ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/357381057

Dijital ve Mobil Pazarlama Bağlamında İzinli Pazarlamayı Yeniden Düşünmek

Chapter · December 2021

CITATIONS
0

READS
61

1 author:



Mehmet Sağlam
Istanbul Ticaret University
78 PUBLICATIONS **315** CITATIONS

SEE PROFILE

All content following this page was uploaded by Mehmet Sağlam on 30 November 2023.

The user has requested enhancement of the downloaded file.

İŞLETME BİLİMİNDE KURAMSAL VE PRATİK PAZARLAMA KONULARI



Editör
Dr. Şahin KARABULUT

Gazi Kitabevi



"En İyi Akademi, Bir Kitaplıktır."

İŞLETME BİLİMİNDE KURAMSAL VE PRATİK PAZARLAMA KONULARI

Editör
Dr. Şahin KARABULUT
ORCID: 0000-0001-7955-6404

© Gazi Kitabevi Tic. Ltd. Şti.

Bu kitabın Türkiye'deki her türlü yayın hakkı Gazi Kitabevi Tic. Ltd. Şti'ne aittir, tüm hakları saklıdır. Kitabın tamamı veya bir kısmı 5846 sayılı yasanın hükümlerine göre, kitabı yayınlayan firmanın ve yazarlarının önceden izni olmadan elektronik, mekanik, fotokopi ya da herhangi bir kayıt sistemiyle çoğaltılamaz, yayınlanamaz, depolanamaz.

ISBN • 978-625-8443-09-7

1. Baskı • Aralık 2021, Ankara

Dizgi/Mizanpaj • Gazi Kitabevi
Kapak Tasarımı • Gazi Kitabevi

Gazi Kitabevi Tic. Ltd. Şti.
Yayıncı Sertifika No: 44884

Merkez
Bahçelievler Mah. 53. Sok. No: 29 Çankaya/ANKARA
0.312 223 77 73 - 0.312 223 77 17
0.544 225 37 38
0.312 215 14 50
www.gazikitabevi.com.tr
info@gazikitabevi.com.tr

Mağaza
Dögol Cad. No: 49/B Beşevler/ANKARA
0.312 213 32 82 - 0.312 213 56 37
0.312 213 91 83

Sosyal Medya
gazikitabevi
gazikitabevi
gazikitabevi

Vadi Grafik Tasarım Reklam Ltd. Şti.
Sertifika No: 47479

Matbaa
İvedik Organize Sanayi Bölgesi 1420. Cadde No:58/1 Yenimahalle / ANKARA
0.312 395 85 71

ÇALIŞMAYA YAZAR OLARAK KATKI SAĞLAYAN BİLİM İNSANLARI

Prof.Dr.	Bilal GEREKAN	Karadeniz Teknik Üniversitesi
Prof.Dr.	Nilsun SARIYER	Muğla Sıtkı Koçman Üniversitesi
Prof.Dr.	Süleyman BARUTÇU	Pamukkale Üniversitesi
Doç.Dr.	Banu KÜLTER DEMİRGÜNEŞ	Kırşehir Ahi Evran Üniversitesi
Doç.Dr.	Halil Semih KİMZAN	Eskişehir Osmangazi Üniversitesi
Doç.Dr.	İsmail Tamer TOKLU	Recep Tayyip Erdoğan Üniversitesi
Doç.Dr.	Pelin VARDARLIER	İstanbul Medipol Üniversitesi
Doç.Dr.	Yıldırım YILDIRIM	Düzce Üniversitesi
Dr.Öğr.Üye.	A. Selçuk KÖYLÜOĞLU	Selçuk Üniversitesi
Dr.Öğr.Üye.	Ayşe AYGÜN ÖZGÖZ	Afyon Kocatepe Üniversitesi
Dr.Öğr.Üye.	Fatih ELİBOL	Tokat Gaziosmanpaşa Üniversitesi
Dr.Öğr.Üye.	Fatih ŞAHİN	Bandırma Onyedi Eylül Üniversitesi
Dr.Öğr.Üye.	Gülçin BİLGİN TURNA	Recep Tayyip Erdoğan Üniversitesi
Dr.Öğr.Üye.	Mehmet Can DEMİRTAŞ	Kırklareli Üniversitesi
Dr.Öğr.Üye.	Mehmet SAĞLAM	İstanbul Ticaret Üniversitesi
Dr.Öğr.Üye.	Neslihan PAKER	İzmir Kavram Meslek Yüksekokulu
Dr.Öğr.Üye.	Nur ÇAĞLAR ÇETİNKAYA	Çankırı Karatekin Üniversitesi
Dr.Öğr.Üye.	Onur AKDAŞ	Dokuz Eylül Üniversitesi
Dr.Öğr.Üye.	Reyhan BAHAR	Bandırma Onyedi Eylül Üniversitesi
Dr.Öğr.Üye.	Taner SIĞINDI	Muğla Sıtkı Koçman Üniversitesi
Öğr.Gör.Dr.	Deniz ÜNAL ADIGÜZEL	Pamukkale Üniversitesi
Öğr.Gör.Dr.	Mehmet Ozan KARAHAN	Uşak Üniversitesi

Araş.Gör.Dr.	Hilal ÖZTÜRK KÜÇÜK	Artvin Çoruh Üniversitesi
Dr.	Ahmet AYDIN	--
Dr.	Özgür ULUDAĞ	Eskişehir Osmangazi Üniversitesi
Araş.Gör.	Ahmet TUZCUOĞLU	İstanbul Üniversitesi
Araş.Gör.	Emine GÜNDOĞMUŞ	İstanbul Medipol Üniversitesi
Araş.Gör.	Oğuz Yusuf ATASEL	Karadeniz Teknik Üniversitesi
Bilim Uzmanı	Tuğba KÖYSÜREN	Kırşehir Ahi Evran Üniversitesi
	Ayşen AYDIN	İstanbul Üniversitesi
	Talha DOĞAN	Düzce Üniversitesi

Yazarlar unvanları dikkate alınarak isimlerine göre alfabetik olarak sıralanmıştır.

"Bu kitapta yer alan bölümlerde kullanılan kaynakların, görüşlerin, bulguların, sonuçların, tablo, şekil, resim ve her türlü içeriğin sorumluluğu yazar veya yazarlarına ait olup ulusal ve uluslararası telif haklarına konu olabilecek mali ve hukuki sorumluluk da yazarlara aittir."

Dijital ve Mobil Pazarlama Bağlamında İzinli Pazarlamayı Yeniden Düşünmek 171
Mehmet SAĞLAM

Online Hizmetlerde Pazarlama Anlayışı 197
Ahmet AYDIN

Hizmet Hataları ve Telafisinde Kullanılabilecek Stratejiler 219
Reyhan BAHAR

İş Pazarındaki Müşteri İlişkileri Yönetiminde Sosyal Medya Araçlarının Kullanımı 233
Taner SIĞINDI

Kurumsal Sosyal Sorumluluk Faaliyetleri: Bir Lojistik İşletmesi Olan Arkas Holding (1902) Örneği 257
Oğuz Yusuf ATASEL, Bilal GEREKAN

Tüketici Yabancılaşması 275
Nilsun SARIYER

Tüketici Marka İlişkileri ve Marka İhlalleri 297
Fatih ŞAHİN

Tüketicilerin Gsm Operatörü Tercihlerinde Demografik Özelliklerin Etkisi 321
A. Selçuk KÖYLÜOĞLU

Tüketicilerin Sürdürülebilir Modaya Yönelik Tutum ve Davranışlarının Değerlendirilmesi 337
Banu KÜLTER DEMİRGÜNEŞ, Tuğba KÖYSÜREN

Gelişmeleri Kaçırma Korkusu (FOMO)'nun Pazarlama Alanındaki Kullanımı ve Tüketici Davranışlarına Yansımaları 375
Yıldırım YILDIRIM, Talha DOĞAN

DİJİTAL VE MOBİL PAZARLAMA BAĞLAMINDA İZİNLİ PAZARLAMAYI YENİDEN DÜŞÜNMEK

Mehmet SAĞLAM[1]

"Kimsenin bilmesini istemediğin bir şey varsa, belki de yapmamalısın."
— Eric Schmidt, Google CEO (Huffington Post-Aralık 2009)

1. GİRİŞ

Dijital pazarlamacılar için ilgi çekici bir kanal olarak görülen mobil akıllı telefon teknolojisinin artan şekilde benimsenmesi, mobil pazarlama faaliyetleri için daha fazla olanak sağlamıştır. Persaud ve Azhar (2012) 'ın da belirttiği gibi, "akıllı telefonların artan yetenekleri, pazarlamacılara tüketicileri araştırmak ve hizmet vermek için önemli ölçüde genişletilmiş olanaklar sunmuştur" (Persaud ve Azhar, 2012:1). Mobil telefonların artan kullanımı yanında günlük yaşamda dijital teknolojilerin kullanımının yaygınlaşması, olağanüstü miktarda veri üretilmesine ve bu verilerin çeşitli bulut depolama alanlarıyla işletmelere aktarılmasına neden olmuştur. Veriye ulaşmanın, anlamlandırmanın ve kullanmanın büyük önem kazandığı bu dönemde, rekabet avantajı elde etme, dijital bilgilerden yararlanma ve kişisel verilere sahip olma arayışlarında olan her türden işletme, riskleri yönetme, veri gizliliği ve tüketici güveni sağlama konusunda zorlanmaktadır. Süreçlerin dijitalleşmesi ve mobil teknoloji kullanımının artmasıyla birlikte, hem işletmeler hem de tüketiciler için daha fazla risk ortaya çıkmaktadır. Yaygın olarak kullanılan dijital ve mobil teknolojiler, bu anlamda topluma eşi görülmemiş tehditler getirmektedir.

1 Dr. Öğr. Üyesi, İstanbul Ticaret Üniversitesi, İşletme Fakültesi, İşletme Bölümü, msaglam@ticaret.edu.tr, ORCID: 0000-0002-1909-4284.

İzinli pazarlama açısından, pazarlama iletişiminin ana yolunun kısa mesaj veya SMS mesajları yoluyla olduğu akıllı telefon öncesi çağda yapılan önceki çalışmalar, tüketicilerin mobil pazarlama iletişimini çeşitli şekillerde rahatsız edici (Muk, 2007), müdahaleci (Monk vd., 2004) ve mahremiyet istilası olarak algıladıklarını göstermiştir (Windham ve Orton, 2002).

Son zamanlarda ise gizlilik ihlalleri hakkında pek çok haber manşetiyle, gizlilik ölmüş gibi görünebilir. Bazı tüketiciler, tüm verilerinin zaten kaydedildiğini ve saklayacak hiçbir şeyi olmadığını düşünürken, bazıları, kişisel verilerin paylaşılması zorunluluğuna bağlı olarak gizlilik ihlali endişesiyle mobil ve dijital teknolojileri kullanmaktan korkmaktadır. Bu durum birer pazarlama kanalı olarak dijital ve mobil pazarlama etkinliklerinin izinli pazarlama çerçevesinde yeniden sorgulanmasını gerekli kılmaktadır.

Bireyler mobil cihazları ve dijital teknolojileri, hava durumu öğrenme, navigasyon, mobil alışveriş, sosyal ağlarda gezinme, haberleri takip etme, cihazlar arası paylaşım yapma gibi çeşitli amaçlarla kullanmaktadır. Uygulama geliştiricileri ve pazarlamacılar ise bu kullanıcıların yaşı, cinsiyeti, e-posta adresi, medeni durumu, gezindiği, takip ettiği sosyal medya sayfaları, mobil alışveriş siteleri gibi kişisel verilerini toplamakta ve müşteri profilleri (müşteri avatarı) oluşturmaktadır. Elde edilen bu veriler ve oluşturulan profiller ise, pazarlama iletişim çalışmaları kapsamında kullanılarak her profile uygun iletişim çabaları hazırlanmakta ve işletmeye daha fazla müşteri çekilmeye çalışılmaktadır. Aynı zamanda bu veriler hem kendi amaçları için kullanılmakta hem de ticari çıkarlar için üçüncü taraflara satılabilmektedir. Bu nedenle bireylerin bilgilerini istemeye ve işlemeye dayalı izinli pazarlama temelinde toplanan verilerin gizliliğinin ve mahremiyetinin sağlanması, saklanması, korunmasına ilişkin gizlilik endişeleri gibi konular önem kazanmıştır.

Pazarlama ve ilgili disiplinlerdeki araştırmalar, verilerin ve dijital gizliliğin yasal ve etik yönlerine (Nill ve Aalberts 2014), kişiselleştirme ve mahremiyet arasındaki bağlantılara (Aguirre vd.,2015), tüketici güveni ve firma performansıyla ilişkili olarak mahremiyet ilişkisine (Martin,

2018) değinmiştir. Bu konu yeni görünmese de, tüketicilerin, işletmelerin, hükümetlerin ve sosyal medya platformlarının tümünün bu endişelere uyum sağlama biçimleri, veriyi toplama ve kullanma yetenekleri hala değişmektedir ve net bir çözüme ulaşılmış değildir.

Bu çalışmada, öncelikle izinli pazarlama kavramı tanımlanmış, dijital ve mobil pazarlama bağlamında izinli pazarlama temelinde kullanılan yöntemlerin, dijital teknolojilerdeki ve mobil uygulamalardaki kişisel veri gizlilik ihlallerinin, tüketicilerin gizlilik endişelerinin, kendilerini korumaya çözüm önerilerinin, yasal düzenlemelerin neler olduğu ele alınmış ve karşılıklı çözüm önerileri sunulması amaçlanmıştır.

2. İZİNLİ PAZARLAMA

İzinli pazarlama, bir müşterinin bir haber bültenine kaydolduğunda, Facebook'ta bir işletme sayfasını beğendiğinde ya da başka şekilde marka ile iletişime geçip pazarlama iletişimine yönelik mesajlar almayı kabul ettiğinde ortaya çıkan durumdur. Kavramsal olarak ilk defa Seth Godin (1999) tarafından ortaya atılmıştır ve "İzin Pazarlaması: Yabancıları Dostlara ve Dostları Müşterilere Dönüştürme" isimli kitabıyla popüler hale gelmiştir.

Godin (1999) bu kitapta, tüketiciler tarafından memnuniyetle kabul edilen pazarlama iletişim mesajlarının tüketicilere gönderilmesi için tüketici izninin rolünü açıklamış, küçük ya da büyük şirketler ve çevrimiçi ya da çevrimdışı tüm pazarlar için yararlı olduğunu belirtmiş ve izinli pazarlama aracılığıyla şirketlerin müşterileriyle uzun dönemli ilişkiler kurabileceğini söylemiştir (Godin, 1999).

İzinli pazarlama, geleneksel pazarlama iletişim araçlarından doğrudan pazarlamadan, beklenen, kişisel ve ilgili olma gibi üç noktada farklılaşmaktadır (Godin, 1999); Birincisi, işletmelerin posta listelerine dahil olma ve ticari mesajlar almayı beklemesi (beklenen), ikincisi, gönderilecek mesajların doğrudan kişiye özel ve kişileştirilmiş olması (kişisel), üçüncüsü, mesajların müşterilerin ilgilendiği ürün ve hizmetlerle ilgili olması (ilgili) anlamına gelmektedir.

Krishnamurthy (2000) ise Godin (1999)'e ek olarak izinli pazarlamanın 6 özelliğini açıklamıştır. Birincisi, izin örtük, gizli olmamalı, aldatıcı taktiklerden yoksun olmalı ve açık bir şekilde alınmalıdır. İkincisi, tüketici iletişim amaçlı herhangi bir izne onay verdiğinde kimliği doğrulanmalı ve bunun için kişisel e-posta hesabı kullanılmalıdır. Üçüncüsü, tüketici devam eden iki yönlü bir ilişkiye girdiğini anlamalıdır. Dördüncüsü, tüketici firmanın kendisi hakkında ne bildiğini tam olarak bilmelidir ve bu bilgileri herhangi bir zamanda değiştirebilmelidir. Beşincisi, tüketici kendisine gönderilen mesajların niteliğini ve sayısını kontrol edebilmelidir. Sonuncusu ise, tüketici herhangi bir noktada bir izinli pazarlama ilişkisinden çaba harcamadan çıkabilmelidir (Krishnamurthy, 2000). İzinli pazarlamanın taşıması gereken bu özellikler müşterilerle iyi ilişkiler kurma ve sürdürme üzerine geliştirilmesine rağmen, zamanla değişen ortama bağlı olarak farklı kullanım alanları ortaya çıkmış ve kişisel verilerin gizliliği, güvenliği gibi konular gündeme gelmiştir.

İzinli pazarlama, başlangıçta e-posta ya da kısa mesaj (SMS) gönderimi gibi uygulansa da, internetin etkisiyle kullanım alanları artmıştır. İnternetin etkisi yanında mobil ve dijital alanda yaşanan gelişmeler sonucu özellikle tüketiciler arasında çevrimiçi gizlilik endişeleri arttığı için bu durum son zamanlarda popüler hale gelmiştir (Holmes 2000). Bu nedenle, müşterilerle ilişkilerin sürdürülebilirliği için bu tür mecralarda paylaşılan bilgilerin kullanılması ve mesajların iletilmesinde tüketici rızalarının alınmasını amaçlayan bir izin süreci tasarlamak birçok işletme için öncelik olmuştur. Bilgilerin yüksek derecede kişiselleştirme içermesi, tüketici gizlilik endişelerinin artmasına neden olmuştur (Tucker, 2014). Yapılan araştırmalarda tüketicilerin verilere kimin erişimi olduğu ve nasıl kullanıldığı konusunda endişeli oldukları ve bilgi sahibi olmak istedikleri ve bu tür verileri işletmelerle paylaşmaları ve mesaj gönderilmesine onay verilmesi karşılığında fayda aradıkları ortaya çıkmıştır (Groopman 2015).

Dijital teknolojiler, mobil akıllı telefonlar ve sosyal medya mecraları işletmeler için tüketicilerle iletişime geçme ve bu ortamlardaki verilerini kullanma açısından izinli pazarlamaya dahil edilen araçlardır. Bunun nedeni bu ortamlarda büyük miktarda veri akışının gerçekleşmesi ve

kişisel bilgilerin izin/onay dahilinde kullanımına olanak sağlanmasıdır. Ancak tüketiciler gerçeğin farkında değildir. Satın aldıkları eşya, araç ve otomobillerdeki teknolojileri kullanırken, bu araçların kullanımı için onay verirken, akıllı telefonlarına herhangi bir uygulama indirirken, konum özelliği açıkken, mobil alışveriş sitesine kayıt olurken ya da Google ya da Facebook gibi hesapları kullanarak oturum açarken, sosyal medya mecralarında paylaşım yaparken ve gezinirken, sayfaları beğenip yorum yaparken otomatik olarak birçok işletmeye kişisel bilgilerinin aktarılmasına imkan sağlamaktadırlar.

3. DİJİTAL TEKNOLOJİLER ÜZERİNDEN İZİNLİ PAZARLAMA

Dijitalleştirme süreci, veri toplama, ayrıştırma ve depolama maliyetlerini azalttığından, pazarlamanın birçok alanının veriyi benzeri görülmemiş derecede benimsemesine olanak tanımıştır (Goldfarb ve Tucker, 2019). Firmalar, pazarlama iletişimi başta olmak üzere birçok pazarlama faaliyeti için dijital ve mobil teknoloji araçlarından elde ettikleri tüketici verilerini kullanmaktadır. Toplanan verilere dayalı müşteri profili (avatarı) oluşturularak hedef pazar belirlenerek, o pazara uygun pazarlama faaliyetleri hayata geçirilmekte, gerekli iyileştirilmeler yapılmakta ve stratejiler geliştirilmektedir.

Tüketicilerden bilgi toplayanlar sadece işletmeler değildir. Hükümetler de ülke vatandaşlarının güvenliğinin sağlanması, gizlilik endişelerinin en aza indirilmesi amacıyla, dijital ayak izleri oluşturmaktadır. Vatandaş ve müşteriler ise o mecralarda işlem yaparken verileri paylaşarak dijital gölgeler oluşturmaktadır. Buralardan toplanan veriler, internetteki uygulamalar, diğer bağlı cihazlar ve sensörler üzerinden işlemler gerçekleştirilirken geride bırakılan kişisel verilerdir (Shave, 2016). Kişisel veriler, yaş, cinsiyet, gelir düzeyi, eğitim durumu gibi demografik özellikleri, yaşam tarzı, satın alma davranışları, satın alım miktarları, ne zaman aldıkları, ödeme yöntemleri, teknolojik araçları kullanım becerileri gibi birçok veriyi içermektedir.

Tüketici verilerinin toplanması ve izinli pazarlama çerçevesinde kişisel verilerin alınması, saklanması, gizliliği gibi hususlarda hala büyük belirsizlikler mevcuttur. Veri toplama açısından işletmelere büyük bir veri akışı sağlayan dijital teknolojilerden biri, birbirine ağ temelli bağlı cihazların kullanıldığı nesnelerin interneti (Internet of Things) teknolojisidir.

Güvenli ve sorunsuz bir sürüş deneyimi sağlamak için diğer araçlar ve trafik merkezleriyle etkileşime giren arabalar, sağlığımızı izlememize yardımcı olan dijital sağlık adı altında faaliyetler, vücudumuzla ilgili verileri toplayan giyilebilir araçlar ve yaşam kalitemizi iyileştirme yeteneğine sahip akıllı ev aletleri, nesnelerin interneti teknolojisinin uygulamadaki bazı örnekleridir. Bu tür örnek uygulamalarla tüketicilerden toplanan veri miktarında önemli bir artışa katkı sağlanmaktadır (Zarandi vd., 2020).

Nesnelerin İnterneti'nin (IoT) ortaya çıkışı, bireysel tüketiciler hakkında toplanan ve paylaşılan veri miktarında kritik bir değişime neden olmuştur. Birçok kullanıcı, nesnelerin internetini içeren teknolojilerin kullanımını kolaylık olarak algılasa da, yine çoğu kullanıcı kişisel olarak tanımlanabilir bilgilerin ihlallerinden büyük ölçüde habersizdir (Menard ve Bott, 2020). Kullanıcılar sürecin hızla tamamlanması için "ileri", "kabul ediyorum" veya "onaylıyorum" düğmelerine tıklayarak doğrudan onay verebilmektedir.

Nesnelerin interneti teknolojisine sahip cihazların büyük miktarda veri üretmesi ve önemli güvenlik açıklıklarına sahip olması, işletmelerin güvenlik, onay ve veri sahipliği açısından dikkate alması gereken önemli bir zorunluluğu ortaya çıkarmaktadır (Peppet, 2014). Bu cihazları kullanan tüketicilerin çoğunluğu gizlilik politikalarından habersizdir ve otomatik olarak onayladıkları, okumaktan çekindikleri unsurların neler olduğunu bilmeden onay vermektedir. İşletmelerin çoğunun gizlilik politikalarında "tüm bilgi, materyal ve içeriğin,,,,,,şirketine ait olduğu ve izin alınarak kullanıldığı" belirtilmektedir. Bu durum tüketicilerin bu cihazları kullanım süresince toplanan verilerin, satın alınan işletme ya da üçüncü taraflar tarafından kullanma hakkını kabul ettiğini göstermektedir. Veri sahipliği ise işletmelerin ve tüketicilerin dikkate alması gereken üçüncü zorluktur. Geleneksel ticarette bir ürün satın alındıktan sonra tüketicilerin ürünün

tüm mülkiyetine sahip olduğu belirtilirken, günümüzde yeni teknolojilerle birlikte nesnelerin interneti teknolojisi içeren herhangi bir cihaz alındığında, içerisinde toplanan veriler nedeniyle müşterinin cihazı paylaşamama, tamir edememe, değiştirememe veya yeniden satamama gibi birçok kısıtla karşılaşması söz konusudur (Bartholomew, 2015).

Nesnelerin interneti teknolojisinin yaygın olarak kullanıldığı cihazlardan bazıları akıllı ev teknolojileri kapsamında kullanılmaktadır. Kullanıcılar bu cihazlardan sağlayacağı faydaya karşı, işletmelere kişisel veri paylaşımı konusunda izin verebilmektedir.

Uzaktan ev kontrolü sağlamak için telekomünikasyon ve web teknolojilerine dayanan uzaktan ev izleme, kontrol etme sistemleri kullanıcılarına zaman kazanma ve hız kolaylığı sağlamaktadır. Kullanıcılar eve gelmeden önce bu cihazlara komutlar vererek çalışmalarını başlatma veya düzenleme konusunda yardımcı olmaktadır. Enerji verimliliği, su tüketim göstergeleri gibi verilerin geri bildiriminin sağlanması tüketicilerde fayda olarak algılanacağı için, izinli pazarlamayı kabul edilebilmektedir (Warkentin, vd., 2017). Bu süreçte işletmeler yine izinli pazarlama kapsamında kullanıcı verilerini kaydetmekte ve dönem dönem kullanıcılarla paylaşarak pazarlama iletişimi kampanyalarında ve stratejilerinde kullanmaktadırlar.

Kişisel verilerin toplanmasında kullanılan bir diğer dijital teknoloji artırılmış gerçekliktir. Artırılmış gerçeklik, "gerçek ve sanal nesneleri gerçek bir ortamda birleştiren; etkileşimli ve gerçek zamanlı olarak çalışan" bir teknolojidir (Harborth ve Page, 2021). Artırılmış gerçeklik teknolojisini kullanıcılara sunmanın bir yolu akıllı gözlük kullanımı, bir diğer yolu ise mobil artırılmış gerçeklik uygulamalarıdır (Kohn ve Harborth, 2018). Her iki yolda da tüketicilerin kişisel verileri toplanmaktadır. Veri toplama süresince yine önemli olan husus, kullanıcı izninin alınmasıdır.

Akıllı gözlük kullanımına yönelik artırılmış gerçeklik uygulamaları dünya üzerinde çok az kullanılması nedeniyle belki veri toplama sürecinde şu an düşük bir etkiye sahipken, mobil artırılmış gerçeklik uygulamalarında kamera erişimine izin verme sonucunda büyük

miktarda veri paylaşılmaktadır. Sonuç olarak birçok kullanıcının kişisel verilerinin gizliliği riski ortaya çıkmaktadır (Harborth ve Page, 2021). Evinizin odalarının boyama ihtiyacına yönelik bir mobil uygulama indirip, telefonunuzun kamerasına erişime izin vermeniz durumunda hangi odada hangi rengin nasıl görüneceğine dair fikir edinirken, kameraya erişim nedeniyle birçok kullanıcı gizlilik endişesine sahip olmaktadır. Benzer şekilde evinize satın almayı düşündüğünüz mobilya, koltuk vb. alışverişlerinizde, online alışveriş mağazasına telefondan artırılmış gerçeklik uygulaması aracılığıyla kamera erişimine izin verip bağlanarak bu ürünlerin evinizde nasıl görüneceği sanal görüntülerle görebilmektedir. Kullanıcılar uygulamayı kullanım sonucu fikir edinme ve satın alma sürecini kolaylaştırma, araştırma maliyetlerinden kurtulma faydası sağlarken, işletmeler hem satış yapmakta, hem de izinli pazarlama dahilinde kişisel verilerinizi alarak sonraki satın alma davranışlarınız için pazarlama iletişimi amacıyla ürün tanıtım, bilgilendirme mesajlarınızı tarafınıza iletmektedir.

4. MOBİL PAZARLAMA ÜZERİNDEN İZİNLİ PAZARLAMA

Cep telefonları üzerinden izinli pazarlama başlangıçta kısa mesaj gönderimi (SMS), çağrı merkezlerinden aranma ve e-posta gönderimi gibi yollarla kullanılırken, akıllı telefon kavramının hayatımıza girmesiyle daha farklı kullanım alanlarıyla mobil pazarlamada kendine yer bulmuştur.

Mobil pazarlama, kısa mesajlar, mobil reklamcılık, konum bilgileri paylaşımı, mobil uygulamalar, mobil içerik sunumu, kullanıcı tarafından oluşturulan içerik ve mobil ticaret yoluyla bir markayla müşteri etkileşimini izne dayalı olarak oluşturmak için sıklıkla kullanılmaktadır. Sunulan geniş olanaklardan fayda sağlamak için bireyler, hava durumu kontrolü, yol trafiği, kişiselleştirilmiş haberler, sosyal medya sayfaları takibi, mobil bankacılık uygulamaları, mobil alışveriş gibi farklı amaçlar için mobil telefonları gün içerisinde sıklıkla kullanmaktadır. Bu süreçte uygulama geliştiricileri ve işletmeler mobil kullanıcılar hakkında profil oluşturmaya

yönelik çeşitli alanlarda büyük miktarda bilgi toplamaktadırlar. Bu tür çoğu uygulama ve hizmetin kullanımı için kullanılıcılardan kişisel verilerin korunması kanununa göre izin istense de, telefonların ekranının küçük görünümü ve aydınlatma metninin uzunluğu nedeniyle birçok kullanıcı bu izni kolaylıkla ve hızlıca verebilmektedir.

Mobil uygulama öneri sistemleri, uygulama indirme ve kullanma süresince kullanıcılara sunulan ve veri toplama amaçlı kullanılan bir sistemdir. Süreç boyunca tarafınızdan toplanan kayıtlar en verimli şekilde kullanılıp sınıflandırılarak, sizinle benzer bir ürün ya da hizmet arayan ve sizin profilinize yakın olan kullanıcı gruplarına özel önerilerde bulunulmasına imkan sağlanmaktadır (Twardowski ve Ryzko, 2015). Bu durumda da yine tarafınızdan herhangi bir izin alınıp alınmadığı merak konusudur. Söz konusu öneri listesi önceki kullanıcıların kim neyi indirdi, neyi satın aldı vb. önerilerle alışveriş verilerinin kaydedilmesi sonucu hem size bir sonraki alışverişinizde hem de benzer profildeki hedef gruplara yeni ürünlerin önerilmesi yapılabilmektedir.

Mobil alışveriş akıllı telefonlarla birlikte gelişim gösteren ve birçok ülkede popüler hale gelen bir alışveriş türüdür. Sunulan rahatlık, hız ve düşük çaba beklentisi nedeniyle tüketiciler internet mağazalarından akıllı telefonlarını kullanarak yaygın şekilde alışveriş gerçekleştirmektedir. Fakat, yapılan bir araştırmada mahremiyet konusunda daha fazla endişesi olan tüketicilerin bu tür mobil alışveriş uygulamalarından yararlanma olasılığının daha düşük olduğunu göstermiştir (Hoffman vd.,1999). Herhangi bir uygulama kullanırken konuk bilgisine erişim isteğine izin verilmesi durumunda tüketicilerde konumun ifşa edilmesi gizlilik endişelerine neden olabilmektedir (Abbas vd., 2014). Bir mobil uygulama indirme sürecinde bile belki de çoğu kullanıcıya göre gereksiz sayılabilecek birçok noktaya erişim izni istenmektedir.

Mobil uygulamalar aracılığıyla toplanan verilerin ne amaçla toplandığı, nasıl kullanıldığı konusunda kullanıcıların farkında olmadığı yapılan araştırmalarda ortaya çıkarılmıştır. Enck ve arkadaşları (2010) tarafından yapılan bir araştırmada, mobil uygulamaların yarısının kullanıcı izni olmadan özel verileri üçüncü taraflara aktardığı tespit edilmiştir (Enck, vd., 2010). Ayrıca uygulamaların çalışması için kişi listesi, fotoğraflara,

dosyalara erişim gibi gereksiz görülebilecek izinleri isteyip toplayan uygulamalar da mevcuttur.

2015 yılında yapılan bir başka çalışmada, mobil uygulamalar aracılığıyla üçüncü taraflara ne tür veriler gönderildiği, Google Play Store ve Apple App Store'da yer alan 110 ücretsiz mobil uygulama üzerinden analiz edilmiştir. Çalışma sonucunda iş bilgileri, sağlık bilgileri, konum bilgileri gibi veriler dahil olmak üzere bu tür verileri toplama ve işleme olasılığı yüksek olan 9 uygulama açıklanmış, kulllanıcıların izni olmadan bu verilere erişimin ve üçüncü taraflarla paylaşımının yapıldığı belirlenmiştir (Zang, vd., 2015).

İzinli pazarlamanın, işletmeler tarafından etik olmayacak şekilde gerçekleştirilmesine örnek olarak birkaç çalışma yapılmıştır (Hayes, vd., 2020). Bu araştırmalarda Uber'in kullanıcılarının konumunu gizlilik politikalarıyla ters düşecek şekilde izlediği ortaya çıkmıştır (Hayes, vd., 2018). Bir diğer çalışmada Angry Birds'ün devlet kurumları tarafından kullanıcıların profil bilgilerini ortaya çıkarma konusunda nasıl kullanılabileceği belirtilmiştir (Snow vd., 2016). Her ne kadar bu işleyişten haberdar olmayan kullanıcı grubu olsa da, profil bilgilerinin zenginliğinin ve öneminin farkında olan ve gizlilik ayarları ile veri paylaşım iznini kontrol edebileceğini düşünen kullanıcı grupları da mevcuttur.

Mobil pazarlama bağlamında kişisel verilerin kullanıldığı mobil uygulama olarak ortaya çıkan diğer bir pazarlama iletişim platformu sosyal medya mecralarıdır. Örneğin her ne kadar sosyalleşme ve eğlence platformu olarak görünse de Facebook, kullanıcılarına kampanya ve pazarlama tanıtım faaliyetlerinin sunulmasında her geçen gün daha fazla kullanılmaktadır. Bu faaliyetlerin uygun hedef gruba yönlendirilmesinde yine kullanıcı kişisel verileri, profil bilgileri kullanılmaktadır.

Sosyal medya platformları, işletmelere hedef kitleye ulaşma, kişiselleştirilmiş reklam gönderme ve iletişim kurma fırsatı sunmaktadır. Bu nedenle şaşırtıcı olmayan bir şekilde birçok marka başta reklam harcamaları olmak üzere pazarlama iletişim bütçelerinin giderek daha fazlasını sosyal medyaya ayırmaktadır (Knoll, 2016). Kişisel bilgileri, paylaşılan içerikleri arkadaşları ile paylaşan kullanıcılar ise bu bilgilerin uygulama geliştiriciler,

işletmeler ve üçüncü taraflar tarafından izinsiz kullanıldığının, izinli kullanılsa da ne amaçla ve güvenilir şekilde kullanılıp kullanılmadığının yine farkında değildirler. Her geçen gün kullanıcı sayısının ve toplanan verilerin büyüklüğünün artması, kullanıcı güvenlik ve mahremiyetlerine ilişkin tehdit seviyesini artırmaktadır (Misra, 2016). Kullanıcıların paylaştığı her içerik ve beğendiği sayfa paylaşımları, takip ettiği sosyal medya marka hesapları, göz izleme teknikleriyle takip edilebilen, hangi paylaşımda ne kadar ilgilendiği, gözünün nerelere odaklandığı gibi diğer tür veriler de işletmelere pazarlama faaliyetlerinde kullanılmak ve yeni stratejiler oluşturmak için yol gösterici nitelikte görülmektedir.

İzinli pazarlamada son dönemde kullanılan bir başka mobil pazarlama alanı mobil mesajlaşma uygulamalarıdır. Bunun bir örneği Facebook Messenger uygulamasıdır. Facebook kullanıcı mesajlarını gözetlemek için teknolojiden yararlandığını ve bu mesajların gerçek bir kişi tarafından görülmediğini açıklamasına rağmen Facebook kullanıcıları bu izinlerin kendi yararlarına nasıl kullanıldığı konusunda endişelidir. 2014'te bu endişeyi destekleyecek bir durum gerçekleşmiştir. Facebook kullanıcıları, Facebook Messenger uygulamasından yararlanmak için uygulamayı indirmeye zorlanmıştır ve ortalama bir uygulamadan daha fazla kişisel bilgiye ve erişime izin istenmesi nedeniyle kullanıcıların başlangıçta temkinli olmasına neden olmuştur. 2018 yılı başlarında ise Facebook kullanıcılarının izni olmadan kişisel verilerinin Cambridge Analytica tarafından toplandığı ortaya çıkınca, Twitter'da #DeleteFacebook hareketi trend olmuştur (Pfohl, 2020).

Facebook yaşanan tepkiler karşısında şifreli, gizli, kendi kendini bir süre sonra imha eden yeni bir özelliğini duyurmuştur. Facebook Messenger uygulamasında aslında kullanıcıların kişisel verileri üzerinde kontole ve güvene sahip olmaları "Gizli Konuşmalar" seçeneğini kullanmaları durumunda mümkündür. Fakat günümüzde birçok kullanıcı bu özelliğin varlığından haberdar değildir. Benzer bir özellik, Facebook'un satın aldığı WhatsApp mobil mesajlaşma uygulaması üzerinde uçtan uca şifreleme kavramıyla tanıtılmıştır. Bu özellik yazılan mesajın ya da tüm paylaşımların karşı tarafa ulaşana kadar karışık bir harf ve rakam olarak görülmesini

ifade etmektedir (Pfohl, 2020). Kullanıcılar açısından bu özellik gizlilik endişelerini azaltmaya yardımcı olsa da aslında yapılan güncelleştirmelerle istenen izinler yine verilerin paylaşımı ve gizliliği konusundaki endişeleri artırmaktadır.

WhatsApp'ın dünyadaki en büyük mesajlaşma uygulaması olması nedeniyle, günlük kullanımda toplanan kullanıcı verilerinin büyüklüğü tartışmasız büyük bir potansiyele sahiptir. Uygulama yüklenirken tarafınızdan istenen gerekli ya da gereksiz görülen birçok izin erişimi her ne kadar güvenlik endişelerini artırsa da WhatsApp kullanıcı sayısında liderliği korumaktadır.

WhatsApp'ın büyüme potansiyelini "WhatsApp Pazarlama" başlığı altında hedef kitleyle etkileşimi mümkün kılma, tüketicileri ile iletişimini kolaylaştırma ve hedef kitleyi büyütme amaçlı kullanılan WhatsApp Business uygulaması takip etmiştir. 2016 yılında ortaya çıkan uygulama, tüketiciler açısından mahremiyet ve gizlilik endişesi konusunu tekrar gündeme getirmiştir. Facebook IQ tarafından 12.500 kişi üzerinde gerçekleştirilen röportaj sonucunda katılımcıların %63'ünün bu uygulama ile işletmelerle iletişim kurulabildiğinin farkında olduğu, %56'sının bir işletmeyi arayıp iletişim kurmak yerine WhatsApp üzerinden mesaj yazmayı tercih ettiği, %61'inin işletmelerden gelen kişiselleştirilmiş mesajları takdir ettikleri ve %50'den fazlasının konum paylaşımları sonucu haritalar aracılığıyla konum geçmişine dayalı kendileriyle iletişim kuran işletmelerden alışveriş yapmaya istekli olduklarını göstermiştir (Jangid, 2019). İşletmeler açısından bu denli önemli olması yanında işletme profil bilgilerinin sunulması, otomatik ve hızlı yanıtların müşterilere sunulması açısından WhatsApp Business uygulaması anlamlı görünse de müşteriler açısından bu tür uygulamalarda erişime izin verilen bilgilerin neler olduğu, niçin kullanıldığı, kendilerine fayda sağlanıp sağlanılmadığı gibi hususlar gizlilik risk ve endişelerini ortaya çıkardığı için, müşterilerin izinlerinin alınması ve verileri üzerinde kontole sahip olduklarının belirtilmesi bu açıdan önemlidir.

4 Ocak 2021'de kullanıcı verilerini Facebook ve diğer işletmelere paylaşılacağını içeren yeni gizlilik ilkesi ve hizmet koşullarını güncelleyen

WhatsApp, Türkiye'de uygulamanın kullanılabilmesi için kullanıcıların bu güncellemeleri kabul etmesi gerektiğini, kabul edilmemesi durumunda ise 8 Şubat 2021 tarihi itibariyle uygulamanın kapanacağını belirtmiştir. AB ülkeleri için geçerli olmayan bu durum Türkiye'de büyük tepkilere yol açmış, birçok kullanıcı WhatsApp uygulamasını silmiş ve diğer mesajlaşma uygulamaları Signal ve Telegram gibi uygulamaların kullanıcı sayısı artışa geçmiştir. Yaşanan bu olay kişisel verilerin ne kadar önemli olduğunu ve kullanıcılardan zorunlu olarak izin istemenin kötü sonuçlara yol açtığının göstergesidir.

5. VERİ PAYLAŞIMLARINA DAYALI GİZLİLİK ENDİŞESİ

Dijitalleşme ve mobil teknolojiler bağlamında yaşanan gelişmeler sonucunda her gün daha fazla işletme tüketici tercihlerinin belirlenmesi, daha iyi ve yenilikçi ürün geliştirilmesi ve müşteri ilişkilerinin iyileştirilmesine katkı sağlarken tüketiciler tarafında gizlilik endişelerini artırmıştır. Tüketiciler izinleri olmadan kişisel bilgilerinin erişilebilir olmasından endişe duymaktadır. İnternet temelli dijital ve mobil teknolojilerin kullanımları sonucunda ifşa edilen bilgilerin nasıl kullanıldığı, kimlerin bu verilere ulaştığı gibi konular hakkındaki inançlar tüketici gizlilik endişelerinin kaynağıdır. Erişim ve kullanımla ilgili belirsizlik arttıkça gizlilik endişeleri daha da artmaktadır.

Yapılan araştırmalarda, tüketicilerin paylaşımlarının taşıdığı mahremiyet konusunda yüksek düzeyde endişeye sahip olmaları durumunda, işletmelerle açık iletişime ve bu ilişkinin devamlılığına daha fazla değer verme eğiliminde olduklarına (Sheehan ve Hoy, 2000), işletmelerin ise yine tüketicilerin endişelerinin yüksek düzeyde olduğu durumda iletişim ve bilgi gizliliğine daha fazla saygı duyma ve daha fazla bilgi şeffaflığı sağlama eğilimde oldukları (Hung ve Wong, 2009) sonucuna ulaşılmıştır. Tow ve arkadaşları (2008) tarafından gerçekleştirilen bir başka çalışmada ise, tüketicilerin genellikle gizlilik sorunlarının farkında olmadıkları, bu nedenle endişenin ve risk düzeyinin çok düşük düzeyde algılandığı tespit edilmiştir (Tow, vd., 2008). Bu sonuçların, paylaşılan bilgi miktarı ile

orantılı olarak değişiklik gösterdiği söylenebilir. Erişim izni isteği arttıkça, kişiselleştirilmiş mesaj gönderimi ve hedef kitle tahmini doğru yapıldıkça endişe düzeyi artacaktır.

Tüketiciler ve işletmeler arasında bilgi paylaşımının sağlanması ve kullanımına izin verilmesi arasındaki dengelemenin sağlanması zordur. Tüketicilere paylaştığı bilgiler üzerinde daha fazla kontrol alanı sunulması durumunda, izinli pazarlamanın daha uygun şartlarda gerçekleştirilebilir işletmeye duyulan güven düzeyi artırılabilecektir.

Yapılan bir çalışmada, katılımcıların üçte ikisinin kişisel verilerinin sosyal medya şirketleri tarafından nasıl kullandılığına ilişkin endişe duyduğu, büyük çoğunluğun sosyal medya hesap ve kimlik bilgilerini diğer hizmet sağlayıcılar, web siteleri ve uygulamalarla paylaşmaktan çekindikleri ve %35'inin ise ancak üçüncü taraflara güven duyması durumunda bilgilerini paylaşabilecekleri tespit edilmiştir (Valentine, 2020).

Gizlilik endişe düzeyleri dijital ve mobil teknolojilere göre farklılık gösterebilirken, sektörden sektöre, ülkeden ülkeye hatta farklı kültürler arası değişkenlik gösterebilecektir. Emami-Naeini ve arkadaşlarının (2019) yaptıkları çalışmada kullanıcıların özel ortamlardan ziyade, halka açık yerlerde toplanan verilere yönelik gizlilik endişesinin daha düşük düzeyde olduğu, benzer şekilde biyolojik verileri paylaşma konusundaki endişe düzeyin çevresel verileri paylaşım konusundaki endişe düzeyine göre daha düşük olduğu tespit edilmiştir (Emami-Naeini vd., 2019).

Tüketicilerin gizlilik endişesi duyduğu bir başka alan, kullanıcıların herhangi bir web sitesinde, mobil uygulamada, sosyal medya mecralarında ya da online alışveriş sitelerine erişim sağlarken oturum açmada "hizmet şartları" şeklinde sunulan ve içeriğinde kişisel verilerin nasıl kullanılacağını ve korunacağını ve gizlilik politikalarını içeren belge içerisindeki bilgilerdir.

Steinfeld (2016)'in gizlilik politikalarına karşı kullanıcı davranışını incelediği bir araştırmada, gizlilik politikası varsayılan olarak sunulduğunda katılımcıların oldukça dikkatli şekilde bu politikayı okuma eğilimi gösterdiği, politikayı okumadan imzalama seçeneği sunulduğunda ise katılımcıların çoğunun politikayı okumayı atladığı tespit edilmiştir.

Ayrıca, politikayı okumayı seçen katılımcıların, varsayılan şekilde kabul eden katılımcılara göre onu okumak için daha az çaba ve zaman harcadığı belirlenmiştir (Steinfeld, 2016).

Dijital ve mobil teknolojilerin kullanımı sonucu büyük risk ve gizlilik endişesi gerçeğinin ortaya çıktığı süreçte, kullanıcıların bazıları yüksek düzeyde endişe duyarken, bazıları fayda-maliyet çerçevesinde bilginin açığa çıkma riskine değdiği düşünülen faydalar karşısında belirli bir gizlilik derecesinden vazgeçebilmektedir. Krishnamurthy (2001)'in önerdiği fayda maliyet modeli bu açıdan bir temel oluşturmaktadır. Modelde, kullanıcıların kendilerine gelen mesajın ilgi düzeyi ve parasal anlamda fayda sağlaması durumunda izinli pazarlamanın olumlu karşılandığı, bilgi girişi yapılması, bilgi değiştirme ve güncelleme isteği, mesajın işlenme maliyeti gibi gizlilik maliyetlerinin ise izinli pazarlamayı olumsuz yönde etkilediği sonucuna ulaşılmıştır (Krishnamurthy, 2001). Bu model, teorik açıdan değerlendirildiğinde maliyet-fayda değiş tokuşuna dayalı gizlilik hesaplama teorisine karşılık gelmektedir (Culnan ve Armstrong, 1999; Li, 2012). Teori, insanların kişisel bilgilerini açığa çıkarma niyetlerini maliyet ve fayda temelinde değerlendirerek olumlu olanları en üst düzeye çıkarmaya, olumsuz olanları en aza indirmeye çalışarak olası sonuçları gizlilik hesabına dayandırdıklarını öne sürmektedir.

Acquisti ve Grossklags (2007) da kullanıcıların sağlayacağı ekonomik faydalara karşı, gizlilik düzeylerinden vazgeçmeye ikna edilebileceklerine vurgu yapmıştır. Çalışmada, bazı kullanıcıların ücretsiz sinema bileti ya da bir yarışmaya katılma gibi anlık ekonomik fayda ve tatmin sağlaması durumunda işletmelerin gizliliğe müdahale eden uygulamalarını kabul etmeye istekli oldukları belirtilmiştir (Acquisti ve Grossklags, 2007).

6. GİZLİLİĞİN KORUNMASINA YÖNELİK ÇÖZÜM ÖNERİLERİ VE YASAL DÜZENLEMELER

Gizliliğin korunması ve risklerina azaltılması için kullanıcıların uygulayabileceği çeşitli mekanizmalar bulunmaktadır (Hogben ve Dekker, 2010). Bu mekanizmalar riski azaltma avantajı yanında kullanılmaları

durumunda ek zaman alması, etkileşime karışıklık katması ve kullanıcıların amacına ulaşmada engel ortaya koyması gibi dezavantajlara da sahiptir (Kraus, 2017).

Sun ve arkadaşlarının (2019) yaptığı çalışmada, gizliliğin korunması yönelik teşvik mekanizmalarının sağlanması ve güvenli veri oluşturulmasına odaklanılması gerektiği belirtilmiştir. Kullanıcıların veri paylaşımına olanak sağlaması için yeterli teşvik mekanizmalarının tasarlanması gerektiği, veri talep eden işletmelerin kullanıcılarınının belli bir dereceye karşılık gelecek şekilde ödül ile ödüllendirilmeleri, toplanan verinin güvenliliğinin sağlanması, başka işletmelere veri sızdırılmaması gibi güvenli veri toplanmasına yönelik önerilerde bulunulmuştur (Sun, vd., 2019).

Gizliliğin korunmasına yönelik veri paylaşımına ve izinli pazarlamaya kontrol imkanı sağlayan mekanizmalarından bazıları reklam engelleyiciler, hedeflenmiş reklamcılık, özel tarama ve arama motorları, şifreli mesajlaşma uygulamalarıdır (Hennig, 2018). Bunların haricinde çerezleri engelleme yazılımları da gizliliğin korunmasına yönelik kullanılan bir mekanizmadır.

Çerezler, internet ortamında bağlanılan ağlar aracılığıyla kullanıcıların bıraktığı ayak izleri ve gölgeleri içeren tüm verileri kapsamaktadır. Kullanıcılar, bu tür çerezlerin kullanımına izin vermesi durumunda internet ortamında tüm çerez niteliğindeki verilerin kullanımına izin vermiş olmaktadır. Bu veriler, kişisel bilgiler, hangi sitede ne kadar kaldı, nereye baktı, nereye tıkladı vb, şeklinde tarayıcınızda saklanan tüm verileri içermektedir.

Gizliliğin korunmasına ilişkin çerez engelleme yazılımları çerezleri tanımlama, vurgulama ve kullanıcıların bunları seçici ve kapsayıcı şekilde engellemelerine olanak sağlayan ve tarayıcılara adapte edilen bir tür eklentilerdir. Ghostery yazılımı bu uygulamalara bir örnektir. Ayrıca Avrupa İnteraktif Dijital Reklamcılık İşbirliği (EDAA) www.youronlinechoices.eu web syfası aracılığıyla çerezleri engellemek için yardımcı bir program sunmaktadır (Haynes vd, 2016:877).

Gizliliği koruma mekanizmalarından bir diğeri, tarayıcınıza reklam engelleyici uzantılar eklemektir. Bunlardan en çok kullanılanı, Chrome, Firefox ve Safari gibi tarayıcılara ücretsiz yüklenebilen Adblock Plus'tır.

Hedeflenmiş reklamcılık ise sosyal medya mecralarından tarafınıza hangi reklamların yönlendirilmesi ya da yönlendirilmemesi için yaptığınız ayarları içerir. Facebook'ta bu özelliği kapatmak için ayarlar sekmesinden reklam ayarları-"Web siteleri ve uygulamaları kullanımınıza dayalı reklamlar" kısmı açık ya da kapalı bırakılabilmektedir. Arama motorları üzerinde ise yine benzer şekilde çerez kullanımı ve ayarlar bölümünden verilerin saklanmasına, kaydedilmesine izin verilip verilmeyeceği seçilebilmektedir. Arama motorları için ise Google gibi verileri daha çok işleyen araçlar yanında DuckDuckGo gibi verilerinizi işlemeyen ya da daha az işlenildiğine inanılan uygulamalar da kullanılabilmektedir. Bir diğer mekanizma ise şifreli mesajlaşma uygulamalarının kullanımıdır. WhatsApp, Signal gibi uçtan uca şifreli mesajlama uygulamalarının kullanımı, mesajların karşı tarafa ulaşana kadar hiçbir şekilde görünmeyeceğini ifade etmektedir. Burada belirtilen araçların kullanımına belki de tamamen ihtiyaç duyulmasa da kullanımlarının mantıklı olabileceği belirtilmektedir (Hennig, 2018). Her ne kadar kullanıcıların bu seçeneklere sahip olmasına rağmen yine de geri plandaki verilere dayalı olarak izinsiz şekilde paylaşımların tarafınıza yönlendirildiği de görülmektedir.

Tüketici gizliliğinin yönetiminde kullanıcılar, pazarlamacılar ve hükümetler olmak üzere 3 paydaş vardır (Gupta, 2015: 284). Kullanıcılar, gizliliğin yönetiminde veri paylaşımı ve aktarımı noktasında gizlilik politikalarını ayrıntılı değerlendirmeli, kişisel verilerin niteliğine göre kendisi için hassas sayılabilecek ve güvenliğini riske atacak bilgilerin paylaşılması konusunda gerekli önlemleri alması gereklidir. İzinli pazarlama dahilinde işletmeler iyi bir ilişki ve karşılıklı çıkar faydası temelinde paylaşılan veriler yanında, veri sızdırılması sonucu olumsuz durumlar karşısında dolandırılma gibi sonuçlarla da karşılaşılması olağan bir durumdur. İşletmeler açısından ise gizliliğin yönetilmesine ilişkin gerekli belge ve dokümanların, tüketicilerin açıkça anlayabileceği, gerekli tüm düzenleme ve açıklamaları içerecek şekilde hazırlanması ve kullanıcılara sunulması gerekmektedir. Müşterilerle güvene dayalı iyi ilişkiler geliştirmek için bu son derece önemlidir. Ayrıca işletmelerin gerek kendi ülke hükümetleri gerek uluslararası çapta faaliyet gösterilmesi durumunda karşı ülkelerin hükümetleri tarafından kabul edilen yasal

düzenlemelere uyması gerekir ve uyulmaması durumunda cezai yaptırımlarla karşılaşılabileceği unutulmamalıdır.

Yasal düzenlemeler açısından hükümet düzenlemeleri ülkeden ülkeye farklılık göstermektedir. Amerika Birleşik Devletleri'nde federal düzeyde veri gizliliği veya veri güvenliği ile ilgili güncel bir yasa yokken, Kaliforniya eyaleti 2018'de Kaliforniya tüketicileri için internet odaklı veri gizliliği ile ilgili, taraflar için yükümlülükler, bireysel haklar ve uyumsuzluk olması durumunda para cezaları ve özel eylemler içeren Kaliforniya Tüketici Gizliliği Yasası (CCPA) 'nı Ocak 2020'de yürürlüğe koymuştur (Carataş vd., 2019:246).

Avrupa'da ise 2016 yılında kişisel verilerin korunması, Avrupa Birliği'ndeki kişisel bilgilerin kötüye kullanımının önlenmesi ve bireylerin kendi kişisel verileri üzerinde daha fazla kontrole sahip olması amacıyla Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) devreye sokulmuştur (Abdulghani vd., 2019:4).

Türkiye'de ise bu tür faaliyetler 7 Nisan 2016 tarihli resmi gazetede yayınlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) çerçevesinde yürütülmektedir. " Kanun'un amacı 1. maddesinde açıklandığı üzere kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir" (KS, 2017) şeklinde belirtilmiştir. Bu kanun uyarınca Kişisel Verilerin Korunması Kurulunun çalışma usul ve esasları ve ilgili yönetmelikler ve hükümlülükler ayrıntılı olarak www.kvkk.gov.tr internet sayfasında açıklanmıştır. İlgili web sayfasında mevzuat, şikayet modülü, kurul kararları ve veri ihlali bildirimleri gibi sekmeler yer almaktadır (www.kvkk.gov.tr).

7. SONUÇ

Bilgi ve iletişim teknolojilerinin temelinde şekillenen dijital ve mobil teknolojiler işletmelerin pazarlama çabalarını tüketicilerin kişisel verileri etrafında oluşturmasını kolaylaştırmıştır. Tüketici verilerinin elde edilmesi ve işlenmesi sürecinde izinlerinin alınması, veri koruma ve güvenliğinin

sağlanması müşterilerin bu sürece gönüllü katılımını sağlayacaktır.

Teknolojik gelişmeler çerçevesinde her geçen gün veriye ulaşmanın, toplamanın, tüketici ayak izlerini takibinin kolaylaştığı dönemde, verileri izinli pazarlama ile toplamak ve anlamlandırarak pazarlama stratejilerini yürütmek gelecekte daha fazla önem kazanacaktır. Verilerin korunması ve gizliliğine dayalı güven oluşturarak yürütülen müşteri ilişkileri daha sadık, daha tatmin müşterileri meydana getirecektir. Paylaşılan bilgiler üzerinde tüketici izni olması, kontrole sahip olmaları, sürecin şeffaf yürütülmesi bu güven ortamının daha da iyi inşaa edilmesine katkı sağlayacaktır. Belki de gelecekte kişisel verilerin aktarılması ve kullanılmasına bağlı olarak pazarlama mesajlarının iletilmesi izni karşılığında tüketicilere fiyat indirimi, ödeme kolaylığı, hediye sunumları gibi teşvik mekanizmalarıyla hem mevcut hem de potansiyel müşterilerle ilişkiler bu izinler dahilinde gelişecektir. Gizlilik politikalarını ayrıntılı değerlendiren, kendi çıkarlarını fayda maliyet temelinde gözeten tüketiciler, paylaştıkları dijital ayak izleri ve gölgelerin ayarlarını değiştirerek ve düzenleyerek gizlilik endişelerini en aza indirebilecektir.

Kişisel verilerin korunmasına ilişkin gizlilik endişelerinin artmasına rağmen, izne dayalı gerçekleştirilen pazarlamanın aslında doğru yapılması, yasal düzenlemelere uyulması durumunda müşteri sadakati, memnuniyeti ve saygısı kazanılacak, marka ile uzun dönemli ilişkiler geliştirilecektir. Çok az tüketicinin kişisel verilerin toplanması, işlenmesi ve kendileriyle tanıtım faaliyetleri için iletişime geçilmesine izin verildiği düşünüldüğünde izinli pazarlamanın tüketiciler için artan önemi bir kez daha ortaya çıkmaktadır.

Potansiyel müşterilere pazarlama mesajlarının başarılı bir şekilde izne dayalı iletilmesi ile hizmet şartları başlığı altındaki gizlilik politikalarının kullanım koşullarının onayının zorunlu tutulması arasında ince bir çizgi vardır. Pazarlama iletişim çalışmaları doğru zamanda, doğru şekilde, doğru hedef kitleye ulaştırılmaması ve kişiselleştirilmiş mesajların özellikle izne dayalı olarak yürütülmemesi işletmeler için tüketicilerle ilişkiler açısından istenen sonuçları sağlamayacaktır. Ayrıca gizlilik endişeleri ve mahremiyetin korunması şüpheleriyle tüketiciler işletmenin müşterisi olmaktan çıkabilmektedir.

Küçük ya da büyük nitelikteki tüm işletmeler için tüketicilerin gizlilik endişelerini azaltmaya yönelik kullanılabilecek çeşitli stratejiler mevcuttur. Bu stratejilerle gizlilik ve mahremiyet endişeleri azaltılarak rekabet avantajı sağlanacak ve veriye dayalı pazarlama üzerinde olumlu etkiler yaratılabilecektir. İzinli pazarlama ile tüketici verilerinden yararlanan bu işletmelerin karşılıklı anlaşma şartlarını ihmal etmesi durumunda ise marka itibarı olumsuz etkilenecektir. Anlaşma şartlarına bağlı, veriye dayalı ve kullanıcı izninin alındığı pazarlama, gelecekte önemi daha fazla artacak ve pazarlamanın yönünü iletişim ve ilişkisel pazarlama temelinde yeniden değerlendirmesini gerekli kılacaktır.

İzinli pazarlamanın başarıya ulaşması, dijital ve mobil teknolojilerin satın alma öncesinde, kullanım sırasında ve kullanım sonrasında tüketici verilerinden nasıl yararlanıldığı, niçin yararlanıldığı, bunun karşılığında kullanıcı haklarının ve sunulan faydaların neler olduğunun hizmet şartları ve gizlilik koşullarında açıkça ve şeffaflıkla belirtilmesiyle mümkündür. İşletmelerin tüketicileri izin vermeye ve gizlilik endişelerini azaltmaya yönelten etmenlerin neler olduğunun farkında olması, pazarlama iletişim çalışmalarının hazırlık sürecini şekillendirecektir. Bu süreçte güvene dayalı ilişkiler inşaa edilmesi önemlidir.

İşletmeye güven duyan ve verilerin kullanımına izin veren tüketiciler oluşturmak için gizlilik endişelerinin en aza indirilmesi gerekmektedir. Bu kapsamda yapılacak akademik araştırmalarda, toplanan verilerin işlenmesinde anonim olması yerine özelleştirilme ve kişiselleştirme düzeyi, teşvik mekanizmaları sunulması durumunda davranışların nasıl değişeceği, arkadaşların ve ailenin bu sürece ve davranışlara etkisinin ne yönde şekilleneceği, paylaşılan bilgi miktarının ve kullanıcı için önem değerinin kişisel verilere izin verme davranışına etkisi, izin vermelerine ve vermemelerine neden olan faktörlerin etkisi incelenebilir.

Tüketicilerin, gizlilik endişelerine sahip olmalarına rağmen büyük çoğunluğun gizlilik politkalarını okumaması, işlemleri gerçekleştirmek için hızlıca onay vermesi, aslında bazı uygulamaların kullanımında gizlilik ayarlarında yapılabilecek değişikliklerle endişe düzeyinin azaltılabilmesi mümkündür. Tüketiciler bu tür kontrol iimkanına sahip olduğunu

bilmemektedir. Bu nedenle, yapılabilecek deneysel araştırmalarla tüketici davranışların nasıl şekilleneceği, ne yönde değişim göstereceği, işletmelerin gizlilik politikalarını müşterilerine sunması ve izin alma sürecinin tasarlanmasında önemli faydalar sağlayabileceği düşüncesiyle buna yönelik çalışmalar da yürütülebilir.

İşletmeler açısından günümüzde izne dayalı pazarlamanın tüketici güveni temelinde ve gizlilik endişelerinin en az düzeyde olmasına bağlı şekillendiği unutulmamalıdır. Yapılan pazarlama iletişim çalışmalarının hedef gruplara iletilmesi verilerin korunmasına ve yasal düzenlemelere bağlı olarak gerçekleştirilmeli, mesajların tüketicileri sıkmamasına, gönderim zamanlamasına, sıklığına ve süreç boyunca şeffaf olunmaya dikkat edilmelidir.

KAYNAKÇA

Abbas, R., Michael, K., & Michael, M. G. (2014). The regulatory considerations and ethical dilemmas of location–based services: A literature review. Information Technology & People, 27(1), 2–20.

Abdulghani, H.A.., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A Study on Security and Privacy Guidelines, Countermeasures, Threats: IoT Data at Rest Perspective. Symmetry, 11. 1-36.

Acquisti, A., & Grossklags., J. (2007). What Can Behavioral Economics Teach Us About Privacy?, In Digital Privacy: Theory, Technologies and Practices, ed. A. Acquisti et al. Boca Raton, FL: Auerbach Publications. 363-377

Aguirre, E., Mahr, D., Grewal, D., Ruyter, K. D., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. Journal of Retailing, 91(1), 34–59.

Bartholomew, D. (2015). Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201. John Deere Company. Available in http://copyright.gov/ %0A1201/2015/comments-032715/class21/John_Deere_Class21_1201_2014.pdf(10.10.2021)

Carataş, M. A., Spătariu, E.C., & Gheorghiu, G. (2019). Privacy and Cybersecurity Insights, "Ovidius" University Annals, Economic Sciences Series, 19(2). 242-246.

Culnan, M.J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, Organization Science 10 (1), 104–115

Emami-Naeini, P., Dixon, H., Agarwal, Y., Cranor, L.F, (2019). Exploring how privacy and security factor into IoT device purchase behavior. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems-CHI '19 [Internet], Glasgow, Scotland UK. ACM Press, 1–12

Enck, W., Gilbert, P., Chun, B.G., Cox, L.P., Jung, J., McDaniel, P., & Sheth, A.N., (2010). TaintDroid: an Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones. In: Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation, OSDI'10. Berkeley, USA, 393–407.

Glazer, R. (1991). Marketing in an information-intensive environment: Strategic implications of knowledge as an asset. Journal of Marketing, 55(4) 1–20

Goldfarb, A., & Tucker, C. (2019). Digital Marketing. Elsevier, 259–290

Godin, S. (1999), Permission Marketing: Turning Strangers into Friends, and Friends into Customers, Simon and Schuster, USA.

Groopman, J. (2015), Consumer Perceptions of Privacy in the Internet of Things: What Brands Can Learn from a Concerned Citizenry, Available in https://www.prophet.com/thinking/2015/06/new-reportconsumer-perceptions-of-privacy-in-the-internet-of-things/ (09.10.2021).

Gupta, N. (2015). Permission marketing: antecedents, impact and future, International Journal of Teaching and Case Studies, 6(4), 281-289.

Harborth, D., & Page, S. (2021). Investigating privacy concerns related to mobile augmented reality Apps–A vignette based online experiment, Computers in Human Behavior. 122. 1-17.

Hayes, D., Snow, C., & Altuwayjiri, S. (2018). A dynamic and static analysis of the uber mobile application from a privacy perspective. International Journal of Applied Information Systems, 11, 11–22.

Hayes, D., Cappa, F., & Le-Khac, N. A. (2020). An effective approach to mobile device management: Security and privacy issues associated with mobile applications, Digital Business. 1. 1-8.

Haynes, D., Bawden, D., & Robinson, L. (2016). A regulatory model for personal data on social networking services in the UK. International Journal of Information Management, 36, 872-882.

Hennig, L. (2018). Privacy and Security Online: Best Practices for Cybersecurity, Library Technology Reports, 54(3).

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. Communications of the ACM, 42(4), 80–85.

Hogben, G., & Dekker, M. (2010). Smartphones: Information security risks, opportunities and recommendations for users. In: European Network and Information Security Agency.

Holmes, T.E. (2000), Web sites may ask permission, but your boss doesn't have to. USA Today, 7 August, 3.

Huffington Post. (2009). Google CEO On Privacy (VIDEO): 'If You Have Something You Don't Want Anyone To Know, Maybe You Shouldn't Be Doing It.' Huffington Post. Available in http://www.huffingtonpost.com/ 2009/12/07/google-ceo-on-privacy-if_n_383105.html (18.09.2021).

Hung, H., & Wong, Y. H. (2009). Information transparency and digital privacy protection: Are they mutually exclusive in the provision of e-services? Journal of Services Marketing, 23(2–3), 154–163.

Jangid, S. (2019). Ultimate Creative Ideas For Marketing Through WhatsA Tip to Toe, Available in https://www.softwaresuggest.com/blog/creative-ideas-for-marketing-through-whatsapp/ (10.10.2021).

Knoll, J. (2016). Advertising in social media: A review of empirical evidence. International Journal of Advertising, 35(2), 266–300.

Kohn, V., & Harborth, D. (2018). Augmented reality – a game changing technology for manufacturing processes? Twenty-Sixth European Conference on Information Systems, 1–19. ECIS2018.

Kraus, L. (2017). User experience with mobile security and privacy mechanisms, Technischen Universität Berlin, PhD Dissertation.

Krishnamurthy, S. (2000), Spam Revisited. Quarterly Journal of Electronic Commerce, 1(4), 305-321.

Krishnamurthy, S. (2001), A Comprehensive Analysis of Permission Marketing, Journal of Computer Mediated Communication, 6(2).

KS, (2017). Türkiye'de Kişisel Verilerin Korunması Kanunu, KS, Küçükkaya ve Sağlı Avukatlık Ortaklığı, http://www.ksavukatlik.com/wp-content/uploads/2017/10/kisisel-verilerin-korunmasi-KS-V10.pdf.

Liu, D., Gao, X., & Wang, H. (2017). Location privacy breach: Apps are watching you in background. 2017 IEEE 37th international conference on distributed computing systems (ICDCS). 2423–2429.

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. Journal of Business Research, 82, 103– 116.

Menard, P., & Bott, G.J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment,Computers & Security. 95.1-14.

Misra, J.M. (2016). Such, How socially aware are social media privacy controls? Computer 49(3).96–99.

Monk, A., Carroll, J., Parker, S., & Blythe, M.(2004).Why are mobile phones annoying? Behaviour and Information Technology, 23(1), 33–41.

Muk, A. (2007). Consumers' intentions to opt in to SMS advertising'. International Journal of Advertising, 26(2), 177–198.

Nill, A., & Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. Journal of Current Issues and Research in Advertising, 35, 126–146.

Peppet, S.R., (2014). Regulating the Internet of Things: first steps toward managing discrimination, privacy, security, and consent. Texas Law Review. 93, 85

Persaud, A., & Azhar, I. (2012). Innovative mobile marketing via smartphones: are consumers ready? Marketing Intelligence and Planning, 30(4), 418–443.

Pfohl, J. (2020). The Scary Truth About the Facebook Messenger App and Your Privacy, Crambler, October.

Shave, L. (2016). Privacy And Security İn Our Complex Digital World, IQ, Privacy & Security. May. 20-24.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. Journal of Public Policy & Marketing, 19(1), 62–73

Snow, C., Hayes, D., & Dwyner, C. (2016). Leakage of geolocation data by mobile ad networks. Journal of Information Security and Applications and Research, 9, 24–33.

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment, Computers in Human Behavior. 55. 992-1000.

Sun, G., Sun, S., Sun, J., Yu, H., Du, X., & Guizani, M. (2019). Security and privacy preservation in fog-based crowd sensing on the internet of vehicles, Journal of Network and Computer Applications, 134, 89-99.

Tow, W., Dell, P., Venable, J. (2008). Understanding information disclosure behaviour in Australian Facebook users. Journal of Information Technology. 25(2),126–36.

Tucker, C. E. (2014), Social Networks, Personalized Advertising, and Privacy Controls, Journal of Marketing Research, 51, 5, 546–62

Twardowski, B., & Ryzko, D., (2015). IoT and context-aware mobile recommendations using Multi-Agent Systems. In: 2015 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), 1. 33–40.

Valentine, O. (2020). Data Privacy on Social Media and Why It Matters, Thought Leadership, WeAreSocial. (31 March).

Warkentin, M., Goel, S., & Menard, P, (2017), Shared Benefits and Information Privacy: what Determines Smart Meter Technology Adoption? Journal of Associations Information Systems. 18 (11), 758–786.

Windham, L., & Orton, K.(2002). The soul of the new consumer: The attitudes, behavior, and preferences of e-customers (2nd ed.). New York: Allworth Press.

Zang, J., Dummit K., Graves, J., Lisker, P., Sweeney, L., (2015). Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps, technology science; Available in http://techscience.org/a/2015103001/ (08.10.2021)

Zarandi, M. A., Dara, R. A., & Fraser, E. (2020). A survey of machine learning-based solutions to protect privacy in the Internet of Things, Computers & Security. 96. 1-9.

View publication stats