The EDRi papers
6.SAYI

VERİ KORUMAYA GİRİŞ

alternatif bilişim

EUROPEAN DIGITAL RIGHTS

EUROPEAN
DIGITAL
RIGHTS

EDRI.ORG/PAPERS

Çeviri
Hatice Balkanlar

Yayınlayan
Alternatif Bilişim Derneği
Eğitim Mah. Ömerbey Sok.
Keskin Hancı İş Merkezi
No.19/B 34722 Kadıköy İstanbul
+90 216 418 0 417
bilgi@alternatifbilisim.org

Orjinal Broşür

Hazırlayanlar:
EDRI üyeleri ve gözlemciler

Düzelti:
EDRI ve Digital Courage (Almanya)

Tasarım: CtrlSPATE

Fotoğraf: Marnix Petersen

European Digital Rights
20 Rue Belliard1010 Brüksel
Tel: +32 (0) 2 274 25 70
brussels@edri.org

European Digital Rights (EDRI), 20 ayrı ülkeden dijital medyada gizlilik ve dijital sivil haklar savunuculuğu yapan 30 ayrı derneğin oluşturduğu bir birliktir.

SUNUŞ

Bütün dünyada ve Türkiye'de kişisel verilerin korunması konusunda duyarlılık artıyor. Milyarlarca insanı buluşturan İnternet ve yolaçtığı değişim sayesinde her gün devasa büyüklükte veri toplanıyor, işleniyor ve saklanıyor. Önemli bir bölümünün kişisel hassas verilerimiz olduğu aşikar. Bunların özenle korunması, belki de hiç toplanmaması gerekmekte.

Fakat başta kâr odaklı düşünen ticari kuruluşlar ve yurttaşları hakkında daha fazlasını bilmek isteyen devletler gelmek üzere birçok kişi ve kurum, hiçbir yasal düzenleme veya etik ilke olmadan bilgilerimizi toplamakta, işlemekte, kötüye kullanmakta, ticari bir meta gibi satmakta, fişleme yapmaktadır.

Yasal düzenlemelerin ve çeşitli etik ilkelerin olmayışı önemli bir eksikliktir. Öte taraftan, kişisel veri konusundaki genel farkındalık sorunu da can yakıcı düzeydedir. Çoklarınca kişisel veri ve gizlilik (mahremiyet) evmizin ya da yatak odamız duvarları ile sınırlıdır. Sosyal ve kültürel temelleri oldukça derin bu sınırlılık, problemi katmerleştirmektedir. Evin duvarları arasında gösterilen hassasiyetin, tüm yaşam alanlarında da gösterilmesi için farkındalık ön koşuldur. Bu durumun değiştirilmesi ise yasal düzenlemeler yapmaktan çok daha zor.

Elinizdeki broşür bu farkındalığın artmasına yardım etmeyi hedeflemektedir. Kişisel veri ve mahremiyet konusunda referans alınacak bir metindir. Broşür içeriği EDRI* üyeleri tarafından hazırlanmıştır. EDRI tarafından İngilizce yayınlanan bu broşürü Türkçeye kazandırmaktan büyük mutluluk duyuyoruz.

Broşürün çevirisi için Hatice Balkanlar'a, LaTeX yerleşimi için Işık Barış Fidaner ve Uğurcan Ergün'e, kapağın Türkçe düzenlenmesi için Barış Büyükakyol'a, düzeltiler için Mutlu Binark ve İlden Dirini'ye, broşür baskı giderleri için Friedrich-Ebert-Stiftung Vakfı'na teşekkür ederiz.

Bizi gözetim toplumuna doğru götüren gelişmelere karşı, yurttaş farkındalığının artmasına katkı sunması dileği ile...

Alternatif Bilişim Derneği

*: EDRI (European Digital Rights / Avrupa Dijital Haklar Örgütü) 20 farklı Avrupa ülkesinden, 32 kişisel gizlilik ve insan hakları temalı kuruluşun üyesi olduğu bir birliktir. Alternatif Bilişim Derneği EDRI'nin gözlemci üyelerindendir. http://www.edri.org/

EDRI SUNUŞ

Bu kitapçık dijital ortamda veri korumaya ilişkin temel konular ve jargon hakkında genel bir bakış sunma amacıyla hazırlanmıştır.

Veri koruma, özü itibariyle Avrupa Birliği Temel Haklar Şartı, Avrupa Konseyi Sözleşmesi-108 ve diğer uluslararası anlaşmalar ve ulusal anayasalarda karşılığı olan temel bir hakkı koruma ile ilgilidir.

Vatandaşlara ait verilerin işlenmesi ve yeniden kullanımı ekonomik açıdan bakıldığında da giderek önemli bir konu olmaktadır. Bu temel hakkın kanuni yollardan korunmasına engel olmak için yasal çerçevenin değiştirilmesine ve bu hakkın zayıflatılmasına yönelik baskılar söz konusudur.

Bu belgenin tartışmalara olumlu bir katkı sağlamasını, gözden geçirme süreci ile birlikte içinde bulunduğumuz dijital çağda gizliliğin öngörülebilir ve orantılı bir koruma ile garanti altına alınmasını ve Avrupa Birliği'nin bu konudaki küresel liderliğinin daha da güçlendirilmesini umut ediyoruz.

İÇİNDEKİLER

KİŞİSEL VERİLER

NELERDİR? NİÇİN ÖNEMSEMELİYİZ?

Gizlilik ve kişisel verilerin korunması konularına son zamanlarda haberlerde, özellikle sosyal iletişim ağları, çevrimiçi reklam şirketleri tarafından yürütülen müşteri profili çalışmaları ve bulut bilişim (bu kitapçıkta bu konulara ayrıntılı olarak değinilmektedir) kapsamında sıklıkla yer verilmektedir. Ancak bir adım sonrasına geçmeden önce ne tür verilerin kişisel veri olarak değerlendirilebileceğini anlamak gerekir.

Kişisel veri, genel hatlarıyla bir bireyin şahsen tespit edilmesini veya bir kişinin bir birey olarak diğerlerinden ayırt edilmesini sağlayan her türlü bilgi (tek bir bilgi veya birbiri ile alakalı bilgiler olabilir) demektir. Kişinin adı, adresi, ulusal kimlik numarası, doğum tarihi veya fotoğrafı kişisel verilere verilebilecek en bariz örneklerdir. Kişinin aracı varsa, bu aracın tescil numarası, kredi kartı numaraları, parmak izleri, IP adresi (web sunucu gibi bir cihazdan ziyade bir kişi tarafından kullanılıyorsa) veya sağlık raporları da kişisel verilere verilebilecek örneklerdendir.

Kişisel verilerin bireyleri doğrudan doğruya tespit etmek için kullanılan tek veri olmadığına dikkat etmek gerekir. Kişinin adı veya kendisine ait birkaç parça bilgi o kişiyi diğerlerinden ayırt etmek için yeterli olabilir. Bununla

Hazırlayan: Digitale Gesellschaft, Almanya
http://digitalegesellschaft.de

birlikte, bir kişinin sanal ortamdaki davranışlarını takip etmek, o kişinin profilini çıkarmak ve o kişiye uygun teklifleri sunmak isteyen çevrimiçi reklam şirketleri bazı izleme teknikleri ile

“Sayısı giderek artan verilerin önümüzdeki yıllarda içinde yaşadığımız dünyayı bugün tahayyül edemeyeceğimiz şekilde değiştireceği konusunda çok az şüphe var.”

o kişiyi diğerlerinden ayıracak özgün bir belirteç kullanır. Bu reklam şirketinin söz konusu kişinin kim olduğunu bilmesine gerek yoktur. Bu şirketler için 12345678 numaralı kullanıcının bazı web sitelerini sürekli olarak ziyaret ettiğini, bazı web sitelerini “beğen”diğini bilmek yeterlidir. Bu durumlarda, kişinin internetteki arama geçmişi, “beğen”diği web siteleri gibi bilgiler de özgün bir belirteç olarak kişisel veri kapsamına girebilir.

“Uzun vadede şirketlerin yanı sıra vatandaşlar ve demokratik kuruluşlar da güçlü korumalardan faydalanabilecektir.”

Veri miktarının muazzam bir şekilde arttığı göz önünde bulundurulursa (bu kitapçıkta bu olay Büyük Veri olarak tanımlanmaktadır), verilerin önümüzdeki yıllarda içinde yaşadığımız dünyayı bugün tahayyül edemeyeceğimiz şekilde değiştireceği konusunda çok az şüphe duyarız. Güvenilir verilerin işlenmesi bazı trendlerin keşfedilmesini sağlamanın yanı sıra kaynak israfının önüne geçilmesine ve politika oluşturma süreçlerinin iyileştirilmesine katkıda bulunur.

Bununla birlikte, veriler kişilerin tam bir gözetim altında tutulmasını sağlamak amacıyla da kullanılabilir ve bu da temel hakların ihlali anlamına gelir. Birbiri ile bağlantı halindeki elektronik bir dünyada verileri birbirinden bağımsız ve ayrı ele almak mümkün değildir. Verilerin uzun süreli olarak kaydedilebildiği dikkate alınacak olursa, genç bir kullanıcı olarak bugün sergilediğiniz çevirimiçi davranışların yarın kariyerinize etki etme olasılığı söz konusudur. Vatandaşlar kamu yetkilileri ve özel kurumlar tarafından devamlı “izlendiklerinin” farkındadır ve bu konudaki bilinçleri giderek artmaktadır. Özellikle veri toplama işinin gözle görülür bir şekilde yapılmıyor olması vatandaşların kamu yetkililerine de özel kurumlara da güvenini sarsmaktadır. Giderek artan bu güven eksikliği de demokrasimize ve iş dünyasına zarar vermektedir.

Bu nedenle veri koruma çok önemli bir husustur. Vatandaşların ve tüketicilerin ülke idaresine, iş dünyasına ve diğer özel kurumlara güvenebilmesi için korumanın sağlanması gerekir. Eğer günümüz dünyasında veriler yeni bir para birimi gibi değerli ise bizim de bankacılık sektörünün yaşadıklarından ders çıkarmamız gerekir. Regülasyonun zayıf olması ve her şeyin oluruna bırakılması sektöre olan güvenin sarsılmasına neden olur ve bu durum her bir vatandaşı olumsuz etkiler.

Her ne kadar anlaşılır olsa da kısa vadeli iş çıkarlarından ziyade, veri toplama, işleme ve paylaşımı konularında değeri temel olan bir dizi Avrupa normu ve prensini oluşturma doğrultusunda güçlü ve akıllıca bir yaklaşım sergilemek gereklidir. Nitekim böyle bir yaklaşım en nihayetinde kaçınılmaz olacaktır. Uzun vadede yalnızca şirketler değil vatandaşlar ve demokratik kuruluşlar da veri toplama, işleme ve paylaşımında güçlü korumaların faydasını görecektir. ■

ANONİMLEŞTİRME

SİZ BİR SAYI DEĞİLSİNİZ

İnternet'te dolaştığımız veya başka ağlar üzerinden veri gönderdiğimiz her an elektronik iz bırakırız. Bu izler bizi ve bizim iletişim halinde olduğumuz insanları tespit etmek için kullanılabilir. Anonimleştirme, bir kişinin doğrudan veya dolaylı tespit edilmesini sağlayacak elektronik izlerden ilgili bilginin kaldırılması veya karartılması anlamına gelir.

Anonimleştirmenin en büyük avantajlarından biri, normal koşullarda gizlilik kaygısı sebebiyle yapılamayacak olan bir araştırmaya imkân tanımasıdır. Örneğin, herkesin tıbbi kaydı kullanılabilse hastalık takipleri kolaylaşır ve bu da sağlık sektöründe iyileşmeye olanak verir. Ancak, bu insanların gizliliğinin ihlal edilmesi anlamına da gelir. Bu meseleye çözüm olarak isim, doğum tarihi ve adres gibi doğrudan belirteçlerin kaldırılması önerilmektedir, böylelikle verilerin bireye kadar indirgenemeyeceği iddia edilmektedir. Hükümetler, ilgili sektörler ve araştırmacılar kişisel verilerin etkili bir şekilde anonimleştirilmesinin mümkün olduğunu ve etkin bir anonimleştirmenin bireyin gizliliğini korurken toplumun zengin veri kaynaklarına erişimini kolaylaştıracağını ileri sürmektedir.

Hazırlayan: Foundation for Information Policy Research, İngiltere. http://fipr.org

Ne yazık ki bilim insanlarının da uzun süre önce ortaya koyduğu gibi, durum bu kadar basit değildir. Örneğin 1997 yılında araştırmacılar, üzerinde yalnızca posta

"Anonimleştirme, bir kişinin doğrudan veya dolaylı tespit edilmesini sağlayacak elektronik izlerden ilgili bilginin kaldırılması veya karartılması anlamına gelir."

kodu ve doğum tarihi bilgisi olan tıbbi kayıtları inceleyerek bireyleri tek tek tespit etmeyi başarabilmiştir. 2006'da yapılan bir çalışma Netflix (çevrimiçi video kiralama sitesi) üzerinde bir kullanıcının yalnızca 6 filme oy vermesinin Netflix kullanıcılarının %99'unu tespit etmeye yettiğini göstermiştir.

Bu nasıl mümkün oluyor? Meselenin aslı şu: Bir dizi veri arasından kişilere ilişkin doğrudan belirteçlerin (isim, adres,

“Meselenin aslı şu: Bir dizi veri arasından kişilere ilişkin doğrudan belirteçlerin (isim, adres, ulusal kimlik numarası, doğum tarihi) ortadan kaldırılması ile etkin anonimleştirme yapılamıyor. Burada önemli olan ölçü “anonimlik setinin” büyüklüğüdür. Diğer bir ifade ile verinin ilgili olabileceği bireylerin ne büyüklükte bir set oluşturduğu önem taşıyor.”

ulusal kimlik numarası, doğum tarihi) ortadan kaldırılması ile etkin anonimleştirme yapılamıyor. Burada önemli olan ölçü “anonimlik setinin” büyüklüğüdür. Diğer bir ifade ile verinin ilgili olabileceği bireylerin ne büyüklükte bir set oluşturduğu önem taşıyor. Örneğin siz bir “adam” olarak tanımlanıyorsanız, anonimlik setinin büyüklüğü üç buçuk milyardır. Ancak “orta yaşlı, Danimarkalı, sakallı bir adam” olarak tanımlanıyorsanız, anomimlik setinin büyüklüğü yarım milyonu bulabilir. “Cambridge yakınlarında yaşayan, orta yaşlı, Danimarkalı, sakallı bir adam” olarak tanımlanırsanız bu büyüklük üç veya dört ile ifade edilebilir.

Takma isim vermek (örneğin John Smith, 1 High Street olarak bilinen bir kullanıcıya 45684231 takma adını vermek) verilen takma ismin ne kadar iyi şifrelenebildiğinden bağımsız olarak sorunu çözmeye yetmez. Farz edelim ki dünyada yaşayan herkese başka numaralarla bir kimlik kartı verdik. Ne olacak? Bir ilaç reçetesinde ilk takma ismi deniyoruz diyelim: “45684231 no’lu insan 3 Şubat 2009’da penisilin aldı”. Burada anonimlik setinin büyüklüğü yedi milyardan birkaç yüz bine doğru daralır. İkinci bir ilaç reçetesi vakası olsun: 3.265.679.016 no’lu insan 14 Mayıs 2009’da kodein aldı”. Bu sefer, anonim seti birkaç yüze hatta birkaç düzineye düşer. Birkaç vaka sonrasında da söz konusu bireyi tek başına tespit etmek mümkün olacaktır.

Giderek artan sayılarda “Büyük Veri”nin ortaya çıkması ile, herhangi bir “anonimleştirilmiş” veri seti arasında bir kişiyi tespit etme olasılığı artmaktadır, çünkü başka veri setleri arasından veri kullanma olasılığı artmaktadır. Mevcut ve öngörebildiğimiz gelecekteki teknolojiye dayanarak, kimliklerin aktif bir aramaya tabi tutulduğu durumlarda anonimleştirmenin işe yaramayacağını söylemek doğru olur. Burada şimdiye kadar pek önemsenmeyen “Büyük Veri” konusuna ilişkin önemli tehditler söz konusudur.

Gördüğümüz gibi anonimleştirmenin tamamen güvenli bir yol olduğunu söyleyemeyiz. Bu bağlamda, kullanılan teknolojilerde şeffaflık, güvenlik mühendisleri tarafından yapılan açık eş düzey denetimler ve gerekli sorumluluğu içinde barındıran teşhir işlemleri en azından erken uyarı yapılmasını sağlayacak ve standartları yükseltecektir. ■

AMACIN SINIRLANDIRILMASI İLKESİ

SADECE BELİRTİLEN AMAÇ İÇİN KULLANINIZ

Bir internet kullanıcısı internetten bir ürün satın aldığı zaman, ürünü satın aldığı şirkete, ilgili web sitesine ve o web sitesini kullanmasına izin veren internet sağlayıcısına kişisel bilgilerini verir. Bu verileri kullanan kuruluşlara " veri kontrolörleri" denir. Veri kontrolörleri ellerindeki verileri veri koruma kanuna göre kullanır. Bu kanun, veriler kim ile paylaşılırsa paylaşılsın ilgili bütün taraflar nezdinde kişisel verilerin korunmasını gerektiren bazı temel ilkelere dayanmaktadır.

Bu ilkelerden en önemli olanı amacın sınırlandırılması ilkesidir. Amacın sınırlandırılması ilkesine göre veri kontrolörleri kişisel verileri yalnızca belli bir amaç için toplayabilir ve kullanabilir. Bu amacın ne olduğu düzgün bir şekilde tanımlanmalı ve verisi işlenecek olan şahsa (veri öznesi) açık bir şekilde bildirilmelidir. Veri öznesi ancak bu şekilde kendisine ait veriye ne olacağını öğrenebilir. Veri kontrolörleri bazı koşullarda ellerindeki kişisel verileri ilk başta belirtilen amaç dışında kullanabilirler. Örneğin, çevrimiçi bir ürün satın aldığınızda, ürünü satın aldığınız şirket siz karşı çıkmadığınız sürece size pazarlama mesajları iletebilmek için kişisel bilgilerinizi bir dosyada saklı tutabilir. Siz kişisel bilgilerinizi yalnızca söz konusu ürünü satın alabilmek için paylaşmış dahi olsanız, şirket sizinle daha iyi bir iletişim kurabilmek için satın alma geçmişinize ilişkin bilgileri de saklayabilir. Yasalara göre kişisel veriler ilk başta belirtilen amaç haricinde kullanılamaz. Buradan şu anlam çıkar: Bazı veri kullanımlarında sınır yoktur. Yani bilgilerinizi paylaştığınız bir şirket sizin bilgilerinizi başka bir şirkete veya kuruma satabilir (izniniz olmadan) veya başka kaynaklardan alınan bilgilerinizle elindeki bilgileri birleştirerek profilinizi çıkarabilir.

Hazırlayan: Bits of Freedom, Hollanda
http://bof.nl

Amaç sınırlandırılması ilkesi olmazsa veri kontrolörleri ilk başta belli bir amaç için bilgilerinizi toplar ve sonrasında başka amaçlarla kullanmaya devam eder. Bu nedenle, bu ilke gizliliğin korunması anlamında önemli bir dayanaktır. Bu ilke ile bir bilgi veri kontrolörü tarafından toplandığı zaman o bilginin ne kadar koruma altına alındığı belirlenir. Bu ilkenin zayıflatılması kullanıcıların gizliliğine bir darbe vurulması demektir. ■

"Kişisel verilerin işletilebilmesi için gerekli altı yasal dayanaktan biri de rızadır."

VERİ İŞLEMEYE RAZI OLMAK

İZNİNİZLE

Hazırlayan: Bits of Freedom, Hollanda
http://bof.nl

Bir veri kontrolörünün kullanıcılara ait kişisel verileri işleyebilmesi için kullanıcıların rıza göstermesi gerekir. Kişisel verilerin işlenebilmesi için gerekli olan altı temel hukuki şarttan biri kullanıcının rızasıdır. Veri işleme için gerekli olan diğer hukuki şartlar sözleşmeden doğan yükümlülüklerin yerine getirilmesi veya yasalara uyum sağlanması zorunluluğudur. Veri işlemeye gösterilen rızanın geçerlilik kazanabilmesi için bazı gerekliliklerin karşılanması gerekir.

İlk olarak, rızanın açık olarak belirtilmesi gerekir. Kişinin göstereceği rızayı genel kullanım koşulları arasına sıkıştırmak, kullanıcıdan hiçbir ilave bilgi temin etmeden sadece "Kabul Ediyorum" seçeneğini tıklamasını beklemek yeterli değildir. Kullanıcıların daha önceden işaretlenmiş olan kutulardaki işaretleri kaldırmasını beklemek de rızanın alındığını gösteren geçerli bir yöntem değildir.

İkinci olarak, rızanın özgül bir durumda gerekli bilgiler temin edildikten sonra alınması gerekir. Bu, kullanıcıların veri işlemeye başlanmadan önce rıza gösterecekleri şey konusunda ayrıntılı olarak bilgilendirilmesi gerektiği anlamına gelir. Veri işlemenin amacı açıkça belirtilmeli ve kullanıcılar kendilerine ait verilerden hangilerinin işleme alındığı konusunda aydınlatılmalıdır. Kullanıcılar ayrıca veri işlemenin sonuçlarını ve kendilerine ait verilerin işlenmesinin ileride ne gibi sonuçlar doğurabileceğini anlamalıdır. Kullanıcılara verilen bilgiler çoğunlukla bu koşulları karşılamaz. Veri işleme ekseriyetle karmaşık bir süreçtir ve

"Özetle, bir rızanın geçerli olabilmesi için anlamlı olması, kullanıcının özgür iradesine dayanması, kullanıcının spesifik olarak bilgilendirilmesini takiben alınmış olması ve açık bir şekilde dile getirilmesi gerekir."

“Veri işlemenin amacı açıkça belirtilmeli ve kullanıcılar kendilerine ait verilerden hangilerinin işleme alındığı konusunda aydınlatılmalıdır. Kullanıcılar ayrıca veri işlemenin sonuçlarını ve kendilerine ait verilerin işlenmesinin ileride ne gibi sonuçlar doğurabileceğini anlamalıdır.”

verilerin kombine edilmesini ve kullanılmasını içerir. Veri işlemenin ileride ne sonuçlar doğuracağı da bilinmez.

Bu nedenle, veri işleme konusunda bilgilerin kanunlara uygun bir şekilde verilmesi gerekir.

Son olarak, kullanıcılar rıza gösterirken özgür iradelerini kullanmalıdır. Bu kriter kullanıcının veri işlemeye rıza gösterip göstermeme konusunda gerçekten bir seçim hakkı olması gerektiği anlamına gelir. Oysa kullanıcı ile veri kontrolörü arasında bu kriterin uygulanabilmesini sağlamak için gerekli olan denge her zaman kurulamayabilir. Bir çalışan ile işverenleri arasındaki ilişki dengeli bir örnek olabilir, ancak veri kontrolörünün büyük bir piyasa gücü varsa veya veri kontrolörü hiç kimsenin sunmadığı bir hizmeti sunuyorsa dengeden bahsedilemez.

Özetle, bir rızanın geçerli olabilmesi için anlamlı olması, kullanıcının özgür iradesine dayanması, kullanıcının spesifik olarak bilgilendirilmesini takiben alınmış olması ve açık bir şekilde dile getirilmesi gerekir. Bu koşullar geçerli olduğu sürece, kullanıcılar rıza gösterebilir. ■

BÜYÜK VERİLER

ENDÜSTRİYEL HAM MADDE

Hazırlayan: Privacy International, İngiltere
http://privacyinternational.org

"Büyük Veri" çok büyük ve karmaşık veri tabanlarını tanımlamak için kullanılan yaygın bir terimdir. Büyük Veri, tek bir sunucu veya masaüstü bilgisayarda yürütülen geleneksel "yerel" tekniklerle yönetilemeyen veya analiz edilemeyen ve milyonlarca kaynaktan gelen veri kitlelerini (bir arama motorunun deposundan, internet araştırmalarından, Wikipedia'nın veri tabanından alınan veriler gibi) ifade etmek için kullanılır.

Veri işleme gücünün durmaksızın geliştirilmesi ve veri analizine yönelik yeni tekniklerin ortaya çıkarılması, "Büyük Veri"nin sayısız pek çok kaynak kullanılarak yaratılabileceğini ve başka koşullarda gözden kaçabilecek olan yönelimlerinin ve özelliklerin keşfedilmesi amacıyla geliştirilebileceğini gösterir. Örneğin milyonlarca telefon görüşmesi içinden "iletişim verisini" alıp analiz ederek iletişimin doğası, kullanıcılar arası ilişkiler ve tüketicilerin davranışlarına ilişkin bir sürü faktörün kombinasyonunu elde etmek mümkündür.

Büyük Veri uygulaması ile daha önce aşikâr olmayan veya kaynak bilgi içerisinde gösterilmeyen veriler konusunda bilgi toplanabilir. Örneğin tıbbi bir araştırmada, sağlık sektöründen hizmet alan bir kişi başkalarıyla olan genetik ilişkisinin ortaya çıkarılması gibi bir amaç gütmeyebilir, ancak Büyük Veri'nin sunduğu bağlantılarla bu bilgiye ulaşılabilir. Büyük Veri ile farklı veriler arasında bağlantılar kurulabilir. Bu tekniğin en güçlü tarafı artık exabit[1] olarak ölçülen verilerin kullanılmasına izin vermesidir. Bu ölçeklerde verilerin işlenmesi için binlerce sunucuya ihtiyaç duyulur.

The Gartner Group Büyük Veri kavramını "karar verme süreçlerini iyileştirebilmek için ihtiyaç duyulan yeni veri işleme formlarının kullanılmasını gerektiren yüksek hacimli, yüksek hızlı ve/veya çok çeşitli bilgi varlıkları toplamı" olarak açıklar. Büyük Veri kavramına farklı kaynaklardan alınan sıradan bilgi kitleleri arasında saklı olan bilgilerin çıkarılması için daha önce eşi görülmemiş bir veri işleme yeteneğinin uygulamaya geçirilmesi olarak da bakılabilir.

Bu teknik, şirketler ve hükümetler için giderek daha da değerli bir hal almaktadır. Örneğin Walmart saat başı 1 milyon müşteri işlemi gerçekleştirmekte. Bu işlemler 2.5 petabit[2] büyüklüğünde (ABD Kongre Kütüphanesi'nde bulunan bütün kitapların içinde yer alan bilgilerin 167 kat fazlası) veriler içerdiği tahmin edilen veri tabanına aktarılmaktadır. Bu bilgiler ayrıntılı analizlere tabi tutularak, kullanıcıların davranış trendlerinin ortaya konmasında ve akla hayale gelmeyecek kadar detaylı düzeyde ayrıntılı bir tüketici profili oluşturmakta kullanılabilir. ■

1: Bir exabit 10 18 bite tekabül etmektedir. Bilgisayar kullanıcıları megabit ve gigabit terimlerine aşinadır. Exabit, bir milyar gigabit demektir.

2: Bir petabit 10 15 bit, yani bir milyon gigabittir.

VERİ GÜVENLİĞİ VE VERİ İHLALLERİ

DİKKATLİ DAVRANINIZ

Bilgisayar sistemlerinin kişisel verileri kaydetme ve işleme kapasitesi son yıllarda sürekli olarak artmaktadır. Bilgisayar sistemleri bünyesinde yer alan kişisel veriler öyle büyük bir ölçeğe ulaşmıştır ki kavrayabilmek neredeyse imkânsızdır.

Aslında, genel olarak kabul edilen görüşe göre herhangi bir bireye ilişkin olarak kaydedilen bilgilerin denetimini sağlamak artık mümkün değildir. On sene önce İngiliz gazetesi The Guardian bu konu ile ilgili bir araştırma yürüttü. Bu araştırmanın sonunda şu ortaya çıkarıldı: "gelişmiş bir ülkede yaşayan ve ekonomik olarak aktif olan ortalama bir yetişkine ait veriler 700 büyük veritabanında yer almaktadır".[3]

On sene öncesine kıyasla bilgisayar sistemleri dahilinde tutulan kişisel veri miktarı muazzam bir ölçüde artmıştır. Bunun sebebi yalnızca teknik alanda kaydedilen ilerlemeler değil çevrimiçi sosyal paylaşım ağları ve Web 2 gibi kullanıcı tabanlı sistemlerin ortaya çıkmasıdır.

3: The Guardian Private virtue
http://www.guardian.co.uk/uk/2002/sep/07/privacy2

Hazırlayan: Privacy International, İngiltere
http://privacyinternational.org

Kişisel veri kitleleri büyüyerek bulut bilişim ve Büyük Veri gibi yeni veri işleme ortamlarına doğru geçiş yaptıkça, güvenlik tehditleri de çoğalmaktadır. Güvenlik önlemlerini sıkılaştırmak ve standart hale getirmek için çok büyük çalışmalar yapılsa da kişisel verileri ellerinde tutan tüm kurum ve kuruluşlar için tehlike devam etmektedir.

"gelişmiş bir ülkede yaşayan ve ekonomik olarak aktif olan ortalama bir yetişkine ait veriler 700 büyük veritabanında yer almaktadır."

Bu tehlikenin yarattığı gerginlik, büyük ve karmaşık bilgi sistemleri ile eski ve daha istikrarsız bilgi teknikleri (USB ve diz üstü bilgisayarlar gibi) bir araya geldiğinde daha da çok hissedilmektedir.

“Privacy Rights Clearing House’a göre ABD’de Ocak 2005-Mayıs 2008 döneminde, hassas kişisel veriler içeren toplam 227.052.199 bireysel kayıtta güvenlik ihlalleri gerçekleşmiştir.”

Neredeyse bütün büyük kuruluşlar bu güvenlik sorununu bazen talihsiz sonuçlar eşliğinde yaşamaktadır. Privacy Rights Clearing House’a göre ABD’de Ocak 2005-Mayıs 2008 döneminde, hassas kişisel veriler içeren toplam 227.052.199 bireysel kayıtta güvenlik ihlalleri gerçekleşmiştir.

Birleşik Krallık’ta da durum endişe vericidir. Birleşik Krallık’a bağlı Information Commissioner’s Office tarafından verilen rakamlara göre son beş senede yerel hükümete ait verilerde sızıntı vakaları % 1609 artmıştır. Diğer kamu kuruluşları ise bu vakalarda %1380 artış olduğuna işaret etmektedir. Özel kurumlar ise veri sızıntılarında % 1159 artış olduğunu belirtmektedir.

Veri sızdırma vakalarının belki de en bilineni 2007 senesinde yaşanmıştır. Her Majesty’s Revenue and Customs (HMRC) tarafından saklanan ve çocuk yardımı talebinde bulunan ailelerin bilgilerinin kayıtlı olduğu CD’ler kaybolmuştur. Independent Police Complaints Commission, verilerin HRMC tarafından tutulmasını uygunsuz olarak nitelendirilmiş ve çalışanların da ortalığı bulandırdığını ileri sürmüştür. Bu veri sızıntısından yirmi beş milyon insan etkilenmiştir. ■

TERCİHE GÖRE VERİ KORUMA VE VARSAYILAN VERİ KORUMA

GİZLİLİK İLKESİNE GÖRE TASARLANMIŞTIR

Giderek büyüyen internet ekonomisinin önünü açabilmek için kullanıcıların çevrimiçi sunulan hizmetlere güven duymasını sağlamak gerekir. Bu, tüketicilerin şirketlere kullandıkları hizmet için gerekenden daha fazla bilgi verdiklerini düşünerek endişelenmemesi gerektiği anlamına gelir. Gereksiz olarak kaydedilen her türlü bilgi bir risk teşkil eder.

Bu yüzden, ürün ve hizmetlerin tasarımı ve uygulanmasında gizliliğin korunmasına yönelik önlemlerin alınması giderek daha fazla önem kazanmaktadır. Bu, Avrupa Birliği Veri Koruma Yönetmeliği'nin 23. Maddesi'nde tercihe göre veri koruma ve varsayılan veri koruma terimleri ile açıklanmaktadır. Bu yaklaşımın temelinde kullanıcılara kişisel verileri üzerinde daha fazla kontrol hakkı vermek yatmaktadır.

Tercihe göre veri koruma, veri kontrolörlerinin – şirketler veya kamu kuruluşları- gizliliğin korunması

Hazırlayan: Access International
http://accessnow.org

konusunda olumlu bir yaklaşım içerisinde olduğunu göstermektedir. Tasarıma göre veri koruma yöntemini tercih eden veri kontrolörleri bu yöntemi hem teknolojilerine (örneğin bilgisayar çipleri gibi donanımlar ve sosyal paylaşım ağı platformları gibi hizmetler) hem de kurumsal politikalarına (örneğin gizlilik etki değerlendirmelerinin tamamlanması) entegre eder. Bu yöntem, herhangi bir ürün veya hizmeti

"Kullanıcılar hangi gizlilik ayarını seçerse seçsin yüksek düzeyde koruma garantisi altındadır."

geliştirmeye başlarken gizlilik ve veri koruma konularına öncelik vermeyi gerektirir. Bu tür önlemler en başından

“Kullanıcılar ne kadar bilgiyi paylaşacaklarına kendileri karar verir, servis sağlayıcı bu karara karışmaz, buradaki kilit nokta kullanıcıların kontrolü elinde tutmasıdır.”

alınırsa, gizlilik haklarının ihlallerinin önüne geçilebilir, bu tür hak ihlallerinin hem vatandaşlar hem de şirketler nezdinde yaratabileceği hasar engellenebilir.

Bu yaklaşımın odak noktası varsayılan, yani hizmetin/ürünün içinde en başından beri yer alan gizlilik özelliğidir. Bu şu anlama gelir: Bir kullanıcı bir ürün veya hizmet satın aldığında gizlilik ayarları mümkün olduğunca sıkı bir şekilde yapılmış olur. Kullanıcının bu ayarları değiştirmesine gerek kalmaz. Bu sayede, herkes yüksek düzeyde koruma garantisi altındadır. Üstelik kullanıcılar hizmet sağlayıcısının sunduğu gizlilik ayarları yerine kendi istedikleri gizlilik ayarını seçtiklerinde de aynı korumadan faydalanabilir. Servis sağlayıcılarının kullanıcıları gizlilik ayarlarını değiştirebilecekleri kullanıcı dostu uygulamalarla desteklemesi gerekir. Ayrıca veri işleme uygulamaları konusunda şeffaf olmaları ve anlaşılır gizlilik politikaları sunmaları beklenir.

Bu kavramların sosyal paylaşım ağları gibi bazı servisler için geçerli olmayacağını düşünenler olabilir. Fakat, varsayılan ayarların gizliliği destekleyecek şekilde konfigüre edilmesi zor değildir. Örneğin, bir sosyal paylaşım ağına katıldığınızda, ilk baştaki ayarlar bilgilerinizin sadece sizi tanıyanlar tarafından görüntülenmesini ve tanımadığınız kişilerin erişimine kapalı olmasını sağlayacak şekilde yapılabilir. Varsayılan gizlilik ayarları bazı sosyal paylaşım ağlarında zaten uygulanmaktadır, dolayısıyla bu fikir ne yenidir ne de devrim niteliğindedir. Paylaşmak illa ki gizliliğe son vermek anlamına gelmez. Aslında, tercihe göre ve varsayılan gizlilik ayarları etkin bir şekilde uygulandığı zaman hem paylaşımda bulunabilirsiniz hem de gizliliğinizi koruyabilirsiniz. Burada önemli olan kullanıcıların ne kadar bilgi paylaşacaklarına kendilerinin karar vermesi ve bu karara servis sağlayıcısının karışmıyor olmasıdır. Tercihler ve varsayılan gizlilik ayarları, kullanıcıların kendi bilgilerinin sorumluluğunu almasını sağlar, isterlerse varsayılan ayarları kabul ederler isterlerse kendileri tercih ettikleri gizlilik ayarını seçerler. ■

SOSYAL PAYLAŞIM SİTELERİNDE GİZLİLİK VE VERİ KORUMA

PAYLAŞIRKEN DİKKATLİ OLALIM

Hazırlayan: Access International
http://accessnow.org

Sosyal paylaşım ağları son yıllarda insanların birbiri ile iletişim kurmasında ve kendilerini ilgilendiren meselelerde daha hızlı bilgi paylaşımında bulunabilmesinde giderek daha önemli bir rol oynamaktadır. Sosyal paylaşım ağlarının vatandaşların daha aktif ve bilgili olmasını sağladığı düşünülürse bu olumlu bir gelişmedir.

Sosyal paylaşım ağlarına katılmak çoğunlukla ücretsizdir, peki bu ağlar nasıl para kazanır? Bu ağlar bize ait verileri toplar-bizim paylaştığımız bilgiler sayesinde- ve bu veri tabanlarını hedef reklam şirketlerine satar. Bu verilerin arasında resimler, makaleler, kullanıcının oluşturduğu içerik olarak da bilinen durum güncellemeleri, arkadaş listemizdeki kişiler, arkadaşlarımızın bizim hakkımızda paylaştıkları bilgiler, ziyaret ettiğimiz ve reklam içeren veya "beğen" tuşu olan web siteleri ve benzeri yer almaktadır. "Trafik verisi" denilen ve bir siteye giriş yaptığımız zamanı, bulunduğumuz konumu ve benzeri bilgileri içeren veriler ne tür bir insan olduğumuza dair varsayımlarda bulunabilmek ve ne tür reklamların ilgimizi çekebileceğini tespit etmek için kullanılır. Diğer bir ifadeyle bir sosyal paylaşım ağında bize ait olan bilgilerin şahsımız veya arkadaşlarımız tarafından paylaşılması yolu ile aslında sosyal paylaşım ağlarından almış olduğumuz hizmet için dolaylı olarak para ödemiş oluyoruz. Bundan dolayı veri koruma artık sadece bir gizlilik hakkı değildir, çünkü veri artık ekonomik bir mal haline gelmiştir, ekonomik mal da aslında bir mülktür.

Çok fazla bilgiyi toplamak, kaydetmek, paylaşmak, satmak, satın almak ve kombine etmek mümkün olduğu için, bu işlerle ilgilenen şirketler bizim kim olduğumuza (veya en azından bizim kim olduğumuzu düşünüyorlarsa) dair oldukça ayrıntılı bir profil tutarlar. Bu şirketler varsayımlarını yine varsaydıkları sağlık durumu, yaş, cinsiyet, cinsel

“Kendi gizlilik ayarlarınız üzerinde de kontrol sahibi olmanız önemlidir, böylelikle kiminle bilgi paylaşımında bulunduğunuz konusunda bilinçli olarak bir karar vermiş olursunuz.”

yönelim ve benzeri konularda ayrımcılık yapmak için kullanırsa, bu durum sorun teşkil eder. Hükümetler bu verilere erişmek ve bu verileri kullanmak isterse sorun daha da karmaşık bir hal alır ki bu bir garantiye veya yasal izne tabi olmayan gayri resmi hükümet/sektör ilişkileri nedeni ile daha da sık karşılaşılan bir durumdur.

Bir sosyal paylaşım ağına katılırken takma isim kullanmak (kimlikteki isminiz ile doğrudan bağlantılı olmayan bir isim) – bu her ne kadar bazı sosyal paylaşım ağlarında gereksiz bir şekilde yasaklanmış da olsa- gizliliğin sınırlı da olsa korunabilmesi için uygulanabilecek yöntemlerden biridir. Ayrıca, kendi gizlilik ayarlarınız üzerinde de kontrol sahibi olmanız da önemlidir, böylelikle kiminle bilgi paylaşımında bulunduğunuz konusunda bilinçli olarak bir karar vermiş olursunuz.

Kullanıcılar aldıkları hizmetten veya şirketin bilgilerini kullanış biçimden memnun değilse, bu şirket ile paylaşmış oldukları bilgileri geri çekme yetkisine sahip olmalıdır. Buna “veri taşıma hakkı” denir. Verilerin kolay bir şekilde transfer edilebilmesi rekabet, tüketici tercihlerini ve inovasyonu artıracaktır.

Ayrıca, kullanıcıların hangi platformu kullanacakları konusunda bilinçli bir tercih yapabilmesi için hizmet sözleşmelerinin açık ve anlaşılır olması gerekir. Sosyal paylaşım ağlarında sıkı bir gizlilik korumasından faydalanabilirsek - ve ifade özgürlüğü gibi diğer haklardan da-, teknolojinin aleyhimize değil lehimize işlemesini sağlayabiliriz. Bu sayede inovasyon için gerekli güvenilir ortam yaratılır. ■

BULUT BİLİŞİM

ÖNGÖRÜLEMEYEN BİR ORTAMDA ÖNGÖRÜLEBİLİR KORUMA

Hazırlayan: Privacy International, İngiltere . http://privacyinternational.org

Bulut bilişim ismi, grafik ve diyagramlarda interneti temsil etmek için kullanılan bulut sembolünden esinlenerek ortaya atılmıştır. Oldukça belirsiz olan bu kavram için çok fazla tanım önerilmiştir. Bu tanımlardan en yaygın olanı ABD Ulusal Standartlar ve Teknoloji Enstitüsü tarafından ortaya atılmıştır: "Her yerde sağlanabilen, isteğe bağlı internet erişiminin [...] çok hızlı olarak yedeklenebilen, yönetimsel anlamda az çaba gerektiren ve servis sağlayıcısı ile kolaylıkla etkileşime geçebilen konfigüre edilebilir bilgisayar kaynaklarından oluşan ortak bir havuza aktarılması için geliştirilen bir model".[4] Layman'a göre bulut bilişim, bilişim hizmetlerini – yazılı veya veri kaydı- kendi bilgisayarınızda değil ama internette bir yerde, başkaları tarafından işletilen ve yönetilen sunucular üzerinde kullanmak demektir. Hotmail veya Gmail gibi web tabanlı e-posta hizmetler, internet üzerinden müzik veya video yayını, fotoğraf paylaşımı, sosyal ağlar üzerinden iletişim kurma, ödeme hizmetler veya online ofis uygulamaları (kelime işlem veya elektronik hesap çizelgeleri gibi) bulut bilişime örnek olarak verilebilir. [5]

Bulut bilişim aslında yeni bir teknoloji değildir, fakat bilişim hizmetlerini vermenin yeni bir şekli olarak yorumlanabilir. Google, Amazon, Microsoft ve eBay gibi bu sektörün önde gelen şirketleri kendi işlerini yürütebilmek için global İnternet ağına çok hızlı bağlanarak büyük veri merkezleri oluşturdukça bulut bilişim kavramı ortaya çıkmıştır. Bulut bilişim

4: NIST: Bulut Bilişim terimine NIST'in önerdiği tanım, 2011, s.2 http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
5: Cloud Computing, How the Internet Works
http://www.edri.org/files/2012EDRİPapers/how_the_internet_works.pdf

“Bulut bilişim hizmetleri kullanıcılarına özellikle esneklik, maliyet, kullanım kolaylığı, çevirim içi içeriğe daha kolay erişim, otomatik bakım ve güncelleme gibi alanlarda pek çok avantaj sunmaktadır. Bununla birlikte, verilerin hangi kontrol merkezinde olduğu ve bulundukları coğrafi lokasyon konusunda ciddi endişeler mevcuttur.”

daha sonrasında veri saklama ve bilişim hizmetlerini başka şirketlere satmanın bir yolu olarak, diğer bir ifade ile bir gelir kaynağı olarak görülmüştür. Bahsedilen bu veri merkezleri AB içinde veya dışında, dünyanın herhangi bir yerinde oluşturulabilir.

Bulut bilişim hizmetleri kullanıcılarına özellikle esneklik, maliyet, kullanım kolaylığı, çevrimiçi içeriğe daha kolay erişim, otomatik bakım ve güncelleme gibi alanlarda pek çok avantaj sunmaktadır. Bununla birlikte, verilerin hangi kontrol merkezinde olduğu ve bulundukları coğrafi lokasyon konusunda ciddi endişeler mevcuttur. Bu verilere kim erişim sağlamaktadır? Bu veriler nasıl kullanılabilir? Verileri bir bulut bilişim hizmetinden diğerine aktarmak ne kadar kolaydır? Bulut bilişim ne kadar güvenlidir? Verilerin kaybolması veya kötüye kullanılması durumundan kim sorumlu tutulur?

Mevcut veri koruma yasaları bu soruları yanıtlandırmakta yetersiz kalmaktadır. Bulut bilişim hizmeti sağlayıcıların rolü ve sorumlulukları, AB yasalarının ne zaman uygulanıp ne zaman uygulanmayacağı, kuralların nasıl uygulanacağı, olası bir sorunun nasıl çözüleceği, AB dışındaki ülkelere nasıl veri transferi yapılacağı, başka ülkelerin kendi yasaları çerçevesinde verilere erişip erişemeyeceği (bkz sayfa 21) gibi konularda belirsizlikler söz konusudur. Bu sorunlar kapsamlı ve etkili bir şekilde ve öngörü ile ele alınamazsa, Avrupa Temel Haklar Şartı’nda yer alan gizlilik hakkının korunması imkânsız hale gelecektir. ■

PROFİL OLUŞTURMA

TERCİHLERİ TAHMİN ETMEK İÇİN KİŞİSEL VERİ KULLANIMI

Profil çıkarma kullanıcılar ve kullanıcıların ilerideki davranışları hakkında tahminde bulunabilmek için kullanıcılara ait bilgilerin toplanması ve kullanması demektir[6].

Mesela, sıklıkla bebek kıyafeti ve bezi alan bir kişinin bebek arabası da alması beklenir. Daha soyut bir şekilde ifade edecek olursak "X ve Y davranışını sergileyen kişiler Z davranışını da sergilemiştir." Siz bir kullanıcı olarak X ve Y hareketinde bulundu iseniz, size Z hareketinde bulunma ihtimaliniz de varmış gibi muamele edilir. Bu mantık en başından itibaren yürütülebileceği gibi daha önce toplanan verilere dayanarak da bu mantığa varılabilir. Bu tür varsayımlara ulaşmak için kullanılan matematiksel mantık, profil algoritması olarak bilinir.

Hazırlayan: Foundation for Information Policy Research, İngiltere http://fipr.org

Kayda değer miktarda ilerleme kaydeden veri toplama yeteneği ve bilgisayar sektörünün artan gücü ile birlikte bu algoritmalar son derece karmaşıklaşmaktadır. Profil çıkarma ile ilgili üç temel sorundan bahsedilebilir:

- Algoritmalar mükemmel bir biçimde tasarlanmamıştır. Algoritmaları ne kadar az kullanırsanız, hata yapma riski o kadar artar. Daha basit bir ifadeyle, profil çıkarabilmek için çok nadir rastlanılan karakteristiklerden faydalanılamayacağı gibi çıkarılan profile dayanarak bireyler hakkında önemli kararlar da alınamaz.[7]

- Profil çıkarmanın sosyal eşitsizliği ve ırk, etnik köken, din ve mezhep ayrımcılığı ve diğer azınlıklara yönelik ayrımcılığı sürekli hale getirmesi ve

6: Daha ayrıntılı bir analiz için: http://protectmydata.eu/topics/limitations/ and Korff, Douwe, Comments on Selected Topics in the Draft EU Data Protection Regulation (September 18, 2012), http://ssrn.com/abstract=2150145

7: Bu konu hakkındaki farklı fikiler için (ve daha fazla referans için) http://www.schneier.com/blog/ adresinde, Bruce Schneier tarafından hazırlanan "güvenlik bloğu" sitesinde, 3 Eylül 2006 tarihli, Why Data Mining Won't Stop Terror yazısına bakınız

“Profil çıkarmanın sosyal eşitsizliği ve ırk, etnik köken, din ve mezhep ayrımcılığı ve diğer azınlıklara yönelik ayrımcılığı sürekli hale getirmesi ve güçlendirmesi kaçınılmazdır. Bu nedenle, hem profil çıkarmanın doğuracağı sonuçlar hem de altta yatan algoritmalar titiz bir şekilde takip edilmelidir.”

güçlendirmesi kaçınılmazdır. Bu tür bilgiler doğrudan kullanılmasa bile profil çıkarmanın dolaylı olarak böyle bir etkisi olabilir. Bu nedenle, hem profil çıkarmanın doğuracağı sonuçlar hem de altta yatan algoritmalar titiz bir şekilde takip edilmelidir.[8]

- Profil algoritmaları o kadar karmaşıktır ki bunları kullanan kurumlar bile artık bunların mantığını çözememektedir. Aslında, bu mantığı anlamaya çalışmadıkları veya anlayamayacakları bile söylenebilir, çünkü algoritmalar çoğunlukla “ ticaret sırrı” olarak saklanmaktadır. Bireyler ve gruplar açısından hayli önemli olan durumlarda, gerekli kontroller sağlanmadan ve gereken denge kurulmadan hareket edilmesi ve neticede güvenilir olmayan ve ayrımcılık içeren profil çıkarma tekniklerinin kullanılması riski yüksektir[9].

Profil çıkarma hukukun üstünlüğü kavramına, demokratik bir toplumda vatandaşlar ile hükümet arası ilişkilere ve müşteriler ile şirketler arası ilişkilere yönelik önemli bir tehdittir.

8: Bkz Oscar Gandy, Coming to Terms with Chance: Engaging Rational Discrimination and Cummulative Disadvantage, 2009, bkz http://www.ashgate.com/isbn/9780754679615

9: ABD ulusal güvenlik yetkilileri tarafından kullanılan nitelikli sistemler konusundaki tartışmalar için bkz. Korff&Brown’un hazırladığı Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004 ve geliştirilen teknolojiler için bkz. Douwe Korff tarafından hazırlanan “Total Information Awareness” programı, Sayfa No:3: TIA & PNR,
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/tia_and_pnr.pdf

YABANCI KANUNLARA DAYALI ERİŞİM

KANUNUN ELİ UZUN

İnternet ve iletişim hizmeti sağlayıcıları çoğunlukla müşterilerinin tabi olduğu adalet sisteminin dışında veya "bulut" bilişim kapsamında veri işleme ve kaydetme operasyonu gerçekleştirmektedir. Bu, bir dava hakkında soruşturma yürütürken faydalı bir kanıt niteliği taşıyabilecek verilerin soruşturmayı yürüten kurumun dâhil olduğu adalet sisteminin dışında saklanması gibi bir neticeye yol açmaktadır. Bu gibi durumlarda, kurumlar karşılıklı olarak kararlaştırılmış adli yardım prosedürlerini kullanmaktansa, bulut bilişim hizmeti sağlayıcılarından verilerin kendi adalet sistemleri dışında saklanmasını talep eder.

Çevrim dışı dünyada alışkın olduğumuz işleyişe kıyasla bu çok büyük bir değişimdir. Normalde, bir ülkede ulusal güvenlik kurumları veya emniyet teşkilatı başka bir ülkedeki bir kanıta erişmek istediğinde Karşılıklı Adli Yardım Sözleşmeleri sürecinden geçer. Bu sözleşmeler iki taraflı (iki devlet arasında) olabileceği gibi AB-ABD Karşılıklı Adli Yardım Sözleşmesinde olduğu gibi çok taraflı da olabilir.

Hazırlayan: Foundation for Information Policy Research, İngiltere http://fipr.org

Genel olarak, bu tür sözleşmelere göre başka ülkede bulunan delillerin ele geçirilmesi için delili isteyen ülkenin mahkemesi delilin bulunduğu ülkenin mahkemesine bir talepte bulunur. Bu gibi durumlarda ilgili tüm kişilerin ve kurumların hukuki haklarının korunması için gereken yasal süreç işletilir. Karşılıklı Adli Yardım Sözleşmeleri uygulamada karmaşık olabilir ve çok iş yükü doğurabilir. Ancak, bu sözleşmeleri es geçmek istenen verilerin bulunduğu ülkenin egemenlik hakkının ihlaline ve ilgili tarafların bu ülkenin adalet sistemi dâhilinde sahip olduğu haklarının çiğnenmesine yol açar. Devletler sözleşmeye dayanarak birbirlerinden

"Kurumların, bulut bilişim hizmeti sağlayıcılarından verilerin kendi adalet sistemleri dışında saklanmasına yönelik talepleri giderek artmaktadır."

“Özellikle acil durumlar ve yaşama hakkına yönelik yakın tehdit riskine karşı prosedürlerin standart hale getirilmesi ve hızlandırılması gerekmektedir.”

adli yardım isteyebilir ve bu sözleşme kapsamında bir veriye ihtiyacı olan devlet veriye sahip olan diğer devletten söz konusu veriyi temin edebilir.

Devletler uzun süre bu tür taleplere göre davranırsa, bu durum uluslararası teamül hukuku kapsamında kabul edilebilir hale gelebilir. Ancak bu, internet ve iletişim hizmetleri sağlayıcıları tarafından tutulan bilgilere yönelik talepler için henüz söz konusu değildir.

Bu nedenle devletler mevcut uluslararası hukuk çerçevesinde Karşılıklı Adli Yardım Sözleşmeleri prosedürüne uygun davranmalıdır. Bu gerekliliği yok sayma yönünde giderek artan eğilim internet ile ilişkili olarak uluslararası hukuk düzenine yönelik bir tehdittir. Bundan dolayı devletler kendi sınırları dâhilindeki verilere erişim yönündeki taleplerin mevcut Karşılıklı Adli Yardım Sözleşmeleri (iki taraflı veya çok taraflı) kapsamında iletilmesi konusunda ısrarcı davranmalı ve kendi adalet sistemleri dâhilinde herhangi bir veriye erişme yönünde sınır ötesinden iletilen taleplerin egemenlik haklarının bir ihlali olduğu konusunda net olmalıdır. Adalet, Temel Haklar ve Vatandaşlık’tan sorumlu AB Komisyonu Üyesi Reding konunun önemini vurgulamış ve “AB menşeli şirketler ABD yetkililerine talep üzerine doğrudan veri temininde bulunursa, AB veri koruma kanununu ihlal etme olasılıkları vardır” diyerek bu konuya dikkat çekmiştir[10].

Tüm bunlar bu alanda reform yapılmasına gerek olmadığı anlamına gelmez. Tam aksine Karşılıklı Adli Yardım Sözleşmelerine ilişkin sürecin iyileştirilmesi ve özellikle acil durumlar ve yaşama hakkına yönelik yakın tehdit riskine karşı işlemlerin standart hale getirilmesi ve hızlandırılması gerekmektedir. Ancak bu yapılırken uluslararası insan hakları standartlarına, uluslararası politikalara ve emniyet hizmetlerinin yürüttüğü soruşturmalara dikkat etmek gerekir. Aksi takdirde, bir kişi hakkında yabancı bir ülkeden veri temin etmek o kişinin kendi ülkesinden veri temin etmekten daha kolay olur ki bu da çelişkili bir durumdur.

Bu bölüm Brown&Douwe Korf’un 2012’de Global Network Initiative kapsamında hazırladığı Digital Freedoms in International Law Practical Steps to Protect Human Rights Online isimli rapor temel alınarak hazırlanmıştır.

Söz konusu rapora: https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf adresinden ulaşılabilir. ■

10: Avrupa Birliği Parlementosu yazılı soru 2430/2012
http://www.europarl.europa.eu/sides/getAllanswers.do?reference=E-2012-0002430&language=EN

İŞE YARAR BİR ŞEY YAPMAK

İYİ BİR YASA İYİ BİR UYGULAMA GEREKTİRİR

Avrupa Birliğinin mevcut Veri Koruma Yönergesini kabul etmesinden bu yana geçen on yedi yıl boyunca veri koruma konusundaki temel hakkın savunulmasına ilişkin yanlışlar ve doğrular konusunda pek çok şey öğrendik.

Yaşadıklarımızdan çıkarabileceğimiz en iyi ders iyi bir yasanın iyi bir uygulama gerektirdiği olabilir. Bazı Avrupa ülkeleri yetkin ve bağımsız veri koruma yetkilileri tarafından yürütülen sıkı veri koruma yasalarına sahiptir. Veri korumadan sorumlu organlar gereken hukuki yetkiyi ve teknik uzmanlığı da haizdir. Ancak, bu durum Avrupa çapında farklılık göstermektedir ve dolayısıyla bazı vatandaşlar diğerlerine göre daha zayıf koruma önlemlerinden faydalanmakta ve yine bazı şirketler de çok karmaşık süreçleri takip etmek zorunda bırakılmaktadır. Avrupa Birliği Komisyonu işte bu nedenle tüm AB ülkeleri için geçerli olacak tek bir yönetmeliğin hazırlanmasını önermiştir.

Avrupa genelinde etkin bir uygulama sistemi olduğu sürece Avrupa Birliği'nin gizliliğin koruması alanındaki küresel liderliği de güçlenir ve ileriye taşınır. Ayrıca, böyle güçlü bir sistem gizliliğin korunmasını şirketler için uyulması gereken bir mecburiyet olmaktan çıkarıp bir refleks haline getirecek ve müşteriler nezdinde de gizliliğin korunması bir umuttan çok bir talep olacaktır.

Sosyal paylaşım ağları, Büyük Veri ve bulut bilişim hizmetleri tarafından önerilen pek çok fırsat göz önünde bulundurulursa bugün böyle bir gelişim kaydedilmesi son derece önemlidir. Vatandaşların bu gelişmelerden azami düzeyde faydalanabilmesi için öncelikle bu gelişmelere güvenmesi gerekir. Güvenin tesis edilebilmesi için de tasarım sürecinin her aşamasında, tercihe göre gizlilik ayarlarında, uygulamada, amaç sınırlandırılmasında ve varsayılan gizlilik ayarlarında gizliliğin öncelikli bir kaygı olarak ele alınması gerekir.

Veri koruma çerçevesi başarılı bir reform sürecinden geçirilmezse, pek çok yasal boşlukla karşı karşıya kalabilir ve hiç kimsenin – ne vatandaşlar ne özel şirketler- hangi yasanın uygulanacağını bilmediği ve herkesin aşağı doğru çekildiği bir rekabet durumun içine itilebiliriz. Şimdi karşılıklı güven ortamında daha güçlü bir yasal çerçeve geliştirmek, iyi uygulamaları desteklemek, açık ve öngörülebilir yasal ilkelerden ve kurallardan faydalanmak, ticari anlamda azami düzeyde olanak yaratmak için elimizde bir fırsat var. Bu konuların daha ayrıntılı analizi ve EDRI'nin veri koruma çerçevesinin yeniden değerlendirilmesi için teklif ettiği değişiklikler için http://protectmydata.eu sitesini ziyaret edebilirsiniz.

Taslak yönetmeliğin ilgili kısımları konusunda kapsamlı bir analize Korff, Douwe, Comments on Selected Topics in the Draft EU Data Protection Regulation (September 18, 2012) kaynağından ulaşabilirsiniz.: http://ssrn.com/abstract=2150145 Özetler ve önerilen değişiklikler için: http://ssrn.com/abstract=2150151

EUROPEAN DIGITAL RIGHTS

EDRI.ORG/PAPERS

Bu broşür Alternatif Bilişim Derneği tarafından çevrilmiş ve yayınlanmıştır.

AB Temel Haklar ve Vatandaşlık Programı'nın finansal desteği ile hazırlanmıştır.

Friedrich Ebert Stiftung Türkiye'nin finansal desteği ile basılmıştır.

alternatif bilişim
www.alternatifbilisim.org

FRIEDRICH EBERT STIFTUNG
Türkei