ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMANIN TÜKETİCİ DAVRANIŞLARI ÜZERİNDEKİ ETKİLERİ
ve
KİŞİSEL VERİLERLE İLİŞKİSİ

Ali Burak ENSARİ
111692005

İSTANBUL BİLGİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

Danışman: Yrd. Doç. Dr. Leyla KESER BERBER

2014

ÇEVRİMİÇİ DAVRANIŞSAL PAZARLAMANIN TÜKETİCİ DAVRANIŞLARI ÜZERİNDEKİ ETKİLERİ
ve
KİŞİSEL VERİLERLE İLİŞKİSİ

THE EFFECTS OF ONLINE BEHAVIORAL ADVERTISING ON CONSUMER BEHAVIOUR AND ITS RELATIONSHIP TO DATA PRIVACY

Ali Burak ENSARİ
111692005

Yrd. Doç. Dr. Leyla KESER BERBER :

Yrd. Doç. Dr. Nilgün BAŞALP :

Yrd Doç Dr. R. Bülent ÖZEL :

Tezin Onaylandığı Tarih :

Toplam Sayfa Sayısı : 153

Anahtar kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Çevrimiçi Davranışsal Pazarlama	1) Online Behavioral Advertising
2) E-Mahremiyet	2) e-privacy
3) Kişisel veriler	3) Personal Data
4) Davranışsal Hedefleme	4) Behavioral Targetting
5) Derin Veri Analiz	5) Deep Packet Inspection
6) Çevrimiçi Profilleme	6) Online Profiling
7) Önceden İzin Alma	7) Opt in

Özet

Küresel rekabet kuruluşları, müşterilerine daha iyi hizmet sunabilmek için onları daha yakından tanımak, istek ve beklentilerini anlamak üzere satın alma tercihlerine yön veren davranışlarını ayrıntılı bir biçimde izlemeye yönlendirmiştir. Bu çerçevede ürün ve hizmetlerin tasarımı, üretimi, müşterilere sunulması ve satış sonrası hizmetlerin verilmesi sürekli bir gelişim göstermiştir.

Mevcut ve hedef müşteri kitlelerinin gelecekteki beklentilerini daha hızlı ve önce fark edebilenler rekabet güçlerini arttırmış; müşterilerine gelecek beklentilerini karşılayabilecek değeri sunabilmeyi sürdürebilenler lider konumlarını koruyabilmişlerdir.

Müşteri gelecek beklentilerinin sağlıklı tahmin edilmesi, müşterilerin daha iyi, daha yakından tanınması ile mümkündür. Pazarlama kavramı ve uygulamalarının ortaya çıkışı ile bu konu üzerinde daha fazla çalışılan bir alan olmuştur. Özellikle bilgi teknolojilerinin gelişimi ile tüketici davranışlarının izlenerek, satın alma kararlarını oluşturan kişisel davranış biçimlerinin değerlendirilebilmesi mümkün olmuştur. Böylece ürün ve hizmetlerin, internet ortamında, müşterilerin belirlenmiş profillerine göre özel olarak sunumu ve satışı küresel ölçekte yaygınlaşmıştır.

Bunun faydası hem ürün ve hizmeti sunanlar hem de onu almayı planlayan tüketiciler için verimlilik artışı ve etkililik getirmesidir. Ancak diğer taraftan bu uygulamalar tüketicilerin bireysel mahremiyetlerinin ihlali riskini de gündeme getirmiştir.

Bu riskin minimize edilebilmesi başta ABD ve AB olmak üzere çeşitli yasalar, yönetmelikler ve özdenetim amaçlı sözleşme benzeri araçların gündeme getirilmesi, uygulanması ve bu uygulamalardan dersler çıkartılarak sürecin iyileştirmesi ile sağlanmaya çalışılmaktadır. Bu konudaki önleyici yasal ve özdenetim alt yapısı ülkemizde ABD ve AB'ye göre oldukça iyileştirmeye açık bir alandır.

Abstract

Global competition have led organizations to track the behaviours of their customers closer and in detail to understand them better, to discover their needs and expectations that affect their purchasing preferences. In this context the design, production, marketing, promotion and after sales management of products and services have been developing since then.

The ones who is able to estimate the future expectations of the current and potential customers earlier and faster were able to strenthen their competitive advantages; and the ones who were able to sustain to offer the values that meet the future expectations of their customers have continued to protect their leadership position.

The future expectations of the customers can be estimated better if we can know more about them. This has become an area where product and service providers paid more attention as marketing concepts, principles and implementation came into the scene. The tracking the behaviors of the consumers enabled the assessment of the individual behavioral styles that purchasing decisions of the individuals are based upon. This has lead worldwide to a tailored proposal of the products and services in the internet environment to each customer in accordance with their tracked-profiles worldwide

The benefit created out this process is the increase in effectivity and efficiency both for the provider and the customer as well. Though on the other hand such implementations bring up the risk of infringement of privacy of consumers.

To minimize such a risk, various tools like legislations, regulations and self-assessment frameworks have been proposed, passed and entered into force by relative parliaments and other relative institutions in USA and EU; and have been being improved further upon feedbacks from the stakeholders. In this respect, legislative framework in Turkey is an area for improvement regarding the existance of comprehensive preventive regulations, frameworks and self-assessment substructures

İÇİNDEKİLER

KISALTMALAR

AB:	Avrupa Birliği
ABD:	Amerika Birleşik Devletleri
ABTHB:	Avrupa Birliği Temel Haklar Bildirgesi
ABTHB:	Avrupa Birliği Temel Haklar Bildirgesi
AEA:	Avrupa Ekonomik Alanı
AİHS:	Avrupa İnsan Hakları Sözleşmesi
AİHS:	Avrupa İnsan Hakları Sözleşmesi
AOL:	America Online
APT:	Online Advertising Platform

BT:	Behavioral Targeting (Davranışsal Hedefleme)
BUS:	Business Applications) (İş Uygulamaları)
CMK:	Ceza Muhakemesi Kanunu
CRISP-DM:	Cross Industry Standard Process for Data Mining
CSS:	Cascading Style Sheets (Basmaklı Biçim Şablonları)
DAA:	Digital Advertising Alliance (Dijital Reklamcılık Birliği)
DNT:	Do Not Track (İzleme)
DPA:	Data Protection Act (Veri Koruma Kanunu)
DPI:	Deep Packet Inspection (Derin Veri Analizi, Derin Paket Analizi)
EFF:	Electronic Frontier Foundation (Elektronik Cephe Vakfı)
ENISA:	European Network and Information Security Agency, Avrupa Birliği Ağ Güvenliği Ajansı
FCC:	Federal Communication Commission (Federal İletişim Komis.)
FPC:	First Party Cookies (Birinci taraf çerez)
FTC:	Federal Trade Commission (Federal Ticaret Komisyonu)
GPS:	Global Positioning System, Küresel Konumlama Sistemi
Http:	Hyper Text Transfer Protocol (Hiper Metin Transfer Protokol.)
IAB Europe:	Interactive Advertising Bureau, Europe (İnteraktif reklamcılık Bürosu, Avrupa)
ICO:	Information Commissioner's Office
ID:	Kimlik (Identification)
IDS:	Intrusion Detection System (Saldırı sezme Sistemi)
IMP:	Interception Modernization Programme
IND:	Indefinite (Belirsiz Süre)
IP:	Internet Protocol Adress (İnternet Protokol Adresi)
ISP:	Internet Service Provider (İnternet Servis Sağlayıcı)
İSS:	Internet Servis Sağlayıcısı
KLM:	Royal Dutch Airlines
LSO:	Local Shared Objects (Yerel Paylaşılmış Objeler)
OBA:	Online Behavioral Advertising (Çevrimiçi Davranışsal Pazarlama)
OPT-IN:	Opted in for receiving (önceden izin alınması)
OPT-OUT:	Opted out for not receiving (reddetme hakkı - iletilmek istenen ürün-hizmet bilgilerini almak istememek; dışarıda kalmayı tercih)
P3P:	Privacy Protection Project (Gizlilik Tercihleri Protokolü)
PET:	Privacy Enchancing Technologies (Mahremiyeti Güçlendirici Tek.)
TBK:	Türk Borçlar Kanunu
TC:	Türkiye Cumhuriyeti
TCBMM:	Türkiye Cumhuriyeti Büyük Millet Meclisi
TCK:	Türk Ceza Kanunu
TPC:	Third Party Cookies (Üçüncü taraf çerez)
URI:	Uniform Resource Identifier
URL:	Uniform Resource Locator (Tek biçimli kaynak konumlayıcı – internetteki resmi adres sistemi)
W3C:	World Wide Web Consortium (İnternet Sunucuları Ağı Birliği)
XSS:	Cross Site Scripting

KAYNAKÇA

Adoko — *Webbugs,* Adoco.com, Online Security Information Resource http://www.adoko.com/webbugs.html (erişim tarihi 23.05.11)

Anand/Grobelnik ve diğ. — Sarap Anand/Marko Grobelnik/Dietrich Wettscherek, *Cross-Industry Standard Process for Data Mining*, Tutorial presented on 23 September 2003, http://staff.science.uva.nl/ ~netten/lerenenbeslissen/extra/ kd standardsfinal%5B1%5D.ppt erişim 05.05.2011

Ahmand/Aljumah	Yasir Ahmand/Abdullah Aljumah, *Paradigm Shift in the Security-n-Privacy Implementation of Semi Distributed Online Social Networking*, Computer and Information Science Volume 6 No:1, 2013, Salman Bin Abdulaziz University Saudi Arabia
AİH Sözleşmesi	*Avrupa İnsan Hakları Sözleşmesi* (14. Protokol dahil)(2013 tarihli 15 ve 16. Protokoller henüz yürürülüğe girmedi), Adalet Bakanlığı, Ankara, http://www.inhak.adalet.gov.tr/temel/aihs.pdf, erişim 24 Ocak 2013
Ajdari/Hofnagle	Donnya Ajdari/Chriss Hofnagle ve diğerleri, *Web Privacy Tools and Their Effects on Tracking and User Experience on the Internet*, Team for Resarch in Ubiquitous Secure Technology, National Science Foundation, California, 2013
Akgöbek/Çakır	Ömer Akgöbek/Fuat Çakır, *Veri Madenciliğinde Bir Uzman Sistem Tasarımı*, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri**,** Harran Üniversitesi, Şanlıurfa, 2009
Alabay	Nurettin Alabay, *Geleneksel Pazarlamadan Yeni Pazarlama Yaklaşımlarına Geçiş Süreci,* Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2010. C.15, Isparta, 2010
Arias	Martha L. Arias *INTERNET LAW - Behavioral Advertising in the United States*, http://www.ftc.gov/opa/2009/02/behavad.shtm erişim 26.04.2013
Arrington	Samantha C. Arrington *Got Cookies*, JICLT Journal of International Commercial Law and Technology, Vol. 8, No.1,, January 2013, USA, 2013
Baird	Eleanor Commont Baird *Targeted Online Advertising: Persuasion in an Era of Massless Communication*, MBA Thesis, MIT Sloan School of Management, Massachusetts June 2008
Barkuus/Dey	Louise Barkuus/Anind Dey, *Location Based Services for Mobile Telephony: A Study of User's Privacy Concerns*, Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction, Tokyo, July 2003
Bloux/Desfougeres	Valentin Bloux, Desfougeres, Jean-Marc Desfougeres, *Behavioral Advertising on Facebook: the users perspective regarding leisure industry,* Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in marketing, Halmstad, 2nd June 2011
BTK Duyuru,	*http://www.tk.gov.tr/duyurular/duyuru.php?ID=3749* erişim 23 Ağustos 2014
BTK 2012 DK-14/623	http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf erişim 23 Ağustos 2014
BTK 2012 DK/641	http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2012%20DK-14-641.pdf erişim 23 Ağustos 2014
BTK 2013 DK-SDD/228	http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf erişim 23 Ağustos 2014
Butler/Teddy/Waugh	Eric Butler/John Teddy/Martin Waugh, *First Party Cookie for Tracking Web Traffic*, United States Patent Application Publication, Pub. No.: US 2006/0265495 A1, Nov,23,2006
Bygrave	Lee. A. Bygrave, *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law and Security Reporter, vol.17, s.17-24, London, 2001 *http*://folk.uio.no/lee/oldpage/articles/ Minding_machine.pdf erişim tarihi 03 Şubat 2014

Carus/Altan	Aydın Carus/Mesut Altan, *Web Kullanım Madenciliği Uygulaması*, II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul, 17-19 Kasım 2005
Castelluccia/Narayanan	Claude Castelluccia/Arvind Narayanan *Privacy Considerations of Online Behavioural Tracking*, Report by ENISA European Network and Information Security Agency, 19 October 2012
Chaabane/Kaafar/Boreli	Abdelberi Chaabane/Mohamed Ali Kaafar/Roksana Boreli, *Big Friend is Watching You: Analizing Online Social Networks Tracking Capabilities, Computer and SocietyPublic Policy Issues-Privacy* WOSN (Workshop on Online Social Networks), Helsinki, 17 Ağustos 2012
Clauß/Kesdogan/Kölsch	Sebastian Clauß/Dogan Kesdogan/Tobias Kölsch, *Privacy Enhancing Identity Management: Protection Agaist Re-Identification and Profiling*, Technische Universitat Dresden, Fakultat Informatik, Dresden, November 11, 2005
Cox/Cline	Jeffrey T. Cox/Kelly M. Cline, *Parcing the Demographics: The Challenge of Balancing Online Behavioral Advertising and Privacy Considerations*, Journal of Internet Law, March 2012
Debussere	Frederic Debussere, *The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster*, International Journal of Law and Information Technology Vol. 13 No.1, 2005
De Lima/Legge	Desiree De Lima/Adam Legge, *The European Union's Approach to Online Behavioral Advertising: Protecting Individuals or Restricting Business*, Computer Law and Security Review No.30, s.67, 2014, www.compseconline.com/publications/prodclaw.htm www. Sciencedirect.com erişim 05.03.2014
Dwywr	Catherine Dwyer, *Behavioral Targetting: A Case Study of Consumer Tracking on Levis.com*, s.8, Proceedings of the Fifteenth Conference on Information Systems, San Francisco, California, August 2009 http://csis.pace.edu/~dwyer/research/AMCIS Dwyer2009.pdf erişim 15.05.2011
Eckersley	Peter Eckersley, *How Unique is Your Web Browser,* Electronic Frontier Foundation, https://panopticlick.eff.org/ (erişim tarihi 23.08.2011)
Eijk ve diğ.	N. van Eijk/N. Kool Helberger/A. L. van der Plas/B. van der Sloot, *Online Tracking: questioning the power of informed consent* Emeral Group Publishing Limited, Vol.14 No.5, Bingley, Bradford, 2012
Eren	Kenan Eren, *İnternet Tüketicisinini Satun Alma Davranışlarının İncelenmesi Üzerine Bir Araştırma*, Çukurova Üniversitesi, Yayınlanmamış Y. L. tezi, Adana, 2009
e-Tic DIR: 2000/31/AT	*e-Ticaret Direktifi 2000/31/AT,* Topluluk Resmi Gazetesi No: L 178, 17.07.2000 s. 0001-0016, e-Ticaret Merkezi.net http://www.e-ticaretmerkezi.net/abdirektif.php, erişim tarihi 28.02.2014)
EU, Amend to 2002/58/EC	2009/136/EC, http://eurlex.europa.eu/LexUriServ/LexUri Serv.do?uri= OJ:L:2009:337:0011:0036:en:PDF, 2009, Erişim 28 Ocak 2014
EU, Charter Fund. Rights	*Charter of Fundamental Rights of the European Union* (26.10.2012 tarihli belge), Official Journal of the European Communities, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 12012P/ TXT: EN:NOT erişim 24 Ocak 3013
EU, Data Protection Dir.	Data Protection Directive, 95/46/EC, Official Journal of European Communities, http://ec.europa.eu/justice/ policies/privacy/ docs/95-46-ce/ dir 995-46_part1_en.pdf , erişim 24 Ocak 2014
EU, e-Privacy Dir.	*e-Privacy Directive 2002/58/EC, ve 2006/24/EC, 2009/24/EC değişiklikleri*, http://eurlex.europa.eu/ LexUriServ/LexUriServ.do? uri= CONSLEG:2002 L0058:20091219:EN:PDF, **2009** Erişim 26 Ocak 2014

EU/LIBE, Data Protection	*General Data Protection Regulation*, Inofficial Consolidated Version After LIBE Committee Vote Provided by the Rapporteur, 22 October 2013, http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf erişim 05 Mart 2014
Evans	David S. Evans *The Online Advertising Industry: Economics, Evolution and Privacy* Journal of Economic Perspectives, Vol. 23, No.3, Summer 2009
Facebook	http://developers.facebook.com/blog/post/108/ (erişim tarihi 28.05.2011)
FTC, Reg. OBA FTC	*Regulation of Behavioral Advertising*, Wikipedia, http://en.wikipedia.org/wiki/FTC_regulation_of_behavioral_advertising erişim 15 Ekim 2012
FTC Report 2012	Final Report, *Protecting Consumer Privacy in an Era of Rapid Change, Reccomendations for Business and Policymakers*, FTC Report, s. i-iii, March 2012, http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy , erişim 4 Ocak 2014
FTC Staff Report	FTC Staff Report, *Protecting Consumer Privacy Era of Rapid Change,* Federal Trade Commision, December 2010,
Goldfarb/Tucker	Avi Goldfarb, Tucker, Catherine E. Tucker *Online Advertising, Behavioral Targeting and Privacy* (Viewpoints, vol. 54, no. 5, Communications of the ACM May 2011)
Grutese/Liu	Marco Grutese, Liu, Xuan Liu, *Protecting Privacy in Continious Location Tracking Applications*, IEEE Computer Society, Vol. 2 No. 2, March-April 2004
IAB Europe	IAB Europe, *EU Framework for Online Behavioural Advertising*, April 2011,
IAB/Revenue Report	IAB Interactive Advertising Bureau, *Internet Advertising Revenue Report 2012*, http://www.iab.net/media/file/IAB_Internet Advertising_Revenue_Report_FY_2012.pdf (IAB & PWC April 2013) erişim 05.03.2014
IAB, Turkey	http://www.iabturkiye.org/icerik/iab-turkiye, erişim, 01.03.2014
İyiler	Zeynep İyiler, *Elektronik Ticaret ve Pazarlama, İhracatta İnternet Zamanı:1*, T.C. DTM İhracatı Geliştirme Etüd Merkezi, Ankara, Aralık 2009
Kang/Washington Post	Cecilia Kang, *Senators introduce Internet privacy bill,* Washington Post, 04.12.2011, http://www.washingtonpost.com/blogs/post-tech/post/senators-introduce-internet-privacy-bill/2011/04/1/AFL0CjRD blog.html, erişim 13.02.2014
Kaya/Köymen	Halil Kaya/Kemal Köymen *Veri Madenciliği Kavramı ve Uygulama Alanları,* Fırat Üniversitesi Doğu Anadolu Bölgesi Araştırma ve Uygulama Merkezi Cilt 6- Sayı 2; Şubat 2008, s.159
Keser Berber/Rapor	*Leyla Keser Berber, Çevrimiçi Davranışsal Reklamcılık Uygulamaları Özelinde Kişisel Verilerin Korunması*, İnternet Geliştirme Kurulu, Raporu, 16 Ocak 2013, www.internetgelistirmekurulu.org/tr/Rapor_Dosya. aspx?D =MjR... , Erişim 3 Şubat 2013
Kırlıdoğ/Fidaner	Melih Kırlıdoğ/Işık Barış Fidaner, *Derin Veri Analizi: İnternetteki Temel Gözetim Aracı*, XIV. Akademik Bilişim Konferansı, Uşak, 1-3 Şubat 2012
Killkelly, AİHM Md.8Klvz.	Ursula Kilkelly, *Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı, AİHS 8. Maddenin Uygulanmasına İlişkin Kılavuz*, İnsan Hakları Genel Müdürlüğü, Avrupa Konseyi, Cedex http://www.ihop.org.tr /index.php?option= com_content&task= view&id =34&Itemid=64, erişim tarihi 24 Ocak 2013

Malin ve diğ, RE-IDENTİF.	Bradley Malin/Latanya Sweeney/Elaine Newton, *Trail Re-Identification: Learning Who You Are From Where You Have Been*, LIDAP-WP2 Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, March 2003
Malin UNLINKABILITY	Bradley Malin, *Trail Re-Identification and Unlinkability in Distributed Databases*, Carnegie Mellon University, Institute for Software Research, International School of Computer Science, PhD Thesis, Pittsburgh, May 2006
Martinez	Juan Martinez, Facebook: The Black Sheep of Online Behavioral Advertising, Customer Relationship Management, Destination CRM.com, January 2011 http://www.destinationcrm.com/Articles/Editorial/Magazine-Features/Facebook-The-Black-Sheep-of-Online-Behavioral-Advertising72863.aspx, erişim 23.05.2012
Mayer/Mitchell	Jonathan R. Mayer/Mitchell, John C. Mitchell *Third-Party Web Tracking: Policy and Technology*, IEEE Symposium on Security and Privacy, San Francisco, May 20-23 2012
Mevzuat/Bilgi Edinme	*4982 sayılı Bilgi Edinme Hakkı kanunu* http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf, erişim 22.02.2014
Mevzuat/Borçlar K.	Borçlar Kanunu (güncel), tp://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098.pdf erişim 16.02.2014
Mevzuat/CMK 75-79	*5271 sayılı Ceza Muhakemesi Kanunu* (güncel), Md. 75, 76, 78, 79 www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm,, erişim 17.02.2014
Mevzuat/CMK 135	*5271 sayılı Ceza Muhakemesi Kanunu* (güncel), Md. 135, www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm,, erişim 17.02.2014
Mevzuat/İş K.	8423 Sayılı İş Kanunu (güncel), Md. 75, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4857.pdf, erişim 17.02.2014
Mevzuat/ Kişisel Bilgi	*Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik*, Md.1, 2, 3, 6, 7, 8, http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf, erişim 17.02.2014
Mevzuat/ POLİS VZF. K.	*2559 Sayılı Polis Vazife ve Salahiyetleri Kanunu*, www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.doc erişim 22.02.2014
Mevzuat/TCK	Türk Ceza Kanunu (güncel), http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, erişim 16.02.2014
Mevzuat/TCK GRKÇ 135-6	*Türk Ceza Knununu Gerekçe* www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, erişim 16.02.2014
Mevzuat/TCK GRKÇ 138	*Türk Ceza Kanunu Md. 138 Gerekçe,* www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc ,erişim 16.02.2014
Mevzuat/T. Medeni K.	Türk Medeni Kanunu (güncel) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4721.pdf Türk Medeni Kanunu (güncel), erişim 16.02.2014
Net Age	*The Online Decision Making Process*, Net Age, http://www.netage.co.za/articles/resources/all/74 erişim 05.02.2014
Nolet	Mike Nolet, *What's Really in my Cookie Cache,* Mike on Ads, February 27th, 2007, Mike on Ads, http:/ www.mikeonads.com/2007/02/27/whats-really-in-my-cookie-cache/ (erişim tarihi 19.05.11)
O'Donoghue/Brimsted,	Cynthia O'Donoghue/Kate Brimsted, *Breakthrough Vote by European Parliament Sets Delayed Data Protection Overhaul Back on Track*, Global Regulatory Enforcement Law Blog, posted on October 22, 2013 by Christine Nielsen Czuprynski, http://www.globalregulatoryenforcementlawblog.com/2013/10/articles/data-security/breakthrough-vote-by-european-parliament-sets-delayed-data-protection-overhaul-back-on-track/ erişim tarihi **05.03.2014**

Office of Fair Trading — *Online Targeting of Advertising Prices*, A market study, Office of Fair Trading,, http://www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf. London, May. 2010

Oğuzlar Ayşe Oğuzlar, — *Veri Ön İşleme,* Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 21, Kayseri, Temmuz-Aralık 2003

Orzan/Platon — Gheorghe Orzan, Platon, Otilia-Elena Platon *Consumer Opinions Towards Online Marketing Communication and Advertising on Social Networks*, Lex et Scientia. Economics Series LESIJ NO. XIX, VOL. 2/2012

Özmen, Müjdat — Müjdat Özmen, *Müşteri Değeri Üzerine Bir Örnek Olay Uygulaması*, Eskişehir Osmangazi Üniversitesi, Yayınlanmamış Doktora Tezi, Eskişehir, Haziran 2008

Özmen, Şule — Şule Özmen, *İş Hayatı Veri Madenciligi ıle İstatistik Uygulamalarını Yeniden Keşfediyor,* http://www.suleozmen.com/teblig_sunumlar/3is_hayati_veri_madenciligi_istatistik.pdf , erişim tarihi 9.05.2013

Pastor/Saldana — Esther Martinez Pastor, Saldana, Mercedes Munoz Saldana, *In Search of Balance Between Regulation and Self-regulation of Online Behavioral Advertising*, Estudios sobre el Mensaje Periodistico Vol.19 Special Edition, Universidad Complutense, Madrid, 2013

PwC/IAB France/SRI — PwC, *Measuring the Effectiveness of Online Advertising*, Study conducted by PwC for IAB France and SRI (Syndicat des Regies Internet), https://www.pwc.com/en_GX /gx/entertainment-media/pdf/IAB_SRI_Online_Advertising_Effectiveness_v3.pdf, erişim 05.03.2014

RG/Intern. Ortam. Yayın. — *İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, Md 3, Md. 8*, Resmi Gazete Sayı: 26716 Tarih: 30.11.2007, http://www.resmigazete.gov.tr/eskiler/2007 11/20071130-6.htm 13.10.2013

Schreurs ve diğ, — Wim Schreurs, Mireille Hildebrandt, Els Kindt, Michael Vanfleteren, "Cogitas, Ergo Sum: The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector", Mireille Hildebrandt ve Serge Gutwirth (eds), *Profiling the European Citizen*, s.241-270, Springer Link, http://link.springer.com/book /10.1007 /978-1-4020-6914-7 , 2008

SEJ; Alton — Larry Alton (posted by), *The Basics of Online Marketing in 2013*, Search Engine Journal, 24 September 2013, http://www.searchenginejournal.com/the-basics-of-online-marketing-strategy-in-2013/66623/, erişim 05.03.2014

Smith-Grieco — Anthony N. Smith-Grieco *The İnternet as Recommendation Engine: Implicationns of Online Behavioral Targeting*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010

Sottiaux — Stefan Sottiaux, Stefan, *Terrorism and the Limitation of Rights*, Law and Politics Book Review, Vol. 18 No. 7 (July, 2008) pp.673-*676* http://www.lawcourts.org/LPBR/ review s/sottiaux0708.htm , erişim 24 Ocak 2014

Speier — Jackie Speirer, *Consumer Protection and Personal Privacy* , Washington D. C., 2014 http://speier.house.gov/index. php ?option =com_content&view=article&id=203&Itemid=46 erişim 13.02.2014

Stallworth — Brian Stallworth, *Future Imperfect: Googling for Principles in Online Behavioral Advertising*, Federal Communications Lae Journal; Mar 2010; 62,2; ABI/INFORM Complete

Steindel — Tracy A. Steindel *A Path Toward User Control of Online Profiling 6/7/2011,* Michigan Telecommunications and Technology Law Review.459, Michigan, 2011 http://www.mttlr.org/volseventeen/steindel.pdf erişim_05.03.2014

Suuberg	Alessandra Suuberg, *The View from the Crossroads: The European Union's New Data Rules and the Future of U.S. Privacy Law*, Tullane Journal of Technical & Intellectual Property, Vol. 16, 2013
Talaga	Paul Talaga, *Exploiting Data Locality in Dynamic Web Applications*, Syracuse University, Electrical Engineering and Computer Science Dissertation, August 2012
TCBMM/ANAYASA	*Türkiye Cumhuriyeti Anayasası, Türkiye Cumhuriyeti* Büyük Millet Meclisi, , http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf, erişim 15.02.2014
TCBMM/e-Tic K.. Tas.	*Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı ile Avrupa Birliği Uyum Komisyonu, Bayındırlık, Đmar, Ulastırma ve Turizm Komisyonu ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu Raporları*, Türkiye Cumhuriyeti Büyük Millet Meclisi, *http://www.tbmm.gov.tr/gundem/gundem.htm ,erişim_5_Mart 2014*
TCBMM/Gündem	Türkiye Büyük Millet Meclisi, Gündem, http://www.tbmm.gov.tr /gundem/gundem.htm, erişim 5 Mart 2014
TCBMM/Int..Yay.Suç 2007	*Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, *Md. 6 (2),* Türkiye Cumhuriyeti Büyük Millet Meclisi, , http://www.tbmm.gov.tr /kanunlar /k5651.html , Erişim 17.02.2014
TCBMM/Int.Yay.Suç. 2014	*Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Değişikliği*, 6518 Sayı 06.02.2014 tarihli torba yasa, Madde 85-100, http://www.tbmm.gov.tr/kanunlar/k6518.html erişim 06.03.2014
Tene/Polonetsky	Omer Tene/Jules Polonetsky, *To Track or "Do Not Track": Advancing Transperancy and Individual Control in Online Behavioral Advertising*, Minnesota Journal of Law, Science & Technology Volume 13 Issue 1, 2/28/2012
Topaloğlu	Ceren Topaloğlu *Tüketicinini Satın Alma Davranışını Etkileyen Alışveriş Motivasyonları Online Alışveriş üzerine Bir Uygulama*, Yayınlanmamış Y. L. tezi, Gebze Y. T. Enstitüsü, Sosyal Bil. Enst. 2009, Gebze,
TOR	TorProject, http://www.torproject.org erişim tarihi 28.10.2013
TUİK	TUİK *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması* (2013), Sayı:13569 Ağustos 2013, Ankara
Tureng, Dictionary DCTN	*Tureng English-Turkish Dictionary,* http://tureng.com/search/ deduction erişim tarihi 28.02.2014
Türkay	Ayşegül Türkay, *Satınalma Davranışları Açısından Üniversite Öğrencileri Arasında Marka Bağımlılığının Önemi*, Yayınlanmamış Y. L. Tezi, Süleyman Demirel Üniversitesi, Isparta, 2011
Tynan	Dan Tynan *Consumer Alert: Watch Out for Online Ads That Watch You,* www.pcworld.com, March 2007, http://www. techhive.com/article/128272/article.html
Uygun	Murat Uygun *Avrupa Birliğinin 95/46 Sayılı Veri Koruma Yönergesi Işığında Kişisel Verilerin Korunması*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010
Vahaplar/İnceoğlu	Alper Vahaplar/Mustafa Murat İnceoğlu *Veri Madenciliği ve Elektronik Ticaret* Ege Üniversitesi Bilgisayar Mühendisliği Bölümü, Türkiye'de İnternet Konferansı VII, İstanbul, 1-3 Kasım 2001
Van Bebber	Philipp Van Bebber *Informed Consent in Behavioral Advertising,* Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011
Yahoo, B. Targetting	http://advertising.yahoo.com/products-solutions/behavioral-targeting html (erişim tarihi 12.05.11)

Yun/Kim Keunho Yun/Daijin Kim. *Robust Location Tracking using a dual layer particle fitler*, Pervasive and Mobile Computing 3 (2007), Science Direct, Elsevier, available online 12 December 2006

ŞEKİL VE TABLOLAR

Çevrimiçi Davranışsal Pazarlamanın Tüketici Davranışları Üzerindeki Etkileri ve Kişisel Verilerle İlişkisi

§1.GİRİŞ

I. Problem Tanımı

Internet üzerinden yapılan reklamcılık faaliyeti - çevrimiçi reklamcılık- *web* tabanlı iş dünyasında önemli bir gelir kaynağı haline gelmiştir.[1] Bu gelişimin geçmiş on yıldaki artışı gelecek ile ilgili önemli işaretler vermektedir. Bu hızlı gelişim beraberinde ekonomiye farklı ve önemli bir katkı sağlarken diğer yandan teknolojinin sağladığı imkânlarla tüketici bireylerin özel yaşam alanlarına kendi rızaları olmadan erişimi de mümkün kılmaktadır. Mevcut kanunlar ve kurallar bu sistemi kontrol altına almakta ve doğru yönlendirmede yetersiz kalmaktadır. Bir tarafta tüketiciye onun ilgisini çekebilecek ürün ve hizmetleri özel bir çerçevede, reklam / pazarlama kirliliğine neden olmadan en ekonomik şekilde sunmak, diğer taraftan da en temel insan haklarından olan, bireyin mahremiyet alanına rızası olmadan girmemek, dengenin sağlanması ve yönetilebilmesi gerekli alan olarak görülmektedir.

Çevrimiçi reklamcılık iki önemli potansiyel ekonomik verimliliğin sağlayıcısıdır. Birincisi çevrimiçi reklamcılığın potansiyel alıcıları belirlemek ve sınıflandırmak üzere oluşturulacak içeriğe ayrılacak kaynak ihtiyacını azaltarak ekonomi yaratmak; ikincisi de çevrimiçi pazarlamanın satıcı ile alıcı uyumunun hassasiyetini arttırmasıdır. Böylece satıcı, sunduğu ürün ya da hizmeti gerçekten alabilecek müşterilere yönelme becerisini arttırır; tüketici de bu durumda yararlı

[1] Bkz. *Evans*, Journal of Economic Perspectives, Vol. 23, No.3, Summer 2009 p. 37

mesajları alabilecek; zaman alıcı ve kendisini ilgilendirmeyen mesajları almayacaktır.[2]

Diğer taraftan, farenizin her tıklaması ve her *web* sitesi ziyaretiniz, kredi kartı ile kimlik numaralarınız, şifreleriniz, hatta tıbbi kayıtlarınız da dâhil olmak üzere üçüncü şahısların kişisel bilgilerinize sizin onayınız olmadan erişimi için potansiyel oluşturmaktadır. Nielsen ve Pew Araştırma Merkezi'nce 2010 yılında yapılmış bir araştırma bulgularına göre "Amerikalıların % 55 i İnterneti her gün kullanmaktadır" ve "ayda 60 saatlerini çevrimiçi geçirmektedirler". "Dünyada *web*'de geçirilen zamanının % 36 sı e-posta göndermek, alış veriş yapmak ya da *web*'de arama yapmak için kullanılmaktadır;" "Bu zamanın % 42 si de içerik gözden geçirmesine ayrılmaktadır" "Bir aylık süre içerisinde bir kullanıcı toplam 2646 web sayfasını ziyaret etmekte olup, günde 56 defa internete girmektedir. Bu sayılar söz konusu mahremiyetin ihlali riskine açık olan boyutu açıkça ortaya koymaktadır.[3]

Şubat 2008'de gerçekleştirilen bir araştırmaya göre en üst düzeydeki 100 *web* sitesinin 56 tanesinde reklamlar yer alıyordu ve aynı araştırma bulgularına göre çevrimiçi reklamların toplam reklamlar içindeki payı % 8,8 idi.[4]

Söz konusu gelişimin boyutunun güncel durumu ile ilgili bir fikir sahibi olabilmek için 16 Nisan 2013 tarihli IAB (*Interactive Advertising Bureau*) ve PwC (*PricewaterhouseCoopers*) tarafından hazırlanan rapordaki verileri aktarmak yeterli olacaktır. Buna göre; ABD'de (Amerika Birleşik Devletleri) 2012 de İnternet Reklamcılığı toplam yıllık gelirleri 36,6 milyar $'a ulaşmış olup bu toplam 2012 den % 15 daha fazladır.

2012 deki bu toplam geçmiş on yıllık süre dikkate alınırsa ortalama yıllık ortalama % 19,7 'lik bir büyümeye karşılık gelip aynı dönem için hesaplanan GSMH (Gayri Safi Milli Hasıla) artışı % 1,5 dur. [5]

---

[2] Bkz. *Evans*, Journal of Economic Perspectives, Vol. 23, No.3, Summer 2009 p.43

[3] Bkz. *Arrington*, JICT, Journal of International Commercial Law and Technology, Vol. 8, No. 1, 2013 p. 13

[4] Bkz. *Evans*, Journal of Economic Perspectives, Vol. 23, No.3, Summer 2009 p. 37

[5] Bkz. *IAB/Revenue Report*, http://www.iab.net /media/file /IAB Internet Advertising Revenue Report FY 2012.pdf Interactive Advertising Bureau, *Internet Advertising Revenue Report 2012*, pp. 4, 7

Dan Tyan'a göre "çevrimiçi reklamlar sadece bir patlama göstermemekte; yuvarlanmakta, hızla dönmekte, haykırmakta, şarkı söylemektedir; aynı zamanda siz onlara baktıkça onlar da sizi gözlemekte, tıklama alışkanlıklarınızı, alışılagelmiş çerezlerden daha hassas bir biçimde profilinizi keşfetmeye çalışmaktadırlar."

Ağlar, davranışsal reklamların, reklam verenler için daha etkili, tüketiciler için de daha az rahatsız edici olduğunu ifade etmektedirler. Ancak bireysel gizliliği savunanlar ise kötü amaçlı kullanılma potansiyelinin yüksek olduğunu iddia etmektedirler. Ancak internet kullanıcılarının büyük çoğunluğu da internetteki davranışlarının bu kadar yakından izlendiği ile ilgili fikir sahibi değildir.[6]

Davranışsal Pazarlamayı kısaca tanımlamak gerekirse, çevrimiçi reklamcılık şirketlerinin, arama motorları ve genellikle internet reklamcılığıyla meşgul olan kurumların, internet kullanıcıların arama verilerini toplamalarıdır. Örneğin klasik müzik araması yaptığınız bir andan sonra, en iyi klasik müzik seçeneklerini teklif eden bir e-posta almanız böyle bir veri toplama ve değerlendirmenin sonucudur. Kullanıcıların internet kullanımı takip edilir ve böylece reklamcılık şirketleri bu verileri kullanır. Bu durum akla davranışsal reklamcılığın bireysel mahremiyeti ihlal etmesi konusunu bir soru olarak gündeme getirmektedir. [7]

Konuya biraz daha ayrıntılı bakarsak yine ABD'de FTC'un (*Federal Trade Commission* - Federal Ticaret Komisyonu) davranışsal pazarlama tanımını 2009 da "bireylerin internet faaliyetlerini, izleyerek onların ilgilerine yönelik hedefli (ısmarlama) özel reklamların onlara yönlendirilmesini sağlama uygulaması" olarak yapmıştır. Uygulama "iş çevrelerinin reklamlarını, izleyicilerinin ilgi alanları ile uyumlu hale getirmelerine imkân" verecektir. Örneğin, tüketici bazı ürün ve hizmetler internette araştırdığı zaman, bir *web* sayfasına sahip olan ve onu yöneten kuruluş, tüketicinin aramada kullandığı dili, ziyaret ettiği diğer *web* sayfaları bilgilerini toplayabilir (ve üçüncü şahıslarla paylaşabilir). Benzer şekilde, "*facebook*" dâhil birçok sosyal ağ uygulamaları, kişiye ilişkin verileri

---

[6] Bkz. *Tynan*, http://www.techhive.com/article/128272/article.html PcWorld, s. 26

[7] Bkz. *Arias*, http://www.ftc.gov/opa/2009/02/behavad.shtm, 2009 s. 1

kullanıcılarına haber vermeden, pazarlama ve internet izleme kuruluşlarına iletmektedirler. Ayrıca, tüketiciler yer-belirleme özellikli akıllı telefon uygulamalarını kullandıklarında, söz konusu bireyin nerelerde bulunduğuna ilişkin hassas/tam bilgiye birçok kuruluşun erişimi söz konusudur; hatta bu yere ilişkin bilgileri *web*'de gezinme ve sosyal medya bilgilerine ilişkilendirebilmekte; bu şekilde diğer iş kuruluşları da aynı bireysel tüketicinin kişisel profilini yapılandırabilecek bilgiyi toplayabilmektedir. Bu tür izleme ve ayak izi genel olarak, "tüketicilerin" hareketlerini/faaliyetleri izleyebilen çerezler tarafından izlenerek ve bu hareketler özel bir bilgisayar veya cihaz ile ilişkilendirilerek yapılmaktadır / gerçekleştirilmektedir. [8]

Bu endüstrinin kalbinde tüketiciye ilişkin verilerin, çoğunlukla söz konusu tüketicinin onayı olmadan hatta bilgisi dışında toplanması, ayrıştırılması ve çözümlenmesi yer almaktadır. Bu veri firmalara reklamlarını, bu reklamlardan en fazla etkilenecek özel gruplara yönlendirmelerine olanak vereceği gibi aynı zamanda söz konusu reklamla karşılaşan kullanıcıların daha sonraki davranışlarını izleyerek reklamlarının ne kadar başarılı etki yarattıklarını ölçebileceklerdir. Giderek artan bir endişe böyle kontrolsüz veri toplamanın tüketicilere zarar vereceği yönündedir. ABD'de FTC 10 Aralık 2012 tarihli bir raporunda bu ortamdan zarar görecek tüketicileri üç gruba ayırmaktadır. Birinci grup kendilerine ait bilgilerin toplanması ve paylaşılmasından güç durumlara düşenlerdir. İkinci grupta ise bu bilgi toplama ve paylaşımından haberi bile olmayanlar yer almaktadır. Üçüncü grubu da böyle bir paylaşımdan haberdar olan ancak bunun içerdiği riskleri değerlendiremeyenler – örneğin gençler – oluşturmaktadır.[9]

Tüketicilerin çevrimiçi davranışlarına ilişkin veriler, kuruluşlara çevrimiçi pazarlamayı olağanüstü hassasiyette iletme olanağını yaratmıştır. Örneğin bir Lexus bayisi reklamlarını öylesine hedefleyebilir ki bu reklamlar, sadece otomobillerle ilgili web sayfalarında son günlerde yüksek-sınıf araçları araştıranlara görünmektedir. Bu tür davranışsal hedefleme pazarlamacılara çok açık

---

[8] Bkz. *Cox/Cline*, Journal of Internet Law, March 2012, s. 3

[9] Bkz. *Goldfarb/Tucker*, Viewpoints, vol. 54, no. 5, Communications of the ACM May 2011, s. 26

bir biçimde çıkar sağlamaktadır; bu şekilde hedef olmayan tüketicilere yönelik reklama ayrılan kaynakların israfı azaltılabilmektedir. Bunun yerine, pazarlamacılar kaynaklarını, söz konusu reklamlardan en çok etkilenebilecek tüketici davranışlarına odaklamaktadırlar. Ancak tüketiciler için ise davranışlarına yönelik bu reklamlar yetkisiz hatta izinsiz sayfalarına sızmış gözükebilmektedir. Bunun sonucunda da tüm dünyada çevrimiçi verilerin pazarlama amaçlı toplanmasına ve kullanılmasını kısıtlayıcı yeni hukuki düzenlemelerin oluşturulmasına yönelik istekler gündeme gelmiştir. [10]

Birçok kişi yönlendirilmiş pazarlamaya olumlu bakmamakta ve kuruluşların kendi faaliyetlerini izlemesi fikrinden hoşlanmadıklarını ifade etmektedirler. Birçok araç da kullanıcılara, davranışsal pazarlama amaçlı izlenip izlenmediklerini kontrol edebilme imkânını, gücünü sağlamakla beraber kullanıcıların izlemeleri ve OBA'yı (*Online Behavioral Advertising* – Çevrimiçi Davranışsal Pazarlama) bu yollarla etkin bir biçimde kontrol edebilecekleri de kuşkuludur.

Davranışsal reklamcılık ilerleyen yıllarda en çok konuşulan konulardan biri haline gelecektir. İnternet kullanıcılarının çevrimiçi işlemlerini izlemek ürün veya hizmet sunan şirketlerin hedeflerinden birisidir. Ancak tüketicilerin de gizlilik hakkı vardır ve resmi kurumlar bu konuda devreye girip kişilerin mahremiyetini korumak ihtiyacını duymaktadırlar. İnternette arama yaptıktan sonra sayısız spam'e tahammül etmek yerine bir orta yol olmalı ve bulunmalıdır.[11]

Diğer taraftan bir başka gerçek "firmaların yenilikçi yaklaşımlarla, rekabetçi olmaları ve tüketicilerin yararına ürün ve hizmetler sunabilmeleridir". Bu amaç dikkate alındığında reklam destekli internetin, mahremiyeti denetleyen kurallardan ne şekilde etkilendiğini anlamak da son derecede önemlidir. [12]

Dolayısı ile bu tez çalışmasında, konuyu tüm ayrıntıları ile dünyadaki gelişmeler, uygulamalar ve görüşleri dikkate alarak analiz etmek, çözüme götürücü, olası ortak yolları ortaya çıkartmak; daha da önemlisi bu konuda yasal çerçevenin

---

[10] Bkz. *Goldfarb/Tucker*, Viewpoints, vol. 54, no. 5, Communications of the ACM May 2011, s. 25

[11] Bkz. *Arias*, http://www.ftc.gov/opa/2009/02/behavad.shtm, s. 1

[12] Bkz. *Goldfarb/Tucker*, Viewpoints, vol. 54, no. 5, Communications of the ACM May 2011, s.26

henüz emekleme aşamasında olduğu ülkemiz için gerek ABD gerekse AB (Avrupa Birliği) deneyimlerinden yararlanarak en uygun proaktif çözüm önerilerinin akademik çevrelerce araştırılmasına, ilgililer ve yetkililerce geliştirilebilmesine katkı sağlayabilecek, araştırmaya dayalı çözümlemeler sunabilmek amaçlanmıştır.

II. Yöntem

Bu yüksek lisans tezi Özet ve Kaynakça bölümleri dışında dört ana bölümden oluşmaktadır. Bölüm §1'in ilk kısmında tez çalışmasında odaklanılacak alana ilişkin genel bilgilerle problem tanımı; ikinci kısmında da tez çalışmasında benimsenen çalışma yöntemi ile tez içeriğine ilişkin kısa bir bilgilendirme yer almaktadır.

Bölüm §2'de önce tüketici davranışları ve çevrimiçi reklamcılık ilişkisinin tarihsel gelişimi; bu kapsamda tüketicinin çevrimiçi satın alma karar süreci ile ilgili kurumların internet pazarlama stratejilerine kısaca yer verilmiştir; daha sonra konuya ilişkin kavramsal çerçeve ile davranışsal pazarlama ilgili tanımlar ve terminoloji açıklanmıştır. Bu kısımda davranışsal pazarlama nedir? Kişi profili oluşturmada kullanılan veri madenciliği vb. metodolojiler nelerdir gibi soruların açıklamalarına yer verilirken aynı zamanda çevrimiçi reklamcılığın paydaşları tanımlanmış, çevrimiçi reklamcılık ağlarının, *web* sayfalarının, sosyal ağların ve ISP'lerin (*Internet Service Providers* - İnternet Servis Sağlayıcılar) kullanıcılarını nasıl izlediklerine ilişkin bilgilere yer verilmiştir. Bölüm §2'nin son kısmında ise çeşitli tekniklerin pazarlamacılar, sosyal ağlar ve akıllı telefon uygulamacıları tarafından izleme ve profillemede kullanma şekilleri ele alınmıştır.

Bölüm §3'de çevrimiçi izlemenin olası riskleri ile getirebileceği tehlikeler ve bunlara karşı koruyucu önlemler incelenmiştir. Koruyucu önlemler; Teknolojik / Pazar Temelli Çözümler, Düzenleyici Yasal Temelli Yaklaşımlar (A.B.D.. A.B. ve Türkiye'de), Özdenetim (*Self Regulation*) ve Eğitim yaklaşımları başlıkları ile sunulmuştur.

Teknolojik ve Pazar Temelli Çözümler kapsamında Görselleştirme ve Engelleme Araçları ile Mahremiyet Tabanlı Tasarım ve Mahremiyet Koruyucu

Sistemlerle ilgili kısa bilgiler verilmiştir. Düzenleyici Yasal Temelli Yaklaşımlar konusunda ise önce Avrupa Birliğindeki hukuki mevzuat incelenmiştir. Bu kapsamda AİHS (Avrupa İnsan Hakları Sözleşmesi), ABTHB (AB Temel Haklar Bildirgesi), Veri Koruma Direktifi (95/46/EC) ile E-Özel Yaşam Direktifleri (2002/58/EC) kişisel verilerin korunması ve bireysel/özel yaşama saygı çerçevesinde incelenmiş; bu yasal çerçevedeki davranışsal pazarlama için ne gibi işaretler bulunduğu değerlendirilmeye çalışılmıştır. İkinci olarak aynı şekilde ABD'de FTC'nin Davranışsal Reklamcılıkla ilgili düzenlemeleri, ilgili kanunlar ve uygulamalar kronojik sıra ile verilmiş, FTC'nin 2010 taslak ve 2012 nihai raporları tez konusuna ilişkin ayrıntıları ile incelenmiştir. Bölümün izleyen kısmında bu kez Türkiye'deki yasal mevzuat ele alınmıştır. Bu kapsamda 1982 Anayasası, TMK (Türk Medeni Kanunu), TCK (Türk Ceza Kanunu), CMK (Ceza Muhakemesi Kanunu), İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yolu ile İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve ilgili diğer kanunlar güncel şekilleri ile aynı çerçevede incelenerek ilgili maddeleri sunulmuştur. Bunun yanı sıra TCBMM'de (Türkiye Büyük Millet Meclisi) görüşülmek üzere bekleyen Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarının ilgili maddelerine de AB ve ABD ile karşılaştırmaların daha sağlıklı yapılabilmesi için yer verilmiştir. Bölümde daha sonra Çevrimiçi Davranışsal Reklamcılıkta Özdenetim (*self-regulation*) konusu ele alınmış ve bu konuya ilişkin olarak IAB Global (*Interactive Advertising Bureau, Global* - İnteraktif Reklamcılık Bürosu, Küresel) IAB Europe (*Interactive Advertising Bureau, Europe* - İnteraktif Reklamcılık Bürosu, Avrupa) ve IAB Türkiye (*Interactive Advertising Bureau, Turkey* – İnteraktif Reklamcılık Bürosu, Türkiye) ilgili kuruluş amaçları vb bilgiler özetlenmiştir. AB'de ilgili kuruluşların aralarında uzlaşarak oluşturduğu ve imzaladığı "IAB Avrupa Çevrimiçi Davranışsal Pazarlama için AB Çerçeve Sözleşmesi"ne ise ayrıntılı olarak yer verilmiştir.

Bölüm §4 olan sonuç ve önerilerde tezin önceki bölümlerinde yapılmış olan tespit ve değerlendirmelerin dikkate alınması ile çevrimiçi davranışsal pazarlamanın tüketici ve davranışları üzerindeki etkisi ve bunun bireysel verilerin mahremiyetinin ihlali ile ilgisi özetle değerlendirilmiş; ekonomik hayatın

teknolojik gelişmelerle kolaylaştırılmasının, diğer taraftan bireyin mahremiyetinin onun izni olmadan ihlalini önleyebilecek gerek yasal, gerekse paydaşlarca oluşturulmuş farkındalık oluşturma ve özdenetim yaklaşımlarını kapsayan çözüm önerilerinin gündeme getirilmesine odaklanılmıştır. Bu çerçevede Sonuç ve Öneriler bölümünün ilk kısmında ABD ve AB deneyimleri ve gelişimlerinin bir değerlendirmesi yapılmış olup ikinci kısımda da bu deneyimler gerek birbiri ile gerekse Türkiye'deki uygulamalarla kıyaslanarak sorunlara olası en iyi çözüm önerileri getirilmeye çalışılmıştır.

§2. KAVRAMLAR, TANIMLAR VE TERMİNOLOJİ

I. Tüketici Davranışları ve Reklamcılık İlişkisinin Gelişimi ve Kuramsal Çerçeve

A. Çevrimiçi Reklamcılığın İlk Günleri

Davranışsal / hedeflenmiş pazarlama kavramı basılı medyada, radyoda ve televizyonda internetten önce demografik, içeriğe bağlı ve günün saatlerine göre hedeflemeyi kullanan pazarlamacılar için yeni bir şey değildir.

Geçmişteki sorun belirlenmiş geniş tüketici gruplarını hedefleme için daha rafine hale getirmenin ya da reklamlara verdikleri reaksiyonları daha hassas ayarlamanın maliyetinin yüksek oluşu idi.

1997 öncesinde İnterneti'in ilk günlerinde segmentasyon, hedefleme konuları sıcak, ilgi çeken başlıklar değildi. Çünkü örneğin beyaz, erkek ve üst gelir vb gibi gruplarda yer alan izleyicilerin, daha ileri bir değerlendirme yapılmasını gerektirmeyecek kadar aynı yapıda oldukları düşünülüyordu.

Ancak 1990'lı yılların sonuna doğru internet kullanımı biraz daha yaygınlaşınca, yayıncılar televizyoncular, radyocular ve basılı yayınlardan ödünç aldıkları bazı hedefleme tekniklerini internet ortamında da denemeye başladılar. 2000 li yılların

başında kullanıcıların tıklama motiflerine dayalı hedefleme seçenekleri pazarda ilgi çekmeye başladı.

Geçmiş on yıl içerisinde de hedefleme tekniklerinde çok hızlı gelişimler oldu. Reklam hedefleme ağı (*Ad targeting network*) kurucularından Joe Wilson, 1990 lı yılların sonunda bir gazetenin interaktif bölümünde teknik eleman olarak çalışıyordu. O tarihlerde yayıncıların, kullanıcı profillerini reklamları hedeflemek için topladıkları verilerin nasıl kullanılabileceğine ilişkin yoğun tartışmalar sürüp gidiyordu; ancak *server*'ların yavaş hızı ile tüketicilerin her seferinde içeriklere bakmak üzere net girmeyecekleri algısı bir engel oluşturuyordu.

O tarihlerde kullanılan en karmaşık yöntemler; reklamları web sayfasının belirli bölümlerinde döndürmek, günü belirli saatlerinde, değişen boyutlarda yayınlamak gibi uygulamalardan ibaretti.

Davranışsal özellikleri belirlemek ve hedefleme yöntemleri bu bakımdan oldukça yenidir. 1990'lı yılların sonuna doğru tartışılmış olmasına rağmen davranışsal hedefleme o dönemdeki teknoloji patlaması içinde kaybolmuştur. Teknoloji 2000'li yılların başındaki durgunluk döneminde tekrar ilgi çekmeye başlamıştır; bu durum 2003 sonu 2004 başında ticari basında yer alan kuruluşlar tarafından benimsendiğinde oluşmuştur. [13]

Elektronik ticaret, örgütsel ve bireysel seviyede tüm ticari faaliyetlerle ilgili işlemleri kapsamaktadır. Bu alanda üretilmiş, işlenmiş ve aktarılmış tüm sayısal veriler, metinler, sesler ve görsel imajların işlenmesi ve aktarılmasına dayanmaktadır. E-ticaretin gittikçe büyüyen ticari hacmi ve popülaritesinin nedeni; bütün paydaşlarına fayda sağlama potansiyelidir. Tüketici açısından bakıldığında; ona toptancı, perakendeci ve bazı durumlarda da taşıyıcı gibi aracıları ortadan kaldırdığından dolayı, hızlı, kolay ve daha ucuz alışveriş imkânı sunmaktadır. Dünya gündemine 1996 yılında giren e-ticaret işleminin hızlı bir şekilde büyümesinin diğer bir nedeni de, özellikle bilgisayar ve iletişim teknolojisindeki gelişmelerin internete olan ilgiyi artırması ve erişim kolaylıklarını beraberinde getirmesi, düzenlenen cazip bilgisayar ve internet erişim kampanyalarının artması

[13] Bkz. *Baird*, s. 13-14

ve internete bilgisayar dışındaki araçlarla (cep telefonu, televizyon) erişimin sağlanmasıdır.

Günümüzde teknolojik alandaki hızlı değişimler ve internetin yaygınlaşarak hayatımıza girmesiyle birlikte birçok sektörde olduğu gibi perakendecilik sektöründe de değişimler ve gelişmeler gözlenmiştir. Yeni bir alışveriş ortamı olarak nitelendirilen internet, tüketicilere geleneksel alışveriş alışkanlıklarından çok farklı bir alışveriş ortamı sunmaktadır. Hemen hemen her işlemin bilgisayarlarla yapılabildiği "bilgisayar çağı"nda, alışverişleri de bilgisayar üzerinde yapmak kaçınılmaz olmuştur. İnternet ve getirdiği kolaylıklar, alışveriş sektörünün de kısa zamanda ilgisini çekmiş ve birçok firma internet üzerinde de satış yapmaya başlamıştır.[14]

Gelişmiş ülkelerde olduğu gibi Türkiye'de de tüketicilerin hayat tarzının değişmesi ve zaman darlığı gibi faktörler, fiziksel ortamlarda alışverişe alternatif bir yöntem olan internet üzerinden alışverişin yaygınlaşmasına zemin hazırlamaktadır. Açılan çok sayıda sanal mağaza bu konuda tüketicilere giderek artan sayıda seçenekler sunmaktadır. Tüketicilerin web siteleri üzerinden her türlü mal veya hizmete erişmesi, mal ya da hizmet hakkında bilgi ve fiyat alması, rakip firmalarla kıyaslama yapabilmesi, elektronik ödeme, elektronik bankacılık ve sigortacılık, danışmanlık işlemleri, vb. yapabilmesidir. Elektronik alışveriş yapan tüketiciler Internet'te detaylı ürün bilgileri ve çok fazla çeşit seçeneği bulmanın rahatlığını yaşamaktadırlar.

Internet alışveriş ortamını olabildiğince kişiselleştirmektedir ve kişiye özel hizmet veya ürünlerin alışverişinde gizlilik açısından kolaylık sağlamaktadır. Alışveriş için fiziksel bir çaba sarf edilmediğinden çok sayıda web sitesi kısa zamanda gezilebilmekte ve bu da internet ortamında tüketici davranışını belirleyen en önemli etkenlerden birisi olan zaman tasarrufunu ön plana çıkarmaktadır. Ayrıca alıcılara hız kazandırması, ürün, marka, fiyat ve firma karşılaştırmalarına fırsat vermesi ve bunlara bağlı olarak alıcıları bazı maliyetlere katlanmaktan kurtarması

[14] Bkz. *Topaloğlu*, s. 1-2,

gibi zaman ve maliyet üstünlükleri internet üzerinden satın almanın tüketicilerin davranışlarını etkilemede ön plana çıkmaktadır

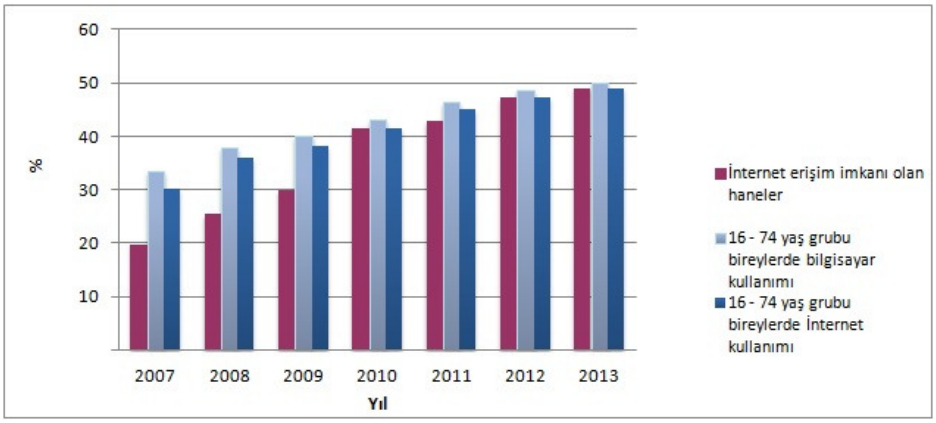
Yapılan araştırmalarda internet üzerinden alışveriş, elektronik posta gönderimi ve internette gezinmenin hemen sonrasında üçüncü en popüler internet aktivitesi olmuştur [15]

TUİK'in (Türkiye İstatistik Kurumu) 22 Ağustos 2013 Haber Bülteninde 2013 yılının ilk üç ayında (Ocak-Mart) 16-74 yaş grubundaki bireylerde bilgisayar ve İnternet kullanım oranlarının sırasıyla %49,9 ve %48,9 olarak belirlendiğine işaret edilmektedir. Bültende bu oranların 2012 yılında sırasıyla %48,7 ve %47,4 olduğu vurgulanmaktadır.

Aynı bültende 2013 yılı ilk üç ayında (Ocak-Mart 2013) 16-74 yaş grubundaki tüm bireylerin %39,5'inin İnterneti düzenli olarak (hemen her gün veya haftada en az bir defa) kullandığı bilgisi de verilmektedir..

Temel göstergeler ilişkin 2007-2013 değerler aşağıda grafik olarak gösterilmiştir

Temel göstergeler, 2007-2013



Şekil.1 Hanehalkı İnternet Erimi ve Kullanımı Temel Göstergeleri

(Bkz. *TUİK*, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması (2013), Sayı:13569, sf.1)

Aynı rapora göre İnternet kullanan bireylerin İnternet üzerinden kişisel kullanım amacıyla mal veya hizmet siparişi verme ya da satın alma oranı %24,1'dir.

[15] Bkz. *Eren*, s. 25

Önceki yıl İnternet üzerinden alışveriş yapanların oranı ise %21,8 idi. Bu oran 2007 yılında da %5.65 idi. 2012 yılı Nisan ile 2013 yılı Mart aylarını kapsayan on iki aylık dönemde İnternet üzerinden alışveriş yapan bireylerin %48,6'sı giyim ve spor malzemesi, %25,8'i elektronik araç, %25,6'sı ev eşyası, %20'si seyahat ile ilgili diğer faaliyetler (konaklama hariç), %15,9'u kitap, dergi, gazete (e-kitap dahil), %15,7'si gıda maddeleri ile günlük gereksinimler aldığı görülmektedir.[16]

B. Çevrimiçi Tüketici Davranışı

İnternet yapısı ve işleyişi bakımından yeni bir tüketici tipi yaratmaktadır. Bu tüketici tipi özellikle davranışsal açıdan geleneksel tüketici tiplerine göre farklı özellikler taşımaktadır. Bu farklılıklar internetin şu özelliklerinden kaynaklanmakta ve tüketici davranışlarında değişikliği kaçınılmaz hale getirmektedir.

Aracısız Alışveriş ve Yeni Araçlar: Geleneksel satın alma sürecinde üretici ile tüketici arasında çoklu bir dağıtım sistemi bulunmaktadır. Bu ürün veya hizmetlerin üreticiden tüketiciye akışında zaman ve yer açısından farklı işlevlerin satın alma sürecine eklenmesini gerektirmektedir. Bu durumda ürün veya hizmetlerin üreticiden tüketiciye akışında alış veriş işlevini aracılar gerçekleştirmektedir; aynı zamanda tüketicinin gereksinim duyduğu bilgi akışı da yine aracılar üzerinden gerçekleşmektedir. Bu yapıda üreticilerin tüketiciyle iletişimi ya hiç yoktur ya da çok az olmaktadır.

Oysa İnternet tüm bu akışı başından sonuna kadar değiştirdiğinden özellikle küçük büyük işletme ayırımı ortadan kalkmaktadır. Üretici ile tüketici arasındaki iki yönlü doğrudan iletişim çok sayıda yönetsel görevin otomatize edilmesi çok sayıda tüketiciye aynı anda ve de etkin bir biçimde ulaşmada üstünlük sağlamaktadır. İnternet ürün ve hizmetlerin üreticiden tüketiciye akışında daha büyük değerleri daha düşük maliyetle dağıtabilen yeni aracılık sistemini oluşturmaktadır. Otomatik sipariş sistemleri, değerleme hizmetleri gibi yeni

[16] Bkz. *TUİK*, Hanehalkı Bilişim Teknolojileri Kullanım Araştırması (2013), Sayı:13569, sf.1, 22

aracılık mekanizmaları tüketici davranışlarını satın alma karar süreci açısından etkilemektedir.

Ortak Üretici Olarak Müşteri: Müşterilerin satın alacakları ürünlerin üretiminde giderek daha fazla rol aldıkları, tasarımdan ambalaja kadar birçok konuda üretime müdahale ettikleri bir döneme doğru gidilmektedir. Bu akımın yakın bir gelecekte self servis perakendeciliğe dönüşmesi beklenmektedir. Örneğin Amazon ve benzeri şirketler müşterilerinin siparişlerini, müşteri hizmetleri bölümünün yardımı olmaksızın izlemelerini sağlamaktadır.

Gücün Pazarlamacılardan Tüketicilere Geçmesi: Gelişmiş bilgi teknolojileri araçlarını kullanabilen, pazar araştırması yapabilen, diğer tüketicilerle iletişim kurup, ortak hareket edebilen, zaman ve mekân kısıtlamalarına tabi olmayan yeni tüketici tipi gücü kendisinde toplamakta ve pazarlamacılara, talep ettiği ürünün tasarımından, geliştirilmesine, satın alınmasından, satış sonrası hizmetlere kadar her aşamada yön vermektedir.

Daha Fazla Değer Bilinci: Pazarlamada meydana gelen radikal değişiklikler tüketicinin kendi kontrolündeki zaman, para, çaba ve yer konularındaki beklentisini arttırmaktadır. Fiyat artışını aşan bir değer artışı kendisine sunulduğunda, tüketici daha fazla bedel ödemeye gönüllü olacak, alışveriş için harcadığı zamanı en aza indirmek isteyerek daha basit ve kolay satın alma süreçlerini tercih edecek ve sonuçta bir defada çok miktarda satın almaktan kaçınacaktır. Bu anlamda değer yaratan, yaratıcı fiyat farklılaştırmalarına giden şirketlerin ürünlerine yönelme olması kaçınılmaz olmaktadır. Demografik ve davranışsal açıdan yukarıda belirtilen özelliklere sahip yeni bir tüketici kitlesinin oluştuğu görülmektedir.[17]

Bir başka ifade ile tüketici alışveriş sırasında göreve odaklı ve rasyonel bir tutum içerisinde bir değer arayışı içerisinde ise bu faydacı satın alma davranışıdır. Satın alma tecrübesi sonucu elde edilen duygusal ve psikolojik deneyim ise hazcı satınalma davranışıdır.

Faydacı değer, fonksiyonel fayda ve zararların genel değerlendirmesi olarak tanımlanır; ekonomik olarak "hesaplı" ve zaman kazanmanın, uygunluğun

[17] Bkz. *Eren*, s.27-29

muhakemesi gibi bilişsel durumları daha fazla içine alır. Faydacı değere etki eden alışveriş motivasyonları; maliyet, uygunluk, seçenek, bilgiye ulaşma, sosyalleşme eksikliği ve ürünlerin isteğe göre düzenlenmesidir.

- Maliyet, çevrimiçi ortamda tüketiciler aynı kalitedeki ürüne daha uygun fiyattan sahip olabilirler.
- Uygunluk, internet alışverişi 7/24 durmaksızın hizmet sağlar, bu zamanla, mekânla, hava durumu ile sınırlandırımaz. Tüketicinin çevrimiçi alışveriş yapmayı sevmesinin temel nedeni, uygunluğun önemidir.
- Seçenek, çevrimiçi mağazalar daha düşük maliyetle daha fazla seçenek sağlayabilirler
- Bilgiye Ulaşma, tüketiciler sadece birkaç tıklama ile çevrimiçi mağazalar ve ürünler hakkında çok fazla bilgiye ulaşabilmektedirler. Toplanan bilgiler gelecekteki karşılaştırmalar için kopyalanabilmekte ve saklanabilmektedir. Çevrimiçi alışveriş tüketicinin araştırma, karşılaştırma yapmasına, bilgiye ulaşabilmesine sadece fiziksel mağazası olan işletmeye göre çok daha kolay kılan bir alt yapı sunmaktadır.
- Sosyalleşme Eksikliği, teknoloji ara yüzü çevrimiçi alışveriş yapanlara ürünleri satış personelleri tarafından rahatsız edilmeden göz atma imkânı verir.
- Ürünlerin İsteğe Göre Düzenlenmesi, çevrimiçi mağazalar tüketicilere çeşitli özelleştirilmiş ürünler sağlayabilmektedir. İnternet özelleştirmeyi sağlamak için en uygun ortamdır

Hazcı değer, tüketicinin bencilliğiyle ve duygularının hoş tutulmasıyla ilgilidir. Hazcı alışverişin genel nedenleri olarak "sosyal deneyimler, ortak ilgilerin paylaşımı, bireyler arası cazibe, hazır statüler ve yarış heyecanı" sayılabilir. Hazcı (hedonik) yararlar duygusal, fiziki zevkler, düşler ve estetik özellikleri içerir. Tüketiciler sıklıkla bir görevi tamamlamaktan çok yaşadıkları tecrübelerin zevki için alışveriş yaparlar. Hazcı değere etki eden alışveriş motivasyonları macera, sosyallik, yenilikçilik, değer, otorite ve statüdür.

- Macera, müşteriler çevrimiçi alışveriş sırasında yeni ve ilginç şeylerle karşılaşırlar ve alışveriş süreci boyunca araştırmanın eğlencesini yaşarlar.

Alışveriş yapanların alışveriş sürecinin kendisi için duyduğu çoşku ürün için olandan daha fazladır.

- Sosyallik, alışverişin sağladığı sosyal iletişim genellikle tüketicilerin alışverişe gitmesinin asıl amacıdır. Sanal topluluğun ortaya çıkması sosyal faydaları arkadaşlar ve yakınlardan internet vasıtasıyla bilinen arkadaşlara çevirmiştir. İnternetten alış veriş yapanlar çevrimiçi olarak bilgi ve alışveriş deneyimlerini paylaşırlar.
- Yenilikçilik, internetten alışveriş yapanlar için en güçlü motivasyonlardan birisi keşfetmek ve yeni ürünleri bulmaktır. Çeşitlilik arayışı çevrimiçi durum içinde önemli bir güdü olmaya uygundur.
- Değer, alışveriş yapanlar pazarlık sırasında satıcılarla tartıştıkları zaman zevk oluşur; tüketiciler elde edebildikleri indirimimin "kazanma" gösterişini göz önünde bulundurduklarında mutlu hissederler. İnternetten alışveriş yapanlar alışveriş sürecinde hazcı değer sağlayabilirler; bu da duyusal ilişki ve heyecanın artmasını sağlayabilir.
- Otorite ve Statü, alışveriş yapanlar fiziksel mağazalarda satış personeli tarafından sağlanan birebir hizmeti almaktan otorite ve statü elde ederler. İnternetten alış veriş yapanlar ise daha yüksek kontrol seviyesi ve otoriteye sahip olabilirler. Bu iki durumda otorite ve statü kaynakları farklıdır.[18]

İnternet Üzerinden Satın Almada Tüketici Davranışlarını Etkileyen Faktörler aşağıda gruplandırılarak sunulmuştur:

Sosyal Faktörler;

- Kültür, insanların yarattığı değer sisteminin ahlak, sanat, sembol, inanç, gelenek ve göreneklerin karışımıdır. Kültür bireylerin her hareketini etkilediği gibi, tüketicinin satın alma davranışını da doğrudan etkilemektedir. İnternetin ortaya çıkması kültürü yakından etkilemiş ve dünyanın küçülmesini beraberinde getirirken, kültürlerin daha yakından öğrenilmesini sağlamıştır. Geleneksel pazarlamada olduğu gibi, internet üzerinden pazarlamada da kültürün etkisi hissedilmekte ve yapılan

[18] Bkz. *Topaloğlu*, s. 24-30

alışverişler genellikle o ülkenin veya çevrenin kültürüne uygun olmaktadır. Yine de internette pazarlama stratejileri geliştirilirken, farklı kültürlere uyumlu pazarlama karması geliştirmenin gerekliliği ortaya çıkmaktadır.

- Aile, Pazarlama karmasının oluşturulması bakımından gerçek satın almayı kimin yaptığının yanı sıra alım kararını kimin etkilediği, ailede kadının ve çocukların rollerinin ne olduğu, nasıl değiştiği satın alma davranışını etkilemektedir. Özellikle bireysel olarak aileden bağımsız genç nüfusun yaygın olduğu toplumlarda, internet üzerinden satın almada karar verme yetkisine sahip tüketiciler alışveriş eylemini daha rahat gerçekleştirmektedirler.
- Sosyal Sınıf, bu kavram tüketici davranışları bakımından tüketim yapıları, satın alma yapıları, harcama ve tasarruf yapıları gibi konularda incelenebilmektedir. Zaman faktörü, zaman kaybetmeme en çok göze çarpan internetten alışveriş nedenidir. Mağazaları gerçekten gezme ile zaman kaybetmemek, sinemaya sıra beklemeden bilet alma, bankadan bankaya gitmeden havale yapma gibi örnekler orta sınıf tercih sebepleridir. Kredi kartı kullanımı üst grup için alternatif bir ödeme şekli olurken, alt gruplar için alım güçlerinin olmadığı şeyleri alma imkânı sunan bir araç olmaktadır.
- Referans Grupları, kişinin tutumlarını, fikirlerini ve değer yargılarını etkileyen herhangi bir insan topluluğu referans grubu olarak tanımlanır. Bunlar başta aile olmak üzere kişiyi yüz yüze ilişkilerde etkileyen yakın çevresidir. Bir diğer grup da kişinin üyesi olmadığı gruplar ve yüz yüze olmadığı ünlü sinema yıldızları, sporcular vb. kimselerdir. Pazarlama açısından referans kimse ve grupların önemi bunların tüketici tercihlerini ve davranışlarını yönlendirmesine dayanmaktadır.

Bireysel Faktörler;

- Kişilik, insanların kişiliği kalıtımsal olduğu kadar, çevresi tarafından da biçimlendirilmektedir. Toplumun değer yargılarına bağlı olarak belirli kişilik olguları bastırılmakta, bazıları da ortaya çıkmaktadır. Kişilik özellikleri tüketicinin hangi mağazadan alışveriş yapacağına etkide

bulunabilmekte iken tüketicinin kendine güveni hangi mağazayı seçeceğiyle de ilgili olabilmektedir.

- Öğrenme, kişilerin düşünce biçimleri ve öğrenme şekilleri önemli farklılıklar göstermektedir. Değişik kültürdeki kişilerin yaklaşımları birbirlerinden farklı olabilmektedir. İnternet aracılığı ile arzu edilen ürün ya da hizmet hakkında çok kolay detaylı bilgilere ulaşılabilmesi herkes için aynı sonucu doğurmamaktadır. Gerekli bilgiye nasıl ulaşılacağı, ilgili siteden nasıl satın almanın gerçekleştirilebileceği, bazı elektronik araçların kullanımı hakkında kolay öğrenmeme gibi sorunlar, tüketicilerin internet üzerinden satın alma faaliyetlerini etkileyebilmektedir.
- Algılama, kişilerin birlikte şahit oldukları aynı konu veya olay hakkında çok farklı düşünebilmeleri, aynı olaya birlikte şahit olmaları, ancak onu farklı algılamış olmalarından kaynaklanmaktadır. Web sitesinin kalitesi, sadeliği, karmaşık işlemlerin olmaması, sitede var olan küçük ve büyük reklam bandı olması, sitenin arama motorlarında kayıtlı olması, anahtar kelimelerin kolay bulunması, sitenin prestiji ve tanınması bakımından önemli noktalardır. Ayrıca sayfadaki reklam, ürün imajı, fiyatı, üretildiği ülke, ilgili kurum imajı gibi konular da algı üzerinde etkili olurlar.
- Tutumlar, Değerler, İnançlar ve Din, değişik toplumlarda değer yargıları farklı olduğundan, bu değerler tüketicilerin kararlarını ve satın alma davranışlarını önemli ölçüde etkilemektedir. Yabancı pazarlarda inanç ve tavırlar, işletmelerin çok dikkat etmesi gereken hassas bir konudur ve yerel pazara sunulan ürünün, o toplumun inanç ve tavırlarına ters düşmemesi gerekmektedir – renklerin belirli kültürlerde farklı anlamları bulunması, tüketicilerin sahip olduğu değerlerin bilinmesi, toplumlarca kutsal olan, saygı gören veya düşmanlık beslenen sembollerin olup olmadığının araştırılması vb gibi. [19]

[19] Bkz. *Eren*, s.30-35

C. Çevrimiçi Tüketicinin Satın alma Karar Süreci

Bir şeyi çevrimiçi satın almak üzere seçim yapmak çeşitli bir dizi faktörü içerir. Satın alma işlemi fiili olarak satın almadan uzun bir süre önce başlar ve satın almadan uzun bir süre sonrada etkilerini gösterir. Tüketicinin satın alma karar süreci her ürün için aynı olmayabilir. Müşteriler, bazı safhaları atlayabilirler veya belirtilen sırayı değiştirebilirler. Kapsamlı bir karar verme sürecine giren kişiler bu karar sürecinin tüm aşamalarından geçerken, sınırlı bir karar sürecine giren kişiler bu karar sürecinin bazı aşamalarını atlayabilmektedir. Tüketicilerin satın alım kararlarını nasıl verdiklerini anlayabilmek pazarlama açısından çok önemlidir.

Çevrimiçi satın alma sürecinin temel adımları aşağıda en basit şekli ile açıklanmıştır.

1. İhtiyacın Belirlenmesi (Farkına Varmak)

Sürecin ilk adımı "bir ihtiyacın tanımlanmasıdır". Daha basit olarak bu, potansiyel müşterinin bir ürünü satın almaya ya da bir hizmetten yararlanmaya ihtiyacı olduğunun farkına varmasıdır. Bu ihtiyaç kişinin içgüdüsünün yarattığı bir ihtiyaç olabildiği gibi, toplumun etkisiyle veya işletmelerin tanıtma faaliyetleri suretiyle yaratılmış bir ihtiyaç olabilmektedir. İhtiyaç, kişinin sahip oldukları ile sahip olmak istedikleri arasında fark bulunmasıyla ortaya çıkar.

2. Bilgi Arama (Alternatiflerin Belirlenmesi)

İhtiyaç tüketici tarafından belirlenir belirlenmez bir sonraki adım ihtiyacın nasıl giderilebileceğine ilişkin "bilgi arayışı" başlatmak ve yürütmektir.

Dijital çağda bu arayış, ortamı daha kolay ve rahat olduğu için, giderek daha yoğun bir biçimde çevrimiçi yürütülmektedir. Ancak bu adımda, yola birlikte çıkanlardan % 17 si sürecin dışında kalır; bunun nedeni %9 unun istedikleri bilgiyi bulamadıkları veya belirleyemediklerinden; kalan %8 inin de satınalma bilgisine

sahip olmadıklarındandır.; Bu arayış tatmin olacakları alternatifleri buluncaya kadar sürer.

3. Değerlendirme Adımı (Alternatiflerin Değerlendirilmesi)

Başka bir deyişle tüketiciler, belirsizliği azaltacak ve alternatifleri değerlendirmeye açacak bir temel oluşturması için bilgi arama sürecine girerler. Bu aşamada tüketici ürün veya hizmetten en fazla hangisi ile yarara veya tatmine ulaşacağını düşünür ve ona ulaşmayı hedefler. Bu aşamada zaman unsuru rol oynar. İhtiyaç acil değilse, alternatiflerle ilgili olarak daha fazla zaman harcanır.
Araştırma tamamlandığında, tüketicinin ne seçeneklerden hangisinin kendi ihtiyacını karşılamaya en uygun olduğunu değerlendirmeye başlaması ile değerlendirme basamağı başlamış olur. Sürecin bu adımında karşılaştırma için teklifler istenebilir ve çoğu zaman teklifleri dikkate alınacak olan İş Tedarikçilerinin güvenirlikleri için ek araştırmaları gerektirir.

Ancak bu adım aynı zamanda en büyük kaybın gerçekleştiği adımdır. Alışverişe çıkanlardan araştırmaya başlayanların %25 i bu adımdan ileriye gitmeden süreçten kopmaktadırlar.

4. Satın Alma Kararı (Satın Alma)

Alternatiflerin değerlendirilmesi tamamlandığında bir sonraki adım "satın alma kararı'nın verilmesidir; bunun sonunda da %12 lik bir kesim daha satın alımı gerçekleştirmeme kararını verirler.

Değerlendirmenin sonucu olumlu ise, tüketici; malın cinsine, markasına, fiyatına, rengine, miktarına ve satın alacağı yere ilişkin bir dizi karar verir; hangi ürünü satın alacağına karar verir ve kararını uygulamaya geçirir. Bu aşamada pazarlamacı, reklam ve diğer yollarla tüketiciye bilgi verir; karar almayı kolaylaştırır. Satın alma ürün veya hizmet için para ödemesinin yapıldığı bölümdür. Bazı kaynaklarda Satın alma kararının verilmesi ve satın alma iki ayrı adım gibi de yorumlanmıştır.

5. Satın Almanın Değerlendirilmesi

Karar alma sürecinin son adımı gerçek satın alımdan sonra gelen "satın almanın değerlendirilmesi" basamağıdır. Bu adımda müşteri satın aldığı ürün ya da hizmetin beklentilerini karşılayıp karşılamadığının değerlendirilmesidir.
Pek çok durumda, insanlar yaptığı alışverişlerden büyük oranda tatmin olurlar. Bazı durumda ise insanlar büyük hayal kırıklığı ve tatminsizlik yasayabilirler. Bu süreç adımı sadece müşterinin tekrar alım yapmasına etki yapmaz aynı zamanda müşterinin diğer potansiyel müşterilere olumlu ya da olumsuz tavsiyede bulunmasını tetikler.[20] [21]

D. İnternet Pazarlama Stratejileri

Çevrimiçi reklamcılık, reklamcıların izleyicilerini daha hassas segmente etmelerine ve kullanıcılarla karşılıklı iletişim kurmalarına imkân vermektedir. Reklamcılar için çözümleri bütünsel bir biçimde sağlayan altı temel hedefleme modeli vardır. Bu modeller ile temel ilkeleri ve kriterleri ile bir sonraki sayfadaki çizelgede gösterildiği gibidir.

Bunlardan ilk dördü uzun yıllardan beri yaygın bir biçimde kullanılmaktadır. Davranışsal pazarlama ve yeniden hedefleme ise e-ticarette giderek daha fazla önem kazanmayı sürdürmektedir. eMarketer tarafından 2010 yılında yapılan bir tahmin çalışmasında 2009-2014 dönemi için davranışsal pazarlamada, gelecek 5 yıl boyunca, yıllık ortalama % 23 lük bir bir büyüme öngörülmektedir. Bu da yaklaşık 2,6 milyar ABD dolarına karşılık gelmektedir. Avrupa'da da benzer bir trend beklenmektedir. [22]

---

[20] Bkz. *Türkay*, s.32-35
[21] Bkz. *Net Age,* http://www.netage.co.za/articles/resources/all/74
[22] Bkz. *PwC/IAB France/SRI,* https://www.pwc.com/en_GX/gx/entertainment-media/pdf/IAB_SRI_Online_Advertising_Effectiveness_v3.pdf sf. 50

Hedefleme Türü	Hedefleme İlkeleri ve Kriterleri
Demografik	Müşterileri yaş, cinsiyet, sosyoekonomik kategori ve ailevi durumuna göre hedefleme
Coğrafi	Belirli bir yere göre tüketicileri hedefleme: Ülke, bölge, şehir vb
Zamana Dayalı	Reklam mesajlarını azami etki yaratmaları için yılın belli dönemlerinde, belirli gün ve saatlerde iletmek
İçerik Özellikli	Reklamları ziyaret edilen web sayfasındaki ilgili içerik özellikli yerleştirmek
Davranışsal	Reklamları kişinin önceki ziyaret tercihlerine göre yerleştirmek. Profiller bu durumda ilgi alanlarına, önceli satın alım türlerine ve demografik kriterlere göre yapılandırılır
Yeniden Hedefleme / Yeniden mesaj Gönderme	Belirli bir ürüne daha önceki ziyaretinde ilgi göstermiş ya da satın alma sürecini yarım bırakarak çıkmış potansiyel müşterilere reklam iletmek

Çevrimiçi pazarlamada internetin yeni kullanım yolları**:** Çevrimiçi reklamcığın gelişmesine yardımcı olmak üzere internetin yeni kullanım yolları aşağıda özetlenmiştir:

- İnternet ve TV'nin birlikte kullanımı; internetin ortaya çıkışı, başta özellikle TV olmak üzere, diğer medyanın reklam amaçlı kullanımının yerine geçmemiştir. İnternet, TV deneyiminin bir uzantısı olarak rol üstlenmiştir. Microsoft tarafından yürütülen bir araştırma internet kullanıcılarının % 78'i

çevrimiçi video izlemelerinin TV kullanımlarını tamamlayıcı bir rol oynadığı inancında olduklarını göstermektedir. İnternet kullanıcıları özel, alışılmışın dışında ve daha önce erişilmesi mümkün olmayan içeriklerin arayışındadır. Medyanın kullanımındaki bu eş zamanlılık marka deneyiminin çevrimiçi medya ile güçlendirilmesine olanak vermektedir; bu da reklamcıları web ile diğer medyadan bir karma yapmaya yönlendirmektedir.

- İnternet kendisini satın almayı etkileyen ve ortamını hazırlayan bir araç olarak kanıtlamaktadır; günümüzde internet satın alma sürecinin kalbinde yer alır. 2010'da FEVAD-Mediametrie (*Federation e-commerce et Vente a Distance*) barometresi internet kullanıcılarının % 78'inin bir ürün satınalmadan önce bir web sayfasına baktıklarını göstermektedir. Bu gelişim reklamcıların tüketiciler tarafından kullanılan çoklu kanallardan satınalmaları ile ilgili olarak olabildiğince ayrıntılı analiz yapmalarının önemini ortaya koymaktadır. Reklamların, çevrimdışı satışlar üzerindeki etkisi, özellikle de tüketicilerin katılımını sağlaması ve kararlarını etkilemesi bakımından yaşamsal önem taşımaktadır.
- Sosyal ağlar reklamcılara kendilerini ifade için yeni bir platform sunmaktadır; yine *Mediametrie / net Rating* araştırması internet kullanıcılarının kısa mesajlar için ayda 3 saat 40 dakika, toplumsal ağlarda 4 saat 8 dakika, e-mail haberleşmesinde 2 saat 40 dakika ve çevrimiçi müzayede ve sınıflandırılmış reklam sayfalarında da 1 saat 15 dakika geçirdiklerini göstermektedir. Medyanın toplumsal ve sosyal ağları da kapsayan bu yeni kullanımı, reklamcılar için önemli ölçüde hedefleme fırsatları taşıyan ilave bir reklam sahası yaratmaktadır (daha yüksek derecede hedefleme kapasitesi ve daha uzun zaman tüketiciyle karşılaşma zamanı sağlayarak). Reklamcılar, bu yeni reklam alanı olanaklarının geçerliliği ve etkililiğini, kendi iletişim amaçlarına göre değerlendirmek durumundadırlar [23]

[23] Bkz. *PwC/IAB France/SRI,* https://www.pwc.com/en_GX/gx/entertainment-media/pdf/IAB_SRI_Online_Advertising_Effectiveness_v3.pdf s. 13

Çevrimiçi pazarlama stratejisi oluşturmanın öğeleri: Başarılı bir çevrimiçi strateji formülasyonu için sağlam temeller gereklidir. Bu temeli çevrimiçi pazarlamanın üç önemli kavramı oluşturur. Bu üç kavram; Arama Motoru Optimizasyonu, İçerik Pazarlama, Sosyal Medya Pazarlamadır.

- Arama Motoru Optimizasyonu; arama yapılan bir terim ile ilgili olarak arama motorlarının en ön sayfalarda ilişkili göstereceği bir web sitenin oluşturulmasıdır. Örneğin arama yapanların % 95'i Google ve Yahoo'da ilk sayfada gözüken sayfaları tıklamaktadırlar.

  Sağlam bir Arama Motoru Optimizasyonu (*Search Engine Optimization*) stratejisi öncelikle ilgili doğru kelimelerin bulunmasından ve bu kelimelerle ilgili değerli içerik sağlanmasından oluşur. Arama Motoru Optimizasyonunun; İlgili Kelimeleri, Paylaşılan Değerli İçeriği, Hızlı Yüklenen Bir *Web* Sayfasını, Resim ve İçerik Zenginliği ve Saygın Web Sayfalarından Link'leri olmalıdır.
- İçerik Pazarlama; yeni bir kavram değildir. Bu yöndeki örneklerin ilki 1895 de John Deere'in yayınlamaya başladığı *The Furrow* dergisinde yer alır. İçerik pazarlama markanın oluşturulması ve şirkete güven duygusunun geliştirilmesi bakımından önemlidir.

  Çevrimiçi içerik pazarlama alanı blogları, eğitim videolarını, internet üzerinden ses ve görüntü yayınlarını hatta video oyunlarını kapsayarak genişlemiştir. Ancak bu stratejide de kalite düşüklüğü en yaygın hatalardan olup sıralamayı ve marka imajını olumsuz etkileyebilir. Siteye yerleştirilen içerik, potansiyel müşterinizin kuruluşunuzla ilgili izlenimlerinin oluşmasına yol açabilecektir.
- Sosyal Medya Pazarlama; iş çevreleri için Arama Motoru Optimizasyonu ile İçerik Pazarlamayı bir araya getirmenin bir yoludur. Arama Motorları sayfaların, içeriklerini sıralarken kaç defa paylaşıldığını da dikkate alır. Sosyal medya içeriklerin paylaşılmasındaki en önde gelen yol olmaktadır. *Twitter*, *Google+* ve *Facebook* gibi sosyal medya siteleri tüm tüketicilerin değerli buldukları içerikleri kendi ağları içinde paylaşmalarına müsaade

etmektedir. Araştırmalar göstermektedir ki kişiler, güvendikleri kişilerin kendileri ile paylaştıklarına daha fazla güvenme eğilimindedirler.

Ancak sosyal medya stratejilerinden en yüksek düzeyde katkı alabilmek için izleyicilerinizle, taraftarlarınızla interaktif bir ilişki içerisinde bulunmanız ve gerçek bir topluluk yaratmalısınız. Sadece sayısal olarak izleyicilerin, taraftarların olması yeterli değildir. Kişiler soru sorma imkânı, sesli iletişim, hatta şikâyetlerini dinleme bakımından size erişebilir olmalıdır. Soruna profesyonel yaklaşım gerekecektir. Onlara ilgi çekici içerik sunun; unutmayın ki sosyal medya her şeyden önce sosyaldir.

Hedeflerinize ulaşma imkânı verecek çevrim içi stratejilerinizi ancak böylesine güçlü bir temeli oluşturarak formüle edebilir, yaşama geçirebilirsiniz.[24]

II. Çevrimiçi Davranışsal Reklamcılık

A. Veri Madenciliği

Verilerin dijital ortamda saklanmaya başlanması ile birlikte, yeryüzündeki bilgi miktarının sürekli arttığı günümüzde, veri tabanlarında saklanan veri miktarı da benzer oranda artmaktadır. Veri tabanları artık terabyte'larla ölçülmektedir. Bu ölçekteki büyük veriler, stratejik öneme sahip bilgileri gizlerler. Veri madenciliği, büyük veri tabanlarındaki gizli bilgi ve yapıyı açığa çıkarmak için, çok sayıda veri analizi aracını kullanan bir süreçtir.[25] Veri madenciliği, eldeki yapılandırılmamış veriden, anlamlı ve kullanışlı bilgiyi çıkarmaya yarayacak tümevarım işlemlerinin formüle ve analiz edilmesi dahil, uygulamaya yönelik çalışmaların bütününü içerir[26].

---

[24] Bkz. *SEJ/Alton,* http://www.searchenginejournal.com/the-basics-of-online-marketing-strategy-in-2013/66623/

[25] Bkz. *Oğuzlar,* Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı: 21, Temmuz-Aralık 2003, s.67

[26] Bkz. *Vahaplar/ İnceoğlu*, VII. Türkiye'de İnternet Konferansı, 1-3 Kasım 2001, Bildiri s.1

Arka planında veri tabanı yönetim sistemleri, istatistik, yapay zekâ vb. çeşitli işlemlerin bulunduğu bu veri analiz tekniklerini, veri tabanında bilginin keşfi olarak da adlandırmak mümkündür. [27]

Özetle veri madenciliğinde amaç çok büyük miktardaki ham verinin toplanması ve bunlardan değerli/anlamlı bilginin çıkarılmasıdır.[28] [29]

Yüksek kapasiteli işlem yapabilme gücünün ucuzlamasının bir sonucu olarak, veri saklama hem daha kolay olmuş, hem de verinin kendisi ucuzlamıştır. Günümüzde oldukça yaygınlaşan elektronik ticaret ve çevrimiçi alışveriş mekanizmalarının da artmasıyla birlikte, bu alanda birbirlerine rakip olan firmaların çalışmaları, veri madenciliğinin önemini ön plana çıkarmaktadır.[30]

Bugünün yoğun rekabet ortamında müşteriler için yaşanan kıyasıya rekabet, işletmelerin bu müşteriler hakkında bilgi sahibi olmalarını zorunlu hale getirmiştir. Öte yandan günümüz pazarında müşteriler artık hemen her şey hakkında bilgi sahibi olmakta ve her zamankinden daha fazla seçme şansına ulaşmış durumdadırlar. Böyle bir durumda söz konusu müşteriler hakkında rakiplerin sahip olmadıkları bilgilere ulaşmak bir rekabet avantajı sağlayabilmektedir. Müşterilerle kurulması hedeflenen uzun dönemli ilişkilerin gerçekleşebilmesi için bu müşterilerin ileride ne şekilde davranacaklarını kestirmek gerekir ki, bu da ancak bilgiye dayalı olarak yapılabilir. Şüphesiz ki işletmeler bu tahminleri her zaman olduğu gibi daha önce de sahip oldukları bilgilere dayanarak yapmaktaydılar. Ancak klasik pazarlama anlayışının yerini uzun dönemli müşteri ilişkilerine dayalı anlayışa bırakmasıyla birlikte, işletmelerin verecekleri kararlar da daha karmaşık hale gelmiştir. Sahip olunan bilgilerin ötesinde daha fazla bilgiye sahip olmak ve bu bilgileri ifade ettikleri anlamları bakımından daha da derinleştirmek müşterilerin davranışlarını daha iyi anlayabilmek ve dolayısıyla daha doğru kararlar verebilmek demektir.

---

[27] Bkz. Kaya/ Köymen, Fırat Üniversitesi Doğu Anadolu Araştırma ve Uygulama Merkezi Cilt-6, Sayı 2, Şubat 2008, s.159

[28] Bkz. *Özmen*, *Şule*, http://www.suleozmen.com/teblig_sunumlar/3is_hayati_veri_madenciligi_istatistik.pdf ,

[29] Bkz. *Akgöbek/ Çakır*, Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, 11-13 Şubat 2009, Harran Ünüversitesi, s. 809

[30] Bkz. Carus/Mesut, *Web Kullanım Madenciliği Uygulaması,* II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, MBGAK 2005, 11-19 Kasım 2005, s..121,

İşletmelerin müşterilerle uzun dönemli başarılı ilişkiler kurabilmeleri, bilgilerin keşfedilmesi süreci ile bu bilgilerin pazarlama stratejileri için en uygun biçimde kullanımının doğru bir biçimde bütünleştirilmesiyle olanaklıdır. Böylelikle pazarlamacılar müşteriler hakkında geniş kapsamlı ve isabetli olma olasılığı düşük olan genellemeler yapmak yerine müşterilerinin gereksinimlerini daha yakından tanıma ve anlama fırsatı bulmuş olacaklardır. [31]

Veri madenciliğinde en eski ve yaygın kullanılan süreç modeli CRISP-DM'dir (*Cross Industry Standard Process for Data Mining*)[32]. Bu modelin aşamaları süreç ile ilgili daha bütünsel bir anlayışın sağlanması amacıyla aşağıda özetlenmiş ve şematik olarak gösterilmiştir: [33]

1. İşin Anlaşılması

İlk aşamada, proje hedefleri ve gereksinimleri hakkında bilgiler toplanır. Bu bilgiler, veri madenciliği sorununu ve hedefe nasıl ulaşılacağını açıklamak için kullanılır.

2. Verilerin Anlaşılması

Öncelikle verilerin toplanması gerekmektedir. Bu adım insanlara doğrudan sorarak açık bir şekilde veya davranışlarını gözlemleyerek gizli bir şekilde yapılabilir. Hâlihazırda mevcut olan veriler de bu amaçla kullanılabilir. Reklamcılık şirketleri, veri madenciliği amacıyla kullandıkları çok büyük veri tabanlarına sahiptir. Veriler toplandıktan sonra, fikirler anlaşılabilir ve altkümeler oluşturulabilir.

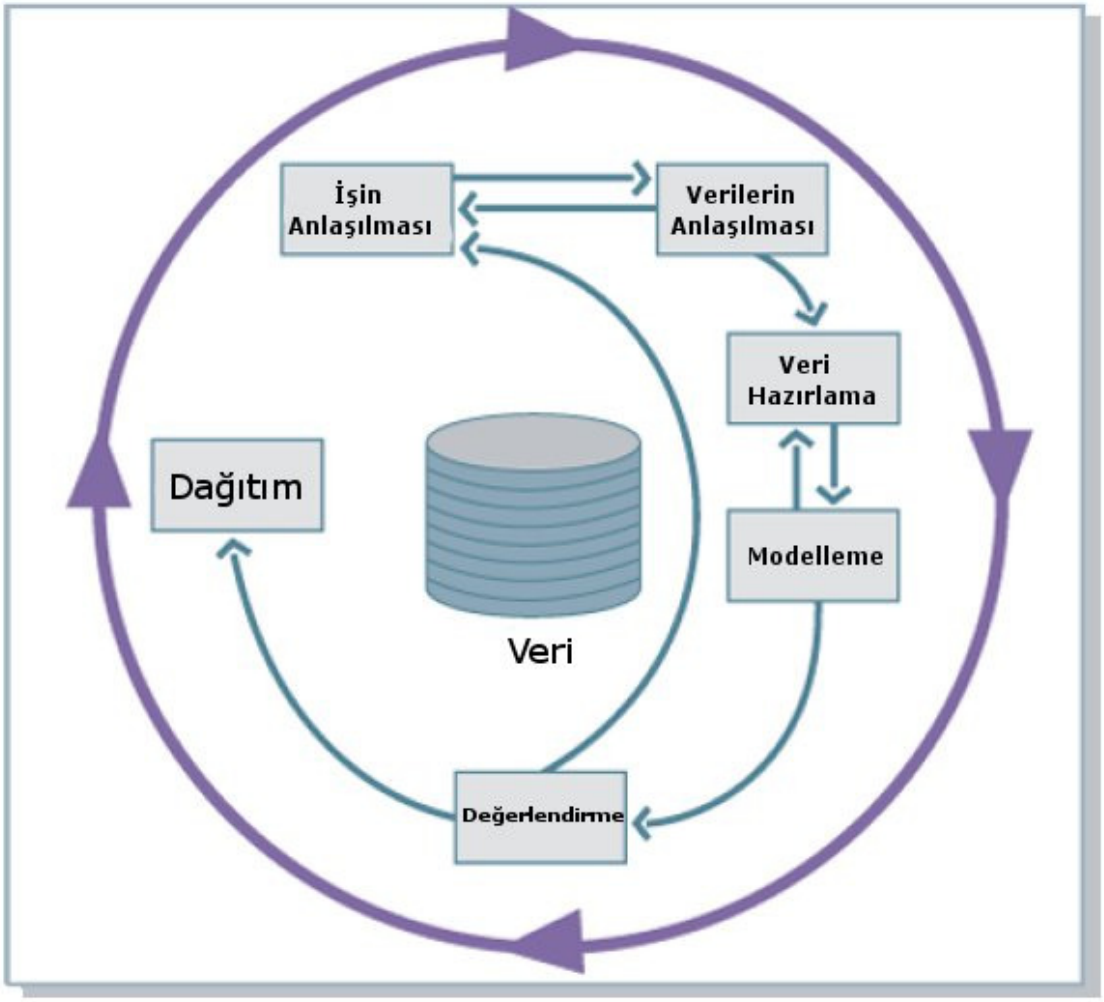
Davranışsal reklamcılıkta, hem kişinin izlenen bilgileri hem de kendisi tarafından verilen bilgiler bir araya getirilir.

---

[31] Bkz. *Özmen., Müjdat,* Eskişehir Osmangazi Üniversitesi İİBF, Yayınlanmamış Doktora Tezi, Haziran 2008, s.49

[32] Bkz. *Anand/Grobelnik ve diğ.,* Tutorial presented on 23 September 2003, http://staff.science.uva.nl/~netten/lerenenbeslissen/extra/kd_standards_final%5B1%5D.ppt

[33] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.13-15,



Şekil 2 CRISP-DM Modelinin Aşamaları

Bkz. http://staff.science.uva.nl/~netten/lerenenbeslissen/extra/kd_standards_ final%5B1%5D.pptm

(erişim tarihi 05.05.11)

3. **Veri Hazırlama**

Ham veriler tekrar düzenlenerek ve sıralanarak son veri seti oluşturulur. Ayrıca, verilerin ön gruplandırılması da bazen faydalıdır.

4. **Modelleme**

Bu aşamada farklı veri madenciliği algoritmaları uygulanır. İhtiyaçları karşılayabilmek üzere daha iyi sonuçlar elde etmek için parametreler sıkça değiştirilir. Veri madenciliğinde, neyin arandığını bilmek gerekli değildir. Veri

madenciliğinin güçlü yanı, yeni ve bilinmeyen ilişkiler veya kalıpları ortaya çıkartabilmesidir. Varsayımlar doğrulanabilir, ama diğer yandan yanlış oldukları sonucuna da varılabilir. Grup profilleme kümelemesinde ise çoğunlukla sınıflandırma ve regresyon teknikleri kullanılır. Kümeleme işlemi, benzer özelliklere sahip gruplar oluşturmaya odaklanırken, sınıflandırmada ön tanımlı gruplar kullanılır. Elde edilen kalıplar daha sonra grupları tanımlamak için kullanılır. Aynı grubun mensupları birkaç ortak özelliği veya davranışsal reklamcılıkta ilgi alanını paylaşırlar.

5. Değerlendirme

Bu aşamada, geliştirilen model değerlendirilecektir. Uygulanan tekniğin istenen sonucu verip vermediğini kontrol etmek için, testler yapılmalıdır. Bu bağlamdaki önemli olgu maskelemedir. Maskeleme, belirli özellikler arasında bağlantı kurulmasıdır; böylece belirgin özelliklerin, hassas özelliklerin göstergeleri olarak kullanılması mümkün olabilir.

6. Dağıtım

Son aşamada süreç ile ilgili eylemler tanımlanmalıdır. Davranışsal reklamcılıkta bu adım, farklı müşteri profil gruplarının, istatistiksel olarak ilgi alanlarıyla uyuşan uygun reklamlarla, ilişkilendirilmesi şeklinde gerçekleştirilir.

Davranışsal pazarlama ile ilgili olarak veri madenciliği devamlılık gösteren bir süreçtir. Devamlı olarak yeni grup profilleri yaratılacak, mevcut olanlar güncellenecek ya da iptal edilecektir. Bir bireyin belirli bir grubun üyesi olarak kategorize edilmesi ve bir ay sonra aynı kişinin toplanan yeni bilgilerin değerlendirilmesi sonucu bir başka gruba aktarılması olasıdır.[34]

[34] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.15

B. Grup Profili Oluşturma

21. yüzyılın iş dünyasında önemli değişimler yaşanmaktadır. İşlem sayısındaki artış ve müşterilerle ilgili olarak kısa zaman dilimlerinde katlanan veri yığını, İnternet pazarlamayı, neredeyse her bir müşteriyi tek bir segment gibi görmemizi sağlayacak araçlarla genişletmiş, güçlendirmiştir. Gelecekte e-pazarlama uygulamaları daha da yenilikçi yöntemlerle devam ederken[35] işletmeler de, toplanan verileri bir veri tabanında toplayarak, müşteri dilimlerini ortaya çıkarmak, bölümlendirmek ve hangi müşteri grubu dilimine hangi pazarlama stratejileriyle hitap etmesi gerektiği hesaplarını yapma gibi işlevleri yerine getirmek durumunda olacaklardır[36].Aslında süreç, çok geniş müşteri kitlelelerinden, giderek birbirine benzeyen tüketici gruplarına, oradan da tek tek profillerini net biçimde çizebildiğimiz bireylere doğru ilerlemektir.[37]

Çevrimiçi Profil çıkartma, tüketicinin internet ortamındaki hareketlerini izleyerek, tüketicinin ilgi alanlarını bulmaya yarayan bir uygulamadır. Çevrimiçi Profil Çıkartmanın temel amacı reklamı, bireylerin ilgi alanlarına uygun hale getirdikten sonra göndermektir. Grup Profili Çıkartma, Çevrimiçi Davranışsal Pazarlamanın içinde yer alan bir uygulamadır. Bu amaca ulaşabilmek için, yayımcılar ve reklamcılar bireylerin İnternet ortamında ki davranışlarını çerezler ve benzeri uygulamalar ile izlemektedirler. Yayımcılar ve reklamcılar genellikle bilgileri bir araya toplarken, çevrimdışı kaynaklardan da yararlanırlar ve bireyleri yaş, gelir, ilgi alanları gibi özelliklere göre sınıflandırılırlar. Reklamcılar bu şekildeki bir ayrıştırma ile özgün tüketici gruplarını oluşturabilirler. Böylece istedikleri hedeflere ulaşma imkânını elde ederler.[38]

Çevrimiçi Reklamcılık endüstrisi, Çevrimiçi Davranışsal Pazarlamanın ve bununla bağlantılı olarak Grup Profili çıkartmanın tüketiciye kaygı vermeyeceğini

---

[35] Bkz. *İyiler*, T.C. Başbakanlık DTM İhracatı Geliştirme Etüd Merkezi, Aralık 2009, Ankara, s 1

[36] Bkz. *Alabay*. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2010. C.15 ss.217, Isparta

[37] Bkz. İyiler, T.C. Başbakanlık DTM İhracatı Geliştirme Etüd Merkezi, Aralık 2009, Ankara s.129

[38] Bkz. *Steindel*. Michigan Telecommunications and Technology Law Review.459, Michigan, *s. 459-460,* 2011, http://www.mttlr.org/volseventeen/steindel.pdf

savunmaktadır; hatta tüketiciye, yayımcıya ve reklam endüstrisine dikkate değer bir yarar sağlamakta olduğunu ifade etmektedirler. Oysa tüketici mahremiyetinin ihlali konusu ile ilgili hukukçular ise Çevrimiçi Davranışsal Pazarlamanın mahremiyete saldırı niteliği taşıdığını ve tüketici beklentileriyle uyum içerisinde olmadığını; hatta ayrımcılık uygulamalarına davetiye çıkardıklarını belirtmektedirler. Bu konudaki sorunların çözümüne ilişkin ilk girişimlerin, ABD'de FTC tarafından yapılmasına rağmen, FTC, endüstriyi, sadece Çevrimiçi Pazarlamayla ilişkili olarak öz düzenleme yapmak konusunda yönlendirebilmiştir. Ancak bu yeterli değildir; ziyaretçilere-tüketicilere, hedeflenmiş reklam yapan ve profilleme yöntemini kullanan web sitelerine ilişkin temel seviyede bir mahremiyet koruması sağlayacak bir mevzuata ihtiyaç vardır.[39]

Kullanıcılar çevrimiçi profillemenin farkına vardıklarında, bu alana olan tepkileri basit bir kaygının ötesine geçmektedir. Bir anket sonuçlarına göre tüketicilerin %72 si çevrimiçi aktivitelerinin izlendiği konusunda "endişeli"dir ve tüketicilerin %93 ü de kuruluşlar tarafından alınan kişisel bilgilerin izin alınmadan kullanılmamaları gerektiğini düşünmektedirler.[40]

Grup profilleme işleminde, sınırlı bilgiden dolayı tümdengelim (*deduction*) genellikle mümkün değildir. Tümdengelimde genel ifadelerden spesifik örneklere doğru gidilir, ancak grup profillemede genellikle bunun tam tersidir. Daha büyük bir grup için kestirimler yapmak amacıyla, spesifik örnekler kullanılır. Dolayısıyla, grup profillemede tümevarım (*induction*) daha sık kullanılmaktadır,
Ayrıca dışa çekim (*abduction*) adı verilen üçüncü bir yöntem de bulunmaktadır.

---

[39] Bkz. *Steindel*. Michigan Telecommunications and Technology Law Review.,Michigan, s.460, 2011, http://www.mttlr.org/volseventeen/steindel.pdf

[40] Bkz. *Steindel*. Michigan Telecommunications and Technology Law Review.459, Michigan, *s. 468,* 2011, http://www.mttlr.org/volseventeen/steindel.pdf

Yani, tümevarım spesifikten genele doğru sonuca varırken, dışa çekim sonuçtan sebebe doğru sonuca varır. Grup profilleme açısından dışa çekim daha az kullanışlıdır, çünkü dışa çekim durumun ne olabileceğini belirtir. [41] [42] [43]

III. Paydaşlar / Oyuncular / Aktörleri

A. Reklam Ağları

Reklam ağları, reklamları barındırmak isteyen bir web sitesi grubu (ağ) ile, bu sitelere reklam vermek isteyen reklamcılar arasında görev yapan bir aracıdır. Örnek vermek gerekirse, *DoubleClick* en çok bilinen reklam ağlarından birisidir. Üye sitelerinin herhangi birine reklam koyabilir ve daha uygun reklamlar koymak için, bu siteleri kullanan kullanıcıların verilerini işleyebilir. Reklam ağları, reklamlarının değerini arttırmak için internet kullanıcılarının davranışlarını analiz ederler.[44] [45]

1. Google

Google Kullanıcı dostu bir sistem oluşturarak ve sürekli genişleyen web sayfa katalogları ile tüketici bilgisini değerli bir meta olarak kullanmaktadır Tüm dünyada çok yaygınlaşmış olup Stallworth'ün ifadesi ile "kanun koyuculara, ticari kuruluşlara ve tüketicilere ve benzerlerine öncülük etmeye kabiliyeti olan kültürel bir simge halini almıştır".[46] Tüketicilerin ilgi alanlarına yönelik yaklaşımıyla *Google*, araştırma sonuçları ve belirli tüketicilere doğrudan hedeflemiş reklamları eş zamanlı olarak yönlendirebilmektedir. Bu durum, *Google*'ın amaçlarından bir

---

[41] Bkz. Tureng Dictionary DCTN, http://tureng.com/search/deduction
[42] Bkz.Tureng Dictionary DCTN, http://tureng.com/search/induction
[43] Bkz. Tureng Dictionary DCTN, http://tureng.com/search/abduction
[44] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis, Information Science, October 11, 2011, s.18-20
[45] Bkz. Orzan, Platon, Lex ET Scientia. Economics Series LESIJ NO. XIX, VOL. 2/2012 s.236,
[46] Bkz. *Stallworth*, Federal Communications Law Journal; Mar 2010; Volume 62 Issue 2 Article 7, s. 465 – 466

tanesinin de, arama sonuçlarıyla alakalı olarak, çevrimiçi reklamcılık yapmak olduğunu açıkça göstermektedir. [47]

Google'ın çevrimiçi gizlilik konusuna ilişkin yasaya uygun bakış açılarını içeren web siteleri mevcuttur. Gizlilik politikalarının daha anlaşılabilir, daha açık, dürüst hale gelmesi ve bu sayede ve tüketicinin daha iyi eğitilmesiyle *Google* ve diğerleri, FTC'nin şeffaflık konusundaki isteklerinin üstesinden gelebilme konusunda başarılı adımlar atabilmişlerdir. Bu politikanın FTC'nin gereksinimlerini aşamaya yardımcı olmasının yanı sıra yanı sıra, çevrim içi reklamcılık uygulamaları hakkında az miktarda da olsa bir kontrol mekanizması geliştirilmesine önemli katkısı olmuştur.:[48]

2. Yahoo

Yahoo da *Google* gibi bir arama motoruna (*Google*'a nazaran daha az bir yoğunluk içinde olmasına rağmen), reklam ağına ve reklam değişim (*Ad Exchange*) ortamına sahiptir. Ayrıca bir portal ve bir yayımcı olma özelliklerini taşır.[49]

Yahoo, *Yahoo Advertising* adında kendine bağlı bir şirkete de sahiptir. Ana sayfalarında BT'yi (*Behavioral Tracking* - Davranışsal İzleme) kullanarak doğru zamanda doğru müşterilere ulaşabildikleri ifade edilmektedir. [50]

B. Yayıncılar

Günümüzde ticari web siteleri ve bloglar veya topluluklar gibi diğer siteler, sitelerine üçüncü kişi içeriği ekleyerek para kazanmaktadırlar. Bu tür siteleri ziyaret eden kullanıcılar ise, kaç üçüncü taraf şirketin, kendileri hakkında bilgi edindiğini genellikle bilmemektedir. Bu konuda iki. örnekten ilki, *Levis.com*'u araştıran

---

Bkz. *Stallworth*, Federal Communications Law Journal; Mar 2010; Volume 62 Issue 2 Article 7, s.470

[48] Bkz. *Stallworth*, Federal Communications Law Journal; Mar 2010; Volume 62 Issue 2 Article7, s. 470- 484

[49] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 28, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1 erişim 12.05.2011

[50] Bkz. *Yahoo, B. Targetting,* http://advertising.yahoo.com/products-solutions/behavioral-targeting.html (erişim tarihi 12.05.11)

Catherine Dwyer'ın yaptığı bir vaka çalışması, ikincisi ise Greg Conti'nin msnbc.com analizidir. [51]

1. Levis.com

Dwyer öncelikle, *Levis.com'un* gizlilik politikasını incelemiştir. Bu politika metninde kişisel bilgilerin nasıl ele alınacağı ve bu bilgilerin, müşterinin rızası olmadan paylaşılmayacağı belirtilmektedir. Kişisel olmayan bilgilerin toplanması ise ayrı bir kategoride açıklanarak *Levis.com*'un müşteri trafiği kalıpları ile site kullanımı ve diğer bilgileri topladığını belirtilmiştir. Ayrıca, gizlilik politikasında biri reklamcılık amacıyla web sitesi ziyaretleri hakkında anonim bilgileri toplayan, diğeri de sitenin kullanımını hesaplayan iki tane üçüncü taraf şirketten bahsedilmektedir. [52]

Dwyer, *Levis* ana sayfasının içeriğini kaydetmek için bir *Firefox* eklentisi kullandığında bulduğu şeylerden biri, *Levis* ana sayfasının, sekiz reklam şirketine link gönderen dokuz farklı *web* işaretçisi içermiş olması idi. Müşterileri takip etmek için sekiz işaretçi; ve tanımlı verileri toplamak için bir işaretçi kullanılmakta idi. Yukarıda bahsi geçen gizlilik politikasında bu reklam şirketlerinin hiçbirinin adı geçmiyordu. Tüm işaretçilerin bir P3P politikası (veri toplama işleminin amacını beyan etmek için web sitelerine uygulanan bir protokol) olduğu görülmekte idi. Bu işaretçilerin P3P'sine göre, üç işaretçi verileri IND (*indefinite* – belirsiz) bir süreyle tutacak; diğer altısı ise verileri BUS (*Business Applications* - İş Uygulamaları) için toplamakta idi.

---

[51] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.22

[52] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.22

Web işaretçisi	***Bağlantılı şirket***	***P3P (Privacy Proyection Project) var mı?***	***Tanımlı veriler topluyor mu?***	***Takip için kullanılıyor mu?***	***Veri Saklama***
tracking.searchmarketing.com	*Channel Advisor*	Evet	Evet	Evet	IND
beacon.afy11.net	*Adify*	Evet	Hayır	Evet	IND
leadback.advertising.com	*Advertising.com*	Evet	Hayır	Evet	BUS
ad.yieldmanager.com/pixel?id= 164939&t=2	*Right Media*	Evet	Hayır	Evet	BUS
bh.contextweb.com	*Context Web*	Evet	Hayır	Evet	BUS
ad.yieldmanager.com/pixel?id= 101690&t=2	*Right Media*	Evet	Hayır	Evet	BUS
bp.specificclick.net	*Specific Media*	Evet	Hayır	Evet	BUS
a.tribalfusion.com	*TribalFusion*	Evet	Hayır	Hayır	BUS
gsiclevi.112.2o7.net	*Omniture*	Evet	Hayır	Evet	IND

Tablo 3 Levis.com: Web işaretçileri [53]

(Bkz. http://csis.pace.edu/~dwyer/research/AMCIS Dwyer2009.pdf , s.8)

Sonuçta, söz konusu araştırma P3P şartnamesine göre, iş uygulamaları için veri toplayan şirketlerin, bunu sağlayıcının gizlilik politikasında belirtmek zorunda olmalarına rağmen Levis'ın bunu yapmadığını göstermektedir. Bu araştırma sadece bir *web* sitesini incelemiştir, ancak bu değerlendirmeden hareketle, ticari web sitelerine takip içeriğinin eklenmesinin yaygın bir uygulama olduğu varsayılabilir. [54]

2. Msnbc.com

Msnbc.com web sitesi, 10 farklı şirketin 16 tane üçüncü taraf web alanını içermektedir. Şekil 2.5'te msnbc.com'daki üçüncü taraf *web* alanlarının bir tablosu verilmektedir. [55]

Kullanıcıların sadece tek bir *web* sitesini ziyaret etmesiyle takip edilmelerinin boyutu, oldukça büyük olabilir. *Msnbc.com*'u ziyaret ettiğinizde, 16

[53] Bkz. *Dwyer*, Catherine, , Proceedings of the Fifteenth Conference on Information Systems, San Francisco, California, August 2009, s.8, http://csis.pace.edu/~dwyer/research/AMCIS Dwyer2009.pdf

[54] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.22

[55] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.23

kayıt dosyası oluşturulmaktadır. Bir web sitesinin ziyaretçilerinin takip edilmesi ve bu bilgilerin çok sayıda üçüncü taraf şirketlere yayılması yaygın bir uygulama gibi gözükmekte ve ziyaretçilerin çoğunun bu üçüncü taraf şirketleri bilmediği anlaşılmaktadır. Bu şirketler de genellikle arka planda çalışmaktadırlar.[56]

Alan Adı	Notlar
a365.ms.akamai.net a509.cd.akamai.net	Akamai.com'a ait bir *web* alanı, medya içerikleri için bir ikizleme hizmeti
ad.3ad.doubleclick.net	Google'ın satın aldığı dijital pazarlama hizmeti
amch.questionmarket.com	Çevrimiçi anketlerin koyulduğu *web* sitesi
c.live.com.nsatc.net c.msn.com.nsatc.net rad.msn.com.nsatc.net	Ağ oluşturma ve barındırma sağlayıcısı *Savvis Communications*'a kayıtlı
context3.kanoodle.com	Arama odaklı sponsorlu *link*ler hizmeti
global.msads.net.c.footprint.net hm.sc.msn.com.c.footprint.net	Büyük ağ sağlayıcısı *Level 3 Communications*'a kayıtlı
msnbcom.112.2o7.net	*Web* analiz ve çevrimiçi iş optimizasyonu sağlayıcısı Omniture'e kayıtlı
prpx.service.mirror-image.net wrpx.service.mirror-image.net	Kayıtlı içerik teslim, veri akışı ortamı ve web programlama hizmeti Mirror Image Internet'e kayıtlı
switch.atdmt.com view.atdmt.com	Dijital pazarlama şirketleri ana kuruluşu *aQuantive*'e kayıtlı
www-google-analytics.1.google.com	*Google*'ın sağladığı trafik ölçüm ve interaktif raporlama hizmeti

Tablo 4 Msnbc.com'a girildiğinde ziyaret edilen üçüncü taraf siteler

(Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.21-23

[56] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.21-23

C. İnternet Servis Sağlayıcıları (ISP)

Bu ekosistemin içinde İnternet Servis Sağlayıcılarının (ISP) görevi gerçekten çok mühimdir. İnternet Servis Sağlayıcılar bu sistemde ki manzarayı değiştirecek bir güce sahiptirler. ISP'ler çevrimiçi reklamcılık ekosistemine katılmıyor gibi gözükseler de bazı durumlar da yayımcı sitelerin reklamlarını kendi seçtikleri reklamlar ile değiştirmektedirler. Buna ek olarak ISP'ler web sitelerine reklam yerleştirme işini yönetme girişiminde de bulunmuşlardır.[57]

ISP'ler, genelde çevrimiçi satın alma işlemlerinde, banka hesaplarına girişlerde ve diğer hassas bilgiler içeren konularda kullanılan şifreli iletişimler hariç olmak üzere kendi kullanıcılarının bunların dışında kalan diğer tüm irtibatlarını, bağlandıkları web sitelerini ve bu sitelere gönderdikleri bilgilerle geri bildirim bilgilerini görebilmektedirler. Ayrıca bazı *web* siteleri ile kısıtlı olanağa sahip olan reklam ağları ve bazı yayımcılardan farklı olarak, ISP'ler kullanıcılarının adlarını ve sokak adreslerini de bilmektedirler. Bu da ISP'lerin, kullanıcıları hakkında topladıkları veriler ile diğer kaynaklardan toplanılan verilerin çapraz eşleştirilmelerini olanaklı kılmaktadır. Tek kısıtlılık noktası ise ISP'lerin kendi ağlarında akış halindeki çok büyük çapta olan verileri depolama kabiliyetine ilişkindir. Bununla birlikte ISP'ler, bu veriyi filtre ve analiz eden "Derin Veri Analizi" sistemini gittikçe artan bir şekilde dikkate almaktadırlar. ISP'lerin davranış tarzıyla ilgili olan güncel kısıtlılıklar ise yasal ve siyasaldır. Bu kısıtlılıklar söz komusu olmasa idi, ISP'ler, kişilerin, sokak adresleriyle eşleşen ve daha sonra sokak adresleri bazındaki satın alma faaliyetlerine bağlı olan diğer veritabanları ile ilişkilendirilebilecek davranışsal profillerini çıkartma olanağına sahip olabilirlerdi. ISP'lerin izlemesinden kaçınmak için veri akışını "*Tor*"[58] ve benzeri bir takım

---

[57] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 26, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1 erişim 12.05.2011

[58] Bkz. *TOR,* http://www.torproject.org

şifreli *Proxy*'lere yönlendirmek gibi yöntemler mevcuttur. Ancak bunlar çok tanınan ve çok kullanılan yöntemler değildir.[59]

ISP'ler, *web* siteleri üzerinden, şifrelemeli uygulamalar (örneğin, çevrimiçi satın alma, hasta bilgileri veya finansal bilgiler gibi hassas işlemlerde) haricindeki bütün tarama kayıtlarını inceleyebilmektedirler. [60]

ISP'ler diğer reklam ağlarına, yayımcılara ve reklam ajanslarına kıyasla, kullanıcılarının bilgi akışlarına dair eksiksiz bir görüş alanına sahiptirler (yine kullanıcıların yönettiği finansal hesaplar veya çevrimiçi kredi kartı ödemeleri gibi şifrelenmiş haberleşmeler istisna olmak üzere) . [61]

Temel sorun ISP'lere, taşıdıkları paket içeriklerine, ne kadar derinlemesine inceleme izni verileceğine ilişkindir. [62]

Temel sorun ISP'lere taşıdıkları paket içeriklerine ne kadar derinlemesine bakabileceklerine müsaade edilebileceğine ilişkindir - davranışsal reklamcılık, bu noktada düzenleyici ve politik konularla ilişkilendirilmektedir; bu özellikle de, ağ tarafsızlığı ile telifli eserlerin içeriklerinin yasal olmayan dağıtımının denetlenebilmesi için derin veri analizinin kullanımı için söz konusudur, Her iki tartışmanın da kapsamında, hangi ISP'nin kendi ağlarından geçen trafik akışını hangi boyutta inceleyebileceği vardır. Bir tarafta ISP'lerin, kendilerine gönderilen paketlerdeki bilgilerden kendilerine en az gerekecek miktar kadar bilgiyi – kaynak dosya ve hedef IP (Internet Protokol) adresi - incelemeye izinleri olması gerekliliği tartışılırken; diğer tarafta bazı ISP'ler de, içerik sağlayıcılara belirli çeşitlerde içerik

---

[59] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 48, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1

[60] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 53, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1

[61] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 50, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1

[62] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 61, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1

ihtiva eden geliştirilmiş hizmetleri (örneğin daha güvenilir görüntü akışı gibi) sunabilecek kabiliyete sahip olmayı istemişlerdir.[63]

IV. İzleme Araçları / Teknikleri / Yöntemleri

A. Çerezler

Bilgisayarın faresinin tuşuna her bir tıklayışta ve her bir web sitesine erişim sağlandığında, kendi kişisel bilgilerinizi, kredi kartı numaralarınızı, sosyal güvenlik numaralarınızı, şifrelerinizi ve sağlık bilgilerinizi girdiğinizde, bu bilgilerinize üçüncü kişiler tarafından ve sizin rızanız olmadan, olası bir erişim potansiyeliyle karşı karşıya kalırsınız. [64]

Genel anlamı ile web siteleri tarafından, interneti daha kolay ve daha hızlı hale getirmek maksadıyla faydalı bilgileri depolamak amacı ile kullanılan, küçük boyutlu dosyalara çerez adı verilmiştir. Bu dosyalarla aldığımız ve ilgilendiğim iz reklam türleri de anlaşılabilmektedir. Greg Conti "*Googling Security: How Much Does Google Know About You*" adlı kitabında şöyle demektedir; "çerezler, bilim adamlarının doğa belgesellerinde yabani hayvanlara attıkları takip okları gibidir". Bir bakıma çerezler de davranışsal reklamcılık bağlamında tam olarak aynı şeyi yapmaktadır. Farklı çerez türleri olmakla birlikte, ancak genelde kalıcı ve oturum çerezleri olmak üzere iki tür kullanılmaktadır. Oturum çerezleri takip amacıyla kullanılmaz, çünkü sadece kısa bir süre kalırlar. Oturum çerezinin tipik bir örneğini, internet bankacılığı işlemi yaparken görebiliriz. Kullanıcı hesabına her giriş yaptığında, bir oturum çerezi kullanılır. Oturum çerezleri etkileşimi kolaylaştırır, çünkü bu çerez olmadan, kullanıcı her yeni bir talep gönderdiğinde tekrar giriş yapmak zorunda kalır. Kalıcı çerezler, adından da anlaşılacağı üzere, uzun süre var olurlar. Dolayısıyla, genellikle kullanıcıları takip etmek için kullanılırlar, çünkü kullanıcı bu çerezi yayınlayan web sitesini her ziyaret ettiğinde, *web* sunucusuna

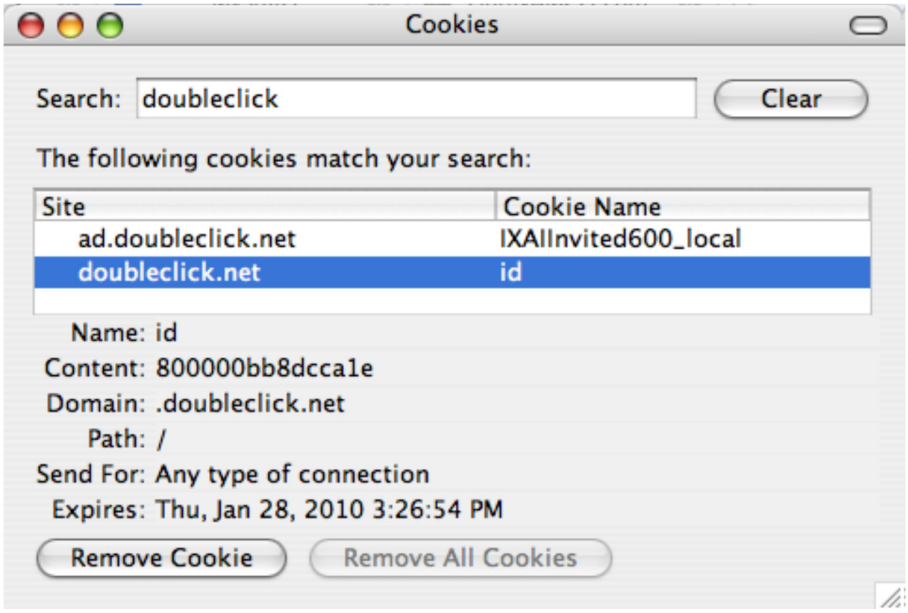
---

[63] Bkz. *Smith-Grieco*, Master of Science in Technology and Policy at the Massachusetts Institute of Technology, February 2010 s 61, http://dspace.mit.edu/bitstream/handle /1721.1 /59567/668246989.pdf?...1

[64] Bkz. *Arrington*, JICLT Journal of International Commercial Law and Technology, Vol. 8, No.1,, January 2013, USA, 2013 p.13

giriş yapacaktır. Kullanıcının, reklam ağının web sitesini ziyaret etmek gibi bir niyetinin olmadığı durumlar haricinde, reklam ağları tarafından hazırlanan çerezler için de aynısı geçerlidir. Bu tür çerezler, TPC (*Third Party Cookies* - üçüncü taraf çerezler) olarak adlandırılır ve web siteleri çoğunlukla reklam şirketlerinin gömülü içeriğini taşıdıkları için yayınlanırlar. Bir çerezin yapısı, *DoubleClick* tarafından hazırlanmış örnek baz alınarak aşağıda açıklanmaya çalışılmıştır. [65]

Tüm çerezler aynı yapıya sahiptir; ad, içerik, alan adı, yol, gönderilen ve bitiş tarihi alanı vardır. Davranışsal reklamcılıkta, içerik alanı bunlardan en önemlisidir, çünkü bir tanımlayıcı içerirler. Greg Conti kitabında örneğin Google çerezlerinin 2 yıl sonra sona erdiğini, *Yahoo* çerezlerinin ise 29 yıl sonra sona erdiğini, ancak *Google* çerezlerinin süresinin *Google*'a her giriş yapıtlığında otomatik olarak uzatıldığını belirtmektedir. İnternet kullanıcılarının *Google*'ı iki yıl içinde birden çok daha fazla kez ziyaret ettiğini varsayabiliriz ve dolayısıyla, bu çerez tarayıcı tarafından hiçbir zaman atılmayacaktır. [66]

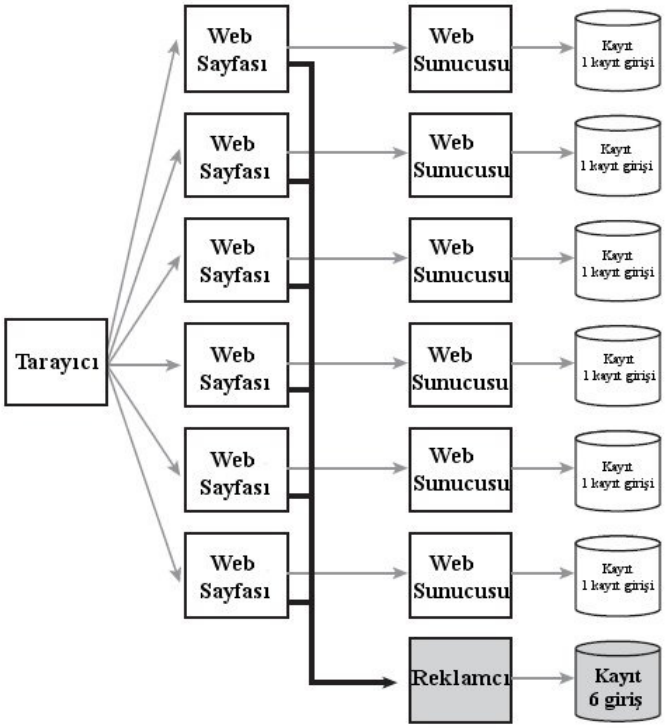


[65] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.24

[66] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.25

Şekil. 5 Reklam şirketi DoubleClick (Google) tarafından hazırlanan çerez örneği.[67] (Bkz. *Nolet,* http://www.mikeonads.com/2007/02/27/whats-really-in-my-cookie-cache/)

Gömülü içerik ve reklamcının sağladığı ilgili çerez yüzünden, bir kişi birden çok siteyi ziyaret ettiği zaman, reklam şirketleri o kişinin davranışını gözlemleyebilmektedir. Aşağıdaki şekilde de bir reklamcının çapraz site takibi gösterilmektedir. [68]



Şekil 6 Bir reklamcının çapraz site takibi

(Bkz. *Van Bebber, g,* Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.26)

Şekilde görüldüğü gibi, farklı web sitelerinin 6 kez ziyaret edilmesi ile reklam ağının sunucusunda 6 kayıt girişi oluşturulmaktadır, çünkü doğrudan ziyaret

[67] Bkz. *Nolet,* http://www.mikeonads.com/2007/02/27/whats-really-in-my-cookie-cache/
[68] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.25

edilen tüm web siteleri, önce de işaret edildiği gibi, reklam ağının gömülü içeriğini taşımaktadır..[69]

Yüksek derecede gizlilik ayarının yapılması halinde bile, şirketler; çerez dosyaları sayesinde kullanıcıları tespit edebilirler; ve bu tespitleri internet kullanıcılarının internet tarama geçmişlerine erişerek temellendirebilmektedirler. Yüksek derecede gizlilik ayarı yapmış kullanıcılar, şirketlerin kullanıcıları tespit edebilmek için daha çok araştırmasına neden olarak onların işlerini zorlaştırırlar; ancak bu durum çevrimiçi reklamcılık yapmalarını engellemelerine yeterli değildir. [70]

Bir internet kullanıcısı, üçüncü şahısların, tarayıcı geçmişi bilgilerine erişmesini engellemek için, tarayıcı çerezlerini silebilir veya bloke edebilir. Bununla birlikte, bir internet kullanıcısı tarayıcı çerezi sildiğinde, kullanıcı bilgisayarına önceden, kullanıcının bilgisi dışında yerleştirilmiş bir *flash* çerez, tarayıcı çerezi, kullanıcıya haber vermeden ve onun rızasını almadan, tekrar oluşturmaktadır.[71]

B. Web İşaretçileri (Web Beacons)(JavaScript dili ile yazılmış)

Colin Bennett'a göre, *web* böceği veya *web* işaretçisi, *web* sayfasını veya e-posta iletisini kimin okuduğunu takip etmek üzere tasarlanmış olan, bir web sayfasındaki veya e-posta iletisindeki bir grafiktir. *Web* işaretçileri genellikle görünmez, çünkü renksiz ve 1x1 piksel boyutundaki grafiklerdir. Genellikle *JavaScript*'te yazılırlar. *Web* işaretçileri, aslında sayfa yükleme hızlarını arttırmak için tasarlanan tarayıcının önbelleğinde yer alırlar. *JavaScript*'in kullanılması, web

---

[69] Bkz. *Van Bebber*, *g,* Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.24-26

[70] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, p.44

[71] Bkz. *Arrington*, JICT, Journal of International Commercial Law and Technology, Vol. 8, No. 1, 2013 s.5, s.16

işaretçisinin istemiyle birlikte sunucuya kullanıcının ekran boyutu gibi ilave bilgiler gönderme ihtimalini sunar. [72]

Bir e-posta iletisine eklenebilecek olan web işaretçisi kodunun[73] bir örneği aşağıda verilmektedir:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<HEAD></HEAD>
<BODY>
<IMG height=1 src="http://www.adoko.com/mybug.gif" width=1 target="_blank">
This email tests the use of a Web Bug.
</BODY>
</HTML>
```

Eklenen 1x1 boyutundaki görüntü, kullanıcı e-posta iletisini okurken yüklenir. Eğer bir *web* işaretçisi kullanılarak birden çok kullanıcı takip edilmek isteniyorsa, örneğin ad alanına benzersiz bir tanımlayıcı eklenmesi yeterli olabilir. Web sunucusunun kayıt dosyasına baktığımız zaman ise aşağıdaki girdiyi görürüz:

```
2003-06-02 09:39:13
W3SVC110 NTXPW04 212.227.124.8
GET /mybug.gif - 80 -
212.24.161.236 HTTP/1.0 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
```

E-postayı okuyan kullanıcı, görüntüyü 09.39:13'te yüklemiştir. Ayrıca, IP adresi ve tarayıcı türü de kaydedilmektedir.[74]

C. Facebook

Body ve Ellison (2007 pp210-130) sosyal iletişim sitelerini şöyle tanımlamaktadırlar: "bireylerin, sınırları belirlenmiş bir sistem içerisinde, halka tamamen veya kısmen açık profiller oluşturmasını sağlayan, düzenli bir şekilde

---

[72] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.27

[73] *Adoko,* http://www.adoko.com/webbugs.html

[74] Bkz. *Van Bebber*, *g,* Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, p.26-27

birbirine bağlı olan liste halindeki kullanıcıların birbirleriyle bağlantılarını paylaştıkları ve paylaştıkları bağlantıları ayrıntılarıyla inceleyebildikleri veya bağlantı kurduğu kullanıcıların başkalarıyla kurdukları bağlantıları da sistem içerisinde inceleyebildikleri internet temelli bir hizmettir". Bu tür bağlantıların yapılış tarzları ve adları, siteden siteye değişiklik gösterebilmektedir. Yine aynı yazarlara göre sosyal ağların özelliklerinden biri de tanıdığınız kişilerle kolayca etkileşim içine girebilmenizin yanı sıra bunu size tamamen yabancı olan kişilerle de yapabilmenizdir. Bir sosyal ağda profil oluşturma işlemi, yaş, lokasyon, ilgi alanları, işyeri ve çoğu zaman siteye, kendinize ait olan bir resim yükleme gibi temel bazı bilgilerin paylaşılmasıyla gerçekleşir. Profiliniz tamamlandıktan sonra, sistemdeki tanıdığınız veya tanımak istediğiniz kişilere bakmak ve kendi sosyal ağınızı oluşturmaya davet edilirsiniz. Kendi ağınıza eklediğiniz kişiler, sosyal ağa nasıl girdikleriyle alakalı olarak farklı isimlerde olabilirler. En popüler terimler "arkadaşlar" "bağlantılar" "takipçiler" ve "hayranlar"dan oluşmaktadır. Kaç kişinin sosyal ağları kullandığıyla ilgili olarak gerçekten az sayıda araştırma yapılmıştır ama pazarlama ile ilgili araştırmalar göstermektedir ki sosyal ağlara olan ilgi giderek artmaktadır. [75]

Bir sosyal paylaşım sitesi olan *Facebook* ilk kez 2004 Şubat ayında uygulanmaya başlanmıştır. Haziran 2014 itibariyle *facebook*'un yedi binden fazla çalışanı (*http://newsroom.fb.com/company-info/*) ve 600 milyondan fazla günlük kayıtlı kullanıcısı (Haziran 2014 ortalaması) olmuştur. Kullanıcılar profil oluşturmaya, arkadaş eklemeye, veri veya resim paylaşmaya, tartışmaya, birbirlerine e-posta göndermeye ve daha birçok imkan sunan aktiviteleri kullanmaya davet edilmişlerdir. Bu sosyal iletişim ağında kişiler ilgi alanlarıyla alakalı olan bir gruba katılabilir ve ilgilendikleri haberleri izlemeye devam edebilirler. En az 13 yaşını doldurmuş olduğunu beyan eden herkes, *facebook*'a üye olabilmektedir. [76]

---

[75] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.2

[76] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.2

Facebook etkili bir pazarlama platformudur; çünkü ağ bağlantılı iletişim zaten meydana gelmiş durumdadır. Bu da şirketlerin, kolay bir şekilde bu sitede görünmek suretiyle bu platformda yapılan konuşmalarla bütünleşmesini sağlamaktadır. *Facebook*, ürünlerin ve markaların incelenmesi için yeni bir yol bulmuş, bunu tamamlamış ve devreye sokmuştur. Bu yol sadece araştırma ve satın alma bedeli aşamasını başka bir boyuta dönüştürmekle kalmamış, aynı zamanda alış veriş yapan kişilere, sevdikleri ürünleri ve mağazaları desteklemek imkânı tanıyan bir platform meydana getirmiştir. Örneğin ürünlerle ilgili övgü dolu sözler veya eleştiri yazıları hayran sitesinde veya bir uygulamanın içerisinde görülebilmektedir.[77]

The Wall Street Journal'da bildirildiği üzere, *facebook* uygulamaları, kendi kullanıcılarının kimlik bilgilerini yine kendi kullanıcılarına bir bildirim yapmaksızın, reklamcılık ve takip işi yürüten kuruluşlara göndermektedir. Bu konu, *facebook* uygulamalarını kullanan milyonlarca kişiyi etkilemektedir. Rapora göre bu konu, kendi profillerini *facebook*'un en katı gizlilik ayarlarına göre ayarlamış olan kullanıcıları bile ilgilendirmektedir.

Facebook çok büyük miktarda bilgi içermektedir ancak bu devasa bilgiye oranla gizlilik seçenekleri çok zayıf kalmaktadır..[78]

Facebook'ta davranışsal reklamcılık, başka sitelerde rastlanmayacak bir başka avantajı gündeme getirmektedir. "Beğen" ("*Like*") tuşunun kullanılması, tüketiciler ile işletmeler arasındaki olan bağlantının derinleştiği ve yoğunlaştığına ilişkin bir taahhüt niteliğindedir; bu da bir topluluk kurulmasına yardımcı olmaktadır. (www.facebook.com/advertising) . Kullanıcı "Beğen" tuşuna bir kez bastığında, beğendiği kuruluşla ilgili olan bilgileri "Başlıca Haberler" bölümünde görme imkânına sahip olur ki, bu bölüm *facebook* sisteminde, oturum açıldıktan

---

[77] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.2-3

[78] Bkz.*Martinez*, http://www.destinationcrm.com/Articles/Editorial/Magazine-Features/Facebook-The-Black-Sheep-of-Online-Behavioral -Advertising-72863.aspx, January 2011 p.28, 2011

sonraki ana sayfada yer almaktadır. Daha sonra bu reklam, kullanıcının, kendisini eklemiş olan ve kendisinin başlıca haberler bölümüne abone olan bütün arkadaş

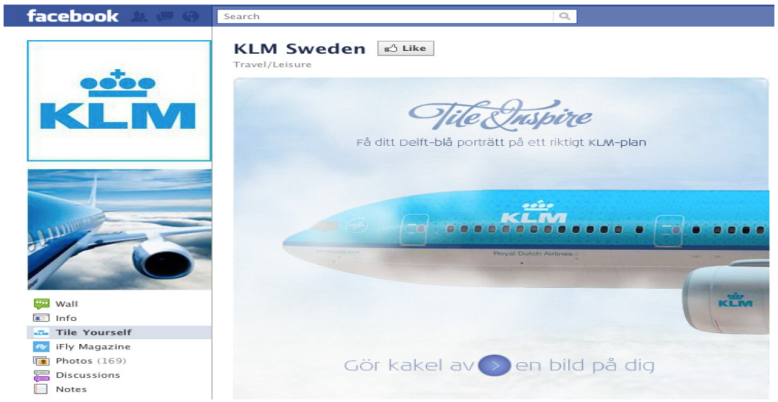
Facebook, sadece kullanıcıları takip edebilecek güçte değil, aynı zamanda takip bilgilerini hesap bilgileriyle bir araya getirerek oldukça zengin kişisel profiller oluşturabilecek yapıdadır. Çoğu *Facebook* kullanıcısı, *Facebook*'a girerken asıl isimlerini kullanmaktadır. Bu noktada önemli soru şudur: *Facebook*, kullanıcılarına hedefli reklamlar sunmak için bu veri kaynaklarını bir araya getirirken kişisel verileri kullanmakta mıdır? [79]

KLM (*Royal Dutch Airlines*) İsveç örneği: Aşağıdaki şekilde (*Şekil 7*) dinlence ve seyahat endüstrisinde faaliyet göstern KLM İsveç'in facebook ortamındaki reklam ilanı gözükmektedir. KLM, seyahat etmekle ilgilenen bireyleri hedefleyebilmek için facebook vasıtasıyla davranışsal reklamcılığı kullanmaktadır. KLM'nin, bu konuyla ilgili başlangıç noktası, , seyahat kavramını, kendi facebook profillerinde ilgi odağı haline getirmek olmuştur. Aşağıda reklamların nasıl uygulandığı konusu, resimlerle beraber anlatılmaktadır. *Facebook* sitesinde gezindiğinizde, sayfanın sağ tarafında, üç veya dört farklı reklamla karşı karşıya kalırsınız. [80]

Şekil 7 KLM İsveç tarafından yapılmış ve facebook sayfasında yer alan bir davranışsal reklamcılık örneğinin ekran resmi
(Bkz. https://www.facebook.com/klmsweden)

[79] Bkz. *Facebook,* http://developers.facebook.com/blog/post/108/
[80] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.34

İsveç'te ikamet eden ve muhtemelen uçuşlarla ilgilenen birisi, evine dönmek veya çevredeki ülkeleri ziyaret etmek amacıyla reklamın üzerine tıkladığında neler ile karşılaşmaktadır? [81]



Şekil 8 Facebook'da KLM sayfası
(https://www.facebook.com/klmsweden)

Reklama bir kez daha tıklama yaptığınızda, kendiliğinden, kuruluşun; facebook'ta ki hayran sayfası ekranda belirmektedir; bu sayfa, kuruluşun alışılmış resmi internet sitesinden farklılıklar içermektedir. Bireylerin, bu sayfaya yönlendirilmesindeki amaç bireylere "bu sayfayı beğendim" beyanında bulunmalarının sağlanması ve dolayısıyla sürekli olarak, beğendikleri kuruluşla ilgili reklam faaliyetlerinden haberdar olmalarıdır. Kuruluş, kendi *facebook* duvarında, uçuş fiyatları hakkında bilgileri veya aşağıdaki örnekte görülebileceği gibi bireylerin bir KLM uçağı üzerinde kendi tasarladıkları resimlerin yer alması gibi fırsatları da yayınlayabilmektedir. [82]

[81] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.34
[82] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.34

Şekil 9 Facebook'da KLM hayran (fan) sayfası
(https://www.facebook.com/klmsweden

"Yaptığınız bir resim gerçek bir KLM uçağının üzerinde yer alabilir! Esin veren bir slogan ile Delft Mavisi çini tasarımınızı yaratmaya davetlisiniz! Bu tasarımınız bir KLM Boeing 777-200 ün gövdesi üzerinde yer alabilir. http://ow.ly/4ynKx i tıklayarak katılınız!"

Kuruluşlar tarafından yapılan bu tür yayınlar ile hayran kitlesi, kuruluş ile doğrudan bir etkileşim kurma imkânına ve duygularını ifade edebilme olanağına sahip olmaktadır. Bu durum, tüketiciler ile kuruluşlar arasında tartışmaya açık ve özgün bir platform oluşturmaktadır. İnternet ağı, bireyleri bir araya getirme ve sanal topluluklar kurulması konusunda yardımcı bir etkiye sahiptir. Üstelik reklam mesajlarının daha hızlı ve geniş bir ölçü çerçevesinde yayılmalarını sağlamaktadır.

Ayrıca kuruluşun *facebook* sayfasında şirketle ilgili bir takım bilgiler verilmektedir ve kullanıcıların istedikleri zaman resmi internet sitesine yönelebilecekleri bir bağlantı bulunmaktadır. KLM örneği ile, tüketicinin bir veya daha çok sayfanın üzerinden geçerek yoluna devam etmesi şeklinde tanımlanan tıklama teorisi arasında bir bağlantı kurmak mümkündür. Ve kuruluşların da, kendi web sitelerine hayran olan kullanıcıların tıklama davranışlarından kolayca faydalanabileceği söylenebilir.[83]

"Beğen" tuşunun kullanılmasıyla birlikte, kullanıcıların, ne ile ilgilendiklerini anlamak gerçekten kolaylaşmıştır. Örneğin, hangi istikamete olan uçuşların veya kuruluş tarafından sunulan hangi hizmetlerin daha çok ilgi çektiği anlaşılabilmektedir. Ayrıca " Beğen " tuşu ile tanımlanabilen tıklama davranışının haricinde, kullanıcıların hayran sitesinde hangi bölümleri ziyaret ettikleri başka yollarla da bulunabilmekte ve dolayısıyla kullanıcıların neyle ilgilendikleri konusunda çıkarımlar yapılabilmektedir.[84]

Gizlilik Konusu: E-Gizlilik olarak ta bilinen çevrimiçi gizliliği: "Bireyin çevrim içi ortamda, izlenmeden, takip edilmeden, kısıtlanmadan hareket edebilme ve kişisel kimliğini teşhis edebilecek bilgilerini kendi rızası olmadan toplanmaktan, başkalarına dağıtılmaktan alıkoyabilme hakkıdır" şeklinde tanımlayabiliriz. Kullanıcılar, kendi lokasyonları, cinsiyetleri ve ilgi alanlarıyla uyumluluk gösteren reklamlarla karşılaştıkları zaman, bunu internette sahip olmaları gereken haklardan biri olan, özel hayatın gizliliğine karşı bir ihlal olarak algılayabilmektedirler. Bu konuda daha fazla bilinçlendirme sağlamak için, facebook gibi çok yönlü sitelerde, gizlilik bölümleri oluşturulmaktadır. [85]

Yüksek gizlilik ayarları benimsendiğinde, reklamcıların, bireylere, onların kişisel verilerinden oluşturduğu bilgiler ile davranışsal hedefleme yapamayacağı

---

[83] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.35

[84] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.35

[85] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.15

zannedilmektedir ve bu ayarlar benimsendiğinde, bireylerin facebook'ta yayınladığı bilgilere sadece kullanıcının listesindeki arkadaşlarının ulaşması sağlandığı varsayılmaktadır. Gizlilik ayarları birçok sebepten ötürü kullanıcılar tarafından tamamen bilinmemektedir. Gizlilik ayarlarının sürekli bir şekilde kullanılmamasının sebebinin de kullanıcılara bu konuyla ilgili bilgilendirmenin yapılmamasından kaynaklandığını ifade edilmektedir. Kullanıcılar hükümler ve koşullar bölümünü okumadan " kabul " tuşuna basmaya eğilimlidirler. Ancak bunu yaparken, üçüncü kişilerin, kendi kişisel verilerine ücretsiz erişim sağlamasına izin verdiklerinin farkında değillerdir. [86]

Davranışsal reklamcılık tekniklerine karşı güvenin arttırılması ve kullanıcılara bu konuda bir takım yetkiler verilmesi için, reklam ağları *opt-out* (*opted out for receving* – reddetme hakkı - iletilmek istenen ürün-hizmet bilgilerini almak istememek; dışarıda kalmayı tercih etmek) adı verilen bir aracı uygulamaya sunmuşlardır. Bu araç kullanıcılara, kendilerinin internet üzerindeki davranışlarını, kimlerin takip ettiği ile ilgili bilgileri görme imkânı sağlamaktadır. Eğer kullanıcı bu hedef tespit etme sürecini sonlandırmak isterse "*opt-out*" tuşuna basması yeterli olmaktadır. Tabii ki bu bütün çevrimiçi davranışsal reklamların birden bire kaybolması anlamına gelmemekte; ancak gösterilen reklamların kişisel veriyi toplay

Bununla birlikte kullanıcıların davranışsal reklamcılıkla ilgili uygulamalar konusunda eğitilmeleri neticesinde, davranışsal reklamcılığı ilgi çekici bulan kullanıcıların sayısı önemli bir ölçüde artış göstermiştir. Kullanıcıların bu uygulamalar ile ilgili kendilerini rahat hissetmeleri ve davranışsal reklamcılığı reddetme yerine, bu uygulamanın performansını arttırabilmeleri için eğitime ihtiyaç duyulmaktadır. Giriş bölümünde açıklandığı üzere davranışsal reklamcılığın temel amacı reklamcılara ve kullanıcılara pozitif değerler katmaya yöneliktir. [87]

---

[86] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.16

[87] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.32

Analiz edilen çeşitli anket bulgularına göre birçok kullanıcı hala *facebook*'ta uygulanan davranışsal reklamcılık konusunda kendilerini güvende hissetmemektedirler. Bundan dolayı bir kısım kullanıcının gizlilik ayarı kendi bilgilerini gizlemeye yönelik olmaktayken diğer bir kesim kullanıcı ise bilgilerini, diğer kullanıcıların ve kuruluşların erişime serbest bırakmaktadırlar. [88]

Kullanıcılara, çevrimiçi davranışsal pazarlama ile ilgili anlaşılabilir bilgi sağlanması ile onların reklam kampanyalarıyla kaynaşması ve bu konudaki korkularının giderilmesi sağlanabilir. Ayrıca son günlerdeki olanaklarla birlikte davranışsal reklamcılık, opt-out fonksiyonu kullanılarak devre dışı bırakılabilmektedir. Bu hizmet kullanıcılara, diledikleri zaman davranışsal pazarlamayı devre dışı bırakma yetkisi vermiştir ve dolayısıyla gizlilik konularıyla ilgili şikâyetlerini azaltıcı yönde etki yaratmıştır. [89]

Araştırmalar, en yüksek düzeyde gizlilik ayarlarının seçilmesinden sonra bile, kuruluşların, çerez dosyaları kullanarak veya kullanıcıların tarayıcı geçmişi bilgilere erişerek, kullanıcılarla ilgili hedef tespitleri yapabildiklerini göstermektedir. Kullanıcıların kararlı bir şekilde yüksek gizlilik ayarlarını kullanmaları durumunda da, kuruluşlar başarılı bir hedef tespiti yapabilmek için zorlanacaklar ancak davranışsal reklamcılık bu varsayımda bile tamamen durdurulamayacaktır. [90]

D. Tarayıcı Parmak İzleri (*Browser Fingerprints*)

Cihaz parmak izi olarak da adlandırılan tarayıcı parmak izi, bir bilgisayarın donanım ve yazılımı hakkındaki bilgilerinden oluşur. Ayrıca, çözünürlük gibi konfigürasyon bilgileri de bu kapsamda yer alır.[91]

---

[88] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.35
[89] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.38
[90] Bkz. *Bloux/Desfougeres*, Halmstad University School of Business and Engineering Bachelor of Science of Business and Economics, Dissertation in Marketing, June 2011, s.38
[91] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s 29, Radboud, 2011

E. Derin Veri Analizi

İnternet, kullanıcılardan detaylı bilgi toplanmasına izin vermektedir. Bu bilgiler doğrultusunda, reklamlar, kullanıcılara göre değişiklik gösterecektir. Dolayısıyla bu, davranışsal şekilde hedeflenmiş reklamcılık alanının kapsamını arttırmaktadır. Bu durumun kullanıcıya sağladığı yararlar ile verdiği endişeler tartışma konusu olmuştur. Toplanan bilgiler doğrultusunda olası bir hedef fiyat belirlemenin yaygınlaşması söz konusudur. Bu ise çevrimiçi pazardaki güven ortamına zarar verebileceği endişelerini ortaya çıkarmaktadır; dolayısıyla bu alanın gelişmesine engel olabilmektedir.[92]

Profil oluşturmak için toplanan verinin ana kaynağı çevrimiçi izlemeyle gerçekleştirilmektedir. Bu yöntemle kullanıcıların hangi sayfaları ziyaret ettikleri, ziyaretlerinin sayısının ne kadar olduğu gibi bilgilere erişilebilinmektedir. Veriler toplandıktan sonra belirli bir sıraya koyulur. Ayrıca hangi sitede ne kadar süre kalındığı bilgisi de toplanılan bilgiler arasındadır. Çevrimiçi izleme genel olarak IP adreslerinin izlenmesiyle ve çerezler vasıtasıyla yapılmaktadır. Bu izleme yapılırken Javascript, Süper Çerezler, Tarayıcı Parmak İzleri ve Derin Veri Analizi teknikleri kullanılmaktadır. Derin Veri Analizi bazı internet servis sağlayıcıları tarafından kullanılmaktadır ve bu uygulama anlaşmazlığa neden olmaya ve tartışmaya yol açmaya devam etmektedir. İleriki bölümde anlatılacağı üzere akıllı telefonların ortaya çıkmasıyla beraber, daha karmaşık donanımlara sahip olan alıcılar vasıtasıyla, yer bilgisi ve fiziksel aktiviteler de profil oluşturma işlemi için önemli veri kaynakları haline gelmektedirler.[93]

Buradaki izleme uygulaması 3. Taraf izleme uygulamasıdır ki bu kullanıcının alışkın olmadığı bir tür izlemedir. Bu izlemede kullanıcının tarayıcısının internetteki faaliyeti esas alınarak, kullanıcıyla bağlantısı olmayan çeşitli web siteleri aracılığıyla, bireysel bir profil oluşturmak ve reklamların

---

[92] Bkz. *Office of Fair Trading,* May. 2010 p.1

[93] Bkz. *Castelluccia/Arvind*, ENISA European Network and Information Security Agency, s. 6, 14 October 2012,

hedeflenmesine olanak sağlamak için veri toplanır ve toplanılan veriler işlenir. Araştırmacılara göre kullanıcılarda huzursuz bir duygu ortaya çıkaran bu uygulamanın adı "Çevrimiçi Davranışsal İzlemedir". [94]

İnternet, üzerinden iletilen mesajlar karşısında, tarafsız bir iletişim ortamı olarak tasarlanmıştır. Net tarafsızlığı denilen bu özellik esas olarak paketlerin yalnızca adres bölümünü okuyup içeriğini okumayan router'lar ile gerçekleşmektedir. İnternet askeri ve akademik amaçlar için ilk kurulduğu zamandan itibaren uzun bir süre net tarafsızlığı egemen olmuş, 1990larda WWW'in kuruluşuyla İnternet, sıradan insanlara ve ticari dünyaya doğru eşi benzeri görülmemiş bir yayılım göstermiştir. **[95]**

Bu yayılımın bir yan etkisi olarak İnternet alanında güvenlik ihlalleri sıklaşmış, bu yüzden değerli bilgileri korumayı amaçlayan çeşitli türlerde güvenlik yazılımları geliştirilmiştir. Bu bağlamda IDS (*Intrusion Detection System* – Saldırı Sezme Sistemi) ortaya çıkmıştır. IDS sunucu ve ağlardaki saldırıları algılayıp engellemeyi amaçlar. Buna dönük olarak, sunucu veya ağdaki etkinlikleri sürekli izleyerek, ya bilindik zararlı yazılım imzalarıyla karşılaştırır ya da sistemdeki bozuklukları algılamaya çalışır. IDS, ağdan akan verilerin içeriğini de incelediğinden , net tarafsızlığı ilkesini, organizasyonel sınırlar içinde de olsa ihlal eder.**[96]**

İnternet'in sürekli artan önemi, kısmen IDS'ten ilham alan, DPI (*Deep Packet Inspection* - Derin Veri Analizi) adında yeni bir kavramın gelişimini hazırlamıştır. Paketlerin yalnızca adres kısmını işleyen geleneksel *router* donanımı ve yazılımından farklı olarak, DPI sistemleri paket içeriğinin hepsini veya çoğunu inceler. 7 katmanlı OSI (*Open Systems Interconnection* - Açık Sistemler Arabağlaşımı) modeline göre bu yalnızca üstbilgi veya adreslemenin yapıldığı ilk katmanı (fiziki katman) değil, yedinciye kadarki bütün katmanların incelenmesidir. Bu yolla paketlerin bütün içerikleri analiz edilmekte ve DPI sistemi iletişim içeriğini algılayıp sınıflandırmanın yanısıra başka bir ortama kopyalayıp işlemeyi

---

[94] Bkz. *Tene/Polonetsky*, 28/2/2012, s.283
[95] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s .967
[96] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 967

sürdürebilmektedir. Sadece 1-4 katmanlarını inceleyen, Sığ Veri Analizi (*Shallow Packet Inspection*) denilen yöntemler de vardır. DPI süreci, bir posta idaresinin elindeki mektupları yalnızca adresine iletmek yerine, hepsini açıp içlerini okumasına benzetilebilir. Bu yüzden DPI uygulamasının özel yaşam ve bilgi güvenliği açısından ciddi sonuçları vardır.[97]

Ayrıca, belirli bir organizasyonu ilgilendiren IDS'in aksine, DPI sistemleri ISP'ler tarafından uygulanmakta ve ISP'leri kullananların tamamını olası özel yaşam ihlallerine açık hale getirmektedir[98.]

Yukarıda belirtildiği gibi çevrimiçi izleme teknolojileri süratle gelişmektedir. Çerezlerle başlayan izleme teknikleri, süper çerezlerle, tarayıcı parmak izleyicileriyle ve aygıt kimlikleyicilerle devam etmektedir. Bilgi yığınlarının oluşması ve çok büyük miktarda bilgisayarla işlenmiş verinin mevcudiyeti, zaten gelişmiş olan izleme teknolojilerini daha da etkili bir hale getirmiştir. Buna ek olarak, günümüzde verilerin toplanıp muhafaza edilebilmesi kayda değer ölçüde kolaylaşmıştır ve düşük bir maliyete yapılabilmektedir. Bu güçlü olgular neticesinde, işletmeler birikmiş olan birçok verinin idare ve analiz edilmesi için çeşitli iş süreçleri oluşturmuş ve yenilikçi bir takım yollara başvurmak üzere harekete geçmişlerdir. [99]

DPI bir organizasyon içinde olabileceği gibi ulusal düzeyde de kullanılabilmektedir,. Tek bir organizasyonun ağındaki akışları izlemek için kullanıldığında, ağ güvenliği, yük dengeleme, İnternet kullanımının kısıtlanması veya izlenmesi gibi kuruluşa ait özel ihtiyaçlara göre tasarlanır. Öte yandan eğer DPI bir ISP tarafından ulusal düzeyde akışları izlemek üzere kullanılırsa, izlemenin "derinliği" de bu ölçüde değişir. [100]

Örneğin ISP'ler, DPI kullanarak, yüklü ağ trafiği isteyen BitTorrent dosya paylaşımı protokolünü sıklıkla kullanan aboneleri tespit edebilir; bu işlemlerden para kesebilir veya tamamen engelleyebilirler. Aynı şekilde akış içeriğinin ISP'lerce tespiti, zararlı yazılım engelleme veya telif hakkı korunması gibi farklı politikaları

---

[97] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 967
[98] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 967
[99] Bkz. *Tene/Polonetsky*, 28/2/2012, s.288
[100] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 967

dayatmalarına da izin verir. Bireysel aboneleri hedefleyen tüm bu kullanımların yanısıra DPI istatistiksel olarak belirli bir kullanıcı kesiminin ağ kullanımını ciro ile karşılaştırarak ne kadar kar getirdiğini araştırmak için de kullanılabilinir. [101]

DPI'ın bir diğer kullanım alanı da devlet tarafından gerçekleştirilen yasal veya yasadışı gözetim ve sansür amaçlı olanlarıdır. Bunlar, çocuk pornografisi gibi genel kabul görmüş suçların engellenmesinden, ülkedeki muhalif hareketlerin izlenmesi ve kontrol altında tutulmasına kadar farklı biçimler alabilir. Genelde amaç ikincisidir; ilki daha çok DPI kurulumunu gerekçelendirmek için kullanılır. Devletler DPI gözetimi için ISP'lerin rıza ve işbirliğine ihtiyaç duyarlar. Bu çoğunlukla fazla zorluk yaratmaz, çünkü ISP'ler çalışabilmek için devlet iznine tabidirler. Sonuç olarak DPI sistemi sınırsızca gözetim için kullanılır ve sonuçta, er ya da geç, ağ kullanıcısının özel yaşamı ihlal edilir. [102]

Birçok devlet, bütün yurttaşlarının İnternet iletişimini kaydetmek istemesine rağmen toplumsal ve teknik engellerle karşılaşır. Teknik zorluklar temelde akan verinin büyüklüğünden gelir. Veriler kaydedilse dahi, detaylı olarak analiz edilmesi yine zorluklar içerir. "Elektrik süpürgesi" yaklaşımı denilen, bir kanaldan akan bütün iletişim sinyallerinin analiz edilmesi, DPI için gerçekleştirilebilir değildir. Yine de ISP'lerde yer alan özel DPI "kutuları" yoluyla bireysel abonelerin teknik takibe alınması her zaman mümkündür. [103]

Çevrimiçi davranışsal izleme yöntemlerinden biri olarak kullanılmaya başlanılması ile birlikte, derin veri analiz teknolojisi yöntemi kayda değer ölçüde ilgi ve endişeyle karşılanmıştır. Önceleri internet servis sağlayıcılar tarafından, güvenlik ve savunma amacıyla kullanılan derin veri analizi yöntemi, daha sonra ; reklamcılık kuruluşları tarafından, kullanıcıların erişim sağladıkları web sitelerine göre kategorize edilmesi ve bunun sonucunda belli bir amaca yönelik olarak kişilere özel "*banner*" tarzında reklamlar göndermek amacıyla kullanılmaya başlanılmıştır. CDT Başkanı (*Democracy and Technology Center* - Demokrasi ve Teknoloji

[101] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 968
[102] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 968
[103] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2012, Antalya, s. 968

Merkezi) Lesie Harris bu durumu "posta hizmetiyle ilgilenen görevlilerin zarfları açıp mektuplarda ki yazıları okumasına" benzetmektedir. [104]

Derin veri analizi, reklamcılara, bireylerin çevrimsel aktivitelerinin aşırı derece detaylandırılması sonucunda oluşan profillerine göre değişiklik gösterecek reklamları sunmalarına olanak sağlar. İnternet servis sağlayıcılar ile ortaklık yapan reklam ağları, bireylerin çevrimiçi trafikleri göz özünde bulundurularak oluşturulmuş olan profillerine erişebilirler; çünkü bu çevrimiçi trafik, yolculuğunu internet servis sağlayıcıların altyapılarının içinde sürdürmektedir. [105]

Derin veri analizi tabanlı hedefleme yapmak suretiyle yapılan reklamcılığa karşı güçlü bir tepki de ortaya çıkmıştır. Bundan dolayı Amerika Birleşik Devletlerinde internet servis sağlayıcıların öncülüğünü yapanlar böyle bir reklamcılık modelini kullanmayı sadece kullanıcının rızasına dayalı olarak yapacaklarını belirtmişlerdir. Bunun bir sonucu olarak Derin Veri Analizi faaliyeti ile ilgilenen ve Amerika Birleşik Devletlerinde bu alanın öncüsü olan NebuAd kapanmak zorunda kalmıştır. Birleşik Krallıkta ise derin veri analizi faaliyetiyle ilgilenen *Phorm* adlı kuruluş yaşanan münakaşalar sonucunda buradaki faaliyetlerini terk etmek durumunda kalmıştır. *Phorm* şu anda sadece Kore ve Brezilya'da aktif durumdadır ve Amerika Birleşik Devletlerindeki hizmetlerine ise *Opt-In* modeli ile bir çözüm bulmaya çalışılmış olmasına rağmen bugüne kadarki faaliyetlerinde pek başarılı olamamıştır.[106]

Web siteleri ve internet servis sağlayıcıların, kendi sistemleri içinden geçen çevrimiçi trafik akışlarını kayıt altına almak ve izlemek için çeşitli sebepleri vardır. Bu sebeplerden bazıları; hizmeti engelleme saldırısı, virüsler ve istenmeyen e-postalar gibi olumsuz aktivitelerin sınırlandırılması, çevrimiçi trafik akışının kontrollü bir şekilde yönetilmesi ve telif hakkı sahipleriyle ilgili olarak, tescilli markalı gereçlere yasa dışı erişimin önlenmesidir.[107]

Tüm dünyadaki birçok devlet yönetimi, hukuki yaptırım gereken durumlarda yasal dinleme yapabilmek için, internet servis sağlayıcılardan derin veri

---

[104] Bkz. *Tene/Polonetsky*, 28/2/2012, s.298
[105] Bkz. *Tene/Polonetsky*, 28/2/2012, s.299
[106] Bkz. *Tene/Polonetsky*, 28/2/2012, s.298-299
[107] Bkz. *Tene/Polonetsky*, 28/2/2012, s. 304

analizi yöntemini uygulamalarını istemişlerdir ve çoğu devlet yönetimi, derin veri analizinin, kabul edilebilir kullanım politikaları çerçevesinde uygulanmasına izin vermektedirler. Bununla birlikte, günümüzde, derin veri analizi, davranışsal reklamcılık alanın da da uygulanmaktadır. *Phorm*, *Front Porch* ve *NebuAd* gibi sağlayıcı kuruluşlar, derin veri analizi yöntemini, bilgisayarlara konulan ve kullanıcının çevrimiçi hareketlerini kaydetmek ve izlemeye yarayan çerez teknolojileriyle kaynaştırarak uygulamaktadırlar ve bunun sonucunda bir davranışsal profil oluşturmaktadırlar. Derin veri analizi yöntemi ile bütün trafik izlenebilmektedir ve daha sonra kullanıcı, hedefleme yoluyla yapılan reklamcılık hizmetleri ile karşılaşmaktadır. Dolayısıyla mevcut reklamların yerini bu reklamlar almaktadır. [108]

Derin paket analizi tekniği kişinin internet trafiğindeki tüm detaylara erişebilmeyi mümkün kılmaktadır. Bu durum özellikle analiz aşamasında başka verilerin de katılımıyla yapılacak veri madenciliği kısmında çok değerli bilgilerin elde edilmesi, bir başka deyişle profillemenin çok zengin kişisel veriler eşliğinde yapılabilmesine imkân sağlamaktadır. Derin paket analizi izleme tekniğinin İSS tabanlı olarak kullanılması ise kullanıcının tüm internet trafiği İSS üzerinden geçtiği için reklam ağının çerezlerden elde edilecek kısıtlı bilgilerin analiz edilmesine kıyasla çok daha büyük bir veri kümesinden veri elde edilmesini sağlamaktadır. İçeriği çok zengin bu trafik verileri, İSS'lerdeki detaylı abonelik bilgileri ile eşleştirildiğinde, internet servis sağlayıcı tabanlı DPI teknolojisi kullanılarak yapılan davranışsal reklamcılık uygulamalarının, çerez tabanlı yapılan davranışsal reklamcılıktan çok daha büyük bir katma değer yaratacağı açıktır [109]

Gözetim amacı ile amacıyla DPI kullanılması örnekleri de ülkeler itibariyle aşağıda özetlenmiştir.

Amerika Birleşik Devletleri: DPI ABD'de bir denetim ve gözetim aracı olarak yoğunlukla kullanılmaktadır. James Bamford *The Shadow Factory* isimli kitabında bu kullanımı ayrıntılı bir şekilde anlatmaktadır. Buna göre bu ülkedeki

[108] Bkz. *Office of Fair Trading*, May. 2010 s. 23
[109] Bkz. *Keser Berber/Rapor*, İnternet Geliştirme Kurulu Raporu, 16 Ocak 2013, p. 26

Internet pazarının büyük bir kısmını kontrol eden AT&T ve Verizon şirketleri DPI uygulamalarını bu alanda uzmanlaşmış iki şirket vasıtasıyla yapmaktadırlar. *AT&T*'nin iş ortağı *Narus*, Verizon'un iş ortağı ise *Verint* isimli şirketlerdir. Bu şirketler asıl olarak Internet trafiğinin geçtiği tesislerde kendilerine ayrılan ve başkalarının erişimi yasaklanmış özel odalarda faaliyet göstermektedirler. Internet trafiğinin bir kopyası bu odalardaki *Narus* ve *Verint* cihazlarından geçerek NSA (*National Security Agency* – Ulusal Güvenlik Dairesi) bilgisayarlarına gitmektedir. [110]

Bamford bir ABD vatandaşı olarak bu ülkedeki Internet trafiğinin tamamına yakınının *Verint* ve *Narus* şirketlerinin donanımları üzerinden geçtiğinden yakınmaktadır. Bir diğer yakınma konusu bu cihazlardan geçen trafiğin uzaktan kolayca denetlenebilmesidir. Bu noktada ABD vatandaşı olmayanların da kaygı duymaları gerekmektedir. Çünkü dünya Internet trafiğinin önemli bir kısmı ABD üzerinden geçmektedir. Örneğin, Çin'den Japonya'ya gönderilen bir mesajın ABD üzerinden geçmesi (ve geçerken bir kopyasını da bu cihazlara bırakması) büyük bir olasılıktır. [111]

İngiltere: İngiltere AB ülkeleri arasında kendi vatandaşlarını dinlemek konusunda kötü bir üne sahiptir. Bu ülkenin elektronik casusluk teşkilatı GCHQ (*Government Communication Headquarters* – Hükümet İletişim Merkezi) Internet üzerinden iletişimin gitgide daha fazla önem kazanması üzerine 2008 yılında IMP (*Interception Modernisation Programme*) adlı bir proje başlatmıştır. İki milyar sterlin bütçeli IMP asıl olarak Internet ağırlıklı olmakla birlikte telefon dinlemelerini de kapsamaktaydı. Proje kapsamında ülkedeki ISS şirketlerinin tüm tesislerine DPI donanımı yerleştirilmesi öngörülmekteydi. Proje açıklandıktan sonra tüm ülkede büyük bir muhalefet dalgasıyla karşılandı. Diğerlerinin yanında saygın *London School of Economics* bir rapor hazırlayarak projenin neden uygulanmaması gerektiğini inceledi (bkz. http://www2.lse.ac.uk/ management/documents/IMP-briefing.pdf). Yoğun muhalefet nedeniyle İngiltere hükümeti projeyi geri çektiyse de kısa bir süre sonra yaklaşık aynı içerikli CCDP

[110] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 969
[111] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 969

(*Communications Capabilities Development Programme*) adlı başka bir proje başlattı. [112]

Türkiye: Türkiye'de tüm yönleriyle bilinen tek DPI uygulaması 2012 yılında faaliyete başlayan TTNET-*Phorm* ortaklığı kapsamında "davranışsal reklamcılık" girişimidir. *Phorm*'un, kişisel mahremiyeti tehdit edebilecek sistemi nedeniyle ABD, İngiltere ve Güney Kore'den sonra Romanya'da da faaliyetleri yasaklanan ve gittiği her ülkede muhalefet gören bir organizasyon olması Türkiye'de de kendisine karşı güçlü bir muhalefetin ortaya çıkmasına neden olmuştur (bkz. *Enphormasyon.org*).

Bu gelişimin sonucunda, BTK (Bilgi Teknolojileri ve İletişimi Kurumu tarafından, 23 Kasım 2012 tarihinde yapılan duyuru "Türkiye'de bir internet servis sağlayıcısı ile ortak çalışmalar yürüten Phorm Solutions firmasının, internet kullanıcıların, trafiklerini takip ettiği, kişsel bilgi güvenliğini ve gizliliğini ihlal ettiği konusunda son zamanlarda gerek yazılı medya kanallarında, gerekse sosyal medya ortamlarında çeşitli haberler yer almıştır. Kişisel bilgilerin gizliliğinin ve güvenliğinin sağlanması hususu BTK tarafından bilgi teknolojileri ve iletişim sektörüne ilişkin düzenlenmiş olup, Kurum tarafından yapılan düzenleme ve denetleme faaliyetleri bu çerçevede gerçekleştirilmektedir. Phorm Solutions firmasıyla ilgili olarak söz konusu iddialar üzerine Kurumumuzca başlatılan çalışmalar, söz konusu firmanın yurt dışında gerçekleştirdiği faaliyetler, anılan faaliyetler ilişkin olarak alınan Kararlar da dahil olmak üzere, konunun bütün yönleri ile değerlendirilerek sürüdürülmektedir. BU kapsamda yapılan çalışmaların neticesine göre, Bilgi Teknolojileri ve İletişim Kurumu tarafından gerekli işlemler tesisi edilecek ve konuyla ilgili kamuoyuna ayrıca bilgi verilecektir" şeklinde.[113]

Nitekim BTK; TTNET A. Ş.'nin Phorm Şirketi aracılığıyla "Kişisel Veri İhlali Yaptığı iddiası" ile ilgili olarak Tüketici Hakları Dairesi Bşk.lığının hazırladığı takriri inceleyerek aşağıda belirtilen hususlara ilişkin olarak; 14.12.2012 tarih ve 2012/DK-14/623 sayı ile,

---

[112] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 969
[113] Bkz. *BTK Duyuru*, http://www.tk.gov.tr/duyurular/duyuru.php?ID=37497

"Kişisel verilerin işlenmesine ilişkin olarak Gezinti.com hizmeti aracılığıyla abonelerden/kullanıcılardan alınan onay sürecinde abonelerin/kullanıcıların kişisel bilgilerinin hangi kapsamda ve hangi süre ile işleneceğine ilişkin gerekli açıklamaları yapmayarak ve aboneleri/kullanıcıları eksik bilgilendirerek Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin "Şeffaflık ve bilgilendirme" başlıklı 6'ncı maddesini, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin "Telekomünikasyonun Gizliliği" başlıklı 8'inci maddesini ve aynı Yönetmeliğin "İzin ve Süre" başlıklı 9'uncu maddesi ve ilgili diğer mevzuat hükümleri kapsamında ihlal ettiği değerlendirilen TTNET AŞ hakkında soruşturma başlatılması;

1. TTNET AŞ tarafından sunulan Gezinti.com hizmetine ilişkin olarak aboneleri/kullanıcıları eksik bilgilendiren ve talep etmeyen abonelerin/kullanıcıların da Gezinti.com kapsamına alınmasına sebebiyet veren TTNET AŞ'nin, Gezinti.com kapsamında yer alan bütün aboneleri/kullanıcıları Gezinti.com hizmetinin kapsamı dışına çıkarması;

2. TTNET AŞ tarafından sunulan Gezinti.com hizmetine ilişkin olarak kişisel verilerin ne şekilde, ne kadar sürede ve nasıl işleneceğine ilişkin açık ve detaylı bir şekilde bilgilendirme yapılması; abonelerin/kullanıcıların açık onaylarının bu çerçevede alınarak Gezinti.com hizmetinin kapsamına dâhil edilmesi;

3. Gezinti.com kapsamına girmek isteyen abonelerin/kullanıcıların tespitinde ise;
    a. Gezinti sayfasından çıkmak isteyen abonelerin/kullanıcıların açılır pencerelere yönlendirilmesi uygulamasına son verilmesi, Gezinti ana sayfasını kapat (X) seçeneğini tıklayarak terk etmek isteyen abonelerin/kullanıcıların Gezinti.com hizmetinden yararlanmak istemedikleri hususunun sisteme işlenmesi ve
    b. Gezinti sayfasında hizmetin alımını kabul ediyorum seçeneğini tıklayan abonelerin/kullanıcıların Gezinti kapsamına dâhil edilmesi"

kararını vermiştir. [114]

[114] BTK DK-14/623, http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf

TTNet Gezinti Hizmeti Soruşturması ile ilgili olarak da BTK, soruşturmayı 3 ay içerisinde tamamlamış[115]; Sektörel Denetim Dairesi Bşk.lığınca hazırlanan takriri ve eklerini inceleyerek, aşağıdaki huşularda 24.04.2013 tarih 2013/DK-SDD/228 Sayı ile verdiği karar metni de aşağıdadır:

> "14/12/2012 tarihli ve 2012/DK-14/623 sayılı Kurul Kararı gereğince; kullanıcılardan Gezinti hizmeti aracılığıyla alınan onay ile kişisel verilerin işlenmesi hususuna ilişkin olarak TTNet AŞ hakkında yürütülen soruşturma kapsamında;
>
> 06/02/2004 tarihli ve 25365 sayılı Resmî Gazete'de yayımlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in "Telekomünikasyonun Gizliliği" başlıklı 8'inci maddesinde yer alan;
>
> "Yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır..."
>
> hükmüne aykırı olarak, 2012 yılı içerisinde Gezinti hizmetine ilişkin olarak talep etmeyen kullanıcıların da Gezinti kapsamına alınmasına sebebiyet veren onay alma sürecinin uygulanması nedeniyle TTNet AŞ hakkında, Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları İle Diğer Müeyyide ve Tedbirler Hakkında Yönetmeliğin 11'inci maddesinin birinci fıkrasının (a) bendinde yer alan;
>
> "a) İşletmecinin, tüketici haklarına ilişkin kurum düzenlemeleri ve Yetki belgesinden kaynaklanan yükümlülüklerini yerine getirmemesi, tüketiciye yanlış veya yanıltıcı bilgi vermesi,"
>
> hükmü ve aynı Yönetmeliğin 32'nci maddesi hükmü çerçevesinde, 2011 yılı net satışlarının (3.150.975.726,02) %0,05 (onbinde beş) i oranında idari para cezası uygulanması hususuna karar verilmiştir."[116]

TTNET-*Phorm* işbirliğinin Internet kullanıcıları açısından en sakıncalı yönü kişisel mahremiyetini korumak isteyen kullanıcılara kaçış imkânı bırakmamasıdır. Çünkü Türkiye'de Internet omurgası TTNET tarafından kontrol

---

[115] BTK DK-14/641, http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2012%20DK-14-641.pdf
[116] BTK DK-SDD/228, http://tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf

edilmektedir. Belli ölçülerde şeffaflığın olduğu ve DPI konusunda serbest tartışmaların yapılabildiği Batı ülkelerinin aksine Türkiye'deki DPI vasıtasıyla gözetim uygulamalarının şeffaflığı sorgulanabilinir düzeydedir. Ülkede halen fazla etkin olmayan bir DPI sisteminin olduğu ve daha "iyisinin" geliştirilmesi sürecinin halen devam ettiğine ilişkin belirtiler mevcuttur. [117]

Özetlemek gerekirse DPI teknolojisi kullanılarak ISS tabanlı davranışsal reklamcılık uygulamasının veri koruması hukuku bakımından incelenmesi gereken ve tartışma yaratan yönleri;

- Amacı aşan ölçüde veri toplaması
- Toplanan verilerin davranışsal reklamcılık dışında başka amaçlarla kullanılması tehlikesi
- Kişisel internet trafiğinin çok detaylı olarak izlenmesinin özel hayatın gizliliğine ilişkin hükümleri ihlal etmesi tehlikesi yaratması olarak sıralanabilir.

DPI tabanlı İSS üzerinden yapılan davranışsal reklamcılık uygulamalarında gerek İSS tarafından kullanılan DPI teknolojisinin topladığı kişisel verilerin İSS tarafından işlenmesi, gerekse toplanan bu kişisel verilerin reklam ağı tarafından ne şekilde ulaşılarak işlendiği, veri koruması hukuku yönünden detaylı olarak incelenmelidir. Bu uygulamanın, kişisel verilerin korunması bakımından yüksek düzeyde risk yaratmasına karşın çevrimiçi davranışsal reklamcılık bakımından da çok önemli bir fayda sağlaması, konunun haklar dengesi bakımından değerlendirilmesini gerekli kılmaktadır. DPI kullanarak İSS tabanlı gerçekleştirilen davranışsal reklamcılık uygulamalarının, reklam ağlarının baskın güç olduğu bir ekosistemde, İSS'lerin de söz sahibi olmasına yol açaçağı söylenebilir. [118]

Kırlıdoğ/Fidaner'e göre "Internet ortamında DPI kullanımının çeşitli türlerinden bazıları kişisel mahremiyet için tehlikesiz, bazıları ise son derece risklidir. Bu ikisinin arasında belli trafiğin hızını azaltmak veya trafiğin içeriğine göre ücret belirlemek gibi gri alanlar da bulunmaktadır. Ancak gerek davranışsal

---

[117] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Ocak 2013, Antalya, s. 969-70

[118] Bkz. *Keser Berber*, İnternet Geliştirme Kurulu Raporu, 16 Ocak 2013, s. 26

reklamcılık, gerekse de devlet gözetimi uygulamaları kapsamında kişisel mahremiyet açısından DPI kabul edilemez niteliktedir".[119]

Kırlıdoğ/Fidaner, Opt-in ile *opt-out* arasındaki kararın, "bütün iş modellerinin nasıl şekilleneceğini tayin etmekte" olduğunu ifade etmektedir. *Kırlıdoğ/Fidaner* bu yönde "eğer belirli bir faaliyetin toplum açısından değeri belli değil ise, o zaman bireyin bu konudaki seçme hakkına odaklanılabilinir ve bu seçim doğrultusunda bir bilgilendirme yapılabilinir; ama eğer ki toplumsal fayda belirgin ise o zaman bir yöntem, varsayılan olarak ayarlanabilir ve kullanıcılara bu yöntemi reddedebilmeleri için bir inisifiyatif tanınabilinir" görüşünü açıklamaktadır. [120]

V. Tekniklerin Pazarlamacılar, Sosyal Ağlar ve Akıllı Telefon Uygulamacıları Tarafından İzleme ve Profillemede Kullanım Şekilleri

A. Birinci Taraf İzleme

Web sitesi hizmetleri genelde "birinci taraf" tarafından işletilir. Web sayfaları içerik sunan hizmetler verirler. Bir *web* sitesindeki içerik sunucusunun birçok sayfası bulunur ve bu sayfalar *web* sitesini ziyaret edenler tarafından kendi bilgisayarlarına yüklenebilmektedir. Bu faaliyet, bilgisayarın alışılagelmiş bir programı çalıştırması gibidir. Ziyaretçinin, bilgisayarına yüklediği sayfa türleri, genelde sunulan hizmetlerle ve yürütülen faaliyetlerle ilgili bilgiler içerir. Çoğu durumda ve özellikle birinci taraf tarafından işletilen sunucularda, sunucu, ürünlerin *web* sayfası aracılığıyla satılmasına veya hizmetin internet ortamından sipariş verilmesine olanak tanır.[121]

FPC'ler birçok amaç için kullanılırlar. Bunlardan birisi de kullanıcıya tarama yapması esnasında yardımcı olmaktır. Örneğin bu çerezler, bir alışveriş

---

[119] Bkz. *Kırlıdoğ/Fidaner*, XV. Akademik Bilişim Konferansı, 23-25 Şubat 2013, Antalya, s. 970
[120] Bkz. *Tene/Polonetsky*, 28/2/2012, sp. 334
[121] Bkz. *Butler/Teddy/Waugh,* United States Patent Application Publication butler et al, Nov,23,2006, s.2, (0020)

sepeti bilgisini, tercih ayarlarını, otomatik kullanıcı girişi bilgisi ve benzeri gibi bilgileri içerebilirler. Kullanıcıların bildiği kadarıyla TPC'ler gereksiz ve FPC'ler ise kullanışlıdır[122]

Dolayısıyla internet kullanıcıların Birinci Parti Çerezleri (FPC) silme eğilimleri, Üçüncü Parti Çerezlere (TPC) göre daha düşüktür. Çünkü FPC'lerin kullanıcılara yardımcı olduğu algısı vardır.[123]

FPC'ler bir kişi tarafından ziyaret edilen web sayfasının yayıncısı tarafından yerleştirilir. TCP'ler ise, ziyaret edilen web sayfası üzerinden, üçüncü kişiler aracılığıyla yerleştirilir. Çerez yerleştirmenin yasal koşulları, kullanıcının bilgisayarına çerezi yerleştiren tarafın yükümlüğündedir ancak eğer üçüncü taraf bir *web* sayfası aracılığıyla çerez yerleştiriyorsa, bu sorumluluğu paylaşan yayımcı ile bir sözleşme imzalamak gerekebilir. Örneğin yayıncının kendi sayfasına çerez yerleştirirken kullanıcıyı bilgilendirmesi, *web* sayfasının kontrolünde olmayan üçüncü kişilerle işlem yapmasından daha pratiktir.[124]

Çerezlerin kim tarafından ve hangi şekillerde yerleştirildiği konusunun çeşitli aktörleri vardır. Kuruluşların büyük bir bölümü, kendi web sayfalarına kendi çerezlerini yerleştirerek, birinci taraf işlevi görmektedirler;. Ama işin içerisine çok sayıda üçüncü taraf da girmektedir. Üçüncü taraflar, kendi *web* sayfalarına ve başkalarının web sayfalarına, başkaları adına çerez yerleştirmektedirler. Gözlenen kuruluşlar, eş zamanlı olarak hem birinci parti hemde üçüncü parti gibi hareket etmektedirler. Sonuçlar, OBA'nın sadece internet kullanıcıları için değil bundan başka OBA'yı sağlayanlar için de ne kadar karışık bir alan olduğunu göstermektedir. İlgililerin yüzde kırkı OBA'yı kullanmak için veriyi çerezler tarafından ve üçüncü parti üzerinden toplamaktadır. Genel olarak web sayfası sahipleri ve yayımcıları, web sayfası istatistiklerini sağlayanların ifadesine göre, çoğunlukla birinci parti işlevi görerek, kendi çerezlerini web sayfaları aracılığıyla kendileri yerleştirmektedirler. Reklamcılar, reklam ağları ve medya ajansları,

---

[122]Bkz. *Butler/Teddy/Waugh,* United States Patent Application Publication butler et al, Nov,23,2006, s.1, (0010)

[123]Bkz. *Butler/Teddy/Waugh,* United States Patent Application Publication butler et al, Nov,23,2006, s.1, (0011)

[124] Bkz. *Eijk ve diğ.*, Emeral Group Publishing Limited, Vol.14 No.5, 2012, s.60

kuvvetle muhtemel olarak üçüncü parti işlevi görmekte ve başkalarının, kendi adlarına çerez yerleştirmelerine izin vermektedirler.[125]

Sonuç olarak FPC'lerden farklı olarak, TPC'ler, *web* sayfasının işleyişi konusunda neredeyse hiç gerekli olmamakla beraber hedeflenmiş reklamcılık da dâhil olmak üzere başka amaçlarla kullanılmaktadır.[126]

B. Üçüncü Taraf İzleme

Web sayfaları genelde üçüncü taraflardan gelen verilere hizmet ederler. Hizmet edilen bu içeriğin çeşitli amaçları olabilir. Bunlardan biri de reklamcılıktır. Üçüncü taraf reklamların ücretsiz hizmetleri ve internet üzerinde olan bilgileri desteklemesiye beraber reklamları hedefleme ve bunu gerçekleştirmek için ölçümlerde bulunma isteği, kullanıcıların izlenmesine yardım etme faaliyetine dönüşmüştür. İzleme faaliyetlerine karşı duyarlı olan kullanıcılar, bunu azaltabilmek için bazı araçlar kullanabilmektedirler.[127]

Üçüncü tarafların internet ortamında izleme faaliyetleri ile ilgili politikaları oldukça çeşitlilik gösteren bir durumdadır. Bütün menfaat sahipleri kullanıcıların, internet ortamında izleme faaliyetinin üzerinde bir takım kontrol mekanizmalarına sahip olması gerektiği konusunda hemfikirdirler. Ancak konunun ayrıntısıyla ilgili olarak bazı noktalarda anlaşmazlıklar bulunmaktadır.[128]

- Kullanıcılar ne üzerinde kontrol sahibi olmalıdırlar? Devlet politikasına yön verenler ve taraftarları, kullanıcıların, internet alanındaki izleme sonucu ortaya çıkan verilerin toplanması hakkında bir kontrole sahip olması gerektiği görüşündedirler. Çevrimiçi reklamcılıkla uğraşan mali gruplar ise kontrol mekanizmasının genişletilmesini, sadece verinin belirli kullanımları üzerinde olması durumunda gerektiği görüşü ile tartışmaya açmışlardır..

---

[125] Bkz. *Eijk ve diğ.*, Emeral Group Publishing Limited, Vol.14 No.5, 2012, s.63
[126] Bkz. *Eijk ve diğ.*, Emeral Group Publishing Limited, Vol.14 No.5, 2012, s.72
[127] Bkz. *Ajdari/Hofnagle*, Team for Resarch in Ubiquitous Secure Technology, National Science Foundation, s.1
[128] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.417

- Saptanmış ve varsayılan değer ne olmalıdır? Avrupa Birliği politikasına yön verenler ,izlemenin yapılmamasının varsayılan değer olarak uygulanmasını belirtmişlerdir, reklamcılıkla ilgili olan mali gruplar ise izlemenin yapılmamasının varsayılan değer olarak uygulanmasını tartışmaya açmışlardır.
- Tercih mekanizmasının tasarımını kim yapmalıdır? Reklamcılıkla ilgili olan mali gruplar tercih mekanizması tasarımının kontrolleri altına alınmasını istemişlerdir. Politikaya yön veren birçok kişi ve kurum ise tasarım sorumluluğunun, tarayıcıyı sağlayanların elinde bulundurulması görüşünü benimsemişlerdir.[129]

Bazı kullanıcı tarafları ile Avrupa Birliği politikalarına yön verenler, çevrimiçi gizliliği bir temel insan hakkı şeklinde görmektedirler. Diğerleri olarak adlandırabileceğimiz birçok araştırmacı ve Amerikan politikasına yön verenler ise, bu konudaki kararın, gizlilik riskleriyle doğrudan ilgili olan kullanıcının seçimine bırakılma yaklaşımını toplumun refahını azami seviyeye çıkarmak için bir araç olarak görmektedirler. Örneğin *Mozilla*, bu konuda bir taraf seçimi yaparak, kullanıcılarına izleme müessesine yönelik bir seçenek sunmasını, ideal bir politika hedefi olarak görmektedir. Üçüncü parti web sayfaları ve reklamcılıkla ilgili olan mali gruplar, büyük bir ölçüde şimdiki uygulamaları savunmaktadırlar. Bu savunmalarını toplumun refaha ulaşmasından kaynaklandığını söyledikleri parametlerle açıklamaktadırlar. Bunların hepsi kullanıcıların rızasına verilen desteğin, kullanıcının gizlilikle ilgili olan risklerinden ve ekonomik haklarından daha ağır bastığını göstermektedir.[130]

Kullanıcılara internet ortamında yapılan üçüncü taraf izleme faaliyetleri üzerinde bir kullanım olanağı sağlamak için teknik olarak üç çözüm geliştirilmiştir: *Opt-out* Çerezleri, Engelleme ve DNT Mekanizması.[131]

---

[129] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.417
[130] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.417
[131] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.422

Opt-Out Çerezleri ve Reklam Seçme Simgesi: Güncel çevrimiçi davranışsal reklamcılık öz denetim düzenlemelerinde kullanıcının seçimi *opt-out* çerezleri ile yerine getirilmektedir. Bu yaklaşımla ilgili bazı problemler ortaya çıkmıştır. [132]

İlk olarak, *opt-out* çerezlerinin kullanıcı tarafından güncellemesinin yapılması gerekmektedir. İkinci olarak bir müddetten sonra çerezlerin süresi sona ermektedir dolayısıyla kullanıcının düzenli aralıklarla *opt-out* çerezlerini yenilemesi gerekmektedir. Üçüncü olarak kullanıcılar, çerezleri sildiklerinde farkında olmayarak *opt*-out tercihlerini de kaldırabilmektedirler. Dördüncü olarak *opt-out* çerezleri hassas olduklarından, üçüncü taraflar için bu çerezleri uygunsuz bir şekilde ayarlamak veya silmek kolay olabilmektedir.

Birçok çevrimiçi reklamcılık şirketi reklamların sergilendiği yerlere davranışsal hedeflemeye ilişkin ve özdenetimle sağlanan seçim mekanizmaları ile ilgili kullanıcı bilincini arttırmak için "*AdChoice*" simgesi (13x13) ve metini (10pt) eklemeye başlamışlardır. Simgeye tıklandığında hedefleme faaliyetinin reklama nasıl uygulandığı hakkında ek bilgi ve birçok durumda kullanıcıların *opt-out* çerezlerinin ayarlarını yapabileceği sayfaya bir bağlantı sağlanmaktadır.

Birkaç araştırmada, öz denetim ile meydana getirilmiş *opt-out* modelinin kullanılabilirliğinin doğruluğunu sorgulanmıştır. [133]

Engelleme: Engelleme yöntemi açık bir şekilde etkili olabilmektedir ancak bu sadece konuyla ilgili ileri düzeyde bilgi sahibi olanlar için uygun bir çözüm gibi gözükmektedir. Bilinen engelleme araçlarından *Ghostery*, *Adblock Plus* ve *Internet Explorer Tracking Protection List* isimli engelleme araçlarının kullanılabilirliğine ilişkin araştırma sonuçları kullanıcıların bu araçlarla yapamaya çalıştıkları engellemem girişimlerinin başarısız olduğunu açıkça göstermektedir.

Do Not Track: DNT kullanıcılara, analiz hizmetleri, reklam ağları ve sosyal platformlar da dâhil olmak üzere, ziyaret etmedikleri tüm web sayfalarınca izlenmelerini engellemelerine olanak veren bir teknoloji ve politika önerisidir.

DNT, güncel çerez mekanizmasına kıyasla son derecede basit bir yöntemle kullanıcıya izlemeyi reddetme olanağı vermektedir. Reddetmeye olanak veren

---

[132] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.422
[133] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.422

çerezler çok değildir, tüm reklam ağları tarafından desteklenmemektedir ve buna uymak istemeyenlerce de farklı şekillerde yorumlanmaktadır (izleme yoksa – davranışsal pazarlama da yok vb). DNT başlığı bu kısıtlamalardan kaçınmaya imkân vermekte olup, gelecekte de geçerliliğinin olduğu ifade edilmektedir; çünkü yeni ortaya çıkan reklam ağları, artık kullanıcının bir girişimini gerektirmemektedir..[134]

C. Çevrimiçi Sosyal Ağ (OSN – *Online Social Network* – Çevrimiçi Sosyal Ağ)) İzlemesi

Sosyal ağ oluşturma katılımcıların sanal bir ağda bilgi paylaşabilmesini ve birbirleri ile iletişime geçebilmesini sağlayan, karşılıklı etkileşmenin yeni bir biçimidir. Sosyal ağlar ve toplum kökenli çevrimiçi hizmetler çok iyi bir eğlence imkânı sunmakta ve gerek bireysel kullanıcılara gerekse kuruluşlara birçok fayda sağlamaktadır. Kullanıcılar eski okul arkadaşlarıyla yeniden ilişki kurmak, kendi ilgi alanlarıyla ilişkili etkinliklere katılmak, sanat eserleri oluşturmak, yeni arkadaşlıklar kurmak ve hatta hayat arkadaşları dahi bulabilmektedirler. Bu platformlarda şirketler de, kendi markalarını güçlü bir biçimde yapılandırabilmekte, müşterilerinin kendilerine ilişkin geri bildirim ve algılama bilgilerine ulaşabilmekte; sorunları, ortaya çıktığı anda çözebilmekte, böylece kendilerine değer katan faaliyetlerde bulunabilmektedirler. Buna rağmen, çevrimiçi sosyal ağ siteleri, dikkatli kullanılmadığı zamanlarda da, kişisel bilgi kaçaklarının kaynağı ve kötü amaçlı yazılım saldırılarının yöneldiği bir ortam olabilmektedir.[135]

Kullanıcı bilgisinin sosyal ağda yayınlanması, kimlik hırsızlığı, çevrimiçi tacizler ve bilgi sızması gibi tehditler ve tehlikeleri de oluşturmaktadır. Sosyal ağ sitelerinde bulunan kişisel bilgilerin geniş hacmi ve ulaşım kolaylığı, bu bilgileri kendi çıkarları için kullanmak isteyen kötü niyetli kişilerin de dikkatini

---

[134] Bkz. *Mayer/Mitchell,* 2012 IEEE Symposium on Security and Privacy, s.424

[135] Bkz. *Ahmand/Aljumah*, Computer and Information Science Volume 6 No:1, 2013 , Salman Bin Abdulaziz University Saudi Arabia, s.140

çekmektedir. Bu durum kullanıcıların gizliliğine ve güvenliğine ilişkin bir takım sorunlara neden olabilmektedir.[136]

Güvenlik ve Gizlilikle İlgili Zorluklar: Çevrimiçi Sosyal ağlarda kullanılan uygulamalar, güvenlik ve gizlilik konularıyla ilgili olarak aşağıda sıralanan bir takım kaygıları oluşturmaktadırlar.

1) Kullanıcının kendi gönderdiği bilgilere, kimin erişebileceği konusunda mutlak bir kontrolü bulunmamaktadır.

2) Çevrimiçi sosyal ağlardaki gizlilik ayarları, yapısı gereği, değişmeyen bir niteliktedir.

3) Sizin uygun bulduklarınız olduğu gibi uygun bulmadığınız kişiler de sizinle ilgili bilgiler gönderebilmektedir.

4) Siteler arası betik çalıştırma, XSS, kimlik hırsızlığı, e-dolandırıcılık ve sosyal mühendislik saldırıları çevrimiçi sosyal ağlarda yaygın durumdadır.

5) Kullanıcıların çevrimiçi sosyal ağlara gönderdikleri bilgiler devamlı olarak varlığını sürdürmektedirler.

6) Kişisel yaşam ve işle ilgili meseleler korunmasız bir şekilde açıktadır

7) Tatile çıkma ve bunun gibi olan kişisel bilgilerin çevrimiçi sosyal ağ sistemine gönderilmesi bazen özel yaşam için tehlikeler oluşturabilir.

8) Uygulama sağlayıcıları, kullanıcı bilgilerini üçüncü taraf sağlayıcılara, iş topluluklarına ve benzeri topluluklara maddi kazanç elde edebilmek için satılabilmektedir.

9) Saldırganlar, çevrimiçi sosyal ağlardaki zengin içerik ve sıkı olan etkileşimler sayesinde, solucanların yardımıyla büyük zombi bilgisayar ağları oluşturabilmektedirler. Kötü amaçlı yazılımlar ise sosyal ağlar üzerinden profillere, etkileşimlere ve üçüncü partilerin sağladığı uygulamalara yayılabilmektedir.

10) Kişisel bilgiler saldırganlar için çok kullanışlıdır. Kişiye özel olan şifreler, banka hesapları ve sosyal güvenlik numarası saldırganların aradığı şeylerdir. Saldırganlar bu bilgileri bir kere ele geçirdikten sonra kimlik hırsızlığına kadar varabilen birçok suç işleyebilmektedirler.

---

[136] Bkz. *Ahmand/Aljumah*, Computer and Information Science Volume 6 No:1, 2013 , Salman Bin Abdulaziz University Saudi Arabia, s.140

11) Sosyal ağlarda saldırganlar kimliklerini gizleyerek meşru bir kullanıcı gibi davranıp, sosyal mühendislik teknikleri kullanarak diğer kullanıcıların kasıtlı bir şekilde hazırlanmış örnek kaynak konumlayıcılara tıklamalarına ve böylece kandırılmalarına neden olabilmektedirler.
12) Kullanıcılarla ilgili dijital bilgilerin (örneğin profil, fotoğraf, video, mesajlar ve benzerleri gibi) tek bir sunucuda merkezileştirilmesi sebebiyle kullanıcıların gizlilik ve güvenliklerine ilişkin tehditler oluşabilmektedir. [137]

Çevrimiçi sosyal ağlarda bulunan "paylaş" özelliği, web sitesi sahiplerinin bu özelliği kendi sayfalarında kullanmasıyla birlikte popülerliğin artmasına imkân sağlamıştır. Bunun yanısıra çevrimiçi sosyal ağlar, kullanıcıların ziyaret ettiği sitelerdeki aktivitelerini izleyebilmesi için de bir yol haline gelmiştir. Kullanıcıların ziyaret ettikleri sayfaların izlenmesinde kullanılan mekanizmalar ile bu izleme faaliyetinin boyutu, en yaygın üç çevrimiçi sosyal ağ olan *Facebook*, *Twitter* ve *Google+* açısından detaylı bir şekilde araştırıldığında, kullanıcıların, çevrimiçi sosyal ağ oturumunu kapattıktan sonra ve hatta izlenebildikleri çeşitli raporlarla kanıtlanmıştır. Bu raporlarda izleme faaliyetlerinden doğabilecek riskler deneysel çalışmalar ile gösterilmiştir. Bu izleme faaliyetinden elde edilebilecek bilgiler ile kullanıcıların çoğunun çevrimiçi ortamda profillerinin oluşturulabilineceği belirtilmiştir.

Twitter, oturum açmış bir kullanıcısı için 15 farklı çerez depolamaktadır.

Ayrıca *twitter* daha önce hiç kendi sitesine girmemiş bir kullanıcının, içinde twitter'da "Paylaş" tuşunu içeren bir web sitesine girmesi durumunda otomatik olarak *guest_id* çerezini ziyaretçinin bilgisayarına yerleştirebilmekte ve belirli bir zaman sonra twitter.com sitesini hiç ziyaret etmemiş kişileri de izleyebilmektedir. Bu davranış kendine özgüdür; çünkü çevrimiçi sosyal ağların hiçbiri bu davranışa benzeyen bir uygulamayı henüz yapmamaktadır.[138]

Araştırmalar çevrimiçi sosyal ağların, dışarıdan gelen uygulamalara ilişkin ağdaki kimlik tanıtıcı bilgileri üçüncü taraf kaynaklara sızdırdığını göstermektedir

---

[137] Bkz. *Ahmand/Aljumah*, Computer and Information Science Volume 6, No:1, 2013 , Salman Bin Abdulaziz University Saudi Arabia, s.142
[138] Bkz. *Chaabane/Kaafar/Boreli,* WOSN (Workshop on Online Social Network), Helsinki, 2012, s.2

Kimlik tanıtıcı bilgilerinin sızdırılması gibi durumlarda, çevrimiçi sosyal ağın teknik olarak bir kusuru bulunmamaktadır. Kullanıcılar dış kaynaklı uygulamalar aracılığıyla ikincil bir sızıntı gerçekleştiğinden haberdar olmayabilirler. *Myspace* ve *Facebook* gibi sosyal ağlardan da dış kaynaklı uygulamalarından doğan isteklerle sızıntı yapılmasının örnekleri vardır.[139]

Kullanıcıların *opt-out* mekanizmaları aracılığıyla yasaklar koymakta başarısız oldukları durumlarda da sosyal ağlardan kişisel bilgiler sızabilmektedir; ancak sızıntı sadece bu kanaldan gerçekleşmemektedir. Çevrimiçi sosyal ağlarda oluşan kullanıcıların özel bilgileri, açık bir şekilde reklam şirketlerine ve ücret ödeyen çevrimiçi ağ kullanıcılarına sızmaktadır.

D. Mobil Cihaz Tabanlı İzleme

Mobil telefon hizmetinin artarak yaygınlaşmasıyla beraber, mobil telefonlarda izleme faaliyetinin uygulanması, konum tabanlı hizmetlerin çeşitli alanlara yayılmasına olanak vermiştir. Mobil telefon sağlayıcılarının GSM'ler (*Global System for Mobile Communication* – Mobil İletişim için Mobil Sistem) ve sonrasında GPS (*Global Positioning System* – Küresel Konumlandırma Sistemi) özelliği etkinleştirilmiş hizmetler aracılığıyla müşterilerin konumlarını izleme faaliyetleri, konum tabanlı teknolojiler ve hizmetlerin kullanılmasıyla beraber, gizlilikle ilgili konuları gündeme getirmiştir.[140]

Mobil aygıtların bireylere ilişik bir durumda olması ve olanaklar çerçevesinde konum belirten sinyaller vermesi, işletmeler ve reklamcılar için, etkili reklam yapabilmek konusunda ilgi çekici hedefler haline gelmelerine neden olmuştur. Mobil aygıtlar giderek masaüstü bilgisayarların programlama gücüne yetişmektedirler; bu nedenle mobil izlemenin ileriki yıllarda daha da ayrıntılı bir şekle dönüşümü beklenmektedir.[141]

---

[139] Bkz. *Chaabane/Kaafar/Boreli,* WOSN (Workshop on Online Social Network), Helsinki, 2012, s.4

[140] Bkz. *Barkuus/Dey*, Proceedings of the INTERACT 2003, 9TH IFIP TC13 International Conference on Human-Computer Interaction, Berkeley, July 2003, s.2

[141] Bkz. *Eubank ve diğ.*, Princeton University, Berkeley, May 2013, s.1

Mobil aygıtlara odaklanmış olan üçüncü tarafların sayısı gerçekten azdır. Üçüncü partiler diğer konulara göre yeni olan bu pazara daha girmemişlerdir; ancak üçüncü partiler yeni oluşmaya başlayan bu pazardaki gelişmeleri yakından izlemektedirler. [142]

E. Konum İzleme

Yeni gelişen bir saha uygulaması olan konum tabanlı teknolojiler, insanlarla veya objelerle ilgili olan fiziki, geometrik ve lojikal konum bilgilerini kullanmaktadır. Konum tabanlı teknolojilerinden biri olan lokasyon kestirimi ile insanların veya objelerin izlenmesi, konum tabanlı teknoloji alanını oluşturan teknolojiler arasındaki en önemlileridir. Konum tabanlı mühendislik bilgisini uygulamak için kızılötesi ışınlar, sesüstü dalgalar, radyo frekansları (RF) ve ultra geniş bant (UWB) gibi algılayıcılar kullanılmaktadır. [143]

Bazı kullanıcılar konum izleme hizmetlerine memnuniyetle abone olsalar da kullanıcıların büyük bir bölümü her durumda konumlarının öğrenilebilir olmasından rahatsızdır. Dolayısıyla araştırmacılar kişilerin hassas bölgelerde bulundukları zaman konumlarını saklamak ve ziyaret ettikleri alanlar ile ilgili yol bilgilerinin ifşa edilmesini kontrol altına almak için çeşitli algoritmalar üzerinde çalışmaktadırlar. [144]

Telsiz konum belirleme ve izleme faaliyetleriyle ilgili son teknolojik gelişmeler bireylerin hareketlerini izleme konusunda daha önce benzeri görülmemiş imkânlar sağlamaktadır. Bu gelişim konum tabanlı hizmetler açısından yararlı olmakla beraber, kişilerin gizlilikle ilgili kaygıları bu duruma rıza göstermelerine ciddi bir engel oluşturabilmektedir.[145]

Bireylerin korunmasını istedikleri gizlilik seviyesinin durumlara göre değişkenlik göstermesi de, konum izleme uygulamalarının, gizlilik ile ilgili sorunları çözmesini zorlaştıran bir başka yöndür. İzlenen aygıt, örneğin bir cep telefonu, kullanıcıdan

---

[142] Bkz. *Eubank* ve diğ., Princeton University, Berkeley, May 2013, s.5
[143] Bkz. *Yun/Kim*, Science Direct, Elsevier, 12 December 2006 s.210
[144] Bkz. Grutese/Liu, IEEE Computer Society, Vol.2, Number 2, March-April 2004, s.28
[145] Bkz. Grutese/Liu, IEEE Computer Society, Vol.2, Number 2, March-April 2004, s.28

her bir konum izleme talebini onaylamasını isteyebilir. Böylesi bir durumda onaylama taleplerinin sıklıkla gelmesi ve her bir talebin el ile onaylanması veya izleme özelliğinin her bir talepte açıp kapanması
gereği zamanla sıkıcı ve kullanışsız bir hale dönüşebilir. Bu bağlamda bilinçli gizlilik politikalarında otomatik gizlilik kararlarına imkân sağlanmakla beraber bu tür politikalar oldukça karmaşık ve tanımlanması güçtür. [146]

Kullanıcılar talep ettikleri dış hizmetlerden gelen konum hizmetlerini çoğu zaman onaylarlar çünkü bu hizmetlerin yakındaki oteller bulmak veya trafik sıkışıklığının hangi güzergâhta olduğunu öğrenmek gibi uygulamalarını kullanışlı bulurlar. Bundan ötürü kullanıcılar kendileriyle ilgili olan veri bütününü saklamak istemezler. Buna rağmen örneğin belirli hassas alanlara giriş yapılması gibi bazı durumlarda kullanıcılar konumlarının gizli kalmasını isteyebileceklerdir. Hizmet sağlayıcılar kullanıcılarına kendilerine göre hassas olan alanları belirleyebilmeleri için önceden tanımlanmış, kullanıcıların kendi ihtiyaçlarına göre uyarlayabilecekleri ve kısıtlayıcı özellikleri bulunan çeşitli politikalar teklif etmektedirler. Örneğin önceden tanımlanmış olan bir politika, haritalar kullanarak konum tespiti yapan bir *broker'*in konum izleyebilmesine umumi yerleşim yerlerinde izin verebilirken, binalarda veya özel mülklerde izleme faaliyetini engelleyebilmektedir. Bu politikalar geliştirilerek bina tiplerinin ayrıt edilmesinde de kullanılabilinir (toplu konut veya ticari yapılar gibi). [147]

F. Yeniden Özdeşleştirme (*Re-identification*)

Yeniden Özdeşleştirme, görünüşte anonim olan verinin, bu verinin konusu olan kişilerin kimlik bilgileriyle doğru bir ilişkisinin kurulmasını ifade eder. [148]

İnsanlar günlük yaşamlarında çeşitli veri tabanlarına küçük kişisel bilgi parçacıkları bırakırlar. Bireyler kendi verilerinin toplanıp toplanmadığını öğrenmek konusunda kontrole sahip olabilecek kabiliyette değildirler; hatta bazı durumlarda

---

[146] Bkz. Grutese/Liu, IEEE Computer Society, Vol.2, Number 2, March-April 2004, s.28
[147] Bkz. *Grutese/Liu*, IEEE Computer Society, Vol.2, Number 2, March-April 2004, s.29
[148] Bkz. Malin UNLINKABILITY, Carnegie Mellon University, PhD Thesis, s.4, Pittsburgh, May 2006

arkalarında veri bıraktıklarının bile farkında bile olmazlar (örneğin bir bireyin otomobilinin görüntülerinin otoyollardaki çeşitli kameralarla kaydedilmesi veya çeşitli web sayfalarında oturum açmış olan bir kişisel bilgisayarın IP adresi gibi). [149]

Yeniden Özdeşleştirme özgün ve özgül olan öğelerle görünüşte anonim olan verilerin arasında ilişki kurmaktır; bu girişim bir bakıma, veri toplama faaliyeti yolu ile gizlilik hakkına yapılan bir saldırıdır. [150]

Kişiler genellikle iş ya daboş zamanlarını değerlendirme faaliyetleri amaçlı olarak (spor yapmak, aile ile zaman geçirmek) veya şirketlerle olan ilişkilerinde (banka, kitapçı dükkânı) tam olmayan ve birbirinden farklı kimlikler kullanır. Bu kimlik bilgilerinin bazıları değişmezken bazıları dinamik bir şekilde değişmektedir (ilgi alanları gibi). [151]

Örneğin bir çevrimiçi kullanıcı her bir *web* sayfasını ziyaret ettiğinde bilgisayarının IP adresi bu *web* sayfalarında kayıt altına alınmaktadır. Ayrıca bazı *web* sayfalarında açık bir şekilde ad ve adres gibi kimlik bilgilerini içeren verilerin girilmesi istenmektedir. Örneğin *web* siteleri bir satın alma işlemini tamamlayabilmek için kullanıcıdan ad ve adres bilgilerini bir şart olarak istemektedir. Ayrıca bu *web* siteleri kendi sayfalarını ziyaret eden kullanıcıların IP adreslerinin bulunduğu kayıtları paylaşabilmektedirler. Bu *web* sayfaları satın alma faaliyetinde bulunan kişilerin isim ve adreslerini içeren müşteri listeleri gibi açık bir şekilde tanımlanmış olan verileri de işletmelerle paylaşabilmektedirler. Kimliksizleştirilmiş olan verinin içindeki IP adreslerinin hangi konumda ortaya çıktığının incelenmesi ve bu verilerin kullanıcıların ziyaret ettikleri sayfalarda ortaya çıkan tanımlanmış müşteri listeleri ile eşleştirilmesi sonucunda, IP adresleri ile kullanıcıların isim ve adresleri arasında bağlantı kurulabilinmektedir. Bu yeniden özdeşleştirilmiş veriler ise kullanıcıların hangi yerlerde satın alma işlemini

---

[149] Bkz. *Malin UNLINKABILITY*, Carnegie Mellon University, PhD Thesis, s.5, Pittsburgh, May 2006

[150] Bkz. *Malin UNLINKABILITY*, Carnegie Mellon University, PhD Thesis, s.1 Abstract, Pittsburgh, May 2006s.1, Abstract

[151] Bkz. Clauß, Dogan Kesdogan, Tobias Kölsch, Technische Universitat Dresden, Fakultat Informatik, s.85, Dresden, November 11, 2005,

daha çok veya daha az yaptığı hakkında bilgi sağlayabilir. Olaylar bu noktaya gelinceye kadar çoğu kişi de, kimliksizleştirilmiş IP adreslerinden oluşan sistem günlük verilerinin, yeniden özdeşleştirme işlemine tabi tutulamayacağını düşünmekte idi. [152]

Web sayfaları, kişilerin toplanmış özel bilgilerini, genellikle bir ticari meta gibi ele almaktadır. Toplanmış olan veriler önceden belirlenmiş olan çevrimiçi politikalara uygun bir şekilde başka taraflarla kurum içi kullanımlar ve diğer çeşitli amaçlar için yasalara uygun bir şekilde paylaşılabilmekte, lisanslanabilmekte veya satılabilmektedir Örneğin E-ticaret ile ilgili uygulamalarda, müşteri listelerinin düzenli olarak bağlantılı olan üçüncü taraflara iletildiğini söylemek mümkündür. İnternet ortamında ve bunun dışındaki ortamlarda bireyler hakkında toplanan bilgiler, diğer bilgilere oranla daha hassastırlar. Birçok kuruluşun gizlilik politikasında, tanımlanmamış olan verilerin tanımlanmış verilerle bağlantı kurulmasına imkân sağlayacak bir tarzda paylaşılamayacağı ayrıntılarıyla belirtilmiştir. Bu politikayı garanti altına almak için birçok bölge, tanımlanabilen veriyle tanımlanmamış veriyi birbirinden ayırmakta ve iki farklı veri kümesi olarak piyasaya sürmektedir. Çevrimiçi gizlilik politikaları, ABD'de sözleşmeye dayalı anlaşmalara eşdeğer bir şekilde nitelendirilmektedir ve FTC'nin gözetimi alanındadır. Bir *web* sayfasının bağlı kalması gereken gizlilik politikasına bir ihmal sonucu aykırı davranması halinde bu durum Federal Ticaret Komisyonu'nun şartnamesindeki aldatıcı uygulamalar kapsamında nitelendirilmektedir. [153]

---

[152]Bkz. *Malin ve diğ. RE-IDENTIF*, LIDAP-WP2 Carnegie Mellon University, Laboratory for International Data Privacy, s.2, Pittsburgh, March 2003

[153] Bkz. *Malin UNLINKABILITY*, Carnegie Mellon University, PhD Thesis, s.10, Pittsburgh, May 2006

§3. ÇEVRİMİÇİ İZLEMENİN RİSKLERİ/GETİRDİĞİ TEHDİTLER VE KORUYUCU ÖNLEMLER

I. Çevrimiçi izlemenin riskleri, getirdiği tehlikeler

A. Gözetim (devlet / şirketler)

İzlemenin en büyük riski küresel gözetimdir. Bu gözetim güvenlik ve siyasal gerekçelerle, şirketler tarafından da ticari nedenlerle gerçekleştirilebilir. Bir New York Times makalesinde de ayrıntılı bahsedildiği gibi pazarlamacılar tüketicilerin alışkanlıklarını öğrenme ve etkilenmenin getirilerini çoktan anlamış durumdadırlar. Davranışlardaki önemli değişimleri anlamak müşterilerin başka ürünlere yönelme eğilimlerini etkileme şansını arttırmaktadır. Bu izleme daha önce de çeşitli başka müşteri bağlılık kartları gibi araçlarla yapılmakta idi. İnternet yolu izleme tabi ki pazarlamacılara nerede ise anında stratejilerini adapte etme imkânı verdiğinden dolayı çok güçlü bir araçtır. Yukarıda bahsedilen NYT (*New York Times*) makalesinde pazarlamacıların tüketicilerin davranış değişikliklerini izleyerek onların hamile ya da eşlerinden boşanmak üzere olduklarını öngörebildiklerine işaret edilmektedir. İzlemenin büyük ekonomik getirisi olmasına karşın aynı zamanda ciddi şekilde mahremiyetin ihlali sorunlarını gündeme getirmektedir.

Kuruluşlar faaliyetlerinin haklı gösterebilmek için sıklıkla "gizlenecek bir şey yok" argümanını öne sürmektedirler – eğer bir bireyin gizlenecek herhangi bir şeyi yoksa mahremiyeti ile neden bu kadar hassas olsun? Solove bu görüşü, mahremiyete ilişkin dar bir kavram anlayışına, gizliliğe veya bilginin saklanmasına dayandığı için karşı çıkmaktadır. Solove aynı zamanda mahremiyete ilişkin tehlikelerin sadece istenmeyen zarar ve etkileri olması gerekmediğine de işaret etmektedir. Bilgi toplama programları, insanların saklamak istedikleri bilgilerin hiçbir tanesine bile erişilemediğinde de problemlidir. Toplanan bilgiler yanlış ya da değiştirilmiş olabilir ve sonuçta yanlış kararların alınmasına neden olabilir. Bu da sukutu hayal yaratacaktır. Potansiyel zararlı etkiler hata, istismar, şeffaflıktan yoksun olma ve güvenirlik kaybı olacaktır.

B. Hizmet sunumu ve fiyatlandırmada ayrımcılık

İzleme ve profillemenin bir başka sonucu da hizmette ayrımcılık ya da dışlamadır. Profilleme bir kullanıcının belirli bir hastalıktan muzdarip olduğunu ya da böyle bir hastalığa yakalanmaya eğilimli olduğunu ortaya koyabilir. Bu bilgi sağlık sigortası kuruluşunu söz konusu kişiyi sigortalamak istememesine ya da daha yüksek prim istemesine neden olabilir. Fiyat ayrımcılığının hikâyesi çok eskidir ve günümüzde de yaygın bir uygulamadır. Güncel olarak da alıcıların yaşı ya da cinsiyeti gibi özellikleriyle açıkça ilişkilendirilerek gerçekleştirilmektedir. İzleme ve profilleme ile hizmet ve fiyatlandırma her bir müşteri için ona özel yapılabilmektedir.

C. Kişiye özelleştirmenin riskleri

Profilleme, önceki bölümlerde de söz edildiği gibi hizmet sağlayıcılar tarafından içeriklerin kişiselleştirilmesi amacı ile sık sık kullanılmaktadır. Bir haber sitesi, önceki okuma modellerine göre haberleri kişilere gösterebilir. Bir satış sitesi sadece tüketicinin önceki ilgi alanlarına, ihtiyaçlarına ya da tercihlerine uyan ürünleri o tüketiciye gösterebilir. Arama motorları sonuçları, bir kullanıcının önceki arama ve tıklamalarına uygun ayıklayabilir. Ve tabi ki çevrim içi reklamlar sıklıkla davranışsal hedeflidir. Bu kişiselleştirme ilgi gösterilmesi gerekli bir nedendir. Eli Pariser tarafından tartışıldığı şekilde, hizmetin kişiselleştirilmesi ile kullanıcılar bir "balon"cuğa hapsedilmekte ve onlar, dünya görüşlerini genişletebilecek başka bilgilere erişememektedirler. Otoriter ülkelerde, kişiselleştirme, haberlerin bazı kullanıcılar için seçilerek gösterilmesi ile sansürün arttırılması amacı ile de kullanılabilmektedir.

Tam aksine, içerik ve hizmetin kişiselleştirilmesi aynı zamanda bilginin sızdırılması için bir kaynak olabilmektedir; Çünkü bir tüketicinin ilgilerini, ona sağlanan içerik/hizmetlerden bazı tekniklerle anlamak ve çıkartmak mümkündür. Örneğin bir kullanıcının *Google* geçmişi, onun arama isteklerinden kısmen yeniden yapılandırılabilmekte ve bir kullanıcının profili, ona hedeflemiş reklamlardan

çıkartılabilmektedir. Bir başka örnekte de bir adam, *US superstore*'dan kendisine gelen bebek maması kuponlarından kızının hamile olduğunu anlamıştır; çünkü kızı satınalma davranışları ile hamile olarak profillenmiştir.[154]

II. Çevrimiçi izleme ve profillemenin riskleri ve getirdiği tehditlere koruyucu önlemler

A. Teknolojik Önlemler / Pazar Temelli Çözümler

1. Görselleştirme ve engelleme araçları (*Visualisation and blocking Measures*)

Collusion ya da *PrivacyBucket* gibi bazı "*browser plugin*"ler kullanıcılara izleyicilerin kendileri hakkında ne kadar bilgi edinebileceklerini gösterebilmektedir. Ayrıca üçüncü taraf izleyicilerin tümünü yada belirlenen bir kısmını bulmaya ve engellemeye imkan verecek başka bir çok "*browser tools*" ve "*plugin*"ler vardır. Örneğin bir *Firefox add-on*'u olan *NoScript*, *JavaScript* gibi işletilebilir bir içeriğin çalıştırlmasına, ancak güvenilir bir alanda "*host*" ediliyorsa müsaade etmektedir. *BetterPrivacy Firefox plugin*'i süper çerezler sorununu hedefleyerek, *hard drive*'daki Flash çerezleri tespit etmekte ve düzenli olarak silmektedir. Diğer benzer araçlar arasında *Ghostery, DNT, Plus ve AdBlock Plus* sayılabilir.

TPL (*Tracking Protection List* – İzleme Koruma Listesi) yaklaşımı, farklı organizasyonlar tarafından düzenlenmiş ve uygun olmayan izleme yapan sitelerin web adreslerini içeren bir listeye dayandırılmıştır.

Bunlardan başka üçüncü taraf izlemeye özel olmayan ancak yine bir miktar koruma sağlayan bazı mahremiyeti güçlendirici araçlar da vardır. Bunların örnekleri

[154] Bkz. *Castelluccia/Arvind*, ENISA European Network and Information Security Agency, s. 13-14, 19 October 2012,

arasında önemli bilinen tarayıcıların ya da isimsiz ağların özel *browsing mode*'ları vardır.

Opt-out: İzleme kuruluşlarının birçoğu bu süreci basitleştirmek için kullanıcıların *BeefTaco* gibi bazı opt-out çerezleri kurmalarına *ve Beef Taco* gibi bazı araçları kullanmalarına müsaade etmektedir. Birçok reklam ağı da bu çerezleri yönlendirilmiş reklamları opt-out etme aracı olaraka değerlendirseler de kullanıcıları izlemeye ve profillemeye devam etmektedirler. Önde gelen tarayıcılardalar da Beni İzleme *DNT* başlığı uygulamasını yapmakta olup bu başlıkla kullanıcıya izlenmek istemediği web sayfalarını seçme ve tanımlama imkânı sağlamaktadırlar

2. Mahremiyet tabanlı tasarım ve Mahremiyet Koruyucu Sistemler (*Privacy-by-Design* ve *Pricacy-Preserving Systems*)

Mahremiyet tabanlı tasarım, mahremiyetin daha etkili korunması yönünde önemli bir adım olarak değerlendirilmektedir. Yeni bilgi ve iletişim teknolojileri ile mahremiyetin daha fazla tehdit altında kaldığı bir dünyada, giderek benimsenen öneri çözümün bir kısmının yine bu teknolojilerden gelmesi yönündedir. Teknoloji tarafında PET'ler (*Privacy Enhancing Technologies* - Mahremiyeti Güçlendirici Teknolojiler) bilgisayar bilimlerinde on yıllardır aktif bir araştırma konusu olmuş ve çeşitli teknikler önerilmiştir (isimsizleştirme, kimlik yönetim sistemleri, mahremiyet *proxy*'leri, kripto mekanizmaları ve isimsiz *credential*'lar vb gibi). Ancak mahremiyet tabanlı tasarım PET'lerinin kullanımının ötesindedir; mahremiyet gerekleri bir sistemin tasarımının ilk adımlarında dikkate alınmalıdır ve bunların sistemin genel mimarisi üzerinde potansiyel etkisi olacaktır. Bir başka ifade ile mahremiyet tabanlı tasarım bir paradigma değişimidir; "tedavi ediciden çok önleyicidir". 1974 lerde "Adil Bilgi Uygulaması", daha sonra uyarı-ve-tercih, veri bütünselliği ve yaptırımcı mekanizmalar gibi bir dizi genel mahremiyet ilkeleri önerilmiştir.

Yeni olarak da *Adnostic*, *PrivAd* ve *RePriv* gibi mahremiyeti belli başlı bir tasarım gereği olarak gören bazı davranışsal reklam sistemleri de önerilmiştir. Bu

yapıların temel hedefi, bir taraftan davranışsal reklamcılığa destek verirken diğer taraftan izlemeyi kısıtlandırmasıdır. *Privad* izlememeye ve mahremiyetin hedeflenmesine tamamen teknik bir yaklaşım öngörmektedir. Müşteri bir bir kullanıcı profili yapılandırır, aracıdan bu profile uygun reklamları talep eder. Güvenilir taraf reklam ağının kişiyi belirlemesini önlemek üzere kişiyi anonimleştirir. Anonimleştirme performansı etkiler ve tıklama-ile-izlemenin gereçekleştirmesini zorlaştırır. *Adnostic*'te tarayıcı (eklenti –*add-on*- aracılığı ile) kullanıcının davranışsal profilini, onun tarayıcı faaliyetleri ile ilişkili olarak, sürekli güncelleştirir. Reklam ağı da söz gelimi 10 yerine sadece 1 reklamı kişiye yönlendirir; tarayıcı kullanıcı profiline bakarak söz konusu bir taneyi seçer. Reklamlara tıklamalar mahremiyet olarak değerlendirilmez. İzlemenin engellenmesi teknikten çok sözleşmeye dayalıdır. *RePriv*'nin hedefi ise daha genel olup tarayıcıda ilgi profillemesi yolu ile kişiselleştirmeye olanak sağlamaktadır. Uygulamalar kişiselleştirilmiş arama, web sitelerinin kişiselleştirilmesi ve reklam hedefleme şeklindedir. Hedefleme yerel olarak yapılmamakta, ancak onun yerine davranışsal profil sunucuya tarayıcıdan gönderilmeyi içermektedir.

B. ABD, AB ve Türkiye'de Düzenleyici Yasal Temelli Yaklaşımlar

1. ABD

FTC, davranışsal reklamcılığını "tüketicilerin internet üzerindeki eylemlerini analiz eden ve tüketicilerin ilgi alanlarıyla alakalı olduğu tespit edilmiş reklamlar sunan, gelişmiş bir teknolojiye dayanan bir pazarlama yöntemi" olarak tanımlamaktadır. FTC, 2007 yılında, davranışsal reklamcılığa dair bazı ilkeler sunmuştur. Bu ilkeler, "(1) davranışsal reklamcılık amacıyla bilgi toplayan web siteleri, kullanıcılara verilerin reklam amacıyla toplandığını bildiren açık ve kolayca görünebilir bir ifade koymalı ve bu web siteleri tüketicilere tercih etme seçeneği sunmalıdır, (2) tüketicilerin verilerini toplayan şirket web siteleri, bu verilere dair makul bir güvenlik seviyesi sağlamalıdır ve verileri sadece meşru bir iş veya yasaların uygulanması amacıyla gerekli olduğu sürece elinde

bulundurmalıdır, (3) tüketicilerin verilerini toplayan ve kullanan şirketler, bu verileri veriler toplanırken belirtilen amaçlar dışında kullanmadan önce kullanıcıların onayını almalıdır, (4) tüketicilerin hassas bilgilerinin toplanması, tüketicilerin seçimine bırakmak yerine, yasaklanabilir" şeklindedir. Ancak FTC, hangi bilgilerin hassas olduğuna dair halkın yorumlarını dinlemek istedi. Dolayısıyla davranışsal reklamcılık hakkında bir rapor çıkardı. Bu raporda konu hakkındaki yorumlar ve öneriler yer almaktadır. Bu rapora http://www.ftc.gov/opa/2009/02/behavad.shtm adresinden erişilebilmektedir. [155]
New York, eyalet sınırları içinde davranışsal reklamcılığı düzenleyen bir yasa tasarısı çıkan ilk eyalettir. 2008 Üçüncü Kişi İnternet Reklamcılığı Tüketici Hakları Yasası (*Third Party Internet Advertising Consumers Bill of Rights Act of 2008*) olarak adlandırılan bu yasa, davranışsal reklamcılığın kullanımına dair "kişinin hastalık geçmişi ve mali bilgileri hakkında veriler toplanamaz, toplanılan veriler korunmalıdır, çevrimiçi gizlilik yönergeleri uygulanmalıdır" gibi katı kurallar ve koşullar getirmekte olup; tüketicilerin verilerini toplayan üçüncü taraf şirketlerin uyması gereken "tüketiciler verileri toplayan şirketin veri toplama, kullanma, iletme ve raporlama politikaları ve uygulamalarından haberdar edilmelidir" gibi özel kurallarla birleştirilen verilerin (gönderilen veriler) kullanımı konusunda üçüncü kişilere uygulanan belirli kuralları da içermektedir. Yasa tasarısı, bu yasayı ihlal eden şirketler aleyhinde ihlal başına 1.000 Dolarlık veya şirketin belirli bir kalıpta ihlallerde bulunması durumunda 3.000 Dolarlık hukuk davası açma yetkisi vermektedir.[156]

a) FTC Davranışsal Reklamcılık Düzenlemesi

ABD Federal Ticaret Komisyonu, çevrimiçi pazar ortaya çıktığından beri, çevrimiçi gizlilik konularının ve sorunlarının üzerine odaklanmıştır. Bugün FTC; Gramm-Leach-Bliley Yasası, Çocukların Çevrimiçi Gizliliğinin Korunması Yasası (*Children's Online Pricacy Protection Act*), 2003 CAN-SPAM Yasası (*Controlling*

[155] Bkz. Arias, http://www.ftc.gov/opa/2009/02/behavad.shtm
[156] Bkz. Arias, http://www.ftc.gov/opa/2009/02/behavad.shtm

the Assault of Non-Solicited Pronographt and Marketing Act of 2003) ve Tele-pazarlama ve Tüketici Dolandırıcılığının ve Suiistimalinin Önlenmesi Yasası (*Telemarketing and Consumer Fraud and Abuse Act*), Aramama Kuralı (*Do Not Call Rule*) gibi sektöre özgü birtakım gizlilik kanunlarının uygulanması sorumluluklarını da üstlenmiş durumdadır.

FTC 1995, 1996 ve 1997 yıllarında, tüketici verilerinin gizliliği konularına dair halka açık çalıştaylar düzenlemiş; bu çalıştaylarda, çevrimiçi reklamcılık sektörünü savunan kişiler sektörün kendi kendisini düzenlemesi, yani öz düzenleme konusunda baskı yaparken, gizlilik yanlıları da öz düzenlemenin sadece "yasal bilgi gizliliği hakları" ile desteklendiği zaman başarılı olabileceğini iddia etmişlerdir. Sektörün lobicileri ise, tüketici "çekilmediği" ve şirketi, pazarlamaya yönelik gibi belirli bir şekilde kişisel bilgilerini kullanmamasını bildirmediği sürece, şirketlerin kişisel bilgileri bir gizlilik politikasında veya başkaca bir bildirimde belirtilen amaçlara yönelik olarak kullanmasına olanak veren "çekilme" sistemini savunmuşlardır. Gizlilik yanlıları ise tüketicilerin önceden onayının alınmasını savunmuş ve tüketicilerin gizlilik tercihlerini otomatik olarak bildirmesi için bir yazılım kullanılabileceğini önermişlerdir.

FTC 1998 yılında, ticari web sitelerinin gizlilik uygulamalarının açıklamalarını kapsamlı bir şekilde gözden geçirdiği ve Adil Bilgi Uygulaması İlkeleri'ni belirlediği bir rapor yayımlamıştır. Raporda sonuç olarak şu belirtiliyordu; "Komisyon'un yaptığı incelemenin sonuçlarının kanıtladığı üzere ve Komisyon'un, tüketicilerin gizlilik endişelerine yönelik olarak öz düzenleyici bir sistemi destekleyen üç yıllık gizlilik girişimine rağmen, çevrimiçi işletmelerin büyük çoğunluğu henüz en temel adil bilgi uygulamasını bile (bildirim/haberdar etme) uygulamaya sokmamış durumdadır."

FTC, 1999 yılında halka açık bir çalıştay daha düzenlemiş ve 2000 yılının Mayıs ayında bir rapor yayımladı. Bu raporda ilk kez, Meclis'in tüketici odaklı web siteleri için temel bir veri gizliliği koruması seviyesi oluşturmak amacıyla çevrimiçi gizlilik mevzuatı çıkarması önerilmiş idi.

FTC, 2000 yılının Temmuz ayında, ilk kez Çevrimiçi Davranışsal Reklamcılığa yönelik (veya o zamanki adıyla çevrimiçi profilleme) olarak internet

kullanıcısının gizliliğini korumak için bir mevzuat çıkarılması gerektiğini önermiştir. FTC ayrıca şunları belirterek; "Tüketicilerin gizliliğinin çevrimiçi olarak korunmasını sağlamak için, çevrimiçi profillemeyi ele alan bir mevzuata hala ihtiyaç vardır" ve "profilleme ile alakalı olarak tüketici odaklı ticari web sitelerinin" kullanıcılarının gizliliklerine yönelik temel koruma seviyesi ortaya koyan teknolojiden bağımsız bir mevzuatın çıkarılması gerektiğini önermiştir. FTC'nin 2000 önergesi kapsamında, tüketicilerden veya tüketiciler hakkında bilgi toplanmasına izin veren tüm çevrimiçi reklam ağları ve tüketici odaklı ticari web sitelerinin Adil Bilgi Uygulamaları'nı uygulaması ve bunlara uygun hareket etmesi gerekecekti.

Meclis, FTC'nin önerdiği mevzuatı yasalaştırmadı ve FTC'nin tekrar Çevrimiçi Davranışsal Reklamcılığı düzenleyecek bir mevzuat önergesi sunması için bir on yıl daha geçecekti.

FTC Başkanı Timothy Muris 2001 yılında şunları ifade ederek, FTC'nin odak noktasını çevrimiçi gizlilik ve Çevrimiçi Davranışsal Reklamcılıktan başka konulara çevirdi; "İnternettin büyümesinin yavaşlaması, çevrimiçi gizlilik mevzuatının bedelini anlamamız gerektiğini gösteriyor… Şu anda yasaların daha çok uygulanmasına ihtiyacımız var, daha çok yasaya değil". [157]

Düzenleme konusuna tekrar odaklanma: FTC, 2006 yılında, "gelecek on yılda tüketicilerin deneyimlerini şekillendirecek temel teknolojik ve iş gelişmelerini" inceleyen "*Tech-ade*" isimli Kasım 2006 FTC Forum'unda çevrimiçi gizliliğin korunmasıyla tekrar ilgilenmeye başladı. Foruma katılan kişiler, çevrimiçi profilleme alanındaki teknolojik gelişmelerin, bu uygulamanın daha yaygın ve etkili olmasına olanak sağladığını açıkladı.

FTC, *Tech-ade* oturumlarındaki açıklamalar üzerine, 2007 yılının Kasım ayında "Davranışsal Reklamcılık: İzleme, Hedefleme ve Teknoloji" isimli bir genel katılımlı toplantı düzenledi ve bu toplantıda özellikle, davranışsal reklamcılık uygulamalarının gizlilikle ilgili yansımaları ve etkilerine odaklanıldı. Davranışsal reklamcılığın büyümesi ve büyük internet şirketlerinin dar bir şekilde hedeflenen

---

[157] Bkz. *FTC, Reg. OBA, Wikipedia* http://en.wikipedia.org/wiki/FTC_regulation_of_behavioral_advertising

reklamları sunmak için bu teknikleri daha çok kullanmaya başlaması da kısmen bu toplantının yapılmasına sebep oldu. Bu gelişmeler arasında, *Google*'ın *DoubleClick*'i alma planları, AOL'un *Tacoda*'daki hisseleri ve *Microsoft* ve *Yahoo*'nun kendi davranışsal reklamcılık ürünlerini sürekli genişletmesi de vardı.

FTC, 2007 yılının Aralık ayında, çevrimiçi reklamcılık sektörünün gizlilik endişelerini ele almaya yönelik öz düzenleyici çalışmaları için bir temel sunmayı amaçlayan bir takım "ilkeler" yürürlüğe koydu. Bu ilkeler, "şirketlerin, verilerin toplanması esnasında vaat edilenden esas itibariyle farklı bir şekilde verileri kullanmadan önce ve davranışsal reklamcılık amacıyla "hassas" tüketici verilerini toplamadan ve kullanmadan önce, tüketicilerin açık onayını almasını" gerektirmekte idi.

FTC, 2007 yılındaki bu raporuna takiben 2009 yılında bir rapor daha yayımladı ve bu raporda, öz düzenleme ilkeleri açık bir şekilde belirtiliyordu. O dönemlerde, bir tüketici grubu birliği, 2007 yılındaki genel katılımlı toplantıdaki yorumlarında "İzleme" [*DNT*] sistemini önermişti. [158]

b) FTC'nin 2010 Raporu

FTC, 2010 yılının Aralık ayındaki raporunda, tüketici verilerinin gizliliğine dair yeni bir düzenleyici çerçeve önerdi ve bu önerge, internet kullanıcılarının çevrimiçi davranışsal reklamcılık kapsamından çekilmesine olanak sağlayan "İzleme" [*DNT* sistemini de içeriyordu.

FTC bu raporda, mevcut bildirim ve tercih modelinin sınırlamalarını açıklıyordu ve bunu "son yıllarda gitgide daha belirgin hale gelmiştir" şeklinde ifade ediyordu. FTC, bildirim ve tercih temelli modelin, "şirketlerin, bilgi toplama ve kullanma uygulamalarını tüketicilere açıklayan gizlilik bildirimleri hazırlamaya teşvik ettiğini ve böylece tüketicilerin, durumdan haberdar olarak tercihler yapabildiğini" belirtiyordu. Ancak, uygulanan bildirim ve tercih modeli, tüketicilerin anlamayı bir kenara bırakın, genel olarak okumadığı uzun ve

---

[158] Bkz. *FTC, Reg. OBA, Wikipedia* http://en.wikipedia.org/wiki/FTC_regulation_of_behavioral_advertising

anlaşılması zor gizlilik politikalarının hazırlanmasına sebep oldu. Benzer şekilde, zarar tabanlı model de itibara verilen zarar veya takip edilme korkusu gibi gizlilikle ilgili oldukça çeşitli endişeleri dikkate almaması sebebiyle eleştirildi. [159]

Bu sorunları bildirim ve tercih bazlı modelle çözmek isteyen FTC'nin önerdiği gizlilik çerçevesi, şirketleri tüketicilere çevrimiçi davranışsal reklamcılığa dair anlamlı bir tercih hakkı sunmaya çağırıyor, ancak "genel kabul gören uygulamalar" adı verilen "tercihin gerekli olmadığı sınırlı veri uygulamaları" öngörüyordu. Genel kabul gören uygulamalar arasında şunlar vardı: ürün ve hizmetin yerine getirilmesi, iç faaliyetler, dolandırıcılığı önleme, yasal uyumluluk ve birinci taraf pazarlama (içeriksel pazarlama dâhil). [160]

Raporda çevrimiçi davranışsal reklamcılığın, derin paket analizi ile birlikte özellikle "genel kabul gören uygulamalar" olmadığı belirtilmektedir. Ayrıca raporda, FTC'nin çevrimiçi davranışsal reklamcılık için "hassas bilgilerin" (çocuklarla ilgili bilgiler, mali ve tıbbi bilgiler ve konum belirleme verileri) toplanmasıyla alakalı olarak önceden "açık onayın" alınmasını desteklediği ifade edilmektedir. [161]

DNT ("İzleme")**:** FTC, 2010 raporunda, çevrimiçi davranışsal reklamcılık için DNT adı verilen "tek tip ve kapsamlı bir tüketici tercihi sistemi" önerdi. Raporda şu ifade yer alıyordu: "Çevrimiçi davranışsal reklamcılığa yönelik tek tip bir tercih sistemi için en uygulanabilir yöntem muhtemelen, tüketicinin tarayıcısına kalıcı bir çerez yerleştirmeye benzer bir ayar oluşturulması ve bu ayarın, tüketicinin takip edilmeyi veya hedefli reklamları almayı istediğinin veya istemediğinin tarayıcının girdiği sitelere aktarılmasıdır." FTC'nin görüşüne göre, DNT sistemi daha "net, tespit edilmesi kolay ve etkili" olduğu ve kullanıcının takip edilmekten çekilme tercihini doğrudan web sitelerine aktardığı için mevcut tarayıcı tabanlı çerezden vazgeçme modeline göre daha uygundu. [162]

---

[159] Bkz. *FTC Staff Report*, Federal Trade Commision, *s.iii,* December 2010

[160] Bkz. *FTC Staff Report*, Federal Trade Commision, *s.iii,* December 2010

[161] Bkz. *FTC, Reg. OBA, Wikipedia* http://en.wikipedia.org/wiki/FTC_regulation_of_behavioral_advertising

[162] Bkz. *FTC Staff Report*, Federal Trade Commision, *s.66-67,* December 2010

FTC, Kongre'ye Gidiyor: FTC, 16 Mart 2011 tarihinde, ABD Kongresi Ticaret Komitesi'ne çıktı. FTC, görüşmeler esnasında, davranışsal reklamcılık için izinsiz takip karşısında internet kullanıcılarını korumak amacıyla daha sıkı önlemler alınmasını ve tarayıcılara evrensel bir Takip Etmeme ayarının yerleştirilmesini önerdi.

FTC ayrıca, yanıltıcı çekilme mekanizması kullanmasından ötürü ağ reklamcısı Chitika aleyhinde açılan ilk davranışsal reklamcılık davasını açıkladı. FTC, uzlaşmanın bir parçası olarak, *Chitika*'nın tüm reklam yapısını gelecekte etkili bir çekilme sistemiyle ilişkilendirmesini istedi. Bu konu; "çevrimiçi reklamlara iliştirilmiş hyperlink koşulu, "Takip Etmeme" sistemi zorunlu hale gelirse FTC açısından kabul edilebilir türde bir "Takip Etmeme" mekanizmasının güzel bir göstergesidir" şeklinde yorumlanmıştı.

Aynı görüşmede, Barack Obama yönetimi, FTC'ye çevrimiçi davranışsal reklamcılığı düzenleme yetkisi verebilecek olan yeni "internet kullanıcısı hakları yasası" çağrısında bulundu.

Meclis Mevzuatı Sunuyor: 2011 "Beni Çevrimiçi Takip Etme" Yasası: Kongredeki California temsilcisi Jackie Speier, FTC'ye çevrimiçi reklamcıların ve web sitelerinin kullanıcılara, takip etmeme mekanizmasının oluşturulması sayesinde çevrimiçi işlemlerinin takip edilmesinden çekilmesine olanak sağlamasını gerektirecek düzenlemeleri yürürlüğe koyma yetkisi verecek olan "*2011 Do Not Track Me Online* Yasası"nı takdim etti. Yasa kullanıcılara, çevrimiçi davranışsal reklamcılık için verilerin toplanmasını engelleme gücü veriyor, ancak dolandırıcılığı önleme ve envanter kontrolü gibi genel kabul gören uygulamaları bu işlemin dışında tutuyordu. Önerilen düzenlemeler, yıllık 10.000'den daha az ziyaretçiye sahip *web* siteleri için bir istisna hükmü içermesine rağmen, yasa ayrıca FTC'ye *web* yayımcılarının rastgele denetimlerini yaparak yeni düzenlemeler yürürlüğe koyma yetkisi veriyordu. [163]

2011 Kerry/McCain Ticari Gizlilik Hakları Yasası: 12 Nisan 2011 tarihinde Senatör John Kerry ve yasayı birlikte hazırlayan Senatör John McCain, "2011

[163] Bkz, *Speier*, http://speier.house.gov/index.php?option=com_content&view= article&id= 203&Itemid=46, Washington, 2014

Kerry/McCain Ticari Gizlilik Hakları Yasası"nı takdim etti. Yasanın takdimine yönelik basın toplantısında, Senatör Kerry ve Senatör McCain yasanın iş dünyası ile tüketicinin çıkarları arasında bir uzlaşma sağladığını söyledi ve yasanın *Microsoft*, *Intel* ve *eBay* tarafından desteklendiğini belirtti.

Bu yasa, FTC'ye, özellikle çevrimiçi davranışsal reklamcılığı hedef alan kurallar geliştirme görevi veriyordu; bu kapsamda yasa, şirketlerin tüketicilerine, üçüncü kişilerin "davranışsal reklamcılık veya pazarlama" için onların kişisel tanıtıcı bilgilerinin kullanmasına yönelik bir "sağlam, açık ve belirgin" reddetme hakkı *(opt-out*) mekanizması sağlamasını gerekli kılıyordu.

Yasa ayrıca, FTC'nin, tüketicilerin isimleri ve e-posta adresleri gibi kişisel tanıtıcı bilgilerini toplayan işletmelerin "tüketicilerin" kişisel tanıtıcı bilgilerinin izinsiz kullanımı için açık ve belirgin reddetme hakkı sistemi" ile birlikte, verilerin toplanması, kullanılması ve aktarılmasına ilişkin "açık, az ve öz ve zamanında bildirim" sağlamasını gerektiren düzenlemeler hazırlamasını öngörmekte idi.

Yasada, "hassas kişisel tanıtıcı bilgilerinin toplanmasına, kullanımına veya aktarılmasına" önceden izin alınmasını (*opt-in*) gerektiren bir hüküm de yer alıyordu. Kişisel tanıtıcı hassas bilgi "tek başına veya başkaca bilgilerle beraber kaybolması veya izinsiz açıklanması halinde, önemli ekonomik veya fiziksel zarar riski taşıyan bilgi" veya bir kişinin belirli bir sağlık durumu, tıbbi kaydı veya dinsel bağlantısı ile ilgili bilgi olarak tanımlanmaktadır.

Yasa ayrıca FTC'ye, tüketicilere çevrimiçi davranışsal veya konum tabanlı reklamcılıkla ilişkili olarak "açık, belirgin, kalıcı ve etkili" bir reddetme hakkı sağlayacak, öz düzenleyici (*self regulatory*) programları gözden geçirmek, onaylamak ve izlemek amacıyla, gönüllü bir güvenli liman programı oluşturma görevi veriyordu. FTC, böyle bir öz düzenleyici programı onayladıktan ve o programın üyeleri güvenli liman tarafından kapsandığı zaman, bu üyeler yasanın bazı hükümlerinden muaf olabilecek idi.

Yasada, FTC'nin önerdiği İzlememe (*Do Not Track Me*) mekanizması yer almamaktaydı. Senatör McCain basın toplantısında bu konuda şunları söylemiştir; "Bu mekanizma tüketici ile sektör desteği arasındaki dengeyi sağlama kabiliyetimize uygun düşmüyordu".

Yasa saklı dava hakkı içermemekte; uygulama FTC'ye ve eyalet savcılarına bırakılmış durumdaydı. Tüketici ve gizlilik yanlıları ise yasanın yeterince güçlü olmadığını ve FTC'nin İzleme (DNT) önerisini de içermesi gerektiğini belirtmişlerdir. [164] [165]

c) FTC'nin 2012 Nihai Raporu

Bu rapor FTC'nin Aralık 2010 da yayınladığı rapordan sonra aralarında iş çevreleri, mahremiyet savunucuları, teknolojistlerden ve bireysel tüketiciler olmak üzere çeşitli paydaşlardan 450 geri bildirim almıştır. Bu kapsamda sanayicileri de kapsayan geniş bir paydaş grubu çerçevede yer alan ilkeleri desteklerken; birçok kuruluş da bu ilkeleri uygulamakta idi. Aynı zamanda bazı yorum yapanlar da kendi-kendine düzenlemenin gelişme hızının yavaş olduğunu ileri sürdü ve Kongre'nin artık bir temel mahremiyet mevzuatını oluşturma zamanının geldiğine işaret ettiler.

2010 raporunda 21. yüzyüyılda tüketici mahremiyetini korumak üzere bir çerçeve öneriliyordu. Önerilen bu çerçeve, ilk düzenlenişinden bugüne kadar 40 yıl geçmiş olan Adil Veri Uygulama İlkeleri ile uyumlu idi. Bu önerinin temelinde:

- Tasarım ile Mahremiyet: Gizlilik, ürün geliştirmenin her safhasında yapılandırılmalı;
- İş Çevreleri ve Tüketiciler için Basitleştirilmiş Seçimler: Tüketicilere kendi verileri ile ilgili kararları, DNT mekanizması da dâhil olmak üzere, uygun zaman ve içerikte yapabilme becerisini kazandırılmalı; bu sağlanırken gereksiz seçenekleri sağlamaya çaba gösteren ilgili iş çevreleri üzerindeki yükü biraz hafifletmek ve
- Daha Fazla Şeffaflık: Veri toplama ve kullanım uygulamalarının şeffalığını sağlamak vardı.

---

[164] Bkz. *FTC, Reg. OBA, Wikipedia* http://en.wikipedia.org/wiki/FTC_regulation_of_behavioral_advertising

[165] Bkz. *Kang/Washington Post*, http://www.washingtonpost.com/blogs/post-tech/post/senators-introduce-internet-privacy-bill/2011/04/12/AFL0CjRD_blog.html

Komisyon bir ön rapor yayınladığı için, Kongre de mahremiyetle ilgili olarak DNT ve Gençlere İlişkin Mahmremiyet konularını da kapsayan genel ve odaklı bazı yasa önergelerini gündeme getirmişlerdir. Endüstride özellikle *Do Not Track Me* olmak üzere bazı alanlarda bir miktar iyileştirmeler sağlamıştır. Ancak başka alanlarda endüstrinin gelişim hızı oldukça düşük olmuştur. Dolayısı ile yukarıdaki bölümde de daha ayrıntılı söz edilen 2010 raporunda önerilen mahremiyeti koruma önlemlerinden tüketiciler henüz tam olarak yayarlanamamışlardır. Komisyon aynı zamanda endüstriden kendi-kendine düzenleme hızının da arttırılması için baskı yapmaktadır.

Yönetim ve bazı Kongre üyeleri temel mahremiyet yasasının yasallaşması için çağrıda bulunmaktadırlar. Komisyon Kongre ve diğer paydaşlarla bu yasallaşma sürecinde işbirliği yapmaya hazırdır. Ön rapor tarihinden bugüne kadar ki gelişmeler aşağıda özetlenmiştir.

Aralık 2010'dan bu yana kanunların uygulama sorunları ile ilgili olarak Komisyon'ca yapılanlar*:*

- *Google* ve *Facebook* için kanuni yaptırımlar gündeme getirilmiştir. Bu kapsamda kuruluşların verilerle ilgili uygulamalarını değiştirmeden önce tüketicilerin olumlu rızalarını en hızlı şekilde almaları ve bağımsız dış denetçilerin 20 yıl süre ile değerlendirmesine açık şirketin tümünde uygulanan mahremiyet programlarını benimsemeleri istenmekte idi. Bu gereklerin dünya çapında bir milyardan fazla kullanıcıyı koruyacağı öngörülmekte idi.
- Reddetme Hakkı - *Opt out* - uygulamalarını göz ardı ederek etkisiz kılan kuruluşlar için yaptırımlar getirilmiştir. Bu çerçevede uygulanması istenen önlemler tüketiciler kendilerinin reklamcılar tarafından izlenmelerini reddettiklerinde – *opt out* – seçimlerinin gerçekten etkin olması şeklinde tasarlanmıştı.
- Çocukların Çevrimiçi Mahremiyetlerinin Korunması Kanununu ihlal eden mobil uygulamalar ile tüketicinin kişisel verilerinin kendisinini farkında olmadan paylaşımına neden olan önceden tanımlanmış hazır mahremiyet ayarlarına yaptırımlar getirilmiştir.

- Tüketici listelerini, Adil Kredi Raporlama Yasası ihlal ederek pazarlamacılara satan kuruluşlara karşı yaptırımlar getirmiştir
- Veri güvenliğini makul sınırlar içerisinde sağlayamayan şirketler için yaptırımlar getirmiştir

Aralık 2010'dan bu yana FTC ve ekipleri tarafından siyasal alanda gerçekleştirilen çalışmalar*:*

- Gizlilikle ilgili birisi çocuk kimlikleri hırsızlığı diğeri de yüz tanıma teknolojileri ile ilgili iki çalıştay organize edilmiştir.
- Kongrede gizlilik ve veri güvenlik konularında on defa görüşmeye katılınmıştır
- FCC, HSS de (*Department of Health and Human Services* - Sağlık ve İnsani Hizmetler Bakanlığı) dâhil olmak üzere çeşitli federal kurumlarla söz konusu kurumların gizlilik konusundaki girişimleri ile ilgili olarak görüşmeler yapılmıştır. Komisyon, Ticaret Bakanlığının farklı endüstriyel sektörlerin gizlilikle ilgili mesleki davranış ilkelerinin oluşturulması için paydaşlarını biraraya getirme girişmini desteklemiştir
- Çocuklara yönelik mobil uygulamalar konusundaki bir veri toplama araştırma sonuçlarını yayınlamıştır
- Çocukların Çevrimiçi Gizlilik Kanunu'na değişiklik önerisinde bulunmuştur.

Aralık 2010'dan bu yana Komisyonca eğitim alanında yapılanlar:

- FTC'nin tüketici çevrimiçi portali *OnGuardOnline.gov* üzerinden çeşitli formatlarda – makaleler, oyunlar, testler ve videolar – tüketicinin bilgisayarlarını güvence altına almak ve kişisel bilgilerini korumalarına yardımcı olmak amacı ile yürütülen süregelen çabalar. Bu portal ayda yaklaşık 100,000 farklı ziyaretçi almaktadır.
- Kimlik hırsızlığı, *Wi-Fi* bağlantı bölgeleri, çerezler ve mobil cihazlarla ilgili olarak tüketicilere eğitici malzemeler yayınlanmıştır.
- Bireylerin geçmişleri ile ilgili kontroller yapan mobil uygulama pazarlamacılarına onları Adil Kredi Raporlama Kanunu hakkında eğitmek üzere uyarı mesajları gönderilmiştir.

Aralık 2010'dan bu yana Komisyonca kendi-kendine denetimi (özdenetimi) teşvik etme konusunda yapılanlar:

- Özellikle çevrimiçi davranışsal izlemede geliştirilmiş açıklamalar ve seçenekler için çağrısı sürdürmüştür. Bu çağrılara karşılık olara ve Kongre'nin ilgisine olmak üzere gerçekleşenler:
    - Bazı tarayıcı satıcıları, tüketiciler için onlara, web sayfalarının çevrimiçi faaliyetlerini izlememelerini talep etmelerine imkân verecek tarayıcı-temelli araçlar geliştirdiler.
    - Bir internet standartları belirleme organizasyonu olan *World Wide Web* Konsorsyumu üniversal bir Beni İzleme (*DNT*) protokolü geliştirmeye girişti.
    - Medya ve pazarlama organizasyonlarının bir koalisyonu olan DAA (*The Digital Advertising Alliance* - Dijital Reklamcılık Birliği), tüketicilerin bir ikonu tıklayarak erişebilecekleri ve bu yolla çevrimiçi davranışsal reklamcılığın kendisi ve nasıl reddebileceği hakkında bilgi edinebilecekleri bir mekanizma geliştirdi. Ayrıca DAA tüketici verilerinin kredi, istihdam gibi ikincil amaçlar için kullanımını önlemek ve tüketicinin kendi tarayıcıları üzerindeki ayarlardan yapmış olduğu seçimlere riayet edilmesi konularına önemle ilgi gösterdi.
- Asya Pasifik Ekonomik Forumuna üye ülkeler arasında hareket eden tüketici bilgilerinin gizliliğinin korunmasını düzenlemek ve güçlendirmek için sınır ötesi yasal gizlilik kurallarının geliştirlme çalışmalarına katılınmıştır. [166]

[166] Bkz. *FTC Report 2012*, http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy s. i-iii, March 2012

d) ABD'deki Yasal Durumun Özet Değerlendirilmesi

FTC tüketicinin korunmasında lider düzenleyici kurumdur. FTC genel kanun koyucu otoriteyi daraltacak kısıtlılıklar getirmiştir: o ancak "haksız ya da yanıltıcı" iş uygulamalarını önleyebilmektedir; bu yönde kurum, tüketicilere hızlı bir taahhüttün ihlali gibi çok geniş bir ihlalin mevcudiyetini talep etmektedir. FTC sadece tekrar eden kural ihlalcilerine para cezası verebilmektedir. Uygulamada ise FTC'nin daha çok yumuşak gücü olduğunu görmekteyiz; iş çevreleri bir federal kanunun zorunlu kılınmasının maliyetini, yükünü ve etkilerini taşımaya istekli gözükmemektedir. Konuya giderek artan ilgisine ilişkin sinyal veren FTC 2011 de üçüncü taraf *web* izlemelerine ilişkin iki zorlayıcı girişimi gündeme getirmiştir.
Eyalet Baş Savcılarının da üçüncü taraf izlemelerini regüle etmek üzere benzer yetkileri vardır. Ancak bugüne kadar izleme ile ilgili olarak hiçbir başsavcılık güçlendirici bir girişimde bulunmamıştır. Üçüncü taraf web izleme uygulamaları ile ilgili olarak bazı avukatlarca federal ve eyalet düzeyinde yapılmış iddianameler vardır. İlk davalarda bazı kuruluşlar multi-milyon dolarlık anlaşmalar yapmayı kabul etmişlerdir (örneğin, *Flash* çerezlerin kullanımı ile ilgili olarak *Quantas*). Yakın tarihlerdeki trend ise kendilerine karşı dava açılan kuruluşların davalarının düşmesi şeklindedir.[167]

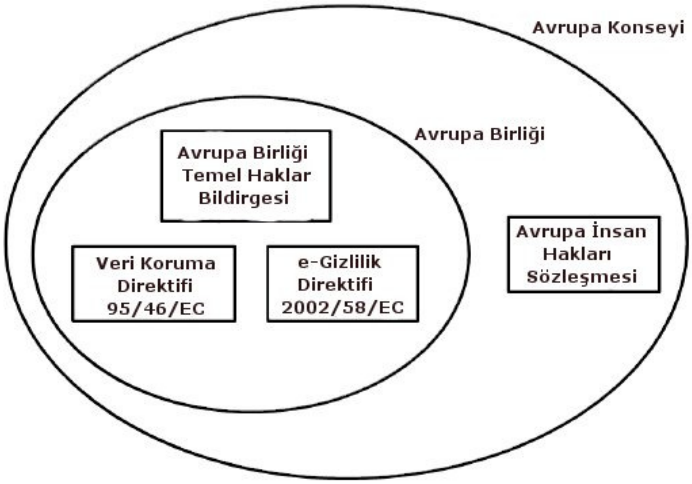
Yasal çerçeveyi özetlemek gerekirse, Amerika Birleşik Devletleri Hukukunda, Avrupa Birliği Hukukundaki 1995 Veri Koruma Hakkı paralelinde kişisel bilgilerin gizliliğini düzenleyen genel bir veri mahremiyeti hakkı bulunmamaktadır. Amerika Birleşik Devletlerinde mahremiyet hukukunu kapsayan bir düzenleme olmamasına rağmen, mevcut koşullardaki kanunlar uyarınca bazı kategorilerdeki bilgilerin gizliliği korunmaktadır. Örneğin FCRA (Fair Credit Reporting Act - Adil Kredi Raporlama Yasası) bazı şartlar altında olmak üzere kişilerin finansal bilgilerinin gizliliğini korumaktadır. Bir diğer adıyla finansal hizmetlerin modernizasyonu yasası olan GLBA da (Gramm-Leach-Bliley Act - Gramm-Leach-Bliley Yasası)

[167] Bkz. *Castelluccia/Arvind*, ENISA European Network and Information Security Agency, s. 13-14, 19 October 2012

bazı finansal verileri korumaktadır. Tıbbi veriler HIPAA (Health Insurance Portability and Accountability Act - Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası) ile korunmaktadır. Çocukların verileri ise COPPA (Children's Online Privacy Protection Act - Çocukların Çevrimiçi Gizliliğini Koruma Kanunu ile korunmaktadır). Gizlilikle ilgili olan bu mevcut düzenlemeler değiştirilmiş olan ve dolayısıyla veri sahibinin tanımlanamadığı verileri genel manada korumamaktadırlar. Federal Ticaret Komisyonu tanımlanmamış olan finansal bilginin kümelenmiş bir halde muhafaza edildiği müddetçe kullanılmasına izin vermiştir. Ancak bu veriler, yardımcı verilerle birleştirildiklerinde yeniden özdeşleştirme faaliyetine konu olabilmektedirler. Buna rağmen bu faaliyete konu olan veriler hassas veri kapsamında değerlendirilmektedirler. Amerika Birleşik Devletlerindeki gizlilikle ilgili olan kaygılar, gizliliğin ihlali söz konusu olduğunda bu ihlalin kasten serbest bırakılmış ve tanımlanabilen kişisel verilerden kaynaklandığını yansıtmaktadır.

2. Avrupa Birliği

Bu bölümde, davranışsal reklamcılık ve özellikle (kişisel) verilerin işlenmesine izin veren çerezlerin ve gelecekteki takip etme teknolojilerinin kullanımına yönelik yasal bir çerçeve ortaya koyan Avrupa hukuku ele alınmaktadır. İlk bölümde, AİHS ve ABTHB ile incelenmektedir. Ayrıca, veri korumasını ve gizliliğini ele alan iki AB direktifinin konumuzu en fazla ilgilendiren maddeleri ele alınmıştır Son bölümde ise, AB mevzuatına dair elde edilen başarılara ve çözülmeyen sorunlara ilişkin bir değerlendirme yapılmıştır



Şekil 10 Uygulanan Yasa Yapısı
(Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.31-32)

Şekil 11'de farklı yasalar ve yargı bölgeleri gösterilmektedir. Avrupa İnsan Hakları Sözleşmesi, bu yapının en üstünde yer almaktadır. Avrupa Konseyi'ne üye ülkelerin vatandaşları, eğer haklarının ihlal edildiğini düşünüyorlarsa, ülkelerindeki yasal çözüm yollarını tükettikten sonra, mahkemeye gidebilmektedirler. Avrupa Birliği'ne üye ülkeler ise ulusal hukuklarında Avrupa Birliği Temel Haklar Bildirgesi'ne uymak ve aynı zamanda Veri Koruma Direktifi 95/46/EC ve e-Gizlilik Direktifi 2002/58/EC'yi uygulamak zorundadırlar.

Şekil 11 İki direktif arasındaki ilişki
(Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.31-32)

Genel elektronik iletişim konusunda e-Gizlilik Direktifi 2002/58/EC her zaman geçerlidir. Bu *Şekil 12*'de gösterilmektedir. Veri Koruma Direktifi ise sadece kişisel veriler kullanılırken geçerlidir.

a) Avrupa İnsan Hakları Sözleşmesi

AİHS, gizlilik konusunu Madde 8'de ele almaktadır:

Madde 8 – Özel ve Aile Hayatına Saygı Hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.[168]

Madde 8 iki bölüme ayrılmıştır. Birinci bölümde, gizlilik hakkı tanımlanmıştır. İkinci bölümde ise, gizlilik hakkını geçersiz kılabilecek istisnai durumlar ele alınmıştır. Temel olarak, sadece hükümetler ile vatandaşlar arasındaki ilişkilerde geçerlidir.[169]

Stefan Sottiaux, Madde 8(1)'in birbiriyle yakından bağlantılı olan dört farklı alanı koruduğunu belirtmektedir. Sottiaux'a göre, "Sözleşme makamları, özel hayatın detaylı bir tanımını vermeyi açık bir şekilde reddetmektedir, bunun yerine bu olgunun sınırlarını oluşturan, insan hayatının farklı alanlarını tespit etmişlerdir" Sottiaux, bu konuyla ilgili davaları inceleyerek, Madde 8'i analiz etmektedir. Madde 8'de, Madde 8'i ihlal etmenin yasal olabilmesi için öncelikle dört koşulun yerine getirilmesi gerekmektedir:

1. Bir ihlalin yasayla öngörülmüş olması gerekir.

---

[168] Bkz. *AİH Sözleşmesi*, Adalet Bakanlığı, Ankara, http://www.inhak.adalet.gov.tr/temel/aihs.pdf,

[169] Bkz. *Van Bebber*, Radboud University Nijmegen, Master Thesis Information Science, October 11, 2011, s.32-33

2. Bir ihlalin, demokratik bir toplumda gerekli olması gerekir.

3. İhlal eden önlemlerin, meşru bir amaca sahip olması gerekir.

4. İhlalin, meşru amaçla alakalı olarak orantılı olması gerekir.

Açık ve ulaşılabilir olmalı ve aynı zamanda gerekli korumalar sağlanmalıdır. Ayrıca, baskı unsuru bir sosyal ihtiyaç ve meşru amaç olmalıdır (Madde 8(2)).

Örneğin, bir eylem sırasında resim çekilmesine izin verilmektedir. Özel hayat, aleniyetten tamamen korunmamaktadır. Madde 8(2) sınırlamaları ele almaktadır. Sadece yasa uyarınca ve demokratik bir toplumda gerekli olduğunda gizlilik konularına müdahaleye izin verilmektedir. [170] Vatandaşların gizli bilgilerini elinde bulunduran üçüncü kişiler de Madde 8 kapsamına girmektedir. Mahkemeye gidip, reklam ağlarının Madde 8'i ihlal ettiğini iddia etmek mümkün değil, çünkü daha önce de belirttiğimiz üzere, bu madde sadece hükümetler ile vatandaşlar arasındaki ilişkilere uygulanıyor. Ancak vatandaşlar, hükümetin davranışsal reklamcılığı yeterli seviyede ele alan koruyucu önlemler sağlamadığını iddia edebilirler (Madde 8 ile ilgili olarak). Dolayısıyla, Madde 8 geniş bir çerçeve sunmaktadır ve ayrıca davranışsal reklamcılık için de geçerlidir.[171]

Davranışsal reklamcılık tüzel kişiler (kuruluşlar) ile vatandaşlar arasında meydana gelir. İlerleyen bölümlerde, ulusal mevzuatın bilgi gizliliğini ve veri korumasını nasıl sağlayabileceğini ele alan iki AB direktifinden bahsedilecektir.

b) Avrupa Birliği Temel Haklar Bildirgesi

AB'ye üye ülkeler, ABTHB'ne tamamen uymak zorundadır. Ülkelerin iç hukuku da bu bildirgeyle uyumlu olmalıdır. Bildirgenin 7. ve 8. maddelerinde gizlilik ve kişisel bilgiler konuları ele alınmaktadır:

---

[170] Bkz. *Sottiaux,* Law and Politics Book Review, Vol. 18 No. 7 (July, 2008) s.673-*676*, http://www.lawcourts.org/LPBR/ review s/sottiaux0708.htm

[171] Bkz. *Kilkelly AİHM Md. 8 Klvz.,* İnsan Hakları Genel Müdürlüğü, Avrupa Konseyi, Cedex, s.35, http://www.ihop.org.tr/index.php?option=com_content&task= view&id =34&Itemid=64

Madde 7. - Özel ve aile yaşamına saygı

Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.

Madde 7, Avrupa İnsan Hakları Sözleşmesi Madde 8(1)'e oldukça benzemektedir, ancak önemli bir fark vardır. Madde 7'de, yazışma yerine haberleşme terimi kullanılır. Yazışma terimi daha çok mektuplarla ilgiliyken, haberleşme terimi her türlü bilgi alışverişini kapsar.

Madde 8. - Kişisel bilgilerin korunması

1. Herkes, kendisine ilişkin kişisel bilgilerin korunmasını isteme hakkına sahiptir.
2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.
3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.

Madde 8'de, kişisel bilgilerin korunması ele alınmaktadır. Madde 8'in içeriği daha somuttur, ancak yine de farklı yorumlamalara yer bırakmaktadır. Veri Koruma Direktifi 95/46/EC ve e-Gizlilik Direktifi 2002/58/EC'de yer alan hükümlere yakından baktığımızda ise, Madde 8'in içeriğinin her iki direktif için de tek bir temel hak oluşturduğunu görüyoruz.[172]

c) Veri Koruma Direktifi (95/46/EC)

Avrupa Birliği 1995 yılında, kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı hakkında bireylerin korunması hakkında 95/46/EC sayılı Direktif'i yürürlüğe koymuştur. Direktif kapsam, orantılılık, şeffaflık ve meşru amaç itibariyle önce genel anlamda değerlendirilmiş; daha sonra direktifin davranışsal reklamcılık alanındaki yansılamaları ve etkileri ele alınmıştır.

---

[172] Bkz. *EU, Charter Fund. Rights*, Official Journal of the European Communities, s. C 364/10-11, **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 12012P/ TXT: EN:NOT**

Genel Giriş ve Kapsam: Direktif'in 2. maddesinde, ilgili terimlerin tanımları verilmektedir. Davranışsal reklamcılık açısından ise en önemli terimler şunlardır:

(a) "kişisel veri" fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özel bir veya daha fazla faktöre veya bir kimlik numarasına atıf başta olmak üzere doğrudan veya dolaylı olarak tespit edilebilen bir tespit edilebilir kişi; tespit edilmiş veya tespit edilebilir gerçek kişiye ("veri öznesi") ilişkin herhangi bir bilgiyi kastedecektir;

(b) "kişisel verilerin işlenmesi (işleme)", silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisini kastedecektir;

(d) "denetleyici", kişisel verilerin işlenme araçlarını ve amaçlarını tek başına ya da diğerleriyle ortaklaşa belirleyen gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir; işleme amaçları ve araçları ulusal veya Topluluk hukuku veya yönetmelikleriyle belirlendiğinde, denetleyici veya atanması için özel kriterler, ulusal veya topluluk hukukuyla belirlenebilir;

(e) "işleyici", denetleyici adına kişisel verileri işleyen bir gerçek veya tüzel kişiyi, kamu makamını, devlet dairesini veya diğer bir kuruluşu kastedecektir;

(f) "üçüncü şahıs", veri işlemek için yetkilendirilen işleyici veya denetleyicinin doğrudan yetkisi altındaki kişiler ve işleyici, denetleyici, veri öznesi dışındaki herhangi bir gerçek veya tüzel kişi, kamu makamını, devlet dairesini veya başka bir kuruluşu kastedecektir;

> (h) "veri öznesinin rızası", kendisine dair kişisel verilerin işlenmesi için veri öznesinin kabulüne işaret eden, özgürce ve bilgilendirilme yapıldıktan sonra alınan rızayı kastedecektir.[173]

Görüldüğü üzerinde denetletici, işleyici ve üçüncü şahıs birbirinden ayrılmaktadır. Sadece denetçi amacı belirleyen kuruluş olarak tanımlanmıştır. İşleyici, kişisel verileri denetleyici adına işlemektedir ve verileri başka bir amaç için verileri işleyemez. İşleme ayrıca üçüncü şahıslar tarafından da yapılabilmektedir. Bu yüzden üçüncü şahıs terimi eklenmiştir. Denetleyici en üstte, üçüncü şahıslar da en altta olacak şekilde açık bir hiyerarşi vardır. Ayrıca, veri öznesinin rızası da tanımlanmıştır. Kişisel verilerin toplanabilmesi ve işlenebilmesi için, önce veri öznesinin kişisel verilerin toplanmasını kabul etmesi gerekmektedir.

3. maddede ise direktifin kapsamı tanımlanmaktadır. Direktif 95/46/EC "kişisel verilerin kısmen veya tamamen otomatik araçlarla işlenmesine uygulanacaktır[174] […]". Direktifin sadece, Madde 2(a)'da tanımlanan kişisel verilerin işlenmesine uygulandığını belirtmemiz gerekir.

Kişisel veriler sadece şu garanti edildiği zaman işlenebilmektedir: orantılılık, şeffaflık ve meşru bir amaç.

Orantılılık: Madde 6'da orantılılık ele alınmaktadır ve Madde 6(2)'de denetleyicinin, kişisel verilere dair aşağıdakileri temin etmesi gerektiği belirtilmiştir (Madde 6(1)):

(a) adil ve yasal olarak işlenmiş

(b) belirli, açık ve meşru amaçlar için toplanmış ve bu amaçlarla uyumsuz biçimde başkaca işlenmemiş

(c) yeterlidir, ilgilidir ve bu amacı aşmaz

(d) doğrudur ve gerektiği yerde güncel tutulur

---

[173] Bkz. *EU, Data Protection Dir.* 95/46/E*C,* Official Journal of the European Communities, s.I - 238 /38-39, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[174] Bkz. *EU, Data Protection Dir*. 95/46/E*C,* Official Journal of the European Communities, s.I-238/39, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

(e) verilerin toplandığı esnada veya sonrasında işlendiği amaçlar için gerekenden daha uzun olmayan süre boyunca, veri öznelerinin tespitine izin veren biçimde tutulur[175]

Ayrıca Madde 8, 14 ve 15'te de orantılılık konusu ele alınmıştır. Madde 8, veri öznesinin açık rızasını verdiği durumlar haricinde, "ırk veya etnik kökeni, sağlık durumunu veya cinsel yaşamı açıklayan kişisel verilerin işlenmesini […]" yasaklamaktadır. Oldukça fazla miktarda veriye sahip olan reklam ağları, veri madenciliği tekniklerini kullanarak bu tür verileri açığa çıkartabilirler. Dolayısıyla, 8. madde orantılılığı doğrudan ele almamaktadır. 14. Madde ise veri öznelerine, doğrudan pazarlama amacıyla kişisel verilerin işlenmesine itiraz etme hakkı vermektedir. Kişisel verileri toplamak isteyen reklam ağları, veri öznesini sadece hakları hakkında bilgilendirmekle kalmayıp (Madde 10, 11 ve 12), aynı zamanda veri öznesine itiraz etme hakkı vermek zorundadır. Madde 15'te ise, bireysel kararın bir sözleşmeye imza atma sürecinde alındığı durumlar haricinde, bir kişinin yalnızca verilerin otomatik işlenmesine dayalı bir karara tabi kalmama hakkı olduğunu belirtilmektedir. Grup profilleme, otomatik işlemeye dayanır ve bu yüzden veri öznelerinin itiraz hakkı olmalıdır. Bu hak sadece yasal sonuçlar oluştura spesifik durumlar veya önemli etkide bulunma durumlarında verilebiliyor. Bu yüzden kalıcı bir haktan ziyade daha çok bir istisna olarak karşımıza çıkıyor. Lee A. Bygrave de bu konudan bahsetmekte ve 15. maddede vaat edilen şeyin, karmaşıklık ve çeşitli belirsizliklerle anlamını yitirdiğini söylemektedir [176]. Ayrıca, hakkın geçerli olabilmesi için öncelikle birçok koşulun da yerine getirilmesi gerekli.[177]

Şeffaflık: İkinci ilke olan şeffaflık, Madde 7, 10, 11 ve 12'de ele alınmaktadır. Kişisel verilerin işlenmesi konusunda sadece 6. madde

---

[175] Bkz. *EU, Data Protection Dir*. 95/46/E*C,* Official Journal of the European Communities, s.I-238/40, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[176] Bkz. *Bygrave*, Computer Law and security Reporter Vol 17, s.1-14, http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf,

[177] Bkz. *EU, Data Protection Dir*. 95/46/E*C,* Official Journal of the European Communities, s.I-238/40-41; 42-43, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

uygulanmamakta,- ayrıca, 7. maddenin koşullarından birinin de karşılanması gerekmektedir.- Örneğin, öncelikle öznenin rıza vermesi veya işlemenin bir sözleşmenin yerine getirilmesi için veya yasal yükümlülüklere uymak için yapılması gereklidir. Uygulamada ise yasada belirsiz bir alan vardır. Veri denetleyicilerinin çoğu, veri işleme şekillerinin bir istisna oluşturduğunu ve dolayısıyla rızanın gerekli olmadığını savunmakta başarılı olmakta, kişisel verileri işlemediklerini söylediklerinde ise, direktifin hiçbir bölümü uygulanmamaktadır. Madde 10, 11 ve 12'de veri öznesine erişi hakkıyla beraber verilmesi gereken bilgiler ele alınmakta, denetleyicinin kimliği ve işlemenin amaçlarının veri öznesine açıklanması gerekmektedir. Erişim hakkı ise veri öznesinin denetleyiciden "ilişkin verilerin otomatik işlenmesiyle ilgili mantık bilgisi […]" alma hakkını içermektedir (Madde 12).[178]

Meşru Amaç: Üçüncü ilke olan meşru amaç ise Madde 6(1)(b)'de ele alınmaktadır. Kişisel veriler sadece belirli bir amaca yönelik olarak işlenebilir ve veri öznesinin rızası olmadan diğer amaçlar için işlenemez. Madde 25(1)'de ise kişisel verilerin sadece yeterli koruma seviyesi temin eden üçüncü ülkelere transfer edilebileceği, Madde 25(2)'de de koruma seviyesinin yeterliliğinin, veri transferini çevreleyen tüm koşullar ışığında değerlendirileceği ifade edilmektedir. 25. maddede, üçüncü ülke tarafından temin edilebilecek koruma seviyesinin nasıl belirleneceği konusunda açık bir yönerge verilmemektedir. Reklam ağı sağlayıcıları genellikle farklı ülkelerde faaliyet göstermekte ve bu yüzden, üçüncü bir ülkeye kişisel veri transfer etmek istedikleri zaman, 25. maddeye uymak zorundadırlar[179].

---

[178] Bkz. *EU, Data Protection Dir*. 95/46/E*C,* Official Journal of the European Communities, s.I-238/40; 41-42, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[179] Bkz. *EU, Data Protection Dir*. 95/46/E*C,* Official Journal of the European Communities, s.I-238/40; 45-46, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

ca) 95/46/EC Veri Koruma Direktifinin Davranışsal Reklamcılığa Yansımaları

95/46/EC sayılı Direktif'in kapsamı, kişisel verilerin işlenmesi ile sınırlı olup anonim veri işleme konusunda geçerli değildir. Reklam ağlarının çoğu, kişisel bilgileri toplamadıklarını söylemektedir. Bir reklam ağı kişisel bilgileri topladığı zaman, veri öznelerinin 12. maddeye göre reklam ağına, kişisel veriler işlenirken ne tür teknikler kullandıklarını sorma hakkı vardır. Otomatik bireysel karar alım (Madde 15), bir kişi tarafından aynı bilgiye dayanılarak alınan kararla karşılaştırıldığında, avantajlı veya dezavantajlı bir şekilde veri öznesini etkileyebilir. Dolayısıyla, otomatik karar alım olumlu ve olumsuz yan etkiler doğurabilir. Bunun ayrıca davranışsal reklamcılık açısından da yansımaları vardır, çünkü veri özneleri reklamlardan çıkarılabilir veya örneğin sunulan ürünler, belirli bir veri öznesi grubu için farklı fiyatlara sahip olabilir. Burada yasa koyucuların, 15. madde dışındaki tüm maddelerde veri öznesi terimini kullandıklarını belirtmemiz gerekmektedir. Madde 15'te ise her kişi ifadesi kullanılmaktadır. Terminolojideki bu değişiklik, tüm maddeler arasındaki karşılıklı bağımlılığı anlamayı daha da zorlaştırmaktadır.

Schreurs ve diğ. profillerin oluşturulmasını engelleyebileceği için Veri Koruma Direktifi'nin grup profillemeye uygulanması gerekmesinin önemli olabileceğini belirtmektedir. Ayrıca Schreurs ve diğ. Veri Koruma Yasası'nın grup profillemeye uygulanmasına iki konuya daha işaret etmektedir. Bunların birincisi, bir grup profilinin, o grup profilinin oluşturulması esnasında profile dâhil olmayan bir kişiye uygulanabilmesi ile uygulanan profilin kullanıldığı zaman ise kişisel veri haline gelmesi; İkincisi de, Veri Koruma Direktifinin sadece, kişisel veriler kullanıldığında grup profillemeye uygulanabilir hale gelmesi; dolayısı ile Veri Koruma Direktifi'nin uygulanabilir olup olmadığının belirlenmesini daha da zor hale getirmesidir[180]

[180]Bkz. *Schreurs ve diğ.*, Mireille Hildebrandt ve Serge Gutwirth (eds), Springer Link, s. 241-270, http://link.springer.com/book/10.1007/978-1-4020-6914-7 , 2008

d) e-Mahremiyet Direktifi (2002/58/EC)

Avrupa Parlamentosu ve Konseyi 2002 yılında 2002/58/EC sayılı e-Gizlilik Direktifi'ni yürürlüğe koydu. Direktif daha sonra, 2009 yılında 2009/136/EC sayılı Direktif ile değiştirildi. Bu bölümde de önce konuya genel bir giriş yapılıp, daha sonra davranışsal reklamcılıkla ilgili bulgular ele alınmıştır.

Genel Giriş: e-Gizlilik Direktifi, genel iletişim servisleri sağlayıcıları için veri koruması ve gizlilik yükümlülükleri konularına odaklanmaktadır. Sadece kişisel bilgi, gizlilik ve mahremiyet konularını ele almakla kalmayıp, aynı zamanda spam, web böcekleri ve çerezler hakkında da hükümler getirmektedir. Çerezlerin temel olarak davranışsal reklamcılıkta bir kişiyi tespit etmek için kullanıldığından, önceki bölümlerde bahsedilmiş idi. Veri Koruma Direktifi sadece bireyleri kapsarken, e-Mahremiyet Direktifi, tüzel kişiler için de geçerlidir (Madde 1(2)).

Bu direktifin kapsamı ve amacı Madde 1(1)'de açıklanmıştır. Direktif amacını, "kişisel verilerin işlenmesine dair temel hakları ve özgürlükleri ve özellikle de mahremiyet ve gizlilik hakkını" korumak olarak ortaya koymaktadır (Madde 1). Hem Veri Koruma Direktifi hem de e-Gizlilik Direktifi *kişisel veri* terimini kullanmaktadır, fakat e-Gizlilik Direktifi tarafından sağlanan ilgili korumalardan bazıları sadece verileri ilgilendirmekte dolayısıyla mutlaka kişisel veri olması gerekmemektedir. Ayrıca, Madde 1(2)'de e-Gizlilik Direktifi'nin Veri Koruma Direktifi'ni ayrıntılandırdığı ve tamamladığı belirtilmekte dolayısıyla iki direktif arasında açık bir ilişki kurulmuş durumdadır.[181]

2. maddede ise kullanılan terimler bağlamında kullanıcı, "bir hizmete abone olması gerekmeksizin, özel veya iş amaçlarına yönelik olarak kamuya açık bir elektronik iletişim hizmetini kullanan gerçek kişi" olarak tanımlanmıştır. Yani bu direktif tüm kullanıcıları kapsamaktadır. Ayrıca, ilgili hizmetlerden de "kamuya açık elektronik iletişim hizmetleri" olarak bahsedilerek (Madde 3) tüm hizmetler

[181] Bkz. *EU, e-Privacy Dir.*, Official Journal of European Community, http://eurlex.europa.eu /LexUriServ/LexUriServ.do?uri=CONSLEG: 2002L0058:20091219:EN:PDF, e-Privacy Directive 2002/58/EC, s. 10-11, 2009

için güvenlik önlemlerinin temin edilmesi (Madde 4) ve gizliliğin garanti edilmesi (Madde 5) gerektiği belirtilmektedir. Çerezler ise Madde 5(3)'de ele alınmıştır:

> "3. Üye Ülkeler, bir abonenin veya kulacının terminal cihazındaki bilgilerin depolanmasının veya hâlihazırda depolanmış olan bilgilere erişim sağlanmasının sadece ilgili abonenin veya kullanıcının, diğerler konulara ilaveten işlemenin amaçları hakkında 95/46/EC sayılı Direktif uyarınca kendisine net ve kapsamlı bilgi sağlanması sonucunda rıza vermesi şartıyla izin verildiğini temin edecektir. Bu bir elektronik iletişim ağı üzerinde bir iletişimin iletiminin gerçekleştirilmesi amacıyla veya abone veya kullanıcı tarafından açık bir şekilde talep edilen bilgi toplumu hizmetinin sağlayıcısı için hizmeti sağlaması amacıyla gerekli olan herhangi bir teknik depolamayı veya erişimi engellemeyecektir."[182]

Yani, kullanıcının rızası sadece kullanıcıya açık ve kapsamlı bir bilgi sağlandıktan sonra verilebilmektedir. Kullanıcının terminal cihazında bilgi depolanması kendi içinde zararsızdır, fakat depolanan bilgilere erişim birçok gizlilik endişesine yol açmaktadır. Ayrıca 2002/58/EC sayılı Direktif'in 24. ve 25. beyanı ve 2009/136/EC sayılı Direktif'in 66. beyanı çerezlerin kullanımını ele almaktadır. Bu üç beyan, "AB Yasal Mevzuatının Davranışsal Reklamcılığa Yansıması" bölümünde incelenmiştir.

Trafik verileri (Madde 6), artık gerekli olmadığı zaman silinmeli veya anonim hale getirilmelidir. Kullanıcının rızasını vermesi durumu bu bir istisna teşkil, etmekle birlikte böyle bir durumda kullanıcı verilerin saklanma amacı ve süresi hakkında bilgilendirilmelidir. 2006/24/EC sayılı Veri Saklama Direktifi, veri saklama konusunu detaylı bir şekilde ele almaktadır. Çoğu durumda, veriler en az altı ay ve en fazla iki yıl depolanmak zorundadır (Madde 6). Veri Saklama Direktifi tez konusu ile dolaylı ilişkisi olması nedeniyle bu çalışmada ayrıntılı olarak ele alınmamıştır.

---

[182] Bkz. *EU, e-Privacy Dir.*, Official Journal of European Community, http://eurlex.europa.eu /LexUriServ/LexUriServ.do?uri=CONSLEG: 2002L0058:20091219:EN:PDF, e-Privacy Directive 2002/58/EC, s. 11-14, 2009

Adres verileri ise, kullanıcı rıza verdikten sonra sadece ticari amaçlar için kullanılabilmektedir (Madde 13).

Özetle, direktifin bir "dâhil olma seçeneği" (*opt-in*) çözümü gerektirdiğini söyleyebiliriz. Hiçbir veri, rıza verilmeden önce toplanamaz, ancak direktif bilinçli rızanın nasıl yapılacağı konusunda net bir yol göstermemektedir. Ayrıca, direktif sadece çerezler gibi takip etme yöntemlerini ele almaktadır. Yükümlülükler daha sert ve katı hale geldikçe, reklam ağlarının yeni takip etme teknolojileri arayacağını varsaymak yanlış olmayacaktır. Örneğin davranışsal reklamcılık amacıyla derin paket analizi kullanılabilmektedir, fakat e-Gizlilik Direktifi'nde bundan bahsedilmemektedir.

e) AB 2000/31/EC Sayılı Elektronik Ticaret Direktifi

Bu çalışmada AB'deki elektronik ticaret direktifinden bahsedilmeye gerek duyulmamıştır. Bunun nedeni, Direktifin (A 2000/31/EC) Giriş Bölümünün 14. Paragrafında, "kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı konularında bireylerin korunması hakkındaki 95/46/EC sayılı Direktif hükümlerinin aynen geçerli olduğu ve bu nedenle 2000/31/EC de bu konunun ayrıca belirtilmesinin gerekli olmadığına" işaret edilmesidir (aynı şekilde kişisel verilerin telekomünikasyon sektöründe işlenmesi ve kişisel mahremiyete uyum konusunda da 97/66/EC Direktifinin aynı nedenlerle yeterli olduğu aynı paragrafın devamında vurgulanmaktadır).

ea) AB Yasal Mevzuatının Davranışsal Reklamcılığa Yansımaları

Reklam ağları kullanıcıları tespit etmek için çerezler ve web böcekleri kullanmaktadır. 2002/58/EC sayılı Direktif'in 24. beyanında, kullanıcıların terminal cihazında bilgi depolanmasını ele alınmaktadır:

> "Elektronik iletişim ağları kullanıcılarının terminal cihazı ve bu cihazda depolanan bilgiler, kullanıcıların özel alanının bir parçasıdır ve İnsan Hakları ve Temel Özgürlüklerin Korunmasına dair Avrupa

> Sözleşmesi kapsamında korunması gerekmektedir. Casus yazılımlar, web böcekler, gizli tanımlayıcılar ve benzer diğer araçlar, bilgilere erişim sağlamak, gizli bilgileri depolamak veya kullanıcının işlemlerinin izini sürmek için kullanıcının terminaline bilgisi olmaksızın girebilmekte ve dolayısıyla, ciddi bir şekilde bu kullanıcıların gizliliğine ve özel yaşamına girmektedir. Bu tür araçların kullanılmasına, ilgili kullanıcıların bilgisi dâhilinde olacak şekilde, sadece meşru amaçlar için izin verilmelidir."[183]

24. beyana göre, kullanıcının terminalinde bilgi depolanmasına sadece ilgili kullanıcıların bilgisi dâhilinde izin verilmektedir. Bu ifadenin, söz konusu ekipmanda depolanan herhangi bir bilgiye gönderme yaptığını belirtmemiz gerekir. Öyle gözüküyor ki bu direktif kişisel bilgi ile anonim bilgiyi birbirinden ayırmıyor. Frederic Debussere herhangi bir bilgi ifadesinin ayrıca Madde 5(3)'e tabi olduğunu öne sürmekte ve dolayısıyla bu direktifin, bir bilgisayarda depolanan bilgiler için uygulandığını belirtmektedir. Bilgilerin toplanması veya kullanıcının terminalinde depolanmasından önce, bilinçli rızanın alınması bir önkoşuldur. Ayrıca, davranışsal reklamcılığın ana parçalarından biri olan kullanıcı takibi, bu beyanda ele alınmıştır ve sadece rıza verildikten sonra izin verilmesi gerektiği belirtilmiştir.[184]

25. beyan ise açık bir şekilde çerezlerin kullanımını ele almaktadır:

> "Ancak, örneğin 'çerezler' gibi bu tür araçlar, web sitesi tasarımının ve reklamın etkililiğinin analiz edilmesi ve çevrimiçi işlemler yapan kullanıcıların kimliğini doğrulama gibi konularda meşru ve faydalı bir araç olabilir. Kullanıcıların kullanmakta oldukları terminal cihazına yerleştirilen bilgiden haberdar olmasını temin etmek için, kullanıcılara 95/46/EC sayılı Direktif uyarınca bu çerezlerin veya benzer araçların amaçları hakkında açık ve net bilgi sağlanması şartıyla, çerezler gibi bu tür araçlar, bilgi toplumu hizmetlerinin

---

[183] Bkz. *EU, e-Privacy Dir.*, Official Journal of European Community, http://eurlex.europa.eu /LexUriServ/LexUriServ.do?uri=CONSLEG: 2002L0058:20091219:EN:PDF, e-Privacy Directive 2002/58/EC, s. 5-6, 2009

[184] Bkz. *Debussere*, International Journal of Law and Information Technology Vol. 13 No.1, 2005, s.83

> sağlanmasının kolaylaştırılması gibi meşru bir sebep için kullanıldığında, bunların kullanılmasına izin verilmelidir. Kullanıcıların, terminal cihazlarında depolanan bir çerezi veya benzer aracı reddetme şansı olmalıdır […] Bilgi verme, reddetme hakkı sağlama veya kullanıcının rızasını isteme yöntemleri olabildiğinde kullanıcı dostu hale getirilmelidir. Spesifik web sitesi içeriğine erişim, meşru bir amaç için kullanılıyorsa bir çerezin veya benzer aracın bilgili bir şekilde kabul edilmesi koşuluna bağlanabilir."[185]

Çerezler *web* sitesi tasarımı ve reklamın analiz edilmesinde faydalı araçlar olarak tanımlanmıştır. Dolayısıyla bu beyan ayrıca çerezleri davranışsal reklamcılık bağlamında kabul etmektedir. 25. beyan ayrıca açık ve net bilgi gereksinimini ifade etmekte ve Veri Koruma Direktifi'ne gönderme yapmaktadır. 25. beyana göre kullanıcıların çerezleri reddetme şansı olması, kullanıcının rızasını isteme yöntemlerinin olabildiğince kullanıcı dostu olması ve kullanıcıya reddetme hakkı verilmesi gerektiğini söylemeliyiz. 25. beyan konuyu "çekilme seçeneği" (*opt-out*) olarak ele alırken, yeni Madde 5(3) ve 6(3) "dâhil olma seçeneği" (*opt-in*) gerektirmektedir. Ayrıca, 66. beyan da "çekilme seçeneğini" (*opt-out*) ifade etmektedir.

2002/58/EC sayılı e-Gizlilik Direktifi, bilinçli rızanın nasıl alınacağı konusunda herhangi bir yol göstermemektedir. Bu direktifte değişiklik yapan 2009/136/EC sayılı Direktif ise bilinçli rıza konusunu 66. beyanda ele almaktadır:

> "Üçüncü kişiler, meşru amaçlardan (belirli tipteki çerezler gibi) tutun da özel alana haksız bir şekilde girişe kadar (casus yazılım veya virüsler gibi) çeşitli amaçlara yönelik olarak bir kullanıcının cihazında bilgi depolamak veya depolanan bilgiye erişim sağlamak isteyebilir. Dolayısıyla, kullanıcıların söz konusu depolama veya erişim sağlamaya sebep olabilecek herhangi bir işlem yaparken kendilerine açık ve kapsamlı bilgi verilmesi hayati öneme sahiptir. Bilgi verme ve

[185] Bkz. *EU, e-Privacy Dir*., Official Journal of European Community, http://eurlex.europa.eu /LexUriServ/LexUriServ.do?uri=CONSLEG: 2002L0058:20091219:EN:PDF, e-Privacy Directive 2002/58/EC, s. 6, 2009

> reddetme hakkı sağlama yöntemleri, olabildiğinde kullanıcı dostu olmalıdır. […] Teknik açıdan mümkün ve etkili olan durumlarda, 95/46/EC sayılı Direktif'in ilgili hükümleri uyarınca, kullanıcının işlemeye dair rızası tarayıcıya eklenecek uygun ayarlarla veya başkaca bir uygulamayla verilebilir. […]"[186]

66. beyan açık bir şekilde, kullanıcının cihazında bilgi depolamak isteyen, reklam ağları gibi üçüncü şahısları ele almaktadır. Bir yandan, açık ve kapsamlı bilgi hayati öneme sahiptir, fakat diğer yandan, uygun tarayıcı ayarlarının kullanılması, rızanın verilmesi için yeterlidir. Çoğu internet kullanıcısının, bir arayıcı yüklerken varsayılan ayarları seçtiğini varsayabiliriz. Dolayısıyla, bu rıza daha çok tarayıcı sağlayıcılar tarafından, daha az ise internet kullanıcıları tarafından verilmektedir, çünkü varsayılan gizlilik ve çerez ayarlarının nasıl olacağına tarayıcı sağlayıcılar karar vermektedir.

Belki de bir yandan, tarayıcının kurulması ve uygun gizlilik ayarlarının seçilmesiyle rızanın verildiği öne sürülebilir, ancak diğer yandan, kullanıcıya açık ve kapsamlı bilgi verildiğini söyleyemeyiz, çünkü gizlilik ayarları genellikle düşük, orta veya yüksek gizlilik şeklinde açıklanmaktadır. Dolayısıyla, iki direktif de davranışsal reklamcılıkta bilinçli rızanın alınması sorununun nasıl ele alınacağına dair işaretler vermektedir, ancak açık ve net bir yol göstermemektedir. Reklam ağları, bazı hususların daha fazla ele alınmasını gerektiğini iddia edebilir ve kendilerine en uygun yorumlamayı tercih edebilir. Nitekim 95/46/EC sayılı direktifin 29. Maddesi ile kişisel verilerin işlenmesine dair bireylerin korunması hakkında danışma statüsüne sahip bir çalışma grubu kurulması ve ne şekilde oluşturulacağı öngörülmüş, 30. Madde'de de bu çalışma grubundan beklenenler sıralanmıştır.[187]

---

[186] Bkz. *EU, Amend to 2002/58/EC,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, 2009/136/EC, s.20

[187] Bkz. *e-Ticaret Direktifi 2000/31/AT,* Topluluk Resmi Gazetesi No: L 178, 17.07.2000 s. 0001-0016, e-Ticaret Merkezi.net http://www.e-ticaretmerkezi.net/abdirektif.php (erişim tarihi 28.02.2014)

f) AB'deki Yasal Durumun Özet Değerlendirilmesi

2002 ePrivacy Direktifi, 2002/58/EC, *web* sitelerini veri toplama uygulamaları ile ilgili bilgi vermelerini zorunlu kılıyor, kullanıcılarına tarayıcılarında kendileri ile ilgili bilgi bulundurulması seçeneğini, kullanıcı tarafından "açıkça talep edilmiş" hizmetlerin sağlanması için "kesinlikle gerekli" bilgiler hariç olmak üzere, reddetmelerine (opt out) imkân vermelerini gerekli kılıyordu. Uygulamada bu direktifin gücü çok az kaldı; Üye devletler uyumu sağlamak üzere hiçbir önlem almadılar ve birçok durumda tarayıcı çerez ayarlarını yeterli uygulama olarak kabul ettiler.

2009'da *ePrivacy* direktifine yapılan bir değişiklik, 2009/136/EC *opt-out* kuralının yerine *opt-in* onay kuralını getirdi. Üye Devletlerin uygulamaları başlangıçta farklılıklar gösterdi. Bazı ülkeler mevcut tarayıcı ayarlarının yeterli olduğu ve öylece kalmasını, bunların direktifte açıkça yazmasa da 'saklı onay' mesajı verdiğine işaret ettiler. Ancak çoğunluğun görüşü, regülasyonun son değişiklik önerisini onaylamakta ve her bir web sitesi için kullanımın açık ve olumlu onayının istenmesi gerekliliğini öngörüyordu. AB ve üye ülke yetkilileri bu kurala uyumu tüm ülkelerde hala güçlendirme ihtiyacındadırlar.[188]

g) AB'deki Son Gelişmeler

Ocak 2012 de AB Komisyonu 1995 veri Koruma Direktifinde (95/46/EC)veri koruması ile ilgili olarak yer alan ilkelerin günccellenmesi konusunda bir yasal günce paket önerisi getirdi. AB Komisyonu, politik amaçları doğrultusunda, daha güçlü yasal yaptırımlarla desteklenen, daha uyumlu, daha zorunlu iddialı bir AB veri koruma çerçevesi önerisi getirdi.

---

[188] Bkz. *Castelluccia/Narayanan*, ENISA European Network and Information Security Agency, s. 13-1419 October 2012,

21 Ekim 2013 tarihinde LIBE (Sivil Özgürlükler Adalet ve İç İşler Komitesi – *Civil Liberties, Justice and Home Affairs Committees*) Stratesbourg'ta merakla beklenen toplantısını yaptı ve Komisyon önerisini oya sundu. Oylamanın önceki toplantılarda ertelenmesinin nedeni uzlaşma sağlanamayan çok sayıda alanın bulunması ile regülasyon taslağında çalışmanın başlangıcından bu yana 3000 den fazla değişiklik yapılmış olması idi.

Komitede kabul edilen 2014 yılı içerisinde AB Parlamento'suna sunulacak olan taslağın önemli noktaları şöyle özetlenebilir:

- Yaptırımlar – veri koruma kurallarını çiğneyen kuruluşlar için 100 milyon Euro'ya ya da global cironun % 5 ine kadar cezalar öngörülmektedir (Komisyonun önerisi 1 milyon Euro veya global satışların %2 si kadardı).
- Muvafakat (Rıza) – Muvafakatin açık bir kanıtı gerekmektedir (beyan ya da olumlu bir hareket ile), rıza gösterilmemesi de, rızanın verilmesi kadar kolaylıkla olabilmelidir. Bir hizmetle ilgili taahhüt ya da provizyonun verilmesi, söz konusu hizmet için doğrudan gerekli olmayan verilerin işlenebilmesine rıza şartına bağlanmamalıdır.
- AEA'da (Avrupa Ekonomik Alanı) olmayan ülkelere veri transferi daha zorlaşıyor – Örneğin bir üçüncü ülke bir kuruluştan (ör. Arama motoru, sosyal ağ veya bulut sağlayıcı) işlenmiş kişisel bilgileri talep ettiğinde bilgi vermek durumunda olacaktır; kuruluşun, herhangi bir bilgiyi göndermeden önce yerel veri koruma otoritesinden yetki alması gerekecektir. Kuruluşun aynı zamanda kişisel bilgileri talep edilenen kişiyi de bilgilendirmesi öngörülmektedir. Veri transferini daha kısıtlayıcı önlemlerin Güvenli Limanları (*Safe Harbour*) riske etme potansiyeli taşımaktadır ve bu yakkaşım Haziran ayında medyada AB vatandaşları ile ilgili olarak yer alan kitlesel veri gözetimine karşı bir önlem gibi gözükmektedir.
- Kişisel verilerle birlikte kullanılmadığı zaman belirli bir bireye atfedilemeyen veriler olarak tanımlanan Takma İsimli (*Pseudonymous*) veri regülasyonda yer alan yeni bir kavramdır ve bu tür bilgiler ayrı bir yerde muhafaza edilir ve onlar ayrıca tanımlanmış kurallara tabidir. .

Pseudonymus veri, örneğin profillemem için gerekli veriler, daha "hafif" bir rejime tabidir.

- Silme Hakkı – Çok itibar gören "unutulma hakkı"nın yerine daha güçlendirilmiş (ve kalitesi arttırılmış) verileri "silme hakkı" getirilmiştir.
- Profilleme – Buna ilişkin verilerin işlenmesi, söz konusu verinin kişinin rızasını gerektiren yasal durumlar ile bir anlaşmanın varlığı durumu ile kısıtlanmaktadır. Verisi bu amaçla kullanılmak istenenlerin buna itiraz etme hakkları olup; böyle bir durumda onlara karşı bir ayrımcılık uygulanmamalıdır.
- Ömürboyu Veri Koruma Yönetimi – Önerilen bu geniş kavram, kişisel verileri işlenen bireylerin sayılarına dayalı olarak Veri Koruma Görevlileri tarafından kişisel mahremiyetlerinin etkilenme değerlendirilmesi ve yüz yüze görüşme yapılmasını gerektirmektedir.

Bu yasal düzenlememnin Mayıs 2014 deki seçimler öncesinde AB Parlamentosunda görüşülerek yürülüğe girmesi beklenmektedir.[189] [190] [191]

3. Türkiye

Özel hayatın gizliliğinin korunması kapsamında bulunduğu kabul edilen kişisel verilerin korunması kavramına Türk Hukukunda çeşitli düzenlemelerde yer verilmiş bulunmakla birlikte bu kavram ile ilgili herhangi bir tanım yapılmış değildir. Esasen, özel hayatın gizliliği konusu 1961 ve 1982 Anayasalarında düzenlenmiş ise de, bu düzenlemelerde özel olarak kişisel veri ve kişisel verilerin korunması kavramına yer verilmemiştir. Ancak kabul etmek gerekir ki kişisel veri

---

[189] Bkz. *O'Donoghue/Brimsted*, Global Regulatory Enforcement Law Blog, posted on October 22, 2013 by Christine Nielsen Czuprynski, 03 Mart 2014 http://www.globalregulatoryenforcement law blog.com/2013/10/articles/data-security/breakthrough-vote-by-european-parliament-sets-delayed-data-protection-overhaul-back-on-track/

[190] Bkz. *Suuberg*, Tullane Journal of Technical & Intellectual Property, Vol. 16, s.268-286, 2013

[191] Bkz. *EU/LIBE; Data Protection*, Inofficial Consolidated Version After LIBE Committee Vote Provided by the Rapporteur, 22 October 2013, http://www.janalbrecht.eu/fileadmin /material/ Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf

ve kişisel verilerin korunması kavramına uluslararası belgelerde de ancak son otuz yılda yer verilmeye başlanmıştır.

a) 1982 Anayasası (güncel düzeltmeler ve değişikliklerle)

1982 Anayasasının 20nci maddesi uyarınca "herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz". Anayasada sayılan haller dışında "kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz". Anayasamızın 22. Maddesine göre de "kimsenin konutuna dokunulamaz, istisnaî haller dışında kimsenin konutuna girilemez, arama yapılamaz ve buradaki eşyaya el konulamaz". Benzer şekilde, m. 22.'ye göre ise "herkes haberleşme hürriyetine sahip olup, haberleşmenin gizliliği esastır"; "haberleşme engellenemez ve gizliliğine dokunulamaz". Bunu yanı sıra "Kişinin Hakları ve Ödevleri" başlığı altında Anayasa m. 17/f.1'de "herkes maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir" yer alır. Madde 12 bu hakkı "Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir" ifadesi ile açıklamaktadır. Kişilerin, manevi varlıklarını korumak için, kural olarak kişisel verilerini işleyen herkese karşı kişiliğinin korunması m. 20 ile ilgili Ek fıkra: 12/9/2010-5982/2 maddede "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir isteyebilecektir" şeklinde ayrıntılı bir biçimde belirtilmektedir. Zira kişi ancak, çevresinin kendisi hakkında sahip olduğu bilgilerin bilincinde olarak manevi varlığını koruyabilecektir. Bu sebeple de, hangi kişisel verilerinin kime veya kimlere iletileceğini kontrol edebilme hakkına sahip olacaktır. Kısaca veri koruması

hakkı kişiye, hangi kişisel verilerinin kim tarafından ve kimin için hangi amaçla elde edildiğini öğrenme hakkı vermektedir. [192] [193]

b) Türk Medeni Kanunu

Özel hukukta kişilik hakkı genel anlamda, Medeni Kanun m. 23, 24 ve Borçlar Kanunu m. 49 çerçevesinde korunmaktadır. Medeni Kanun m.23, kişilik hakkını hukuki işlem yoluyla saldırılara karşı korurken (Kişiliğin Vazgeçme ve aşırı sınırlanmaya karşı korunması), m. 24'de hukuki işlem dışı saldırılara karşı (Kişiliğin saldırya karşı korunması) korumaktadır. Borçlar Kanunun 49. maddesi de Haksız Fiillerden Doğan Borç İlişkileri kapsamında "Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür" demektedir. Dolayısıyla kişilik hakkı ihlali ve bunun sonuçlarıyla ilgili Medeni Kanun ve Borçlar Kanunu maddeleri, kişilik ihlali hangi araçla ve hangi alanda gerçekleşirse gerçekleşsin uygulama alanına sahiptir; çünkü ceza hukukuna hâkim olan suçta ve cezada yasallık ilkesi özel hukukta geçerli değildir. [194] [195]

c) Türk Ceza Kanunu

Genel: Türk hukukunda kişisel verilerin ceza hukuku anlamında korunması öncelikle 26/9/2004 tarihli ve 5237 sayılı TCK'nun İkinci Kitap İkinci Kısmının "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı 135 ilâ 140 maddeleri çerçevesinde sağlanmaktadır.

B. Kişisel Verilerin Kaydedilmesi

---

[192] Bkz. *TCBMM/ANAYASA*, Türkiye Cumhuriyeti Büyük Millet Meclisi, s. 3-6, http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf

[193] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010, s. 89-90

[194] Bkz. *Mevzuat/T. Medeni K*. Türk Medeni Kanunu, s. 8052, http://www.mevzuat. gov.tr /MevzuatMetin/1.5.4721.pdf

[195] Bkz. *Mevzuat/Borçlar K*., Borçlar Kanunu, s. 10764, http://www.mevzuat.gov.tr /Mevzuat Metin/1.5.6098.pdf

5237 sayılı TCK'nun 135. maddesinin birinci fıkrasıyla, "hukuka aykırı olarak kişisel verilerin kaydedilmesi" eylemi suç haline getirilmiştir. Gerekçede de belirtildiği üzere suçun konusu kişisel verilerdir. [196]

TCK'da kişisel veri tanımına yer verilmemekle birlikte, Adalet Bakanlığı tarafından hazırlanan "Kişisel Verilerin Korunması Kanun Tasarısı"nda kişisel veri; belirli veya kimliği belirlenebilir bir kişiye ilişkin tüm bilgileri ifade eder" şeklinde tanımlanmıştır.

Maddenin ikinci fıkrasıyla ise "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi" eylemleri de birinci fıkraya paralel şekilde suç tipi olarak düzenlenmiştir.

Madde gerekçesinde de kişilerle ilgili bilgilerin çeşitli kamu kurumları ve özel sektör tarafından bilgisayar ortamında muhafaza edildiği, "bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan" kişilerin "büyük zararlara" uğrayabildiği, bu nedenle "kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınmasının suç olarak" tanımlandığı ifade edilmiştir.

Bu suç tipiyle T.C. 1982 Anayasasının 20. maddesinde bir temel hak ve özgürlük olarak belirtilen "özel hayatın gizliliği"; kişilerin özel yaşamına müdahale olanağı veren teknolojik gelişmeler ve buluşlar karşısında inceleme konusu suç tipiyle bir hukuksal değer olarak korunmakta ve böylelikle Anayasanın bu hükmü somut hale getirilmektedir. 135. maddede suçun işlenme şekli ve alanı sınırlandırılmamıştır. Suçun en çok işlenebileceği yer bilişim alanı olmakla beraber yalnız bilişim alanıyla da sınırlı değildir. Suç, "Kişisel verilerin hukuka aykırı olarak kayda alınması" "bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayrım gözetilmeden" - ile oluşturacaktır. Buna göre verilerin kaydedilmesi bir bilişim sistemine veya veri taşıma aracına sayısal kod halindeki dar anlamda verilerin girilmesi şeklinde olabileceği gibi, kişisel bilgilerin bir dosya

---

[196] Bkz. *Mevzuat/TCK*, Türk Ceza Kanunu, s. 9000-9001 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf,

kâğıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilecektir. Kişisel verilerin kaydedilmesi suçu serbest hareketli bir suç tipi olarak düzenlenmiştir, bu nedenle verilerin kaydedilmesi işlemi nasıl yapılırsa yapılsın sonuç değişmeyecek ve suç gerçekleşmiş olacaktır. Maddede düzenlenen suç herhangi bir kişi tarafından işlenebileceği gibi, herkes bu suçun mağduru olabilir. Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin hükümlerine geçerlilik tanınmıştır. [197]

Suç kayıt etme fiiliyle gerçekleşmiş olmaktadır. Bu bakımdan işlendiği ortama göre, kayıt etmenin yapıldığı anda suç oluşur. Bilişim ortamında fare (mouse) ile bile kayıt gerçekleştirilebilirken, kâğıda kayıtta yazının bitirilmiş olmasıyla kayıt yapılmış olur. Verileri kaydeden kişiden bu verileri alan kişinin eylemi bu suçu oluşturmaz. Ancak veren kişinin eylemi ayrıca TCK 136. maddesindeki suçu oluşturur (Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır) Suç kasten işlenebilen bir suç olup, maddede fiilin hukuka aykırı olarak işlenmesinden söz edildiği için failin kastının, fiilin hukuka aykırı olduğunu da kapsaması aranmaktadır. Ancak madde gerekçesinde belirtildiği üzere kişinin rızasıyla kendisiyle ilgili bilgilerin kayda alınması veya kanun hükmü gereğince kişisel verilerin kaydedilmesi halinde söz konusu suçu oluşmayacaktır.

Öte yandan maddenin ikinci fıkrasında "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine" ilişkin verilerin kaydedilmesi eylemleri açısından failin yaptığı eylemin hukuka aykırı olduğunu bilmesi hali ayrıca aranmamıştır. Buna göre fail eylemi gerçekleştirirken bunun hukuka aykırı olduğunu bilse de bilmese de hareketin neticelenmesiyle suç gerçekleşmiş olacaktır. Başka bir ifadeyle bu verilerin hiçbir şekilde işlenmesi mümkün değildir. Nitekim madde gerekçesinde kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına

---

[197] Bkz. *Mevzuat/TCK GRKÇ 135-6*, Türk Ceza Kanunu Md. 135-136, s. 220, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc

veya sendikal bağlantılarına ilişkin bilgilerin suçla mücadele gibi bazı hallerde kaydedilmesine izin verilebileceği ifade edilmektedir. [198]

Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme: 5237 sayılı TCK'nın 136. maddesiyle, kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi eylemleri suç haline getirilmektedir (ilgili kanun maddesi önceki bölümde verildi).

Bu suç en yaygın olarak internet ortamında özellikle, kimlik hırsızlığı olarak da adlandırılan ve internet üzerinden kişilerin isim, doğum tarihi, sosyal güvenlik numaraları, kredi kartı bilgileri gibi kişisel verilerinin ele geçirilmesi şeklinde işlenmekte ve bu suretle çeşitli dolandırıcılık eylemleri gerçekleştirilmektedir. Gerçekten de günümüzde artık hemen hemen tüm kişisel bilgiler ve kimlik bilgileri özellikle internette bulunmaktadır. Bu bilgilerin çoğu kişilerin verdikleri rızaya dayanılarak çeşitli sitelere verilmektedir. İşte bu bilgilerin hukuka aykırı olarak üçüncü kişilere verilmesi, yayılması ya da bu verilerin üçüncü kişiler tarafından ele geçirilmesinin suç tipi olarak düzenlenmesi yerinde bir düzenleme olmuştur.

Suçun konusu kişisel veriler olup, 135. maddede olduğu gibi bu suç herkes tarafından işlenebileceği gibi, yine herkes bu suçun mağduru olabilecektir.

Kişisel verilerin başkasına verilmesinde herhangi bir yöntem belirtilmemiştir. Bu nedenle verme hareketi elden olabileceği gibi posta veya elektronik posta gibi çok değişik şekillerde gerçekleştirilebilir. Yayma eylemi de yazılı olarak mektup şeklinde birden fazla kişiye gönderilmesiyle gerçekleştirilebileceği gibi internet üzerinden bir web sitesinde başkaları için erişebilir kılmak da yayma suçunu oluşturacaktır. Bunun yanında kişisel verilerin yayılması eylemlerinin yazılı, görsel veya sanal basın yoluyla da gerçekleştirilmesi mümkündür.

Kişisel verilerin ele geçirilmesi suçu da; yazılı evrakın alınması suretiyle veya verilerin kayıtlı olduğu bilişim sisteminden verilerin bir diskete aktarılması gibi çeşitli şekillerde gerçekleştirilebilir. Evlilik, birlikte çalışma gibi nedenlerle

---

[198] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010, s. 89-92-93

ortak elektronik posta kullananlar, birliktelik sona erdikten sonra da verileri izinsiz olarak açıklayamazlar. Nitekim Yargıtay bir kararında; bir şirkette müdür olarak çalışan sanığın şirketten ayrılmadan önce şirketin müşterilerine ait tüm verileri kendi kurduğu şirketinde kullanmak üzere aktarmasının suç teşkil ettiğini belirtmiştir. [199]

Verilerin Yok Edilmemesi Suçu (m.138): Madde 138-(1) "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir" şeklindedir. İlgili maddenin gerekçesi "kişisel verileri kaydetmek veya ele geçirmenin yanında, hukuka uygun olarak elde edilen verilerin saklama ve işleme süresi dolduğu halde yok edilmemesi de suç olarak tanımlanmaktadır" [200] [201]

Yeni Ceza Kanununda yer verilen bu suç tipiyle de hukuka uygun olarak sistemde bulunan kişisel verilerin sürekli olarak bu sistemlerde bulunması ve böylelikle her an ulaşılabilirliğinin sağlanmasının önüne geçilerek, verileri sistemden çıkarmayanlara yani bu konudaki görevlerini ihmal edenlere yaptırımlar öngörülmektedir.

Bu suç tipiyle kamunun güvenilirliği ile birlikte korunmak istenen diğer hukuki değer ise kişilerin özel hayatı ve hayatın gizli alanı, özel olarak ise kişisel verilerdir.

TCK 138. maddesindeki suçun oluşması için; kanunların kişisel verinin yok edilmesi için süre belirlemiş olması ve kişisel verilerin bu süre içerisinde sistem içinde yok edilmemesi gerekir. Ancak burada geçen "kanunda" ibaresinin geniş

---

[199] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010, s. 89-93-94

[200] Bkz. *Mevzuat/TCK*, Türk Ceza Kanunu, s. 9000-9001 http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf,

[201] Bkz. *Mevzuat/TCK GRKÇ 138*, Türk Ceza Kanunu, Md.138 Gerekçe, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc

şekilde yorumlanması gerekir; bu bağlamda tüzük, yönetmelik, yönerge gibi geçerli, genel ve objektif düzenlemeler de bu kapsamda değerlendirilmelidir.
Bu suçun faili verileri sistem içinde yok etmekle görevli olan kişidir. Bu görev ise konuyla ilgili özel yasalarla düzenlenecektir. Her somut olayda bu yasa belirlenecek ve kimlere nasıl bir veri yok etme görevi verildiği araştırılacaktır.
Suçun hareketi verileri yok etmemektir. Suç ihmali bir hareketle gerçekleşmektedir. İhmali hareketin neticesinde, veri maddedeki koşullarda ilgilisince yok edilmemiş olmalıdır. [202]

Ortak Hükümler: 5237 sayılı TCK'nunda kişisel verilerle ilgili bu suçlara ilişkin ortak hükümler Kanunun 137, 139 ve 140. Maddelerinde düzenlenmiştir. Buna göre kişisel verilerin hukuka aykırı olarak kaydedilmesi, verme veya ele geçirilmesi ile verileri yok etmeme suçlarının soruşturulması ve kovuşturulması şikâyete tabi değildir, re'sen kovuşturulacaktır. Öte yandan, bu suçların kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması suretiyle veya belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi halinde ceza yarı oranında arttırılacaktır.(m 137) Ayrıca bu suçların bir tüzel kişinin faaliyetleri çerçevesinde işlenmesi halinde tüzel kişiler hakkındaki özel güvenlik tedbirlerine hükmedilebilecektir. (m. 140)

d) Ceza Muhakemesi Kanunu

Genel: Ceza muhakemesinde maddi gerçeğe ulaşılması bakımından kriminalistik büyük önem arz etmektedir. Kriminalistik (İz Bilimi), suç olayını maddi gerçeğe uygun olarak araştıran ve ortaya koyan bir bilim dalı olup, uyguladığı bilimsel metotlarla incelediği izlerin bir kısmını da kan, parmak izi, DNA verileri, ses ve koku gibi kişisel veri niteliğindeki bulgular oluşturmaktadır. 04/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunun çeşitli maddelerinde de suç soruşturması esnasında kişisel veri mahiyetindeki bilgilerin kullanılması, bu bilgilerin korunması, saklanması ve yok edilmesine ilişkin çeşitli düzenlemelere

[202] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010, s. 89-92-95

yer verilmiş, 2002/58 sayılı Elektronik İletişim Alanında Kişisel Verilerin Korunması Yönergesine de paralel olarak kişiler arasındaki haberleşmeye müdahalenin AİHS hükümleri ve AİHM içtihatları çerçevesinde gerçekleştirilmesinin şartları belirlenmiştir. [203]

Şüpheli, Sanık veya Mağdurun Beden Muayenesi, Vücuttan Örnek Alınması ve Moleküler Genetik İncelemeler: 5271 sayılı CMK'nun 75 ve 76. Maddeleri uyarınca; "bir suça ilişkin delil elde etmek için" kural olarak "hâkim", "gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı"nın kararı ile "şüpheli veya sanık" veya "mağdur" "üzerinde iç beden muayenesi yapılabilmesine ya da vücuttan kan veya benzeri biyolojik örneklerle saç, tükürük, tırnak gibi örnekler alınabilmesine" karar verilebilecektir.

CMK 78. maddeye göre ise; "75 ve 76 ncı maddelerde öngörülen işlemlerle elde edilen örnekler üzerinde, soy bağının veya elde edilen bulgunun şüpheli veya sanığa ya da mağdura ait olup olmadığının tespiti için zorunlu olması halinde moleküler genetik incelemeler" yapılabilecektir. "Alınan örnekler üzerinde bu amaçlar dışında tespitler yapılmasına yönelik incelemeler yasaktır". CMK 79. Maddeye göre de "78 inci madde uyarınca moleküler genetik incelemeler yapılmasına sadece hâkim karar verebilir". [204]

Genetik İnceleme Sonuçlarının Gizliliği: CMK'nın 80. maddesine göre "75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz ve dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez". Yine aynı maddede "Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir" ifadesi yer almaktadır. [205]

---

[203] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, Ankara, 2010, s. 96-97

[204] Bkz. Mevzuat/*CMK*, Ceza Muhakemesi Kanunu, Md.75, 76, 78, 79, www.ceza-bb. adalet .gov.tr/mevzuat/5271.htm

[205] Bkz. Mevzuat/*CMK*, Ceza Muhakemesi Kanunu, Md.80, www.ceza-bb.adalet. gov.tr /mevzuat/5271.htm

Fizik Kimliğin Tespiti: CMK'nın 81. maddesine göre; "üst sınırı iki yıl veya daha fazla hapis cezasını gerektiren suçlardan dolayı şüpheli veya sanığın, kimliğinin teşhisi için gerekli olması halinde, Cumhuriyet savcısının emriyle fotoğrafı, beden ölçüleri, parmak ve avuç içi izi, bedeninde yer almış olup teşhisini kolaylaştıracak diğer özellikleri ile sesi ve görüntüleri kayda alınarak, soruşturma ve kovuşturma işlemlerine ilişkin dosyaya konur"

Maddenin ikinci fıkrasına göre de, önceki maddelerde olduğu gibi, "kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde söz konusu kayıtlar Cumhuriyet savcısının huzurunda derhal yok edilir". [206]

Ancak bu maddeye göre elde edilen verilerin kolluk tarafından arşivlenmesi hükmünü içeren "Beden Muayenesi Yönetmeliği"nin 17. maddesi, esasa ilişkin yetkilerin yönetmelikle düzenlenemeyeceği, CMK'da ise böyle bir düzenleme yapılmasına değil sadece işlemlerin usulünün yönetmelikle belirlenebileceğinin hüküm altına alındığı, bu nedenle anılan Yönetmelik hükmünün yasal dayanağının bulunmadığı gerekçeleriyle eleştirilmiştir. [207]

İletişimin Tespiti, Dinlenmesi ve Kayda Alınması: Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, araya bir vasıta sokulmak suretiyle gerçekleştirilen her türlü haberleşmenin gizlice dinlenmesi, buradan elde edilen bilgilerin kaydedilmesini ve değerlendirilmesini kapsamına almaktadır.

Hukukumuzda sadece 1999 yılında yürürlüğe giren 4422 sayılı mülga Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanununda öngörülen suçlar bakımından iletişime müdahale öngörülürken, 1412 sayılı Ceza Muhakemesi Kanununda bu konuda herhangi bir düzenleme bulunmamaktaydı. 5271 sayılı CMK ile "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" bölümü başlığı altında 135 vd. maddelerinde iletişime müdahaleye ilişkin ayrıntılı düzenlemelere yer verilmiştir.

---

[206] Bkz. Mevzuat/*CMK*, Ceza Muhakemesi Kanunu, Md 81, www.ceza-bb.adalet.gov.tr /mevzuat/5271.htm

[207] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, sf. 98, Ankara, 2010

Öte yandan, kişiler arası haberleşmenin istihbarat amacı ile dinlenmesi ve kaydedilmesi mukayeseli hukukta daha önceden düzenlenmişken, ülkemizde 03/7/2005 tarihli ve 5397 sayılı Kanunla 2559 sayılı PVSK'ya eklenen Ek 7. madde ve diğer kanunlarda yapılan değişiklikler ile istihbarat amaçlı önleme dinlemesi yetkisi yasal olarak düzenlenmiştir.

Bunun yanında, Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanunun 66. maddesinde hükümlülere hak olarak verilen telefonla görüşmelerinin kayıt altına alınması da bir önleme dinlemesi niteliğindedir.

AİHS'nin özel hayatın gizliliğini düzenleyen 8. maddesi hükümleri yanında, 2002/58 sayılı Elektronik İletişim Alanında Kişisel Verilerin Korunması Yönergesinde iletişimin gizliliğine ilişkin hakların korunmasına ilişkin hükümlerin bulunduğu, ancak Yönergenin 15. maddesinde suçun önlenmesi, soruşturulması ve kovuşturulması gibi bazı hallerde bu hakkın sınırlandırılabileceğine ilişkin düzenlemeye yer verildiği, ancak sınırlama anlamında alınacak bu tür önlemlerin demokratik bir toplumda zorunlu olması ve ölçülülük ilkesine uygun olması gerektiği belirtilmişti.

CMK'da da belirtilen ilkeler dikkate alınarak iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin ayrıntılı hükümlere yer verilmiştir. Bu kapsamda kural olarak CMK Madde 135 de ifade edildiği gibi "bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi tespit edilebilir, dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir". [208]

Ancak aynı ilkeye, 5397 sayılı Kanunla PVSK ve diğer kanunlara eklenen hükümlerle yürürlüğe konulan "önleme dinlemeleri"nde riayet edilmediği, yukarıda da CMK Madde 135 den aktarıldığı gibi iletişimin tespiti için "başlamış bir suç soruşturmasının bulunması", "suç işlendiğine dair kuvvetli şüphe

[208] Bkz. *Mevzuat/CMK 135*, Ceza Mahkemesi Kanunu Md. 135, www.ceza-bb.adalet.gov.tr /mevzuat/5271.htm

sebeplerinin bulunması ve başka bir suretle delil elde etme imkânının bulunmaması" gibi şartlar aranırken 5397 sayılı Kanunda hangi hallerde ve şartlarda bu tedbire başvurulabileceğine dair bir kayıt bulunmadığı ifade edilmektedir.

Öncelikle, iletişime müdahale tedbiri, "bir suç dolayısıyla" ceza soruşturması yapılması koşuluna bağlı tutulduğu için, bu yetkinin delil elde etmek amacıyla halen işlenmiş olan bir suçun kovuşturmasıyla sınırlı olduğu söylenebilir. Öte yandan bu tedbirin uygulanması suretiyle elde edilen bilgiler, hangi amaçla elde edilmiş ise, ancak o amaç çerçevesinde kullanılabilir ve öngörülen amaç dışında başka bir amaçla bu bilgilerden yararlanılması olanaksızdır.(amaca bağlılık ilkesi)

Bunun yanında tedbire, ancak başka bir suretle delil elde edilmesi olanağının bulunmaması durumunda başvurulabilecektir. İletişime müdahale tedbirinin haberleşme özgürlüğüne ağır müdahale oluşturduğu gerçeği, oranlılık ilkesinin somut bir görünümü olarak ikinci derecede uygulanabilirlik koşuluna yer vermek suretiyle göz önünde bulundurulmuştur.

Ayrıca, 135. maddenin altıncı fıkrasına göre; iletişime müdahale tedbirlerinden en ağırını oluşturan dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesi sadece belirli suçlarda uygulanabilecektir. Böylelikle yine tedbirin uygulanmasında oranlılık ilkesi dikkate alınmış bulunulmaktadır. [209]

e) Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Kanun: 04/5/2007 tarihli ve 5651 sayılı Kanunla ülkemize ilk defa internet ortamında hizmet veren aktörler belirlenmiş ve bu aktörlerin yükümlülükleri ile hukuki sorumlulukları düzenlenmiştir. Özelikle internette erişim sağlayıcı ve yer sağlayıcı gibi ara hizmet veren hizmet sağlayıcılarının hukuki sorumluluklarının yasal olarak belirlenmemiş olması eleştirilere neden olmaktaydı.268 Kanunla bu alandaki ihtiyaçlar genel olarak karşılanmış bulunmaktadır.

---

[209] Bkz. *Uygun*, Yayınlanmamış Y. Lisans tezi, Gazi Üniversitesi, s. 100-101, Ankara, 2010

5651 sayılı Kanun, kişisel verilerin korunması bakımından, 2006/24 sayılı Yönergenin 5. maddesinde sayılan; arayan ve aranan telefon numarası, abonenin adı ve adresi, İnternet kullanıcıları için kullanıcı kimliği ve adresi, iletişimin veya bağlantının tarihi, saati ve süresi ve coğrafi konumu gibi bilgilerin hizmet sağlayıcılar tarafından 6 aydan az ve iki yıldan çok olmamak üzere saklanmasının sağlanması çerçevesinde önem taşımaktadır.

5651 sayılı Kanuna göre; erişim sağlayıcılar, "sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla" yükümlü olacaklardır.(m.6) Bu düzenlemeyle 2006/24 sayılı Yönergeye paralel olarak, verilen internet hizmetleri bakımından trafik bilgilerinin saklanmasına ilişkin yasal altyapı sağlanmış, düzenlemenin ayrıntıları yönetmeliklere bırakılmıştır. [210]

6518 Sayılı 06.02.2014 tarihli Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanunun 90 ncı maddesi ile 5651 sayılı kanunun 6. Maddesinden sonra gelmek üzere 6/A maddesi eklenmiştir. Bu madde "kanunun 8 nci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere" "özel hukuk tüzel kişiliğine haiz" "Erişim Sağlayıcıları Birliği"nin kurulmasıdır.

6518 Sayılı ve 06.02.2014 tarihli yasada yer alan bir başka önemli madde de Madde 93 ile yine 5651 saylı kanunun 9. Maddesinin başlığıyla birlikte değiştirilmesidir. İlk haliyle "İçeriğin yayından çıkarılması ve cevap hakkı" şeklinde olan başlık "İçeriğin yayından çıkarılması ve erişimin engellenmesi" şeklinde değiştirilmiş olup 9. Maddenin (1), (2), (3) ve (4) ncü fıkralarında "kişilik haklarının ihlali" konusu ile "içeriğe erişimin engellenmesi"nin yol ve usullerine değinilmiştir.[211]

---

[210] Bkz. *TCBMM/Int. Yay. Suç 2007* 5651 sayılı kanun, Md. 6 (2), http://www.tbmm.gov.tr/kanunlar/k5651.html

[211] Bkz. *TCBMM/Int. Yay. Suç 2014* 5651 saylı kanun değişikliği (6518 sayılı torba yasa) Md. 85-100, http://www.tbmm.gov.tr/kanunlar/k6518.html

Bu son değişikliklerin konumuz ile ilişkisine ve olası etkilerine sonuç ve öneriler bölümünde değinilecektir.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik: 5651 sayılı Kanuna dayanılarak çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelikte "erişim sağlayıcı trafik bilgisi; internet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgiler" şeklinde tanımlanmıştır. Yönetmelikte bunun yanında, "vekil sunucu trafik bilgisi" ile "yer sağlayıcı trafik bilgisi" tanımları da yapılmaktadır. Yönetmeliğin 8. maddesiyle trafik bilgilerinin saklanmasına ilişkin daha ayrıntılı bir düzenleme yapılmıştır. Buna göre; erişim sağlayıcı, sağladığı hizmetlere ilişkin olarak, "erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmekle ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle" sorumlu tutulmuştur. Görüldüğü gibi, 2006/24 sayılı Yönerge uyarınca trafik bilgilerinin saklanması için altı aydan az iki yıldan fazla olmamak üzere belirlenmesi gereken süre, Yönetmelikte bir yıl olarak tespit edilmiştir. [212]

Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik: AB Müktesebatına uyum sağlama çalışmaları çerçevesinde Telekomünikasyon Kurumu tarafından hazırlanan "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik", "406 sayılı Telgraf ve Telefon Kanunu ile 2813

---

[212] Bkz. *RG/Intern. Ortam. Yayın.,* Yönetmelik, Md.3, Md. 8, http://www.resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm

sayılı Telsiz Kanununa dayanılarak" hazırlanmıştır". Bu kapsamda Yönetmelikte 2002/58 sayılı Yönergeye paralel düzenlemelere yer verilmektedir.
Yönetmelikle, "telekomünikasyon sektöründe kişisel bilgilerin işlenmesi ve gizliliğinin korunmasının güvence altına alınmasına ilişkin usul ve esasların belirlenmesi" hedeflenmekte olup, "telekomünikasyon sektöründe hizmet veren ve alan gerçek ve tüzel kişileri" kapsamaktadır.

Yönetmelikle mevzuatımızda ilk defa kişisel veri ve kişisel verilerin işlenmesi tanımlarının yapıldığı görülmektedir. Buna göre "kişisel veriler; tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi" olarak tanımlanmaktadır.

Bunun yanında kişisel verilerin işlenmesi ise; "otomatik olsun olmasın, toplama, kaydetme, hazırlama, yükleme, uyarlama, değiştirme, geri çağırma, danışma, kullanma, aktarma yoluyla açığa vurma, yayma ya da bunların dışında erişilebilir hale getirme, düzenleme, birleştirme, engelleme, silme gibi yollardan, kişisel bilgiler üzerinden yürütülmekte olan herhangi bir işlem ya da işlemler bütününü" ifade etmektedir.

Yönetmelik, içerik yönünden telekomünikasyon sektöründe faaliyet gösteren işletmecilere; iletişim güvenliği ile riskleri konusunda kullanıcının haberdar edilmesi, trafik verilerinin işlenmesinde amaca bağlılık ve ücretlendirme sınırları içinde işlemde bulunma, arayan ve aranan hattın kimliğinin gösterilmesi ile kullanıcı fihristlerinin oluşturulmasında kullanıcı yararına önlem almak gibi önemli külfetler yüklemektedir. Öncelikle "işletmeci, şebeke güvenliğinin ihlaline karşı tüm gerekli teknik ve yapısal önlemleri*"* almalıdır.

Her ne kadar Yönetmeliğin 8. maddesiyle, "yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, iletişime üçüncü şahıslar tarafından dinleme, kaydetme, kayıt vb. şekillerde müdahale edilmesi yasak"lanmakta ise de, böyle bir düzenlemenin ve ihlali halinde yaptırımlarının kanunla düzenlenmesi gerekirdi. Nitekim 5237 sayılı

TCK'nın "Haberleşmenin gizliliğini ihlal" başlıklı 132. maddesiyle bu alandaki ihtiyaç karşılanmış bulunmaktadır. [213]

Yönetmeliğin 9. maddesine göre; "telekomünikasyon hizmetlerini pazarlamak ya da katma değerli hizmetleri sağlamak amacıyla kişisel bilgilerin işlenebilmesi için abone veya kullanıcıların izin" vermesi gerekmektedir. Abone ve kullanıcılar onay verirse "kişisel veriler, ancak bu tür hizmetler ve pazarlama için gerekli kapsam ve sürede" işlenebilecektir.(Amaca bağlılık ilkesi) "Kullanıcı ve aboneler, kişisel bilgilerinin işlenmesi için verdikleri izinleri her zaman geri alabilirler".

Öte yandan Yönetmelikte yer alan bir diğer önemli düzenleme istenmeyen istek dışı haberleşmelere ilişkindir. 20. maddeyle, siyasi propaganda amaçlı iletiler ile doğrudan pazarlama amaçlı iletiler arasında abonelerin izninin alınması bakımından bir ayrım yapılmaktadır. Buna göre; "işletmeciler kişi müdahalesi olmadan çalışan fakslar, elektronik posta, kısa mesaj gibi otomatik arama sistemlerini, abonenin önceden izni olmadan siyasi propaganda amacıyla" kullanamayacaklardır. "Söz konusu otomatik arama sistemlerinin doğrudan pazarlama amacıyla kullanılması halinde ise kullanıcılara gelen her bir mesajı bundan sonrası için almayı reddetme hakkı ücretsiz ve kolay bir yolla" sağlanacaktır. Başka bir ifadeyle siyasi propaganda amacıyla haberleşme yapılırken "opt-in" rejimi benimsenirken, doğrudan pazarlama amacıyla istenmeyen elektronik haberleşmelerde "*opt-out*" rejimi uygulanması öngörülmüştür..

Oysaki 2002/58 sayılı Direktifin 13. maddesi uyarınca; "kullanıcılara, ancak önceden rızaları elde edilmesi kaydıyla, otomatik arama sistemleri, fakslar, kısa mesajlar veya elektronik postalar ile doğrudan pazarlama amaçlı ileti

[213] Bkz. *Mevzuat/Kişisel Bilgi*, Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Md. 1,2,3,6,7, ve 8, http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/Kisisel_Bil_Yon_06_02_04.pdf

gönderilmesinin mümkündür". Bu çerçevede Yönetmeliğin söz konusu hükmünün 2002/58 sayılı Direktif ile uyumlu olduğunu söylemek mümkün değildir. [214] [215]

f) Diğer Kanunlar

Ülkemizde çeşitli kanunlarda kişisel verilerin hukuka uygun olarak elde edilmesi, saklanması ve korunması ile ilgili hükümlere yer verilmektedir. Bu çalışmada örnek olarak İş Kanunu, Polis Vazife ve Selahiyet Kanunu, Bilgi Edinme Hakkı Kanunu, Türkiye İstatistik Kanunu ile Nüfus Hizmetleri Kanunundan bahsedilecektir.

aa) İş Kanunu

Kişisel verilerin korunması iş ilişkilerinde de önemlidir. Bu konu 10.06.2003 tarihinde yürürlüğe giren 4857 sayılı İş Kanununun 75. maddesinde düzenlenmiştir. Buna göre işveren, her işçi için kimlik bilgileri dâhil işçi ile ilgili bir takım kişisel bilgi ve belgelerin bulunduğu özlük dosyası tutmak zorundadır. Özlük dosyasından başka iş ilişkisi için gerekli olan bilgilerin işverence toplanmasında bir sakınca yoktur. Böyle bir gereklilik olmadığı halde, işçi ile ilgili kişisel bilgilerin toplanması, işçinin sanal yollarda izlenmesi ya da e-postalarının kontrol edilmesi hukuka aykırı olur. "İşveren işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin çıkarı bulunan bilgileri açıklamamakla yükümlüdür". [216]

---

[214] Bkz. *EU, e-Privacy Dir*., Official Journal of European Community, http://eurlex.europa.eu /LexUriServ/LexUriServ.do?uri=CONSLEG: 2002L0058:20091219:EN:PDF, e-Privacy Directive 2002/58/EC s. 17, 2009

[215] Bkz. *Mevzuat/Kişisel Bilgi*, Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Md. 9, 20, http://www.tk.gov.tr/mevzuat/yonetmelikler/ dosyalar/ Kisisel_Bil_Yon_06_02_04.pdf

[216] Bkz. *Mevzuat/İş K*., 8423 Sayılı İş Kanunu http://www.mevzuat.gov.tr/ Mevzuat Metin/ 1.5.4857.pdf 8423 Md. 75, s. 8448

bb)Bilgi Edinme Hakkı Kanunu

4982 sayılı Bilgi Edinme Hakkı Kanunu ile ilk defa Madde 1'de Amaç başlığı altında ifade edildiği gibi "demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına" imkân sağlanmış bulunmaktadır.

Madde 2'de Kanunun Kapsamı "Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinde uygulanır" olarak tanımlanmıştır. Bu kanunun Madde 4'ünde Bilgi Edinme Hakkı "Herkesin bilgi edinme hakkına sahiptir" şeklinde hükme bağlanmış olup, Bilgi verme Yükümlülüğü Madde 5'de "Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idari ve teknik tedbirleri almakla yükümlüdürler" olarak tanımlanmıştır.

Bilgi veya belgeye erişim süreleri Madde'11 de "Kurum ve kuruluşlar, başvuru üzerine istenen bilgi veya belgeye erişimi onbeş iş günü içinde sağlarlar" şeklinde belirlenmiştir; İtiraz usulü de Madde'13 de "Bilgi edinme istemi reddedilen başvuru sahibi, yargı yoluna başvurmadan önce kararın tebliğinden itibaren onbeş gün içinde Kurula itiraz edebilir" şeklinde tanımlanmıştır.
Kanunun uygulanması bakımından bazı istisnalar kanunun Madde 15, 16, 17, 18, 19 ve 20'de öngörülmüştür; bu kapsamda devletin emniyetine, dış ilişkilerine, milli savunmasına ve milli güvenliğine, ülkenin ekonomik çıkarlarına, istihbarata, idari ve adli soruşturmaya zarar verebilecek nitelikteki bilgilerin kanun kapsamı dışında tutulmuştur.

Bunun yanında, Özel hayatın gizliliği başlığı altında madde 21'de de "Kişinin izin verdiği haller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması halinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, mesleki ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır" ifadesi yer almaktadır. Ancak "Kamu yararının gerektirdiği hallerde, kişisel bilgi veya belgeler, kurum ve

kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir". [217]

cc) Polis Vazife ve Selahiyet Kanunu

2559 sayılı PVSK'da 2007 yılında 5681 sayılı Kanunla yapılan değişikliklerle çeşitli durumlarda parmak izi ve fotoğrafların kayda alınması ve kişisel veri niteliğindeki bu bilgilerin işlenmesiyle ilgili hükümlere yer verilmiştir. Buna göre kanunda Madde 5 "Polis; gönüllü, her çeşit silah ruhsatı, sürücü belgesi, pasaport veya pasaport yerine geçen belge almak için başvuruda bulunan, başta polis olmak üzere, genel veya özel kolluk görevlisi ya da özel güvenlik görevlisi olarak istihdam edilen, Türk vatandaşlığına başvuruda bulunan, sığınma talebinde bulunan veya gerekli görülmesi halinde, ülkeye giriş yapan sair yabancılar ile gözaltına alınan kişilerin parmak izini alır" şeklinde yetkili kılınmıştır.

Madde 5 "Olay yerinden elde edilen ve kime ait olduğu henüz tespit edilemeyen parmak izleri, kime ait olduğu tespit edilinceye kadar, ilgili soruşturma dosya numarası ile birlikte sisteme kaydedilir. 5271 sayılı CMK'nın 81. maddesi ile 5275 sayılı CGTİHK'nın (Ceza ve Güvenlik Tedbirlerinin İnfazı Hakkında Kanun) 21. Maddesi hükümlerine göre alınan parmak izleri de bu sisteme kaydedilir" şeklinde devam eder..

Maddede bu hükümle beraber, yukarıda sayılan kişilerden elde edilen verilerin hukuka uygun bir şekilde işlenmesi ve korunmasına dair bir takım güvencelere yer verilmektedir. Bu kapsamda, "alınan parmak izlerinin, ait olduğu kişinin kimlik bilgileri ile birlikte, ne zaman ve kim tarafından alındığı belirtilmek suretiyle, bu amaca özgü sisteme kaydedilerek" saklanacak; "Ancak parmak izinin hangi sebeple alındığı sisteme" kaydedilmeyecektir.

Ayrıca "Bu sistemde yer alan bilgiler, sadece kimlik tespiti, suçun önlenmesi veya yürütülmekte olan soruşturma ve kovuşturma kapsamında maddî gerçeğin ortaya çıkarılması amacıyla mahkeme, hâkim, Cumhuriyet savcısı ve

---

[217] Bkz. *Mevzuat/Bilgi Edinme*, 4982 Sayılı. Bilgi Edinme Hakkı Kanunu, http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf , s. 8617-8621

kolluk tarafından" kullanılabilecektir. Yine bir güvenlik önlemi olarak, "sistemde kayıtlı bilgilerin hangi kamu görevlisi tarafından ve ne amaçla kullanıldığının denetlenebilmesine imkân tanıyan bir güvenlik sistemi" kurulması öngörülmektedir. Son olarak "Sistemde yer alan kayıtlar gizlidir; altıncı ve yedinci fıkralarda belirtilen amaçlar dışında" kullanılamayacağı hüküm altına alınmaktadır. "Sisteme kayıtlı olan parmak izi ve fotoğraflar, kişinin ölümünden itibaren on yıl ve her halde kayıt tarihinden itibaren seksen yıl geçtikten sonra sistemden silinir".[218]

dd)Türkiye İstatistik Kanunu

5429 sayılı Türkiye İstatistik Kanunu Tanımlar başlıklı Madde 2'de, veri, bireysel veri, gizli veri kavramlarına yer verilmiş; "bireysel veri, hakkında bilgi toplanan istatistikî birimlerin, özellikleri ile birlikte tanımlandığı veri" şeklinde tanımlanmıştır. Bunun yanında "gizli veri, istatistik birimin doğrudan veya dolaylı bir şekilde özellikleri ile birlikte tanınabilmesine ve bu şekilde bireysel bilgilerin açığa çıkarılmasına imkân sağlayan bireysel veya tablo hâlinde saklı tutulan veriyi ifade" etmektedir.

5429 sayılı Kanunun 13.maddesine göre; "Gizli verilere yalnızca resmî istatistik üretiminde görev alanlar, görevlerini yerine getirebilmek için ihtiyaç duydukları ölçüde erişebilirler". Maddede kişisel veri niteliği kabul edilen bilgilerin korunması için bir takım tedbirlere yer verilmektedir. Buna göre:

- Gizli veriler; "idarî, adlî ve askerî hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz. Bu bilgileri derleyen ve değerlendiren memurlar ve diğer görevliler de bu yasağa uymak zorundadır."
- "Resmî istatistik üreten kurum ve kuruluşların yetkilileri tarafından, gizli verilerin hukuka aykırı erişimine, açıklanmasına veya kullanımına karşı her türlü önlem alınır."

---

[218] Bkz. *Mevzuat/PÜLİS VZF. K*., 2559 Sayılı Polis Vazife ve Salahiyetleri Kanunu, www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.doc , s., 1412-1409

- “Gizli veriler, ancak doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde diğer bilgilerle birleştirilerek yayımlanabilir."

g. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı

Dağıtımı 15.5.2012 tarihinde yapılan ve TCBMM Genel Kururlunda görüşülmek için bekleyen 240 Sıra Sayılı tasarının, mecliste görüşmelerinin tamamlanarak 1 Ocak 2013’den itibaren yürürlüğe girmesi planlandığı ifade edilmiş olmakla birlikte, TCBMM’in 71 inci Birleşimi 1 Mart 2014 tarihli gündeminde hala 92. sırada ve görüşülmemiş olduğu görülmektedir. Tasarının yine TCBMM’sinin 30/10/2012 tarihli 13. Birleşiminde İçtüzüğün 91 inci maddesine göre temel kanun olarak görüsülmesi; birinci bölümünün 1 ila 9. Maddelerden, ikinci bölümünün Geçici Madde 1 dâhil olmak üzere 10 ila 16 ncı maddelerden oluşması şeklindeki Grup önerisi kabul edilmişti. Bu taslakta e-ticaret nedeniyle elde edilen kişisel verilerin ve bireysel gizliliğin korunması yönünde Madde 10 “(1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı; a)Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur. b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz” şeklinde düzenlenmiştir. Tasarının 14. Maddesi ile de “5809 sayılı Elektronik Haberleşme Kanununun50 nci maddesinin beşinci fıkrası”nın da aşağıdaki şekildeki gibi değiştirilmesi öngörülerek “aşağıdaki fıkralar eklenmiş ve diğer fıkralar buna göre teselsül ettirilmiştir”. “(5) İşletmeciler tarafından, sundukları hizmetlere ilişkin olarak abone ve kullanıcılarla, önceden izinleri alınmaksızın otomatik arama makineleri, fakslar, elektronik posta, kısa mesaj gibi elektronik haberleşme vasıtalarının kullanılması suretiyle pazarlama veya cinsel içerik iletimi gibi maksatlarla haberleşme yapılamaz. İşletmeciler sundukları hizmetlere ilişkin olarak abone ve kullanıcılarıyla siyasi propaganda içerikli haberleşme yapamazlar. (6) İşletmeciler tarafından, abone ve kullanıcıların iletişim bilgilerinin bir mal veya hizmetin sağlanması sırasında bu tür haberleşmenin yapılacağına dair bilgilendirilerek ve reddetme imkânı sağlanarak edinilmiş olması halinde, abone ve kullanıcılarla

önceden izin alınmaksızın aynı ve benzer mal ya da hizmetlerle ilgili pazarlama, tanıtım, değişiklik ve bakım hizmetleri için haberleşme yapılabilir. (7) Abone ve kullanıcılara, bu tür haberleşme yapılmasını reddetme ve verdikleri izni geri alma hakkı kolay ve ücretsiz bir şekilde sağlanır."

Kanun halen Meclis gündeminde görüşülüp yürürlüğe girmemiş olmak beraber yukarıda aktarılan madde içeriklerinin de etkililiği ve yeterliliği diğer yönleri ile sonuç ve öneriler bölümünde ele alınmıştır.[219] [220]

h. Kişisel Verilerin Korunması Hakkında Kanun Tasarısı

Tez konumuzla ilgili olarak AB uyum süreci içerisinde gündeme gelmiş, ilk şekli Bakanlar Kurulunda 7 Nisan 2008 tarihinde kararlaştırılan ve 22 Haziran 2008 tarihinde TCBMM Başkanlığına iletilen ve daha sonra 2012 ve 2013 yıllarında tekrar yenilenen son şekli de halen TCBMM'de görüşülememiş yasal düzenleme çalışmalarından birisi de AB'nin 95/46/EC Direktifini esas alarak hazırlanmış olan Kişisel Verilerin Korunması Kanun tasarısı çalışmasıdır. Tasarının ayrıntılarına, TCBMM gündemine henüz alınmamış olduğundan burada yer verilmemiştir. Bu tasarı ile Çevrimiçi Davranışsal Pazarlama ve Kişisel Mahremiyet ilişkisine ise Sonuç ve Öneriler bölümünde yer verilmiştir.

C. Çevrimiçi davranışsal reklamcılıkta özdenetim (self-regulation)

Çevrim içi reklamcılık endüstrisi ABD'de NAI (*the Network Advertising Initiative* - Ağ Reklamcılık Girişimi; *DAA* ve *Interactive Advertising Bureau US*) ve AB'de (*IAB Europe*) özdenetim girişimleri ile büyük ölçüde uyumlu hale getirilmiştir. Bu programlar davranışsal reklamcılık kuruluşlarına aşağıda sıralanan temel isteklerin uygulanması için baskı yapmaktadır:

---

[219] Bkz. *TCBMM/e-Tic.K. Tas*., Türkiye Cumhuriyeti Büyük Millet Meclisi, Komisyon Raporu, http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss240.pdf , 2 Mayıs 2012

[220] Bkz. *TCBMM/Gündem,* Türkiye Cumhuriyeti Büyük Millet Meclisi, Gündem, http://www.tbmm.gov.tr/gundem/gundem.htm

i. Davranışsal reklamcılık uygulamaları ile ilgili olarak kullanıcılara bilgi vermelidirler
ii. Kullanıcılara verilerini davranışsal reklamcılık amaçlı kullanımı reddetme (*opt-out*) imkânı vermelidirler. Bu seçimin sadece verilerin sadece bu amaç için kullanımına ilişkin olduğu not edilmelidir: bundan verilerin toplanması ve üçüncü taraf izlemenin başka amaçlı kullanımları etkilenmemektedir.

Öz-denetim uygulamalarına katılım, konuya regülasyonlarla verilen öneme bağlı olarak kurumlar / ülkeler arasında farklılıklar göstermektedir. Güncel durumda en büyük çevrim içi reklamcılık ve analiz kuruluşları öz-denetime etkin olarak katılmakta iken, küçük kuruluşların çoğunluğu katılmamaktadır. Sosyal ağlar ve içerik sağlayıcılar ise bu konuda neredeyde hiç ortada gözükmemektedirler.

Örneğin, Dijital Reklamcılık Birliği (DAA) 2011 in sonlarında programı tüm üçüncü tarafları kapsayacak şekilde genişleteceğini (bu kapsamda tüketici seçimi gerekliliğini her bir cihazla - her bir kullanıcı değil - ilgili verilerin üçüncü taraflarca kişiselleştirmeye yönelik tüm kullanımları kapsayacak şekilde) duyurduğunda sosyal ağlardan ve içerik sağlayıcılardan henüz bunun kabullenildiğine ilişkin bir işaret gelmemişti,

40 ülkede faaliyet gösteren IAB (Interactive Advertising Bureau), tüm dünyada interaktif reklamcılığın gelişmesi, reklam yatırımlarından daha fazla pay alması için çalışmaktadır. Bu amaç doğrultusunda reklam verenlere, ajanslara ve medya ajanslarına interaktif iletişimin katma değerini anlatmakta, kamu nezdinde yürüttüğü çeşitli faaliyetlerle endüstrinin doğru ve nitelikli biçimde büyümesine katkı sağlamaktadır. Merkezi Amerika'da bulunan IAB'nin, Avrupa'daki ülke bazlı örgütlenmesi IAB Europe tarafından koordine edilmektedir

Araştırmacılar ve sivil toplum kuruluşları, öz-denetimle ilgili olarak, veri toplamaya bir seçim imkânı getirmemesi ve öz-denetime uymayan kuruluşlara anlamlı cezalar öngörmemesi nedeniyle eleştirel yaklaşmaktadırlar.

Konuyu biraz daha ayrıntıları ile incelemek ve irdelemek için IAB Avrupa Çevrimiçi Reklamcılık AB çerçevesi temel ilkelerine aşağıda geniş bir biçimde yer verilmiş olup arkasından da IAB Türkiye yapısı ve faaliyetlerinden bahsedilmiştir.

Ancak bütün bu ayrıntılarda bireysel mahremiyetin korunması ve ihlali öncelikle ele alınmıştır.

İnteraktif Reklamcılık Bürosu, Avrupa (IAB Europe): IAB Europe, Çevrimiçi Reklamcılık AB çerçevesini geliştirmiştir. Bu çerçeve ilgili sektörde faaliyet gösteren çok sayıda şirket tarafından 9 Ağustos 2012 de imzalanmıştır. "Çerçeve, AB/AEA bölgesindeki internet kullanıcıları için şeffaflığı ve tercih hakkını arttırmak amacıyla, söz konusu şirketleri ve İAB ülke dernekleri bağlayıcı olacak iyi endüstri uygulamalarını düzenlemek için bir yapı oluşturmakta ve belirli ilkeleri ortaya koymaktadır".

Bu Çerçeveyi 158 kuruluş, 24 ülke derneği imzalamıştır. Çerçeveyi imzalayan IAB ülke "dernekleri bu çerçeve üzerinde beraber çalışmakta ve reklamcılık ekosisteminin her alanında uygulanmasını desteklemektedir. Bu çerçevede yer alan ilkeler ile internet kullanıcıların tercihlerini veya ilgi alanlarını baz alan reklamcılığın yapılmasını kolaylaştırmak amacıyla, Çevrimiçi Davranışsal Reklamcılık ve çevrimiçi verilerin toplanmasına dair tüketici dostu standartların uygulanması amaçlanmaktadır. Çevrimiçi reklamların içeriğinin düzenlenmesi veya *Ad Delivery (Ad Delivery,* çevrimiçi relamların veya reklamlarla ilişkili hizmetlerin *Ad Reporting* kullanılarak iletilmesidir - *IAB Europe Online Advertising Framework* s. ii*)* konseptinin düzenlenmesi amaçlanmamaktadır". IAB Avrupa Çerçevesi İlkeleri aşağıda sıralanmıştır:

I. İlke "Bildirim" konusundadır**.** "Üçüncü Kişi Gizlilik Bildirimi" konusu "Üçüncü kişiler"in "*web* sitelerine, Çevrimiçi Davranışsal Reklamcılık kapsamındaki veri toplama ve kullanma uygulamalarını açıklayan net ve anlaşılabilir bir bildiri" koymalarını öngörmektedir. "Bu bildirimde aşağıdaki unsurların net bir şekilde yer" almaları vurgulanmıştır:

- "Kimlik ve iletişim bilgileri;
- Çevrimiçi Davranışsal Reklamcılık amacıyla toplanan ve kullanılan verilerin türleri ve söz konusu verilerin Direktif 95/46/EC'nin ulusal uygulamasıyla tanımlandığı şekilde kişisel veri veya hassas kişisel veri olup olmadığına dair bilgi;

- Çevrimiçi Davranışsal Reklamcılık verilerinin işlenme amacı veya amaçları ve Ortak Kontrol kapsamında olmayan alıcılar veya alıcı sınıfları ve bu verilerin kimlere açıklanabileceği;
- Çevrimiçi Davranışsal Reklamcılık çerçevesinde verilen toplanması ve kullanılmasına ve ayrıca bu verilerin OBA amacıyla üçüncü kişilere aktarılmasına dair tercih hakkının kullanılması için kullanımı kolay bir sistem"
- Şirketin bu çerçevede yer alan ilkelere uyduğu gerçeği;
- OBA Kullanıcı Tercihi Site'ye link.

Tüketicilere Yönelik Gelişmiş Üçüncü Kişi Bildirimi"konusu ise "Üçüncü kişiler" yukarıdaki Üçüncü Kişi Gizlilik Bildirimi "bölümünde açıklanan bildirimi sağlamasının yanı sıra, reklamın içinde veya etrafındaki bir simge aracılığıyla, Çevrimiçi Davranışsal Reklamcılık amacıyla verilerin toplandığına dair gelişmiş bir bildirim sağlamalıdır"şeklindedir. Madde "Üçüncü kişiler, eğer *Web* Sitesi Operatörü ile bu bildirimin verilmesine dair bir anlaşmaları varsa, Çevrimiçi Davranışsal Reklamcılık amacıyla verilerin toplandığı web sayfasına koyacakları simge yoluyla bu bildirimi sağlayabilir" olarak devam etmektedir.

Web Sitesi Operatörü Bildirimi konusunda da "*Web* Sitesi Operatörü"ünün "ilgili mevcut yasal yükümlülüklere uymasının yanı sıra, üçüncü kişiler tarafından Çevrimiçi Davranışsal Reklamcılık amacıyla bir web sitesinden verilerin toplanmasına ve o web sitesinde kullanılmasına izin veriyorsa, bu durumda Web Sitesi Operatörü bunu uygun ve yeterli bir şekilde açıklama"sı beklenmektedir.

II. İlke "Çevrimiçi Davranışsal Reklamcılık Konusunda Kullanıcı Tercihi" ile ilgilidir. "Üçüncü kişiler, internet kullanıcılarının Çevrimiçi Davranışsal Reklamcılık amacıyla verilerin toplanması ve kullanılması ve bu verilerin üçüncü kişilere aktarılmasına dair kendi tercihlerini kullanılabilecekleri bir sistem sağlamalıdır." "Şirketler, birçok web alanı üzerinden belirli bir bilgisayar veya cihaz tarafından geçilen URL'lerin tamamı veya büyük ölçüde hepsinden verileri toplamak ve bu verileri Çevrimiçi Davranışsal Reklamcılık amacıyla kullanmak için belirli teknolojiler veya uygulamalar yoluyla verileri topladıkları ve kullandıkları zaman, öncelikle Açık Onay almalıdır". "Açık Onay alan şirketler,

internet kullanıcılarına Çevrimiçi Davranışsal Reklamcılık amacıyla söz konusu verilerin toplanması ve kullanılmasına dair açık onaylarını geri almaları için kullanımı kolay bir sistem sağlamalıdır"

"III. İlke Veri Güvenliği" alanındadır. "Önlemler" başlığı altında "Şirketler, Çevrimiçi Davranışsal Reklamcılık amacıyla toplanan ve kullanılan verileri korumak için uygun fiziksel, elektronik ve idari önlemleri uygulamalı ve sürdürmelidir" ifadesi yer almaktadır. "Veri Saklama" konusunda da çerçeve ile getirilen kısıtlama "Şirketler, sadece tamamen meşru iş ihtiyaçları veya kanun gereğince gerekli olduğu sürece Çevrimiçi Davranışsal Reklamcılık amacıyla toplanan ve kullanılan verileri muhafaza etmelidir" şeklinde tanımlanmıştır..

IV. İlke "Hassas Segmentasyon" konusundaki kısıtlılıkları tanımlamaktadır. İlk bölümde "Çocukların Segmentasyonu" yer alır. Burada çerçeveyi imzalayan kuruluşlar "Çevrimiçi Davranışsal Reklamcılık amacıyla özellikle hedef kitlesi çocuklar olmak üzere tasarlanan bölütler oluşturmamayı kabul eder"ler. "Bu hüküm çerçevesinde, "çocuk" terimi 12 yaşında veya daha küçük kişileri ifade" etmektedir".

İkinci bölüm başlığı ise "Diğer Hassas Bölümler" olup bu maddede, Direktif 95/46/EC Madde 8.1 kapsamında tanımlandığı şekilde hassas kişisel verilerin kullanımına dayanan Çevrimiçi Davranışsal Reklamcılık segment'leri oluşturmak veya kullanmak isteyen şirketler"in, bu bilgileri kullanarak Çevrimiçi Davranışsal Reklamcılık yapmadan önce, ilgili yasa uyarınca internet kullanıcısının açık onayını alacaktır.

V. İlke Çevrimiçi Davranışsal Reklamcılık yapan kuruluşların internetten kullanıcılarını bilgilendirmeleri "eğitim" ile ilgili olup "Çevrimiçi Davranışsal Reklamcılık çerçevesinde verilerin nasıl elde edildiği, nasıl kullanıldığı ve internet kullanıcısı tercihinin nasıl yapıldığına dair kolayca bulunabilir bilgiler dâhil olmak üzere, kişileri ve şirketleri Çevrimiçi Davranışsal Reklamcılık konusunda bilgilendirmek için bilgi" sağlama sorumluluğu ile ilişkilidir. "Bu bilginin "anlaşılması kolay bir dil ve kullanıcı dostu bir formatta (çevrimiçi video gibi)" olmasının yanı sıra "şirketlerin kuruluşların, söz konusu eğitim amaçlı bilgi için tutarlı veya yaygın bir kaynak kullanması önerilmektedir".

VI. İlke "Uyum ve Uygulama Programları" ile ilgilidir. "Bu Çerçeve özdenetimci niteliktedir ve Çerçevede yer alan ilkelere ve yükümlülüklere uygunluğunu kendisi belgelendiren imza sahibi şirketler için yükümlülükler oluşturmaktadır. Çerçevenin imzalanmasını ve simgesinin benimsenmesini takiben, her şirketin 30 Haziran 2012 tarihine kadar uyumluluk sağlaması ve bunu kendisinin belgelendirmesi" istenmişti "Çerçeveyi 1 Ocak 2012 tarihinden sonra kabul eden şirketlerin ise, Çerçevenin imzalanması ve simgenin kabul edilmesinden itibaren 6 ay içinde uyumluluk sağlamaları ve bunu kendilerinin belgelendirmesi" koşulu vardı.

Çerçevede "Uyumluluğun şirketin kendisi tarafından belgelendirmesi, her şirketin iş modeli için geçerli olan koşullarla sınırlı olması", "Bir şirketin birden çok yükümlülüğe tabi olması durumunda da, belgelendirme işleminin tüm bu yükümlülük gereklerini kapsaması", "Şirketin bu Çerçeveye uygunluğunu kendisinin belgelendirmesinin, kuruluşun tabi olduğu ulusal yasalar kapsamındaki yükümlülüklerini yerine getirmekten muaf tutmayacağı" gibi hususlar da da açıklanmıştır. "Belgelendirmenin Denetimi" konusunda da Çerçevede aşağıdaki açıklamalar yer almaktadır:

"II. İlkeye tabi olan şirketler, kendi kendilerini belgelendirme süreçlerinin bağımsız denetimini yaptırmakla yükümlüdürler. Bu denetimler, AB ve AEA Üye Ülkeleri'nde Çevrimiçi Davranışsal Reklamcılık yapan şirketlerin uyumluluğunu gözden geçirecek yeterlik ve kapsamda olmalıdır. Söz konusu denetimlerde aranan asgari özellikler aşağıdadır "

- "Çerçeve kapsamındaki yükümlülüklere uyumluluğu doğrulamak amacıyla şirket web sitelerinin tek tek ve bağımsız bir şekilde gözden geçirilmesine olanak verecek süreçlerin varlığı";
- "I. ve II. İlkelerine uyumluluğun objektif bir şekilde doğrulanabildiği, istatistiksel olarak anlamlı sayıda web sitesinin otomatik veya bireyselleştirilmiş olarak periyodik bir biçimde takip edilmesine yönelik süreçlerin varlığı";

- "Doğrudan imza sahibi şirketle birlikte, uyumsuzluğun olduğu tespit edilen alanların şeffaf bir şekilde ve makul bir zaman diliminde çözümlenmesine yönelik süreçlerin varlığı";
- "Bu çerçeve kapsamında verilmiş taahhütlerle ilgili olarak düzeltilmemiş uyumsuzluklarla aynı zamanda kendi kendi kendisini bu çerçeve kapsamında belgelendirmiş bir veya birden çok şirketin genel iyi uyumluluk örneklerine dair kararların yayınlanıyor olması.

"IAB Avrupa çerçevesinde yer alan Tüketici Şikayetlerinin Ele Alınmasına yönelik programların aşağıdaki unsurları içermesi" beklenmektedir:

- "Şikâyetlerin doğrudan şirketlere yöneltilmesi için kolayca erişilebilir sistemlerin mevcudiyeti";
- "Şikâyetlerin, öz denetleyici reklamcılık organları gibi bağımsız ve alternatif uyuşmazlık çözümü mekanizmaları aracılığıyla ele alınması için şeffaf, kolayca anlaşılabilir ve erişebilir sistemlerin varlığı";
- "Çevrimiçi Davranışsal Reklamcılık yapan şirketlerin, Çerçevenin yükümlülüklerine uyumluluk ile ilgili olarak makul olmayan bir şekilde birden fazla uygulama mekanizmasına tabi olmamasını garanti altına almak için, Şirketler ve öz denetleyici reklamcılık organları dâhil olmak üzere alternatif uyuşmazlık çözümü mekanizmaları arasında koordinasyon olması";
- "Tüketicilerin şikâyetlerini; öz denetleyici reklamcılık organlarının kendi yerel dillerinde basit bir şikâyet yönetim mekanizmasına erişimlerini de mümkün kılacak şekilde; bir şikâyet yönetimi organına iletebilmeleri";
- "Bu çerçeve kapsamındaki taahhütlere uyumsuzluk durumunda kararların, şikâyetin ilk olarak yapıldığı ülkenin dilinde de olacak şekilde yayınlanması".

"Bunlara ek olarak, bu ilkeye tabi olan şirketlerin, OBA Kullanıcı Tercihi Sitesinin oluşturulması için işbirliği yapmaları öngörülmüştür."

"Uyumluluk Programları Arasındaki İlişki**"** de Çerçevede **"**Tüketici şikâyetlerinin işlenmesi ve ele alınması bağlamında mevcut olan öz denetleyici reklamcılık

sistemleri dâhil olmak üzere, ilgili denetim ve uyumluluk programlarının yöneticileri, etkili bir koordinasyon sağlayacaktır ve bu doğrultuda AB ve AEA Üye Ülkeleri'nde ve ABD gibi diğer bölgelerle veya ülkelerle ortak bir denetim formatı sağlayacaktır" şeklinde tanımlanmıştır

İlgili uyumluluk programlarının yöneticileri ayrıca AB VE AEA Üye Ülkeleri'nde uygulamanın şeffaflığını, sürekliliğini ve tutarlılığını sağlamak için işbirliği yapacaktır.

"VII. İlke"de de Çerçevenin hangi koşullarda ve ne şekilde "Gözden Geçirileceği" konusu ele alınmıştır. Bu madde "Aşağıda imzası bulunan şirketler ve kuruluşlar, Çevrimiçi Davranışsal Reklamcılık ve iş uygulamalarının gelişmesine karşılık olarak bu çerçeveyi en az her 3 yılda bir gözden geçirecektir ve uygun görüldüğü takdirde çerçeveyi değiştirecek veya ekleme yapacaktır" şeklindedir. [221]

IAB Türkiye: 2007 yılı Ekim'inde 23 katılımcıyla platform olarak kurulan ve 2011 Temmuz'unda dernekleşen IAB Türkiye reklamveren - ajans - medya üçlüsünün aynı çatı altında temsil edildiği tek meslek örgütüdür. Kuruluş amacı endüstrinin bir bütün olarak, sağlıklı biçimde gelişmesine destek vermektir. Hedefleri doğrultusunda eğitimden ölçümlemeye, endüstriyel standartların oluşturulmasından yarışmalara kadar pek çok alanda faaliyet göstermektedir. Ana hedefleri şunlardır:

A. Endüstriyi standartlar ve kurallar oluşturacak şekilde organize etmek
B. Dijital pazarlama iletişimi sektörünün sağlıklı biçimde gelişmesini sağlayacak denetim ve düzenleme mekanizmalarını oluşturmak, varolana katkı vermek
C. Referans merkezi olmak
D. İnternetin reklam mecrası olarak tek çatı altında ve tarafsız bir biçimde ölçümlenmesini ve denetlenmesini; bu konuda karşılaştırılabilir ve objektif belgeler, veriler hazırlanmasını sağlamak

[221] Bkz. *IAB Europe,* EU Framework for Online Behavioural Advertising, April 2011, sf. i-xi

E. Sektördeki insan kaynağı açığının giderilmesi için çalışmak

F. İnternetin kolay satın alınan ve değer üreten bir mecra haline getirilmesine katkı sağlamak

G. İnternetin reklam mecrası olarak gelişmesine, reklam yatırımlarından aldığı payın artmasına katkı sağlamak

H. Kamu kuruluşlarıyla yakın temas kurarak yasal düzenlemeler hakkında fikir ve görüş vermek

İ. Gerektiğinde kamuoyunu bilgilendirmek

IAB en son gelişim olarak Türkiye'de dijital reklamcılığın küresel standartlar ve kurallar çerçevesinde büyümesine destek vermek üzere Avrupa'da EDAA'nın (European Interactive Digital Advertising Alliance) yönetiminde ilerleyen ODR Öz-Denetim Programı'na katılmıştır. Program, davranışsal reklamcılığın Avrupa genelinde kabul gören kurallar kapsamında yapılması için hayata geçirilmiştir. ODR Öz-denetim Programı katılımcı sayısı şu anda sadece 5 kuruluştan ibarettir [222].

D. Eğitim yaklaşımı

Tüketiciler çevrim içi izlemenin sürmesi ve olası sonuçları ile ilgili daha iyi eğitilirlerse, o zaman çevrim içi teknoloji ve hizmetleri kullanımlarında daha bilgili olarak kararlar verebileceklerdir. Kendilerini, yardımcı araçlarla daha iyi koruyabildikleri gibi çevrim içi izleme ekosisteminde yer alan kuruluşlara rekabetçi baslı uygulayabilecek, dolayısı ile söz konusu pazarın daha sağlıklı işlemesine yol gösterebilecektir. Tüketici eğitimin yolları nelerdir ve bunların etkililikleri nasıldır; aşağıda bu konulara değinilmiştir:

- Çevrimiçi mahremiyet ile ilgili genel bilgilendirme ve çevrimiçi izleme ekosisteminin varlığına ilişkin farkındalığın arttırılması.

  ABD Federal Ticaret Komisyonu sosyal ağlarda güvenlik ve çevrimiçi izleme ile ilgili bazı ipuçlarını vermektedir. ENISA (*European Network and Information Security Agency* – Avrupa Birliği Ağ Güvenliği Ajansı) yakın tarihte çerezlerin mahremiyet riskleri ile ilgili bir rapor yayınlamıştır.

[222] Bkz. *IAB Turkey*, http://www.iabturkiye.org/icerik/iab-turkiye

Demokrasi ve Teknoloji Merkezi, *The Center for Democracy and Technology* üçüncü taraf izleme ve mahremiyete etkileri konularını da kapsayn bir davranışsal reklamcılık rehberi yayınlamıştır. Avrupa Daha Güvenli İnternet girişimi, *The European Safer Internet Initiative* gençlerle ilgili olarak daha güvenli internet kullanımı konusu üzerinde durmaktadır.

- Tüketicileri kendini-koruma araçları konusunda bilgilendirme girişimleri. Sayısız web sayfası tüketicileri periyodik olarak çerezleri temizlemeleri konusunda uyarmakta ve onlara nasıl yapılacağına ilişkin bilgi sağlamaktadırlar. Stanford'un '*donottrack.us*'ı ile *Mozilla*'nın 'DNT' sayfası *DNT*'ın nasıl işlevsel hale getirileceği ve bu yolla neyin mümkün neyin mümkün olmadığı konularında bilgi sağlamaktadır. Aktif destek veren, EFF gibi örgütler çevrim içi izlemeye karşı korumalar da dâhil olmak üzere mahremiyetin korunmasına ilişkin teknolojileri araştırmaktadırlar. Doğal olarak koruyucu teknoloji satıcıları da, kendi ürünleri ile ilgili farkındalığı artırmak için toplumun ilgili kesimlerine erişebilmek için aktiftir.
- Bazı kuruluşların veri toplama uygulamaları hakkında bilgiler ve bu firmaların çevrim içi izleme eko sistemindeki ürünleri. Bunu kuruluşlar kendileri de yapmakta olduklarından bu kategori şeffaflıkla eğitim arasında gidip gelmektedir. Google reklamcılık ve mahremiyetle ilgili bir bilgi sayfası sunmaktadır. Bu tür eğitimde, sıklıkla kişisel mahremiyetin kuruluşlar tarafından ihlal örneklerinin yayınlanması yolu ile çok önemli bir role sahiptir. *The Wall Street Journal* gazetesinin "Ne Biliyorlar" yazı dizisi bunun en bilinen örneğidir. Yakın tarihlerde de akademik araştırmacılar çevrim içi izlemede kişisel mahremiyetin ihlali konularını incelemekte ve yayınlamakta daha aktif oldukları gözükmektedir.

Yukarıdaki tartışmaların ışığında, tüketicilerin eğitilmesine ilgi gösteren çeşitli kurumlar olduğu görülmektedir. Bunlar; resmi kurumlar, temel haklar ve tüketici hakları koruma örgütleri, basın, akademisyenler, çevrim içi izlemem konusunda faaliyet gösteren kuruluşlar ve web tarayıcılar da dâhil olmak üzere mahremiyeti koruyucu araç satıcılarıdır. Bu kurum ve kuruluşların hepsi söz konusu eğitimin

tüm kategorilerinde yer akmazlar; ancak her kategoride çeşitli organizasyonlar aktiftirler.

"Eğitim" bölümüne eklenmesi gerekli kayda değer kapanış yorumu da, kişisel mahremiyet alanında yapılmış uygulamalardan edinilen çok sayıdaki deneyimler çevrim içi hizmet kullanıcılarının çoğunluğu için öncelikli olan;

- Pratiklik / kullanım kolaylığı ve
- Hizmetin maliyeti ('bedava' teklifler tercih öncelikli)' dir.

Açıktır ki kullanıcıların her iki isteği, onların hizmet sunanlara kişisel bilgilerini (ki sunucular bunu paraya dönüştürmektedirler) "bedava" sunulan hizmetler karşılığında verebilmektedirler.[223]

§4. SONUÇ VE ÖNERİLER

Sonuç bölümünde öncelikle AB ve ABD'de yaşanan deneyimi güncel gelişmeler ışığında değerlendirmek, alınacak dersleri sıralamak ve çözüm önerilerini sınırları ortadan kalkmış bir iletişim dünyasında ülkemiz rekabet gücünü en üst düzeye en hızlı çıkartabilmek üzere bu deneyimlerden yararlanarak getirmek uygun bulunmuştur. Bu nedenle sonuç ve öneriler bölümü yaşanmış deneyimlerden alınan dersler ve Türkiye'nin güncel durumu ve ülkemiz için en uygun ve etkili öneriler olarak iki kısımda hazırlanmıştır.

I. Sonuç:

Çalışmada işaret edildiği gibi küresel rekabet, kuruluşları, yaşam ve başarılarını sürdürülebilir kılmak için, müşterilerine daha iyi ürün ve hizmetler sunmalarını gerektirmektedir. Bu durum kuruluşları, müşterilerini daha yakından tanımak, istek ve beklentilerini anlamak üzere, satın alma tercihlerine yön veren davranışlarını ayrıntılı bir biçimde izlemeye yönlendirmiştir.

---

[223] Bkz. *Castelluccia/Arvind*, ENISA European Network and Information Security Agency, s. 15-19, 19 October 2012,

Bilgi teknolojilerinin gelişimi ile, tüketici davranışlarının izlenerek, satın alma kararlarını oluşturan kişisel davranış biçimlerinin, giderek daha kapsamlı ve etkili bir biçimde değerlendirilebilmesi, mümkün olmuştur. Böylece ürün ve hizmetlerin, internet ortamında, müşterilerin belirlenmiş profillerine göre özel olarak sunumu ve satışı küresel ölçekte yaygınlaşmıştır.

Bunun faydası hem ürün ve hizmeti sunanlar hem de onu almayı planlayan tüketiciler için verimlilik artışı ve etkililik getirmesidir. Üretici ya da hizmeti sunan bu şekilde ürün ya da hizmetini doğru müşteri hedef kitlelerine pazarlamak için kaynaklarını mevcut ve potansiyel müşterilerinin satınalma davranış biçimlerine yön veren kişisel verilerini elde etmeye daha çok ayıracaktır; bunun sonucunda da ürün ve hizmetlerini, onlara daha fazla ilgi gösteren ya da böyle bir arayış içinde bulunan kişilere yönlendirebileceğinden satışlarını, pazar payını arttırma ve/veya koruma şansı daha yüksek olacaktır.

Tüketiciler bakımından da yine verimlilik ve etkililikten söz etmek mümkün olacaktır. Çünkü bireyler de giderek artan rekabet sonucu çeşitli pazarlama yöntem ve kanalları ile bir ürün ve hizmet sunumu kargaşası ile sürekli karşı karşıya gelmekten biraz kurtularak çevrimiçi pazarlama yolu ile kendi ilgi alanlarına daha yakın seçilmiş ürün ve hizmet pazarlama sunumu ile sınırlanmış olacaklardır.

Ancak teknolojik gelişmeler, çalışmanın Çevrimiçi Davranışsal Reklamcılık bölümünde ayrıntılı olarak anlatıldığı gibi gelişen veri madenciliği ve profil oluşturma yöntem ve teknikleri ile zaman zaman tüketicilerin bireysel mahremiyetinin ihlal riskini gündeme getirmiştir.

Yine daha önce ifade edildiği gibi Çevrimiçi Davranışsal Pazarlamanın, hem üretici hem de tüketici tarafında yarattığı olumlu etkiyi kaybetmeden, kişisel verilerin toplanması, işlenmesi ve değerlendirilerek grup, kişi profillerinin oluşturulmasında kullanımının, bireysel mahremiyeti ihlal riskini en alt düzeye indirgemek üzere çeşitli çözüm yolları tüm dünyada aranmış ve aranmaya devam edilmektedir.

Çalışmada bu konuda dünyadaki yaklaşımlardan en etkilileri olarak ABD ve AB'dekiler incelenmiş, ülkemizdeki mevcut durum ile karşılaştırılmıştır. Bu kapsamda çeşitli yasal düzenlemeler, farkındalık oluşturucu çeşitli girişimler ve

özdenetim kültürünün yerleştirilmesi yönünde çözüm araçlarının gündeme getirilmiş olduğu gözlenmektedir. Bu yaklaşımların bir kısmı genel olarak özel yaşam ve bireyin buna ilişkin hakları ile bireysel mahremiyetin ihlali konusu ile ilgili ise de bir kısmı da özel olarak Çevrimiçi Davranışsal Pazarlama ve bu konuya ilişkin kişisel verilerin toplanması, değerlendirilmesi, işlenmesi, paylaşımı ve bu konularda tarafların hakları ve sorumlulukları ile doğrudan ilişkilidir.

Ancak bireysel verilere erişim ve birey davranışlarının izlenmesi konusunda teknolojinin hızlı gelişimi ile sağlanan ilerleme, bireysel verilerin mahremiyetini koruyucu önlemlerin karşısındaki en önemli güçlük olarak görülmektedir.

ABD, AB ve Türkiye'de Düzenleyici Yasal Temelli Yaklaşımlar bölümünde ayrıntıları ile açıklandığı gibi ABD'de dikkati çeken en önemli husus öncelikle genel olarak tüketicinin korunmasında lider bir düzenleyici kuruluş olarak FTC'nin görev üstlenmesidir. İkinci önemli nokta da FTC'nin çevrimiçi pazarlama kavramı ortaya çıktığı günden bu yana FTC'nin bu yaklaşımın getirdiği yararların kaybedilmeden çevrimiçi gizlilik konularının ve sorunlarının üzerine odaklanmış olmasıdır. FTC, çevrimiçi pazarlama ile ilgili uyulması gerekli ilk ilkeleri 2007 yılında belirlemiştir. FTC uygulamalara dayalı olarak sürekli bir biçimde ilgili paydaşların görüşlerinin alınmasına ortam yaratan çalıştaylar, toplantılar düzenlemekte, öneriler ve değerlendirmeler içeren raporları, bunlara dayalı yasal gereklilikleri, Kongreye ve kamu oyuna sunmaktadır.

Ancak FTC'nin daha çok yumuşak bir gücü olduğunu görmekteyiz. Bu yaklaşımın temelinde de ABD ve AB yaklaşımlarının temel karşılaştırmasının yorumlandığı bir sonraki bölümde yer alan felsefi farklılık yer almaktadır.

Amerikan yasaları kişinin özel alanına izinsiz girenler karşısında nispeten daha pasif kalan birey, tüketici, kullanıcıyı korumaya odaklıdır (devlete ya da özel aktörlere karşı duvarlar inşa edip etmeme kararını onlara bırakır).

Amerika Birleşik Devletleri Hukukunda, çalışmada belirtildiği gibi, Avrupa Birliği Hukukundaki 1995 Veri Koruma Hakkı paralelinde kişisel bilgilerin gizliliğini düzenleyen genel bir veri mahremiyeti hakkına ilişkin yasal bir çerçeve bulunmamaktadır.

ABD'deki yasal çerçevede yer alan yasalar da (Adil Kredi Raporlama - bireysel finansal bilgilerin gizliliği, Üçüncü Kişi İnternet Reklamcılığı Tüketici Hakları 2008, Gramm-Leach-Bliley - finansal hizmetlerin modernizasyonu, HIPAA - tıbbi verilerin korunması, Çocukların Çevrimiçi Gizliliğinin Korunması, 2003 CAN-SPAM - İstenmeyen Pornografi ve Pazarlama, Telepazarlama ve Tüketici Dolandırıcılığın ve Suiistimalinin Önlenmesi, 2011 Beni Çevrimiçi Takip Etme, 2011 Kerry-McCain Ticari Gizlilik yasaları) bu yaklaşımı doğrulamaktadır.

ABD'de Çevrimiçi Davranışsal Pazarlama ilgili olarak gelinen noktada Tasarım ile Mahremiyet, İş Çevreleri ve Tüketiciler için Basitleştirilmiş Seçimler ile Daha Fazla Şeffaflık gibi temel ilkelerin öne çıktığı, opt-in yaklaşımının tercihi yönünde bir gelişim olduğu görülmektedir. Tüm bu yasal çerçeve ve yaklaşımların gözden geçirilip iyileştirilmesinde tüm ilgili paydaşların katılımına ağırlık verildiği yeni önerilerin bu geri bildirimler dikkate alarak geliştirildiği görülmektedir.

AB'de ise yasal çerçeve çalışmada açıklandığı gibi özellikle kişisel verilerin işlenmesine imkan veren çerezlerin ve birey davranışlarını izleme teknolojilerinin kullanımına yönelik bir yapıdadır.

Bu çerçevede bireyin mahremiyeti ve bireysel verilerine ilişkin hakları AİHS'nin 8. Maddesi ve ABTHB'nin 7. Ve 8. Maddeleri ile genel olarak tanımlanmıştır; genel elektronik iletişim konularının tümü için e-Gizlilik Direktifinin (2002/58/EC), kişisel verilerle ilgili olarak da Veri Koruma Direktifinin (95/46/EC) ilgili maddelerinde ayrıntılara yer verilmiştir.

AB'deki bu yasal çerçeve, çevrimiçi davranışsal pazarlama kapsamındaki tüketici davranışlarının izlenmesine olanak verecek bireysel verilerin toplanması, işlenmesi ve değerlendirilerek tüketici profillerinin oluşturulması ile de ilişkilendirilebilmekle beraber ABD'deki yaklaşıma göre daha genel bir çerçevedir.

Veri Koruma Direktifi 2. Maddesinde yer alan tanımlar (kişisel veri, kişisel verilerin işlenmesi, denetleyici, üçüncü şahıs ve veri öznesinin rızası) çevrimiçi davranışsal pazarlama, tüketici davranışları ve bireysel verilerin korunması bakımından önemlidir. Ayrıca direktifte, konumuz ile ilgili olarak yer alan orantılılık, şeffaflık, meşru amaç kavramları da benzer ilgi ve önemi taşımaktadır.

E-Gizlilik Direktifinin (2002/58/EC) amacı 1. Maddede açıklandığı gibi "kişisel verilerin işlenmesine dair temel hakları ve özgürlükleri ve özellikle de mahremiyet ve gizlilik hakkını korumak"tır. Bu direktif tüm "kullanıcı"ları, tüm elektronik iletişim hizmetlerini, bunlara ilişkin gizliliğin garanti edilmesini ve çerezlerin kullanımını ilgili maddelerde ele almaktadır. Kullanıcılara ait verilerin toplanması, işlenmesi vb. çeşitli amaçlar için kullanımına, kullanıcının kendisine net ve kapsamlı bilgi sağlanması sonunda rıza vermesi şartıyla, izin verilebileceğine işaret etmektedir. Aynı durum adres verileri için de geçerlidir.

Bu durum 2002/58/EC'nin ilk şekli ile konumuzu ilgilendirmesi bakımından reddetme (opt out) imkanı özelliğini taşımaktadır. Ancak bu yaklaşım Direktifte yapılan 2009/136/EC değişikliği ile "opt in"e dönüştürülmüştür.

AB'deki son gelişme de, AB Parlamentosunda görüşülmesi ve yayınlanması sonbaharda beklenen, 95/46/EC Veri Koruma Direktifi'ndeki, değişiklikle ilgilidir. Bu değişiklikte yer alan en önemli konular ihlallere yaptırımların gündeme gelmesi, kullanıcı rızasının verilmemesinin kolaylaştırılması, AEA dışına bireysel veri transferinin zorlaştırılması ve bireylere atfedilemeyen verilerin ayrı bir yerde muhafaza edilmesidir. Bunların yanı sıra, verilerin "unutulma hakkı yerine, güçlendirilmiş "silme hakkı"nın gündeme gelmesi, ve profilleme amaçlı veri kullanımına itiraz hakkının tanınması da önemli diğer konulardır. Bu tasarının yürürlüğe girmesi ile, AB ülkelerindeki en önemli sorun kaynağı olan ülkeler bazında farklı mevzuat ve uygulamaların "tek"e indirilmesidir

Konumuzla ilgili olarak ABD ile AB arasında bir karşılaştırma yapılacak olursa, öncelikle mahremiyet kavramı ile ilgili, felsefi ve kavramsal farklılık dikkati çeker. AB'de mahremiyet "itibar / saygınlık" ve "kişisel bilgiler bakımından özerklik" olarak anlaşılırken, ABD'de "özgürlük" olarak yorumlanır.

Bu kapsamda Avrupa'da bireysel gizliliğin (mahremiyetin) temel değeri kişinin kendi "toplumsal imajını ve onurunu kontrol edebilme hakkı" olarak kabul edilirken; ABD'deki temel değer, kişinin devletin kendisine karışması / müdahalesi ya da bireylerin mahremiyetini incitici girişimlerin gündeme getirilmesi karşısındaki özgürlüğü ya da "kendi başına rahat bırakılması" hakkı olarak yorumlanır.

Özel yaşama ilişkin haklar ABD'de mülkiyet haklarından türetilmiş olup, kişi ile yapısal / doğası gereği değil haricen ilişkilendirilerek tanımlanmıştır. Buna göre bir mülk mülkün sahibini, sahip olduklarını açıklama konusunda, tek yetkili kılar: bu durumda Amerikan görüşüne göre mahremiyet, kişinin kendi özel alanını başkalarının erişimine açmasında tek söz sahibi olmasıdır.

Avrupa'da ise saygınlık ve kişisel bilgilere ilişkin otonomi kavramlarının, bir mülk gibi serbestçe erişilebilir kılınması mümkün değildir. Bu nedenle AB yasaları, bireylere kendilerine ait hangi bilgilerin hangi kişiler/yapılar tarafından bilinebilir olmasının söz konusu birey tarafından kontrol etmesinde aktif rol almasına yardımcı olma yönündedir. Buna karşılık Amerikan yasaları kişinin özel alanına izinsiz girenler karşısında nispeten daha pasif kalanları korumaya odaklıdır (devlete ya da özel aktörlere karşı duvarlar inşa edip etmeme kararını onlara bırakır). [224]

Bu çerçevede AB, bireylerin verilerini ve mahremiyetlerini korumak için elinden geleni yapmaktadır; ve bunu opt-out rejiminden vazgeçip yerine opt-in kurallarını getirerek açıkça göstermiştir. Bu uygulama, iş çevrelerince bireylere ait özel verileri toplamadan, işlemeden ve çevrimiçi reklamcılık amaçlı kullanmadan, onların önceden ve bilgilendirilmiş olarak muvafakatleri alınmasını gerektirmektedir. AB'de yaşayanlar OBA ile ilişkili olarak veri mahremiyeti ve kötü amaçlı kullanıma ilişkin tehlikelere karşı, beklentilerinin üzerindeki bir derecede, koruma altındadırlar[225] [226].

AB Çalışma Grubu ise muvafakat konusundaki mevzuatın, bireysel bilgilerin korunması bakımından, yetersiz olduğu görüşünü sürdürmektedir. Çalışma Grubu, yapılan birçok kamuoyu araştırmalarının, interneti kullanan bireylerin çoğunluğunun, kendilerine ait bilgilerin hedeflenmiş reklamcılık için kullanıldığının farkında olmadıklarını gösterdiğine işaret etmektedir. Bireylerin çoğunluğunun çerezleri, kişisel bilgilerinin ne amaçla kullanılacağını okumadan

---

[224] Bkz. *Suuberg*, Tullane Journal of Technical & Intellectual Property, Vol. 16, s.273, 2013

[225] Bkz. *De Lima/Legge*, Computer Law and Security Review No.30, s. 67, 2014, www.science direct.com ve www.compseconline.com/publications/prodclaw.htm

[226] Bkz. *Pastor/Saldana*, Estudios sobre el Mensaje Periodistico Vol.19 Special Edition, p. 289-290, Universidad Complutense Madrid, 2013

kabul ettiklerini ileri sürmektedirler. Böyle davranmalarının nedeni zaman kazanmak ya da İnternet sitesinin tüm potansiyelinden yararlanma ihtiyacı gibi şeyler olabileceği düşünülmektedir.

Bu durum AB'nin, hedef kişilerin önceden bilgilendirilmiş *opt-in* muvafakatının alınması yoluyla korunması amacının başarılmadığını göstermektedir; bunun nedeni bireylerin kendilerine ilişkin bilgilerin toplandığının ve Çevrimiçi Davranışsal Reklamcılık amacı ile kullanıldığının farkında olmamasıdır; bu nedenle, bu durumda bilgilendirilmiş muvafakat da hükümsüz olmaktadır / veya geçerliliğini yitirmektedir. Bireylerin, okumadan ve mahremiyetleri ile ilgili ne gibi etkileri olabileceğini kavramadan onay vermeleri / muvafakat etmeleri, çerezler ve çerezlerin İnternet deneyimlerine sağlayabileceği yararlar konusunda doğru bilgilendirilmemiş olduklarını göstermektedir. Sayfalarını ziyaret etmek isteyen bireylerin davranışlarını izlemek üzere çerezleri kullanan bazı web siteleri de, bu çerezlere onay verip cihazlarına yerleştirilmesine rıza göstermeyen ziyaretçilerin web sayfalarına erişimlerine izin vermeyebilmektedir. Bireylerin özgürce muvafakat etmesi yerine kabul etmek zorunda bırakılmalarının, AB'nin yeni opt-in gereklerini gündeme getirerek yapmak istediğine ters düştüğü tartışılabilir bir konudur. Bu durum kişisel verilerin ve kişinin mahremiyetinin yasalarla korunmasına ilişkin güncel sorunların önemini ortaya açıkça koymaktadır.

Yine De Lima/Legge'ye göre teknoloji gelişim hızı yasaların oluşturulmasının önünde gittiği için iş çevrelerince Çevrimiçi Davranış Reklamcılığı amacı ile toplanan bireylere ait bilgilerin; okuyabilen, okuduğunu anlayabilen ve verilerinin toplanmasına özgürce muvafakat eden bireylerden elde edildiğini garanti edecek ve doğrulayacak bir yol / yöntemin olmadığı şeklindedir.

Özetle, ABD uygulamaları bireysel verilere kişilerin kendilerinin sahip çıkmaları; bu verilerini yüksek düzey bir farkındalık ile istedikleri kişi ve kurumlarla istedikleri şekilde paylaşabilme özgürlüğünü taşımaları üzerine yapılandırılmıştır; iş çevrelerinin ise kişisel özel verilere gereksinim duymaları durumunda (OBA'da olduğu gibi) bu süreci ve adımlarını şeffaf bir şekilde yürütmeleri; koşullarını, bireylerin üzerinde yaratabileceği olası etki ve sonuçlarını

(yaratabileceği ya da kişilerin alması söz konusu olabilecek riskleri de dâhil olmak üzere) kişisel verilerine erişmek, çevrimiçi davranışlarını ilgili web sayfalarında izlemek istedikleri kişilere anlaşılır ve açıkça ileterek, onların kesin onayını almadan yapmamaları beklenmektedir. Bu sistemin sağlıklı ve etkili çalışmasının da aynen bireylerde olduğu gibi tam bir özgürlük ortamında yürütülmesinin ancak sistemde yer alan kuruluşların kendi-kendilerini değerlendirme/yönetme (öz denetim - *self assessment*) yolu ile mümkün olduğuna işaret edilmektedir. Dolayısı ile ABD'deki tüm yasal çerçeve (anayasal temel haklardan başlayarak) böyle bir sistemin etkili ve verimli çalışmasına olanak yaratacak şekilde kurulmuş olup, paydaş geri bildirimleriyle sürekli gözden geçirilen ve iyileştirilen bir yaklaşımla yönetilmektedir. Bu yasal çerçevenin AB'de olduğu gibi "kişiyi ve mahremiyetini" yasal çerçeve ile korumaya çalışmak gibi bir amacı yoktur. AB'deki durum ise öncelikle AB'nin yasal çerçeve ile oluşturduğu ortam genel ilkeleri ve sınırları çizdiği için en önemli sorun, bu genel tanım içerisinde oluşturulan üye devletler yasal mevzuatında ve uygulamalarında farklılıkların ortaya çıkmasıdır. Bu da uygulamaların bütünselliği bakımından üye devletlerarası veri alış verişinde sorunlar yaratmaktadır. Kaldı ki teknolojinin gelişimi ile bugün gelinen noktada global pazarda sınırlar tamamen kalkmış olduğundan uyumsuzluklar global ölçekte sıkıntılara neden olabilmektedir. Nitekim AB parlamentosuna sunulan ve Mayıs 2014 den önce görüşülerek yürürlüğe girmesi beklenen 95/46/EC'yi güncelleştirme amacı ile hazırlanan tasarının Komisyonda ve Komitede görüşülüp AB Parlamento'suna sunulabilecek hale gelebilmesi, gerek üye devletlerde gerekse ABD'den ve global şirketlerden gelen geri bildirimlerin çokluğu nedeniyle iki yılı aşkın bir süre geçmiştir. Ancak bu yeni Direktif önerisi bile, AB'nin yukarıdaki bölümlerde de açıklanan geleneksel yapısı, felsefesi ve birey özellikleri ile gösterdiği farklılıklar, önceki yaklaşımlar gibi "koruyucu" niteliğini hala korumaktadır. Ancak yürürlüğe girmesi ile sağlanacak en önemli sonuçlardan birisi, üye devletlerde yürürlükte olan ve birbiri ile farklılıklar gösteren yasal çerçevenin tek'e indirgenerek bütünselliğinin sağlanması olacaktır.

Ülkemizdeki durum ise özellikle Çevrimiçi Davranışsal Pazarlamanın Tüketici Davranışlarına Etkisi ve Bireysel verilerle ilişkisi bakımından, yararların

ve risklerin dengeli bir biçimde yönetilmesine yardımcı olmak yönü ile değerlendirildiğinde, daha çok AB yaklaşımına benzemekte ancak ona da tam uyumu sağlanmamış, güncellenmemiş, yetersiz çok genel yasal çerçeveden ibarettir.

Konu ile daha yakından ilgili olarak 04/05/2007 tarih 5671 sayılı yasa ile bu yasanın 9. Md.sinde 06.02.2014 tarih 6518 Sayılı yasanın Md.93 ile yapılan bir değişiklik ve 24.07.2012 tarih 28363 Sayılı RG'de yayınlanan bir Yönetmelik (Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik) ve bu yönetmelikte 15/2/2013 ve 11/7/2013 tarihinde yapılan bazı değişiklikler dışında mevcut tüm mevzuat genel kişi hak ve özgürlükleri ile bazı özel durumlar için geçerli olacak (iş, sağlık, istatistik vb) ihlallerle ilgilidir.

5671 sayılı "Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yolu ile İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile, önceki bölümlerde ayrıntıları iletildiği gibi, internete erişim sağlayıcıları, yer sağlayıcıları vb. hizmet sağlayıcıların hukuki sorumlulukları tanımlanmış; trafik verilerinin saklanma süreleri belirlenmiştir. İlgili yönetmelikte de erişim sağlayıcı trafik bilgisinin tanımı yapılmıştır.

Bu kanunda, 6518 Sayılı ve 06.02.2014 tarihli yasa (Torba Yasa Md. 93) ile yapılan bir değişiklikle "kişilik haklarının ihlali" konusuna ile "erişimin engellenmesinin" yol ve usullerinden söz edilmiştir.

24.07.2012 tarihli Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik'te de mevzuatımızda ilk kez kişisel veri, kullanıcı rızası ve kişisel verilerin işlenmesi tanımı yapılmış olup önce de belirtildiği gibi bu yönetmelikle kişilerin rızasının alınmasından, rızanın geri alınmasından söz edilmekle birlikte yönetmelik genelde, mobil iletişim ve buna bağlı pazarlama amaçlı veri toplama ve işleme konularına odaklanmıştır.

Bu alanlardaki ihlallerin yaptırımı sadece TCK ilgili maddelerince karşılanabilmektedir. 1982 Anayasası, 2010 Anayasa değişiklikleri, TMK; BK, TCK, CMK, İş, Bilgi Edinme, Polis Vazife ve Salahiyetleri ve Türkiye İstatistik

kanunlarında da kişisel hak ve özgürlükler kapsamında kişisel verilerin gizliliğinin ihlali konuları genel olarak ele alınmıştır.

Ülkemizdeki durum açısından bakıldığında, öncelikle yasal mevzuat bakımından, yukarıda değerlendirilen ve karşılaştırması yapılan ABD ve AB uygulamaları temel alındığında, teknolojinin bu kadar hızlı değiştiği bir ortamda, bu ortamın gerek bireyler, gerek iş çevreleri ve gerekse devlet yönetimi açısından etkileri tam olarak tanımlanamamış birçok riski getirebilecektir. Bu da çok yavaş bir biçimde güncellenmeye çalışılan, bütünsellikten yoksun, dolayısı ile Çevrimiçi Davranışsal Pazarlama+nın yararları ile Bireysel mahremiyetin ihlali riskinin dengeli bir biçimde yönetilebilmesine yardımcı olmak bakımından yetersizdir.

Tüketicilerin farkındalığı bakımından da durum yine ABD ve AB ile kıyaslandığında, tüketicilerin (bireysel kullanıcıların) bireysel verilerinin nasıl elde edildiği, işlendiği, ne işe yaradığı ve davranışsal pazarlama aracı olarak nasıl kullanıldığı, üçüncü şahıslarla nasıl paylaşıldığı ve sonunda kendilerine ne gibi etkileri olacakları konularında çok düşük bilinç düzeyinde oldukları açıkça görülmektedir.

Özdenetim konusunda da dernekleşen IAB Türkiye önemli bir başlangıçtır. Önce web sayfasında Çevrimiçi Pazarlamaya ilişkin tanımlara yer vererek hem tüketiciler tarafında farkındalık yaratmaya katkı sağlama ortamı yaratmakta; özellikle de IAB Europe liderliğinde yürütülen çeşitli ilkeler çerçevelerine ve Özdenetim Programlarına katılarak hizmet verenler tarafında da dijital reklamcılığın küresel standartlar ve kurallar çerçevesinde büyümesine, sorumluluk bilincinin ve anlayışının geliştirilmesinde planlı etki yaratma potansiyeli oluşturmaktadır. Ancak bilinirliği ve yayılımı halen yeterli düzeyde değildir.

II. Öneriler

- Yasal uyum çalışmaları kapsamında AB 95/46/EC Kişisel Verilerle ilgili Direktife (e-mahremiyet direktifi) uygun hazırlanan kanun tasarısı (2008 den bu yana TCBMM gündemine alınamamıştır. Oysa AB'de de bu Direktifin, yukarıdaki bölümlerde açıklandığı gibi istenilen amaçları sağlayamadığı gerekçesiyle yenilenmesi gündeme gelmiş ve üzerinde uzlaşılan tasarının bu yıl

sonbahar döneminde yasalaşması beklenmektedir) en süratli şekilde AB'deki güncellemeye uygun olarak revize edilmesi, meclise sunulması ve daha da geciktirilmeden yasalaştırılmalıdır. Bu yasanın yürürlüğe girmesi ile ile Elektronik ortamda bireysel veri ve mahremiyetin yönetilmesi, elektronik ortamda ticaret kapsamında bu kişisel verilerin ve çevrimiçi davranışların elde edilme, kullanılma ve izlenmesi (mahremiyetin ihlali de söz konusu olabilir) konularının yönetilebilmesine ve kontrol altına alınabilmesine ilişkin çerçeve tanımlanmış olacaktır. Bu kurallar Çevrimiçi Davranışsal Pazarlama konusundaki riskleri de azaltmakta katkı sağlayacaktır.

- TCBMM'de görüşülüp yasalaşması gereken ikinci kanun tasarısı e-ticaret ile ilgilidir. Çevrimiçi Davranışsal Pazarlama ve Kişisel veriler ilişkisi bakımından bir özellik içermese de (AB'de de ilgili yasada bireysel verilerin korunması konusunda Veri Koruma Direktifine gönderme yapılmaktadır) e-ticaret ve kurallarının belirlenmesi bakımından TCBMM gündeminde durmadan geri sıralara bıraktırılan bu yasanın da görüşülüp hemen yürürlüğe girmesi gereklidir.

- Dolayısı ile en önemli eksiklik Çevrimiçi Davranışsal Pazarlama ve bunun kişisel veriler ve mahremiyet üzerindeki etkilerinin global trendlere uygun bir biçimde yönetilmesine imkan verecek ticari ve bireysel verilerin korunması ile mahremiyeti ilgilendiren yasal mevzuatın en güncel şekilde (en azından AB ile olabildiğince uyumlu) tamamlanması gerekmektedir. Bu yasal çerçeve eksikliğinin giderilmesi 04.05.2007 tarih ve 5671 sayılı yasanın, 93. Md.de 06.02.2014 de yapılan değişikliği ve 24.07.2014 tarihli Yönetmeliğin bütünleşik olarak karşılayamadığı gereklerin yerine getirilmesinde hem eksiklikleri giderecek sağlayacak hem de bütünselliğe katkıda bulunacaktır. Çevrimiçi Davranışsal Pazarlama ve bunu kişisel veriler ve mahremiyet üzerindeki etkilerinin global trendlere uygun bir biçimde yönetilmesine imkan verecek bir yasal mevzuat çerçevesinin, en azından AB ile olabildiğince uyumlu hale getirilebilmesine imkan sağlayacaktır.

- Bireylerin mahremiyetlerin ihlalini, bilgilerinin farklı amaçlar için kullanımını düzenleyebilecek yasal çerçevenin yanı sıra söz konusu bilincin, farkındalığın oluşturulabilmesi için çeşitli şekillerde eğitimler verilmesi gereklidir. Bu eğitimler devletin yönlendirmesi ve desteği ile basılı ve görsel iletişim araçları, web sayfaları vb vasıtalarla ilgili kamu ve özel ile çeşitli birlik ve STK'lar (Sivil Toplum Kuruluşları) tarafından planlanmalı ve bir bütünsellik içerisinde oluşturulmalı ve iletilmelidir. IAB Turkiye girişimine de bu alanda önemli bir görev yüklenmektedir.
- Son ve en önemli konulardan birisi de öz denetimdir. Çevrimiçi Davranışsal Pazarlama faaliyetlerinde bizzat ve dolaylı yer alan iş çevrelerinin kendi içlerinde organize olarak konuya ilişkin global düzeyde kabul görmüş yönetişim prensiplerini, tanımlanmış ve güncelleştirilmiş yasal çerçeve ile uyumlu olarak yaşama geçirmek olacaktır. Bu yaklaşım ilgili kuruluşları kendi kendilerini denetim altında tutarak hem işlerinin yeni teknolojilerin kullanımı ile geliştirilmesi ancak bunu gerçekleştirirken tüketiciye karşı şeffaf olunması ve tüketicinin kişisel bilgilerini paylaşma kararını, kendisine sağlanan açık bilgilerle en sağlıklı olarak verebilmesine olanak ve ortam sağlanmış olması gerekmektedir. Bu bakımdan IAB Türkiye önemli bir başlangıçtır.

- Bu önerilerin bir bütün olarak planlanması, gerçekleştirilmesi ve sürdürülmesi gerekmektedir. Güncellik en öncelikli konudur. Aksi halde global pazarda da bu yaklaşımın eksiklikleri ve dünya ile uyumsuzluğu ve açık noktaları Türk tüketicisinin zarar görmesine neden olabileceği gibi genel ekonomik / siyasal olumsuzluklara da sebep olabilecektir.

ÖZGEÇMİŞ

Ali Burak Ensari 4 Aralık 1985'de doğdu.

Özel Yüzyıl Işıl İlkokulundan 1996'da, MEF Ortaokulundan 2000'da, Özel Ayazağa Işık Lisesinden 2004 yılında mezun oldu

Lisans öğrenimini İstanbul Bilgi Üniversitesi Hukuk Fakültesinde Temmuz 2010 yılında tamamladı.

Mart 2011 de İstanbul Barosu Hukuk İngilizcesi ve Terminolojisi Kursu Katılım Belgesi aldı.

2011 yılında TÖMER, Ankara Üniversitesi'nden ADP (Avrupa Dil Portfolyosu) B2 Düzeyi Sertifikası aldı.

2011 yılında İstanbul Institute tarafından düzenlenen sertifika programına katılarak Bilgi Teknolojileri Hukuku Sertifikası aldı.

Avukatlık stajını 1 Ekim 2010 – 30 Eylül 2011 tarihleri arasında ilk altı ayda İstanbul Adliyesinde, ikinci altı ayda da Altınsoy Hukuk Bürosunda tamamlayarak avukatlık ruhsatını aldı.

Eylül 2011 de İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programına kaydoldu; Zorunlu derslerini başarı ile tamamladı (GPA 3,39); şu anda tez aşamasındadır.

1 Mayıs 2005 – 30 Eylül 2010 tarihleri arasında Yönetişim Yönetim Danışmanlık ve Tic. Ltd. de asistan olarak, 1 Ocak 2012 – 30 Mart 2013 tarihleri arasında Dayıoğlu Hukuk Bürosunda avukat olarak çalıştı; halen, 10 Mart 2013 de işe başlamış olduğu, CLO Law Office'de avukat olarak çalışmaktadır.