

Çevrimiçi Davranışsal Reklamcılık ve Kişisel Mahremiyet İhlalleri

Melih Kırıldoğ¹

¹ Marmara Üniversitesi Bilgisayar Mühendisliği Bölümü / Alternatif Bilişim Derneği
melihk@marmara.edu.tr

Özet: Çevrimiçi Davranışsal Reklamcılık (ÇDR) Internet ortamında kullanıcıların hareketlerinin izlenerek ilgi alanlarına uygun şekilde reklam gösterilmesidir. ÇDR diğer tür Internet reklamcılığı uygulamalarına oranla daha etkili bir reklam türüdür. Ancak ÇDR vasıtasıyla kişinin hareketlerinin izlenmesi ve ilgi alanlarının saptanması birçokları için hiç arzu edilmeyen bir eylemdir. Tüm Internet kullanıcıları ÇDR uygulamalarının hedefi olmalarına rağmen çok az insan bunun farkındadır.

Anahtar Sözcükler: Çevrimiçi Davranışsal Reklamcılık, Derin Veri Analizi, çerezler

Online Behavioral Advertising and Personal Privacy Violations

Abstract: Online Behavioral Advertising (OBA) is a term used for tracking the behaviors of Internet users and displaying advertisements which are relevant to their interests on their computers. OBA is a more effective kind of advertisements than other types of Internet advertisements. Yet, many people are annoyed by being tracked and interests determined. Although all Internet users are subject to OBA, very few are aware of it.

Keywords: Online Behavioral Advertising, Deep Packet Inspection, cookies

1. Giriş

Çevrimiçi Davranışsal Reklamcılık (ÇDR) (Online Behavioral Advertising) Internet ortamında kullanıcıların hareketlerini takip ederek kişisel ilgi alanlarının saptanması ve bu ilgi alanlarına göre yine Internet ortamında kendilerine reklam gösterilmesini içeren bir kavramdır. Görünüşte masum olmasına rağmen “kişisel ilgi alanlarının saptanması” oldukça sorunludur. “Kişisel ilgi alanları” sadece reklamcılık amacıyla otomobil, cep telefonu, vs. satınalma niyetli insanların saptanmasıyla kalmaz; kişilerin tüm özellikleriyle profillenmesine kadar gider.

ÇDR dünyada ve Türkiye’de Internet ortamında yaygın olarak kullanılmaktadır. Buna rağmen sıradan Internet kullanıcısı bu durumdan habersizdir. ÇDR kapsamında kullanıcıların başkalarıyla e-posta iletişimi ve ziyaret ettikleri siteler çeşitli yazılım ve donanım araçlarıyla analiz edilmektedir. Bu analiz sonucunda kişilerin siyasal, dinsel, felsefi ve cinsel eğilimleri ve siyasi parti, sendika ve dernek gibi kuruluşlara üyelikleriyle birlikte tüketim alışkanlıkları ortaya çıkarılmaktadır. ÇDR’nin amacı tüketim alışkanlıklarına uygun reklam göstermek olmasına karşın açığa çıkan diğer özelliklerinin kişileri “fişlemek” için kullanıldığına dair yaygın bir inanç vardır. Bu yönden denetimsiz ortamlarda ve kanuni düzenlemenin olmadığı şartlarda yapılan ÇDR kişilik haklarına açık bir saldırı olarak tanımlanabilir. Kişilerin ÇDR kullanımından edindikleri yararın sınırlı olması ve ÇDR vasıtasıyla izlendiklerinden habersiz olmaları durumu daha da ağırlaştırmaktadır.

2. ÇDR uygulamaları ve çerezler

ÇDR uygulamaları asıl olarak kullanıcının

bilgisayarına sunucular tarafından bırakılan çerezler (cookie) vasıtasıyla yürütülmektedir. Tarayıcı vasıtasıyla silinebilen alışılmış çerezlerin haricinde başka çerez türleri de bulunmaktadır. Birçok ÇDR uygulaması tarayıcıların kendi çerezlerini değil, Flash programının çerezlerini kullanmaktadır (Local Shared Objects - LSO). Bu yöntemle teknik bilgiye fazla olmayan kullanıcıların ÇDR sisteminden isteseler de çıkamamaları amaçlanmaktadır. Zira, çerezler vasıtasıyla gözetlendiğini öğrenen sıradan bir kullanıcının doğal refleksi tarayıcısındaki çerezleri temizlemek olacaktır. Ancak, tarayıcılardaki “çerezleri temizle” fonksiyonları LSO’ları temizlemez. Bu çerezlerin temizlenmesi için diskünüzde yerlerinin bilinmesi gerekir ki, kullanıcıların ezici çoğunluğunun ne LSO’ların varlıkları, ne de disk üzerindeki yerleri konusunda herhangi bir bilgileri yoktur.

Bazı ÇDR uygulamalarında kullanıcının bilgisayarındaki çerezler ziyaret ettiği web sitesi tarafından değil, Internet Servis Sağlayıcı (ISS) tarafından oluşturulmaktadır. Çerezde kullanıcıya verilen (fakat kendisinin haberdar olmadığı) bir kimlik numarası ile ziyaret ettiği web sitesinin adresi bulunmaktadır. Bu durum, Internet ortamındaki doğal işlerliğe uzak olup kullanıcının kandırılması anlamına gelmektedir. Diğer bir nokta da ziyaretçi bilgisayarlarında çerez bırakmayacağını açıklayan web sitelerinin durumudur. Sunucu yerine ÇDR uygulaması yapan ISS’lerin çerez bırakması ile sadece kullanıcı kandırılmamakta, aynı zamanda bu siteler hiç haketmedikleri halde güvenilir duruma düşürülmektedirler.

3. Türkiye’de ÇDR

ÇDR işlerliği kişilerin ziyaret ettikleri sitelerin sınıflandırılması ve kişisel iletişimlerinin analizi (özellikle Google firması tarafından yaygın Gmail e-posta sisteminin kullanımıyla) yapılmaktadır. Bu işlerlik fazlasıyla rahatsız edici olmakla birlikte, bunlardan daha da tehlikelisi DPI (Deep Packet Inspection - Derin Veri Analizi) yöntemiyle yapılan ÇDR'dir. DPI postanede mektupların sadece zarf üzerindeki adreslere iletilmesi yerine zarfların açılarak içeriklerinin okunmasına benzer bir teknolojidir. Bu teknoloji vasıtasıyla Internet ortamında gönderilen mesajlar ve ziyaret edilen siteler ilgisiz kişi ve kuruluşlar vasıtasıyla gözetlenebilir. Türkiye'de Google'dan başka ÇDR uygulaması yapan birçok şirket bulunmaktadır. Ancak DPI teknolojisini kullanarak ÇDR ülkemizde sadece TTNET ile işbirliği yapan Phorm isimli şirket tarafından gerçekleştirilmektedir. Ağır mahremiyet ihlalleri nedeniyle ABD, İngiltere, Güney Kore ve Romanya'da faaliyeti durdurulan bu şirket ülkemizde de büyük tepki görmüş (bkz. Enphormasyon.org) ve bu tepkilerin sonucunda BTK geçtiğimiz günlerde TTNET ve Phorm aleyhinde soruşturma başlatmıştır.

TTNET-Phorm ortaklığının Gezinti sistemi teorik imkanı vermektedir (opt-in). Ancak, sıradan kullanıcı ilgili bilgi penceresini kapatmak suretiyle anlamadığı ve benimsemediği bu işten kurtulmaya çalışırken sistem tarafından "içeri alınmakta" ve bundan haberi olmamaktadır. Açıkça hile ve yanıltma içeren bu işlerlik BTK'nın açtığı soruşturmanın dayanaklarından biridir.

Alışıl gelmiş çerezler yerine LSO çerezleri kullanan bu şirketin diğer ÇDR şirketlerinden bir başka farkı da faaliyetlerini TTNET ile ortaklaşa yürütmesidir. Bilindiği gibi TTNET Türkiye'de Internet omurgasının sahibi olup tüm Internet trafiği bu omurgadan geçmektedir. Phorm'un yöntemi, sınırlı iş ortaklığı temelinde yürüyen klasik izlemenin tersine deyim yerindeyse "suyun başını tutarak" kullanıcıya hiçbir kaçış imkanı bırakmamaktadır (AB, 2010).

Türkiye'deki diğer ÇDR sistemlerinde kullanıcıya bu kadar bile bilgi verilmemektedir. Basit yöntemler kullanılarak yapılacak bir teknik analiz (örneğin, Windows ve Linux ortamlarında *netstat* komutu çıktısının analizi veya tarayıcılarda *Collusion* ve *Ghostery* eklentilerinin oluşturduğu veriler) sıradan bir Internet kullanıcıını dehşet içinde bırakacak şekilde nasıl ve kimler tarafından gözetlendiğini ortaya çıkaracaktır. Bu gözetleme için kullanıcılardan herhangi bir izin alınması söz konusu değildir. Örneğin, aşağıdaki resim *Ghostery* eklentisi vasıtasıyla Internet üzerinden günlük gazete okuyan bir kullanıcının kimler tarafından izlendiğini göstermektedir. İzleyenlerin listesi sağ üst köşede olup üzerlerinin çizili olması *Ghostery*'nin kendilerini engellediği anlamına gelmektedir.



BTK'nın Phorm şirketinin faaliyeti konusunda TTNET hakkında soruşturma açtığını açıklayan 4/12/2012 tarihli kararında şöyle denilmektedir:

"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 yapılmayarak ve aboneleri/kullanıcıları eksik bilgilendirerek Elektronik Haberleşme Sektöründe Üketiciler Hakkında 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."

Bu ifade doğru olup tümüyle halihazırda ÇDR yöntemini kullanan diğer şirketler için de geçerlidir. Çünkü bu şirketler de yaptıkları iş konusunda kullanıcıları bilgilendirmemektedirler. Dolayısıyla bu şirketlerin de aynı muameleye tabi olması beklenir.

5. Avrupa Birliği ve ÇDR

ÇDR vasıtasıyla Internet kullanıcılarının izlenmesi sadece Türkiye'ye özgü bir durum da değildir. Örneğin, AB müktesebatında (2009/136/EC)

"kişiler hakkında bilgi toplamak veya kişilerin cihazlarında bulunan bilgilere (çerezler vasıtasıyla) erişim ancak ilgili kişinin açık ve ayrıntılı bir şekilde bilgilendirilmesinden sonra kendisinin vereceği onayla gerçekleşebilir"

denmesine rağmen gerçek hayatta bu şart yerine getirilmemektedir. ENISA'ya (European Network and Information Security Agency - Avrupa Ağ ve Bilgi Güvenliği Kurumu) göre Avrupa'da ISS'lerin yüzde

sekseni çerezler vasıtasıyla kendi aboneleri hakkında bilgi toplamaktadırlar (ENISA, 2011). Bu bilgiler asıl olarak ÇDR amacıyla kullanılmakta olup kullanıcılara gözetlendiklerine dair herhangi bir bilgilendirilmemekte veya bilgi sıradan kullanıcının okumadan imza attığı "Hizmet Sözleşmesinin" derinliklerinde anlaşılabilir teknik jargonun arkasına gizlenmektedir. Ayrıntıları sadece belli düzeyde teknik bilgisi olan internet kullanıcıları tarafından farkedile bu durum, sıradan bireyleri de rahatsız etmektedir. Bir Eurobarometer (2011) anketine göre Avrupa'luların çoğu elektronik araçlarla toplanan kişisel bilgileri konusunda endişelidir.

Nitekim, "2002/58/EC" numaralı AB "Directive" web sitelerine kişisel veri toplanması ve çerez kullanımı ile bilgilendirme notu koyma zorunluluğu getirmesine rağmen sitelerin ancak çok küçük bir kısmı buna uymaktadır.

Aslında AB bu konuda olumlu bir düzenlemeyi öngörmektedir. AB kapsamında faaliyet gösteren "Article 29 Data Protection Working Party"e ait 22/6/2010 tarihli ve "Opinion 2/2010 on Online Behavioural Advertising" başlıklı dokümana (AB, 2010) göre ÇDR şirketleri AB kişisel veri koruma konusundaki müktesebatının gereği olarak kullanıcıya nasıl ve ne amaçla izleneceklerini açıklıkla anlattıktan ve aynı açıklıkla onayını aldıktan sonra

- izleme faaliyetini ancak belli bir zaman süreci boyunca yapmalı,
- kullanıcının verdiği izni kolaylıkla kaldırabilmesini sağlayacak düzenlemeler yapmalı,
- izlemenin gerçekleştiği süre boyunca görünebilir işaretlemelerle bu durumu sürekli olarak kullanıcıya anlatmalıdırlar.

Herhangi bir bağlayıcılığı olmayan bu işlemler genellikle ÇDR şirketleri tarafından gerçek hayatta uygulanmamaktadır. Zira bu şirketlerin bu koşulları uygulamaları durumunda izledikleri kullanıcıların bir kısmını kaybedecekleri aşikardır. Dolayısıyla, ÇDR kapsamında AB'nin kişisel veri koruması ile ilgili koşulları havada kalmaktadır. Şirketlerin gücü bu koşulların uygulanmasının önünde engel oluşturmaktadır.

6. ÇDR ve insan faaliyetinin metalaşması

Bilişim sistemleri esas olarak insan faaliyetlerinin soyut düzeye yansımalarından oluşur. Bu yansıma sayısız şekilde tezahür edebilir. Son zamanlarda Web 2.0 olarak adlandırılan kavram değer üretimi ve metalaşma sürecinde yeni ve çok ilginç bir aşamayı temsil etmektedir. Bu kavramla kişilerin bilgisayar ve internet ortamındaki faaliyetleri hiç böyle bir niyetleri olmamasına rağmen pazarda alınıp satılabilen soyut bir mal haline getirilmektedir. Diğer bir deyişle kişi

bilgisayar adı verilen metayı kullanırken durum tersine dönmekte ve bizatihi kişinin kendi davranışları meta haline gelmektedir. Üstelik, bu değeri üreten bireylerin çoğu ürettikleri değerden habersizdirler. Dolayısıyla, ürettikleri değer üzerinde herhangi bir hak talepleri bulunmamaktadır. Tüm bunların doğal sonucu üretilen değerlerin gerçek sahiplerinden izinsiz olarak alınıp kullanılmasıdır. Bu durum hukuki olarak açık bir hak ihlalidir. Denetimsiz yapılan ÇDR tüm bunları gerçekleştirdikten sonra bir adım daha ileri gitmekte ve insanların kişisel mahremiyetlerini ayaklar altına alacak şekilde siyasal, dinsel, felsefi ve cinsel eğilimleriyle birlikte sendika, dernek ve parti üyeliklerini ilgisiz kişi ve kurumlarca bilinir kılabilmektedir.

Tüm bunların anlamı ÇDR vasıtasıyla bireylerin iki yönden zarar görmesidir: Hem kendine ait bir değere izinsiz ve bedeli ödenmeden el konmakta, hem de bu süreçte entemel insan haklarından biri olan kişisel mahremiyeti ortadan aldırılmaktadır. Tüm bunlardan ÇDR uygulamalarına ancak kişinin kendi açık rızası varsa izin verilmelidir.

7. Sonuç

Tüm bunlardan internet reklamcılığının tümüyle zararlı olduğu önermesi çıkarılmamalıdır. Çünkü ÇDR internet reklamcılığı konusunda tek yöntem değildir. Etkinlik düzeyleri ÇDR kadar olmamakla birlikte internet ortamında birçok başka reklam yöntemi mevcuttur. Bu yöntemlerin çoğunun ÇDR'nin mevcut kullanımındaki ağır hak ihlallerinin aksine kullanıcılarına herhangi bir zararı yoktur.

Bunun ötesinde izlenmeyi önemsemeyen ve ÇDR vasıtasıyla bilgisayarlarında kendi zevk ve alışkanlıklarına uygun reklam görmek isteyenler de olacaktır. ÇDR ancak kullanıcının açık onayıyla sadece budurumlarda uygulanabilmeli, yukarıda belirtilen AB önermeleri doğrultusunda istenildiği zaman da uygulama durdurulabilmelidir.

Türkiye'de ÇDR konusunda halihazırda yapılması gereken, AB'nin yukarıda belirtilen üç maddelik önermesi ışığında kanun ve düzenlemelerin çıkarılarak mevcut başıboşluğun veya yoğun mahremiyet ihlallerinin ortadan kaldırılmasıdır.

8. Kaynaklar

[1] AB (2010). "Article 29 Data Protection Working Party: Opinion 2/2010 on online behavioural advertising". http://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CC0QFjAA&url=http%3A%2F%2Fec.europa.eu%2Fjustice%2Fpolicies%2Fprivacy%2Fdocs%2Fwpdocs%2F2010%2Fwp171_en.pdf&ei=N7PaUJ3iB8yVswbsr4GCw&usq=AFQjCNHZGsXPFgpbxmNqWul0FnbrvI9QlA&bvm=bv.1355534169,d.Yms

[2] DPA (tarihsiz). "Data Protection Act, Switzerland".
<http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.CH>

[3] Eurobarometer (2011). " Attitudes on Data Protection and Electronic Identity in the European Union". http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[4] ISA (2011). "Bittersweet Cookies: Some Security and Privacy Considerations". <http://www.enisa.europa.eu/activities/identity-and-trust/library/pp/cookies>