Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi

Enis Karaarslan[1], Mehmet Beşir Eren[1], Serhat Koç[2]

[1] Muğla Sıtkı Koçman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Muğla

[2] Güneli & Koç Hukuk Bürosu, İstanbul

enis.karaarslan@mu.edu.tr, m.besir.eren@gmail.com, avukat@serhatkoc.com

Özet: Çevrimiçi trafiğin takip edilmesi çoğunlukla ticari amaçla yapılmaktadır. Kullanıcının kişisel ilgi alanlarının saptanması ve ona göre reklam gösterilmesine Çevrimiçi Davranışsal Reklamcılık (ÇDR) denmektedir. Bu amaçla kullanılan teknoloji, kişinin tüm özellikleriyle profillerinin oluşturulmasını da sağlamaktadır. Bu çalışmada, bilgi toplama yöntemlerinden çevrimiçi web izleme ve mahremiyet konusu teknik ve hukuki açılardan ele alınmıştır. Kişisel verilerin mahremiyetini sağlamak için kullanılabilecek yöntemlerin etkinliği de ele alınmıştır.

Anahtar Sözcükler: çevrimiçi mahremiyet, tasarımla mahremiyet, çevrimiçi web takibi, çevrimiçi davranışsal reklamcılık

Abstract: Monitoring of the online traffic is often made with commercial purposes. The detection of the user's personal interests and representing advertisements according to these is called Online Behavioral Advertising (OBA). The technology used with this purpose, also provides profiling of the person with all specifications. In this study, online web monitoring which is an information collection method and the privacy issues are addressed with technical and legal aspects. The effectiveness of the methods that can be used to ensure the privacy of personal data, are also discussed.

Keywords: online privacy, privacy by design, online web tracking, online behavioral advertising

1. Giriş

Kullanıcılar Internet ağına bağlı teknolojileri kullanımları esnasında, farkında olarak veya olmayarak çeşitli izler bırakmaktadırlar. IP adresinden bulunduğu yer, mobil cihazlarla ayrıntılı koordinat bilgileri, çerezlerle (cookie) hangi sitelere ne zaman girildiği, sosyal medya aracılığı ile çok daha fazla bilgi internet ortamına sunulmaktadır.

Devletler, şirketler ve çeşitli organizasyonlar çeşitli teknolojik imkanları (internet, cep telefonu altyapısı, kredi kartları, kamera sitemleri vb.) kullanarak bilgi toparlamaktadırlar. Internet üzerinden Çevrimiçi Davranışsal Reklamcılık (ÇDR) ile toparlanan bilgilerin yıllık ekonomik değerinin 39 Milyar dolardan daha fazla olduğu ifade edilmektedir[1]. Toplanan verilerle ilgili kapsamlı bir araştırma [2], The Wall Sreet Journal'da uzun bir süredir yayınlanmaktadır. Kovacks'in sunumunda [1] da belirtildiği üzere, bu tür toplanan veriler kullanıcıların İnternet'i daha etkin kullanması için kullanılabilir ama hangi verilerin hangi firmalar tarafından toplandığının da bilinmesi gereklidir. Kaldı ki bu toplanan bilgiler her zaman kişinin yararına kullanılmaya-bilmektedir. Örneğin firmaların alışveriş yapan kişiye göre fiyatları değiştirebildiği de tespit edilmiştir [2].

Bir kişiyi tek başına belirlenebilir kılabilen ve/veya işaret edebilen her tür bilgiye kişisel veriler denir. Bireyin kişisel verilerinin korunması, anonimlik hakkı, unutulma hakkı ve silinme hakkından söz etmek mümkündür. Kişisel Verilerin Korunması Hakkı, İnsan

Hakları Yaklaşımında şu şekilde açıklanmıştır; insan onuru, bireysel özerklik, bilgilerin geleceğini belirleme hakkı en temel önem arz eden hususlardır. Öyle ki, özel yaşamın gizliliği hakkı, düşünceyi açıklama özgürlüğü, bilgi edinme hakkı, özel haberleşmenin gizliliği ve de bilim özgürlüğü gibi ana hak ve özgürlükler olmazsa olmaz olarak tarif edilmiştir.

Dürüst insanın saklayacak bir şeyi yoktur, diye karşı tezlerle mahremiyet hakkı çürütülmeye çalışılmaktadır. Mahremiyet, saklanacak bir şeyinizin olmamasıyla alakalı değildir [2]. "Mahremiyet size ait olan hayatınız hakkındadır", "fısıldama hakkıdır" [3]. Mahremiyetin korunması, mevzuatın yanı sıra mahremiyet koruma teknolojilerini de gerektirir.

Bu çalışmada bilgi toplama metotlarından çevrimiçi web izleme, mahremiyet ve anonimlik konusu teknik ve hukuki açılardan ele alınacaktır. Çevrimiçi web takibini engellemek için kullanılabilecek yöntemler de açıklanmıştır.

2.Mahremiyetin Hukusal Boyutu:

2.1.Anonimlik ve Unutulma Hakları

Anonimlik verilerin gizlenmesi noktasında iletişim halindeki kişilerin kimliklerini saklamaya yarayan bir yöntem olarak gözükmektedir. Her ne kadar, bu yöntem şifreleme gibi bir güvenlik aracı ise de, doğası itibarı ile farklıdır. Çünkü şifreleme bir teknolojidir fakat anonimlik bir yöntemdir. Anonimlik hakkı, bir kişi ya da grubun görüş ve düşüncelerini, kimliğini ortaya çıkarmadan açıklaması ve yayması anlamını taşımaktadır. Kişilerin internet üzerinde anonim kalarak iletişim kurabilme olanağına sahip olmaları, yaşadıkları toplumda siyasi, sosyal, ahlaki ve benzeri baskılardan kaçarak örgütlemek isteyenler için önemli bir fırsat alanı yaratmıştır. Bu anlamda ACLU-Miller davası önemlidir. 1997 yılında Georgia Eyalet Yüksek Mahkemesi ABD anayasasının 1. ekine dayanarak gönderenin tam olarak belirlenemediği her türlū elektronik iletişimi yasaklayan bir eyalet yasasının iptaline karar vermiştir. Mahkeme kararında internet üzerindeki iletişimi kontrol altına almaya eğilimli olan bu tarz bir düzenlemenin ifade ve iletişim özgürlüğü ile bağdaşamayacağı ve bireyin özel hayatına müdahale niteliği taşıyacağı sonucuna varmıştır. Anonim kalmak isteyenlerin ana fikri, anonim kalmanın bir özgürlük sağlamasıdır. Ancak anonim olarak fikir beyan etme alışkanlığının yaygınlaşması uzun vadede içine kapanık toplumlar oluşturmaktan başka bir işe yaramayacaktır[4]. Anonim kalmanın yanında aslında çok acil bir soruna daha işaret eden unutulma hakkı da bireyin dijital dünyadaki izlerinin ve özellikle de sosyal medya üzerindeki geçmişinin kendi talebiyle silinip silinemeyeceği tartışmasının yoğunlaşmasıyla gündeme gelmiş bir yeni kuşak haktır. Bu konu AB direktiflerinde "Veriler çok uzun süredir toplanış amaçları çerçevesinde kullanılmıyorsa ve kullanıcı da söz konusu verilerin saklanmasına rıza göstermiyorsa 'veri denetçisi' kullanıcıya ait verileri gecikmeksizin silmek ve daha fazla yayılmalarını engellenmesinden sorumludur." şeklinde düzenlenmiş ve fakat istisnası da: "Ancak, ifade özgürlüğünün korunması, genel sağlığı ilgilendiren bir konuda kamu yararının olması gibi şartların varlığının yanı sıra tarihsel, istatistiksel ve bilimsel amaçlar ile Birliğin veya üye devletlerin hukuk sistemlerinin gerekli kıldığı durumlarda denetleyici veriyi tutma ve saklama hakkına sahiptir."

2.2. Uluslararası ve Uluslarüstü Hukukta Kişisel Verilerin Korunması:

Avrupa İnsan Hakları Sözleşmesi'nin "Özel hayatın ve aile hayatının korunması" başlıklı 8. Maddesine göre: "Her şahıs hususi ve ailevi hayatına, meskenine ve muhaberatına hürmet edilmesi hakkına maliktir. Bu hakların kullanılmasına resmi bir makamın müdahalesi demokratik bir cemiyette ancak milli güvenlik, amme emniyeti, memleketin iktisadi refahı, nizamın muhafazası, suçların önlenmesi, sağlığın veya ahlâkın ve başkasının hak ve hürriyetlerinin korunması için zaruri bulunduğu derecede ve kanunla derpiş edilmesi şartıyla vuku bulabilir."

AB Temel Haklar Şartı'nın "Özel hayata ve aile hayatına saygı" başlıklı 7. Maddesine göreyse: "Herkes, özel hayatına, aile ha-

yatına, konutuna ve haberleşme özgürlüğüne saygı gösterilmesini isteme hakkına sahiptir." 8. madde ise "Kişisel verilerin korunması" başlığına sahiptir ve madde açıkça şu 3 hususu ifade eder: "Herkes, kendisini ilgilendiren kişisel verilerin korunması hakkına sahiptir. Bu veriler, adil bir şekilde, belirli amaçlar için ve ilgili kişinin rızasına veya yasa ile öngörülmüş diğer meşru bir temele dayanarak tutulur. Herkes, kendisi hakkında toplanmış verilere erişme ve bunları düzelttirme hakkına sahiptir." BM İnsan Hakları Evrensel Bildirisi'nin 12. Maddesi de aynı yönde olmak üzere: "Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır." hükmüne yer vermiştir. Yine BM Kişisel ve Siyasal Haklar Sözleşmesi'nin "Mahremiyet hakkı" başlıklı 17. maddesi de benzer bir ifade içermektedir: "Hiç kimsenin özel ve aile yaşamına, konutuna veya haberleşmesine keyfi veya hukuka aykırı olarak müdahale edilemez; onuru veya itibarı hukuka aykırı saldırılara maruz bırakılamaz. Herkes bu tür saldırılara veya müdahalelere karşı hukuk tarafından korunma hakkına sahiptir."

2.3.Avrupa Birliği'nde Kişisel Veriler Hukuku:

24.10.1995 tarihli Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi'nin[5] 15. maddesi de insani bir katkı olmaksızın otomatik surette kişisel veri işlenmesi sonucunda alınacak kararlar ve elde edilebilecek kişisel profillerin ancak ilgili kişi hakkında olumsuz olmayan bir değerlendirme içermeleri durumunda dikkate alınabileceğini hükme bağlamıştır. Anılan direktifte kişisel verilerin korunması hukukunun temel ilkeleri de yer almaktadır. Buna göre koruma sadece gerçek kişiler içindir, otomatik ya da otomatik olmayan yollarla gerçekleştirilen veri işlemeler korunabilir, kamu güvenliği, ülke savunması, devlet güvenliği ve ceza hukuku alanındaki faaliyetler kapsam dışına alınabilir. Direktife göre bir yabancı ülkede eşdeğer koruma bulunuyorsa veriler yurtdışına aktarılabilir. Eşdeğer koruma olmayan hallerde, belirli koşullar altında istisnai olarak veri yurt dışına aktarılabilir. Hakkında veri işlenen kişinin, yapılan işlemler ve kendisine tanınan haklarla ilgili bilgilendirilmesi ve de ilgili kişinin verilere erişme, düzeltme, sildirme, engelleme, itiraz ve yasa yoluna başvurma hakkının tanınmış olmasının gerekmesi de en temel ilke olarak karşımıza çıkmaktadır.

AB Veri Koruma Regülasyonu tasarı teklifi[6] Ocak 2012'de AB Komisyonu tarafından kamuoyuna sunuldu. Regülasyon tasarısı teklifi 22 Ekim 2013 tarihinde Avrupa Parlamentosu'nun Sivil Haklar, Adalet ve İç İşleri Komitesi tarafından kabul edildi. Bununla AB'de yerleşik kişilerin, kişisel verilerinin aynı derecede korunmasının sağlanması ve de AB bünyesinde dijital pazarın büyümesine katkı sağlanması amaçlanmıştır.

2.4.Türkiye'de Kişisel Verilerin Korunması:

Verilerin işlenmesi Türkiye'de de gerek kamu ve gerekse özel sektör tarafından her gün yoğunlukla yapılmaktadır. Bununla ilgili Türkiye'de açık bir kişisel verilerin korunmasına/işlenmesinin şartlarına ilişkin yasal düzenleme bulunmamaktadır, Türkiye'de bu anlamda yasal boşluk söz konusudur. Ülkemizde verilerin işlenmesi süreçlerini kontrol edecek ve denetleyecek özel bir kurum da bulunmamaktadır.

Anayasamızın[7] 20. maddesinde yer alan, "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. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmü ile anayasal bir çerçevede kalsa da kişisel veri koruması hukukumuzda bulunmaktadır.

Bununla birlikte Türk Ceza Kanunu'nun[8] 135. maddesindeki: "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan

üç yıla kadar hapis cezası verilir." hükmü ile 136. maddesindeki: "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." hükmü dışında ayrıca yine TCK'nun "Bilişim sistemine girme" başlıklı 243. maddesine ve de "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıklı 244. maddesindeki bilişim sistemlerine karşı işlenen suçlarla ilgili hükümler çerçevesinde ülkemizde kişisel veriler korunmaya çalışılmaktadır.

Oysa ki tüm bu kanuni koruma çabalarına rağmen aslında çok esaslı bir unsur es geçilmekte ve Türkiye'de devlet ve/veya özel sektör tarafından kullanılan bilgi işlem süreçlerinin uygulamalarında sadece yan yana gelmiş rakamlardan ibaret olması ve tek başına hiç bir mahremiyet unsuru içermemesi gereken TC kimlik numarası şu an çoğunda mahrem bir bilgi olarak görülmekte ve buna göre hareket edilmektedir [9].

2.5. Çevrimiçi Davranışsal Reklamcılık: Türkiye'de Phorm Örneğinin Hukuken İncelenmesi

Türkiye'de TTNET ile gezinti.com servisi üzerinden ortaklık yaparak faaliyet yürüttüğü bilenen PHORM şirketinin faaliyetleri hakkında BTK tarafından kişisel veri ihlali yaptığına yönelik bir karar verilmiştir [10]. gezinti.com sitesine abone yapılan tüm kullanıcıların bu sistemin dışına çıkarılmaları ve bu kişilere kişisel verilerin ne şekilde, ne kadar sürede ve nasıl işleneceğine ilişkin açık ve detaylı bir şekilde bilgilendirme yapılması ve bundan sonra abonelerin/kullanıcıların üyelik yönünde açık onaylarının alınması konularında da kesin karar verilmiş ve bu ikincisinin hangi yollarla yapılacağı da gösterilmiş durumdadır. Böylelikle dijital gözetim ve bunun internetteki halinin cezalandırılabilmesinin Türkiye'de belki de ilk örneği olabilecek bir karar TTNET hakkında alınmıştır ve fakat TTNet'e 1,5 milyon TL ceza kesilmesi hakkındaki[11] bu kararın aslında karar öncesinde artan tepki ve protestoları bir şekilde örtbas etmeye yönelik olduğu anlaşılmıştır. PHORM'un Türkiye'deki faaliyeti halen sürmektedir [31].

Vatandaş Hakları Direktifi (Citizen's Rights Directive) olarak da isimlendirilen 20-09/136/EC Sayılı Direktif[32] ile 2002/58/EC Sayılı Direktif'in[33] 5/3. Maddesinde yapılan değişiklik çerçevesinde ÇDR (Çevrimiçi Davranışsal Reklamcılık) uygulamasının kişisel verilerin korunması hukuku ve mahremiyet haklarına saygı gösterilmesi açısından AB bünyesinde ne şekilde değerlendirileceği konusu tartışılmıştır. Gerek Türkiye mevzuatında yer alan hükümler gerekse AB düzenlemeleri incelendiğinde kişilerin verilerinin izlenmesi için önceden rızalarının alınması gerekliliği (opt-in) kesindir.

Bu konuda en ayrıntılı değerlendirme Madde 29 Veri Koruması Çalışma Grubu tarafından hazırlanan 22 Haziran 2010 ve 2/2010 sayılı "Çevrimiçi Davranışsal Reklam Hakkında Görüş"[34] ile ortaya konulmuştur. Madde 29 Çalışma Grubu, konu ile ilgili ilkeler belirleyerek, kullanıcının "aydınlatılmış rızasının" kapsamın tam olarak kavratılmak suretiyle alınması, kolay çıkış bir çıkış hakkı verilmesi, toplanan verilerin anonimleştirilmesinin önemi, anonimleştirilen verilerin tekrardan kullanıcı ile özdeşleştirilebilir olmasının tamamen engellenmesi, toplanılan verilerin sadece toplanma amacıyla sınırlı olması, mahremiyet tabanlı tasarım, hassas içerikli verilerin ve çocukların da bütünden ayrıca korunması konularının altını çizmiştir.

3. Teknik Boyut

Kullanıcı, internet tarayıcısı üzerinden bir web sunucusuna bağlandığında çevrimiçi takip edilme süreçleri başlar. Kullanıcı, makinesinde alacağı bazı önlemlerle takip edilmek istemediğini kendi internet tarayıcı programına ve web sitelerine bildirebilir. Alınan önlemlere rağmen, İnternet Servis Sağlayıcı firmaları tarafından veri trafiğinin izlenmesi ile mahremiyet ihlali mümkündür.

Çevrimiçi trafiğin takip edilmesi çoğunlukla ticari amaçla, yani reklam sektörü için yapılmaktadır. Kullanıcının kişisel ilgi alanlarının saptanması ve ona göre reklam gösterilmesine Çevrimiçi Davranışsal Reklamcılık (ÇDR) denmektedir. Bu amaçla kullanılan teknoloji, kişinin tüm özellikleriyle profillenmesini de

sağlayabilmektedir [12].

Çevrimiçi Mahremiyet konusunda çalışan çeşitli organizasyonlar bulunmaktadır. Electronic Frontier Founda-tion (EFF) bunların en başlıcalarından biri-sidir. EFF, çevrimiçi mahremiyeti korumak için "Do Not Track" [13] adlı bir mekanizma ve bir politika çerçevesi öngörmektedir. Kullanılan internet tarayıcısı, kullanıcı makinası hakkında birçok bilgiyi açığa çıkarmaktadır. Bu konuda ayrıntılı inceleme EFF'nin makalesinde[14] ele alınmıştır. Tekil web sitesine bağlanıldığında bile çoklu web sitesi tarafından kullanıcı hakkında bilgi toplanmaktadır. Çevrimiçi web takibini engellemek için internet tarayıcılarında alınabilecek en temel önlemleri şu şekilde sıralamak mümkündür[3]:

- İnternet tarayıcıları mahremiyet ayarları: Birçok tarayıcıda olan mahremiyet sekmesinde, Private browsing mode'u seçme ve çerez (cookie) kullanmama gibi çeşitli ayarlar yapılabilmektedir. Birçok yeni ÇDR uygulamalarında Flash programının çerezleri kullanıldığından, bu yöntemle çevrimiçi takip edilmeyi engellemek çoğunlukla mümkün değildir [15].

- İnternet tarayıcıları eklenti yazılımları: DoNotTrackMe ve Ghostery gibi eklenti yazılımların devreye alınmasıyla sitelerin bilgi toplamasını engellemek mümkündür.[29]

Web sitelerinin topladıkları verilerle ne yapacaklarını deklare etmelerini sağlayan bir protokol çalışması World Wide Web Consortium (W3C) tarafından gerçekleştirilmiştir. Mahremiyet Tercihi için Platform Projesi(P3P) [16] adı verilen bu proje/protokol, ne yazık ki fazla uygulama alanı yaratamadan askıya alınmıştır.

Kullanıcının internet trafiği, internet hizmeti aldığı Internet Servis Sağlayıcı (İSS) firmaların cihazları üzerinden yapılmaktadır. Bu firmalar, bu trafiği takip edebilecek ve engelleyebilecek sistemler kurmuş olabilirler. Kullanıcı çoğunlukla kendi seçimi olmadan "varsayılan" ayarlarından dolayı bu sistemler tarafından takip edilmektedir. Örneğin, TTNET altyapısında kurulan Phorm ile DPI (Deep Packet Inspection - Derin Veri Analizi) yapılmaktadır [12].

Günlük kullanımımızda daha fazla kriptoloji kullanarak takip edilme süreçlerini zorlaştırmak mümkündür. Bunları şu şekilde özetlemek mümkündür:

- Web trafiğini şifrelemek: İstemcinin web sunucularına HTTPS protokolü ile bağlanması ile sağlanır. Web sunucusuna bağlanırken geçerli bir sertifikanın kullanıldığı denetlenmelidir.

- DNS trafiğini şifrelemek: İstemcinin DNS sunucuların herkese açık (public) şifrelerini kullanarak DNS sorgulaması yapması ile sağlanır. İnternet servis sağlayıcılarının, DNS trafiğini kontrol altına almak için herkese açık DNS sunucularının IP adreslerine bir nevi ele geçirme (hijack) saldırısı yapabildiği [17] günümüzde, dnscrypt benzeri yazılımlar veya yurt dışı VPN sunucular kullanılabilmektedir.[30]

- Bütün internet trafiğini şifrelemek: İstemciden hedefe giden internet trafiğinin şifrelenmesi ve aradaki servis sağlayıcı firmalar ve altyapılarda bu verilerin okunamaması hedeflenir. Bir sonraki başlıkta bu kapsamda kullanılabilecek teknikler ele alınacaktır.

3.1.İnternet Trafiğini Şifreleme Teknolojileri:

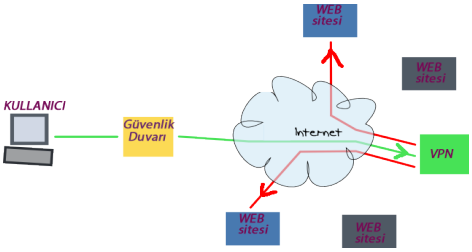
Internet trafiğini şifrelemede, anonimleştirme ve mahremiyeti korumak için çeşitli teknolojilerden söz etmek mümkündür. Tablo 1'de TOR, I2P ve VPN teknolojilerinin temel özellikleri karşılaştırmıştır [18,19]. Bunlar alt başlıklarda anlatılmıştır.

VPN (Özel Sanal Ağ):

Bu çözümde, istemci ile bu hizmeti sağlayan sunucu arasında şifrelenmiş özel bir sanal ağ (VPN) kurulur. Şifrelenmiş trafik sadece sunucuya kadardır, sunucu trafiği deşifre edip kaynak adrese yollamaktadır. Yurtdışındaki VPN sunucularının bir kısmının ücretsiz olarak bu hizmeti verdiği de hesaba katılırsa, buralardaki veri mahremiyetinin ne derecede sağlandığı şüphelidir. Bir hizmet ücretsizse; o zaman bedel siz, yani veriniz olabilmektedir. Şekil 1'de VPN altyapısı açıklanmaktadır.

The Onion Routing (TOR):

TOR projesi[20], kullanıcıların gönüllü olarak sunucularına ve makinalarına kurdukları sistemlerin oluşturduğu bağımsız bir altyapıdır. Anonimleştirme ve sansür aşma gibi konularda güvenli olduğu[22] iddia edilmektedir. TOR altyapısı, iletilen verilerin başkaları tarafından ulaşılmasını oldukça zorlaştırmaktadır [23].



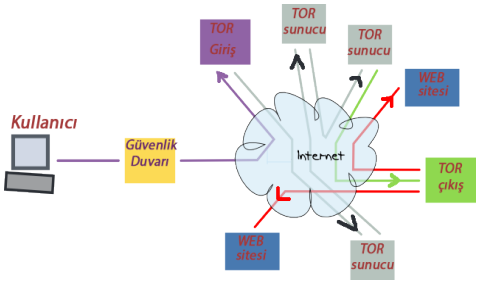
Şekil 1. VPN sistemi

TOR ağınının çalışma şeklini şu şekilde özetlemek mümkündür; Tor altyapısına giriş, bu altyapıdan çıkış ve aradaki sunucular rastsal (random) seçilir. Tor altyapısında kullanılan her sunucu gelen ve giden veri akışını şifreleyerek gönderir. Şifreli veri, rastgele seçilen başka bir sunucuya gönderilir. Bu sunucu da gelen veriyi şifreleyip başka bir sunucuya gönderir. Birkaç sunucudan sonra veri hedefe ulaşır. Sunucular rastgele olduğu, herhangi bir saldırgan giriş ve çıkış yerini saptayamadığı için saldırı gerçekleştiremez. Veri sunucular arasında çok dolaştığı için ağda belirgin bir yavaşlama söz konusudur. Şifrelemede kullanılan her gizli anahtar güvenli bir kanaldan paylaşılır. Anahtar paylaşımı için self-signed ephemeral Diffie-Hellman standardını [24] ve Transport Layer Security (TLS) standardını kullanır. Bütün iletişim bu standartlarda kurulan bu çembersel ağ üzerinden kurulur. TOR ağındaki TCP akışı 512 byte uzunluğundaki hücrelerle gerçekleşir ve ayrıca kesinti durumda ise her hücerede bulunan daha küçük payloadlar kullanılır. Bu özelliği sayesinde interactive protokolleri (SSH, vb.) destekler [13]. Şekil 2'de TOR altyapısı açıklanmaktadır.

C.Görünmeyen İnternet Projesi (I2P):

I2P gizli ve güvenli bir şekilde iletişim kurmaya yarayan ağ yönlendiricilerileri üzerinden çalışan bir internet ağıdır. Ağın giriş çıkış dahil tamamı şifreli olarak geçiş yapar. Dört tabakalı bir şifreleme kullanır ve bir çift genel anahtar (public key) kullanır. I2P grubuna herkes katılıp geliştirebilir ve tamamiyle açık kaynaktır [18]. TOR ile I2P'nin genel farkı I2P'nin şifreli bir tünel kullanmasıdır. Hız olarak TOR'dan iyi olmasının nedeni verinin çok dolaşmasına gerek kalmamasıdır. Aynı özelliklerinin başında ise ücretsiz ve açık kaynak olmasıdır.

Bu konuda çözüm olarak sunulan çeşitli teknolojilerin de kötüye kullanılabildiği bilinmektedir. Örneğin anonimliği sağlamak için kullanılan TOR altyapısında[3] çıkış yönlendiricilerinde veri toparlamaya açık olduğu gösterilmiştir [26].



Şekil 2. TOR sistemi

3.2. Büyük veri ve Tasarımla Mahremiyet

Büyük Veri (Big Data) uygulamalarında, Metadata altında toplanan birçok veri birleştirilerek bireye ait özel bilgilerden kişi profilleri oluşturulabilmektedir. Şirketler bu verilerle bireyin yapacağı tercihleri çok önceden tahmin edebilmekte ve buna göre işlemler yapmaktadır. Büyük veri; yenilik, rekabet ve verimlilik için bir sonraki sınırdır. İnovasyon amaçlı kullanımı günden güne etkinliğini artırmaktadır.

Privacy by design (PbD), Dr Ann Cavoukian tarafından geliştirilen bir kavramdır. Bu kavramın hayata geçirildiği çözümlerin özellikle büyük veride uygulanması mahremiyet için gereklidir. Örneğin, bireyin TC kimlik numarasının tamamının kullanılması yerine ilk ve sondan haneler alınarak çözümler bulunmaktadır. [27]

	TOR	I2P	VPN
Gizlenme yolu	Çembersel (Circuit)	Tünel	Tünel
Ana makine	Sunucu	Yönlendirici	Sunucu
Programlama dili	c	java	bütün diller
Maliyet	ücretsiz	ücretsiz	ücretli
Hız	yavaş	hızlı	hızlı
IP gizlemesi	çok iyi	iyi	iyi
Giriş-çıkış yeri	farklı	aynı	aynı
IP Spoofing (IP sahteciliği)	uygun değil	uygun	uygun
p2p paylaşımı	uygun değil	uygun değil	uygun

Tablo 1.TOR, I2P ve VPN teknolojilerinin temel özelliklerinin karşılaştırılması

4.Sonuç:

Tamamen bilgisayarlaşmış bir toplumda, mahremiyet ciddi bir şekilde tehlikededir ve sadece mahremiyet mevzuatı ile etkili bir şekilde korunamaz. Çevrimiçi web izleme yöntemleri ile toplanan verilerin kontrolsüz şekilde işlenmesi, bazı temel hakların ihlal edilmesine sebep olmaktadır. Kullanıcıların profilleri çıkarılarak yasal dayanağı olmayan bazı veri arşivlerinin tutulması ve fişleme amaçlı olarak da kullanılabilmesi mümkündür.

Kullanıcının bazı programlar kullanarak mahremiyetini bir dereceye kadar koruması mümkündür. Her geçen gün çıkan yeni teknolojilere kullanıcıların ayak uydurması ve yeni önlemleri öğrenip uygulaması ise kolay değildir. Mahremiyeti ön plana çıkaran yazılım ve servislerin artması gerekmektedir. Mahremiyetin gerekleri teknik olarak yerine getirilmeli ve mahremiyet, enformasyon sistemleri için bir tasarım ölçütü olmalıdır.

Aldous Huxley, "Cesur Yeni Dünya" adlı kitabında özgürlük için oluşturduğumuz teknolojilerin sonunda geri dönüp bizi baskı altında tuttuğu bir toplumu tasvir ediyordu[28]. Acquisti'nin de belirttiği üzere, "Ödenecek bedelin aşırı olmasına rağmen bağımsızlık ve özgürlük mümkündür. Bu yüzden, günümüzün belirleyici kavgalardan birinin kişisel bilgiler üzerindeki denetim için, büyük verinin gizlice bizi manipüle edecek bir güçtense özgürlük için bir güç olup olmayacağı için yapılacağına inanıyorum."[28].

İnsanların mahremiyetlerini sağlamak için teknikler öğrenmek zorunda kalmayacağı, mahremiyet hakkının yasalar ve o yasaları uygulayanlar tarafından sağlanacağı bir dünya için farkındalık yaratmak için hepimize görev düşmektedir.

Kaynaklar:

[1] Kovacs G., Tracking our online trackers, 10.6.2014 tarihinde erişildi, http://www.ted.com/talks/gary_kovacs_tracking_the_trackers

[2] What They Know, The Wall Street Journal, 10.6.2014 tarihinde erişildi, http://online.wsj.com/public/page/what-they-know-digital-privacy.html

[3] Schaumann J., Online privacy tools presentation, 10.6.2014 tarihinde erişildi, https://www.netmeister.org/slides/online-privacy-tools.pdf

[4] Av. Serhat KOÇ, "Hukuksal Bağlamda Sosyal Medya Analinizi ve Kıyaslamalı Mevzuat Önerileri", Yayınlanmamış Yüksek Lisans Tezi, s.46-50, 2013, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, http://serhatkoc.com/uploads/tez.pdf

[5] "24.10.1995 tarihli Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi (95/46/EC), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

[6] AB Veri Koruma Regülasyonu tasarı teklifi, http://ec.europa.eu/justice/data-

protection/index_en.htm
[7] TC 1982 Anayasası, http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf
[8] 5237 Sayılı Türk Ceza Kanunu, http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm
[9] Karaarslan, E., Koç S., Akın G. "Vatandaşlık Numarası Bazlı E-devlet Sistemlerinde Kişisel Veri Mahremiyeti Durum Saptaması.", Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitapçığı, 2010, http://web.itu.edu.tr/~akingok/ubhk10/Edevlet_Sistemlerinde_Veri_Guvenligi.pdf
[10] "BTK'nın 24.04.2013 tarihli ve 2013/DK-SDD/228 numaralı kararı", http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf
[11] "BTK, Phorm Soruşturmasında TTNet'e 1,5 Milyon TL Ceza Verdi", http://www.turk-internet.com/portal/yazigoster.php?yaziid=42248
[12] Kırlıdoğ M., Çevrimiçi Davranışsal Reklamcılık ve Kişisel Mahremiyet İhlalleri, Akademik Bilişim 2013, 2013
[13] Do not Track, EFF, 10.6.2014 tarihinde erişildi, https://www.eff.org/issues/do-not-track
[14] Eckersley, Peter. "How unique is your web browser?." Privacy Enhancing Technologies. Springer Berlin Heidelberg, 2010., https://panopticlick.eff.org/browser-uniqueness.pdf
[15] New Cookie Technologies: Harder to See and Remove, Widely Used to Track You, https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide
[16]Platform for Privacy Preferences (P3P) Project, 26.7.2014 tarihinde ulaşıldı, http://www.w3.org/P3P/
[17] Turkey hijacking IP addreses for popular Global DNS providers http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/
[18] A Real-World Case Study Using I2P, Michael Herrmann and Christian Grothoff Technische Universitat München, Germany
[19] In the Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2013), October 2013.
[20] Tor Project: Anonymity Online, https://www.torproject.org/
[22] Tor: The Second-Generation Onion Router, Dingledine, Roger ; Mathewson, Nick ; Syverson, Paul, 2004
[23] A. Back, I. Goldberg, and A. Shostack. Freedom systems 2.1 security issues and analysis. White paper, Zero Knowledge Systems, Inc., May 2001.
[24] W. Diffie and M. E. Hellman. New directions in cryptography.
IEEE Transactions on Information Theory, 1976
[25]Low-Cost Traffic Analysis of Tor, Steven J. Murdoch and George Danezis University of Cambridge, 2005
[26] McCoy, Damon, et al. "Shining light in dark places: Understanding the Tor network." Privacy
Enhancing Technologies. Springer Berlin Heidelberg, 2008.
[27] Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Privacy by Design
Ontario, Privacy by Design, Canada 2009
[28] Acquisti A., Why privacy matters, 10.6.2014 tarihinde erişildi, http://www.ted.com/talks/alessandro_acquisti_why_privacy_matters
[29] Ghostery, https://www.ghostery.com
[30] Dnscrypt, http://dnscrypt.org/
[31] Efe Kerem Sözeri, İnternetSitelerindeki Gizli Kod Bizi Fişliyor mu?, http://www.bianet.org/biamag/insan-haklari/158044-internet-sitelerindeki-gizli-kod-bizi-fisliyor-mu
[32] 2009/136/EC Sayılı AB Direktif, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF
[33] 2002/58/EC Sayılı Direktif, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
[34] Madde 29 Veri Koruması Çalışma Grubu, 22 Haziran 2010 tarihli, 2/2010 sayılı, "Çevrimiçi Davranışsal Reklam Hakkında Görüş", http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf