULGULAR

Çalışmanın bu bölümü yapılan araştırmaya ilişkin bulguları içermektedir.

6.1 DEMOGRAFİK ÖZELLİKLERE İLİŞKİN BULGULAR

Araştırmaya katılan katılımcıların cinsiyet dağılımları Tablo 6.1'de gösterilmektedir.

Tablo 6. 1 Katılımcıların Cinsiyetlerine İlişkin Frekans Analizi Sonuçları

Cinsiyet	**Frekans (f)**	**Yüzde (%)**
Kadın	58	47,2
Erkek	65	52,8
Toplam	123	100,0

Frekans analizi sonrasında bulunan sonuçlar incelendiğinde katılımcıların %47,2'sinin kadın ve %52,8'inin ise erkek olduğu görülmektedir.

Araştırmaya katılan katılımcıların yaş dağılımları Tablo 6.2'de gösterilmektedir.

Tablo 6. 2 Katılımcıların Yaşlarına İlişkin Frekans Analizi Sonuçları

Yaş	**Frekans (f)**	**Yüzde (%)**
18-25	30	24,4
26-33	50	40,7
34-41	26	21,1
42-49	6	4,9
50 ve üzeri	11	8,9
Toplam	123	100,0

Frekans analizi sonrasında bulunan sonuçlar incelendiğinde katılımcıların %24,4'ünün 18-25 yaş aralığında, %40,7'sinin 26-33 yaş aralığında, %21,1'inin 34-41 yaş aralığında, %4,9'unun 42-49 yaş aralığında ve %8,9'unun ise 50 ve üzeri yaşta olduğu görülmektedir.

Araştırmaya katılan katılımcıların eğitim durumu dağılımları Tablo 6.3'te gösterilmektedir.

Tablo 6. 3 Katılımcıların Eğitim Durumlarına İlişkin Frekans Analizi Sonuçları

Eğitim Durumu	**Frekans (f)**	**Yüzde (%)**
İlkokul	2	1,6
Ortaokul	2	1,6
Lise	24	19,5
Ön Lisans	10	8,1
Lisans	49	39,8
Yüksek Lisans	34	27,6
Doktora	2	1,6
Toplam	123	100,0

Analiz sonuçları incelendiğinde araştırmaya katılan katılımcıların %1,6'sının ilkokul, %1,6'sının ortaokul, %19,5'inin lise, %8,1'inin ön lisans, %39,8'inin lisans, %27,6'sının yüksek lisans ve %1,6'sının ise doktora mezunu olduğu görülmektedir.

Araştırmaya katılan katılımcıların sosyal medya kullanım dağılımları Tablo 6.4'te gösterilmektedir.

Tablo 6. 4 Katılımcıların Sosyal Medya Kullanımlarına İlişkin Frekans Analizi Sonuçları

Sosyal Medya Kullanımı	**Frekans (f)**	**Yüzde (%)**
Evet	119	96,7
Hayır	4	3,3
Toplam	123	100,0

Analiz sonuçlarından araştırmaya katılan katılımcıların %96,7'sinin sosyal medya kullandığı ve %3,3'ünün ise sosyal medya kullanmadığı görülmektedir.

Araştırmaya katılan katılımcıların günlük sosyal medya kullanım süresi dağılımları Tablo 6.5'te gösterilmektedir.

Tablo 6. 5 Katılımcıların Günlük Sosyal Medya Kullanım Sürelerine İlişkin Frekans Analizi Sonuçları.

Sosyal Medya Kullanım Süresi	**Frekans (f)**	**Yüzde (%)**
1 saatten az	31	25,2
1-3 saat	74	60,2
4-7 saat	18	14,6
Toplam	123	100,0

Günlük sosyal medya kullanım sürelerine ilişkin yapılan frekans analizi sonuçları incelendiğinde katılımcıların %25,2'sinin 1 saatten az, %60,2'sinin 1-3 saat ve %14,6'sının ise 4-7 saat zaman harcadıkları görülmektedir.

Araştırmaya katılan katılımcıların en çok kullandıkları sosyal ağ dağılımları Tablo 6.6'da gösterilmektedir.

Tablo 6. 6. Katılımcıların En Çok Kullandıkları Sosyal Ağlara İlişkin Frekans Analizi Sonuçları

Sosyal Ağ	**Frekans (f)**	**Yüzde (%)**
Facebook	57	23,6
Twitter	56	23,1
Instagram	112	46,3
LinkedIn	4	1,7
Pinterest	2	0,8

YouTube	3	1,2
Ekşi sözlük	2	0,8
Whatsapp	6	2,5
Toplam	242	100,0

Katılımcıların en çok kullandıkları sosyal ağları belirlemeye yönelik yapılan çoklu yanıt frekans analizi sonrasında bulunan sonuçlar incelendiğinde katılımcıların %23,6'sının Facebook, % 23,1'inin Twitter, %46,3'ünün Instagram, %1,7'sinin LinkedIn, %0,8'inin Pinterest, %1,2'sinin YouTube, %0,8'inin Ekşi sözlük ve %2,5'inin ise Whatsapp kullandığı görülmektedir.

6.2. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN KULLANICI BİLGİ DÜZEYİ BULGULARI

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyini ölçmeye yönelik olarak hazırlanan ölçeğin güvenilirliği test edilmiş ve güvenilirlik analizi sonuçları Tablo 6.7'de verilmiştir.

Tablo 6. 7. Güvenilirlik Analizi Sonuçları

Cronbach's Alpha	N of Items
,838	20

Tablo 6.7'de görüldüğü üzere 20 ifadeden oluşan ölçeğin güvenilirliği test edilmiş ve Cronbach Alpha değeri ,838 olarak bulunmuştur. Bu bulguya göre ölçeğin yüksek derecede güvenilir olduğu sonucuna varılmıştır; $0,80 \leq \alpha < 1,00$.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyini ölçmeye yönelik olarak hazırlanan ölçeğin geçerliliği test edilmiş ve geçerlilik analizi sonuçları Tablo 6.8'de verilmiştir.

Tablo 6. 8. Geçerlilik Analizi Sonuçları

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,706
Bartlett's Test of Sphericity	Approx. Chi-Square	1024,528
	df	190
	Sig.	,000

Tablo 6.8'de görüldüğü gibi Kaiser-Meyer Olkin (KMO) değeri ,706 olarak bulunmuştur. Bu değer 0,5'den büyük olduğu için örneklem büyüklüğünün yeterli olduğu sonucuna varılmıştır. Ana kütlenin bütünlüğünü test eden ve Bartlett tarafından geliştirilen küresellik (sphericity) testi sonucuna göre anlamlılık düzeyi değeri ,000 olarak bulunmuştur. Bu değer %5 hata payından daha küçük olduğu için Bartlett Küresellik testi anlamlı bulunmuştur (Ki-Kare Değeri = 1024,528; p= ,000<,05). Bu sonuçlara göre ölçeğe ilişkin elde edilen verilerin faktör analizine uygun olduğu belirlenmiştir.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyi ölçeği için yapılan betimsel analiz sonuçları Tablo 6.9'da verilmiştir.

Tablo 6. 9. Betimsel Analiz Sonuçları

	Minimum	Maksimum	Ortalama	Standart Sapma
6698 Sayılı Kişisel Verilerin Korunması ve Saklanması Kanunu hakkında bilgiye sahibiyim.	1	5	2,03	1,008
Sosyal medyada hesap açmam kişisel verilerimin işlenmesi için yeterlidir.	1	5	2,25	1,369
Sosyal medyada herhangi bir ödeme yapmanız kişisel verilerinizin işlenmesi	1	5	2,70	1,525

için yeterlidir.				
Kişisel verilerin işlenmesi müşteri bilgi gizliliği ya da verilerin korunması yükümlülüklerinin ihlali anlamına gelmez.	1	5	2,50	1,544
Sosyal medyada kampanyalar, bilgilendirmeler ve hizmet teklifine ilişkin amaçlar için kişisel verileriniz korunur ve saklanır.	1	5	1,94	1,189
Sosyal medyada sizin kişisel verileriniz işlenerek başka müşterileri kazanma çalışmaları yapılabilir.	1	5	2,09	1,324
Sosyal medyada, kişisel verilerin işlenmesine dair rıza vermeyen bireyler ile doğrudan teklifsiz iletişime geçilir.	1	5	3,12	1,540
Kişi sosyal medyada hesap açtıysa sosyal ağ bireyin kişisel verilerine erişir.	1	5	2,03	1,228
Sosyal medyada müşteri memnuniyetini arttırmak, size özel kampanyalar, indirimler sağlamak amacıyla kişisel verileriniz işlenir.	1	5	1,66	,857
Kişisel veriler idari ve resmi makamlarca araştırılmalar yapıldığında ve sosyal ağlardan talep edildiğinde sosyal ağlar tarafından bu makamlar ile paylaşılır.	1	5	2,03	1,201
Sosyal medyada kişisel veriler sosyal ağlar tarafından araştırma süreçleri için kullanılır.	1	5	1,95	1,260

Sosyal medyada kişisel veriler 3. kişiler tarafından dolandırıcılık, sahtecilik, kara para amaçlı olaylar için kullanılabilir.	1	5	1,91	1,343
Kişisel verilerim kullanılarak istismara uğradım ve sonucunda maddi zarar gördüm.	1	5	3,72	1,463
Bireylerin sosyal medyada kişisel verilerinin doğru ve güncel olması sorumluluğu sosyal ağa aittir.	1	5	2,82	1,515
Müşteriler kişisel verilerin nasıl korunduğunu öğrenebilir ve isteğe bağlı değiştirebilir.	1	5	1,82	1,153
Sosyal medyada hesaplarınızı kapatsanız bile kişisel verileriniz istenilen kurum ve kuruluşlarla paylaşılır mı?	1	5	2,67	1,347
Kimlik hırsızlığına karşı alınması gereken tedbirleri biliyorum.	1	5	2,00	,975
Sosyal medya sitelerinin güvenli olarak kullanılmasını biliyorum.	1	4	1,82	,820
Dijital imzanın ne işe yaradığını biliyorum.	1	5	1,77	,974
Kişisel verilerin korunması ve saklanması kanununun faydalı olduğunu düşünüyor musunuz?	1	4	1,50	,751

Betimsel analiz sonuçlarına göre katılımcıların “Kişisel verilerin korunması ve saklanması kanununun faydalı olduğunu düşünüyor musunuz?”, “Sosyal medyada

müşteri memnuniyetini arttırmak, size özel kampanyalar, indirimler sağlamak amacıyla kişisel verileriniz işlenir.” ve “Dijital imzanın ne işe yaradığını biliyorum.” ifadelerine katılımlarının önem düzeyleri sırasıyla 1,50, 1,66 ve 1,77 olarak bulunmuştur. Buna göre katılımcıların kişisel veriler hakkındaki kanunu yararlı buldukları, kişisel verilerinin işlenmesi ve dijital imza konularında bilgili oldukları söylenebilir.

6.3 KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN KULLANICI BİLGİ DÜZEYİ İLE DEMOGRAFİK ÖZELLİKLER ARASINDAKİ FARLILIĞA YÖNELİK BULGULAR

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyinin katılımcıların cinsiyetlerine göre farklılık gösterip göstermedikleri bağımsız örneklem t testi ile incelenmiştir. Elde edilen bulgular Tablo 6.10’da verilmiştir.

Tablo 6. 10 Kişisel Verilerin Korunmasına İlişkin Kullanıcı Bilgi Düzeyi ile Cinsiyet Arasındaki Farklılığa Yönelik Bağımsız Örneklem T Testi Sonuçları

Cinsiyet	N	$\overline{X}$	SS	t	p
Kadın	58	2,2603	,67731	,721	,472
Erkek	65	2,1800	,55746		

Yapılan bağımsız örneklem t-testi sonucunda katılımcıların cinsiyetlerine göre kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri arasında istatistiksel açıdan anlamlı bir farklılığa rastlanmamıştır (t=,721, p>,05).

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyinin katılımcıların yaşlarına göre farklılık gösterip göstermedikleri tek yönlü varyans analizi ile incelenmiştir. Elde edilen bulgular Tablo 6.11’de verilmiştir.

Tablo 6. 11 Kişisel Verilerin Korunmasına İlişkin Kullanıcı Bilgi Düzeyi ile Yaş Arasındaki Farklılığa Yönelik Tek Yönlü Varyans Analizi Sonuçları

Yaş	N	$\overline{X}$	SS	F	p
18-25	30	2,2017	,58139	3,697	,007

26-33	50	2,0940	,65595		
34-41	26	2,1558	,47965		
42-49	6	2,5500	,62849		
50 ve üzeri	11	2,7909	,49740		

Yapılan tek yönlü varyans analizi sonucundan katılımcıların yaşlarına göre göre kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri arasında istatistiksel açıdan anlamlı bir farklılık olduğu görülmüştür (p<,05). Bulunan farklılığın hangi gruplar arasında olduğunu tespit etmek amacıyla varyanslar homojen olmadığından Tamhane's T2 Post-hoc testi uygulanmıştır. Buna göre 50 ve üzeri yaşta olan katılımcıların kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerinin daha yüksek olduğu söylenebilir.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyinin katılımcıların eğitim durumlarına göre farklılık gösterip göstermedikleri tek yönlü varyans analizi ile incelenmiştir. Elde edilen bulgular Tablo 6.12'de verilmiştir.

Tablo 6. 12 Kişisel Verilerin Korunmasına İlişkin Kullanıcı Bilgi Düzeyi ile Eğitim Durumu Arasındaki Farklılığa Yönelik Tek Yönlü Varyans Analizi Sonuçları

Eğitim Durumu	N	$\overline{X}$	SS	F	p
İlkokul	2	2,1000	,00000	1,862	,093
Ortaokul	2	2,2000	,00000		
Lise	24	2,3417	,59612		
Ön Lisans	10	2,6300	,76347		
Lisans	49	2,2112	,54784		
Yüksek Lisans	34	2,0015	,65937		

Doktora	2	2,6500	,00000		

Tek yönlü varyans analizi sonucuna göre katılımcıların eğitim durumları ile kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri arasında istatistiksel açıdan anlamlı bir farklılığa rastlanmamıştır (p>,05).

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyinin katılımcıların sosyal medya kullanımlarına göre farklılık gösterip göstermedikleri bağımsız örneklem t testi ile incelenmiştir. Elde edilen bulgular Tablo 6.13'te verilmiştir.

Tablo 6. 13 Kişisel Verilerin Korunmasına İlişkin Kullanıcı Bilgi Düzeyi ile Sosyal Medya Kullanımı Arasındaki Farklılığa Yönelik Bağımsız Örneklem T Testi Sonuçları

Sosyal Medya Kullanımı	N	$\bar{X}$	SS	t	p
Evet	119	2,2294	,62224	3,853	,005
Hayır	4	1,8750	,14434		

Yapılan bağımsız örneklem t-testi sonucunda kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyi açısından sosyal medya kullanan ve sosyal medya kullanmayan katılımcılar arasında sosyal medya kullanan katılımcılar lehine anlamlı bir farklılık bulunmuştur (t = 3,853, p<,05). Bu sonuca göre sosyal medya kullanan katılımcıların kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerinin daha fazla olduğu söylenebilir.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyinin katılımcıların günlük sosyal medya kullanım sürelerine göre farklılık gösterip göstermedikleri tek yönlü varyans analizi ile incelenmiştir. Elde edilen bulgular Tablo 6.14'te verilmiştir.

Tablo 6. 14 Kişisel Verilerin Korunmasına İlişkin Kullanıcı Bilgi Düzeyi ile Sosyal Medya Kullanım Süresi Arasındaki Farklılığa Yönelik Tek Yönlü Varyans Analizi Sonuçları

Sosyal Medya Kullanım Süresi	N	$\overline{X}$	SS	F	p
1 saatten az	31	2,2145	,65793	,101	,904
1-3 saat	74	2,2047	,58469		
4-7 saat	18	2,2778	,69520		

Yapılan tek yönlü varyans analizi sonucunda katılımcıların sosyal medya kullanım sürelerine göre kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri arasında istatistiksel açıdan anlamlı bir farklılığa rastlanmamıştır (p>,05).

7. SONUÇ

Araştırmada katılımcıların cinsiyet, yaş, eğitim durumu, sosyal medya kullanımı, günlük sosyal medya kullanım süresi ve en çok kullandıkları sosyal ağ gibi demografik özellikleri frekans analizi ile incelenmiştir. Katılımcıların; %47,2'si kadın ve %52,8'i erkek, %24,4'ü 18-25 yaş aralığında, %40,7'si 26-33 yaş aralığında, %21,1'i 34-41 yaş aralığında, %4,9'u 42-49 yaş aralığında ve %8,9'u 50 ve üzeri yaştadır. %1,6'sı ilkokul, %1,6'sı ortaokul, %19,5'i lise, %8,1'i ön lisans, %39,8'i lisans, %27,6'sı yüksek lisans ve %1,6'sı doktora mezunudur.

Frekans analizi sonuçlarına göre katılımcıların %25,2'si günde 1 saatten az, %60,2'si günde 1-3 saat ve %14,6'sı günde 4-7 saat vakit geçirmektedir. %96,7'si sosyal medya kullanırken %3,3'ü sosyal medya kullanmamaktadır. En çok kullanılan sosyal ağlara bakıldığında ise katılımcıların %23,6'sının Facebook, % 23,1'inin Twitter, %46,3'ünün Instagram, %1,7'sinin LinkedIn, %0,8'inin Pinterest, %1,2'sinin YouTube, %0,8'inin Ekşi sözlük ve %2,5'inin ise Whatsapp kullandığı görülmüştür.

Araştırmada kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerini ölçmek amacıyla hazırlanan ölçeğin güvenilirlik ve geçerliliği test edilmiştir. Cronbach Alpha değerine göre ölçeğin yüksek derecede güvenilir olduğu ve Kaiser-Meyer Olkin değerine göre de örneklemin yeterli olduğu ve ölçeklerdeki ifadelerin analizde kullanılmak için uygun olduğu sonucuna varılmıştır.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri ölçeğine ait ifadeler betimsel analiz ile incelenmiştir. Katılımcıların kişisel veriler hakkındaki kanunu yararlı buldukları, kişisel verilerinin işlenmesi ve dijital imza konularında bilgili oldukları tespit edilmiştir.

Kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerinin katılımcıların demografik özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla iki kategorili değişkenler için bağımsız örneklem t testi ve üç ve daha fazla kategorili değişkenler için tek yönlü varyans analizi kullanılmıştır. Bu analizlerde anlamlılık derecesi 0,05 olarak belirlenmiş ve anlamlı bir farklılık bulunduğunda, bulunan

farklılığın hangi gruplar arasında olduğunu tespit edebilmek amacıyla varyansların homojenliğine bakılmış ve incelenen grupların varyansları homojen olmadığından Tamhane's T2 Post-hoc testi kullanılmıştır.

Analiz sonuçlarından; cinsiyet, eğitim durumu ve sosyal medya kullanım süresine göre katılımcılar arasında kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri açısından anlamlı bir farklılık bulunmazken; yaş ve sosyal medya kullanımına göre katılımcılar arasında kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeyleri açısından istatistiki olarak anlamlı farklılıklar olduğu bulunmuştur. 50 ve üzeri yaştaki katılımcıların kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerinin diğer yaş gruplarındaki katılımcılara göre daha fazla olduğu bulunmuştur. Ayrıca sosyal medya kullanan katılımcıların sosyal medya kullanmayan katılımcılara göre kişisel verilerin korunmasına ilişkin kullanıcı bilgi düzeylerinin daha yüksek olduğu tespit edilmiştir.

KAYNAKÇA

Kitaplar

Ajdari, D.ve Hofnagle, C. (2013). *Web Privacy Tools and Their Effects on Tracking and User Experience on the Internet, Team for Resarch in Ubiquitous Secure Technology.* California: National Science Foundation.

Akar, E. (2010). *Sosyal Medya Pazarlaması Sosyal Web'te Pazarlama Stratejileri.* Ankara: Elif Yayınevi.

Akdağ, H. (2013). *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması.* Ankara: Adalet Yayınevi.

Akgül, A. (2016). *Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması* (2. b.). İstanbul: Beta Yayıncılık.

Aksoy, H. C. (2010). *Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması.* Ankara: Çakmak Yayınevi.

Ayözger, A. Ç. (2016). *Kişisel Verilerin Korunması.* İstanbul: Beta Yayıncılık.

Barkuus, L.ve Dey, A. (2003). Location Based Services for Mobile Telephony: A Study of User's Privacy Concerns, Proceedings of the. *INTERACT 2003, 9TH IFIP TC13 International Conference on HumanComputer Interaction 23 July*, (s. 1-20). Tokyo.

Başalp, N. (2004). *Kişisel verilerin Korunması ve Saklanması.* Ankara: Yetkin Yayınevi.

Bebber, P. V. (2011). Informed Consent in Behavioral Advertising. *Master Thesis Information Science*. Radboud University Nijmegen.

Benneth, J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and United States.* London: Cornell University Press.

Bloux, V.ve Desfougeres, J.-M. D. (2011). *Behavioral Advertising on Facebook: the users perspective regarding leisure industry.* Halmstad: Halmstad University

School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in marketing.

Butler, E., Teddy, J.ve Waugh, M. (2006). *First Party Cookie for Tracking Web Traffic.* United States Patent Application Publication.

Carey, P. (2009). *Data Protection-A Practical Guide to UK and EU Law* (3. b.). Oxford: Oxford University Press.

Castelluccia, C.ve Arvind, N. (2012, October 19). *Privacy Considerations of Online Behavioural Tracking*. Report by ENISA European Network and Information Security Agency.

Chaabane, A., Kaafar, M. A.ve Boreli, R. (2012, Ağustos 7). Big Friend is Watching You: Analizing Online Social Networks Tracking Capabilities. *Computer and SocietyPublic Policy Issues-Privacy WOSN (Workshop on Online Social Networks)*. Helsinki.

Gören, Z. (1999). *Anayasa Hukukuna Giriş* (3. b.). İzmir: Dokuz Eylül Üniversitesi Yayını.

Güney, N., Özdemir, K., Özdemir, B.ve Solmaz, Y. (2004). *Yeni Türk Ceza Kanunu.* Ankara: Adil Yayınevi.

Henkoğlu, T. (2015). *Bilgi Güvenliği ve Kişisel Verilerin Korunması.* Ankara: Yetkin Yayınları.

Kalabalık, H. (2009). *İnsan Hakları Hukuku.* Ankara: Seçkin Yayıncılık.

Kanadoğlu, K. (2009). *Özel Yaşamın Gizliliği.* Ankara: Türkiye Barolar Birliği Yayınları.

Kang, J. (2011). *Social Media Marketing İn Hospitaly Industry. The Role of Benefits in İncreasing Brand Community Participation And the İmpact of Participation consumer trust and Commitment Toward Hotel and Restauratnt Brand.* Lowa State University, Ph. UM.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları.* Ankara : Adalet Yayınevi.

Kırlıdoğ, M.ve Fidaner, I. B. (2012). Derin Veri Analizi: İnternetteki Temel Gözetim Aracı. *XIV. Akademik Bilişim Konferansı,1-3 Şubat*, (s. 967-969). Uşak.

Korff, D. (2001). *Ec Study on Implementation of Data Protection Directive (Study Contract ETD/2001/B5-3001/A/49): Comparative Summary of National, Humen Right Centre, Colchester.* UK: University of Essex.

Korkmaz, İ. (2017). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması.* Ankara: Seçkin Yayıncılık.

Küzeci, E. (2010). *Kişisel Verilerin Korunması.* Ankara: Turhan Kitabevi.

Malin, B. (2006, May). Trail Re-Identification and Unlinkability in Distributed Databases, . *PhD Thesis*. Pittsburgh: Carnegie Mellon University Institute for Software Research, International School of Computer Science.

Malin, B., Sweeney, L.ve Newton, E. (2003). *Trail Re-Identification: Learning Who You Are From Where You Have Been,* . Pittsburgh: LIDAP-WP2 Carnegie Mellon University Laboratory for International Data Privacy.

Mayer, J. R.ve Mitchell, J. C. (2012). Third-Party Web Tracking: Policy and Technology. *IEEE Symposium on Security and Privacy, May 20-23,* (s. 417-424). San Francisco.

Özbek, V. Ö. (2005). *TCK İzmir Şerhi.* Ankara: Seçkin Yayınevi.

Özbudun, E. (2012). *Türk Anayasa Hukuku* (13. b.). Ankara: Yetkin Yayınları.

Safko, L.ve Brake, D. K. (2009). *The Social Media Bible.* John Wıley & Sons Inc.

Soyaslan, D. (2005). *Ceza Hukuk Özel Hükümler* (3. b.). Ankara: Yetkin Yayınları.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması.* Ankara: Beta Yayınevi.

Torlak, Ö., Altunışık, R., Özdemir, Ş.ve Sarıkaya, N. (2007). *Yeni Müşteri.* İstanbul: Hayat Yayınları.

Tosun, B. N. (2017). *Marka Yönetimi* (3. b.). İstanbul: Beta Yayıncılık.

Wacks, R. (1989). *Personal Information: Privacy and Law.* Oxford: Clarendon Pres.

Weinberg, T. (2009). *The New Community Rules: Marketing On the Social Web* (1. b.). Sebastopol: O'Reilly Media.

Yun, K.ve Kim, D. (2006, December 12). Robust Location Tracking using a dual layer particle fitler, Pervasive and Mobile Computing 3 (2007). Science Direct, Elsevier.

Süreli Yayınlar

Ahmand, Y.ve Aljumah, A. (2013). Paradigm Shift in the Security-n- Privacy Implementation of Semi Distributed Online Social Networking. *Computer and Information Science , 6(1)*. Saudi Arabia: Salman Bin Abdulaziz University.

Akgün, V. Ö.ve Ergün, G. S. (2017). Yeni Müşteri Kavramı Ve Modern Pazarlama Sürecinde Sosyal Medya Pazarlaması. *Turkish Studies, 12*(32), 17-32.

Arrington, C. S. (2013, January). Got Cookies. *JICLT Journal of International Commercial Law and Technology, 8*(1), 13-16.

Bignami, F. (2007). Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law, 8*(1), 242-243.

Boyd, D. M.ve Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer Mediated Communication, 13*(1), 210-230.

Christopher, M.ve Kuan, H. W. (2012, February). Defining Personal Data in E-Social Science. *Information, Communication & Society Journal, 15*(1), 66-84.

Döner, A. (2006). Kişisel Verilerin Korunması Hakkında Federal Kanun. *Erzincan Atatürk Üniversitesi Hukuk Fakültesi Dergisi (EÜHFD), X*(1-2), 1-16.

Grutese-Liu, M.ve Liu, X. (2004, March-April). Protecting Privacy in Continious. Location Tracking Applications. *IEEE Computer Society, 2*(2), 28-29.

Hacıoğlu, B. C. (2004). Avrupa İnsan Hakları Mahkemesinin İhlal Kararının Türk Ceza Muhakamesi Hukukunda Yeni Bir Muhakamenin Yenilenmesi Sebebi Olarak Kabulü ve İzlenecek Muhakame Usulü Üzerine Bir İnceleme. *Erzincan Üniversitesi Hukuk Fakültesi Dergisi, VIII*(1-2), 93-113.

Kaplan, A. M.ve Haenlein, M. (2010). Users of The World, Unite! The Challenges and Opportunities of Social Media. *Business Horizons, 53*(1), 59-68.

Kılınç, D. (2015). Anayasa Mahkemesinin Özel Hayatın Korunmasına İlişkin 2013/1614 Sayılı Kararı Üzerine Değerlendirmeler. *International Journal of Legal Progress, 1*(2), 197-212.

Küzeci, E. (2014). İstatistikî Birimler ve Bilgilerin Geleceğini Belirleme Hakkı. *Türkiye ve Ortadoğu Amme İdaresi Enstitüsü İnsan Hakları Yıllığı,, 32*, 53-55.

Özdemir, H. (2009). Haberleşmenin Gizliliği ve Kişisel Veriler. *EÜHFD, XIII*(1-2), 285-304.

Özkan, A. F. (2009, Güz). Ekonomik Kamu Düzeni ve Ekonomik Kolluk Faaliyeti. *Ankara Barosu Dergisi, 67*(4), 75-84.

Sancakdar, O. (2017). Kamu Hukukunda Kişiliğin Korunması. *İstanbul Kültür Üniversitesi Hukuk Fakültesi Dergisi, 16*(1), 40-58.

Şahin, E., Çağlıyan, V.ve Başer, H. H. (2017). Sosyal Medya Pazarlamasının Tüketici Satınalma Davranışına Etkisi: Selçuk Üniversitesi İibf Örneği. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 10*(4), 67-86.

Şen, E. (2009/3, MayısHaziran). Kişisel Verilerin Korunması Kanunu Tasarısı'nın Anayasa ve Türk Ceza Kanunu Hükümleri Çerçevesinde Değerlendirilmesi. *İstanbul Barosu Dergisi, 83*, 1197-1208.

Şen, E.ve Yurttaş, Y. (2010). Bilgisayar Programları Karşısında Özel Hayatın Korunması. *Terazi Hukuk Dergisi, 5*(42), 29-44.

Tene, O.ve Polonetsky, J. (2012). To Track or "Do Not Track": Advancing Transperancy and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology, 13*(1), 283-304.

Diğer Yayınlar

Aydın: (2018). Bankacılık Sektöründe Kişisel Verilerin Korunması ve İşlenmesinin Bireyler Üzerinde Algısı ve Etkileri. *Yayınlanmamış Yüksek Lisans Tezi*. İstanbul: İstanbul Arel Üniversitesi.

Anayasa Mahkemesi. (2013, Şubat 14). Esas No: 2011/150, Karar No: 2013/30 . . Resmî Gazete Tarihi: 25.06.2013, Sayı: 28688.

Anayasa Mahkemesi, Esas No: 2014/74, Karar No: 2014/201 (Anayasa Mahkemesi Aralık 25, 2014). Nisan 23, 2019 tarihinde http://kararlaryeni.anayasa.gov.tr/Karar/Content/0e1371e0-2293-43f9-9201711f645e48b7?excludeGerekce=False&wordsOnly=False adresinden alındı

Berber, L. K. (2013, Ocak 16). *Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması*. Mayıs 2, 2019 tarihinde İnternet Geliştirme Kurulu, Raporu: www.internetgelistirmekurulu.org/tr/Rapor Dosya. aspx?D =MjR adresinden alındı

BTK 2012 DK-14/623. (2014, Ağustos 23). http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf adresinden alındı

developers.facebook. (2019). Mayıs 2, 2019 tarihinde http://developers.facebook.com/blog/post/108/ adresinden alındı

Ersoy, U. (2009). Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması. *Yayımlanmamış Yüksek Lisans Tezi*. Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

eur-lex. (2016). Nisan 23, 2019 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1512129685690&uri=CELEX:32016R0679 adresinden alındı

facebook. (2019). Mayıs 2, 2019 tarihinde www.facebook.com/advertising adresinden alındı

İnsan Hakları Evrensel Bildirisi . (2019). *Madde 12*. 23 Nisan, 2019 tarihinde https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf adresinden alındı

İşlek, M. S. (2012). Sosyal Medyanın Tüketici Davranışlarına Etkileri: Türkiye'deki Sosyal Medya Kullanıcıları Üzerine Bir Araştırma. *Yayımlanmamış Yüksek Lisans Tezi*. Karaman: Karamanoğlu Mehmetbey Üniversitesi Sosyal Bilimler Enstitüsü.

Kanun Tasarısı. (2016). *Sayı: 31853594-101-580-249*. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü. Nisan 23, 2019 tarihinde http://www2.tbmm.gov.tr/d26/1/1-0541.pdf adresinden alındı

Martinez, J. (2011, January). *Facebook: The Black Sheep of Online Behavioral Advertising, Customer Relationship Management*. Destination CRM.com: http://www.destinationcrm.com/Articles/Editorial/Magazine-Features/ Facebook-The-Black-Sheep-of-Online-BehavioralAdvertising72863.aspx adresinden alındı

Neti: (2011). Social Media and Its Role in Marketing. *International Journal of Enterprise Computing and Business Systems. Network Marketing*, 2-3. https://www.researchgate.net/publication/260908285 adresinden alındı

newsroom. (2019). Mayıs 2, 2019 tarihinde http://newsroom.fb.com/company-info/ adresinden alındı

Sağlam, F. (2002). 2001 Anayasa Değişikliğinin Yaratabileceği Bazı Sorunlar ve Bunların Çözüm Olanakları. *Anayasa Yargısı Dergisi, 19*, 8-21. http://www.anayasa.gov.tr/files/pdf/anayasa_yargisi/anyarg19/fsaglam.pdf adresinden alındı

Serozan, R. (1994). Kişilik Hakkının Korunmasıyla İlgili Bazı Düşünceler. *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, 93-112. http://dergipark.gov.tr/download/article-file/14235 adresinden alındı

Solove, D. J. (2008). *The New Vulnerability: Data Security and Personal Information*. Nisan 23, 2019 tarihinde GW Law Faculty Publications: http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2090&context=faculty_publications adresinden alındı

Telekomünikasyon Sektöründe Kişisel Verilerin ve Gizliliğin Korunması yönetmeliği. (2004). *KT.06.02.2004, RG. N. 25365*.

Trading, O. o. (2010, May). *Online Targeting of Advertising Prices, A market study, Office of Fair Trading*. Mayıs 2, 2019 tarihinde http://www.oft.gov.uk/shared_oft/business_leaflets/659703/ OFT1231.pdf adresinden alındı

Uygun, M. (2010). Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi ışığında kişisel verilerin korunması. *Yayımlanmamış Yüksek Lisans Tezi*. Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

www.facebook. (2019). Mayıs 2, 2019 tarihinde https://www.facebook.com/klmsweden adresinden alındı

Yayla, K. (2010). İnternet Pazarlamasında Yeni Eğilimler: Çevrimiçi Sosyal Ağların Üniversite Öğrencilerinin Satın Alma Davranışlarına Etkisi. *Yayımlanmamış Yüksek Lisans Tezi*. Manisa: Celal Bayar Üniversitesi Sosyal Bilimler Enstitüsü.

EKLER

Ek 1. Anket Formu

BÖLÜM I. DEMOGRAFİK BİLGİ FORMU

1. Cinsiyetiniz?

( ) Kadın ( ) Erkek

2. Yaşınız?

( ) 18-25 ( ) 26-33 ( ) 34-41 ( ) 42-49 ( ) 50 ve üzeri

3. Eğitim durumunuz?

( ) İlkokul ( ) Ortaokul ( ) Lise ( ) Ön lisans ( ) Lisans

( ) Yüksek lisans ( ) Doktora

4. Sosyal medya kullanıyor musunuz?

( ) Evet ( ) Hayır

5. Sosyal medyada günde kaç saat geçiriyorsunuz?

( ) 1 saatten az ( ) 1-3 saat ( ) 4-7 saat ( ) 8 saat ve üzeri

6. En çok hangi sosyal ağı kullanıyorsunuz?

( ) Facebook ( ) Twitter ( ) Instagram ( ) Diğer .....

BÖLÜM II. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN KULLANICI BİLGİ DÜZEYİ

1=Doğru 2=Kısmen doğru 3=Bilmiyorum 4=Kısmen hayır 5=Hayır

No.		**1**	**2**	**3**	**4**	**5**
1	6698 Sayılı Kişisel Verilerin Korunması ve Saklanması Kanunu hakkında bilgiye sahibiyim.					
2	Sosyal medyada hesap açmam kişisel verilerimin işlenmesi için yeterlidir.					
3	Sosyal medyada herhangi bir ödeme yapmanız kişisel verilerinizin					

	işlenmesi için yeterlidir.					
4	Kişisel verilerin işlenmesi müşteri bilgi gizliliği ya da verilerin korunması yükümlülüklerinin ihlali anlamına gelmez.					
5	Sosyal medyada kampanyalar, bilgilendirmeler ve hizmet teklifine ilişkin amaçlar için kişisel verileriniz korunur ve saklanır.					
6	Sosyal medyada sizin kişisel verileriniz işlenerek başka müşterileri kazanma çalışmaları yapılabilir.					
7	Sosyal medyada, kişisel verilerin işlenmesine dair rıza vermeyen bireyler ile doğrudan teklifsiz iletişime geçilir.					
8	Kişi sosyal medyada hesap açtıysa sosyal ağ bireyin kişisel verilerine erişir.					
9	Sosyal medyada müşteri memnuniyetini arttırmak, size özel kampanyalar, indirimler sağlamak amacıyla kişisel verileriniz işlenir.					
10	Kişisel veriler idari ve resmi makamlarca araştırılmalar yapıldığında ve sosyal ağlardan talep edildiğinde sosyal ağlar tarafından bu makamlar ile paylaşılır.					
11	Sosyal medyada kişisel veriler sosyal ağlar tarafından araştırma süreçleri için kullanılır.					
12	Sosyal medyada kişisel veriler 3. kişiler tarafından dolandırıcılık, sahtecilik, kara para amaçlı olaylar için kullanılabilir.					
13	Kişisel verilerim kullanılarak istismara uğradım ve sonucunda maddi zarar gördüm.					
14	Bireylerin sosyal medyada kişisel verilerinin doğru ve güncel olması sorumluluğu sosyal ağa aittir.					
15	Müşteriler kişisel verilerin nasıl korunduğunu öğrenebilir ve isteğe bağlı değiştirebilir.					

16	Sosyal medyada hesaplarınızı kapatsanız bile kişisel verileriniz istenilen kurum ve kuruluşlarla paylaşılır mı?					
17	Kimlik hırsızlığına karşı alınması gereken tedbirleri biliyorum.					
18	Sosyal medya sitelerinin güvenli olarak kullanılmasını biliyorum.					
19	Dijital imzanın ne işe yaradığını biliyorum.					
20	Kişisel verilerin korunması ve saklanması kanununun faydalı olduğunu düşünüyor musunuz?					