DİJİTAL KÜTÜPHANE KANALI

Keyifli Okumalar Dileriz

Binlerce kategoride milyonlarca PDF e-kitap, ders kitapları, dergiler ve romanlara platformumuz üzerinden ücretsiz ulaşabilirsiniz.

RESMİ WEB SİTEMİZ

https://rantey.org

Yedek ve Duyuru Kanallarımız
Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

• Telegram: https://t.me/birkitapbir

• WhatsApp Kanalımız : https://whatsapp.com/channel/0029VbDHv8uE50Us4IvMoc0Y

MAHREMİYET

Eirik Løkke

MAHREMİYET

DİJİTAL TOPLUMDA ÖZEL HAYAT

Eirik Løkke

2. BASKI

Koç Üniversitesi Yayınları: 168 UÇBEYLERİ
TEKNOLOJİ | HUKUK

Mahremiyet: Dijital Toplumda Özel Hayat
Eirik Løkke

Norveççeden çeviren: Dilek Başak
Redaksiyon: Haydar Şahin
Düzelti: Hülya Hatipoğlu
Kitap tasarımı: Gökçen Ergüven
Kapak tasarımı: Melike Oran

Personvern–etter Snowden: Privatliv i det digitale samfunn

1. Baskı: İstanbul, Mayıs 2018
2. Baskı: İstanbul, Mayıs 2020

NORLA
NORWEGIAN LITERATURE ABROAD
Bu kitap, NORLA'nın çeviri desteğiyle yayınlanmıştır.

Baskı: A4 Ofset
Otosanayi Sitesi, Donanma Sk. No: 16 Seyrantepe/İstanbul
Sertifika No: 44739
+90 212 281 64 48

Koç Üniversitesi Yayınları
Rumelifeneri Yolu 34450 Sarıyer/İstanbul
Sertifika no: 18318
+90 212 338 1000
kup@ku.edu.tr • www.kocuniversitypress.com • www.kocuniversitesiyayinlari.com

Koç University Suna Kıraç Library Cataloging-in-Publication Data
Løkke, Eirik, 1980-
Mahremiyet : dijital toplumda özel hayat = Personvern etter snowden : privatliv i det digitale samfunn / Eirik Løkke ; Norveççeden çeviren Dilek Başak ; editör Haydar Şahin. -- İkinci baskı -- İstanbul : Koç Üniversitesi, 2018.
152 pages ; 13,5x20 cm.-- Koç Üniversitesi Yayınları ; 168. Teknoloji, Hukuk.
ISBN 978-605-2116-46-3
1. Data protection--Law and legislation. 2. Electronic surveillance. 3. Electronic surveillance--Social aspects. 4. Privacy, Right of. 5. Human rights. 6. Civil rights. I. Başak, Dilek. II. Şahin, Haydar. III. Title.
K3264.C65 L6520 2018

Mahremiyet

Dijital Toplumda Özel Hayat

EIRIK LØKKE

Norveççeden çeviren: Dilek Başak

KÜY

İçindekiler

Önsöz

2013 yılında çıkan *The Circle* (*Çember*) adlı çoksatar kitapta, yazar Dave Eggers dijitalleşmenin sosyal sonuçlarını araştırmaktadır. Çok uzak olmayan bir gelecekte, "Çember" adlı şirket Google, Facebook ve Twitter'i satın alır çünkü bu şekilde, internetin önemli bölümünü kontrol edebilecektir. En büyük isteği dünyanın en büyük şirketi için çalışmak olan ana karakter Mabelline (Mae) aracılığıyla, özel alanın iyi niyet kisvesi altında yavaş yavaş aşındırıldığı bir evrene göz atmış oluyoruz.

Dave Eggers'ın hayali evreninde ilginç olan, tam da bu iyi niyetlerin sorun haline gelmesi. Bir çocuğu kaçırılmaktan koruyacaksa, GPS izlemesi ödenecek küçük bir bedel değil mi? Dürüstlüklerinden emin olabilmemiz için, tüm siyasetçilerin, bedenlerinde bir video kamera taşımalarını beklememiz gerekmiyor mu? Şimdiye dek yayınlanmış tüm metin, resim ve videolar kataloglansa fena mı olur? Yabancıların özel hayata erişimine itiraz etmek bencillik hatta, kitapta Mae'nin iddia ettiği gibi, hırsızlık olmuyor mu?

Eggers'in parlak bir biçimde ele aldığı konu, sürekli gözetlenmenin toplumumuz üzerindeki etkisidir. Günün 24 saati çeşitli biçimlerde üzerimize çevrilen kamu spotları bizde ne gibi değişiklikler yapıyor? Dijital toplumda özel hayatın yeri nedir?

Bu işin ürkünç yanı bir sabah uyanıp kendimizi Dave Eggers'ın *Çember* kitabında anlattığına benzer bir toplumda bulmamız; orada kendimizi, ufak adımlarla ilerleyen zorbalık yüzünden, kamunun üzerimizdeki spotlarından kurtulmanın mümkün olmadığı bir duruma sokmamızdır.

"Çember-toplumu"nda son bulmamak için gerekli olan koşul, yeni dijital teknolojinin özel hayatımızı nasıl tehlikeye soktuğunun tartışılmasıdır. Mahremiyet konusundaki önceki tartışmalarının en önemlisi

devletin yetkilerinin ne kadar genişlemesi gerektiğiyken, mahremiyet şimdilerde ticari çıkarlar tarafından da baskı görmektedir. Google ve Facebook gibi şirketler, vatandaşların kişisel verilerini işlemeye dayanan bir iş modeline sahiptir. Sorunsuz diyemeyeceğimiz bu durum yüzünden, farklı düşünceler nasıl savunulabilir konulu, herkese açık ve kapsamlı bir görüş alışverişine ihtiyacımız var. Bu tartışma, 2013'teki Snowden sızıntısından sonra daha da önem kazanmıştır.

Şimdi okumakta olduğunuz, *Mahremiyet*: *Dijital Toplumda Özel Hayat* adlı kitap, benim bu tartışmaya katkımdır. Kitapta, yeni teknolojinin özel hayatlarımızı doğrudan nasıl tehdit ettiğini açıklamaya çalışıyorum, sonra da özel hayatı daha iyi koruyabilmek için ne türden yasal düzenlemelere ihtiyacımız olduğunu ele alıyorum. Ben de Dave Eggers gibi, pek çok izlemenin ardında iyi niyetlerin yatmasının getirdiği sorunlarla ilgiliyim çünkü amaç saygın olduğunda yolumuzu şaşırmaya karşı koymak güçleşiyor. Yüksek Mahkeme Yargıcı Louis Brandeis, 1928 yılında "ABD'ye Karşı Olmestead" davasında verilen karara itirazında şöyle söyler: "Tarih bize gösteriyor ki, özgürlüğün korunmasında en tetikte bulunmamız gereken zamanlar, devletin çıkarının söz konusu olduğu zamanlardır. Özgürlüğe gelecek en büyük zarar, iyi niyetli ama anlayışı kıt, ihtiraslı insanların özgürlükleri ihlal etmesiyle gerçekleşir."

Teşekkür

Oldukça karmaşık teknoloji ve hukuk konularında yeterli bilgiye ulaşmaya çalışmak, bu kitabı yazmanın en büyük zorluklarından biriydi. Yayımlanmış kitap ve makale sayısı çok fazla, ulaşılabilir bilginin miktarı günden güne, hatta saat başı artıyor.

Dolayısıyla, bu konular hakkında çeşitli biçimlerde geniş mesleki bilgilere sahip kişilere, yorumları ve tavsiyelerinden dolayı teşekkür borçluyum.

Özellikle Gard Vaaler, Eirik Newth, Eva Jarbekk, Jon Wesel-Aas, Lars Fredrik Svendsen, Finn Myrstad, Ingvild Næss, Bård Standal, Rozemarijn van der Hilst, Fredrik Gierløff ve Michael Tetzschner'e değerli tavsiyelerinden dolayı teşekkür ederim.

Süreç içerisinde bana yardımcı olan karım Klara Furuberg'e kocaman bir teşekkür.

Her zaman derin minnet duyduğum meslektaşlarım Marius Doksheim ve Kristin Clemet'e, tasarım ve şekiller için Therese Thomassen'e teşekkürler.

Her türlü değerli katkıya rağmen yanlışlıklar ve eksiklikler olacaktır, elbette bunlar tümüyle bana aittir.

Eirik Løkke
Oslo, 10 Ağustos 2016

BİRİNCİ BÖLÜM

Giriş

5 Haziran 2013, mahremiyet konusuyla ilgilenenler için tarihe geçecek bir gündür. O gün, İngiliz gazetesi *Guardian*, National Security Agency* (NSA) olarak bilinen ABD istihbaratının gözetleme programı hakkındaki binlerce belgeden ilkini yayımladı. Bu bilgiler, eski bir NSA çalışanı olan Edward Snowden'ın sızdırdıklarına dayanıyordu.[1]

Sızıntılar, gözetleme toplumunun artık distopik bir geleceğin tanımı olmaktan çıkıp şimdi ve burada başa çıkmamız gereken bir olguya dönüştüğünü gösteriyordu. Bu, dijital toplumda mahremiyetin, yalnızca bu olayla özel olarak ilgilenenler için bir tartışma konusu olamayacağı anlamına geliyordu, çünkü pek çoğumuz, dijital hizmetlerin en büyük tüketicileriyiz.

Faturaları ödemek için internet bankası kullanıyoruz, mal ve hizmetin karşılığını banka kartıyla ödüyoruz ve akıllı telefonları giderek daha fazla sayıda kişi kullanıyor, bu telefonlara yüklediğimiz bir dizi uygulama, biz pek farkına varmasak da, büyük miktarlarda dijital bilgi yayıyor. Günümüz cep telefonları pek çok yönden mükemmel birer "gözetleme aracı" ve 21. yüzyılda, hem vatandaşlar hem de toplum için birtakım büyük sorunlara yol açmadan sistemden çıkmak zor gibi gözüküyor. Kişi, akıllı telefonsuz, internetsiz ya da banka kartsız yani tamamen analog bir hayat sürmeye kalkıştığında, bu tavır yöneticilerde kuşku uyandıracaktır. İnsanlarda, söz konusu kişinin saklayacak bir şeyi olduğuna dair, pek de nedensiz olmayan bir merak uyanacaktır çünkü o kişi, sadece elektronik iz bırakmamak adına, bir sürü angarya işe katlanmayı kabul etmeye razıdır.

---

* Ulusal Güvenlik Teşkilatı –çn.

Bu konuda biraz bilgiye sahibiz çünkü *Wall Street Journal*'da çalışan gazeteci Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance* [Kuşatma Altındaki Ulus: Sürekli Gözetlenen Bir Dünyada Mahremiyet, Güvenlik ve Özgürlük Arayışı] adlı kitabında, tamamen analog bir hayat sürdürmeye çalışır; amacı elektronik gözetlemeden kaçmanın ne kadar mümkün olabildiğini araştırmaktır.[2] Bu çabasının sonuçlarından biri, yalnızca gözetlemeden kurtulmaya çalışması yüzünden resmi mercilerin dikkatini çekmesi olmuştur.

Angwin, modern insanların, dijital ekonomi içerisinde yaşamaya neredeyse mahkûm olduklarını göstermektedir.

Dijital teknoloji kullanımının sonuçlarından biri, büyük elektronik izler bırakıyor olmasıdır ve bunların düzenlenmesiyle, bu teknolojiyi işleyenler, ister yetkililer ister özel şirketler ya da diğerleri olsun, büyük miktarlarda özel bilgiye erişmektedir. Bu da suiistimal olanaklarının artmasına yol açmaktadır. Güvenlik sistemleri oluşturursanız da kişisel bilgilerin kaydedilmesindeki artışın kendisi, mahremiyet için büyük sorunları beraberinde getirmektedir. Bu sorunlar o kadar büyük görünmektedir ki, pek çok kişi, dijital bir toplumda geleneksel anlamda bir özel hayatın mümkün olup olamayacağı sorusunu sormaktadır.

Aynı zamanda, bilginin kaydedilmesinden kaçınmak ne mümkündür ne de istenmektedir. Tam tersi: Gelecekte, özel sektörde ve kamu sektöründe yenilikçi çözümlere ve daha iyi hizmet vermeye katkıda bulunmak açısından büyük miktarlarda verinin sistemleştirilmesi ve kullanımı daha da önemli olacaktır. Bu gelişme henüz emekleme aşamasındadır ve ortak bir terimle anılmaktadır: Büyük Veri. Büyük Veri'nin en büyük faydası, bilginin yeniden kullanımıdır; bu da bilgiyi kaydetmenin değerini oldukça artırmaktadır.

Bu nedenle hem mahremiyetin önemseneceği hem de faydalı dijital araçların ve hizmetlerin gelişmesini sağlayacak bir dengenin bulunması önemlidir. Verimlilik ve mahremiyeti dikkate alma konusunda nasıl bir denge kurulacağı da, mahremiyetle güvenlik arasındaki dengeyle nasıl başa çıkılacağı da belli değildir.

Özellikle Paris, Brüksel ve Türkiye'deki saldırılardan sonra pek çok kişinin gözetlemenin artmasından söz ettiği bir zamanda, uluslararası terörizm gibi bir tehdidin, tüm korkunçluğuna rağmen, örneğin eski Sovyetler Birliği'nin Batı dünyasında yaşayan vatandaşlar için oluşturduğu tehditlerden temel anlamda çok daha küçük olduğunu hatırlatmakta yarar var. Genişlemeci komünizm Batılı devletlerin bekasına karşı varoluşsal bir tehditti, oysa günümüz terörizmi için bunu söylemek zor. Bu, terörizm ciddi bir tehlike oluşturmuyor anlamına gelmesin, ancak bu tartışmayı soğukkanlılıkla yürütmemiz gerekiyor ve Başsavcı Tor-Aksel Busch'un *Til forsvar for personvernet* [Mahremiyeti Savunmak Adına] adlı kitabında yazdığı gibi terörizm korkusu tehlikeli bir yoldaştır.[3]

Tam da bu yüzden, mahremiyete yapılan müdahalelerin gerekçeleri konusunda sıkı taleplerde bulunmak gerekmektedir. Müdahale ne kadar genişse gerekçeler için talebimiz de o kadar güçlü olmalıdır ve her türlü veri kaydı ve saklanması, "mümkün olduğunca az, mümkün olduğunca kısa" ilkesi çerçevesinde yapılmalıdır. Gözetleme ve özel hayat arasındaki dengeye liberal yaklaşımın temel ilkesi bu olmalıdır. Bilginin kayıt altına alınmasına ve ülkenin güvenliği öne sürülerek izleme yapılmasına şüpheyle yaklaşmanın ne kadar gerekli olduğunu tarih ve özellikle de Snowden'ın itirafları göstermiştir.

Ülkede olağanüstü hal yönetimi geçerliyse, yetkililerin bilgileri kayıt altına almasına büyük bir anlayış gösterilmelidir, şeklinde belirgin bir tutum vardır. Ancak denetlemek için izlemek büsbütün gerekli bir koşul olsa bile yeterli bir koşul olarak anlaşılmamalıdır.

Snowden'ın ifşaatından sonra bile, gelişmelerden rahatsızlık duyanların sınırlı sayıda olması, özel hayatın baskı altında olduğunu iddia eden bizim gibiler için ayrı bir sorundur.

2016 yılında *Vårt Land* gazetesinde yapılan bir ankette katılımcıların yarısı, yetkililerin ileri sürdüğü hedef, terör hareketlerini önlemekse polise vatandaşları gözetleme konusunda daha fazla imkân tanınmasının "büyük ölçüde" ve "oldukça büyük ölçüde" kabul edilebilir olduğu yönünde cevap vermiştir. Ayrıca yüzde 28'i, "bir dereceye kadar" diye cevap vermiştir. Yüzde 20'nin altında bir oran, terörü engellemek için

daha fazla gözetleme yapılmasının "az" kabul edilebilir ya da "hiçbir şekilde" kabul edilemez olduğunu düşünmektedir.[4]

Gözetlemenin aslında çoğu kişi açısından sınırlı bir sorun olması buna gerekçe gösterilebilir elbette; ancak bunun nedeni dijitalleşmenin artmasının ardından gelen potansiyel tehlikeler ve sorunlarla ilgili çok az kişiye bilgi verilmesi de olabilir.

Bu kitap, yeni dijital teknolojinin mahremiyeti ne kadar güçleştirdiği hakkında daha fazla bilgi edinmeye katkıda bulunmayı amaçladığı gibi, ticari olanaklarla özel hayat arasındaki korunması güç dengeye de önemli ölçüde dikkat çekmektedir. Toplumun bir yandan bireylere iyi hizmet verip bir yandan da özel alanı nasıl koruyacağı sorusuna net bir cevap vermek söz konusu değildir. Oslo Üniversitesi'nde araştırmacı olan Lee Bygrave'in yazdığı *Data Privacy Law: An International Perspective* [Veri Mahremiyeti Kanunu: Uluslararası Bir Bakış Açısı] kitabında belirttiği gibi, güçlü bir mahremiyet mevzuatı ve giderek artan bilgi işlem kullanımı arasında her zaman için bir çıkar çatışması söz konusu değildir. Bazı durumlarda, artan bilgi işlem kullanımı, internette mahremiyet mevzuatının güçlenmesine katkıda bulunabilir. Ancak çoğunlukla, çatışan çıkarlar söz konusu olmaktadır.[5] Çıkar çatışmalarının yaşandığı durumlarda hangi değerlerin galip geleceği belli değildir.

Bu kadar derin ve karmaşık olan bir konuya tek bir kitapta bütün yönleriyle değinmek mümkün değil. Bu yüzden bu kitap, teknolojik gelişmenin siyaseti nasıl zorladığı konusuna genel bir giriş yapmayı hedeflemektedir.

Kitap, dokuz bölüme ayrılmıştır.

Birinci Bölüm'de, mahremiyet sorusunun neden yeniden güncellik kazandığı açıklanmaktadır. İkinci Bölüm'de, özel hayat hakkının Batı demokrasilerinde neden temel bir hak olduğuna dair liberal anlayışa dayalı ilkesel bir savunma sunulmaktadır, ayrıca mahremiyet ve özel hayat kavramlarından semantik olarak ne anladığımıza dair bir kavram açıklaması yapılmaktadır. Üçüncü Bölüm'de, dünya tarihinde eşi benzeri olmayan bir dijital gözetleme düzenini mümkün kılan teknolojik gelişim anlatılmaktadır. Dördüncü Bölüm'de, demokrasinin olası hassas noktaları tartışılmaktadır. Hem uluslararası tarihin hem de

Norveç tarihinin bize gösterdiği gibi, liberal demokrasiler bile otoriter akımların kurbanı olabilir; 1950'lerdeki McCarty'cilik döneminde ve Lund Komisyonu'nun 1990 ortalarında belgelediği üzere Soğuk Savaş sırasında Norveç'te olduğu gibi.

Beşinci Bölüm'de Büyük Veri kavramı ele alınıp açıklanmaktadır. Olanaklar ve sorunlar, yeni teknolojinin devasa miktarda veriyi rekor bir sürede işleme yeteneğinden kaynaklanmaktadır. Sonraki bölüm olan Altıncı Bölüm'de, yeni gözetleme ekonomisi, bizzat Facebook ve Google'ın iş modelinin mahremiyetle ilgili kendine has sorunları da nasıl beraberinde getirdiği konusuna ağırlık verilerek anlatılmaktadır. Yedinci Bölüm'de, ABD ve Avrupa'daki gözetleme yetkileri ve mahremiyet mevzuatıyla bağlantılı hukuksal ve siyasi ilişkiler tartışılmaktadır. Sekizinci Bölüm'se, Noveç'te devlet iznine bağlı olan gözetleme uygulamalarını gözden geçirmektedir.

Kapanış olarak, Dokuzuncu Bölüm'de, hangi gelişmelerin özellikle endişe uyandırdığı vurgulanıp süreç özetlenmektedir.

İKİNCİ BÖLÜM

Özel Hayat ve Mahremiyet Neden Önemlidir?

Özel hayatın önemini göstermek için en iyi yöntem, totaliter devletlere göz atmaktır. Totaliter devletlerin en önemli ayırt edici özelliği, rejimin, devlet ve toplumu bir alanda bütünleştirme isteğidir. Bu tür toplumlarda özel hayat alanı oldukça sınırlıdır, rejimin gözetimi o kadar bütünseldir ki, vatandaşların davranışlarına nüfuz etmiştir. Bu, vatandaşların, özel düşüncelerini yakınlarıyla paylaşırken dikkatli olması anlamına gelir çünkü her türlü bilgi, hem kendileri hem de yakınları için korkunç tehlikeler doğurabilir. Kuzey Kore bu tür bir topluma gösterilebilecek en iyi örnektir. Bu toplumda rejim, yalnızca gücü elinde tutmakla yetinmemekte, ayrıca toplumun her kesiminde tam anlamıyla bir denetim sağlamayı hedeflemektedir. Özel alanın tamamen ortadan kalkması istenir.

Kuzey Kore şartlarında yaşamanın nasıl bir şey olduğunu hayal etmek çoğumuz için oldukça zordur, hatta mümkün bile değildir. Batı demokrasilerinde yaşayanların çoğu, iktidarı eleştirme ve alternatif bilgi kaynaklarının kolay ulaşılabilir olması geleneği içerisinde sosyalleşmiştir. Kuzey Kore'de bunun tam tersi geçerlidir. Kişinin, doğduğu günden itibaren rejim propagandasıyla beyni yıkanır, kişiyi putlaştırmaya dayalı bir toplum içerisinde sosyalleşilir ve her türlü muhalefet acımasız tepkilere, hatta ölüm cezasına yol açar. Kuzey Kore özel alana sahip olmayan bir toplumdur.

Bu totaliter ideali, Alman Demokratik Cumhuriyeti'nin (DDR) güvenlik ve istihbarat örgütünün (Stasi) şefi Erich Mielke'den daha net açıklayan olmamıştır: "Her şeyi anlayacaksak, her şeyi bilmeliyiz." Her şeyi bileceksek, doğal olarak herkesin, her zaman gözetlenmesi gerektiği sonucu ortaya çıkmaktadır. DDR'de 15 milyonun üzerinde insan

yaşıyordu ve bunların neredeyse yaklaşık 100 bini Stasi görevlisiydi. Ayrıca kurumun 173 bin muhbiri bulunmaktaydı. Her 55 vatandaşa bir Stasi düşüyordu.[1]

DDR'de hiç kimse, özel alanın varolduğuna dair bir güvence hissetmiyordu. Vatandaşlar, her yerde her zaman gözetlenebilecekleri gerçeğiyle başa çıkmak zorundaydı. Rejim, vatandaşların davranışlarının toptan gözetimini istiyordu. Anti-sosyalist denen ve aslında yetkililere yönelik eleştirilerin tümünü kapsayan girişimler ancak böylece ortaya çıkarılabilirdi. Vatandaşların özgürlüğü tam anlamıyla göz ardı ediliyordu.

Bu türden bir gözetleme toplumu başka insanlara, hatta kendi ailene bile güvenmeyi olanaksız kılar. Toplumdaki güven ortamını yıkmak için bundan daha etkili bir sistem az bulunur. Polonya kökenli Amerikalı yazar Anne Appelbaum, eski komünist diktatörlükleri tanımlarken Mussolini'den bir alıntı yapmıştır: "Devletin dışında bir hiçsin."

Iron Curtain: The Crushing of Eastern Europe, 1944-1956 [Demir Perde: Doğu Avrupa'nın Ezilmesi, 1944-1956) kitabında da yazdığı gibi, Doğu Avrupa'daki sıradan insanların hayatı tamamen komünist sistem tarafından tanımlanıyordu.[2] Ne yaparsanız yapın, kimle konuşursanız konuşun, ne derseniz deyin, nerede olursanız olun: Devlet ve komünist sistem toplumla bütünleşmiş bir parçaydı.

George Orwell olarak bilinen yazar Eric Arthur Blair, *Hayvan Çiftliği*[3] ve *1984*[4] romanlarında, özel hayatın anlamını gözler önüne serdi. "Büyük Birader seni izliyor" ifadesini ve "yenikonuş" sözcüğünü ilk ortaya atan Orwell'dir. Kitaplar, özel alanı yok etmenin nelere mal olduğunu göstermektedir. Orwell'in öne sürdüğü nokta, doğal olarak, böylesi bir gözetleme toplumunun, özgürlük kavramını herhangi bir şekilde anlamayı olanaksız kılmasıydı. Orwell, aynen böyle bir durumun Stalin'in Sovyetler Birliği'nde de gözlemlendiğini ileri sürüyordu. Liderin paranoyasıyla birleşen bir gözetleme toplumu, kişinin, sürekli tehdit altında olduğu duygusuyla dolaşmasına neden oluyordu. Milyonlarca vatandaşın gözetleme, ispiyonlama ve yalanlar neticesinde yakalanıp rejim tarafından öldürüldüğü gerçeği göz önüne alındığında, bu duygu tamamen sebepsiz değildi. Stalin'nin Sovyetler Birliği'ni ve DDR'yi

özetleyen şey, vatandaşların özel hayat talebinde bulunma düşüncesini ortadan kaldırmaktı.

Bu ülkelerde parti, devlet ve ideoloji örtüşüyordu, siyasi bir muhalefete dönüşebilecek küçük eğilimleri bertaraf etmek için özel alanın denetimi çok gerekliydi. Bu da, özel hayatın korunmasının, iktidar eleştirisi ve karşı denge için nasıl gerekli bir koşul olduğunu göstermektedir.

Başka bir deyişle, özelin ilkesel olarak kabulü, yani devletin dışında bir şey olarak kabulü, düzgün işleyen bir demokrasi için mutlak bir koşuldur ve özgürlük kavramından ne anladığımızı ortaya koyan çok önemli bir boyuttur. Kişinin kendi özel alanı üzerinde denetimi olması anlamındaki bir özel hayat, yetkin bir vatandaş olarak katılımı mümkün kılan temeldir. Özelimiz, bireysel alanı tanımlar, bir vatandaş olarak senin birisi hakkındaki hangi bilgi, hangi duygu, düşünceler ve kişisel özellikleri başkalarıyla paylaşmayı dilediğini tanımlar. Başka bir deyişle, 1970'lerdeki siyasi solun "kişisel olan politiktir", bu yüzden de kamu yararınadır sloganı, özel hayat hakkından anlamamız gerekenin karşı tezidir.

Özel hayat alanı, vatandaşların hareketlerinin, özel hukuk ilişkilerini düzenlemek için toplumun koyduğu yasaları çiğnememesi koşuluyla, ilkesel olarak kamudan ayrı tutulmuş ve vatandaşların özgür ilişkisine bırakılmıştır. Çoğunluk, sosyal varlıklar olarak insanların hem özel hem de kamusal alanlara ihtiyacı olduğunu kabul etmektedir. Bu alanlar birbirinin yerine geçemez ancak neredeyse birbirini tamamlar, birbirleriyle örtüşürler de. En azından özel alanın, kamu alanının işgaline ne kadar dayanması gerektiği konusunda anlaşmazlıklar olduğunu da söyleyebiliriz.

Bu gri alanlar, tamamen kamuya ait olmayıp özele de ait olmayan, genellikle "yarı kamusal" alanlar olarak anılır. Hangi özel bilgilerin kamunun yararına olduğu konusunda farklı görüşler söz konusudur. Bu, zamanla da değişebilir.

Ayrıca, özel ve özel hayat anlayışı da değişmektedir. ABD'deki özel hayat hakkını konu alıp tartışan ilk ve en etkileyici hukuk makalelerinden biri, hukukçu Louis Brandeis (sonradan Yüksek Mahkeme yargıcı oldu) ve hukukçu Samuel Warren tarafından, 1800'lerin sonuna

doğru kaleme alınmıştır. "The right to privacy" ["Mahremiyet hakkı"] başlıklı makalenin çıkış noktası, değişen toplum koşullarının –Warren ve Brandeis'in durumdaysa haber yayın organlarının ve medyada yer alan haberlerin– özel alanla ilgili anlayışımızın değişimine katkısıdır. [5]

Eirik Newth'in *Overvåkningssamfunnet* [İzleme Toplumu] kitabında tanımladığı gibi, ABD'deki kanunlar, bilgileri kamuya açıklama konusunda o güne kadar pek az sınırlanmıştı.[6] Brandeis ve Warren, bilgilerin mahremiyeti ihlal edecek şekilde açıklanmasını engellemek için temel esaslar oluşturmak istiyorlardı. Makalenin bu kadar büyük bir etki yaratmasının sebeplerinden biri, yazarların, mahremiyeti ihlal edecek bilgilerin aynı zamanda kamu yararına olabileceğini ve bu yüzden de yayımlanabilir olması gerektiğini çok iyi anlamalarıydı. O zamandan bu yana, özellikle de internetin gelişimiyle birlikte, hem basın ahlakı hem de hukukla ilgili tartışmalar şu görüş etrafında dönmektedir: Demokratik toplumlarda özel hayatın öneminin kabul edilmesi, bilgileri yayımlamaktaki kamu yararının aleyhinedir.

Daha önce de belirtildiği gibi, özel hayatı korumak kamunun alanını hiçe saymak anlamına gelmez. Hatta tam tersi: Hem özel hem de kamusal alana ihtiyacımız vardır. Ancak vatandaş olarak, ne zaman kamusal alanda, ne zaman özel alanda bulunduğumuzu bilmeye ihtiyacımız olduğu da ortadadır. Bu nedenle özel alanın nerede bitip kamusal alanın nerede başladığı o kadar da önemli değildir. Önemli olan bizim, vatandaşlar olarak, hangi alanda bulunduğumuzu her an anlamamızdır. Mahremiyetin önemli bir yanı da her vatandaşın toplum içindeki itibarının korunması ve özel bilginin denetiminin kesinlikle elzem olmasıdır. Kamudaki itibarımız bizim kendimizi kanıtlama olanaklarımızı, diğerleriyle ilişkilerimizi ve ticari etkinliklerimizi büyük ölçüde etkileyecektir. Kişisel özgürlüğümüz önemli ölçüde resmi itibarımıza bağlıdır.

Özel hayata saygı, bireyin bütünlüğünün vazgeçilmez bir parçasıdır. Batılı liberal gelenek içerisinde, böylesine bir bütünlük, özgür bireylerin iyi bir toplum oluşturabilmesi için gerekli koşul olarak görülür. Bireyin bütünlüğü, hür bir birey –yani insanın içine doğduğunu söyleyebileceğimiz aile gibi grup bağlarından ayrılmış özgün bir benlik– kişisel bir kimlik geliştirmek için gerekli bir koşuldur. Kişinin bu "benlik"

değerini nasıl yüceltebileceğine örnek olarak, devletlerin yasalaştırdığı, çocuğun aile, arkadaşlar ve grup etkisi oluşturan diğer yapılardan farklı biçimde kendi kişisel kimliğini geliştirme hakkını korumaya yönelik kararlar gösterilebilir. Özel hayata saygı, vatandaşların bireysel özgürlük ve etik konusunda gelişim gösterebilmelerinde belirleyici bir etken olarak görülmektedir. Mahremiyeti koruma altında olan herkesin sonunda yüksek ahlaki değerlere sahip insanlara dönüşeceği söylenemez. Tam tersi durumlara pek çok örnek verebiliriz. Özel hayat hakkının, ahlaklı davranan kişilere evrilmenin garantisi olmadığı ortadadır, ancak özel hayat hakkı, bireyin bütünlüğünün anlamlı bir şekilde korunmasının, ayrıca başkaları ile birbirimizi anlamlı bir biçimde etkilememizin de koşuludur.

Mahremiyet, kamusal olanın karşıtı olarak yorumlanmamalıdır çünkü insan biyolojisi büyük ölçüde sosyaldir, yani başka insanlarla sosyal ilişki kurma arayışı içerisinde olduğumuzdan kişisel bilgilerimizi, kamusal bağlamda da, farklı derecelerde paylaşmak için doğal bir ihtiyaç duyarız. Mesele, özel bilgiyi kimlerle paylaşacağımıza kendimizin karar verebilmesidir. Bu ihtiyaç çoğu zaman "sosyal roller" olarak tanımlanır. Sosyal rollerimize bürünür, içinde bulunduğumuz şartlara göre, hangi kişisel bilgiyi ne zaman başkalarıyla paylaşmayı dilediğimize karar veririz. İşte, aşkta, ailede vs. farklı sosyal roller üstleniriz. "Kendin olmak" durumunu gerçekmişçesine yaşarız, yani bu bağlamda, birey şartların her an gerektirdiği rollere uyum sağlama olanağına sahiptir.

Tam da bu gerçek, yani tüm kişiliğimizin ve davranışlarımızın özel mi yoksa kamusal alanda mı bulunduğumuza bağlı olması, liberal demokrasiye sahip olduğunu iddia eden tüm toplumlarda özel hayat alanının elzem olmasının en temel nedenidir. Düşünür Lars Fr. Svendsen'ın öne sürdüğü gibi:

> Özel hayat, kişiliğini geliştirebilmesi için bireyin düşünüp kendini ifade edebildiği ve rahatlayabildiği bir alanı içerir. Özel alan, başkalarının tepkilerinden, yani bizim bu alana girmelerine izin verdiklerimizin dışında kalanlardan çekinmeden, dilediğimizi yapabileceğimiz bir yerdir. Ayrıca söz konusu olan sadece başkalarının olası yargılayan bakışlarından kaçtığımız bir alan değil, bu bakıştan kurtulduğumuz için kendimizi gözlemlemekten de

> kaçtığımız bir alandır. Hayatlarımızın bazı yönleri, kesinkes ve tamamen yalnızca kendi kendimize kaldığımız koşullar altında var olabilir. Mesele, saklayacak bir şeyimizin olması değil, insanın, sakladığı bir şeyi olup olmadığını düşünmeye hiç mi hiç gerek duymadığı alanlarının olmasıdır.[7]

"Saklayacak bir şeyiniz yoksa korkacak bir şeyiniz de yoktur" argümanı çeşitli biçimlerde dile getirilmektedir. Google'ın o zamanki patronu Eric Schmidt 2009 yılında, "Başkalarının bilmesini istemediğiniz bir şeyler yapıyorsanız, belki de her şeyden önce bunu hiç yapmamanız gerekmektedir,"[8] demişti. Schmidt tutumunu hiç kuşkusuz yumuşattı ve sonraki söyleşilerinde, özel hayatın öneminin altını çizerek, "Özel hayatı korumak için mücadele etmeliyiz, yoksa onu kaybetme tehlikesiyle karşı karşıya kalırız" dedi.[9]

Özel hayatın önemli bir parçası da, "Saklayacak bir şeyim var mı acaba?" diye düşünmekten, dolayısıyla kendine dışarıdan bakma zorunluluğundan ve böylelikle kendi davranışlarını kısıtlamaktan kurtulmaktır. Durmaksızın gözlenmek ve kayıt altında tutulmak davranışlarımızı etkiler. Özel hayat, saklayacak bir şeyinizin olup olmamasıyla ilgili değildir, ancak vatandaşların kendi istekleri ve olanakları doğrultusunda hareket edebilme özgürlüğünün korunmasıdır; başka bir deyişle, vatandaşların kendi başlarına iyi bir hayattan ne anladıklarını tanımlamaya ve bunu en iyi biçimde gerçekleştirmeye olanak bulabildikleri bir alanı yaratmaktır.

Düşünür Isiah Berlin, bireyin bütünlüğünün Batı'nın kültür dünyasında niçin bir mihenk taşı olduğunu, özel hayatın anlamına işaret ederek özetler:

> Müdahalelere maruz kalmama ve kendi haline bırakılma arzusu hem bireyler hem de toplumlar söz konusu olduğunda yüksek medeniyetlerin ayırt edici özelliği olmuştur. Özel hayat ya da kişisel ilişkiler alanı fikrinin dokunulmazlığı vardır; bu fikir özgürlük kavramından doğmuştur. Özgürlük kavramının gelişmiş şekliyse, dini köklerine rağmen, Rönesans ve Reform Hareketi'nden daha gerilere uzanmaz. Eğer bu fikir yok olursa, tüm bir medeniyet, tutarlı bir ahlaki perspektif de yok olacak demektir.[10]

Mahremiyet, Kişisel Bilgilerin Korunması ve Özel Hayat

Mahrem/mahremiyet, yani İngilizcedeki *privacy* kavramlarıyla ne kastettiğimizi eksiksiz tanımlamak semantik açıdan zordur. Bu kavramı hakkıyla tanımlamak, kavramın tüm önemli özelliklerini kapsayan basit bir tanımla anlatmak kolay değildir. "Mahrem"den tam olarak ne anladığımız tarih boyunca farklılık göstermiş ve ortamla bağlantılı olmuştur. Ancak mahremiyete ne anlam yüklersek yükleyelim, korunaklı özel hayatın demokratik bir toplum için taşıdığı sosyal değeri yadsıyacak bir anlayışa pek rastlanmaz; bu durum da liberal demokrasilerin yasalarında karşılığını bulur. Bu yüzden, özel hayatın karşılaştığı sorunlara değinirken geniş bir yaklaşımda bulunmamız gerekir.

Günlük dilde mahrem kavramı, kamusal olanın tersine, çoğunlukla soyut bir biçimde kullanılır ve burada kavram (çeşitli biçimlerdeki) bireysel alanı tanımlar. Bu alan içerisinde biz vatandaşlar, diğerleriyle hangi değiş tokuşlara ve/veya hangi işbirliklerine gireceğimize kendimiz karar veririz.

Mahremiyetin sosyal anlamı, "NOU 2009: Birey ve Bütünlük: Dijital Toplumda Mahremiyet" raporunda etraflıca tartışılır, günlük konuşmalarda komisyondan Mahremiyet Komisyonu diye söz edilir. Komisyon, raporunu 2009 yılında II. Stoltenberg hükümetine sundu.[11] 4.2.5 sayılı maddede komisyon, mahremiyet hakkının hem bireysel özgürlük hem de kolektif fayda olarak görülmesi gerektiğini öne sürer ve John Locke, Isiah Berlin, John Rawls ve John Stuart Mill gibi isimlere göndermeler yapar. Son belirttiğimiz isim, Mahremiyet Komisyonu'nda faydacı argümanlar görüşüldüğünde özellikle önem kazanmaktadır. Komisyon'un kaleme aldıkları aşağıdaki gibidir:

> Özel hayat ve mahremiyet hakkının tamamen faydacı bir biçimde gerekçelendirilmesi sorunlu olabilir çünkü bireylerin ya da grupların bütünlüğünü artan bir toplumsal fayda için feda etmek çok kolaylaşacaktır. Çoğunluğun yararı için zayıf azınlığın mahremiyetinin sınırlandığı bir durumu düşünebiliriz örneğin. Öte yandan, mahremiyet toplumun çıkarlarının ve diğer hakların karşısına konulacaktır [...]. Mahremiyet, terörü ve başka suçları önleme amacının, sağlık ve esenlik ihtiyacının, demokratik karar mekanizmaları hakkında bilgilendirilmenin, araştırmaların ve baş-

> ka hakların aleyhinde olacaktır. Mahremiyet bir insan hakkı olarak kabul edildiğinden, sağlık yardımları düzeyini ya da toplumdaki güvenliği artırmak isteyen kararlar, her zaman için, bireylerin insani değerini ve özerkliğini en iyi biçimde gözetiyor mu sorusuyla değerlendirilmelidir. [12]

Ancak, özel hayat hakkı mahremiyetten ne şekilde farklıdır? Siyasi tartışmalarda ve kavramların gündelik kullanımında, özel hayat ve mahremiyet birbirinin yerine kullanılır.

Mahremiyet Komisyonu, araştırmasında kavramları tartışmaktadır ve mahremiyetin, pek çok durumda, kişilik bütünlüğü için kullanılan bir diğer sözcük olduğunu öne sürer. Ayrıca İfade Özgürlüğü Komisyonu'nun 1999'da yaptığı araştırmaya değinir:

> "Özel hayatın huzuru" ve "mahremiyet" arasındaki, özellikle önemli olan farkların altını çizmek gereklidir. Özel alanın korunmasının ("özel hayatın huzuru") gerekçesi, mahremiyetinkinden de önemlidir; bu gerekçe, kolektif ya da toplumsal olanın işleyiş biçimiyle ilintilidir. Somut olarak bu, kamuyu ilgilendiren tartışmaya gösterilen özen hakkındadır. Öte yandan mahremiyet, özellikle, kişinin özel bir kişi olduğundan değil, kamusal bir kişi (kamusal itibar) olması nedeniyle korunmasıyla ilgilidir.[13]

Mahremiyet Komisyonu, Norveç'teki gündemin bu ayrımı kaçırdığını ileri sürer.

> "Mahremiyet"in, "özel hayatın huzuru"nun aksine, kendi gerekçesini yalnızca bireysel (kolektifin karşıtı) çıkarlarda araması gibi bir durum söz konusu değildir. Mahremiyet söylemi –en azından Oslo Üniversitesi'ndeki bilişim hukukuyla ilgili çevrede– her iki türden çıkarı da çoktandır mahremiyetin bir parçası olarak bünyesine katmıştır.[14]

Kişinin, kişisel bilgilerini denetleyebilmesi ve bu bilgilerin akıbetine mümkün olduğunca kendisinin karar vermesi, ayrıca başkalarının kendisi hakkında hangi bilgilere sahip olduğunu bilme hakkı, mahremiyetin önemli bir unsurudur. Norveççede bu, kişisel verilerin korunması olarak anılmaktadır. Kişisel verilerin korunması aynı adlı kanuna, sağlık kayıtları kanununa ve gizlilik anlaşması usulleri gibi kapsamlı yasal düzenlemelere tabidir. Özel hayatın gizliliği ayrıca, genel olarak

hukukun koruması altındadır, özel hayatın huzurunu koruma amaçlı ceza hukuku hükümleri buna örnek olarak gösterilebilir.

Bu yüzden, özel hayatın korunması, daha genel olarak mahremiyete ve kişisel verilerin korunmasına işaret eder. Mahremiyet Komisyonu, araştırmasında özel hayat ile mahremiyeti birbirinden ayırmazken, mahremiyet ve kişisel verinin korumasını ayırmıştır. Bu ayrım mantıklı görünmektedir.

> Özel hayatın korunması kişisel bütünlüğü muhafaza etmekle ilgilidir: Her bir bireyin, özel hayatını, kendi kendine karar verebilme (otonomi) ve kendini ifade edebilme olanağını muhafaza etmeyi kapsar. Özel hayatın korunması hakkındaki kararlılığa, özel hayatın huzurunun, ceza kanunuyla koruma altına alınmış olması örnek gösterilebilir.
>
> Özel verilerin korunması, kişisel verilerin işlenmesi hakkındaki usuller ve esaslarla ilgilidir ve burada temel amaç mahremiyetin koruma altına alınmasıdır. Usullerin sebebi, her bir bireyin kendisi hakkındaki bilgilerin işlenişi üzerinde denetim ve gözlem yapabilmesini güvence altına almaktır. Belirli birkaç istisna dışında, her bir birey, başkalarının onların kişisel koşulları hakkında neler bilebileceğini belirleme hakkına sahip olabilmelidir. Özel hayatı koruma hukukunun bu kısmı, en kapsamlı yasal düzenlemelere tabidir, örneğin özel verilerin korunması kanunu, sağlık kayıtları kanunu, gizlilik anlaşması vb.[15]

ÜÇÜNCÜ BÖLÜM

İnternet ve İzleme

Tarihçiler insanlığın gelişimini tanımlarken genellikle biz insanların birlikte yaşama biçimimizi kökten değişime uğratmış iki büyük teknolojik devrimden söz eder: İlk büyük devrim, insanların avcı toplumundan toprağı ekip biçmeye geçtikleri dönemdeki Tarım Devrimi'dir. Bu, ilk medeniyetlerin temelini oluşturmuştur. Bu tür tarıma dayalı ilk toplumların ne zaman ortaya çıktığı tam olarak bilinmemektedir, ancak yaklaşık 8-10 bin yıl önce, Mezopotamya (günümüz Irak'ı ve Ortadoğu'su) civarındaki bölgede görüldüklerini tahmin ediyoruz. İkinci önemli büyüklükteki teknolojik devrimse Sanayi Devrimi'dir, 18. yüzyılın sonlarına doğru Büyük Britanya'da buhar makinesinin keşfi ve James Watt'la ilişkilendirilir. Sanayi Devrimi dev boyutlarda sosyal ve ekonomik adımların atılmasına yol açtı. Bu gelişmenin başlıca sebebi, elektrik ve giderek otomatikleşen makine teknolojisinin, iş gücünden tasarrufu beraberinde getirmesidir. Sanayi Devrimi, ekonomik büyümeyi ve insanoğlunun daha önceleri hiç görmediği kadar servet artışını mümkün kıldı.

Günümüzün sorusu, üçüncü bir devrimi yaşayıp yaşamadığımızdır: "Dijital Devrim". Bizler belki bugün, tarihçilerin 1000 yıl sonra Tarım ve Sanayi Devrimi'yle karşılaştıracakları türden, sosyal koşulların köklü bir değişimini yaşıyoruzdur. En azından, toplumun dijitalleşmesinin, biz insanların hayat şeklimizi ve birbirimizle olan ilişkilerimizi değiştirdiğinden şüphemiz yok. Bu değişimin boyutlarını günümüzde pek kavramış değiliz.

Bu değişimin ardında tabii ki pek çok itici güç bulunmaktadır ancak, mikroçipin ve internetin gelişimi hiç şüphesiz önemli iki dönüm noktasıdır. İnternetin gelişmesine yol açan teknolojinin kökenleri uzun

zaman öncesine dayanmaktadır ancak, internetin keşfinin 1969 yılında olduğunu söylemek mümkündür, o yıllarda US Advanced Research Projects Agency (ARPA) –günümüzde DARPA olarak bilinmektedir– araştırmacıları, California Üniversitesi ve Stanford Araştırma Enstitüsü arasında bir veri ağı kurdu. Sisteme ARPANET adı verildi. 1971 yılında bir tür elektronik posta (e-posta) oluşturuldu, iki yıl sonra da, veri trafiğinin dörtte üçü e-postadan ibaretti ve ARPANET, 40 farklı bilgisayar ağı içeriyordu. 1973 yılında University College London ağa bağlandığında, ilk kıtalararası bağlantı gerçekleşti. Aynı günlerde başka ülkelerde de benzer ağlar oluşturulmaktaydı ve bu bilgisayar ağlarını birbirine bağlamak için bir sistem geliştirildi. Bu sisteme, bugün de hâlâ kullanılan TCP/IP adı verildi. "İnternet" sözcüğünün kullanımı, bu tür bilgisayar ağlarının, daha büyük bir bilgisayar ağı oluşturması için birbirine bağlanmasına işaret eder. [1]

Günümüz internet kullanıcıları bu ilk versiyonu çok zor tanıyacaktır çünkü web sayfaları mevcut değildi ve tüm iletişim yalnızca metne dayalıydı. İnternetin popüler olmasını sağlayan büyük çıkışı, bilgisayar mühendisi İngiliz Tim Bernes-Lee gerçekleştirdi. Bernes-Lee, araştırma merkezi CERN'de bulunduğu sırada, çoğumuzun bugün internet olarak bildiği World Wide Web hizmetini geliştirdi. Berners-Lee'nin yaptığı, internetteki farklı kaynakları birbirine bağlayan bir hiper metin kullanmaktı; böylelikle dünyanın dört bir yanındaki kullanıcıların, bir tarayıcı aracılığıyla web sayfalarını gezebilmeleri sağlandı. İlk web sayfası 1991'de yayınlandı. Tarayıcılar HTML-Lisanı olarak bilineni, kullanıcı dostu siteler olarak yeniden biçimlendirdi, böylelikle metinler, resimler ve videolar mümkün olduğunca çok insana ulaşabildi.

2015'te, internetin ISP'ler (İnternet Servis Sağlayıcı) aracılığıyla kitlelere ulaşmasının üzerinden 25 yıl geçmişti ancak ilk gerçek anlamda yaygın tarayıcı olan Mosaic'le, ilk kez 1993 yılında tanıştık. 1996 yılında Hotmail ilk web tabanlı e-posta hizmetini başlattı ve 1998 yılında, arama motoru devi Google kuruldu.

Bir yandan internet küresel iletişimi mümkün kılarken, bir yandan da birleşik devrelerin gelişimi, internete bağlanmamızı sağlayan bilgisayar ve akıllı telefonlar gibi elektronik aletleri kullanmamızda belirleyici bir etkendi. İlk bilgisayarlar çok yer kaplıyordu. İngiliz matematikçi

Alan Turing, 1943'te pek çok kişinin ilk bilgisayar olarak kabul ettiği aleti yaptığında, bu bilgisayar neredeyse odanın tamamını kaplıyordu. Mikroçip olmasaydı, bu tür makineler, çok veri işleyemeyecek, hâlâ çok büyük olacaktı. Halkın çoğu da bu makineyi elde edemeyecekti. İlk bilgisayarlar, ayrık elektronik devrelerle birbirlerine bağlanabiliyordu, bu da makinede yer alabilecek devrelerin sayısını kısıtlıyordu. Bu durum, daha küçük ve güçlü makinelerin gelişimini engelliyordu.

Mikroçip teknolojisini geliştirme onurunun kime ait olduğu konusunda görüş ayrılıkları vardır, ancak bu konudaki önemli isim, 1958 yılında ilk prototipin Texas Instruments adına patentini alıp geliştiren ve pazara sunan Jack Kilby'dir. Kilby'nin katkısıyla, ayrık elektronik bileşenlerin sebep olduğu engel aşılmış oldu. Mikroçip, mikroişlem biriminin gelişmesini sağladı. Mikroişlem birimi, tüm merkezi işlem birimini içinde barındıran basit bir mikroçiptir, yani bilgisayarın bu parçası belirli bir programdaki talimatları yerine getirir.

Ayrık elektronik devreler sorununun çözülmesiyle giderek daha da küçülen elektronik ürünlerin üretimi mümkün oldu. Bu ürünler aynı zamanda daha fazla veri akışını daha ucuz bir biçimde işleyebiliyordu.

Bu, Moore Yasası'na kaynak olmuştur. Bu yasaya göre bir mikroçipin içindeki transistör sayısı her 24 ayda bir, iki katına çıkacaktır. 1965 yılında bu kehanette bulunan kişi, Intel'in kurucularından Gordon Moore'dur.[2] Önemi göz ardı edilemeyecek bu gelişme, bizlerin giderek küçülen elektronik birimlerde giderek büyüyen işlem gücü elde etmemizi sağlar. Bu durum, veri akışının işlenmesinde çok büyük sonuçlar doğurmaktadır, ki bu da internetteki özel hayatımız için büyük sonuçları beraberinde getirir, çünkü interneti oluşturan teknoloji aynı zamanda kullanıcıların her gün internete yüklediği verilerin yığınsal belleğinin oluşmasını mümkün kılar.

Nesnelerin İnterneti

İnternet hem profesyonel hem de özel hayatlarımızın iyice içine girdiği için mahremiyet tartışması köklü bir değişikliğe uğramıştır. Veri devriminden önce, (özellikle Soğuk Savaş yıllarında) bazı özel grupların izlenmesine rağmen ve Norveçliler farklı veri tabanlarında (örneğin

vergi kayıtları) kayıt altındayken yine de gündelik hayatımızda büyük bir anonimlik söz konusuydu. İnternet, akıllı telefonlar ve sosyal medyanın yükselişiyle birlikte, anonimlik çoktan ortadan kalkmıştır. Hâlâ "offline" olabilmek mümkün, ancak izlenmenin hem niteliksel hem de niceliksel olarak kökten değiştiğine hiç şüphe yok. Nitelikselden kastım, internette neyin özel alan olarak görüleceğinin net olmamasıdır ve niceliksel değişikliğin nedeni de internete konan kişisel verilerin dev boyutlara ulaşması ve işlenebilmesi için büyük kaynaklara ihtiyaç duyulmasıdır.

Gelecek yıllarda artış gösterecek olan dijitalleşme bu sorunu daha da büyütecek. Öncelikle internetin öneminin azalacağına inanmak için bir neden yok. "Nesnelerin İnterneti" (IoT) adını alan fenomene giderek daha çok şahit oluyoruz. Bu fenomen, gelecekte neredeyse herhangi bir şeyi internete bağlayabilme olasılığını içinde barındırıyor.

Samsung Electronics'in Yönetim Kurulu Başkanı B.K. Yoon, 2015'te şunları söylemiştir: "Beş yıl içerisinde, Samsung'un üreteceği bilgisayar donanımlı her şey internete bağlanacaktır."[3] Geleceğin evinin neye benzeyeceğini kafamızda canlandırmaya çalışalım: Normal bir ev internete bağlanabilen eşyalarla dolu olacaktır. Yakın bir gelecekte, teknoloji uzmanlarına göre, tüm fiziksel objelerin, nesnelerin –belki de bizim bile– internetine bağlanacağını söylemek yanlış olmaz.

Bunu başarmanın koşulları çok zor değil. Esasen yalnızca üç farklı bileşene ihtiyaç var.

- İnternette kendine ait bir kimlik (herhangi bir internet sayfası gibi).

  Bir verici (wi-fi kapsama alanı).

  Koku, hareket, ses ya da benzeri şeyleri kaydeden bir sensör.

Bir örnek verecek olursak: Diyelim ki bir bisiklet aldınız. Bunu, yukarıdaki üç bileşenle internete bağlayabilirsiniz. Bisikletinize ait bir kimlik, internete bağlanan bir verici (örneğin 4G), bisikletin kullanıldığını kaydeden sensörler, örneğin bisikleti uzaktan kontrolle (baterisi ve motoru varsa tabii ki) belirli bir yere yönlendirme olanağı.

Teknolojik olanaklar işin bir yönü. Sorulması gereken soru, bunların kullanıcıya kolay gelecek biçimde nasıl uygulanacağı. Örneğin bisikletinizi internete bağlamak faydalı bir şey olarak görülebilir tabii. Her şey bir yana, kullanımını ele alacak olursak, IoT'nin çok farklı biçimlerde kullanılabileceğini ve bunun da hayat şeklimize nüfuz edeceğini görürüz.

İlk olarak, nesnelerle iletişime girmemizi sağlayacak. Kullanılmış bir bisiklet alacak olursanız, ihtiyaç duyduğunuz verilere ulaşabilirsiniz. Bisiklet kaç kilometre gitmiş? Nerelerde kullanılmış? Kim kullanmış? Nasıl bakım görmüş? İkinci olarak, IoT nesneleri gözlemlemek ve denetlemek –vatandaşlar da dahil olmak üzere– için kullanılabilir. Örneğin kalp ameliyatı geçirmiş, kalp pili takılı bir hastanın kontrolünü düşünün. Kalp pili arıza çıkarır çıkarmaz, ambülansa otomatik olarak mesaj çekilebilir, ambülans da geriye, yolda olduklarına dair SMS yollar. Bu tür gözlemler, demans hastaları ya da küçük çocuklar için kullanılabilir; böylelikle hem aile fertleri hem de anne babalar daha kolay denetim sağlayabilir. Üçüncü olarak internet, arama işlemi için kullanılabilir: Anahtarlarım nerede? Ya da bisikletim nerede?

Dördüncü olarak, internete bağlı nesneler şehir planlaması, trafik, hava kirliliği ve etkin elektrik dağıtımı da dahil olmak üzere, nesnelerin kümelenmiş verisine dayanarak daha kolay halledilebilir. Kullanımın artacağı son bir alan da insanların oyun ve eğlence ihtiyacını karşılamaya yönelik olacaktır, yani *gaming*'e. Her birimizin, 2030'a kadar, internete bağlanan binlerce nesneye sahip olacağımız tahmin edilmektedir.[4]

Özel hayatla ilgili sonuçlar o kadar kapsamlı olacak ki, özel hayat rafa kaldırılmadıysa, en azından kavram olarak tamamen değişecektir.

İngiliz filozof Jeremy Bentham, 1700'lerin sonunda, panoptikon (eski Yunancada "bütünü gözlemlemek" anlamına gelir) düşüncesini, hapishaneler ya da başka kurumlar inşa etmek amacıyla ortaya attı. Bentham'ın fikrine göre, pasta dilimi şeklindeki demir parmaklıklı hücrelerden bir halka oluşturulacak, çemberin ortasında bir nöbet kulesi olacaktı. Tüm mahkumlar buradan gözlenebilecek, ancak kendileri gözlenip gözlenmediklerini bilemeyecekti. Bentham'a göre panoptikon "görünmez bir her şeye kadir olma" duygusu yaratacaktı. Panoptik kavramına, nesnelerin internetinin gelişiminden daha iyi bir örnek

verilemez. Vatandaşlara verilen hizmetin gelişiminde kullanılabildiği için bu yeni teknolojinin faydası çoktur ancak mesele, mahremiyeti nasıl koruyacağımızdır.

Dijital teknoloji ve internetin, devlet güçlerine, kişisel verileri kayıt altına alma ve izleme konusunda, tarihte daha önce hiçbir devlet gücünün sahip olmadığı bir biçimde sonsuz olanak sunduğu şüphe götürmez, Edward Snowden'ın itirafları bu doğrultuda korkunç bir resim ortaya koymuştur.

İzleme Teknolojisinin Gelişimi

Snowden'ın sızdırdıkları, ister ilgilenin ister ilgilenmeyin, mahremiyetin herkesin sorunu olduğunu gösteriyor. Ne yazık ki tartışma, Snowden'ın hareketlerinin ne kadar yasal olduğu ve bu yüzden de Snowden'ın ne kadar "hain" ya da ne kadar "kahraman" olduğu etrafında döndü. Bu tartışmanın konuyla alakasız olmadığı ortadadır ancak, en azından daha az önemli sayılırdı, sayılmalıydı. Bunun yerine, tartışma sızıntının özü hakkında olmalıydı, özellikle de Amerikalı ve Batılı istihbarat kurumlarının emriyle milyonlarca kişinin kapsamlı bir biçimde izlenmesi tartışılmalıydı.

Snowden'ı eleştirenler, onun ABD'ye zarar verdiğini, ülkenin düşmanlarına yardım ettiğini ve endişelerini dile getirmesinin başka yolları olduğunu öne sürüyor. Ne de olsa Amerika bir demokrasi ülkesi, orada istihbarat demokratik denetim altında ve kendi istihbarat kurumlarını demokrasiye karşı bir silah olarak kullanan pek çok ülkedekinin tersine, orada demokrasiyi koruma amacı taşıyor. Bu görüşler konuyla ilgili, belki de Snowden, NSA'ya ve onların gizli izleme programlarını kullanmasına dikkat çekebilmek için yanlış yöntemler kullandı.

Ancak meselenin açıkça bundan ibaret olduğu da söylenemez. Geçen yüzyılın en büyük ihbarcısı, "Pentagon Belgeleri"nin ardındaki isim, 1971 yılında Johnson yönetiminin, ABD'nin Vietnam Savaşı'ndaki rolü üzerine gerçekleri anlatmadığını ortaya çıkartan Daniell Ellsberg, Snowden'ın yaptıklarına olumlu yaklaşmış, bunun gerekçesi olarak da, ABD'deki siyasal iklimin 40 sene öncesinden çok daha farklı olmasını göstermiştir[5] Her halükârda bu tartışma, öncelikle Snowden'ın yap-

tıklarına değil, dijitalleşmeye neredeyse tamamen geçmiş ve istihbarat organlarının gelişkin teknolojiye sahip olduğu küreselleşmiş dünyada mahremiyetin en iyi nasıl korunabileceği üzerine odaklanmalıdır.

ABD'nin, modern internetin gelişiminden çok önce, dijital uydu teknolojisine dayandırdığı bir izleme geliştirdiğini unutmayalım. NSA ve GCHQ'dan* alınan onaylanmış bilgilere göre, 1960 yılllarında Sovyetler ve Doğu Bloku'nu gözetlemek amacıyla Echelon uydu projesi geliştirilmiştir. Proje ABD, İngiltere, Yeni Zelanda ve Kanada arasında yapılan bir ortak çalışmanın ürünüdür. Bu uydu teknolojisi –örneğin sinyal istihbaratı ("SIGNNT")– sinyal toplama işlevini yerine getirir, örneğin kripto analizi ve deşifrenin çok önemli yer tuttuğu radyo sinyalleri toplamak gibi. Echelon pek çok uydu sistemini eşzamanlı olarak yakalayabilen ve bir gün içerisinde üç milyar gibi bir sayıdaki mesajın sinyallerini toplayabilen, türünün tek yazılım sistemi olarak tanımlanmıştır. Pratikteki önemine şöyle dikkat çekebiliriz: Stasi, 20 kişinin 24 saat gözetlenmesi için bir kişiye ihtiyaç olduğunu hesaplamıştır. Echelon'la bir kişi 24 saat boyunca 10 bin kişiyi izleyebilir.[6]

ABD istihbaratı ve Echelon üzerine en çok yazan kişilerden biri olan James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* [Sır Küpü: Çok Gizli Ulusal Güvenlik Teşkilatı'nın Anatomisi] adlı kitabında, yerel baz istasyonları aracılığıyla veri yakalayıp toplayan bir sistemi tanımlar. Aynı tanım, Avrupa Parlamentosu'nun (2000 ve 2001) bir raporunda da karşımıza çıkar. Burada iddia edildiğine göre, "Echelon sözcüğü birçok bağlamda kullanılmıştır ancak delillerin bize sunduğu, bu ismin sinyal istihbaratı toplama sistemine verildiği doğrultusundadır". Sistem telefon konuşmaları, fakslar, e-postalar ve uydu sinyalleri aracılığıyla yapılan diğer veri akışını yakalayabilmektedir.[7]

Başka bir deyişle Echelon, modern anlamdaki ilk kitle istihbaratı programı olarak tanımlanabilir ve varlığı kabul edilmiş olsa da program hâlâ büyük bir sır perdesi altındadır.

---

* Government Communications Headquarters: Siber saldırılara ve tehditlere karşı kurulmuş İngiliz güvenlik ve istihbarat kurumu –yn.

Ancak son yılların gerçek anlamdaki en büyük tartışması, Edward Snowden ve NSA'nın interneti oldukça müdahaleci bir biçimde izlemek amacıyla programlar geliştirdiği hakkındadır.

İstihbarat kurumunun şefi James Clapper'a ait, çok kullanılan bir alıntı, izlemenin boyutlarının nerelere geldiğini göstermektedir: "Her şeyi toplayın."[8]

Şifrelemenin Önemi

Guardian, ABD ve İngiliz istihbaratlarının teknolojiyi nasıl kullandıklarını, daha doğrusu, teknolojinin altını nasıl oyduklarını anlatmaya çalışmıştır.[9]

İnternette, özel hayatın temelini sarsarak yaptıkları şeye şifreleme denmektedir. "Kriptolama", etimolojik olarak, gizli olan ya da saklanan şey anlamına gelmektedir. Bu, bilgiyi koruma amaçlı bir araçtır; mesajları, paylaşmasını istemediğimiz kişiler için anlaşılmaz hale getirmek demektir. Tarihsel olarak şifreleme, ulusal güvenlik için önemli bilgileri koruma amacı taşıyan etkili bir araçtır ancak şifreleme önemsiz sayılabilecek alanlarda da etkilidir çünkü söz konusu kişinin özel bilgiyi paylaşmaya niyeti yoksa, bilgi ne kadar önemsiz olursa olsun ona ulaşılamıyor olması gerekir.

Guardian NSA'nın, internetin yapısının ("the fabric of internet") altını oyabilen ve bildiğimiz şekliyle interneti bozan bir teknolojiyi geliştirdiğini iddia etmektedir. Gazeteye göre, NSA ve GCHQ, özel bilgiyi koruma amacıyla şifrelenmiş bilgiyi kırabilmek için oldukça gelişmiş, büyük teknolojik kaynaklar kullanmaktadır. Ayrıca teknoloji şirketleriyle gizliden yapılan ortak çalışmalar için de büyük kaynaklar kullanmaktadırlar, bu işbirliğinin amacı ürünleri zayıflatmaktır. Başka bir deyişle, istihbarat örgütleri, milyonlarca insanın, *online* olan özel verilerini koruduğuna inandığı şifrelemelerin pek çoğunu kırmış bulunmaktadır. Pek çok ticari şirket, kendi politikalarına ters düşen bir şekilde, verileri teslim ederek, kendi müşterilerinin güvenini boşa çıkarmıştır.[10]

ABD ve İngiliz istihbaratının her türlü şifrelemeyi çözdüğü de doğru değildir. Snowden'ın *Guardian* okurlarına anlattığı gibi, NSA büyük

ihtimalle pek çok şifreleme protokolünü kırmayı başarabilse bile (bu konu hâlâ tartışmalı), sağlam bir şifreleme güvenliğin halen en büyük garantisidir. Ancak, NSA ve GCHQ, öncelikle şifrelemenin uluslararası standartlarını etkileyebilir çünkü yapıyı ve sistemi tanıyorlar ve ikinci olarak, program yazılım sistemlerine arka kapılar inşa edilmesini sağlayabilirler. *Guardian*'a göre, ticari aktörlerle yapılan çok gizli işbirlikleri sayesinde her iki durum da gerçekleşmiştir.

Bu bağlamda "arka kapı" tam da çağrıştırdığı şeyi yapmaktadır. Bu, bilgiye ulaşmak için gizli bir giriştir ve bunu bir evle karşılaştırabiliriz: Dört girişi olan bir ev yapmak istediğinizi gözünüzde canlandırın. Bu girişler için anahtarlarınız var. Anahtarları kriptolamaya benzetebiliriz. Ancak evi inşa edenler, anahtarı ya da denetimi sizde olmayan, bodrumdan gizli bir giriş, bir kapı yapmışlarsa bu, siz farkında olmadan özel verilerinize (e-posta, belgeler vb.) ulaşabilecekleri anlamına gelmektedir, hem de şifreniz olmasına rağmen.[11] Ama bu gerçekten büyük bir sorun mudur?

Otoritelerin böylesi "arka kapı"lara ulaşabilir olması doğru sayılmaz mı?

2015 yılının Aralık ayında, California San Bernadino'da meydana gelen terör olayını takiben ortaya çıkan tartışma güncel bir örnektir. Bu olayda 14 kişi ölmüş ve 22 kişi yaralanmıştır. Olayların hemen ardından, FBI şüphelinin iPhone'undaki verilere ulaşabilmek için Apple firmasından izin istemiştir. FBI açısından baktığımızda, araştırmanın bir parçası olarak bunu istemeleri tabii ki anlaşılır bir şey, ancak Apple, iPhone'un şifresini vermenin özel hayata karşı genel bir tehdit oluşturabileceğini savunmuştur.[12]

Bu dava, ikilemi her ne kadar gözler önüne serse de San Bernardino olayı ile genel olarak arka kapılar arasında önemli bir fark bulunmaktadır. San Bernardino olayında iPhone'da arka kapı yoktur ve FBI'nın istediği, Apple'ın sıradan bir veri hırsızlığına uygun hale gelecek şekilde telefonu güncelleme imkânını kullanmasıdır ve Apple, her zaman için buna karşı çıkmıştır. 28 Mart 2016'da *PC World*, FBI'ın, Apple'ın yardımı olmadan iPhone'un kodunu kırmayı başardığını bildirmiştir.[13] Bu olay, arka kapıların yetkililer için ne kadar yararlı olabileceğini tüm

açıklığıyla göstermektedir ancak arka kapılar, özel hayat hakkıyla ilgili olan herkes için çok sorunlu olabilir.

Yetkililerin arka kapılara erişiminin olduğunu kabul ederseniz, bir ülkedeki anahtar üreticilerinin devletin belirlediği ekstra bir ana anahtar kullanacağını söylemiş olursunuz. Haliyle bu anahtar önceden belirlenecek ve (sadık olmayan fabrikaların yaptıkları hariç) tüm kilitleri etkileyecektir. Arka kapıların gündeme gelmesiyle ortaya çıkacak bir diğer sorunsa, biz vatandaşların, bize ait bilgilerin artık özel olarak kalıp kalmayacaklarını bilememizdir. Bunun nedeni, böyle bir ana anahtarın kopyalanmasının kolaylığı ve ardında hiçbir iz bırakmadan kullanılabilmesidir. Yetkililerin, arka kapı sisteminde yaptıkları özel hayat ihlallerinin boyutları o yüzden belirsiz olacaktır. Ayrıca bu tür arka kapıların sıradan suçlular ya da yabancı güçlerin eline geçmeyeceğinin garantisi nasıl verilebilir?

Arka kapıların getireceği sorunların biraz daha altını çizecek olursak: Şifreleme, veri sistemlerinde güvenilirliği korumak için kullanılır, örneğin bankaların işlem listeleri. Bir arka kapı olması durumunda, pratikte biri, bankayı ardında hiçbir kişisel iz bırakmadan soyabilir çünkü uydurma bir işlemi korumak için ana anahtarın mı, yoksa bankanın kendi anahtarının mı kullanıldığını belirlemek mümkün olmayacaktır.

Bu nedenlerden dolayı, arka kapıları mutlaka olması gereken bir şey olarak görmek zordur. Bunlar, sistemin tüm güvenliği ve internetin güvenilirliği için kesinlikle çok zararlıdır. Özel bilgilerin şifrelenmesi ve güvenliği, internet kullanıcıları için elzemdir.

Bir evin anahtarları analojisini tekrar kullanacak olursak: Örneğin, belirsiz sayıda yetkilinin gayet güzel bir şekilde, hiçbir iz bırakmadan ve elinde arama emri olmadan evlerimize girdiği bir toplumu kabul eder miydik? Böyle bir kurum, birini bile kaybetmeden çok sayıda ana anahtarı elinde ne kadar uzun süre tutabilir? Dünyanın önde gelen istihbarat çevrelerinin, internetteki özel hayatı ihlal edecek bir teknolojiyi ele geçirmiş olmaları bugün bile endişe verici bir durumdur çünkü kriptolama teknolojisinin gizliliğinin ne kadar ihlal edildiğini bilmek bile bizim için sorun çıkarabilir.[14]

Panama Belgeleri adıyla anılan ve Nisan 2016'da yayımlanan sızıntının sonrasında ortaya çıkan büyük ifşaatlar, kriptolamayı savunmanın ne kadar önemli olduğunu bir kez daha göstermiştir. The International Consortium of Investigative Journalists [Araştırmacı Gazetecilerin Uluslararası Konsorsiyumu], vergi cennetlerinin nasıl kullanıldığı ve ekonomik suçlar hakkında kapsamlı fikir veren milyonlarca belgeyi inceledi. Bu olaylar tabii ki kamunun yararınadır.

Peki, şifreleme konuyla ne bakımdan ilgilidir?

Cevap, her yeriyle.

Panama Belgeleri, söylendiğine göre, belgelere ulaşabilen güvenilir bir çalışan aracılığıyla sızdırılmıştı ve bu kişinin amacı suçları ortaya çıkarmaktı. Ancak, John Doe* adını kullanan söz konusu kişi, bilgiyi alan *Süddeutsche Zeitung*'daki gazeteciye konuşmaları için bir koşul öne sürmüştü: Tüm haberleşme şifrelenmiş dosyalar aracılığıyla olacaktı ve asla fiziksel olarak görüşmeyeceklerdi. Bu şartları anlamak çok kolay çünkü sızıntılarda, suç çevrelerinin çok güçlü liderlerinin adı geçiyordu ve bu yüzden ihbarcının hayatı, kimliği bilinecek olursa, çok büyük tehlikedeydi.

Panama Belgeleri'nin ortaya çıkmasının koşullarını şifreleme sağlamıştır.

Hukukçu Bård Standal, Facebook sayfasında, görüşmelerin nasıl yürüdüğünü ve kriptolamanın neden belirleyici olduğunu anlatır:

> Obermayer ve John Doe, her görüşme için şifrelenmiş başka kanal kullandılar. Tüm kayıtları sildiler çünkü mesaj kanallarında bunu yapmak mümkün. Belgeler şifrelendiğinde, ICIJ belgelere 2-faktörlü kimlik doğrulama arama motoru oluşturdu. Bunun linki, söz konusu medya organlarıyla (örneğin Norveç'te *Aftenposten*'la) şifrelenmiş e-posta aracılığıyla paylaşıldı. Farklı ülkelerden gazetecilerin, kendilerinin oluşturduğu şifrelenmiş bilgiyi paylaşabilecekleri, gerçek zamanlı bir chat kanalı da mevcuttu. Yetkililer arka kapılara sahip olsalardı, ne Panama Belgeleri ortaya çıkardı ne de John Doe şifrelenmiş chat kanalına güvenebilirdi. "Yetkililerin

* John Doe, ABD'de gerçek kimliği belirlenemeyen ya da yasal gerekçelerle gizli tutulması gereken kişiler ve kimliği saptanamayan cesetler için kullanılan bir takma isimdir -yn.

> şifrelenmiş haberleşmelere ulaşmasının benim için mahsuru yok – benim gizli saklım yok" diye düşünenlere, durumun John Doe için farklı olduğunu hatırlatmakta fayda var. Bir Rus polonyum zehriyle ölmek pek de keyifli bir şey olmasa gerek.[15]

Kasım 2015'te dijital duyarlılık konusundaki araştırmalarını sunan Uluslararası Aydınlatma Komisyonu'nun (NOU 2015:13), kriptografi ve arka kapıların gelişkin kullanımı sorusu hakkında aynı sonuca varması bu yüzden sevindiricidir. Üstelik komisyon Norveçli yetkilileri, şifrelemenin düzenlenmesi ve yasaklanmasına karşı uluslararası çalışmalara katılmak için teşvik etmektedir.[16]

Gelecekteki etkileşim için kesinlikle büyük anlam taşıyacak olan epey güvenli teknoloji "blok zinciri" teknolojisidir. Özünde, bu teknoloji, güvene dayalı ilişkinizin olmadığı kişi ya da kurumlarla bağlantı kurmanızı mümkün kılar. Bu durum, özellikle finans kurumları ile aracıları etkileyecektir ancak bu, birbirimizle etkileşimimizin tümü üzerinde devrim niteliğinde etki bırakacak potansiyele sahiptir. Büyük miktarda hisse senedinin açık pazarlardan özel pazarlara aktarılması gibi, sık sık adı geçen *Bitcoin* de blok zinciri teknolojisine örnektir.

Bu teknolojiyi eşsiz kılan, dolandırıcılık ya da usulsüzlükler yapmayı çok zorlaştırması, pek çok kişiye göre de imkânsızlaştırmasıdır. Bunun sebebi, farklı halkaların, değiştirilemez ya da bir kez uygulamaya konduğunda etkilere kapalı, emsalsiz veriler içermesidir. Bu halkalar bu şekilde birbirine bağlıdır, yani her bir halka başka bir halkayla birleşerek diğer halkalara bağlanır. Uygulamaya konmuş bir halkayı birileri değiştirmeye kalkıştığında sistem (blok zinciri), manipülasyonu anında haber verir. Tam da bu yüzden teknoloji, dijital işlemleri onaylama tarzımızda köklü bir değişiklik yapmaktadır.

Norwegian University of Science and Technology araştırmacıları Simon McCallum ve Mariusz Nowostawski, *Aftenposten*'da bunun nedenini şöyle açıklıyor:

> Böyle bir zincirin en zayıf halkası her zaman insanlardır. Hata yaparız, bilerek ya da bilmeyerek. Ancak insani öğeyi ortadan kaldırmak mümkün mü, ya da en azından, bizim işin içine karışmamızın etkisi azaltılabilir mi? Cevap, evettir. Blok zincirinin yardımıyla bu mümkün. Blok zinciri, insanlarla güvenli ve doğrulanmış bir algo-

> ritma (bir dizi hesaplama) arasındaki itimada dayalı ilişkinin yerini tutar. Ancak ortaya çıkan sorun şudur: Yazılım hata yapabilir mi?
>
> Cevap, hayırdır çünkü yazılım kendini matematik yardımıyla denetler. Bu da hile katılması çok zor anonim ve saydam bir işlemle sonuçlanır. Dolandırıcılık girişimleri hemen ortaya çıkar çünkü hilekârlık, çok sayıda insan ve makine için anında görünür hale gelir.[17]

Blok zinciri teknolojisi ve onun pek çok etkisi daha büyük bir kitabın konusu olabilir, ancak mahremiyet tartışması üzerine iki güncel etkisinden söz edebilirim. Öncelikle blok zinciri, isimsiz işlem ve ilişkilerin önünü açar, ki bu da vatandaşların mahremiyeti açısından olumludur. İkinci olarak, blok zinciri teknolojisi, NSA itirafları ve Panama Belgeleri'nde olduğu gibi, sansürlenmesi neredeyse mümkün olmayan bir kanal oluşturabilir. Bu durum, ihbarcılar ve basın özgürlüğü için olumludur ancak aynı zamanda kişisel, hassas bilgileri bu teknoloji tarafından ortaya dökülecek insanların özel hayatına karşı büyük bir tehdidi de beraberinde getirir. Sistemin parçası olmayan kişiler bile, hassas bilgilerinin geri dönüşü olmayan bir şekilde ortalığa dökülmesi riskiyle karşı karşıya kalabilir, bu da mahremiyeti çok büyük bir riske atacaktır.

Blok zincirine dayalı çözümler, henüz gelişim aşamasındadır ve teknolojinin nasıl ve ne kadarının uygulamaya konacağını söylemek hâlâ zordur ancak, gelecekte birbirimizle etkileşime girme tarzımızda büyük etkisi olacak bir teknoloji olduğu bugünden ortadadır. Hem olumlu hem de olumsuz etkileri olabilecek bu teknolojiyle buluştuğumuzda, özel hayatımızı koruma amacıyla tedbirli olmamız gerekmektedir.

Üst Veri (Metadata)

Üst veri kavramı, Snowden'ın ifşaatlarından bu yana sıkça kullanılan bir ifadedir. Üst verinin anlamını açıklamak için eski CIA şeflerinden Michael Haydens'a ait, çok şey anlatan tartışmalı bir alıntı kullanılabilir: "Üst veriye dayanarak insan öldürdük." Birbirine bağlandığında üst veri, SMS'ler, e-postalar ya da telefon görüşmelerindeki somut içeriği bilmeye gerek kalmadan, kişinin hareketleri hakkında çok belirgin bilgiler verebilir.

Başkan Barack Obama, izleme skandalının ardından NSA'nın telefon görüşmelerini dinlemediğini, kişisel SMS'ler ile e-postaları okumadığını iddia etmişti. Bu tamamen doğru olsa da dikkatleri üst verinin öneminden başka yöne çekme girişimidir. Demeç tartışmalıdır çünkü NSA, "üç derecelik ayrım"* kararı aracılığıyla içerik verilerine ulaşabilir. Şüpheli biriyle ilişki kurmuş insanlarla ilişki kuranların tüm yazışmalarını gözden geçirebilir. Şüpheli biriyle bağlantısı olan kişiyle bir ilişkiniz varsa, ya da arkadaşıysanız, NSA pratikte sizin de kişisel verilerinizi kontrol etme yetkisine sahiptir, yani milyonlarca kişi bu tür bir izlemeye takılmıştır.[18]

Üst veri ya da metadata (Yunanca *meta* "hakkında", Latince *data* "bilgi"), başka bilgileri anlatan ya da açıklayan bilgidir.

Üst veriyi açıklamanın en iyi yolu bir mektubu örnek vermektir: Arkadaşınıza mektup yazıp yollarsanız, zarfın üzerindeki bilgi *meta* (hakkında), mektubun kendisi *data* (veri) olacaktır.

Teknoloji Kurulu ve Veri Koruma Kurumu 2014 yılındaki raporunda sadece üst veri için bir bölüm ayırmıştır. [19]

Fenomeni şöyle tanımlarlar:

Üst veri, dijital ekosistemdeki bir bilgi kaynağını, örneğin e-postayı tanımlayan, açıklayan, yerini belirten ya da ona erişmeyi, kullanmayı ve onun yönetimini kolaylaştıran bilgidir. Başka şeylerin yanı sıra, e-postanın kimden geldiğini, kime yollandığını anlatır. Bir e-posta alışverişinde üst veri, tipik bir biçimde şu bilgileri içerir: Yollayan ve alıcının adı, e-posta adresi, IP adresi ve sunucu zamanı, tarih ve zaman dilimi. E-postanın ekindeki dijital resim de bir üst veriye sahiptir ve şunları anlatır:

> Resmin ne zaman çekildiği (kamera, sahibini tanıyorsa fotoğrafçının kim olduğu)
>
> Resmin nerede çekildiği

---

* Three degrees of separation: Dünyadaki herhangi iki insanın, birbiriyle ilişkili en fazla altı insan mesafesinde bağlı olduğunu öne süren "altı derecelik ayrım" (six degrees of separation) teorisinden yola çıkarak, NSA'nın hedefindeki kişiye ulaşmak için onunla en az üçüncü dereceden ilişki kurmuş insanların bilgilerini topladığı istihbarat yöntemi -yn.

Resim dosyasının teknik bilgileri (pikseller, boyut, çözünülürlük, yönelim)

Kamera modeli ve kamera ayarları

Guardian, konunun ne anlama geldiğine dair somut bir örnek sunmak için, internet sayfasına çok iyi bir resim koymuştur. Resmin altında, @Guardian US'nin twitter mesajlarını tanımlayan üst verinin kısa versiyonu bulunmaktadır. Üst veriye erişim, genellikle hizmeti sunanlar aracılığıyla mümkündür, bu durumda Twitter aracılığıyla. Üst verilere yapısal formatta -ya ham metin olarak, ya XML olarak ya da başka formatlarda- erişilebilir. Bilgisayarınız ve telefonunuz, hangi internet sitelerine ne zaman girdiğiniz dahil olmak üzere, sürekli üst veri üretmektedir.


```
{
  "created_at": "Mon Jun 10 21:09:19 +0000 2013",
  "id": 344199622916448260,
  "id_str": "344199622916448256",
  "text": "Need to catch up? Our complete #NSAFiles coverage is here: http://t.co/iZPkknopxk",
  "source": "<a href="http://www.socialflow.com" rel="nofollow">SocialFlow</a>",
  "truncated": false,
  "user": {
    "id": 16042794,
    "id_str": "16042794",
    "name": "GuardianUS",
    "screen_name": "GuardianUS",
    "location": "New York",
    "description": "Featuring the Guardian's US coverage, conversations and reporters.",
    "url": "http://t.co/eqPiqNUSme",
    "protected": false,
    "followers_count": 55597,
    "friends_count": 509,
    "listed_count": 2414,
    "created_at": "Fri Aug 29 14:52:08 +0000 2008",
    "favourites_count": 860,
    "utc_offset": -18000,
    "time_zone": "Eastern Time (US & Canada)",
    "geo_enabled": true,
    "verified": true,
    "statuses_count": 41567,
    "lang": "en",
    "contributors_enabled": false,
    "is_translator": false,
```


Kaynak: *The Guardian*

Üst veriyi işleme olanağının artışı aslında kitlesel izlemenin ardındaki itici güçtür. Küçük grupların ya da bireylerin detaylı gözetlenmesinin yerini kitlesel izleme, yani vatandaşların gönderdiği ya da aldığı her bir e-postanın, SMS ve telefon görüşmelerinin saklanması almıştır.

Peki, bu tür bilgilerin saklanması aslında bir sorun mu?

Bu veriler SMS, e-posta ya da telefon görüşmelerinin içeriği hakkında bir şey söylemiyor. Doktoruma belli bir zamanda bir e-posta yolladığımı devlet ya da diğer kişiler kaydetmiş olsa bile bu bilgiler, doktorumla ne görüştüğümü açığa vurmaz etmez. Yoksa vurur mu?

Olaya tek başına bakacak olursak bir sorun yok. Sorun, üst verinin üst üste konmasıyla hareketiniz hakkında pek çok şeyi açığa vurmasında; neredeyse özel yazışmanızın içeriğini ifşa edecek kadar. Bilgisayar uzmanı Jacob Appelbaum'un işaret ettiği gibi: "Bir araya getirilen üst veriler içeriktir."[20]

Günlük hareket kalıplarımızın birkaç kez gözlenmesi, belli bir vatandaşa atfedilecek özgün bir düzeni ortaya çıkarmaya yeter.

Nature'da çıkan bir makaleye göre, MIT ve Louvain Üniversitesi'ndeki araştırmacılar, nerede, ne zaman (lokasyon metadatası) bulunduğunuza dair günde sadece dört gözlemin, vatandaşların özgün kimliğinin yüzde 95'ini ortaya koyabildiğini göstermiştir. Bu ilginçtir, çünkü cep telefonlarımız nerede bulunduğumuza dair bilgiyi sürekli yaymaktadır; bu bilgi, sadece üst verilerimize bakılarak kim olduğumuzu tanımlayabilir.[21]

Telefon operatörlerinden bu tür üst verilere erişim büyük ölçüde başkaları için de mümkün olduğundan, bu sorun giderek büyümektedir. Akıllı cep telefonlarının yaygınlaşması, internetle iletişim kurabilen, bu yüzden de elektronik ayak izleri bırakan çeşitli uygulamaların çapraz bağlantı kurmalarını sağlar. Üst veriler bir araya getirildiğinde bilgi, vatandaşların hareketlerini büyük ölçüde ortaya çıkaracaktır.

Doktoruma gönderdiğim, görünürde sınırlı bilgiyle ilgili örneğe geri dönelim. Bu bilgi tek başına, içerik hakkında bir şey söylemez.

Ancak bu bilgi, benim hareket seyrime bağlı başka üst veriye çapraz bağlantıyla bağlanırsa, aniden müdahaleye elverişli bir hale dönüşüverir. Doktorla yazışmamın hemen ardından HIV bilgisi içeren bir internet sayfasına girmişsem, sonra da eczaneye e-posta yollamışsam ve bu bilgiler arasında çapraz bağlantı yapılırsa üst verilerden çok şeyin okunabileceği ortadadır. Başka bir deyişle, *Wired*'da yayımlanan makalenin örneklediği gibi, zamanla toplanan üst veri, kiminle sevgili olduğumuz, kimlerle ilişkimizin olduğu, nerede çalıştığımız, nerede

bulunduğumuz ve hangi meselelerle ilgilendiğimiz de dahil olmak üzere, hayatımız hakkında detaylı tanımlar sunar.[22] *Wired,* NSA'nın üst verileri toplayıp saklamasını "kişisel ilişkilerin ulusal veritabanı"na benzetir.[23]

Üst veri sorunsalını bu kadar büyük yapan bir dizi etken vardır. Dijital bilgiye erişim ve kullanımda patlama yaşanmakta, her şey büyük miktarlarda üst veri içermekte, bu da yine, bilgiyi birbirine bağlamayı kolaylaştırmaktadır. İnternet haberleşmesinin yüzde 90'ı ABD aracılığıyla gerçekleşmektedir, *online* bilginin çoğu, az sayıdaki ABD şirketi (bulut hizmetleri diye bilinen şirketler) aracılığıyla saklanmaktadır.[24] Ayrıca üst verinin işlenmesi, içerik bilgilerine kıyasla çok daha ucuz ve kolaydır. İlki genel özellikler açısından daha yapısaldır, bu da bilgisayarın verileri kolayca işlemesini sağlar ve yorumlamak için daha az kaynak kullanımı gerekir. İçerik verilerinin tersine, üst verinin işlenmesi için, dil ve kültür hakkında pek fazla bir şey bilmeye gerek yoktur. Teknoloji Kurulu ve Veri Koruma Kurumu'nun mahremiyet raporunda özetlendiği üzere üst veri, özelliklerinden dolayı, modern istihbaratın bilgi kaynağı olmuştur, teknolojik gelişimin de bu verilerden faydalanmayı kolaylaştırdığını görüyoruz.[25]

İnternetin Düzenlenmesi

Bu bölümün örneklediği gibi, modern toplumda internetin önemini ne kadar abartsak az, popüler kültür de bunu sık sık işliyor. İnternetin gelişimine uygun olarak, dijital duyarlılıkla Hollywood da ilgilenmeye başlamıştır. *Die Hard 4* filmi (2007) dijital duyarlılığı göstermeye çalışan bir popüler kültür örneğidir.

Konunun çıkış noktası, ABD'nin altyapısına yönelik, felaketle sonuçlanacak büyük bir ***hacker*** saldırısıdır. Öykü oldukça abartılıdır, film on yıllık olmasına rağmen zamanın ruhunu etkili bir biçimde yakalamaktadır. Ulusal yetkililer siber güvenliği iyileştirmek için çalışmaları önemli derecede artırmıştır. Bu çalışmaya, artan izleme aracılığıyla interneti denetleme arzusu eşlik eder.

Günümüz internet düzenlemeleri, çokuluslu ve oldukça açık olmasıyla özgün bir nitelik taşır. Somut olarak söylersek, günümüzün küresel interneti ICANN tarafından organize edilmektedir. ICANN'ın açılımı

İnternet Tahsisli Sayılar ve İsimler Kurumu'dur. ICANN, Amerika California'da bulunan, kâr amacı gütmeyen bir kurumdur, internet adreslerinin (DNS-isim ve protokol parametrelerinin) küresel tahsisini organize etmek amacıyla 1998 yılında kurulmuştur. "*One world. One internet.*" düsturuyla ortaya çıkmış, açık, sansürsüz ve küresel bir interneti korumak için çalışmıştır. Tam tersi bir şekilde, günümüz küresel internetinin dağılacağı ve daha küçük, kapalı bir ağın onun yerini alacağı korkusu gerçekten hissedilmektedir. Özellikle Rusya ve Çin gibi otoriter devletler günümüzdeki düzenden hoşnut değiller, Uluslararası Telekomünikasyon Birliği (ITU) yönetiminde, BM (Birleşmiş Milletler) öncülüğünde bir düzenleme istemektedirler. Böyle bir örgütlenme, internetin nasıl düzenleneceğinin yanı sıra, internete erişimin sansürü konusunda ülkelerin etkili olmasını da kolaylaştıracaktır. ABD ve AB bu politikaya karşı çıkmaktadır, özgür interneti sürdürmeyi zorlaştıracağını öne sürerek BM'nin düzenlemelerini istememektedirler.

Özgür internetin koşulu olan ağ tarafsızlığı, bugünlerde Avrupa'da yürütülen önemli bir paralel tartışmadır. Ağ tarafsızlığı, prensip olarak servis sağlayıcıları aracılığıyla tüm internete erişim sağlayabilmeniz, trafikte öncelik hakkını sunan ağlar/uygulamaların bulunmamasıdır. Ulusal Haberleşme Müdürlüğü NKOM, ağ tarafsızlığını somut olarak tanımlamak amacıyla üç net kural belirlemiştir:

1. İnternet kullanıcılarının belirli bir kapasite ve kalitede internet bağlantısına sahip olma hakkı vardır.
2. İnternet kullanıcılarının aşağıda sıralananlara erişim sağlayan internet bağlantısına sahip olma hakkı vardır:

   İstedikleri içeriği alma ve sunma.

   İstedikleri hizmetleri ve uygulamaları kullanabilme.

   İnternete zarar vermeyecek istedikleri yazılımları kullanma, aletlere bağlanma.
3. İnternet kullanıcılarının uygulama türü, servis, içerik tipi ve gönderenle alıcının kim olduğuna bakılarak yapılabilecek ayrımcılıktan muaf internet bağlantısına sahip olma hakkı vardır.[26]

Aynı zamanda ağ tarafsızlığı, Avrupa Parlamentosu'nun tarafsızlığı istediğini belirten kararına rağmen, AB'nin baskısı altındadır. 4 Kasım 2015 tarihli *Bergens Tidende* gazetesinde, yorumcu Frode Bjerkestrand, Avrupa Parlamentosu'nun kararının ağ tarafsızlığı için neden büyük bir sorun oluşturduğundan söz eder.[27] Parlamento ağ tarafsızlığına desteğini her ne kadar ifade etmiş olsa da, yasa kendini yadsıyan bir istisnaya yol açmaktadır; pratikte bu, kaynakları güçlü şirketlerin Avrupa Parlamentosu'nun korumak istediğinin altını oyması anlamı taşır. Bu karar büyük yankılar uyandıracaktır.

Günümüzün kırılgan internet düzenlemelerinin eksikleri vardır ve Batılı istihbarat örgütleri eylemleriyle ağ bütünlüğünün altını oymaya katkıda bulunmuşlardır. İnternetin olabildiğince özgür işlemesini sağlayan düzenlemeleri getirmeye devam etmek ve ifade özgürlüğünü kısıtlamak isteyen ülkelerin interneti düzenlemelerine izin verecek gelişmelerin karşısında durmak önemlidir. Ancak bunu gerçekleştirmek için, Batılı toplumların ağ tarafsızlığını koruyacak gücünün olması, aynı zamanda, internette özel hayat hakkına yalnızca teoride değil, pratikte de saygı gösterilmesi için yasal altyapıyı güncelleyip güvenilir hale getirmeleri gerekmektedir.

"Unutulma Hakkı"

Bir yanda ifade özgürlüğü, bir yanda çoğunlukla resmi itibarı korumaya işaret eden hakaret yasaları (özel hayat) arasında uzun zamandır bir gerilim vardı, özellikle internet, Google gibi arama motorlarının kullanımı bu gerginliği iyice artırdı.

Brandeis ve Warren, İkinci Bölüm'de söz edildiği gibi, gazetelerin kamu malı olmasının özel hayat için doğurduğu sonuçları tartıştı. Bu tartışma bugün daha da önem taşır çünkü, internette herkes her şeyi paylaşabilir, sonra bu sadece birkaç saat içinde, gerçekliğini kontrol etme fırsatı olmadan milyonlarca kişiye ulaşabilir. İnternette yazılıp dağıtılanların çoğu, redaktörün sorumluluk alanına girmemektedir. Yazılar internette sonsuza dek saklanabilir, insanların resmi itibarını zedeleyecek bilgiler içerebilir, ancak aynı zamanda kamuoyunun yararına da olabilir ve ifade özgürlüğü açısından korunur.

İfade özgürlüğü ve mahremiyet arasındaki mevcut gerilim, google'lamak olarak bilinen aramaların kapsamlı kullanımıyla birleşince, arama sonuçlarının silinmesi ya da değiştirilmesine (unutulma hakkı) Google'ın olumlu yaklaşması talep edilmektedir.

AB Mahkemesi Mayıs 2014'te, AB vatandaşlarının, söz konusu kişiyi ilgilendiren bilginin yanlış, geçmişte kalmış, alakasız ve yetersiz olduğu durumlarda, arama motorlarının arama sonuçlarındaki kişisel bilgileri kaldırmasını talep etme hakkı olduğuna karar vermiştir.[28]

Dava, İspanyol bir gazetenin, González'in bir borç anlaşmazlığına karıştığı iddiasıyla ilgilidir. İlginç olan, haberin doğruluğunun sorgulanmamasıdır, mahkeme González'in, bilginin ağ tarayıcıdan silinmesine tamamen hakkı olduğunu belirtmiştir.

İspanyol Veri Koruma Kurulu'na göre gazete suçlu değildir çünkü dosyanın yayımlandığı tarih itibarıyla bilgiler doğrudur, ancak Google, arama motorundan gazetenin bağlantısını silmek zorundadır. Google kendi saklamadığı bilgiler için bir sorumluluk taşımadığını öne sürmüştür. AB Mahkemesi yine de, kendi aramalarında ortaya çıkan bilgilerden arama motorlarının sorumlu olduğu konusunda ısrarlıdır.[29] Son karara göre, ulusal kurumlar da Google'ı aramalardan bilgi silmeye zorlayabilir. Karardan bu yana, arama motorundan bilgi sildirmek için Google'a 300 binden fazla başvuru yapılmıştır, kendi söylediklerine göre, başvuruların yüzde 40'ı kabul edilmiştir. Şubat 2016'da Google, Fransız Veri Koruma Kurumu'nun baskısıyla, aramaları tüm Google *domain*'lerinden (alan adlarından) silmek zorunda kalmıştır.[30]

Karar pek çok yönden sorunludur. Özellikle, serbest bilgi akışını, son kertede de fikir özgürlüğünü zora sokmaktadır. Hangi bilginin hükmünün kalmadığına ya da alakasız olduğuna karar vermek kolay değildir. Örneğin güç elde etmeye çalışan kişilerle ilgili eleştiri oklarına hedef olmuş olaylar yıllar önce meydana gelmiş bile olsa, kamunun yararına mı sayılacaktır? Yoksa artık hükmü yoktur, diye mi sınıflandırılacaktır?

Antidemokratik devletlerde aramanın düzenlenmesine ne diyeceğiz? Arama sonuçlarının düzenlenmesi, daha otoriter toplumlarda aynı türden "düzenlemeleri" yasal kılabilecektir. Son bir eleştiri de bu konuda

kararı kimin vereceğiyle ilgili. Yayının ilk kaynağı (gazeteler, bloglar, özel Facebook durumu vb.) mı?

Giderek artan aramalar ve kişisel bilgilere erişimin büyük ölçüde mümkün olması, aramanın düzenlenmesini kesinlikle gerekli kılıyor ancak bunu şeffaf bir şekilde yapmak önemli; temel ifade özgürlüğü bir bütün olarak korunabilmeli, ara sıra alınan kararlarla değil.

DÖRDÜNCÜ BÖLÜM

Demokrasi ve Otoriter Akımlar

Refahın en önemli kaynaklarından biri teknolojik ilerlemelerdir. Daha önce de değinildiği gibi, toplumun dijitalleşmesi, özellikle internetin gelişimiyle hem insanlar hem de toplum için, gerek ekonomik gerekse sosyal anlamda büyük olanaklar sağlamıştır. Ekonomik açıdan üretimde büyük bir artış sağlanmış, sosyal açıdan coğrafyaların farklı olmasına rağmen ilişkilerin kurulması daha fazla mümkün olmuştur.

Teknolojik bakımdan yeni kazanımların her zaman için bir de öteki yönü vardır: Ahlaki değerlerden yoksun kişiler, teröristler ve suçlular da aynı teknolojiden faydalanmaktadır, bu yüzden topluma zarar verecek imkânlara sahiptirler. Bu sebeple, teknolojik kazanımları ahlak sorunundan ayrı değerlendirmek mümkün değil. Yeni bir teknoloji kullanılmaya başladığında toplum her zaman ikilemlerle karşı karşıya kalacaktır. Teknoloji, zarar vermek isteyen insanlar tarafından her zaman kötüye kullanılabilir.

Bu yüzden vatandaşların çoğu, bir tür izleme aracılığıyla bile olsa güvenliği sağlamanın devletin en temel hak ve görevleri arasında olduğunu kabul eder. Liberal demokrasilerde yasayla düzenlenip demokratik denetim altına alınan güvenliği sağlama yöntemleri, ilkesel olarak demokratik iradenin ifadesidir. Yetkilerin tümü demokratik denetim altında olduğundan, kesinlikle tehdit olarak değil, yalnızca bireyin bütünlüğünü korumaya yönelik kullanılabilir; izleme üzerine yapılan tartışmalarda tekrarlanıp duran tema budur. Pek çok kişi izlemeye kesin ihtiyaç olduğunu savunup kişisel hakların korunması yönündeki isteklerini ahlaki neden olarak göstereceklerdir. Tartışmanın elle tutulur bir yanı vardır. En azından, Batılı istihbarat örgütlerini DDR'nin

Stasi'siyle karşılaştırmak çok da anlamlı değildir. NSA'nın izlemesi ile Stasi'nin izlemesi arasında temel ahlaki farklılıklar vardır.

İzleme Toplumu kitabında yazar Eirik Newth, izlemeye izin vermek için bir sürü argümanın bulunduğunu gösterir. İzlemenin demokrasilerin hayatta kalabilmesi için kesin koşul olduğunu iddia eden Harvardlı hukukçu Alan Dershowitz'den alıntı yapar.[1] Suçla ve terörle, izleme yapılmadan mücadele etmenin zor olduğu bir dereceye kadar doğrudur. Ancak bu, liberal demokrasilerde izleme yapılması için verilen tam yetkilerin sorunsuz olduğu anlamına gelmez.

Burada sorulması gereken, demokratik yönetimlerin böyle bir sorunla karşılaşınca yasalar çerçevesinde (ya da yasaların amacı doğrultusunda) hareket ettiğine ne derece güvenebileceğimizdir. Çoğunluğun suça karşı mücadelede müdahaleci yöntemleri yasal olarak kabul ettiğini düşünerek, potansiyel tehlikeleri görmek çok önemlidir.

Maksat, vatandaşların özgürlüğünü korumaktır. Ama cehenneme giden yolun iyi niyet taşlarıyla döşenmiş olduğu bilinir; o yüzden liberal demokrasilerin de nasıl kırılgan olabileceği yakından incelenmelidir. Demokrasinin diğer yönetim biçimlerine üstünlüğü, demokratik toplumlara, alternatiflerinden daha fazla güven duyulmasından kaynaklanır. Pek çok demokratik ülkede, vatandaşların yetkililere duydukları güven oldukça fazladır. Bu da demokrasinin bir koşuludur ancak aynı zamanda, güvenin kötüye kullanılması tehlikesini de bünyesinde taşır. Demokrasiler kabul edilemez türden bir izlemeyi meşrulaştırabilir çünkü, ellerinin altında kendilerine duyulan büyük bir güven vardır. Demokratik devletler, otoriter akımlardan muaf değildir; demokrasilerde bu tür akımların vatandaşların güvenini kötüye kullanmasına tarihte rastlarız.

McCarty'cilik

1950 yılının Şubat ayında Wisconsin senatörü, West Virginia'da yaptığı bir konuşmada ABD Dışişleri Bakanlığı'na komünistlerin sızdığını bildiğini iddia etti. Konuşma "İçimizdeki düşmanlar" olarak bilinir.[2] Bu genç senatörün adı, 1950-1954 tarihleri arasında Amerika'yı kasıp kavuran "McCarthy'cilik" kavramına adını veren Joseph McCarthy'ydi.

Bu dönemde "komünizmle ilgisi" olduğu şüphesiyle 2000 resmi görevlinin işine son verildi. Pek çok durumda, bu tür bağlantıları ispatlayacak ya çok az delil vardı ya da hiç delil bulunmuyordu, Sovyetler Birliği'yle kanunsuz ilişkilere dair delil daha da az mevcuttu. En şaşırtıcı olan, senatör McCarthy'nin yöntemleriydi. Kongre'deki sorgularda, geçerli delil olmadan ciddi suçlamalar yapılıyor, tehditler savuruluyordu. Bu dönem, savaş sonrası ABD'deki otoriter akımların belki de en net örneğidir. Pek çok ABD vatandaşının sivil haklarının ihlal edildiğinden hiç şüphe yoktur.

1950'lerin başına damgasını vuran komünizm paranoyası, sıradan Amerikalılara sadece fiziksel anlamda bir saldırı değildi. Bu paranoyanın korkunç bir sindirici etkisi vardı. Pek çok Amerikalının karşı koyacak cesareti yoktu. 1954'te ABD'li seçmenlerinin yüzde 50'den fazlası McCarthy'yi destekliyordu.[3] McCarthy'nin yöntemleri kamuoyuna yansıdığında halkın desteği epeyce düştü, sonraları McCarthy'nin acımasız yöntemleri Kongre tarafından da kınandı. McCarthy'cilik, iktidarı eleştirmeye cesareti olan eleştirel bir basının ve sivil toplumun önemini açığa çıkarmıştır. Ancak süreç, Kongre üyelerinin tacizlerine maruz kalan vatandaşları koruyan ve iyi işleyen bir hukuka sahip olmanın önemini de ortaya koymuştur. McCarthy'nin elinde bugünün teknolojisi olsaydı ne türden tacizler yapılabilirdi, siz düşünün.

McCarthy'cilik 1954'ten sonraki en kötü paranoya sayılsa da FBI ve kurumun şefi J. Edgar Hoover da şüpheli komünistleri izlemek için geniş yetkilerle donatılmıştı.[4] Devletin, istihbarat kaynaklarını politik çıkarları için kullanmasına en iyi, daha doğrusu en kötü örnek olarak, Eski Başkan Richard Nixon verilebilir. Watergate Skandalı, Nixon'ın Demokratlar'ın merkezini izlemek istemesi üzerine çıkmıştır. Watergate Skandalı, Nixon'ın utanç içinde görevinden çekilmesiyle son buldu ancak artan istihbaratın beraberinde getirdiği sorunlar Nixon'ın gidişiyle son bulmadı.

ABD'de o dönemdeki istihbaratın işleyişi, kısmen düzenlemelerin yetersizliğinden, kısmen de Hoover'ın yasalar çerçevesinde hareket etmeye karşı esnek bir tavır içinde olmasından kaynaklanıyordu. Bu konularda bildiklerimizi, araştırmacı gazetecilikleriyle Watergate Skandalı'nı ortaya çıkaran Carl Bernstein ve Edward Woodward'a borçluyuz; Seymour

Hersch ve Christopher Pyle'ı da unutmamak gerekir. Bu gazeteciler, 1970'lerde sıradan ABD vatandaşlarının kapsamlı bir biçimde izlendiğini ortaya çıkarmıştır. Araştırmacı gazeteciliğin sayesinde Kongre, Frank Church'ün başkanlığında Church Komitesi'ni oluşturmuştur. [5] Komite, yetkililerin, siyasal nedenlerden dolayı ABD vatandaşlarını izlemek için gizli programları olduğunu belgelemiştir. Church ve diğer pek çok kişi, NSA'nın istihbarat kapasitesine dikkat çekti ve Amerika'da istihbarat yeni güçlenmekteydi. Komite, istihbaratın gerekliliğini kabul ediyordu ancak, NSA'nın ulaştığı kapasite, Amerika gibi liberal demokrasiyle yönetilen bir ülkede, gizli servisleri zamanla ne resmi yasalar ne de parlamenter denetim yoluyla denetim altında tutamayacakları bir durumun ortaya çıkmasına neden olabilirdi. Tam tersine, kendi görüşlerine göre, güçlü bir liberal demokrasiye sahip olan ABD'de, gizli servislerin ihtiyaçlarını meşru kılmalarının ve genişletilmiş tam yetkiler elde etmelerinin daha kolay olacağı düşünülebilirdi.

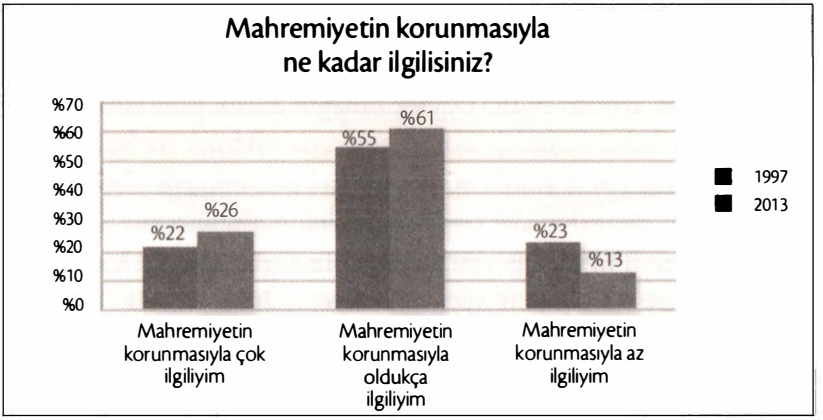
Bu sorunlar, internetin gelişimiyle azalmış değil ve Snowden'ın ifşaatları, gizli servislerin görevlerini ne şekilde yerine getirdiğini, liberal demokrasilerde yaşayan bizlerin de çok dikkatli takip etmemiz gerektiğine örnektir.

Lund Komisyonu'nun belgelediği kadarıyla, ABD için söz konusu olan mekanizmaların Norveç toplumunu etkilemeyeceği söylenemez. Lund Komisyonu 1996'da, hukuksuz siyasal izlemenin nasıl yürütüldüğüne dair beş bin sayfalık ayrıntılı bilgi sunmuştur.[6] Komisyon başkanı Yüksek Mahkeme Yargıcı Ketil Lund'du ve Avukat Regine Ramm Bjerke, Profesör Berge Furre, Korgeneral Torkel Hovland ve hukukçu Ingse Stabel komisyon üyeleriydi. İncelenen iddialar, polis teşkilatının istihbarat servisi, ordunun güvenlik hizmetleri ve istihbarat servisinin Norveç vatandaşlarını kanunsuz ve usulsüz bir şekilde izlemesi hakkındaydı. Komisyona, özel bir yasayla, mahkemelerin sahip olduğu tanıkları sorgulama yetkisi verilmişti. Rapor 1996 baharında kamuoyuna sunulduğunda büyük yankı uyandırdı çünkü Norveç'te 1945 yılından bu yana, kanunsuz siyasal izleme yapıldığı belgelenmişti. Raporda aynı zamanda, İşçi Partisi'nin önde gelen politikacıları ile gizli servisler arasındaki yakın ilişki de şiddetle eleştiriliyordu.

Lund Komisyonu'nun ortaya çıkardığı iş takdire değerdir ve istihbaratla ilgili köklü bir hesaplaşmaya giden Norveç bununla haklı olarak gurur duyar. Lund Komisyonu Raporu'nun içeriği ve Norveç gibi iyi işleyen bir demokraside Norveç vatandaşlarının kanun dışı izlenmesi üzerinde düşünülmesi gerekir. Lund Komisyonu Raporu ve gizli servislerle yaşananlar, yönetenlerin yetkilerini değerlendirip güncellerken bir tür uyarı olmalıdır, böylelikle gizli servislerin ihtiyaçları karşılanırken vatandaşların özel hayat hakkı ihlal edilmemiş olur.

Sürekli dijitalleşen bir dünyada mahremiyetle ilgili en büyük sorun, insanların bu konuda çok az endişelenmeleridir. Pek çok kişi gelişmeden hiç rahatsızlık duymamaktadır. Tam tersine, normal vatandaş izlenmeyi ve devletin yetkilerinin genişletilmesini, en azından pratikte, neredeyse büyük ölçüde kabul etmektedir. Bununla beraber Snowden'ın ifşaatlarının sonrasında Norveç vatandaşlarının mahremiyet sorunuyla ilgili öncesinden daha fazla endişelendiğine dair belirtiler vardır.

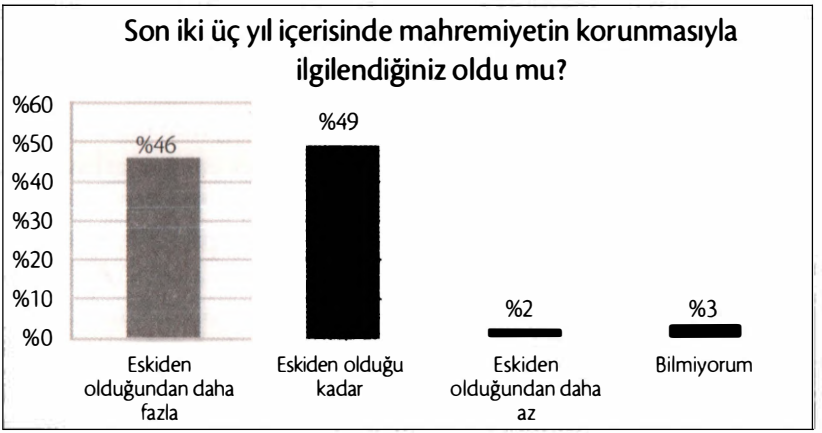
Veri Koruma Kurumu ve Teknoloji Kurulu Raporu'nda şunlar belirtilmiştir[7]:



Kaynak: Veri Koruma Kurumu ve Teknoloji Kurulu

Doğrudan sorulduğunda çoğunluk, mahremiyetle ilgili olduğu ve geçmişte olduğundan daha fazla ilgilendiği cevabını veriyor. Aynı zamanda, cevap veren kişilerin mahremiyetle tam olarak ne kadar ilgili olduğunu söylemek zor aslında. Dikkate aldıkları diğer şeylere kıyasla mahremiyetin ne kadar öncelik taşıdığı da aynı nedenle net değildir.

"Mahremiyetle ilgiliyim" cevabının eşiği oldukça düşüktür. Mahremiyetle daha çok ilgilendiğini söyleyenlerin neredeyse yarısının üzerinde Snowden'ın ifşaatları etkili olmuştur. Ancak bu soru da güvenlik karşısında değerlendirilecekse, mahremiyetin nispi değeri hakkında net bir cevap vermemektedir.



Kaynak: Veri Koruma Kurumu ve Teknoloji Kurulu

Batı dünyasında en fazla güvenlik kamerasına sahip şehrin Londra olduğu ileri sürülür ve Büyük Britanya, belki de kamerayla izlemeyi en çok kullanan demokrasidir. Devlet, örneğin çocuk pornosu ve dosya paylaşımına karşı mücadele etmek amacıyla internet trafiğine başka ülkelerde olduğundan çok daha fazla sayıda kısıtlama getirmiştir. Ancak bu durumun İngilizleri çok endişelendirdiğini görmüyoruz.

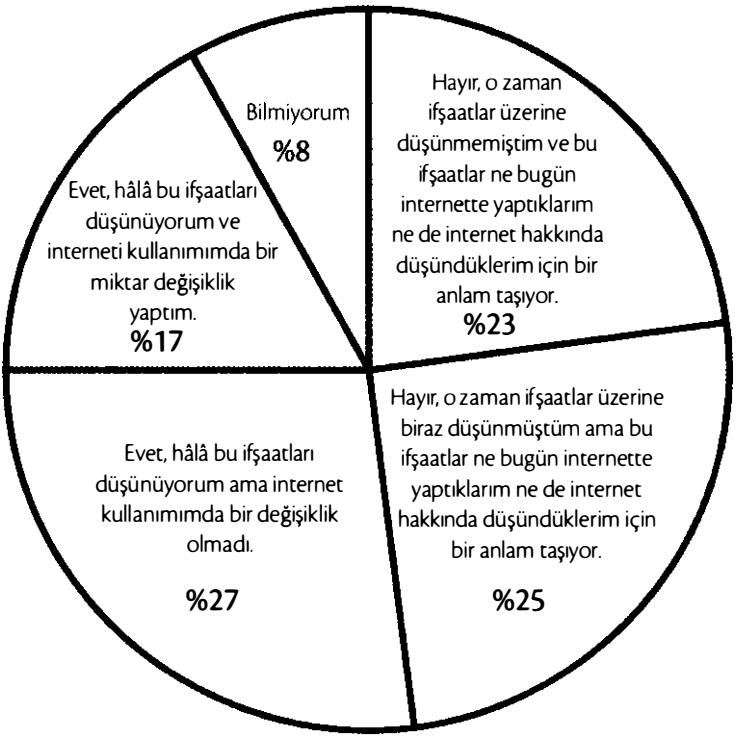
Eirik Newth'in yazdığı gibi, İngilizlerin özgürlüklerini kısıtlanmış hissettiklerine dair çok az veri var. Newth, 2012 yılında "İngiltere Ne Kadar Demokratik?"[8] raporunu yayımlayan Democracy Audit (Demokrasi Denetimi) adlı örgütten söz eder.

Rapordan çıkan tatsız sonuca göre İngiltere'de demokrasi çökmek üzeredir; politikada paranın önemi, politikacılara duyulan güvensizlik, politik katılımdaki düşüş başlıca nedenler arasındadır. Öte yandan vatandaşlar artan izlemeyi özgürlükler ve demokrasiye karşı bir tehdit olarak görmemektedir. Rapor ilginçtir çünkü vatandaşların çeşitli zorlukları birbirine kıyasla değerlendirdiğini göstermektedir; o zaman da

izleme listenin başını çekmez. Oldukça kapsamlı izlemeleri insanların kabul ettiği görülmektedir.

Vatandaşların gelişmeler karşısında fazla endişelenmediğinin bir başka işareti de Snowden ifşaatlarının internet alışkanlıklarımız üzerinde pek etkisinin olmamasıdır. Aşağıdaki şekilde gördüğümüz üzere ifşaatların internet alışkanlıklarını değiştirdiğini söyleyenler yalnızca yüzde 17 oranındadır. Cevap verenlerin yüzde 44'ü, ifşaatlar üzerine düşündüklerini söylemektedir ancak pek az kişi alışkanlığını değiştirdiğini belirtmiştir, ki bu da insanların endişelerinin aslında ne düzeyde olduğunun ifadesidir.

Snowden'ın ifşaatları, günümüzde internet izlemesi ve internette neler yaptıklarınız üzerine düşüncelerinizi etkiledi mi?



Kaynak: Veri Koruma Kurumu ve Teknoloji Kurulu

Snowden'ın ifşaatları, internetteki izlenme üzerine düşüncenizi etkiledi mi ve bugün internette ne yapıyorsunuz?

Norveç'te son yılların belki de en büyük mahremiyet tartışması Veri Saklama Yönergesi (DLD) olarak geçen AB yönergesi 2006/24/EF'yle ilgilidir. Bu yönergeyle, telefon operatörlerinin internet, e-posta ve telefon kullanımına bağlı verileri otomatik olarak saklaması uygulamaya kondu, polis ve istihbarat servisleri suça karşı mücadelede bu verileri kullanabilecekti.[9] DLD'nin uygulanmasına, Parlamento'da çoğunluk oyuyla karar verildi. Lehte oy verenler İşçi Partisi ve Sağ Parti'nin büyük bir çoğunluğuydu ancak AB Mahkemesi Nisan 2014 tarihli kararında yönergenin geçersiz olduğunu, uygulanabilmesi için değiştirilmesi gerektiğini belirtti.[10]

Bu bağlamda, Norveçlilerin yönergeyle ilgili tavırlarına bakmak ilginç olacaktır. DLD hakkındaki tartışma kapsamlıydı ve siyasi partiler içerisinde de büyük yankı uyandırmıştı. Bütün bunlara rağmen, *Minerva* dergisi için Synovate'in yaptığı anketlere göre soru yöneltilenlerin açık ara çoğunluğu, DLD'nin uygulanmasından yanaydı.[11] Sol Parti'ye oy verenlerin arasında bile yönergeden yana olanlar çoğunluktaydı. DLD'nin halktan destek görmesinin nedeni, muhaliflerin çoğunun ileri sürdüğü gibi, kamuoyunun politikacılar ve polis tarafından korkuyla beslenmesiydi, ancak insanların çoğunun artan izlenmeden pek endişe etmediğini ve devlet izlemesini kabul ettiğini de düşünebiliriz.

Bu tutumlar, izleme karşısında Avrupalıların tutumu üzerine yazılmış daha kapsamlı bir raporda ifade edilmektedir. Bir AB projesi olan SUPRISE, (İzleme, Mahremiyet ve Güvenlik sözcüklerinin kısaltılmışı) 2015 yılının Mart ayında kamuoyuna sunuldu.[12] Bu raporda Avrupalı vatandaşların mahremiyet karşısındaki tutumları incelenmişti. Projenin Norveçli ortağı Teknoloji Kurulu'nun rapor özetinde şu ifade vardı: "Halk güvenlik teknolojisi üzerine daha çok bilgilendiğinde daha şüpheci oluyor ancak resmi izlemeye, özel izlemeden daha fazla güven duyuyor."[13] Toplumda güvenliği sağlamlaştırmak için daha fazla izleme ve güvenlik teknolojisi kullanmak zorunda mıyız sorusuna, hem Norveç hem de pek çok Avrupa ülkesinde ezici çoğunlukla evet denmesini, son söylediğimize örnek olarak verebiliriz. İlginç farklı tutumlara, Norveç ve Almanya arasında rastlıyoruz. Norveçlilerin yüzde 70'i toplum güvenli-

ğini güçlendirmek için güvenlik teknolojisi ve izlemenin kullanılmasını mantıklı bulurken, bu oran Almanya'da yüzde 20.[14]

İzlenmenin, yasal hedefi olsa bile kontrolden çıkabileceğini düşününce, "Demokrasiye nereye kadar güvenebiliriz?" sorusu yalnızca ilginç olmakla kalmıyor, daha derin anlamlar da taşıyor. Demokrasinin ayakta kalabileceğine güvenebilir miyiz? I. Dünya Savaşı'nın bitiminde Hitler'in iktidara gelmesine kadar süren Weimar Cumhuriyeti, pek çok zayıf yönüne rağmen Almanya'da demokratik bir oluşumdu. Ancak kurumların kırılganlığı ve talihsiz uluslararası koşullar yüzünden demokrasi ayakta kalamadı.

Ancak teknolojik gelişme Nazilerin yönetimi altında durmuş değildi. Hitler'in Almanya'sı çağdaşlığı ve onun teknolojik olanaklarını korkunç bir biçimde kullandı. Soykırımın endüstriyel bir biçimde yapılması pek çok örnekten biridir. Naziler ayrıca, Weimar Cumhuriyeti sırasında Alman devletinin toplamış olduğu tüm resmi veri tabanlarını kullandı. Naziler bilgiyi, denetimi ele geçirmek ve Almanya'yı totaliter bir rejime sürüklemek için kullandı. Bu tarihi tecrübe Almanlarda büyük iz bırakmıştır, ayrıca DDR'deki komünistler de izlemelerinde ve bilgiyi saklamakta aynı amacı güdüyorlardı: Demokrasiyi güçsüzleştirmek.

Günümüz Almanya'sı ve pek çok Avrupa ülkesindeki demokratik kurumlar, 80-100 yıl öncesinde olduğundan çok daha güçlüdür. O yüzden pek çok kişi, bugün izleme teknolojilerinin meşru nedenlerle kullanılmasına karşı tartışmaların demokrasinin yıpratılması tehlikesine işaret etmesini çok abartılı bulmaktadır. Aynı zamanda üst verilerin saklanması ve ulusal veri tabanlarının kullanımının yalnızca teröristleri ve suçluları ortaya çıkarmak için söz konusu olduğu ileri sürülür. Ancak bugün amaç her ne kadar meşru olsa da yönetim biçimi değiştiğinde, belki de demokrasi otoriter akımlara yenik düştüğünde, bilgiler ve teknoloji hâlâ el altında olacaktır. Bazıları bu şekilde düşünmenin günümüz demokrasisinin gelişim olanaklarının önüne gereksiz engeller koyduğunu iddia etmektedir. Norveç ya da başka Batılı ülkelerin otoriter yönetimlerin eline geçeceğine dair varsayıma dayalı bir durum yerine, günümüzdeki durum değerlendirilmelidir.

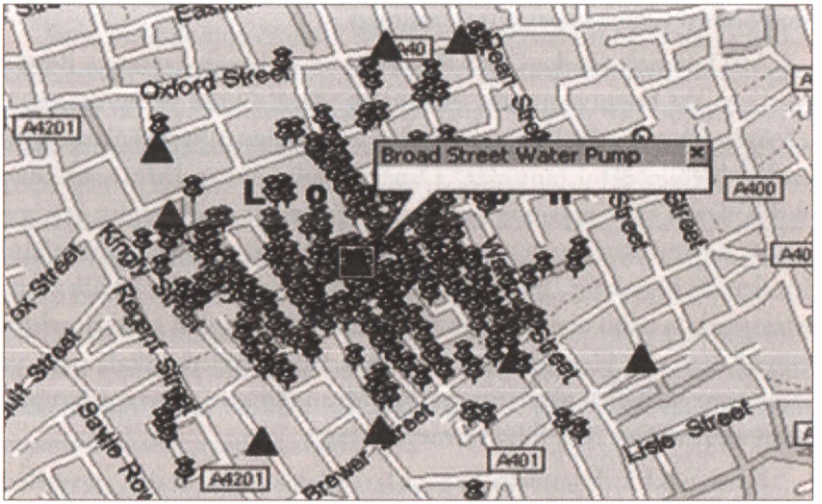
Liberal bir demokraside, özgürlük ve güvenlik arasındaki denge içerisinde neleri meşru gördüğümüz, bunların yasal mevzuatının en iyi nasıl düzenleneceği tartışması hiç şüphesiz en önemli tartışmadır. Liberal bir demokraside bile gizli servislerin denetlenmesine dair büyük sorunlar mevcuttur, sonraki bölümde bu konu tartışılacaktır.

Ancak aynı zamanda günümüz teknolojisinin sağladığı olanaklar ve bilginin saklanmasının, niyet değişecek olursa, nasıl kötüye kullanılabileceği hakkında düşünüp tartışmak akıllıca olacaktır. Eski Başkan Gerald Ford, yönetimi sırasında Thomas Jefferson'dan bir alıntı yapmıştır: "Sana her ihtiyacın olanı sunabilecek güçte bir devlet, aynı zamanda sahip olduğun her şeyi senden çekip alabilecek güçtedir."

BEŞİNCİ BÖLÜM

Büyük Veri Devrimi

1854 yılında Londra'da ortaya çıkan kolera salgınında, Doktor John Snow hastalığın baş gösterdiği yerlerin bir taramasını yapmaya karar verdi.[1] Çalışması sayesinde Snow, salgının çıktığı noktanın Broad Street'teki su pompası olduğunu buldu. (Bkz. aşağıdaki harita)



Kaynak: Haitiwater.org

Bu detaylı haritalama sayesinde Snow, hem kolera salgınının nedenini ortaya çıkardı hem de salgının yayılmasını önledi. Bu öncü çalışma, gelişmiş veri işlemenin temelini atmıştır. Snow'un yaklaşımı modern biçimiyle *Big Data* (Büyük Veri) olarak anılır.

Google'da "Büyük Veri"yi aradığınızda 368 milyondan fazla sonuç bulursunuz. Sadece Amazon'daki "Big Data" araması yaklaşık 20 bin

sonuç verecektir. Bir başka deyişle, "Big Data" moda bir sözcük olmuştur. Terim, normal veri araçlarının kaydedemeyeceği, depolayamayacağı ve de analiz edemeyeceği kadar devasa veri yığınlarına işaret etmektedir. Büyük Veri'den klasik olarak anladığımız, geleneksel yöntemlerle bilgi yakalayamayacağımız kadar kapsamlı veri yığınlarıdır. Terimin yaygın tanımı,[2] 2000'lerin başında Doug Laney tarafından geliştirilmiştir ve Laney, Büyük Veri'yi üç V yardımıyla açıklar: *Volume* (hacim), *Velocity* (hız) ve *Variety* (çeşitlilik).[3]

Hacim veri büyüklüğünü tanımlar, yani yeni teknoloji sayesinde depolanan verinin miktarını. Hız, çoğunlukla gerçek zamanlı diye bilinen süre içerisinde (yani olay olurken) veri yığınlarının ne kadar hızlı işlenebildiğini tanımlar. Çeşitlilik, hem yapılandırılmış hem yapılandırılmamış farklı veri formatlarını, e-posta, video ve metin dosyalarını işleme kapasitesini tanımlar.

ABD teknoloji şirketi SAS Enstitüsü bu üç klasik kavrama, Büyük Veri'nin iki boyutunu daha eklemiştir: *Değişkenlik* ve *karmaşıklık*. *Değişkenlik*, veri yığınlarının belli olaylar ve zaman dilimleri olarak nasıl izole edilebileceğini tanımlar.[4] Örneğin polis, bizim hafta sonundan farklı olarak hafta arasında nasıl davrandığımızla ilgilenebilir. Pek çok şirket, davranışlarımızın yemek öncesi ve sonrası ne derece değiştiğini incelemek isteyebilir. Bu konudaki üçüncü bir örnekse, büyük organizasyonlara bağlı olarak davranışımızdaki değişimleri görebilmektir. Büyük Veri'nin işlenmesi, belli olaylara bağlı verileri yakalamaya ve izole etmeye, belirli olayların, sıradan olsun olmasın, davranışlarımızı nasıl etkilediğine dair bilgi vermeye yarar.

Karmaşıklık, kompleks bağlamları işleme kapasitesini ve verileri farklı sistemler karşısında dönüştürürken aynı zamanda bağlantıları da görmeyi tanımlar. Büyük Veri, büyük, karmaşık ve değişik veri yığınlarını, büyük bir hızla, neredeyse anında işleyerek, bir bakıma niteliksel yeni bir şeyi temsil etmektedir. Büyük Veri analizlerinin toplumu ilgilendiren yanı, kararların büyük ölçüde verilere dayanılarak alınmasıdır. Büyük Veri, karar sürecini en verimli hale getiren ve masrafları, riskleri ve zayıflıkları azaltma olanağı sağlayan koşulları oluşturur.

Büyük Veri analizleri, insan davranışlarını anlama ve kalıplarını çözme konusunda, daha evvel olduğundan çok daha fazla katkı sağlayabilir, gelecekteki davranışları hassas bir biçimde tahmin edebilir. Bu şekilde insanlar, Büyük Veri analizlerini, eskisine kıyasla kararları optimize etmek için kullanabilir. Bu ancak ham veriye erişimle mümkün olabilir.

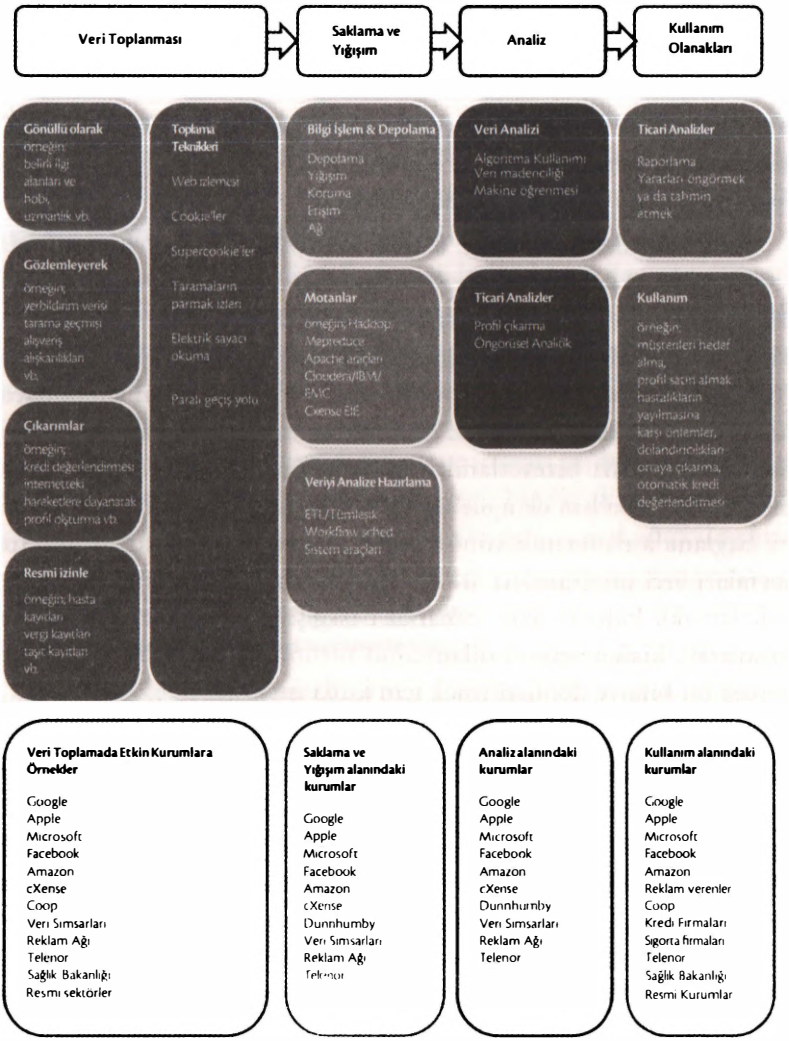
Toplam veri yığınlarının ne kadar küçük bir bölümünün işlendiğini düşünecek olursak, kararların optimize edilmesi için büyük bir potansiyelin örtülü olarak kaldığını görürüz.

2012'de 2.8 zetabite (1 zetabit=1 milyar terabit)[5] tekabül eden miktarda veri depolanmıştır. 2020 içerisinde depolanan veri miktarı 50 misli artacaktır. SAS Enstitüsü'ne göre bu veri miktarının yüzde 33'ünün işlenmesi fayda sağlayacaktır. Kıyaslayacak olursak, bugün veri miktarının yalnızca yüzde 0,5'i işlenmektedir.[6]

Şunu vurgulamak önemli: Büyük Veri analizinin başarısı, ne kadar çok verinin saklandığında değil, bilgi yakalama, davranış ve kalıplarını tahmin edebilme kapasitesinde yatar. Büyük Veri analizlerinin nasıl verimli kullanılabileceğine örnek, vatandaşların elektrik gerektiren işleri (çamaşır yıkamak, yemek yapmak gibi) hangi zamanlarda yaptığının analizidir. Elektrik tüketimini kayıt altına alarak, elektrik dağıtım firmaları hizmetlerinin kalibrasyonunu yapar, böylece hem enerji üreticileri hem de ağın sahipleri kaynaklarını mümkün olan en iyi biçimde kullanmış olur. Örnekler, vatandaşların çoğunluğunun normal günlerde 06.00 ve 08.00 saatlerinde kalktığını gösteriyorsa, elektrik ağı, ham veriden çıkarılan bilgiye göre elektrik miktarını otomatik olarak ayarlayacaktır.

Sağlanabilecek potansiyel faydaya bir başka örnek de internet aramalarıdır. John Snow 1854'te kolera salgınının haritasını çıkarmak zorunda kalmışken, günümüzde Google kimin, nerede, ne aradığını kaydederek olayları kaydetme potansiyeline sahiptir. Örneğin, hastalıkların yayılması resmi sağlık kurumlarından önce fark edilebilir. Çoğumuz, kendi kendimize teşhis koyabilmek için aramalar yaparız. Google, belli bir bölgedeki hastalık belirtileriyle ilgili arama sözcüğünde hızlı bir artışı kaydettiğinde salgını erkenden, neredeyse gerçek zamanlı ortaya çıkarabilir. Ancak Google 2008 yılında, gribin belirtilerini belirleme girişimi

Google Flu Trend'i (Google Grip Furyası) lanse ettiğinde başarısızlığa uğradı çünkü konuyla ilgili bilgileri izole etmeyi beceremedikleri için tahminlerinde yanıldılar.[7] Bu olay yine de, Büyük Veri analizlerinin gelecekte yaklaşık nasıl kullanılacağının çarpıcı bir örneğidir. Analizler, sağlık hizmetlerinin az gelişmiş olduğu, salgın hastalıkların kolayca ortaya çıktığı, yani analizlere en çok ihtiyacı olan ülkelerde büyük fayda sağlayacaktır.[8]



Kaynak: Veri Koruma Kurumu

Arkamızda bıraktığımız elektronik ayak izleri, hem endüstrilerin hem de sektörlerin ilgi alanında olacaktır. Tutumları tahmin edebilmek için veriyi bilgiye dönüştürme anlamında işlemek, gelecekte bizlere sunulan hizmetin ne kadar iyi olacağını belirleyecektir.

Büyük Veri analizlerinin potansiyel değerinin yüksek olmasının en önemli nedeni, veriyi yeniden kullanabilme olanağıdır. Depolama kapasitesi genişledikçe, işleme olanakları arttıkça verilerin yeniden kullanılma olanağı da artacaktır. Bu, arkamızda bıraktığımız elektronik izlerin, belirli bir amaç için toplanıp depolanmış verilerin yanı sıra başka amaçlar için de kullanılabileceği anlamına gelmektedir; büyük olasılıkla da bizim onayımız olmadan. Yeniden kullanılan verilerin Büyük Veri analizi, hem masrafları azaltmayı sağlayabileceği hem de ihtiyaca göre düzenlenmiş çözümler sunabileceği için çok değerli olabilir.

Ancak bu aynı zamanda mahremiyetin korunmasını zorlaştıracaktır. Bu zorlukların bazıları daha sonraki bölümlerde ayrı ayrı ele alınacak. Bu bölümde yalnızca, Büyük Veri kullanımının getirdiği daha önemli ve genel sorunlar tartışılıyor.

Devasa boyutlarda verilerin ortaya çıkardığı sorunun ana nedeni, bunların, bilgi kapsüllerini (*HTTP cookies*) kullanan iz sürme teknolojisi aracılığıyla sizi birey olarak tanımlayabilmeleridir. Bilgi kapsülleri, tekil kullanıcıya has olan elektronik ayak izleridir. Bilgi kapsüllerinin bu bağlamda en önemli yönünü internet sayfaları oluşturur. İnternet sayfaları veri programları aracılığıyla yalnızca kişisel ve tarihsel veri yakalamakla kalmaz, aynı zamanda başka şeylerin yanı sıra tıklamaları sayayarak, kişisel veriyi kullanıcının tutumları ve talepleri hakkında gerçek bir bilgiye dönüştürmek için kullanır.[9]

Firmaların sizin tutumlarınız hakkında bilgi depolayabilmesinin doğrudan neticelerinden biri, istemediğiniz halde onların ısmarlama ticari sunumlarda bulunabilmesidir. Örneğin Google, başkalarına bilgi satabilir ya da sizin aramalarınıza dayandırdığı ticari ürünleri kendisi size sunabilir. Veri bilgisinin büyük ticari önem kazanmasının en önemli koşulu çerez kullanımıdır. Bu tür bilgi kapsüllerinin kullanımının yasayla düzenlenmesi bu yüzden önemlidir.

Norveç'teki Ekom Yasası bilgi kapsüllerinden nasıl faydalanılacağını düzenler, sorumlu internet sayfalarının şu bilgileri vermelerini zorunlu kılar: 1) Hangi türden çerezler kullanılmaktadır, 2) hangi bilgiler kullanılmaktadır, 3) kullanımdaki amaç nedir ve 4) bu bilgileri kimler kullanacaktır.

Çerezlerin fonksiyonlarından dolayı onay ilkesine uyulması önemlidir, tüketici bilgi kapsüllerinin depolanmasını kabul ettiğini belirtmelidir. Ancak bu, büyük bir sorundur: Ulusal İletişim Kurumu'nun Norveç'teki 500 büyük internet sitesinde yaptığı incelemenin sonuçlarına göre, her beş firmadan dördü bilgi edinme koşullarını yerine getirmeyerek yasayı ihlal etmektedir.[10] Ayrıca Veri Koruma Kurumu'nun başkanı Bjørn Erik Thon da mevzuatın, bilgilendirilmiş iyi bir onay politikasının ilkelerinin oluşturulmasına yeterince yardımcı olmadığına dikkat çeker.[11] Hakkında bilgi sahibi olduğumuz seçimleri yapabilmemizi, şirketlerin internetteki uygulamaları kolaylaştırır. Günümüzde onay uygulamasının zorlukları o kadar kapsamlıdır ki, bunlar sonraki bölümde tek başına ele alınacaktır.

Verilerin kaydedilip depolanma yöntemi önemlidir ancak ayrıca analiz edilmesi bazı özel sorunlar içerir. Büyük miktarlardaki verilerin analiz edilebilmesi, Büyük Veri'nin mahremiyet açısından neden tehlikeli olduğunu anlamak için önemlidir. Aslında en büyük sorun elektronik ayak izleri değildir. Ham veri, özel hayatımız hakkında aslında fazla bir şey anlatmaz. Sorunlar, sıra analize gelince ortaya çıkar. Bu noktada, verileri birbirine bağlama olanakları çok büyüktür.

Şu noktada "Big" gereklidir: Analizciler verileri farklı kaynaklardan toplayabilir, başka analizcilerle paylaşabilir. O zaman da bireyler, ileri düzeyde bilgi işlemlerle tanımlanabilir, oysa bilgiler esas olarak anonimdir. Bu, ilk zamanların bilgi işleminden çok farklıdır. Bu tür analizler temelinde hizmet geliştirenler büyük bir sorunla karşı karşıyadır: Ellerindeki verileri, talep edilen ısmarlama hizmetleri sunmak için mi kullanacaklar, yoksa hizmetleri kullananların özel hayatlarını mı koruyacaklar?

Verilerin depolanması, analiz edilmesi ve analizlerin kullanılması arasındaki yakın ilişki, depolamayı bir sorun haline getirir. Bu bakım-

dan, depolama ve analiz arasındaki ilişki üzerine yapılan tartışmalar, silah yasaları hakkındaki tartışmalardan farklı değildir: Silahın kendi kendine kimseyi öldürmediği doğrudur, tetiği çekecek bir parmağa ihtiyaç vardır ("İnsanları öldüren silahlar değildir, insanları insanlar öldürür"). Ancak, insanların ellerine aldığı silah sayısı arttığında daha çok tetik çekilecektir. Aynı şekilde: Ne kadar çok verinin depolanmasına izin verirseniz, özel hayat için o kadar çok sorun çıkarırsınız, çünkü verinin analizler sırasında (kötüye) kullanılması ihtimali artar, böylelikle özel hayat hakkı gayet kolay ihlal edilebilir.

Taylor Armerding, bir makalesinde, Büyük Veri'yle bağlantılı beş büyük sorunu özetler:[12]

- Ayrımcılık: Veri analizleri belirli özellikleri (etnik köken, cinsiyet, din vb.) olan kişilerin, başkalarıyla aynı olanaklara sahip olması konusunda zorluk çıkarabilir.

  Güvenlik ihlali: Kişisel verileriniz sızdırılabilir, sonradan işlenmeleri için büyük fırsatlar doğar. Örneğin, şimdilerde, özellikle uyuyan çocukların web kamera resimlerini arayan arama motorları (Shodan) vardır.

  Anonimliğe veda: Büyük Veri setlerine bağlanarak anonim kişilerin kimliği yeniden tanımlanabilir.

  Devlete verilen geniş yetkiler: Büyük Veri ayrıca, izleme ve devletin organlarına hangi yetkilerin verileceği sorununu da gündeme getirir.

  Düzenlenmemiş bilgi işlem: Pek çok kişisel veriniz, bilgi işlemin doğru yapıldığı konusunda bir saydamlık ya da garanti sunulmadan işlenebilir.

Temeli belirsiz sistematik ayrımcılık fırsatları, özel hayat için ciddi tehlikeler oluşturabilir. Bazı alanları örnek verecek olursak analizlerin, kimin güvenlik tehlikesi oluşturduğu, kimin kredi verilebilir olduğu, kimin çeşitli işlere uygun olduğu ve ne kadar sigorta primi ödeyeceğine karar vermek için kullanılma olasılığı büyüktür. Gelecekte, bir Facebook kullanıcısının ne kadar kredi verilebilir olduğu arkadaşlarına bakılarak belirlenebilir. Tüketiciyi Koruma Kurumu'ndan Finn Myrstad'ın belirt-

tiği gibi, Facebook'taki arkadaşlık tekliflerini ret ya da kabul ederken pek az insan bu tür şeylere dikkat eder.[13]

Bu yüzden internetteki sosyal ağınız ve tutumunuz, gelecekte hangi hizmeti alacağınızı ve nasıl bir bedel ödeyeceğinizi belirleyebilir. Bu kendi başına zaten sorunlu bir durumdur, ancak ticari amaçlar için hangi verinin gerçekten kullanılacağı net olmayacağı için daha da sorunlu bir hal alacaktır.

Obama yönetimi son yıllarda, mahremiyet sorunlarıyla ilgili çalışmalar yaptı. Bu sorunla ilgili olarak Obama için çerçeveyi belirleyen Başkanın Bilim ve Teknoloji Danışmanları Kurulu'ydu (President's Council of Advisors on Science and Technology-PCAST). Bu kurul, Mayıs 2014'te "Büyük Veri ve Mahremiyet: Teknolojik Perspektif" raporunu yayınladı.[14]

Raporda altı çizilen, teknolojinin sınırlarını belirlemesi gerekenin siyaset olduğudur çünkü serbest gelişmesine izin verilirse teknolojinin kendi başına özel hayatı koruyacağına inanmak mümkün değildir.[15] Kurul aynı zamanda, teknolojik olanakların kısıtlanmasından çok, toplumun veri toplama amaçlarına ağırlık vermesini önermektedir. Teknolojinin köhneleşmesinden kaçınmak için, "nasıl" sorusunun yerine "ne" sorusuna odaklanmalıyız.[16]

Kurul ayrıca, Büyük Veri analizinin avantajları ve mahremiyet açısından sıkıntıları arasındaki dengelerin de teknolojik bir sorun olduğunun altını çiziyor. Raporda şunlar belirtiliyor:

> Yürütülecek politika, mahremiyet üzerindeki kötü etkileri azaltmayı sağlayabilecek teknolojilerin geliştirilip ticarileştirilmesini ve yeni teknolojik seçeneklere yönelik araştırmaları hızlandırmalıdır. Teknolojiyi daha verimli kullanarak Ulus, mahremiyet için söz konusu olan sorunları sınırlarken, Büyük Veri'nin pek çok faydasından yararlanmada dünya lideri olabilir. Son olarak, PCAST Büyük Veri'yi mahremiyete hassasiyet gösterecek şekilde geliştirip kullanacak uzmanlığa sahip yeterli sayıda yetenekli kişinin yetişmesini güvence altına alacak girişimlere çağrıda bulunmaktadır.[17]

Büyük Veri söz konusu olduğunda mahremiyet hakkını koruyacak araçlar bulunmadığından, sadece verilerin toplanmasını kontrol altına almaya dayalı bir siyaset de gerçekçi olmadığından (ve pek istenme-

diğinden), yasamaya, verilerin kullanımı ve veri analizleri üzerine yoğunlaşmak, teknolojik görüş açısından daha mantıklı olacaktır.[18] Beyaz Saray'da (Beyaz Saray çalışma grubunca) yayınlanan "Büyük Veri: Fırsatları Yakalamak, Değerleri Korumak" raporunda,[19] Obama yönetiminin Büyük Veri söz konusu olduğunda da özel hayatı koruma niyeti tekrarlanmaktadır, raporu hazırlayanlar Tüketicinin Mahremiyeti Hakları Beyannamesi'ni oluşturmayı istemektedir.[20]

Obama yönetiminin, Büyük Veri analizlerinin belirgin olumlu yanlarını kısıtlamadan, özel hayatı korumayla ilgili hangi somut politikanın en iyisi olacağına dair soruya şimdilik iyi bir cevap veremediği açıktır:

> Mahremiyet konusundaki araştırma ve atılımlara yapılan yatırımı önemli ölçüde artıracağız, teknolojileri geliştireceğiz, sadece bilgisayar bilimi ve matematiği içeren çapraz araştırmaları değil, ayrıca sosyal bilimler, iletişim ve hukuk disiplinleriyle ilgili araştırmaları da teşvik edeceğiz.[21]

Veri Koruma Kurumu'nun "Büyük Veri – Mahremiyetin Korunması İlkeleri Baskı Altında"[22] raporunda (Eylül 2013), Obama yönetiminin dikkat çektiği aynı sorunlara ağırlık verilmiştir; bu da, olay hakkında yürütülen uluslararası tartışmaların birbirinin aynı olduğunu gösterir. Hem Büyük Veri'nin büyük ve olumlu potansiyeli hem de mahremiyetin korunmasına karşı oluşturduğu tehlike için geçerlidir bu. Ancak Veri Koruma Kurumu, "Bu analiz biçimini kullanırken, aynı zamanda bireylerin mahremiyet hakkına saygı göstermenin mümkün olduğunu", Başkan Obama'nın çalışma grubundan daha kesin bir dille belirtmiştir.[23] Veri Koruma Kurumu raporunda, Büyük Veri kullanılırken uygulanması gerekli beş ana mahremiyeti koruma ilkesi tavsiye etmektedir:

> Kişisel bilgilerin işlenmesi esasen onaya bağlı olacaktır. Onay almanın mümkün olmadığı ya da istenmediği durumlarda bilgiler anonim kalacaktır.
>
> Bilgilerin anonimleştirilmesi ve kimliksizleştirilmesi için iyi yöntemlere sahip olmak büyük önem taşımaktadır. Bu durum, yeniden kimlik saptama tehlikesini azaltacaktır.
>
> Büyük Veri, tümleşik mahremiyet hakkı ilkelerine uyularak kullanılmalıdır (varsayılan olarak mahremiyet).

> Büyük Veri'yi kullanan şirketler, topladıkları kişisel bilgileri nasıl işledikleri hakkında açık olmak zorundadır. Bu da, profilleri geliştirmek için hangi karar kriterlerinin (algoritmaların) temel alındığını ve hangi kaynaklardan bilgilerin toplandığını kişinin görebilmesini sağlamayı gerektirir.
>
> Kişi, şirketlerin elinde tuttuğu tüm verilerin, kullanıcı dostu formatta kendisine teslim edilmesi olanağına sahip olmalıdır. Veri taşınabilirliği, müşterilerin kabul edilemez koşullara sahip hizmetlere mahkûm kalmasını engellemelidir. [24]

Bunlar, mahremiyetin nasıl korunabileceğine dair güzel tavsiyelerdir, ancak hem Büyük Veri analizlerindeki olanakları sonuna kadar kullanıp hem de bu ilkelere uyabilmek zordur. Bu tür analizlerin potansiyelinden faydalanma ve geleneksel anlamda mahremiyet arasında bir çelişki vardır. Bu durum, Veri Koruma Kurumu'nun raporunda da ele alındığı gibi, verilerin amacı çok aşan yeniden kullanılmasında geçerlidir. Kurumun altını çizdiği nokta şudur: "Amacın sınırlandırılması ilkesi, toplanmış kişisel bilgilerin, toplama amacına ters kullanılamayacağını belirtir, bu tür kullanımlar için yazılı onay gereklidir."[25] Ancak, "amacına ters" ifadesinin ne anlama geldiği net değildir; bu durumda belirleyici olan, amaç sınırlandırılmasının kapsamlı mı, yoksa dar mı olacağıdır. Amacın sınırlandırılması ilkesi, mahremiyete karşı Büyük Veri analizleri tartışmasındaki ana sorundur. Dar bir sınırlama Büyük Veri analizinin olumlu yönlerine ağırlık verirken, kapsamlı sınırlama mahremiyetin çıkarlarını gözetmeye ağırlık verecektir. Sorunların üstesinden gelmenin yolu, anonim verileri kullanmaktır. Ancak bunu yapmanın koşulu, verileri anonim olarak saklamayı gerçekten başarabilmek ve anonim verinin yeniden tanımlanabilmesini engellemektir. Bunu sağlamak zordur. Bu tür işlemlerin ister bilinçli seçimlerden ister ihmalkârlıktan doğan ihlallerini önleyebilecek tedbirler alınmalıdır.

ALTINCI BÖLÜM

İzleme Ekonomisi

Büyük Veri devriminin sonuçlarından biri verilerin değer kazanmasıdır. Verilere erişim ve verilerin kullanımı büyük ticari değere sahiptir ve gelecekte de sahip olacaktır. Pek çok kişi verileri yeni hammadde olarak adlandırmaktadır. Bu hammaddenin değerinin artışı ticari başarı için önemlidir. Verilere erişimin aslında "size erişim" anlamına geldiğine dikkatinizi çekerim, yani şirketler için değerli olan sizin kişisel verilerinize erişebilmektir. Yeni dijital ekonomi, pek çok yerde *izleme ekonomisi* olarak anılır.[1] İzleme ekonomisi kavramına spekülatif olduğu için karşı çıkılabilir ancak verilerinizi ticari olarak kullanmak isteyen şirketler ile sizin özel hayatınızı koruma arzunuz arasında gizli bir çatışma olduğu açıktır. Şirketler Büyük Veri'yi potansiyel kâr olarak görmektedir, mahremiyet aktivistlerinin gördüğüyse, özel hayatla ilgili çok büyük potansiyel sorunlardır.

Soru şudur: Ortalama bir vatandaş ne görmektedir?

Ticari çıkarlar ve özel hayat ilişkisi üzerine süregelen tartışmalarda anlamlı birçok şart vardır. Siyasal sorunlarla ilgili daha net bir resim çizebilmek için üç şartı tartışmak önemlidir.

İlk olarak: İş modelleri başlı başına bir tehdit oluşturabilir mi? Şirketlerin para kazanma yöntemi, özel hayatı korumaya ters düşüyor olabilir mi?

Mahremiyet 2016 raporunda, Veri Koruma Kurumu ve Teknoloji Kurulu, gelişmekte olan iş modeline dair kuşkuları olduğunu dile getirdi.[2] Raporda şu belirtilmiştir: "Süregiden izlemenin bir haritasını çıkarmaya başladığımızda, bu iş modellerini yeniden değerlendirmek için daha büyük nedenler ortaya çıkar. Bizler için bu iş kötü bir alışveriş çünkü, kendimizden gerçekten ne verdiğimiz ve izlemenin aslında ne

kadar kapsamlı olduğu ortaya konmuyor. Hayatlarımız giderek artan bir şekilde tümüyle izleme altında – internet ekonomisinin karanlık yanı sürekli daha da belirginleşiyor."

Rapordaki iddia eğer doğruysa, insanlar neden kötü anlaşmalar yapmayı seçiyor? Bu da bizi, tartışılması gereken bir sonraki soruya yönlendiriyor: Bizler vatandaşlar olarak, şirketlerin hizmetlerinden faydalanabilmemiz için koşullarını kabul ettiğimizde neyi onayladığımızı anlayacak durumda mıyız? Üçüncü olarak, ticari çıkarlarla karşı karşıya kaldığında özel hayat hangi somut hukuki koruma altında olmalıdır ve hangi yargı alanı her zaman için geçerli olacaktır?

Teknoloji ve ekonomi ulusal sınırlarla giderek daha az kısıtlanırken, ekonomik ve teknolojik çözümleri düzenlemek için pek az uluslararası kanun mevcuttur. Mahremiyet açısından şanssız bir durum.

İş Modeli ve Mahremiyet

Microsoft, Apple, Google, IBM, Samsung ve Facebook gibi şirketler dijital gelişimin öncüleri arasındadır. Şirketlerin ürünlerini geliştirme kapasitesi ekonomik başarıları beraberinde getirmiştir. *Forbes*'e göre Apple, Microsoft ve Google dünyanın en değerli üç şirketidir. 2016 yılının başında (Google'ın konglomeratı) Alphabet, *Financial Times*'a göre, dünyanın en değerli şirketi sıralamasında Apple'ı geçmek üzeredir.[3] Kişisel verileri toplama ve analiz etmenin öneminin büyüklüğünü teyit eden bir örnek daha. Bu tür analizler, Google'ın para kazandığı iş modelidir, Apple'ınsa en büyük gelir kaynağı, ürettiği klasik ürünleridir hâlâ. *Forbes*'in listesinde ayrıca IBM, Samsung ve Facebook en değerli ilk 10 şirket arasındadır.[4]

Bu şirketlerin başarısının en büyük nedeni tabii ki halkın istediği ürün ve hizmetleri sunmalarıdır. Dünyanın en değerli şirketlerinin bedava hizmetler sunuyor olması ilginç bir paradokstur. Google denince akla gelen ilk ürün arama hizmetleridir, Facebook'sa milyarlarca kişiyle iletişime girilebilecek sosyal bir alan sunar. Her iki hizmet de tüketiciler için ücretsizdir. Bu şirketler dünyadaki en değerli şirketler arasında yer almalarına rağmen, *Fortune*'un en çok kazanan 500 şirket listesine göre, önemli sayıda şirket daha fazla para kazanmaktadır.[5] Facebook

ve Google'ın, ücretsiz hizmetler sunmalarına rağmen gelir sağlayan çok sayıda hizmetleri bulunmaktadır, bunların içinde en önemlisi reklamlardır. Google'ın en büyük gelir kaynağı, Adwords ve Adsense hizmetleri aracılığıyla sağladığı reklam gelirleridir.

Örneğin Adwords'ün dev bir gelir kaynağı olmasının nedenlerinden biri, tüketicilerin tercihleri doğrultusunda çalışmasıdır. Herhangi bir sözcüğün aranmasında en uygun sonuçlar en üstlerde görünür. Şirketler Adword aracılığıyla arama sözcüklerini satın alabilir, böylelikle kendi ürünleri normal bir arama yapıldığında yan tarafta beliriverir. Fiyatı daima pazardaki rekabet belirler. Örneğin "tatil" sözcüğü turizm şirketleri için caziptir. Fiyat, "tatil" sözcüğüyle ilintili reklam vermekle kaç kişinin ilgilendiğine, ne kadar para ödemek istediklerine bağlıdır. Google, aramaların kullanıcılarla ne kadar alakalı olduğuyla ilgilendiğinden, çeşitli firmaların ödeyeceği fiyat da firmaların tekil arama sözcükleriyle ne kadar alakalı olduğuna bağlıdır. Bu tür reklamcılıktan Google yılda milyarlarca dolar kazanmaktadır.[6]

Reklamlar Facebook için de önemlidir. Şirket gelir kaynağı bulmakta yıllarca sıkıntı çektikten sonra son yıllarda reklam gelirlerinden gayet iyi paralar kazanmıştır.[7]

Bu şirketler dünyanın en değerlileri arasında yer almasına rağmen, pek çok şirket Google ve Facebook'tan oldukça fazla kazanmaktadır. Google ve Facebook'un, ana hizmetlerinin bedava olmasına rağmen pazar değerlerinin bu kadar yüksek olmasının nedeni, kullanıcı sayısı ve firmaların büyük miktarda veriye erişimidir. Şirketler verileri ve kullanıcıları gelire dönüştüren pek çok iş modeli yarattıklarında, hayal bile edilemeyecek kadar gelir olanakları ve mahremiyet sorunları ortaya çıkar.

Mahremiyet sorunları, bir anlamda, şirketlerin bedava hizmetlerinden kaynaklanmaktadır. Ürün siz olduğunuzdan, hizmetler ücretsizdir. Sizin kişisel verileriniz, ücretsiz hizmetlerin karşılığını ödemenin bir yolu olarak anlaşılır. Ne yaptığınız, nerede olduğunuz, internetteyken neyin üzerine tıkladığınız ve ne satın aldığınız değer kazanır. Sizin verileriniz ve kendiniz, sizi ticari anlamda ilginç kılacak bir biçimde tümleştirilir.

Ancak bu durum çok sorunludur. *To Save Everything Click Here: The Folly of Technological Solutionism* [Her Şeyi Saklamak İçin Buraya Tıklayın: Teknolojik Çözümcülüğün Ahmaklığı] adlı kitabında, dünyanın önde gelen internet ekonomisi eleştirmenlerinden Evgeny Morozov, yeni teknolojinin büyük ölçüde ticari bir mantıkla işlediğini öne sürer.[8] Morozov, ticari şirketlerin vatandaşların kişisel verilerini kapsamlı ticarileştirmelerine izin verilecekse bile, nereye kadar izin verilebileceği sorusunu ortaya atacak kadar ileri gider. Kişisel verilerin pazarını, canlı organ pazarıyla kıyaslar.[9] Bu biraz abartılıdır ancak, kişisel verilerin nasıl kullanılacağına dair daha esaslı tartışmaları teşvik etmemiz gerektiği konusunda hemfikirim çünkü, vatandaşların verilerinin büyük ticari değer taşıdığına hiç şüphe yoktur.

Guardian'da çıkan bir makaleye göre, Facebook kullanıcısı, şirket için günümüzde ortalama 12 dolardan fazla gelir sağlamaktadır ve bu miktarın artması beklenmektedir.[10] Bu durumda verilerimizi ucuza mı sattığımız sorusu ortaya çıkar. Yazar Eirik Newth *İzleme Toplumu* kitabında tam olarak bunu yaptığımızı belirtmektedir.[11] Newth, müşterilerin yönünden bakacak olursak, reel kaybın belki de özel hayatımızı kaybetmemiz değil, tüketicilerin kişisel verilerini çok ucuza satması olduğunu yazar. Pek çok kişinin özel hayatını (bedava) hizmetler karşılığında paylaşmayı seçmesi tabii ki normaldir. Pek çoğumuz iyi, ucuz, uygun hizmetlerle ilgileniyoruz ve özel hayatımızla ilgili pek endişe duymadan, kişisel verilerimizin ticari amaçlarla kullanılmasını kabul etmeye hevesli görünüyoruz.

Bu tutum, şirketlerin iş modellerinin kişisel verilerimizi kötüye kullanmayacağına aslında itimat ettiğimizin delili. Bu da şirketleri, bu güveni suiistimal etmemeye teşvik ediyor. Suiistimal ederlerse, müşteri ve kâr kaybına uğrama riskine girerler.

Ayrıca tüketicilerin, ticari şirketlerle ne gibi anlaşmalar yaptıklarından tamamen haberdar olup olmadıkları pek net değil. Aslında hiç haberleri olmadığına inanmamız için neden bile var. Öte yandan, bu bir sorun olarak görülmüyor. Tam tersi, şirketlerin bizim verilerimizi kötüye kullanmayacaklarına dair, halk arasında yaygın bir inanç söz konusu. Resmi kurumlarda ve özel şirketlerde sürekli veri sızıntıları

olmasına rağmen, şirketlerin, hakkımızda topladıkları veriler üzerindeki kontrollerini kaybedecekleri konusunda da vatandaşlar endişeli değil.

İzleme ekonomisine karşı kısıtlı bir direnişin olmasının bir diğer açıklaması, genel bir kabullenme olabilir. Pennsylvania Üniversitesi'nin bir araştırmasında, Amerikalıların çoğunun kişisel verilerini daha iyi hizmetler karşılığı değiş tokuş etmeye kuşkuyla baktığı, ancak yine de gelişime karşı durmanın faydasız olduğunu düşündükleri için bunu yaptıkları öne sürülmüştür. Araştırmaya katılanların büyük çoğunluğu, şirketlerin nasıl olsa özel hayatlarını ortaya dökebileceğini, bu yüzden de daha iyi ve ucuz hizmetler karşılığında veri sunabileceklerini belirtmiştir. Dijital ekonomi hakkında daha fazla bilgi edindikçe, ucuz hizmetler karşılığı kişisel bilgilerinizi değiş tokuş etmeye aktif olarak katılma olasılığınızın daha yüksek olduğu görülmüştür.[12]

Onay

Bağımsız insanların kendi çıkarları hakkında aklı başında kararlar alma yeteneğine sahip olduğuna inanmak önemli bir liberal ilkedir. Bu, vatandaşların her zaman doğru kararları alacağı anlamına gelmez, yanlış seçimleri ortadan kaldırmak mümkün (ya da istenen bir şey) demek de değildir. Öncelikle, neyin "kötü seçim" olarak kabul edildiği de belli değildir. İnsanların farklı öncelikleri vardır. Siz özel bilgiyi paylaşmaya olumlu bakarken, ben karşı görüşlere sahip olabilirim. Bu, birinin diğerinden daha doğru olduğu anlamına gelmez. İkinci olarak, objektif bir "doğru seçim" var olsaydı bile, istersek "yanlış"ı da seçme olanağımız olmadığından, seçim özgürlüğü ve kişisel otonomiden söz etmek zorlaşır.

Yine de ticari şirketlerle muhatap olduğumuzda, iyi bilgilendirilmiş seçimleri ne derece yapabilecek ve kavrayabilecek durumda olduğumuz tartışılır. Sosyal medyanın kullanım koşullarını kabul edenlerden kaçı mahremiyeti koruma bildirimlerini gerçekten okumuştur? Okudunuz diyelim, anladınız mı? İnternetteki lisanslı ürünlere dair mahremiyeti koruma bildirimlerini kaç kişinin okuduğu hakkında tutarlı rakamlar bulunmamaktadır ancak, bu tür bildirimleri gerçekten okumanız için

ayırmanız gereken zamanı göz önünde bulundurursak, bu sayının oldukça düşük olduğuna inanmamız için nedenlerimiz var.

Obama'nın Bilim ve Teknoloji Kurulu (PCAST), onay pratiğinin, bugün işlediği şekliyle gerçek dünyadan çok hayal dünyasına uygun olduğu konusunda çok nettir.

> Bildirim ve onay, günümüzde, tüketicinin mahremiyetini korumak için en kapsamlı biçimde kullanılan yöntemdir. Kullanıcı yeni bir uygulamayı kendi mobil aletine indirdiğinde ya da bir ağ servisi için hesap oluşturduğunda, kullanıcının uygulama ya da hizmeti kullanmaya başlamadan önce olumlu onay vermek zorunda olduğu bir bildirim ekranda gözükür. Bir hayal dünyasında kullanıcı bu bildirimleri gerçekten okur, yasal sonuçlarını anlar (gerekirse avukatına danışır), benzer hizmet sağlayıcılarından daha iyi mahremiyet işlemleri alabilmek için pazarlık edip sadece ondan sonra onayladıklarını belirtmek için tıklar. Gerçek farklıdır.[13]

Terms & Conditions May Apply [Hüküm ve Koşullar Uygulanabilir] adlı belgeselde film yapımcıları, ticari şirketlerin mahremiyet politikası yüzünden özel hayatın nasıl zora sokulduğunu anlatır.[14] Belgesele göre, çeşitli internet sitelerinin kullanım şartlarını okumak için her yıl 180 saat gerekmektedir, yani bunları okumak için gerçekten vakit ayıracak olursanız. Şirketlerin öne sürdüğü koşullar pek ufak tefek sayılmaz. Facebook, sizin tüm bilgilerinizi ticari amaçlar için kullanma hakkını elinde tutar. Sosyal internet sitesi Linkedin de aynı şartlarla çalışır. Milyonun üzerinde Norveçli kullanıcısı olan Snapchat, son günlerde şartlarını değiştirdi:

> İçeriğinizi, her türlü medya ve dağıtım yöntemi (şimdi bilinen veya daha sonra geliştirilen) üzerinden saklamak, kullanmak, yeniden üretmek, birleştirmek, düzeltmek, parçalarını kullanmak, yayınlamak, radyo-televizyonda yayınlamak, dağıtmak, gazetelere satmak, reklamını yapmak, sergilemek ve kamuya açık şekilde göstermek için Snap'a, dünya çapında, süresiz, telifsiz ve devam eden izin vermektesiniz.[15]

Kullanıcıların kişisel resimlerini paylaştıkları sosyal internet sitesi Instagram da Snapchat ile aynı şekilde, kullanıcıların yayınladığı resimleri telifsiz kullanma hakkına sahiptir. Pek çok kullanıcının bu duruma itirazı olmayabilir, ne de olsa hizmetler bedavadır ancak Instagram

kullananların pek çoğu, şirketin kişisel resimleri istediği şekilde kullanabileceğinden habersizdir. Kullanıcıların bunu bilmek zorunda oldukları ileri sürülebilir şüphesiz, en azından mahremiyet konusunda endişe duyanların. Ancak içine düştüğünüz durumun karmaşıklığı ve kapsamı göz önünde bulundurulduğunda şartları bilmemenin bir ihmal olarak değerlendirilmesi gerektiği hemen varılabilecek kesin bir sonuç değildir.

Tüketiciyi Koruma Kurumu, uygulamaların kullanım şartlarının ne kadar saçma işlediğini ortaya koymak için, çeşitli uygulamaların kullanım şartlarını okumak amacıyla 24 saatlik canlı yayın yaptı.[16] Bir diğer ilginç, aynı zamanda açıklayıcı örnek de, İngiltere merkezli Game Station internet şirketinin 2010 yılında yaptığı 1 Nisan şakasıdır. İnternet sitelerinde alışveriş yapmanın şartlarından biri, müşterinin ruhunu satmasıydı.[17] Game Station, 10 kişiden 8'inin, sitede alışveriş yapmak için gerekli şartları okumadığını belirtti, bu da vatandaşların internetteki koşullar ve şartlar karşısındaki tutumunu gözler önüne seren bir olaydır.[18]

Peki ama neden böyle oluyor? Pek çoğumuzun internet etkinliklerinin altında yatan koşulları kontrol etmememizin nedenleri nedir?

Ne yayılan elektronik ayak izleri sayısının ne de ihlallerin doğuracağı tehlikelerin bizi pek endişelendirmemesi en önemli neden olabilir. Öte yandan şirketlerin internet anonimliğini yok etmeyi planlamaktaki çıkarlarını küçümsememeliyiz. Anonim kullanıcıların kötü bir iş modeli olduğu ortaya çıkmıştır, oysa elektronik veriye erişim, büyük ticari potansiyele sahiptir.

Şirketler, onayın, tüketicilerin şartları kabul edip etmemekte özgür olduğunu gösterdiğini ileri sürer. Bu, liberallerin anlayabileceği bir argümandır. Pazar ekonomisi sisteminde vatandaşlar, kendi hayatlarıyla ilgili kararları kendileri almak zorundadır. Her iki tarafın da anlaşmadan eşit faydalar sağlayacağının garantisi yoktur, ancak pazarlar sübjektif bir fayda üzerine kurulur ve bir taraf diğerinden daha avantajlı olsa da, bir işlemi gönüllü gerçekleştirmek, her iki taraf için de hiç gerçekleştirmemekten daha faydalıdır. İşlemin gerçekleşmesinin gerçekleşmemesinden

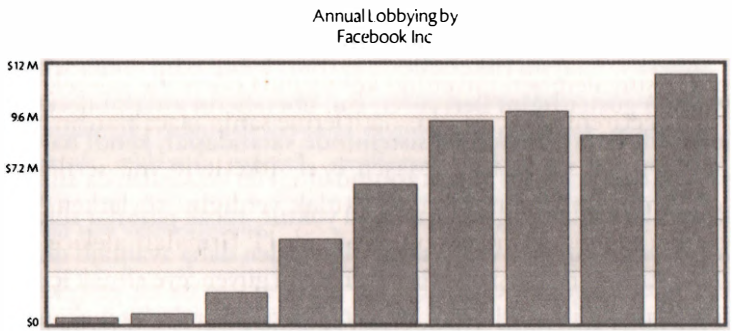
daha çok işlerine geldiğini iki taraf birden düşünmezse, bu işlem kural olarak gerçekleşmez.

Bununla birlikte, pazar ister kişinin istediği anlaşmaları yapma hakkının dahil olduğu gönüllülük üzerine kurulmuş ister kurulmak zorunda olsun, "mantıksız anlaşmalar"a itibar edilmemesi gerektiğinde pek çoğumuz hemfikirizdir. "Mantıksız anlaşmalar"dan ne anlaşıldığı bir tartışma konusudur tabii, ancak buna insanların kendilerini esir olarak satmaları ya da ruhlarından vazgeçmelerini içeren anlaşmalar örnek verilebilir. Başka bir deyişle, bir anlaşmayı gönüllü olarak kabul etmek için, ayrıca vatandaşların mahremiyet ilkelerini hesaba kattıklarını umduğumuzda "mantıklılık" talep ederiz.

Günümüzde, şirketler tarafından sunulan şartları vatandaşların dikkate almasını beklemenin çok mantıksız olduğu ortadadır. Yine Obama'nın kurulundan alıntı yaparsak: "Bildirim ve onay, mahremiyetin korunmasının yükünü esasen bireye yıkmaktadır, ki bir haktan kastedilen şeyin tam tersidir bu."[19] Günümüzün onay uygulaması, özel hayatın korunması açısından tatmin edici değildir.

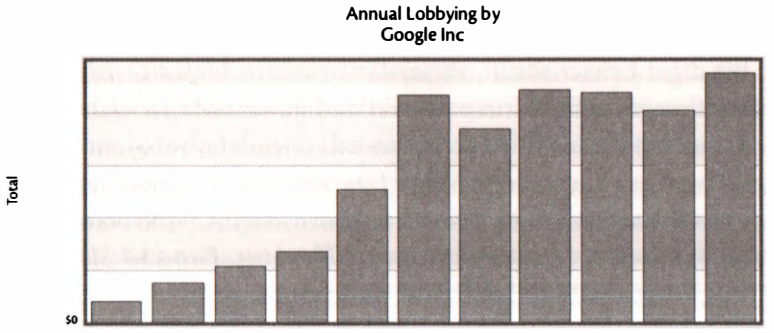
Büyük şirketler, onay uygulamalarının özel hayat için çok az tatmin edici olmasından pek endişe duymamaktadır. Bunun ışığında, Facebook ve Google'ın ABD Kongresi'ni etkilemek için ne kadar çok para harcadığını görmek düşündürücüdür.

Aşağıda Facebook'un ABD Kongresi'nde lobicilik için harcadığı paraların bir şemasını göreceksiniz.



Kaynak: Center For Responsive Politics

Aşağıda da Google'ın ABD Kongresi'nde lobi faaliyetlerine yönelik harcamalarına genel bir bakış yer almaktadır.



Kaynak: Center For Responsive Politics

Center For Responsive Politics adlı kurum, ABD siyasetinde para kullanımı hakkında bilgilendirme üzerine uzmanlaşmıştır ve onların görüşüne göre, Facebook ve Google son beş yıl içerisinde Kongre'de lobicilik faaliyetleri için 100 milyon dolar harcamıştır.[20] Bu şirketlerin lobicilik faaliyetleri için oldukça büyük miktarlarda para harcamaları ne bir sürpriz ne de eleştirilecek bir durumdur, ancak toplum ve siyasetçiler bu şirketlere, ticari amaçları olmayan iyi niyetli şirketler yerine, çıkarları olan özel şirketler olarak davranmalıdır.[21]

Toplumun ticari firmalar karşısındaki bir avantajı, firmaların müşterilerin insafına kalmış olmasıdır. Parlamento üyesi Michael Tetzchner (Sağ Parti), *Mahremiyeti Savunmak Adına* kitabında, mahremiyet için en büyük tehdidin iş dünyası olmadığını yazar: "Daha bilinçli müşteriler, girişimcilere veri güvenliği konusunda taleplerle gelecek ve başka teklifler getirenleri seçme alternatiflerine sahip olacaklardır."[22]

Piyasa mekanizmaları, esasen özel şirketlerin müşterilerinin sesine, resmi tekellerden daha çok kulak verdiğini söylerken haklıdır. Snowden'ın ifşaatlarından sonra, büyük IT firmaları alelacele, devlet istihbaratına karşı müşterilerinin verilerini güvenceye almak için güvenlik uygulamalarını sıkılaştıracaklarını belirtiklerinde, bu mekanizmanın işlediği çok güzel ortaya çıktı.

Daha bilinçli müşterilerin ortaya çıkmasının koşulu, vatandaşlar olarak bizim, günümüz ticari pazarında iyi bilgilendirilmiş bir biçimde hareket etmemizi sağlayacak tatminkâr olanaklara sahip olmamızdır. Bu, Obama'nın kurulunun belirttiği gibi her zaman söz konusu değildir.

Bir diğer benzer sorun, varsayılan ayarların (*default settings*) nasıl değiştirileceğidir. Bunların nasıl ayarlandığı, vatandaşlar olarak bizim, kendi özel hayatımızı fiilen korumamızda önemli bir rol oynar. Richard Thaler ve Cass Sunstein'in *Nudge* (*Dürtme*) adlı kitabında yazdıkları gibi, varsayılan ayarları çok az insan değiştirmektedir.[23] Ekonomi dalında Nobel ödülü olan Daniel Kahneman, *Thinking, Fast and Slow (Hızlı ve Yavaş Düşünme)* adlı kitabında, varsayılan ayarların insan davranışı üzerindeki özel etkisine dikkat çeker. [24]

Biz vatandaşların hangi ayarları istediğimize kendimizin karar verebilmesinin ve bu olanağa sahip olmamızın en önemli nokta olduğu öne sürülebilir. En azından, mahremiyeti koruma ayarlarını kendimizin seçebilmesi gerekmektedir. Ancak bu yeterli değildir. Facebook'un, 2009'da olduğu gibi bilgi vermeden, varsayılan ayarları değiştirmeye karar verebilmesi gerçeği tüketiciler için bir sorundur. 2009'da Facebook, bilginin en çok sayıda kişiyle paylaşılabilmesi için ayarları değiştirdi. Bu da veriye erişimi artırıp Facebook için daha büyük bir potansiyel sağlamış oldu. Olaya ticari mantıkla yaklaştığınızda, bu değişiklikleri anlamak zor değil, iş modelinin taşıyıcı öğesi bu. Benzer bir örnek de, Eric Schmidt'in şirketin bunu yapmaya niyeti olmadığını daha önceden açıklamış olmasına rağmen, Google'ın 2012 yılında farklı servislerden gelen tüm kullanıcı bilgilerini tek bir profil altında toplamasıdır.[25] Google'ın, tüm hizmetlerini bir araya getirmeyi seçmesinin nedeni, ticari amaçla kullanmak üzere kullanıcılardan en çok veriyi toplama ihtiyacıdır, örneğin kullanıcıların dijital tutumlarına dayalı reklamlar sunmak gibi. Çoğu zaman bu uygundur ancak, kişisel verinin paylaşımı için makul bir şekilde onay vermiş olmamız, verilere kimin erişebileceği ve bunları nasıl kullanacağının da saydamlık kazanması gerekmektedir.

PCAST, günümüzdeki uygulamaların piyasa başarısızlığı olduğunu iddia eder ve şunları yazar:

> Malı temin eden, "al ya da bırak" tarzı karmaşık şartlar teklif etmektedir, bir sürü yasal ateş gücünü de arkasına alarak, kullanıcıya da pratikte, teklifi değerlendirmek için zihinsel bir gayret göstermeye ayrılmış yalnızca birkaç saniye verilir çünkü kullanıcının amacı olan işlemi tamamlamak için onay gereklidir, çünkü şartlar çabucak kavranamayacak kadar zordur. Bu bir tür piyasa başarısızlığıdır. Başka durumlarda, bunun gibi bir piyasa başarısızlığı, önemli sayıda kullanıcıyı temsil eden ve onlar adına pazarlık yapan üçüncü bir taraf aracılığıyla hafifletilebilir.[26]

Günümüz onay uygulamasına en iyi alternatif, anlaşmaları ve şartları mahremiyeti koruma açısından standartlaştıracak yöntemler bulmaktır, böylelikle onay uygulaması biz tüketicilere gerçek anlamda uygun olabilir. Diğer bir olanak da özel hayatın korunma derecesini değerlendirebilecek üçüncü bir taraf için (örneğin, Veri Koruma Kurumu, Teknoloji Kurulu vs.) piyasada yer açmaktır. Ayrıca, "mahremiyeti koruma değerlendirmesi" yapan özel girişimler, ücret karşılığı, özel hayatın korunması için standart profiller geliştirip bunları uygulama konusunda uzmanlaşabilir. Buna ek olarak Apple, Microsoft ve Google gibi büyük uygulama dükkânları, kendi platformlarında olan farklı uygulamaların mahremiyetini ne derece koruduğunu kendileri değerlendirebilir. Son olarak, bizlerin daha uyanık olmamız ve vermemiz gerekmeyen bilgileri paylaşmamamız da önemlidir.

Üçüncü Taraflarla İşbirliği: Şirketler ve Yetkililer

Vatandaşların ticari şirketlere bilgilerini sunarken dikkatli olmaları için bir diğer neden de bu bilgilerin üçüncü kişilere satılabilme ve onlar tarafından kullanılabilme olasılığıdır.

Hüküm ve Koşullar Uygulanabilir adlı belgeselde, ticari şirketlerle istihbarat servislerinin ilişkisi mercek altına alınır. Snowden'ın ifşaatları bu işbirliğinin ne kadar derinlere uzandığını göstermiştir. İstihbarat servislerinin, büyük teknoloji şirketleriyle işbirliği yapmakla ilgilenmesinin nedenlerinden biri, 11 Eylül 2001 terör olayları ve bu olayların sonrasında "teröre karşı savaş"tır. New York'a yapılan terör saldırısının en doğrudan sonucu, ABD'li yetkililerin interneti sistematik bir biçimde izlemeye almasıdır, bundan sonra da anonim iş görmek oldukça zorlaşmıştır.

Bu süreçte, güvenlik endişeleri ticari çıkarlarla iç içe geçmiştir çünkü internette anonimlik kötü bir iş modelidir. Bu anlamda, bizim mümkün olduğunca fazla elektronik ayak izi bırakmamız, büyük internet firmaları için ticari açıdan kârlıdır. [27]

Google'ın mahremiyet ilkelerinin 2000 yılından 2001 yılına nasıl değiştiğine bakmak yeterince açıklayıcıdır. Google'ın mahremiyeti koruma politikası, 2000 yılında anonimliği garanti ediyordu. Google, aynı bilgisayarın daha önce Google'ı ziyaret eden bilgisayar olup olmadığının kaydını tutmasına rağmen, bu kişinin kim olduğunu, hangi ülkede bulunduğunu bilemiyordu. 2001 yılında, mahremiyeti koruma ilkeleri şu şekilde değiştirildi: İhtiyaç duyulduğunda, Google yalnızca sizin kim olduğunuzu tanımlamakla kalmayıp üçüncü kişilerle bu bilgiyi paylaşabilecektir.[28]

PRISM programının gösterdiği gibi, teknoloji firmaları ve NSA arasında, kamunun haberi olmadan kapsamlı bir işbirliği yapılmıştır. Kişisel verilerin paylaşılmasıyla ilgili sosyal ölçüler, önceden olduğundan çok daha fazla paylaşma yönünde gelişme göstermiştir. Bu yüzden, istihbarat yetkililerinin bu akımdan yararlanmak istemeleri anlaşılır bir durumdur. Ancak mahremiyet açısından çok olumsuz olmasına rağmen, şirketlerin üçüncü kişilerle (yetkililerle) bilgi paylaşmaya istekli olmaları düşündürücüdür aynı zamanda.

Özel şirketlerle istihbarat birimleri arasındaki işbirliğinin ortaya çıkardığı siyasi sorunlardan biri de, işbirliğinin önemli ölçüde gizli yürütülmesi ve daha küçük programlara ayrılmasıdır. Bu yaklaşım, ABD'li yetkililerin internetin izlenmesi konusunda en başlardaki tutumundan oldukça farklıdır. İzleme için hazırlanmış ilk programlardan biri Toplam Bilgi Farkındalığı adını taşır ve tüm veri akışını saklamak amacıyla George W. Bush yönetimi tarafından 2003 yılında başlatılmıştır. Program, Mayıs 2003'te, yoğun eleştiriler sonucunda Kongre tarafından kısıtlanmıştır. Örneğin, Amerikan Sivil Özgürlükler Birliği (ACLU) programdan özel hayata tehdit olarak söz etmiştir.[29]

Bu programın başarısızlığının muhtemel nedeni, hedefinin kitlesel izleme olduğunu gizlememesidir. Bu program açık forumlarda tartışılmak zorunda kalmıştır, oysa sonraki izleme programları halktan

gizlenmiştir. Snowden'ın ifşaatlarının özel şirketleri kötü durumda bıraktığı ortadadır, yaptıkları işbirliği her ne kadar tüketicilerin şirketlere sırtını dönmesini şimdilik sağlamamış olsa da gelecekte firmaların, yetkililer karşısında tüketicilerin verilerine daha çok özen göstereceğine inanabiliriz.

Ne Tür Yasal Düzenlemeler?

ABD yasalarının Avrupa ve Norveç için önemli olmasının nedeni, Avrupa piyasasında çoğunlukla ABD'li şirketlerin faaliyet göstermesidir. Bu yüzden, onların mahremiyet ilkeleri, Norveç mahremiyet ilkeleri için çok büyük önem taşımaktadır. Örneğin, Norveç'teki iPhone kullanımı, ABD'de saklanan veriler üretir.

Bu durumda kimin yargı sistemi geçerli olacaktır? Hangi yasalar geçerli olacaktır ve bu yasalar nasıl uygulanacaktır? Örneğin, AB'nin mahremiyet yasaları, veriler ABD'de saklanıp işlendiğinde, Avrupa vatandaşlarının özel hayatlarının ihlal edilmemesini nasıl sağlayacaktır? Avrupalılar, Google ve ABD'li yetkililerin Avrupa vatandaşları hakkında hangi verileri sakladıkları hakkında kısıtlı bilgiye sahiptir.

Tüketicinin (Avrupa) ve firmanın (ABD) farklı yargı alanlarına sahip olmasının altında yatan küresel soruna, ruhsat vermekle pratik bir çözüm bulunmuştur. Avrupa'da bulunan şirketler, ABD'li servis sağlayıcılarına yasal olarak veri aktarabilirler.

Bu düzenlemeye Güvenli Liman (*Safe Harbour*) adı verilmiştir. [30]

Güvenli Liman anlaşması, 2000 yılında ABD Ticaret Bakanlığı ve Avrupa Komisyonu arasında yapılmıştır. Anlaşmanın nedeni, AB'nin 1995 tarihli mahremiyet yönetmeliğidir. Bu yönetmeliğe göre, Avrupa'daki kişisel bilgilerin AB dışındaki ülkelere (AEA–Avrupa Ekonomik Alanı) transferi koşullu kabul edilmiştir. Bu şekilde veri transferlerinde, her bir durum için ayrı ayrı özel onay alınması, ülkelerin AB'ye bilgileri yeteri kadar koruyacaklarının garantisini vermeleri gerekiyordu. Dijital Devrim'in ve AB'den ABD'ye veri transferlerinin dev boyutlara varması bu düzenlemeyi yetersiz kıldı.

Avrupa'daki şirketlerin, kişisel verileri ABD'li servis sağlayıcılarına her transfer etmek istediklerinde özel onay almak durumda kalması

işleri yokuşa sürüyordu. Bu yüzden ABD ve AB/AEA arasında, kişisel verilerin transferini kolaylaştırmak amacıyla Güvenli Liman anlaşması yapıldı. Anlaşmaya göre şirketler, ABD'li yetkililerin AB'nin mahremiyeti koruma yönergesindeki ilkeleri koruyabileceğini garanti etmesi koşuluyla, ABD ve AB arasında veri transfer edebilecekti. Şirketler "Güvenli Liman" ruhsatı alabilecek ve Avrupa'nın kişisel bilgilerini yasal olarak saklayıp transfer edebileceklerdi. [31]

24 yaşındaki Avusturyalı Max Schrems'in 2011 yılında Güvenli Liman uygulamasına karşı Avrupa Adalet Divanı'nda açtığı dava, 6 Ekim 2015 yılında olumlu sonuçlandı. Maximillian Schrems'in veri koruma komiserine karşı açtığı C-362/14 nolu davada, Avrupa Birliği Adalet Divanı, "Komisyonun ABD Güvenli Liman Anlaşması'nın geçersiz olduğunu" ilan etti çünkü bu karar, Avrupalı vatandaşların mahremiyetinin korunması için yeteri kadar garanti vermemekteydi.

Adalet Divanı, mahremiyetin AB vatandaşları için temel bir hak olduğuna dikkat çeker, ABD'nin uzun zamandır ulusal güvenliğin mahremiyetin önüne geçmesine izin vermesinden dolayı, ABD'li yetkililerin anlaşmanın taahhütlerini yerine getirmelerinin zor olduğunu görmüştür. Mahkemenin kararı, mahremiyetin korunmasıyla ilgili Avrupa'nın talebini çiğneyen bir uygulamayı ifşa eden Snowden'dan bağımsız değerlendirilemez. Mahkeme kararını etkileyen bir diğer önemli gerçek de ulusal koruma kurumlarının Avrupalı vatandaşların izlenmesi konusunda herhangi bir denetiminin söz konusu olmaması ve Avrupalı vatandaşların, kişisel bilgilerini istismar edenleri ABD'de mahkemeye verme olanaklarının kısıtlı olmasıdır.

Mahkeme kararının birincil sonucu, Avrupa ve ABD'nin kendilerini belirsiz bir hukuksal durum içinde buluvermesidir. Avukat Jon Wessel-Aas, ABD'ye kişisel bilgiler aktaran firmalar için kararın çok dramatik olduğunu belirtir çünkü, firmaların dayandığı hukuksal temel geçersiz ilan edilmiştir.[32] Mahremiyet Anlaşmazlıkları Kurulu Başkanı ve hukukçu Eva Jarbekk, *Aftenposten* gazetesinde krizi tırmandırmanın gerekmediğini, ancak veri aktarımı için gerçekçi alternatiflere bakmak gerektiğini yazmıştır.[33]

Şirketlerin Avrupa ve ABD arasında kişisel veri aktarımı yapamamaları gibi bir durumu düşünmek zor olduğu için taraflardan beklenen oldu ve 2016 yılının başında, şirketlerin temel veri koruma haklarını ihlal etmeden kıtalararası kişisel bilgi aktarmaları konusunda anlaşmaya varıldı. Bu anlaşmaya, AB-ABD Mahremiyet Kalkanı adı verildi.

AB-ABD Mahremiyet Kalkanı, Avrupa Ekonomik Alanı dolayısıyla Norveç'i de kapsamaktadır. *Dagens Næringsliv* gazetesinde yer alan yazılarında Håkon Haugli (Abelia) ve Kristine Beitland (Microsoft), anlaşmanın hem Norveç hem de Avrupa iş dünyası için çok önemli olduğunu, bununla birlikte Norveç mahremiyetinin korunması gerektiğini belirtir. Ayrıca Mahremiyet Kalkanı, artan dijital gelişime kolay uyum sağlamayı mümkün kılan dinamik bir anlaşmadır.[34] Anlaşmanın çerçevesi, şirketlerin kişisel verileri işlemesine dair güçlü yasal düzenlemeler içerir. Örneğin, bu anlaşmaya katılmak isteyen tüm şirketler, anlaşmadaki mahremiyet ilkelerini nasıl uygulamayı düşündüklerini göstermek zorundadır. Bir diğer değişiklik de şirketlerin her yıl denetlenmesi ve yeniden ruhsat almalarının düzenlenmesidir.

Çerçeve anlaşma, ABD'li yetkililerin Avrupalıların kişisel bilgilerine nasıl erişebileceğine dair mevzuatı daha güçlü düzenler. Bu sıkılaştırmalara ek olarak, ABD Ticaret Bakanlığı anlaşmaya uyulduğuna dair yıllık raporlama yapacaktır. Üçüncü değişiklik, şikâyetlerin ne şekilde ele alındığını inceleyen, ABD Dışişleri Bakanlığı'na bağlı kamu denetçisi (ombudsman) düzenlemesidir. Son olarak, AB-ABD Mahremiyet Kalkanı için bağımsız bir tahkim düzenlemesi yapılacaktır. Bu yapının içinde hem Avrupa'dan hem de ABD'den temsilciler yer alacaktır. Tahkim Komisyonu, gösterilen adaylar arasından seçilen üç üyeden oluşacaktır. Bu düzenleme vatandaşlar için ücretsiz olacaktır ve kişisel bilgileri işleyen şirketler, şikâyetleri verilen süre içerisinde incelemek zorundadır, şikâyetlerin takibi ABD Ticaret Bakanlığı'nın güvencesi altındadır, bundan dolayı, şikâyet düzenlemesinin işleyişine dair yıllık inceleme yapılacaktır.[35]

Çerçeve anlaşmayı gerçekleştirmekte başarılı olunsa da hâlâ muğlak olan hukuksal sorunlar mevcuttur. AB içerisinde, "Madde 29 Çalışma Grubu", Mahremiyet Kalkanı anlaşmasını tartışmaktadır. Bu gruba, ulusal veri koruma denetçiliğinden (DPA), AB'nin kendi veri koruma

denetçiliğinden (Avrupa Veri Koruma Denetçiliği – EDPS) ve AB Komisyonu'ndan temsilciler dahildir. Birlikte, AB içindeki mahremiyeti korumak amacıyla bir işbirliği organı oluştururlar ve AB sistemine, mahremiyet hukukunu nasıl dikkate alacaklarına dair tavsiyelerde bulunurlar. Madde 29 Çalışma Grubu, şu ana kadar Mahremiyet Kalkanı anlaşmasına eleştirel yaklaşmıştır, ancak AB'nin çerçeve anlaşmasını bir kenara bırakması şeklinde bir tavsiyede de bulunmamıştır. Öte yandan grup, en son 1 Haziran 2016'da, Mahremiyet Kalkanı'ndaki mahremiyet kararlarının iyileştirilmesi gerektiğinin altını çizmiştir.[36]

Hem ABD hem de AB için şimdi yapılması gereken, sonunda onaylanmış bir anlaşma imzalamaktır, hukuksal temel halen muallaktır. AB'nin Güvenli Liman'a karşı aldığı mahkeme kararı, ABD'li yetkililerin, Avrupa vatandaşlarının özel hayat hakkını yeteri kadar koruyamadığını söylemektedir. Mahremiyet Kalkanı'nın, AB Mahkemesi'nin özel hayat talebi kararına uyup uymayacağı net değildir. İş Dünyası Merkezi ve Kamu Siyaseti kurumunun başkanı Larry Downes, *Harvard Business Review*'da, mahkeme kararının yarattığı etkilerin muallak olduğunu ve olayın netliğe kavuşmasının bir yıl sürebileceğini yazar:

> AB'nin mustarip olduğu karmaşık bürokrasinin bir aynası olan Mahremiyet Kalkanı anlaşmasının son tasdiki, resmi ve yarı resmi mahremiyeti koruma yapılarının, Komisyonun kendisinin ve üye devletlerin bir dizi baş döndüren incelemelerde bulunmasını içermektedir. Hukuksal sorunlar muhakkak ortaya çıkacaktır. Belirsizlik, internet bazlı şirketlerin yurtdışında iş yapmasını aylarca, belki de yıllarca zorlaştıracaktır.[37]

Rekabette Avantaj Olarak Mahremiyet

Hem onay uygulaması hem de büyük şirketlerin istihbarat servisleriyle işbilirliği, özel hayat olanaklarının ticari çıkarlar karşısındaki durumu hakkında endişeye kapılmamıza neden olmaktadır. Pek çok şirket, müşterilerinin kişisel verilerini korumakta yeterince başarılı olamamıştır. Tüketicilerin verilerinin özensizce kullanımı uzun vadede önemli sonuçlar doğurabilir, özellikle daha iyi alternatifler ortaya çıktıkça. Bu yüzden, mahremiyeti korumayı öne çıkararak rekabet avantajı sağlamayı giderek daha fazla şirketin istemesi sevindiricidir.

En heyecan verici ifadelerden biri, Apple'ın patronu Tim Cook'un 1 Haziran 2015'te yaptığı yorumlardır. Elektronik Mahremiyet Bilgi Merkezi'nde (EPIC) yaptığı konuşma sırasında Cook, Apple'ın, müşterilerinin özel hayatını korumayı istediğinin altını çizerken, özel hayat hakkını net bir biçimde savunmuştur:

> Pek çoğunuz gibi biz de Apple'da, müşterilerimizin mahremiyet ve güvenlik arasında kalıp birinden ya da diğerinden vazgeçmesi fikrine karşıyız. Her ikisi için de eşit ölçüde hizmet sunmalıyız ve sunmak zorundayız. ABD halkı bunu talep ediyor, nayasa bunu talep ediyor, ahlaklılık bunu talep ediyor. Bedava olduğunu sandığınız ancak aslında çok büyük bedeller ödenen bir hizmet için özel hayatınızdan asla ödün vermemeniz gerektiğini düşünüyoruz. Sağlığınız, finansal durumunuz ve konutlarınız hakkındaki verileri aletlerimizde sakladığımız için, bu durum özellikle şimdi için doğrudur. Bizler, müşterilerin kendi bilgileri üzerinde denetimleri olmasına inanıyoruz. Bu sözümona bedava hizmetleri beğeniyor olabilirsiniz, ancak e-postalarınızın, arama geçmişinizin ve hatta şimdilerde aile fotoğraflarınızın veri kazımaya tabi tutulup, kim bilir hangi reklam amacıyla satılmasına, bunun değmeyeceğini düşünüyoruz. Ve bizce, günün birinde müşteriler de işin iç yüzünü görecekler.[38]

Apple uzun zamandır, örneğin şu bilgileri sunarak, mahremiyeti daha iyi koruyanlardan olmuştur:

1. Hangi verileri saklamaktadır?
2. Bu verileri neden saklamaktadır?
3. Bu verileri ne için kullanmayı düşünmektedir?[39]

Bu, daha çok sayıda firmanın ders alması gereken bir uygulamadır, belki gelecekte o da olur. Tim Cook'un verdiği sinyaller, dünyanın en büyük IT firmalarının, politikalarını –ahlaki nedenlerden değil de kârlı olduğu için– değiştirme arifesinde olduğunu gösteriyor. Aynı zamanda, hatırlamamız gereken, Apple ve Tim Cook'un çoğunlukla donanım ürettiğidir, kişisel bilgiler üzerinden büyük kâr elde etmedikleri için, bu şekilde çıkış yapmak onlara pahalıya patlamaz. Bu yüzden asıl sorun, Facebook ve Google gibi devlerin, Güvenli Liman kararı ve Snowden ifşaatları karşısında ne yapmayı seçeceğidir.

Bu şirketlerin daha önceki patronlarının beyanları endişe vericidir. Facebook'un kurucusu ve CEO'su Mark Zuckerberg, 2010 yılında,[40] "özel hayatın hükmü kalmadı" derken, onun "sosyal bir norm" olmaktan çıktığını anlatmaktadır. Bir ay önce de Eric Schmidt Google'da, "Başkalarının bilmesini istemediğiniz bir şeyler yapıyorsanız belki de her şeyden önce bunu hiç yapmamanız gerekmektedir," demiştir.[41]

Olumlu haberse, tutumların değişiyor olmasıdır; Google ve Facebook'ta da. Teknoloji şirketlerinin veri paylaşımı yaparak NSA'ya yardım etmesi hakkındaki iddia ve tartışmalar, pek çok tüketiciyi endişelendirmiş ve doğal olarak, büyük firmaların, internette paylaşılan kişisel bilgilerin iyi korunması hizmetini yerine getirmezlerse çok para kaybedebileceklerini fark etmelerine neden olmuştur. Hizmetlerine ve özel hayatın korunmasına karşı güveni artırmaya katkıda bulunacak tedbirleri branşın kendisi alabilir.

Tüketiciyi Koruma Kurumu'nun tavsiyelerinden bazıları şöyledir:

Veri toplanması ve kullanımında daha fazla şeffaflık.

Kullanıcılara, kendi verilerinin nasıl kullanıldığına dair daha fazla erişim hakkı.

Gereğinden fazla bilgi toplanmaması.

Bilginin bir müddet sonra silinmesi.

Ayrımcılığı önlemek – en azından ayrımcılığın nasıl yürüdüğü konusunda açık olmak.

Mahremiyet hakkında anlaması kolay, iyi branş standartları hazırlamak. [42]

YEDİNCİ BÖLÜM

Uluslararası Hukuki Gelişim ve Teröre Karşı Savaş

The Road to Serfdom (*Kölelik Yolu*) adlı kitabında F.A. Hayek, "Özgür ve özgür olmayan toplumlar arasındaki en büyük fark, vatandaşların hukuk devleti ilkelerinden (*The Rule of Law*) ne ölçüde yararlanabildiğidir," diye yazar.[1] Özgür bir toplumun özelliği yönetenlerin sınırlamalara tabi olmasıyken, özgür olmayan bir topluma belirsizlik damgasını vurmuştur.[2] Hayek'e göre, yetkililerin yaptıklarının belirgin ve anlaşılır yasalarla sınırlandırılması bağlamındaki özgür toplum tanımı sadece bir üslup meselesine indirgenemez, aynı zamanda işleyiş yönünden de geçerlidir. Bir toplum yalnızca hukuk devleti ilkeleriyle yönetiliyorsa, resmi kuralların (yasaların) uygulanması işlemi de önceden belirli çerçeveler içinde yapılır.

Özel hayatın en iyi nasıl korunacağı sorusuna gelince, prosedürel yönlerine de büyük özen gösterilmiş, iyi işleyen hukuki bir altyapı çok önemlidir. Yeni yasaların hazırlanışı, özel hayata karşı olası tehditlerin mümkün olduğunca etraflı değerlendirmesini içermelidir.

Mahremiyete dair yasama, özellikle dört nedenle karmaşık bir sorundur.

İlkin, mahremiyetin korunması çoğunlukla çatışan çıkarlarla ilişkilendirilir, örneğin mahremiyet ile verimli hizmetler arasındaki denge.

İkinci olarak, dijitalleşme karmaşıklığın daha da artmasına katkıda bulunur.

Üçüncü olarak, minik adımlar zorbalığından söz edebiliriz. Genel olarak tek başına ele alındığında, artan izlemenin büyük bir etkisi olduğundan söz edemeyiz ancak tüm öğeleri bir araya getirince ortaya çıkan toplam, özel hayat için tehlike oluşturur.

Dördüncü olarak, küreselleşme, sadece ulusal yasalara sırtımızı yaslamayı zorlaştırır: Pek çok Norveçli'nin, verilerinin önemli kısmının yurtdışında işlenip saklandığı akıllı telefonlara sahip olmasıyla ilgili ne yapacağız?

Ulusal yasalar, gelişimin sonucu olarak gereklidir ancak özel hayatın tatminkâr bir biçimde korunmasında tek başına yeterli değildir. Bu durumda, uluslararası hukuki gelişmeler Norveç için giderek önem kazanmaktadır. Bizler, Avrupa İnsan Hakları Sözleşmesi (AİHS) yoluyla Avrupa İnsan Hakları Mahkemesi (AİHM) ve uluslararası hukuka tabiyiz zaten. Ayrıca, diğer ülkelerde yapılan kanunlar Norveçli vatandaşların mahremiyetini etkileyebilir. Bu yüzden, diğer ülkelerin mahremiyet yasalarına ve bunların Norveç'le nasıl bir ilişkisi olduğuna daha fazla dikkat etmeliyiz.

Avrupa ve dolayısıyla Norveç hukukundaki en önemli kararlardan bazıları, AİHS'de yer alan Madde 8'in belirttikleridir:

Özel ve aile hayatına saygı hakkı

1. Herkes özel ve aile hayatına, konutuna ve yazışmalarına saygı gösterilmesi hakkına sahiptir.
2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş olması ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suçun önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusudur.

Norveç AİHS sözleşmesine taraf olduğu için bu karar ülkenin yasalarına tatbik edilmiştir ve Norveçli vatandaşların özel hayatı korumakta nihai merci, AİHS aracılığıyla bu karardır. Ancak Madde 8, özel hayatın korunması ile diğer tedbirlerin çatışması sorunu söz konusu, ne liberal demokrasilerde yasal olarak kabul edilebilir nihai bir sınır çeker ne de böyle bir hedefi vardır. Bu yüzden, AİHS hukuki uygulamalarında, özel hayatı korumak için nihai sınırları belirleme konusundaki yargı kararlarında sınırlı davranmıştır.

AİHS, mahkeme yeni teknoloji ve sosyal eğilimlerle uyumlu olabilsin diye, yasa koyucu faaliyetlerinde maddeyi dinamik bir şekilde yorumlar. Özel alan, sosyal âdet ve ilişki doğası gereği özelse, kamu alanında da geçerliliğini korumalıdır. Başka bir deyişle, kamuya açık alanlarda cep telefonuyla konuşup, SMS ya da e-posta yollasak bile, ilkesel olarak, özel hayatımızın korunmasını talep etme hakkımız vardır. İletişimin amacı özel nitelikteyse, maddenin 2. fıkrasında belirtilen istisnalar kapsamında değilse, iletişimin kanunlarla hukuken korunduğu kabul edilir. AİHS'nin özel hayat hakkındaki maddesi özünde budur.

Hukuki Koruma Baskı Altında

Ancak hukuki koruma, terör olaylarına gösterilen tepkilerden dolayı baskı altındadır. Bu tartışma, özellikle 11 Eylül olaylarıyla ilintilidir. Bununla birlikte, Madrid (2004), Londra (2005), Paris (2015), Brüksel (2016), İstanbul'daki (2016) terör olayları, dikkatleri terörle mücadele üzerinde toplamıştır. Pek çok kişi, mahremiyetin bu odaklanmaya kurban edildiğini düşünmektedir.

Eleştirel yaklaşanlardan biri de Pieter Omtzigt'dir. Omtzigt, Avrupa Konseyi Parlamenterler Meclisi için hazırladığı raporunda,[3] Snowden'ın Haziran 2013'te[4] ortaya çıkardığı NSA izlemesinden duyduğu derin endişeyi dile getirir. Omtzigt'e göre eylem, "insan haklarına karşı bir tehdit ve AİHS'nin 8. maddesinin ciddi bir ihlalidir" Bir diğer endişe duyulan konuysa, kitlesel izlemenin gerekli şeffaflık ve kontrol olmaksızın yapılmasıdır, bu da hukuk devleti ilkelerinin etkin biçimde uygulanmasını zorlaştırır. Omtzigt ayrıca, gizli yasaların kullanılmasının ve davaların kamuya kapalı olmasının, gerekli denetimi zorlaştırdığını belirtir. Gelişmenin tehlikeli bir sonucuysa gizli servislerin, kaynaklarının gücünden dolayı çok fazla etkili hale gelebilmesi, yani demokratik denetimi, dolayısıyla da siyasi sorumluluğu (hesap sorulabilirlik) potansiyel olarak tehdit edebilmesidir. Bu da demokrasinin taşıyıcı sütunlarını zayıflatmak anlamına gelecektir.

İfşaatların neticesinde Omzigt, hem ABD'de hem de Avrupa'da özel hayat hakkının daha iyi bir şekilde gözetilmesinin güvence altına alınması için 8. maddede kapsamlı yasal revizyonlar yapılmasını önerir.

Snowden'ın ifşaatlarından sonra müttefikler arasında uluslararası bir güven yeniden inşa edilecekse, özellikle ABD'nin bu tür revizyonlar yapması çok gereklidir.

Oslo Üniversitesi'nden Rozemarijn van de Hilst, doktora tezinde (2013) terörle mücadelenin AİHS'nin 8. maddesiyle nasıl çatıştığını analiz eder. "Mahremiyeti Sınava Çekmek: Terör Karşıtı Teknoloji Avrupa Konvansiyonu'nun İnsan Haklarına Dair 8. Maddesiyle Çatışmaktadır" adlı tezinde, terörle mücadele adına giderek artan izlemeye karşı bizleri uyarır. Çıkardığı sonuçlardan biri şöyledir:

> Terör karşıtı girişimlerin dijitalleşmesi sonucu mahremiyete yapılan gerçek müdahalelerin yarattığı endişelerin yanı sıra, gerçek bir ihlal durumu olmadan da izlemenin, genel nüfus üzerinde bırakacağı olası sindirici etkinin mahremiyete zarar vereceği tartışılmaktadır ki, bu etki demokratik bir toplum için zararlıdır. [5]

Artan izleme özel hayatın huzurunu sadece doğrudan kaçırmaz, ayrıca sindiren etki (*chilling effect*) olarak bilinen dolaylı bir tehlikeyi de temsil eder, yani vatandaşlar büyük olasılıkla izlendikleri için hareketlerini kısıtlar ya da değiştirir. İfade özgürlüğü derneği PEN'in ABD şubesinin Kasım 2013'te[6] yaptığı araştırma bu etkiye bir örnektir. Araştırmaya göre, derneğin her altı üyesinden biri otosansür uygulamıştır ve izlenme korkusu nedeniyle farklı görüşlerini ifade etmekten kaçınmışlardır. Özellikle tartışmalı durumlarda bu tür bir otosansür daha kolaylıkla ortaya çıkacaktır.

Sindirici etkinin, izleme kadar medyadaki haberlerden de kaynaklandığı öne sürülebilir. Bazılarına göre, sindirici etkiyi medyanın tek yanlı ve yoğun haberler sunmasına borçluyuz. Eleştirenler, medyada çıkan haberlerin vatandaşları etkilediği konusunda tabii ki haklılar, ancak Snowden'ın ifşaatlarından sonra basının olayı ele alışını abartma olarak nitelendiremeyiz. Aynı şekilde, medyada çıkan haberleri otosansürün açıklaması olarak göstermek, olayı aydınlatacağına muallak kılar. PEN'in araştırması, vatandaşların otosansürü basında çıkan haberlerden dolayı değil, izleme yüzünden uyguladığını göstermektedir.

Böyle bir otosansürün etkileri, sadece vatandaşların her biri için değil, aynı zamanda toplum ve demokratik süreç için de olumsuzdur.

Demokrasi için özel hayatın taşıdığı önem, Rozemarijn van der Hilsts'ın doktora tezinin temel sonuçlarından biridir:[7]

> Kavramsal belirsizlikler söz konusudur – örneğin, mahremiyet çoğunlukla bir insan hakkı olarak kabul edilir, aslında öte yandan, mahremiyetin sosyal faydaları da vardır. Bunlardan biri, insanların ahlaki olarak özerk olmalarını talep eden demokratik süreçtir. Mahremiyet, insanların ahlaki özerklik geliştirmeleri için gerekli alanı sunar. Mahremiyet ve güvenliği iki karşıt kavram olarak değerlendirmek yerine, onların daha ziyade karşılıklı olarak birbirlerini güçlendirdiğini ve demokratik bir devletin işlerliği için her ikisinin de gerekli olduğunu kabul etmeliyiz. Bu sosyal faydalar tanınmadığı sürece, "Güvenliğe Karşı Mahremiyet" tartışmasının kaybedeni muhtemelen mahremiyet olacaktır.

Mahremiyetin alanı daraltıldığında, toplumun ortaklaşalığı da zayıflatacaktır. Bu yüzden özel hayatın huzurunu sadece bireysel hak olarak görmeye karşı uyarılarda bulunmalıyız. Mahremiyetin kendine has değeri olduğu doğrudur, ancak izleme ikilik anlamında yani bireye karşı toplum şeklinde değerlendirildiğinde, özel hayatın ortaklaşalık için taşıdığı anlamı reddedersiniz. Van der Hilsts'in öne sürdüğü bakış açıları çok önemlidir. Özel alan duyguları denetlemek, ahlaki sorunlar üzerine kafa yormak ve ahlaki bir bağımsızlık geliştirmek için önemlidir.

Zayıflamış özel alanın, yeni düşüncelerin gelişimini ve geleneksel zihniyete meydan okuma olanaklarını kısıtlayacağından korkmamız için nedenlerimiz var. Bunlar ekonomik sonuçlar da doğurabilir. Toplum yeni düşünce ve alternatif çözümleri denemeye erişimi kısıtlarsa, kolaylıkla durgunluk içine girer. Bu açıdan, özel hayatın korunması, özel hayatın kendi içerisinde bir hak olduğu anlayışının ötesinde, bir dizi kayda değer fayda içerir. Öte yandan, tartışmayı tersine çevirebiliriz, Eirik Newth'in öne sürdüğü gibi, zayıflatılmış bir özel alan, kişisel veri endüstrisini doğurmuştur. Google ve Facebook gibi şirketlerin ekonomik gelişim ve yenilikler için önemi büyüktür, kıtada ABD'li şirketlerle baş edecek tek bir şirketin olmaması Avrupa için bir sorundur. AB mahremiyete güçlü bir şekilde ağırlık verirse, pek çok kişinin Nokia'nın çöküşüyle akıllı telefon dalgasını da atlattığımızı iddia ettiği gibi, Büyük Veri ve IoT dalgasını geride bırakabiliriz.

AB Mahremiyet Düzenlemesi

AB'nin Mart 2016'da kabul edilen Kişisel Veri Koruma Tüzüğü, Norveç hukukunu etkileyecek uluslararası kararlardan biridir. Yeni düzenlemenin direktif yerine tüzük niteliğinde olması, ulusal hareket alanını daha da dar, AEA ve Norveç içerisindeki veri koruma kurallarını öncekinden daha eşgüdümlü kılacaktır. Tüzük gereği, AEA Konseyi yasayı AEA anlaşmasının parçası olarak yürürlüğe sokacaktır, sonrasında yasa Norveç'in anayasasına dahil edilecektir. AB Kişisel Veri Koruma Tüzüğü gereği, özel hayatın yasalarla korunması güçlendirilecektir. Veri Koruma Kurumu en önemli değişiklikleri şöyle özetlemiştir:[8]

> Kararlar, AB içerisinde mal ve hizmet sunan tüm iş birimleri için geçerlidir.
>
> İlk toplanma amacını aşan veri kullanımı olanağı sınırlanmıştır. Kişisel veriler yalnızca belirlenmiş, kesin amaç olduğu durumlarda işlenebilir ve amaca uygunluk konusunda bir endişe varsa, tüzükteki "uygunluk testi"yle bu endişe giderilecektir. Amaç uygun değilse, onayın alınması ya da yasada belirtilen şekillerde izin alınması gerekmektedir.
>
> Tüzük yeni somut haklar tanımaktadır, bunlardan biri de veri taşınabilirliği hakkıdır, yani kişisel bilgilerinizi bir hizmetten alıp diğerine taşıyabilme hakkı. Müşteri ilişkisi bittiğinde ya da bir hesap kapatıldığında, veri sahibi verilerinin silinmesini talep edebilir.
>
> Vatandaşların artık "ya hep ya hiç" çözümlerini kabul etmek zorunda kalmayacakları yeni onay şartları. Veri sahibi, şartların bazı bölümlerine onay verirken, diğer bölümlerini reddetme hakkına sahiptir.
>
> Veri korumanın gerekli şekilde yerine getirilmesi (belgeleme yükümlülüğü) konusunda firmalara genişletilmiş sorumluluklar verilmiştir ve büyük ölçüde kişisel veriyi işleyecek büyük özel firmalar, veri koruma görevlisi istihdam etmelidir. Bu durum kamu kurumları için de geçerlidir.

AB, bilginin açık ve belirli olması yönündeki taleplerini keskinleştirmiştir. Veri işleme ve veri korumanın manası anlaşılmaz veri koruma beyanlarının ardına saklanmayacak, vatandaşların hangi verinin işleneceğini ve ne için işleneceğini kolaylıkla anlayabileceği bir biçimde sunulacaktır. Kesin ve açık bir dilden tam olarak ne anlaşıldığı tabii ki bir tartışma konusu olabilir.

Son olarak, veri koruma tüzüğü ilkelerinin ihlali durumunda, veri koruma otoriteleri oldukça yüksek para cezaları kesme yetkisine sahiptir.

Düzenleme yeni bir ulusüstü organ kurmayı öngörür: AB ile AEA'nin farklı veri koruma otoriteleri arasında uyum sağlayacak Avrupa Birliği Veri Koruma Platformu. Düzenlemenin kesin amacı, Veri Koruma Kurumu da dahil olmak üzere, ulusal denetim otoritelerini güçlendirmektir.

Hayata geçirme konusunda doğal olarak büyük belirsizlikler söz konusudur. Rekabet avantajı ve vatandaşların otomatikleşmiş kararlara karşı koymasını mümkün kılan fiil olarak veri korumanın sınırlarının pratikte nasıl çizileceğini görmek zor. Birilerinin sizin kişisel verilerinizi analiz etmesi sonucu –çoğunlukla "verilerin diktatörlüğü" olarak anılır– muhtemelen ayrımcılığa uğradığınızda buna gerçekten nasıl karşı koyabilirsiniz sorusuna bu noktada gerçekçi bir cevaptan çok, beslenen umutlar ve iyi niyetler dile getirilmiş.

ABD

Konu Avrupa ve Norveç'te görüşülürken ABD'deki veri koruma tartışmasını göz ardı etmek zor. ABD'nin istihbarat örgütünün kapasitesi diğer ülkelerinkinden daha yüksek, bundan dolayı gizli servisler geniş ve derin faaliyet alanlarına, küresel dallara sahip. Norveç ve Avrupa ülkelerinin ABD gizli servisleriyle sıkı bir işbirliği içinde olduğu iyi biliniyor. Aynı zamanda ABD'lilerin müttefiklerini gözetlediğine dair ciddi ve inandırıcı suçlamalar yapıldı.[9] ABD'deki gizli servislerin hangi yetkilerle donandığı Norveç'in çıkarlarını doğrudan ilgilendirmektedir. Bu yüzden, Norveç'teki veri koruma tartışması, ABD'nin koşulları ve yasal düzenlemeler hakkında bir miktar bilginiz olmasını öngörmektedir.

Mahremiyet ve özel hayatın huzuru, 1776'da cumhuriyetin doğuşundan bu yana tartışılan bir konudur. ABD Anayasası'nda özel hayatın huzuruna ilişkin somut hükümler yoktur ancak, özel hayatı kapsayan bir dizi dolaylı hüküm bulunmaktadır. Bunlar bireysel haklar olarak formüle edilmiştir. Örneğin ABD Anayasası'nın Birinci Ek Maddesi, dini inancın özel bir mesele olduğunu öngörür.[10] İkinci ve üçüncü ek maddelerde, vatandaşların kendi özel konutları hakkında karar verme hakları güvence altına alınır, örneğin kanunsuz ev aramalarına karşı yasal bir önerge vardır. Kararlar, ABD'de anayasayı hazırlayanların, özel hayatın vatandaşların özgürlüğü için neden önemli olduğuna ve bu yüzden güçlü bir hukuki korumanın temin edilmesine dair temel bir anlayışa sahip olduklarını gösterir. Öte yandan, özgürlük ve güvenlik arasında çıkabilecek gerginlikleri de görmezden gelmemişlerdir. Toplumsal değerin en güçlü ifadesi, Benjamin Franklin'in çok alıntılanan sözlerinde belirttiği gibi, yine de özgürlüğe duyulan ihtiyaçtı: "Geçici güvenlik için temel özgürlüğünü feda edenler ne özgürlüğü hak eder ne de güvenliği."

Anayasanın ek maddelerinde ve keyfi ev aramalarına karşı duruşta sergilendiği gibi, güvenlik duygumuz için özgürlüğün taşıdığı anlamın altının çizilmesi, Franklin açısından bu yüzden önemliydi. Bağımsızlık Bildirisi'nin mimarı Thomas Jefferson, özgürlük ve güvenlik arasındaki olası bir "değiş tokuş" durumunda, liberal duruşu şöyle özetler: "Çok özgürlük tanınması sonucu ortaya çıkan talihsizlikleri, özgürlüklerin çok kısıtlanması sonucu ortaya çıkan talihsizliklere yeğlerim."

Devletin yetkilerini, güvenlik söz konusu olsa da kısıtlamayı öngören klasik liberal tutum, ABD tarihinde özel hayatın konumuyla ilgili kalıcı bir özelliktir. Ancak bu, gizli servisler tarafından belli zamanlarda zorlanmıştır. Gizli servislerin, bilinen sebeplerden dolayı, yetkilerini genişletmek için büyük çaba gösterme eğilimi vardır. James Bamford'un *New York Review*'daki makalesinde belirttiği gibi, yetki alamadıklarında her zaman yasal çerçeve içinde kalmamışlardır.[11] Daha 1920 yılında, NSA'nın öncüsü Black Chamber, istihbarat toplamak amacıyla kurulmuştur. Çalışmalarının en önemli bölümü, ülke dışına yollanan telgraflara erişimi sağlamaktı. Öte yandan, böyle bir erişim yasal değildi çünkü özel mesajlar Radyo Haberleşme Kanunu'nun ilk

versiyonu tarafından yasal koruma altındaydı. Ancak Black Chamber buna rağmen, mesajları günlük olarak teslim etmesi konusunda Western Union'ı ikna etmişti.[12]

O yüzden, bazen tam sınırda bazen de sınırlarını aşarak iş halletmenin ABD istihbaratı içinde ve çevresinde tarihsel bir gelenek olduğunu görmek zor değildir. Bu durum ABD'ye has değildir, ancak Amerikalıların otoritelere karşı beslediği içkin şüphe, istihbaratın şimdi olduğundan daha fazla büyüyememesine katkıda bulunmuştur.

Daha önce de belirtildiği gibi, Senatör Frank Church ve Church Komitesi, istihbarat örgütlerinin (bir kısmı yasal olmayan) operasyonlarını ortaya çıkarmıştır. Komite, örneğin NSA'nın çalışmalarını içinde yürüteceği yasal çerçevenin yeniden düzenlenmesine katkıda bulunmuştur.

James Bamford özetle şunları yazar:

> NSA tarafından on yıllarca yasal olmayan şekilde yapılan izlenmenin sonucunda, 1978 yılında Yabancı İstihbarat İzleme Yasası (FISA) imzalanarak yürürlüğe girmiş ve Yabancı İstihbarat İzleme Mahkemesi (FISC) kurulmuştur. Yasanın amacı, ilk kez olarak, Amerikalıları dinleme için NSA'nın yasal onay alması talep edilmektedir. Mahkeme bir arama ya da bilindiği adıyla arama emri talebini her ne kadar ender olarak geri çevirse de ABD halkını, sorunlu bir geçmişe ve kontrol edilmediği sürece casusluk sınırlarını genişletme eğilimlerine sahip bir servisten korumak mantıklı bir önlemdir.[13]

FISC, gizli servisleri denetlemede yetersiz kaldığı yönünde suçlamalara maruz kalsa da NSA'nın mahkemenin onayı olmadan hareket edememesi hakkında minimum bir yargı güvenliği garantisi sunmaktadır. Bu yasal uygulama zayıflıklarına karşın işlemiştir – ta ki 11 Eylül 2001 terör saldırılarına kadar.

Teröre Karşı Savaş ve Vatanseverlik Yasası

11 Eylül 2001 saldırısının ardından Bush yönetimi, Terörizme Müdahale ve Engelleme İçin Gerekli Uygun Araçların Sağlanması, Amerika'yı Bir ve Güçlü Yapma Yasası, İngilizce baş harfler bir araya geldiğinde

oluşan kısaltmayla USA PATRIOT Yasası'nı ezici çoğunlukla kabul etti.[14] Yasanın amacı, otoritelerin terör saldırılarını önlemesini güçlendirmekti. Vatanseverlik Yasası, ABD'nin yakın tarihinde en çok tartışılan yasalardandır. ABD'deki, devlete şüpheyle yaklaşma geleneği, yerini toplu bir travma içerisinde, anında karşılanması gereken bir güvenlik ihtiyacına bırakmıştır. Georgetown Üniversitesi'nden Profesör Amitai Etzioni, *Weekendavisen*'de çıkan röportajında, saldırıdan sonraki gün Amerikalıların yüzde 70'inin güvenliğin artık anayasadan daha önemli olduğuna inandığını anlatır.[15]

Bush yönetimi ve Kongre, Başkan Bush'a göre otoritelere, terörle mücadelede gerekli araçları sağlayan ABD Vatanseverlik Yasası'nı alelacele çıkararak karşılık verdi. Kongre yasayı onayladığında, 11 Eylül'ün üzerinden henüz bir buçuk ay geçmişti. Yasa Temsilciler Meclisi'nde 357 oyla (66 aleyhte oy vardı) onaylanırken, Senato'da sadece Russ Feingold (D) aleyhte oy verdi.[16]

Yasanın amacı, devletin izleme olanaklarını artırmak ve ABD halkının güvenliğine etkili katkıda bulunmaktı. Yasaya karşı çıkanlar, vatandaşların yargı güvencesini gözden çıkarmadan yasayı uygulamanın zor olduğunu irdelediler. Yasa, örneğin, yabancıların belirsiz süre için gözaltında tutulmasına, gizli aramaların yapılmasına ve finansal veriler de dahil olmak üzere vatandaşların izlenmesine artırılmış imkânlar tanıyordu – tüm bunlar mahkemeden izin alınmadan yapılabilecekti.

Yasa, kütüphanelerden hangi kitapların ödünç alındığını otoritelerin kontrol etmesine izin veriyordu. Ayrıca yasa, bütçeden pay (tahsisat) alma ve ülke içindeki eyalet bürolarıyla daha fazla bilgi paylaşma olanaklarını içeriyordu. Yasa, terör kapsamına giren eylemler için daha detaylı ve daha fazla ceza hukuku hükümleri içeriyordu.

Yasanın bir sona erme tarihi vardı. Bu açıdan Kongre'de yasa "olağanüstü hal kararı" olarak görüldüğünden anlayışla karşılanmıştı, dönemin Başkanı George W. Bush'un da yaptığı tanımla, 11 Eylül saldırısı "savaş nedeni" olarak görülüyordu. Bir diğer deyişle, ABD Vatanseverlik Yasası, "normal koşullar" altında değil, bir savaş durumunda işlemesi gereken bir yasa olarak ele alınıyordu.

Öte yandan pek çok kişi ABD Vatanseverlik Yasası'nı geçici bir karardan sürekli bir karara dönüştürmek arzusundaydı. Yasayı eleştirenler pek çok hükmü kaldırmak istiyorlardı çünkü pek çoğu devlet izlemesine kesinlikle geniş imkânlar tanıyordu. Tartışmayı etkileyen bir diğer şey, bu kararların terörü engelleme konusunda etkili ya da gerekli olup olmadığı üzerineydi. Bu sorular, Thomas Kean başkanlığında yürütülen 11 Eylül Komisyonu'nun çalışması sonrasında önem kazandı. Komisyon çalışmasını 585 sayfalık bir rapor yayımlayarak 22 Temmuz 2004'te tamamladı.[17] Rapor, saldırıların geri planı ve güvenliğin nasıl daha fazla iyileştirilebileceğine dair öneriler hakkındaydı. 22 Temmuz terör saldırısına ne kadar hazırlıklı olunduğunu inceleyen Gjørv Komisyonu raporu ile Kean raporu arasında benzerlikler vardır. Hem biçim, hem içerik hem de raporun kamuda kullanılış biçimi açısından pek çok paralellik görülür.

Ayrıca güvenlik sorumluluğunu üstlenmiş devlet kurumlarını sert bir biçimde eleştiren rapor sonucu da Gjørv Komisyonu'nun sonuçlarına benzer. Komisyon, olayı "istihbarat hatası" olarak tanımlar ve FBI ile CIA'nın, Başkan Clinton ve Başkan Bush döneminde görevlerini tatminkâr bir biçimde yapmadıklarını iddia eder. Komisyon, saldırı öncesinde pek çok bilginin mevcut olduğuna dikkat çeker ancak bilgi parçalarını bir araya getirmekte yetersiz kalınmıştır. Bu sonuç, ABD Vatanseverlik Yasası'na karşı çıkanlar için oldukça önemliydi: İzleme ve bilgi toplama zaten mevcuttu ancak asıl sorun bilginin işlenemeyecek kadar çok olmasıydı. Bu yüzden, daha fazla izlemenin ve daha da fazla bilgi toplamanın teröre karşı mücadeleyi güçlendirmeye katkıda bulunacağı şüpheliydi. İzlemeye dair kanun hükümlerinin genişletilmesi yerine, istihbaratın analiz yönünü iyileştirmek ve örgüt içi bilgi alışverişindeki engelleri ortadan kaldırmak daha mantıklı olabilirdi.

Bill Clinton ve George Bush dönemlerinde güvenlik ve anti-terör önlemleri için ulusal koordinatörlük yapmış olan Richard Clarke bu alandaki en uzman kişidir. Clark, Bush yönetiminin anti-terör politikasını en önce eleştirenlerden biri olmuştur. *Against All Enemies: Inside America's War on Terror* [Tüm Düşmanlara Karşı: Amerika'nın Terörle Savaşı] ve *Your Government Failed You: Breaking the Cycle of National Security Disasters* [Hükümetiniz Sizi Hayal Kırıklığına Uğrattı: Ulusal

Güvenlik Faciaları Döngüsünü Kırmak] adlı kitaplarında, otoritelerin terör saldırılarına verdiği karşılığı eleştirir. Bush yönetiminin teröre karşı aldığı önlemler, sadece Amerikan değerlerine ters düşmekle kalmaz, ayrıca anayasayı da ihlal etmektedir. Clarke aynı zamanda, ABD Vatanseverlik Yasası'nı da etkisiz olarak değerlendirir.

Eski Başkan Yardımcısı Dick Cheney ve hem Eski Güvenlik Danışmanı hem Eski Dışişleri Bakanı Condoleezza Rice, bu tahlillere (doğal olarak) katılmaz.[18]

Cheney ve Rice'ın argümanlarındaki ortak nokta, 11 Eylül'ü "fiilen" yaşadıklarını ve ulusal güvenlik konusundaki görüşlerinin şekillenmesinde bu olayın etkisi olduğunu belirtmeleridir. Sorumluluk sahibi politikacıların, ABD halkını başka terör olaylarına karşı savunmak için her fırsatı değerlendirmesi gerektiğini düşünmektedirler. 11 Eylül'ü yaşamayan eleştirmenlerin, Bush yönetiminin saldırı sonrası karşılaştığı zorlukları anlaması bu yüzden zordur. Bu tepki anlaşılabilir bir tepkidir, gerçeklik payı da vardır. Ancak yürüttükleri mantık pek çok yönden sorunludur.

Richard Clarke, Cheney ve Rice'ın argümanlarını eleştirir.[19] Cheney ve Rice gibi Richard Clarke da 11 Eylül'ü yaşadı. Clarke o sıralar güvenlik koordinatörüydü. Clarke şöyle yazmaktadır:

> Bu argümanı pek anlayışla karşılamıyorum. Evet, günlerce uykusuz kaldık ve başka saldırıların da geleceğini sandık hepimiz. Ancak Bush yetkililerinin sonraki aylar ve yıllar içerisinde –Irak, kamplar, sorgulamalar, dinlemeler üzerine– aldığı kararlar doğru değildi. Tüm kuralları çiğnemek itkisiyle hareket etmek yerine, dikkatli analizler yapılabilirdi, özellikle de 11 Eylül saldırıları yüzünden. Bu saldırılar, dehşet verici olmasına rağmen deneyimli yetkilileri şaşırtmamalıydı. 9/11'in ülkeye yapılan tehditlerin yeniden değerlendirmesine yol açtığına dair Cheney'nin itirafı, üst düzey yetkililerin, CIA ve NSC çalışanlarının, büyük çaplı bir El Kaide saldırısını önlemek için acil harekete geçilmesi[20] yönündeki uyarılarını aylarca nasıl görmezlikten geldiğini ortaya koyar.

Clarke'a göre Bush yönetimi şok geçiriyordu, mantıklı ve tutarlı bir tepki vermek için ortam kötüydü. Korku, bu yöntemlerin iyi olup olmadığı değerlendirilmeden abartılı yöntemlere izin verilmesine yaradı. Bu

durum, ABD'nin dünyaya yaydığı temel geleneksel değerlerin politika yüzünden zayıflatılmasına yol açtı. Cheney ve Rice'ın 11 Eylül her şeyi değiştirdi demelerine karşın, Clarke hukuk sisteminin tam da zor koşullar altında sınanmasını savunuyor ve ABD'nin sınavı geçemediğini söylüyor. Clarke, 11 Eylül'ün bir dizi şeyi değiştirdiğine ancak her şeyi değiştirmediğine, özellikle de ABD Anayasası'nı değiştirmediğine parmak basıyor.[21]

Çekincelere rağmen ABD Vatanseverlik Yasası'nın süresi, kapsamlı değişiklikler yapılmadan Mart 2006'da uzatıldı. ABD'deki siyasi tartışmalar hâlâ güvenlik ve terörle mücadelenin anlamı etrafında dönmekteydi. Kongre ABD Vatanseverlik Yasası'nı ve yasanın süresinin uzatılmasını onaylayarak, 1978 yılında alınan FISA kararıyla gizli servisler üzerindeki denetimi güçsüzleştirdi. Başka bir deyişle, 1970 yılında Church Komitesi'nin ertesinde gerçekleşen sivil hakların güçlendirilmesi çalışmaları geriledi.

Richard Clarke, yasanın ve yasanın sonucu olan uygulamanın anayasayla çeliştiğini iddia ederken yalnız değildi. James Bamford, Clarke'la aynı görüşte olanlardandı ve ABD otoritelerinin, mahkemenin onayı olmadan ABD vatandaşlarını dinlemeye karar verdiklerinde yasayı çiğnediklerini kesin bir dille belirtti.[22]

Sivil haklar uzmanı olarak Georgetown Üniversitesi'nde ve CATO Enstitüsü'nde görev yapan Patrick Eddington da istihbarat örgütlerinin faaliyetlerinin yasadışı olduğu kanısındadır.[23] Clarke gibi Eddington da geçmişte istihbarat ajanlığı yapmıştır ve 11 Eylül'den sonraki programların sadece hukuksuz olmakla kalmayıp aynı zamanda etkisiz de olduklarını söyler: Bilgi eksikliği ne geçmişte bir sorundu ne de şimdi – mesele, zaten mevcut olan bilgiyi analiz etme konusunda yetersiz kalmaktır. Bu şekilde kitlesel izleme, istihbarat faaliyetini güçleştirecektir.

Derin endişe uyandıran bir diğer sorun da demokratik denetime tabi olan istihbarat şeflerinin Kongre'ye rahatlıkla yalan söyleyebilmeleridir. Ulusal İstihbarat Direktörü James Clapper, 12 Mart 2013 tarihinde Kongre'ye NSA'nın sıradan ABD vatandaşları hakkında bilinçli olarak bilgi toplamadığını anlatmıştır (üstelik yeminliyken). Snowden sızıntılarından sonra bunun doğru olmadığı ortaya çıkmıştır.

Gerçek, NSA'nın bilinçli olarak bilgi topladığıdır. Clapper daha sonra bir röportajında, söylediklerini şöyle savundu: "Mümkün olduğunca az yalan söyleyerek soruları cevapladım."[24]

Bu ifadenin hiçbir politik sonuç doğurmaması, Obama yönetiminin gerçekle olan ilişkisi hakkında şüphe uyandırır. James Bamford'un da aralarında bulunduğu pek çok yorumcu, bu ifadelerin en iyisinden bir Orwellvari Yenikonuş olduğunu söyler.[25] Kongre'de yalan söylemeye kovuşturma açılmaması şeklinde bir gelişme, uzun vadede hukuk devletini zayıflatır.

Öte yandan, ABD'deki atmosfer şimdilerde değişmiştir, en azından bir miktar. Değişen atmosferi dile getiren NSA'nın yeni başkanı Amiral Mike Rogers'tır. Rogers, Ocak 2016'da, ABD vatandaşlarının mahremiyetini korumak için şifrelemenin taşıdığı öneme dikkat çeker.[26] Eski NSA Şefi Michael Hayden da şifrelemenin mahremiyeti korumak için artan öneminin altını çizer.[27]

ABD Özgürlük Yasası

Bu değişim Snowden'ın ifşaatlarından bağımsız olmamıştır. Elektronik Sınır Kurumu (EFF), dijital mahremiyet için uğraşan kurumların arasında belki de en önemlisidir. NSA'dan çok daha düşük bütçesi olmasına rağmen, kurum kitlesel izleme konusunda hem siyasi tartışmalarda hem de ABD yargı sisteminde NSA'ya kafa tutmuştur.[28] Bu çabalar sonuç vermiş, mahremiyetten yana olan görüş ABD'liler arasında daha fazla destek görmeye başlamıştır.

Daha da önemlisi, ABD Vatanseverlik Yasası'na karşı durmak için Kongre'de yapılan yasal değişikliklerdir. Mayıs 2015'te Senato'nun çoğunluğu, ABD Vatanseverlik Yasası'nın telefon verilerinin yığınsal toplanması hakkındaki 215. bölümünün yenilenmesi aleyhinde oy kullandı. Bu kararı, kitlesel izlemeyle son bir hesaplaşma diye nitelenen pek çok yasadan biri olan ABD Özgürlük Yasası[29] takip etti. Bu hüküm, NSA'nın kitlesel izleme yetkilerini kısıtlamaktadır. Örneğin, NSA'nın telefon verilerine ulaşmak için mahkemeden onay alması gerektiği için, FISC'nin rolü yeniden önem kazanır. Bunun sadece ABD vatandaşları için geçerli olduğunu unutmayınız.

New York Times karardan, önemli bir değişim, Kongre'de izlemenin nasıl görüldüğüne dair kültürel bir dönüşüm olarak söz eder, ancak yine de NSA'nın Amerikalıları izleme olanaklarının ne ölçüde kısıtlanacağı sorusunu yöneltir.[30] EFF ayrıca, NSA'nın haklı bir gerekçe olmadan telefon bilgilerini toplama yetkisini yasanın gerçekten ne kadar sınırlayacağı konusunda endişelidir. EFF'nin özellikle endişe duyduğu konu, NSA'nın FISC'den izin alabilmeye dayanak teşkil eden nedenin ne olacağıdır. Talep genellikle "makul şüphe"ye dayandırılır, ancak kanun metninde bu konu çok net değildir.[31]

EFF yine de, ABD Özgürlük Yasası'nın önemli değişiklikleri temsil etmesine karşın, bunun sadece istihbarat ortamının yenilenmesi yönünde atılan bir ilk adım olduğunu belirtir.

11 Eylül'den sonra ortaya çıkan, istihbarattaki dev büyüme özel hayatın gizliğini koruma açısından kesinlikle endişe vericidir. ABD Özgürlük Yasası önemli bir düzeltme gerçekleştirmiştir. Ancak değişikliklerin 11 Eylül 2001 tarihinden neredeyse 15 yıl sonra yapıldığı gerçeğini de göz ardı edemeyiz. Mahremiyeti koruma tartışmasının, yeni bir büyük terör saldırısını ne şekilde etkileyeceği cevabı olmayan bir sorudur hâlâ. ABD'nin 11 Eylül'de olduğundan farklı bir tepki gösterip göstermeyeceği de belli değildir.[32]

Senatör Frank Church bu olayları önceden görebilenlerden biriydi, daha 1970'lerde, istihbaratta kullanılan teknolojik olanakların ne tür tehlikeler taşıdığından söz etmişti, özellikle de devletin otoriterleşme yolunda ilerlediğinde teknolojik olanakları kullanarak geleceğin diktatörlüğünün temelini atabileceğini belirtmişti.[33]

SEKİZİNCİ BÖLÜM

Norveç'te İzleme: Rahatsız Edici Gelişmeler

Uluslararası gelişmeler Norveç için önemlidir. İlk olarak biz, açık ve uluslararası bir ekonomiye sahip, küçük bir ülkeyiz. Küresel ekonomiyle en çok bütünleşmiş ülkeler arasında, aynı zamanda dünyadaki en gelişmiş teknolojik toplumlar arasında yer almaktayız. Yeni teknolojik çözümler hem resmi hem de özel sektörde eskiden olduğundan çok daha hızlı bir tempoda uygulanmaktadır. Teknolojik gelişme, gördüğümüz gibi, özel hayatı koruma sorunlarını da etkilemektedir. Uluslararası sözleşmelere imza koyduğumuz için uluslararası hukuktaki gelişim de mahremiyeti koruma sorunlarını etkiler.

Norveç yasalarının sürekli olarak güncellenmesi gerekmektedir. Sorun, genel olarak teknolojinin siyaset ve hukuktan önde gitmesidir. "Teknik politikaya üstün gelir" ifadesi yeniden yorumlanacak olursa, "teknik etiğe üstün gelir".[1]

Teknolojik gelişim hiçbir şekilde gerilemeyeceği için bizler teknolojinin önüne geçmeye çalışmalıyız – ilerlemeyi durdurmak için değil, teknolojinin mahremiyet hakkıyla çelişip çelişmeyeceğini değerlendirmek için. Bu tartışma uluslararası gelişimden etkilense de, dijital toplumda mahremiyet hakkının ne kadar yer kaplayacağına dair kararı, Norveç Parlamentosu bağımsız olarak vermek zorundadır ve verecektir.

2009 yılında raporunu teslim eden Mahremiyeti Koruma Komisyonu, teknolojideki yeniliklerin bir sonucu olarak mahremiyetin karşılaştığı tehlikelerin artışına dikkat çekti ve bu tehlikelerin özel hayat üzerindeki etkileri söz konusu olduğunda dikkate alınması gereken bir dizi koşulu tespit etti.[2] Bu tehlikeler son yıllarda azalmış değildir. Tehlikelerin arttığını söylemek daha doğru olacaktır. Bu yüzden farklı değerler ve faydalar arasında nasıl bir denge tutturabiliriz ve hangi somut du-

rumlarda özel hayata başka hususlar karşısında öncelik tanınacaktır sorularıyla etraflıca ilgilenmeliyiz.

Devlet İzlemesi ve Yetkiler

Polise getirilecek kısıtlamalar ve imkânları değerlendirmeden önce, açık ve liberal bir demokrasinin kırılganlığını kabul etmek önemlidir. Liberal bir demokrasinin temelinde çoğunlukla, sınırlı bir denetimin olduğu, yöneten ile yönetilen arasındaki güvenin önemli bir zemin oluşturduğu özgürlük anlayışı yatmaktadır. Bu, liberal demokrasilerin organize suç ve güvenlik tehditleri karşısında hareket alanını sınırlar.

Mahremiyetin Savunması Adına başlıklı kitabında Başsavcı Tor-Aksel Busch, terör korkusunun ilkeli düşünceyi gölgelememesi gerektiği konusunda uyarılarda bulunur.[3] Güvenlik güçlerinin ve istihbarat örgütünün yetkilerinin genişletilmesini öngören güvenlik tedbirleri, işler kötüye giderse, mahremiyetin korunmasına karşı büyük bir tehdit oluşturacaktır. Busch, tüm bunlara rağmen, toplum ve birey arasındaki dengenin hukuk devletinin ilkeleri doğrultusunda genel olarak oldukça iyi korunduğunu yazar.

Busch, mahkeme denetiminin aslında yeterli olmadığını iddia eder; sadece mührü basıp geçen bir kuruluşa dönüşmemek için gerçeğe uygunluk denetimini de yapmaları gerekmektedir. Burada kullandığı örnek ilginçtir: 11 Eylül sonrasında dönemin hükümetinden (Bondevik II) gelen bir öneriye göre PST* , ciddi suçlara kalkışmaya hazırlanan belirli kişiler hakkında "soruşturma yapmak" için zorla müdahalede bulunma izni istiyordu. Bu şekilde formüle edilmiş öneriye, esasen, mahkemeye daha yakından bir inceleme yapmak için amacın denetimi fırsatı tanındığında neredeyse her durumda onay alınması mümkündür. Hükümet o zaman başsavcıdan gelen tavsiye doğrultusunda, ifadeyi "soruşturma yapmak için gerekçe" şeklinde değiştirmiştir. Mahkeme, "soruşturma yapmak için" yerine "soruşturma yapmak için gerekçe" üslubunu kullanarak, PST'nin taleplerinin özünü, aynı zamanda müdahaleyi gerektirecek uygun bir sebep olup olmadığını değerlendirmek zorunda kalır. Zorla müdahale, PST çeşitli kişileri ya da grupları daha

---

* Norveç İstihbarat Teşkilatı –çn.

yakından soruşturmak istedi diye kullanılamaz. Başsavcıya göre, zorla müdahalenin koşulu olarak bu türden uygunluk değerlendirmesi, mahremiyet koruma güvenliğini sağlamak için şarttır.[4]

Bu noktadan sonra hukuktaki gelişmelerin ters yönde ilerlemesi endişe vericidir. Toplumsal Araştırmalar Enstitüsü için yazdığı raporda Avukat Jon Wessel-Aas, 1999 ve 2014 yılları arasında, bu alanda ortaya çıkan hukuki gelişimi anlatır.[5] Rapor PST'nin, vatandaşları izlemeye erişim faaliyetini nasıl genişlettiğini gösterir, bunun yasadaki adı haberleşme denetimidir.[6] Wessel-Aas genişlemenin iki şekilde gerçekleşebileceğine işaret eder: Ya izleme yetkisi almak için gerekli talepler esnetilir ya da neyin cezalandırılabilir olduğunun tanımı genişletilir.[7] Busch, "soruşturma yapmak için" ve "soruşturma yapmak için gerekçe" ifadeleri arasında büyük fark olduğunu belirtmekte haklıdır ancak, Busch'un sözünü ettiği değişiklikler, yine de PST'nin izlemeyi kullanma yetkilerini esaslı bir biçimde genişletmiştir. Özellikle, cezai olayları soruşturmada zorlayıcı tedbirler ile gerçekte cezai suç ortaya çıkmadan önce suçu engellemek arasında ilkesel bir fark vardır. Argüman anlaşılsa bile ve insan erken bir safhada, nispeten müdahaleci bir yetkiyi kanunun amacının yasal kılmasını kabul etse de durum sorunludur.

Bununla birlikte, mahremiyeti korumayı en çok zorlaştıran, 2013'te yapılan değişikliklerdir. Terör yasasındaki sıkılaştırmayı 2011'deki terör olayından bağımsız değerlendirmek zordur. 22 Temmuz Komisyonu'nun (Gjørv Komisyonu) çalışmalarını takiben, Parlamento sıkılaştırma tartışmaları yönünde ilk adımı attı. Parlamento, terörle bağlantılı faaliyet hazırlıklarına kovuşturma açılmasını sağlamak için hukuk sisteminin güçlendirilmesini istiyordu. Bu da terör hareketi planladığından şüphelenilen kişi hakkında kovuşturma açmak için eşiğin düşürülmesi anlamına geliyordu. [8]

Bu değişiklikler 2013'te yasayla resmileşti ve Wessel Aas'ın belirttiği üzere, yasal hüküm ayrıca bireylerin terörist eylem hazırlıklarını da suç kapsamına almaktadır.[9] 2011'deki terör olayını failin tek başına planlayıp gerçekleştirdiği düşünüldüğünde bu değişikliği anlamak zor değildir.

Ancak terör eylemi planlamak ne anlama gelir?

Kanun teklifinde ifade edilen, planlamanın ileriye götürme niyetine işaret etmesidir, yani fail teröre yönelik olduğu görünen faaliyetlerde bulunmuş kabul edilir. Savcılar, hazırlıkların tüm detayları bunu netleştirmese de failin terör eylemini gerçekleştirme kararı aldığını ispat etmek zorundadır.[10]

Başsavcı henüz 2002 yılında, terörist eyleme hazırlığın genel suç kapsamına alınması önerisini geniş kapsamlı, kullanışsız ve kabul edilemez olarak tanımladığı uyarısıyla, bu kanun teklifinin, özellikle müdahaleci değişiklikler içerdiğini desteklemektedir. Terör suçunu işleme kastı, tamamen günlük eylemden sayılan faaliyetleri bazı aşırı durumlarda suç gibi sunabilir ve özünde kötü niyeti uydurma kanıtlarla gösterme çabasıdır. Bu durumsa temelde, ceza kanununun ana amacı olan somut hazırlık çalışmalarına odaklanmaktan farklıdır. [11]

Terör hazırlıklarını henüz düşünce aşamasındayken suç kapsamına sokma girişiminin neden sorunlu olduğu açıktır. Örneğin, internette *bomba nasıl imal edilir* araması yapmak ya da internet ortamında, kuramsal olarak terör olayı gerçekleştirmeyi düşündüğünü tartışmak, hazırlık yapmak olarak mı nitelendirilecektir? Bu tür davranışlar bir bakıma ilk hazırlıklar olabilir ve terör kastına işaret edebilir ancak çoğu durumda da zararsız birtakım düşünceler olabilir. Pek çok durumda tamamen günlük alışveriş sayılabilecek gübre, araç gereç, benzin vb. gibi şeyler satın almak daha da sorunludur çünkü, belirli şartlar altında, terör faaliyetine hazırlık olarak görülebilir. Bu tür hareketleri politik görüşlerle ilişkilendirdiğimizde durum özellikle endişe verici olabilir. Bir çiftçi, işinin gereği büyük miktarlarda gübre, araç gereç ve benzin almışsa, öte yandan göçmen karşıtı internet sayfalarında aktifse, bu durum söz konusu kişinin yakından izlenmesi gerektiğine dair haklı bir gerekçe mi teşkil edecektir?

Hukuk Profesörü Erling Johannes Husabø, 2013'te kabul edilen değişikliklere karşı uyarılarda bulunmuştur. Bu değişiklikler aslında halk arasından büyük grupların izlenmesi için PST'ye "sınırsız yetki" verilmesi anlamına geliyordu.[12] Mahkemelerin denetiminin zayıflatılması tehlikesine karşı, Busch gibi Husabø da uyarıda bulunuyordu. PST'nin önleyici izleme yapabilme olanağına sahip olması, hukukta giderek daha sık rastlanan bir durumdur, diye yazar Wessel Aas.[13]

Terörü önleme arzusunu anlayabiliriz ancak bu yüzden işi, düşünceleri ve fikirleri cezalandırmaya vardırmaktan kaçınmalıyız. Düşünceler suç kapsamına girmemelidir.

Parlamento'nun Haziran 2016'da onayladığı gizli zorlayıcı tedbirlere dair ceza hukuku usulündeki değişiklikler kararı, mahremiyeti korumayı baskı altında bırakan bir diğer resmi karardır.[14]

Kararda ilk göze çarpan nokta, hükümetin teklifinin gerekçesinin sağlam bir biçimde araştırılmadığıdır.[15] Dijital Duyarlılık Kurulu'nun vardığı sonuçlardan biri, müdahaleci yeni dijital izleme yöntemlerinin geniş çaplı araştırılmasıdır. Bu yüzden karar daha da endişe vericidir. Dijital Duyarlılık Kurulu'nun ana sonuçlarından bir alıntı yaparsak:

> Kurul, istihbarat ile polisin bu tür bir teklifi getirme ihtiyaçlarını tanımaktadır ancak tekliflerdeki müdahaleci nitelik yüzünden, bunlar kamuya açık bir tartışma yapılmadan önce yürürlüğe konmamalıdır. Böyle bir tartışmaya hazırlık, bu tür tedbirlerin kapsamlı bir tartışmasını içeren resmi bir inceleme aracılığıyla yapılmalıdır. İstihbaratın ihtiyaçları, teknolojik uzmanlık ve mahremiyet dikkate alınmalı ve meselelerin ortaya çıkardığı teknolojik, hukuksal ve toplumsal sorunların özenle incelenmesi sağlanmalıdır.[16]

Buna rağmen hükümet teklifi gündeme getirmeyi seçti, Parlamento suçu önlemek için otoritelere genişletilmiş yetkiler tanımayı onayladı. Bu karar içerisinde, özellikle veri okuma sorunludur çünkü, böyle bir yetki polise, söz konusu kişinin kaydettiği metin dosyalarına, internet aramalarına vb. göz atmak için kişisel bilgisayarları, cep telefonlarını ve diğer elektronik araçları hackleme olanağı tanır. Vatandaşın özel alanına bundan daha fazla giremezsiniz herhalde. Adalet Bakanı Anders Anundsen, Lysne Kurulu'nun tavsiyelerini göz ardı ederek alınan kararı şöyle savunur: "Tedbir olarak veri okuma kararı bir an önce çıkmalıydı." [17]

Nettavisen'de yazdığı blogda Anundsen argümanını derinleştirir. "Polisin iyi araçlara ihtiyacı var. Terör tehlikesi artmıştır, diğer ciddi ve organize suçlar alanlarını genişletmektedir. Polisin, topluma karşı görevlerini yerine getirmesi için ve günümüzün tehditlerinden vatan-

daşları koruyabilmesi için, ciddi suçlarla mücadelede daha iyi araçlarla donatılmış olması gerekmektedir."[18]

İlk olarak, terör tehlikesinin ve örgütlü suçun arttığına dair iddialar hakkında iyi gerekçeler sunulmamıştır. Ancak daha da düşündürücü olan nokta, yeni yetkilerin önceden sağlam bir süreçten geçmeden yürürlüğe konmasıdır. Vatandaşların bilgisayarlarındaki verileri okuma olanağının tanınması, aslında onların düşünsel faaliyetleri hakkında detaylı bilgiler toplanmasına yol açar. 10 yıl ve daha fazla cezası olan davalarda, ek yöntem olarak veri okumanın kullanımına izin verilmesi, son derece müdahaleci bir tutumdur. Parlamento bu yöntemi, en ciddi davalarda kullanmakla sınırlandırmamıştır. Bu yüzden Parlamento'nun yaptığı yasa değişikliği pek çok uyarı almıştır.

Parlamento'daki sözlü sorular görüşmesinde, Uluslararası Hukukçular Komisyonu'ndan gelen uyarılar da dahil olmak üzere pek çok uyarı alınmıştır.[19] Uyarılar özellikle, yasanın zayıf düşürüldüğü, bu kadar geniş çaplı müdahaleci yöntemlerin somut bir biçimde hangi durumlarda kullanılacağının çok az belirtilmiş olduğu ve bu yüzden de yeterli bir gerekçe olmaksızın kitlesel izlemeyi gerçekte serbest kıldığımız yönündedir. [20]

Avukat John Christian Elden de değişiklikleri, temel mahremiyeti korumanın önemi üzerinden eleştirmiştir. Yasa teklifi hakkındaki bir eleştirisini Elden şöyle dile getirmiştir: "Bu yasa başka sınırlamalar getirilmeden teklif edildiği şekliyle geçirilirse, yasama çerçevesinin demokrasiye uygunluk sınavını geçip geçemeyeceği konusunda endişeliyim."[21]

Önde gelen hukukçular, Parlamento'nun kararının Anayasa'nın mahremiyeti koruma kararlarıyla uyumlu olmadığı iddiasındadır. Suç koşullarının oluştuğu hakkında somut şüpheler varsa, müdahaleci yöntemlere başvurulması anlaşılır bir durumdur. Anayasa'nın 102. maddesi şöyle der: "Cezai durumlar dışında hiçbir durumda konut araması yapılamaz."[22] Ancak Parlamento, suçu önleme amacıyla müdahaleyi kabul etmekle, özel hayatı korumaya yönelik çok daha sorunlu bir müdahaleyi kabul etmiş oldu. Bu yüzden bu kararın Anayasa'nın 102. maddesiyle çelişip çelişmediği tartışma konusudur. Hükümet çelişmediği sonucuna varmıştır:

> Bakanlık, Anayasa'nın 102. madde, birinci fıkra, ikinci bendindeki "cezai durumlar" ibaresinden, özel konutlarda zorlayıcı tedbirler uygulama hakkı verilmesi için cezai bir suçun işlenmiş olması talep edilir manasını çıkaramayacağımız sonucuna varmıştır. Suçun işlenmesini önlemek ve suçu bertaraf etmek için zorlayıcı tedbirleri kullanma hakkı verilmesinin değerlendirilmesinde, nizami müdahalenin meşru amaca uygun olup olmadığına ve orantılılığının teminatına bakılmalıdır.

Öte yandan, hukukçu Profesör Dr. Alf Petter Høgberg ve araştırma görevlisi Marius Stub, Denetim Yöntemi Kurulu hakkındaki yorumlarında, Anayasa'nın 102. maddesi uyarınca değerlendirildiğinde, önleme maksadıyla zorlayıcı tedbirlerin kullanılmasının sorunlu olduğunu belirtir.[23]

Profesör Erling Johannes Husabø da Denetim Yöntemi Kurulu'yla ilgili yorumunda aynı sonuca varmıştır.[24] Hem 102. madde hem de suçu önlemek için dijital izlemenin getireceği sorunlar göz önüne alındığında hükümet, devlet tarafından yapılan izlemenin sınırlarını genişletme konusunda dikkatli olmalıdır. *Overvåkning i en rettsstat* [Hukuk Devletinde İzleme] adlı kitabında merhum Profesör Jon Bing şöyle yazar: "Gündelik hayatın bütünlük taşıyan kalıbından, yapboz oyunuyla bir korku ve endişe resmi yaratılmasına karşı kendimizi korumalıyız. Bu yüzden, izlemenin gerekçeleri her ne kadar toplumumuzu korumaya yönelik olsa da, gizli servisleri denetlemek çok önemlidir."[25]

Parlamento'da yasanın geçerlilik süresi belirlenmelidir, özellikle müdahaleci olan, etkisi belirsiz yasalar için. Devlet bu şekilde yasanın etkisini daha iyi değerlendirebilir ve vatandaşlar da bu yöntemlerin genel bir kitlesel izleme biçimine dönüşüp dönüşmediğini ya da hükümetin, bu yasaların sadece ciddi durumlarda kullanılacağına dair verdiği sözü tutup tutmadığını değerlendirir. Ayrıca geçerlilik süresi olan yasalar kamuya, otoritelerin "ciddi meseleler"den ne anladığını daha iyi gösterir, bugün itibariyle bu konu muallaktır.

PST ve Veri Saklama

PST, gizli zorlayıcı tedbirlerin Parlamento'da kabulüyle istediği yöntemlerin çoğuna kavuşmuştur. Buna rağmen PST'nin şefi Benedicte

Bjørnland, vatandaşların elektronik haberleşmelerini izlemek için daha büyük olanakların tanınmasını istemektedir. 2014 yılında Bjørnland, PST'nin Büyük Veri erişimi olması gerektiğini savunmuştur.[26] NRK.no'da, PST'nin mevcut kısıtlamalarda şu değişikliklere gidilmesini istediği yazılıdır:

> PST şifreli bilgilere erişim istemektedir.
>
> PST Norveç'in bir veri saklama direktifi hazırlamasını istemektedir.
>
> PST Büyük Veri toplama ve saklama yetkisi istemektedir.
>
> PST gizlilik ilkesinin yumuşatılmasını ve sağlık kurumlarından, okullardan ve çocuk esirgeme kurumundan bilgi talep edebilme olanağını istemektedir.

Bu türden değişiklikler, mahremiyeti korumayı zorlaştıracaktır ve PST yetkilerini bu yönde genişletecek olursa, Büyük Veri'ye dayanan ve NSA'nın yapmakla suçlu duruma düştüğü bir tür kitlesel izleme gerçekleşecektir. Bu izleme, PST'nin radarı altına girmesi ya da kayıt altına alınması için herhangi bir neden bulunmayan insanların yine de bu durumlara düşmesine yol açacaktır.

Tam tersi bir şekilde, Büyük Veri'yi kayıt altına alma olanağını kısıtlamak için mevzuatı değiştirmeyi düşünmeliyiz. Kişiler hakkında toplanmış Büyük Veri, daha önce de belirtildiği gibi, kişilerin tavırları ve özellikleri hakkında pek çok şey anlatır ve bu yüzden de özel hayata müdahaledir. Norveç'teki Büyük Veri tartışmasının büyük kısmı veri saklama yönergesi hakkındadır. Bu yönerge, telefon ve internet hizmeti sunanların Büyük Veri'yi depolama sürelerini altı ayla sınırlar. Teknoloji Kurulu ve Veri Koruma Kurumu'nun "Büyük Veri ve Yeni İzleme" (2014) raporunda belirttiği üzere PST (ABD'deki NSA'dan farklı olarak) yalnızca açık bir mahkeme tarafından verilen onay doğrultusunda bu verilere erişimi istemektedir.[27] Bu durumda, Norveç'te ABD'de görüldüğü türden bir kitlesel izleme gerçekleştirmek zorlaşır. Veri Saklama Yönergesi taraftarları, Büyük Veri aracılığıyla izleme yapmanın, içerik verisiyle izleme yapmaktan daha az müdahaleci olacağını savunur. Bu argüman, Snowden'ın ifşaatlarından sonra revize olmaya hazır hale

gelmiştir ve DLD-yönergesini hatırlatan veri saklamanın her biçimi reddedilmelidir.

PST'nin daha fazla yetki isteğini endişeyle karşılamayı gerektiren bir diğer argüman da *Aftenposten* gazetesinde yer alan, sahte baz istasyonlarının ortaya çıktığına dair haberdir.[28] PST, araştırma laboratuvarı Simula tarafından yapılan kendi denetim ölçümlerine dayanarak sözde bulguları reddeder.[29]

Öte yandan, bu konuyla ilgili olarak en düşündürücü olan, sahte baz istasyonları sorunu değil, PST'nin hukuk devletine saygısızlığıdır. *Minerva* yorumcularından Jan Arild Snoen, 2013'te ulusal güvenlik otoritelerini haberdar etmeleri kaydıyla cep telefonlarının dinlenmesi için sahte baz istasyonlarını kullanma izni alan PST'nin bu emri görmezden geldiğine dikkat çeker. [30] PST bu yöndeki uyarıların gizlilik yükümlülüğüyle çelişeceğini iddia etmiştir, bu iddia kanun koyucu tarafından reddedilmiştir. Kanun koyucu ile PST anlaşamazsa, imtiyazlı taraf kanun koyucudur. Bu güncel meselede bizi daha da endişelendiren, Adalet Bakanı Anders Anundsen'in, kendisine ait müdürlüğün yasalara uymamasından rahatsızlık duymamasıdır. Aksine bakan, PST'nin yasadışı faaliyetlerini yasal kılmaya çalışmaktadır.

Polis Yasası ve Elektronik Haberleşme (Cep Telefonu İzleme ve Sinyal Kesme Alanları Düzenlemesi) Yasa Teklifi oturum tutanaklarında Adalet Bakanlığı'nın sahte baz istasyonlarının ulusal iletişim otoritelerine ya da telefon şirketlerine haber vermeksizin kullanılabilmesini ve polisin bu araçları nerede ve ne zaman kullanacağına mahkemenin onayı olmaksızın kendisinin karar verebilmesini önerdiği görülür.[31]

En azından bir mahkeme onayı bile içermeyen öneri, mahremiyeti koruma açısından endişe vericidir, Ulusal İletişim Makamı (Elektronik İletişimi Denetleme Teşkilatı), *Aftenposten* gazetesinde, hükümetin teklifiyle ilgili aynı görüşü bildirir. Teklifin özellikle sorunlu yanları şöyledir:

> Polisin izleme yöntemleri "oldukça kapsamlı"dır.
>
> Cezai durum ya da mahkeme denetimi talebi yasada yer almadığından, vatandaşın adalet güvencesi iyi bir şekilde gözetilmemiştir.

> Teklif, vatandaşların elektronik haberleşme gizliliğinin halihazırdaki korunmasını ihlal etmektedir.
>
> Teklif, bu korunmayı "yoruma müsait bir dizi kuralla" ihlale açık hale getirmektedir.
>
> Geniş yetkiler, sıkışık durumlarda Anayasa'nın ve Avrupa İnsan Hakları Beyannamesi'nin sınırları içinde kalınmasını zorlaştırır.[32]

İsteği doğrultusunda genişletilmiş yetkiler aldığında, PST'nin terör saldırılarını önlemesi tabii ki kolaylaşacaktır. PST tarafından bakanlığa yazılan bir mektupta belirtildiği gibi, PST'nin mahremiyet konusunda dengeleri koruyacağından şüphe duymamız için pek neden yoktur. [33] Ancak bu tür genişletilmiş yetkiler, mahremiyet açısından uzun vadede tehlikeli olabilir. Aynı zamanda, hukuk devletinin PST'ye koyduğu sınırlamaların, PST'nin terörü ve diğer suçları engellemede gerçekçi olarak ne kadar başarılı olacağı üzerine beklentileri de etkileyeceğini toplumun kabul etmesi önemlidir. Daha önce de belirtildiği gibi, açık toplumda paradokslar yaşanması kaçınılmazdır; toplumlar, polis devletleri olmadığı ve olmayacakları için kırılgandır.

Ancak bu sadece lafta kalmamalıdır. Bizler bilerek ve isteyerek PST'nin hukuk devleti çerçevesi içerisinde çalışmasını talep ettiğimizde, PST'nin hareket olanaklarını sınırladığımızı tanımanın sorumluluğu da politikacılara düşmektedir. 22 Temmuz teröründen sonra, PST kurum dışı soruşturma raporu (Traavik Kurulu) Aralık 2012'de Adalet Bakanlığı'na teslim edildi. Raporda, PST çalışanlarının, toplumun bu durumu anlamasını istediklerinin altı çizilmektedir. [34]

> 22 Temmuz Komisyonu'nun, "Riskin bu üstü kapalı kabulü otoriteler tarafından çoğunlukla yeterince dile getirilmemiştir," ifadesine kurul katılmaktadır. Kurulun görüştüğü 10 PST görevlisi bu durumu bir sorun olarak görmektedir. Pek çok PST görevlisi, siyasilerin PST'den beklentilerinin çoğu zaman, servisin kaynaklarıyla, çerçeve ilkeleriyle, mahremiyetin korunmasına yönelik sert kurallara uyulma ihtiyacıyla makul bir bağlantısı olmadığını hissetmektedir. Bu durumda, PST'den ne talep edildiğine dair kamuya daha net ve gerçekçi bir anlayış sunabilmek için beklentilere açıklık getirilmesine ihtiyaç duyulmaktadır.

Traavik Kurulu, iyileştirmeler yapmak için 50'den fazla öneri getirmiştir ancak bu öneriler, organizasyonla ilgili koşullara değinmektedir, PST'nin yasal zemini komisyonun salahiyet alanı dışında tutulmuştur.

Doğal olarak en çok, gizli servisin faaliyetlerindeki müdahaleci yönlere odaklanılmıştır. Ancak gizli servislerin, vatandaşları hem içeride hem dışarıda olabilecek izlemelere karşı koruma sorumluluğu da vardır. Giderek artan dijitalleşmenin, doğası gereği uluslararası olması, ulusal altyapımızı daha da duyarlı kılar. Bu bağlamda hem PST hem de E-hizmetler önemli bir rol üstlenir. PST ve E-hizmetler, Ulusal Güvenlik Makamı'yla (NSM) birlikte resmi olarak gizli servisleri oluşturmaktadır. PST ve E-hizmetler arasındaki belirleyici fark, PST'nin ana görevinin ulusal güvenlik olmasıdır, bu yüzden operasyonel sorumluluğu kraliyet sınırları içindedir, öte yandan E-hizmetler'in ana görevi ülke sınırları dışındaki Norveç çıkarlarına karşı olası tehditlerin tanımlanması ve analizlerinin yapılmasıdır. Günümüzün tehdit ortamında bu ayrımlar her zaman için kusursuz değildir.

İstihbarat Örgütü ve Norveç'e Karşı Tehditler

İyi işleyen bir istihbarat ve güvenlik hizmetinin temelini "Önleyici Güvenlik Hizmeti Yasası" (Güvenlik Yasası) oluşturur. Dev dijital büyüme, gelecekte karşılaşacağımız tehditlere karşı koymada yasanın uygun olup olmadığını sürekli değerlendirmemizi gerektirir, aynı zamanda, Norveç vatandaşlarının mahremiyeti korunmalıdır. Bu yüzden hükümet, 2001'de yürürlüğe giren Güvenlik Yasası'nda yapılacak değişiklikleri değerlendirecek yeni bir Parlamento komisyonu kurdu. Komisyonun önünde çeşitli sorunlar var.

Temmuz 2015'te *Dagens Næringsliv* (*DN*) gazetesinde çıkan, Norveç'in de dahil olduğu pek çok Avrupa ülkesinde elektronik haberleşme aracılığıyla izleme yapıldığı iddiaları bu sorunlara örnektir. [35] Avrupa Parlamentosu üyesi Eva Joly ile yakın işbirliği olan Avusturya Parlamentosu üyesi Peter Pilz, *DN*'nin haberine göre, yabancı istihbaratların Norveç'le ilgili ne türden bilgileri istediğine dair listelerin elinde olduğunu iddia eder. Dosya, Almanya'da araştırılmaktadır ancak

bu dosyanın ortaya çıkaracağı gerçek ne olursa olsun muhtemelen bu türden davaların kapsamı genişleyecektir.

Ulusal Haberleşme Makamı (NKOM) Bölüm Müdürü Einar Lunde, *DN*'ye şunları belirtmiştir: "Bu, en yüksek düzeyde gerçek bir sorundur[...] Herkesin dost göründüğü kadar düşman da olabildiği bir dünyada yaşıyoruz ve uluslararası alanda, kendi bilgilerimizi kendimiz güvence altına almalıyız."[36]

Lunde'nin ifadesi, elektronik bilginin hassasiyetini ortaya koyar, bu bilgi esasen kraliyet sınırları içindeki adresler arasında, ayrıca da üçüncü ülkeler arasında gidip gelmektedir. Bu da bizlerin ne Norveç yasaları ne de denetimlerine bağlı olan dış işletmeler ve yetkililerin gözetim ve denetimine tabi olduğumuz anlamına gelir.

Teknoloji Kurulu'nun üst veri raporunda[37] değindiği gibi, verilerin coğrafi olarak nerede bulunduğu, yargı alanı söz konusu olduğunda önemli bir sorun olarak ortaya çıkar.

Raporun belirttiği gibi:

> Norveç gibi küçük bir ülke için, Çin'in gerçekleştirdiği türden sürdürülebilir bir ulusal internet altyapısı oluşturmak zor olabilir. Yine de Snowden'ın ifşaatları ışığında, Norveçli kullanıcıların güvenliğini Norveç'teki özel hayatın gizliliğini koruma yasaları aracılığıyla, mümkün olan en iyi şekilde güvence altına almak için Norveçli otoritelerin hangi adımları atması gerektiği değerlendirilmelidir. Norveçli kullanıcıların kullandığı sağlık hizmetleri uygulamaları gibi bazı verilerin Norveç'te ya da aynı düzeyde mahremiyet garantisi veren başka ülkelerde saklanması zorunlu kılınmalıdır.[38]

Sorun, konuyla yakından ilgilidir ve hem Snowden olayı hem de *DN* makalesi, Norveç toplumunun yabancı güçler karşısındaki hassasiyetini ortaya koymaktadır. İnternetin bölünmesiyle ülke içi trafiğinin güvenliği daha iyi sağlansa da mahremiyetin korunması açısından mutlak bir avantaj sağlanacağı kesin değildir. En önemlisi, uluslararası bir işbirliği için çaba göstermektir. Aynı zamanda, uluslararası güçlerin Norveç vatandaşlarının temel mahremiyet haklarını ihlalini engellemek, istihbarat örgütünün özel sorumluluğundadır.

Bu endişeleri dengelemek amacıyla hükümet, ülke içinde ve dışında gerçekleşen veri akışının izlenmesiyle ilgili istihbarat örgütünün olanaklarını ve kısıtlamalarını inceleyecek yeni bir komisyon atadı. [39] İstihbarat örgütünün eski şefi Kjell Grandhagen, internet ve küresel haberleşmenin parçalarına Norveçli otoritelerin erişme hakkının olmamasını kabul edilemez bulduğunu belirtmişti daha önceleri, çünkü bu, Norveç'e saldırmak isteyen grupların neredeyse hiçbir engelle karşılaşmamaları anlamına geliyordu. [40] İstihbarat örgütünün ülkeye girip çıkan tüm veri trafiğini izlemesine izin vermek için genel olarak çok endişeli olmak gerekir, ancak raporunu Ağustos 2016'nın sonunda sunacak olan Profesör Olav Lysne (Dijital Duyarlılık Kurulu'nun da başkanlığını yapmıştır) başkanlığındaki komisyondan sağlam gerekçeler beklenmektedir. [41]

EOS Komisyonu

Ülkenin gizli servislerinin yasalarla denetleniyor olması, bu örgütlerin hukuk devleti çerçevesinde hareket etmelerinin gerekli bir koşuludur. Ancak yeterli bir koşul değildir. Yasayla denetime ek olarak, gizli servislerin yasalara uyup uymadıklarını ve talimatlar doğrultusunda hareket edip etmediklerini denetleyecek bağımsız bir denetçiye ihtiyaç vardır. Norveç'te, Parlamento'nun EOS Komisyonu (İstihbarat, İzleme ve Güvenlik İçin Denetim Komisyonu) bu görevi yerine getirir. Komisyon'un yedi üyesine ek olarak bir de kendi müdüriyet personeli vardır. [42]

EOS Komisyonu, önceden belirlenmiş birimleri denetlemez, ancak Norveç devletinin herhangi bir zamanda iş gördüğü gizli servisleri denetler. Günümüzde EOS Komisyonu İstihbarat Teşkilatı, Polis Güvenlik Hizmetleri, Ulusal Güvenlik Makamı ve Silahlı Kuvvetler Güvenlik Bölümü'nün denetiminden sorumludur. Organizasyonla ilgili değişiklikler ortaya çıktığında, EOS Komisyonu, bunları hangi birimin yönettiğinden bağımsız olarak denetim hizmetini eskisi gibi sürdürür. [43]

EOS Komisyonu, esas olarak "ardından denetim" ilkesi doğrultusunda kontrollerde bulunur, ancak komisyon buna gerek görürse, güncel meselelerle ilgili yerinde denetim ve ifade verilmesi talebinde bulunabilir. Öte yandan, EOS Komisyonu'nun, gizli servislerin uygu-

lamalarını değiştirmesi için talimat ya da emir verme yetkisi yoktur. Komisyon yalnızca rapor sunabilir, bunun üzerine gizli servisler uygulamalarını kendileri değiştirmelidir. Sadece hükümet talimatlar verebilir ve Parlamento, yasalar aracılığıyla, gizli servislerin hizmetlerinde belli değişiklikler yapabilir.

EOS Komisyonu'nun yetkilerini değiştirmek için acil bir neden yoktur, ancak Komisyon gizli servisleri etkin bir şekilde denetleyebiliyor mu sorusu sorulabilir. Sorunu şöyle gösterebiliriz: İstihbarat örgütü ve PST'nin 2015 bütçeleri iki milyar krondur. [44] EOS Komisyonu, bu rakama kıyasla, 10 milyon krondan biraz fazla bütçeye sahiptir. [45] Gizli servislerin kaynakları ve gücü o kadar büyüktür ki, EOS Komisyonu'nun etkili bir denetim yapması tehlikeye girer.

Parlamento Başkanlığı'na Mart 2016'da teslim edilen harici bir tetkikte, EOS Komisyonu'nun kaynaklarının artırılması talebine dikkat çekilmiştir. Denetlemenin etkili bir biçimde yürütülebilmesi için, EOS Komisyonu'na fazladan kaynak aktarılmasının önemi vurgulanmıştır. Komisyon'un özellikle teknik yeterliliğini güçlendirmeye ihtiyaç vardır. Bu harici tetkik, bütünlüklü ve stratejik düşünmeyi mümkün kılabileceğinden, EOS Komisyonu başkanı, pozisyonun tam zamanlı olmasını önermektedir. [46]

EOS Komisyonu'nun daha fazla kaynağa acil ihtiyacı olmasına rağmen, Komisyon'un amaçları doğrultusunda çalıştığı ve gizli servislerin denetlenmesi konusunda Norveç modelinin iyi bir model olduğu uluslararası kabul görmüştür.[47] Kaynaklar artsa bile, gizli servisler ile denetleme işlemleri arasındaki bütçe farkı astronomiktir ve bu fark, mahremiyet ihlalleri konusunda olası bir sorundur.

Polis ve İzleme Teknolojisi

Mahremiyetin durumunu büyük ölçüde etkileyen, kolluk güçlerinin yetkileri ve uygulamalarıdır. Bu bağlamda, sadece gizli servisler değil, giderek artan bir biçimde teknoloji kullanan polis de özel hayata fazladan müdahalelerde bulunuyor olabilir. Kısa bir süre sonra, polisin kamuya ait alanı izlemede teknolojiyi büyük ölçüde kullanacağı düşünülebilir. Bu tartışmaya hazır mıyız?

Polisin, günlük işlerinde teknolojiyi yardımcı araç olarak kullanma olanaklarında korkunç bir gelişmeyle karşı karşıyayız. Sorun, teknolojinin gelişimi yönlendirmesine izin verip vermeyeceğimiz.

Kamusal alan ile özel alan arasındaki ilişkinin öncüllerini ve kamusal alana geçildiğinde özel hayat hakkının gözetilmesini ne dereceye kadar bekleyebiliriz sorusuna cevabı netleştirmek önemlidir. Çoğumuz, kamuya açık ortamlarda aynı derecede bir özel hayat beklenemeyeceğini içgüdüsel olarak düşünürüz, aynı zamanda özel nitelikli bir davranışın, bu davranış kamusal alanda yapılmış olsa da özel kalacağını düşünürüz. Telefon görüşmelerini, SMS ya da e-postalarınızı evinizin oturma odasında nasıl algılıyorsanız, bir alışveriş merkezinde de aynı şekilde algılarsınız. Ancak kamuya açık alanlardaki hareketleriniz, kaçınılmaz olarak başkalarının sizin hareketlerinizi izleyebilmesine neden olacaktır. Bu durum normalde çoğumuz için özel hayata müdahale olarak algılanmaz çünkü birlikte olduklarından başka, kamuya açık alanda kimlerin olduğuyla pek az kişi ilgilenir – birileri anormal davranışlar sergilemiyorsa eğer.

Kamusal alanlarda özel hayatla ilgili karşılaşılan sorunlardan biri, giderek artan sayıda güvenlik kamerasının kullanılmasıdır. Norveç'te toplam kaç adet kameranın kullanımda olduğunu kimse bilmemektedir ancak *Aftenposten*'da çıkan bir makaleye göre, sadece Oslo'da 1000'nin üzerinde güvenlik kamerası bulunmaktadır. [48] Bu gelişmenin nedenlerinden biri, pek çok kişinin kamusal alanda izlendiği ve bu yüzden artan sayıda kameranın özel hayata bir müdahaleyi temsil ettiği üzerine muhtemelen pek düşünmemesidir.

Ancak kişinin izlendiği konusunda bilinçlendirilip bilgilendirilmesi, davranışlarını etkiler ve kaçınılmaz bir biçimde özel hayatın huzurunu kaçırır. Sorun, bunun yine de kabul edilebilir olup olmadığıdır?

Güvenlik kameralarının kullanımının bu kadar artmasının bir diğer sebebi, kamera yerleştirmek için özel bir onayın gerekmemesidir, yalnızca mevzuata uyulması yeterlidir. [49] Kamera izlemesinin gerekliliği için, verili amaca uygun gerçekçi gerekçeler olması en önemli taleptir. Eğer böyle bir gereklilik yoksa, kamera yerleştirmek yasal değildir. Ayrıca bölgenin kamerayla izlendiği açıkça belirtilmelidir. Polisin il-

gisini çekebileceğinin düşünülmesi gibi geçerli bir neden olmaksızın, kayıtların saklanmasına izin verilmemektedir.

Parlamento, hükümet binası, Yüksek Mahkeme, askeri tesisler gibi resmi binaların izlenmesine kesinlikle ihtiyaç duyulmaktadır. Kurumların güvenlik amacıyla kapalı devre televizyon sistemiyle gözetleme yapması yasaldır. Aynı amaca uygunluk argümanı, havaalanı, tren istasyonları, limanlar vb. gibi kamuya ait bağlantı noktalarında izlenme için, az da olsa, kullanılabilir. Bu durumlarda da kapalı devre gözetlemenin güvenlik talebi gibi yeterli bir gerekçesi olmalıdır.

Tramvay, tren ve otobüs gibi toplu taşımacılık hizmetlerinde genel gözetleme yapmak için çok haklı nedenler vardır. Kapalı devre televizyon gözetlemesi hiç şüphesiz özel hayata bir müdahaledir, ancak aynı zamanda, olumsuz davranışları sınırlar, suçu engeller ve soruşturmalarda delil olarak kullanılabilir, örneğin tehditkâr ya da istenmeyen bir davranış karşısında, şoför video gözetlemeyi açabilir. Genel video gözetlemesine izin verilecekse, soruşturma ya da benzer şekilde kullanımına ihtiyaç görülmediği takdirde, tüm kayıtların vakit geçmeden silinmesi gereklidir. Aynı görüş hız tespiti için de geçerlidir; hız ölçerler yalnızca ortalama hız ölçtükleri sürece hız sınırları içinde kalanların tümünün otomatik olarak silinmesi gerekmektedir. Bu şekilde, hız ölçeri kullanmanın amacına (trafik kazalarını önlemek ve şoförlerin yol trafik kanunlarına uymalarını güvence altına almak) uyulmuş olur.

Mevzuatı değiştirmek ya da normal vatandaşların kamera kurmaları için dilekçe verme zorunluluğu getirmek genel olarak gerekmemektedir. Gelecek dilekçelerin miktarı düşünüldüğünde, Veri Koruma Kurumu'nun bunları değerlendirmesi mümkün değildir. Bununla beraber, mevzuat konusunda iyi bilgilendirme yapmak, rastgele denetimlerde bulunmak ve illegal kamerayla gözetlemeye göz yummamak önemlidir.

Mahremiyetin en büyük sınavı, teknolojinin gelecekte polisin operasyonlarını nasıl etkileyeceğiyle ilgili olacaktır. Savcı Svein Bakkevig'in belirttiği gibi: "Kameraları, sabit durup film çeken polis memurları olarak görebiliriz, bunlar bizim için çoğunlukla çok faydalıdır."[50] Ancak yazar Newth, izleme teknolojisinin pek yakında çok daha akıllı ve çok

daha müdahaleci olacağını ve eskiden olduğu gibi, ABD'nin bu alanda başı çekeceğini belirtir.

New York'ta polis, Microsoft'la birlikte Alan Farkındalık Sistemi'ni geliştirdi. Bu sistem, Büyük Veri'ye yeni bir biçimde entegre olup devasa boyutta bilgiye erişim sağlamaktadır. Sistem polise, belirli bir bölgedeki tüm kameralara erişebilme, kayıtları geri sarma, başka kayıtlara bağlanabilme ve aynı alan içerisindeki yardım çağrılarını bulup çıkarma olanağı sunar. New York polisi, kısa bir süre içerisinde, 34 bin polis memuruna sisteme erişimi sağlayan terminaller dağıtmayı planlamaktadır. [51]

2013'teki terör olayından sonra, Boston polisi yapay zekâ yazılımlı bir izleme sistemi geliştirmektedir. Yazılım, katı algoritmalara uymaktan çok, tecrübeyle öğrenmek de dahil olmak üzere, insan zekâsını taklit etmektedir.

Bir yandan polis yetkilileri akıllı gözetleme sistemleri geliştirirken, öte yandan büyük miktarlarda bilgiyi işleyip analiz ederek suç konusunda daha iyi öngörülerde bulunabilen "öngörücü polislik" (*PredPol*) gelişmektedir.[52] *Time* dergisi 2011 yılında PredPol'u yılın en önemli 50 buluşuna aday göstermiştir. [53] Bu yöntemi kullanan Los Angeles gibi polis bölgelerinde, suç işlemede önemli bir düşüş kaydedilmiştir.[54] PredPol potansiyel suçu, suçluyu ve kurbanı öngören bir araç geliştirmiştir. Polis, gelişmiş istatistiksel modeller aracılığıyla suçu öngörmeye çalışır. Mevcut suç istatistiği, suçun tekrarı tehlikesi, biyografik bilgi ve hava durumu bile konuyla ilgisi olan bilgiden sayılabilir.

PredPol sistemi, farklı verilerin analizinde ileri düzey programlar kullanarak, belirli bir davranışın olasılık hesabını yapabilir, bu da suçu öngörme becerisinde bir devrimdir. Bazı tür suçların nüfusun çok az bir kesimi tarafından işlendiğini biliyoruz. PredPol'un yapmaya çalıştığı (başarılı olması için daha çok yol kat etmelidir), bu kişilerin kimler olduklarını tanımlamasıdır ve böylelikle suçun olasılığı azaltılır. [55]

İzleme teknolojisinin polisin günlük hayatını nasıl etkileyeceğine dair bir diğer örnek de polis memurunun üzerine giyebileceği kamera kullanmasıdır. Bu şekilde polisin çalışmaları sürekli izlenebilecektir. Böylelikle polisin halkla olan etkileşimi videoya kaydedilir. Newth'ten bir örnek kullanacak olursak; California'nın Rialto şehrinde sürdürülen

bir yıllık deneme projesi, polis hakkındaki şikâyetlerin yüzde 88, polis şiddetinin yüzde 60 oranında düşmesiyle sonuçlanmıştır.[56]

Polisin aktif görev başındayken hareketlerinin belgelenmesi için video kullanımı, ABD'de son yıllarda özellikle tartışılan konulardan biri olmuştur. Video kameralar, bir dizi olay esnasında polis görevlilerinin vatandaşları öldürdüklerini tespit etmiş ve bunun adalet ve düzeni sağlamak için gerekli bir durum olmadığını ortaya çıkarmıştır. Bu durumdan özellikle Siyah Amerikalılar mustariptir. Eski polis görevlisi Reddit Hudson, Amerikan internet sitesi Vox'a yazdığı bir yazıda, polis memurlarının video kamerayla donatılmaları gerektiğini çünkü bunun, memurların davranışlarını denetlemenin en objektif yolu olduğunu yazar. Polis görevlilerinin video kameralarla donatıldığı bir sistem polise güvenin artmasını sağlayabilir çünkü polisin vatandaşla karşı karşıya kaldığında ırkçı ya da başka ayrımcı tutumlar sergilemesini zorlaştırır.[57]

Bu teknolojinin suçla mücadelede faydalı olacağı görülmektedir. Sorun, mahremiyet üzerindeki etkilerle baş edip edemeyeceğimizdir.

Alan Farkındalık Sistemi gibi sistemler aslında kişinin kamuya açık alanda izlenmeden bulunmasını zorlaştıracaktır, ayrıca mikro düzeydeki hareketleriniz (neler satın aldığınız, kimlerle konuştuğunuz) izlenebilecektir. Örneğin Oslo'daki tehdit düzeyinin ya da genel suçların böyle bir müdahaleci aracın kullanılmasına gerekçe olabileceğini söylemek zordur. Ancak yine de uygulanacaksa verilerin silinmesine ve izlemeye kimlerin erişebileceğine dair çok ciddi taleplerde bulunulmalıdır. Aynı itirazlar, yapay zekâ kullanan gözetleme sistemlerinin kullanımı için de geçerlidir.

Verilerin Diktatörlüğü

Yapay zekânın kullanımı ve PredPol'la ilgili bir diğer endişe edilen nokta da dolaylı ya da dolaysız ayrımcılık tehlikesidir. Olasılık hesaplamalarının istatistikleri büyük ölçüde azınlıkları etkiler ve etkileyecektir, bu tür bir teknoloji kullanımı profil çıkarma tehlikesini beraberinde getirir.

Profil çıkarma işlemi, belirli grupların bazı özelliklere (etnik köken, din, cinsiyet, vb.) sahip olduğunu belirtir. Gruplardaki bireylerin suça bulaşma eğilimlerinin istatistik olarak yüksek çıkmasından dolayı,

bu benzer özellikler, azınlıkların daha fazla izlenmesine yol açacaktır. Bu, eşit muamele görme ilkesini tehdit edebilecek bir tür veri diktatörlüğüdür.

Polislerin video kameralarla donatılması sorununa gelince, bu uygulamanın hem polis memurları hem de halk açısından mahremiyeti güçlendireceğini savunanlar vardır çünkü video kayıtları gerçek koşulları belgelemektedir. Bu argüman, güvenlik güçlerine aslında tam güven duymayan gruplar için geçerlidir özellikle. Bu uygulamaya karşı çıkan pek çok kişi vardır. Polis memurlarının görev başındayken güvenlik güçlerini temsil etmelerine karşın, aktif görev başındayken onların da mümkün olduğunca özel hayat talepleri vardır. Norveç'te çalışanlar normalde izlenmemektedir. Bunun polis için uygulanmasında eşiğin yükseltilmesi gereklidir. Bir diğer eleştiri de sürekli izlenmenin, polis memurlarının önemli koşullardan çok, davranışlarının nasıl algılandığıyla ilgilenmelerine yol açma olasılığıdır. Polisler, güvenlik görevlerini iyi bir şekilde yerine getirmek yerine çekingen davranabilirler.

Amaç ve gerekçe arasında ölçülü bir ilişki olmasının altını çizmeliyiz. Müdahale, amaç ve geçerli zemin açısından sağlam gerekçelere sahip midir, değil midir, bunun değerlendirilmesi gereklidir. Amaç ve araç orantılılık ilkesini düşünecek olursak, polis kameralarının ABD'nin bazı bölgelerinde kullanılması, örneğin Oslo'da kullanılmasından daha uygun olabilir. Pek çok silahlı adam vurma olayı yaşandığından, ABD'de polise karşı bir güvensizlik söz konusudur. Yeniden güven inşa etme çalışmalarında video kullanımının olumsuzdan çok olumlu yönleri olması muhtemeldir. ABD'deki ve Norveç'teki durum arasında kökten farklılıklar vardır. Tehdit durumu ve toplumdaki genel güven, izleme konusunda en kapsamlı teknolojiyi kullanmakta çok dikkatli olmamız gerektiğine işarettir.

Verilerin Saklanması ve Kaydedilmesi

Veri Saklama Yönergesi (DLD) hakkındaki tartışma, son onyıllar içerisinde Norveç'teki kamuoyu tartışmaları arasında en kapsamlı mahremiyeti koruma tartışmasıdır. Bu tartışmanın başlamasının sebebi, pek çok kişinin, Norveç vatandaşlarına ait üst verilerin saklanmasını

sorunlu bulmasıdır. DLD, Nisan 2011'de, Parlamento'da Sağ Parti ve İşçi Partisi'nden destek görüp çoğunlukla kabul edilmiştir, ancak 2014'te AB mahkemesi yönergeyi hükümsüz kılmıştır, çünkü yönergenin mahremiyet mevzuatına uygun olmadığına kanaat getirmiştir.[58] Mahkeme kararının ana gerekçesi, DLD yönergesinin bireylerin mahremiyetine geniş çaplı bir müdahale olduğu ve ulaşılmak istenen amaç için bu kapsamlı müdahalenin gerekli olduğuna yeterli derecede açıklık getirilmediğidir. Bu ayrıca, özel bir orantılılık ilkesi değerlendirmesidir ve AEA sözleşmesi gereğince, Norveç'in bu yönergeyi yürürlüğe sokma yükümlülüğü olmadığı anlamı taşır.

Hükümet, Profesör Hans Petter Graver'e (Özel Hukuk Enstitüsü, Oslo Üniversitesi) ve avukat Henning Harborg'e (Thommessen AS Avukatlık Firması), kararın ışığı altında, veri saklama ve insan hakları arasındaki ilişkiyi araştırma görevi verir. Hükümetin verdiği görev, aşağıdakilerin incelenmesini kapsamaktadır:

> Norveç Anayasası'nın 102. maddesinin düzenlediği mahremiyet hakkını ihlal etmeden ve AB Mahkemesi'nin 8 Nisan 2014 tarihli veri saklama direktifi anlayışı içinde insan hakları ilkelerini ihlal etmeden, Norveç saklama yasası düzenlemeleriyle birlikte hangi somut biçimlerde uyarlanabilir? Önerilen çözümün, 2002/58 EF sayılı haberleşmeyi koruma yönergesiyle de uyumlu olmasına dikkat edilmelidir.[59]

Veri Saklama ve İnsan Hakları Raporu'nda Graver ve Harborg, DLD'nin saptadığı veri saklamanın kapsam ve amaçları, AİHS'nin veri saklama uygulaması yüzünden insan haklarıyla çelişmektedir. Özellikle de resmi mercilere çeşitli nedenlerle mevcut bilgilere erişim yetkisi veren yönetmelikler ve muhtemel ceza davalarının açıklığa kavuşturulması amacıyla, normal şartlarda saklanmayacak verilerin saklanmasını sağlayan yasal hükümler bu çelişkiye sebep olmaktadır. Graver ve Harborg şöyle yazar:

> Veri özellikle olası cezayı gerektiren suçları aydınlığa kavuşturmak ve bunlarla mücadele etmek için saklandığında, mesele aslında bir tür izlemeden ibarettir. Haberleşmenin içeriği saklanmasa da bireylerin iletişim ve hareketlerinin incelenmesine yarayan bilgilerin sistematik olarak toplanmasından söz ediyoruz. Bu veriler özel bağlantılar, tercihler, alışkanlıklar, sempati duyulanlar, antipati duyulanlar ve özel niteliğe sahip bir dizi başka ilişki hakkında çok

> şey anlatabilir. Veriler ayrıca, profesyonel bağlantılar, iş stratejileri ve diğer mesleki ya da işle ilgili konularda bilgi verebilir. Dar bir çerçeveden bakacak olursak, bu tür ilişkiler özel hayatın bir parçası olarak tanımlanmasa da bunlar, AİHS madde 8 kapsamında koruma altındadır.[60]

Bu yüzden yazarların, veri saklanması kararlarının, AİHS kararları ve AİHM'nin madde 8'den anladığıyla uyumlu olmadığını söylemeleri şaşırtıcı değildir.

Hem DLD kararı hem de Graver/Harborg'un incelemesi, toplumun yalnızca veri saklanmasını yeniden değerlendirmekle kalmayıp aynı zamanda artan miktardaki verilerin resmi kayıtları nasıl etkilediğini tartışması için bir davettir. Resmi kurumlar çeşitli türde kayıtlar için veri topladığında, mahremiyetin güçsüzleştiği pek çok durumla karşılaşılır. Kayıt edilmek, kişisel bilgilere sizden başka pek çok kişinin erişebileceği anlamına gelir.

Aynı zamanda, resmi kayıtları kabul edilebilir kılan faydalar da söz konusudur. Bu yine orantılılık ilkesiyle bağlantılıdır, yani ulaşılması gereken amaca kıyasla, müdahale gayrimeşru olmamalıdır. Bu anlamda, Brønnøysund Kayıtları diye bilinen kayıtlar çok az sorun çıkarır.[61] Çeşitli kurumlar (ticari ve ticari olmayan) için hazırlanmış şeffaf sistemlerin faydası, özel hayata getirdiği yükten fazladır. Basit ve anlaşılır bilgi, vatandaşların hukuki haklarının gözetilmesine katkıda bulunur. Aynı şey, resmi kayıtlı tüm hakların özeti olan Devlet Eşleştirme Kurumu'nun *ana-kitap* yayını için de geçerlidir. Ana-kitapta tapu senetleri kayıtlıdır ve her türlü mülkiyetle ilgili bilgi mahremiyeti güçsüzleştirse de mülkiyet haklarıyla ilgili bu tür bir genel özetin hukuksal anlamı önemlidir çünkü ulaşılmak istenen amaç, resmi kayıtları meşrulaştırmaktadır.

Bir diğer endişe verici durum vergi ödeme listeleridir çünkü medyanın bunları kullanması mahremiyete zarar vermektedir. Kamuya açık vergi ödeme listeleri, Norveç'teki şeffaflık kültürünün bir parçasıdır. Norveç'in resmi sektörü ve vergilendirme sistemi genel olarak güzel işlemektedir. Bununla beraber, vergi ödeme listelerinin medyada açıklanmasının, şeffaf bir tartışma ortamı hazırlamak için gerekli olup olmadığı pek net değildir. Bu yüzden, gelirinizi kimin kontrol ettiğine dair sizi uyaran sistemin bir benzeri kullanılmaktadır. [62] Böylelikle, örneğin meşru amacı olan

gazeteciler, mevkilerine eleştirel yaklaşma fırsatı bulurlar, aynı zamanda mahremiyet uyarılar sayesinde gözetilmiş olur. Bu, toplumdaki farklı çıkarlar arasında denge tutturmanın iyi bir yoludur.

DNA Kayıtları

Hangi verilerin saklanacağını ve duyarlı veri içeren kayıtlara kimin erişebileceğini denetlemek için doğal olarak daha büyük taleplerde bulunulmalıdır. Eskilere uzanan bir tartışma da DNA kayıtları hakkındadır. Neden tüm halkın DNA'sı tek bir kayıt altında toplanamaz? Bu durumda, aydınlığa kavuşturulmuş ceza dosyalarının oranı artacaktır ve kazalarda ölenlerin kimlikleri daha kolay tespit edilecektir.

Forskning.no'da yazdığı bir makalede Kripos'tan* Vigleik Antun cinayete mahkûm olanların pek azının önceden cinayet işlediğini ancak ciddi suç işleyenlerin yarısının önceden küçük suçlar işlediğini belirtmiştir.[63] Tüm halkın DNA'sının kayıtlı olması hiç şüphesiz faydalıdır. Halkın tamamının DNA kaydının en önemli faydası önleyici etkisidir, yani insanlar suç işlemeden önce yakalanma riskinin yüksek olduğunu bileceklerinden bir kez daha düşüneceklerdir. Suç davalarındaki şüpheli kişiler DNA profillerinden kontrol edilebileceği için mülkiyet hakkı korunması (bu yüzden bazı durumlarda mahremiyeti koruma) güçlendirilebilir. Faydasının dezavantajlarına üstünlüğü bir yana, herkesin DNA'sının kayıt edilmesi için yapılan büyük müdahalenin, amacından yola çıkılarak meşru bir araç olduğunu iddia etmek, orantılılık ilkesinin önerdikleri açısından kuşku uyandırır. Bir üçüncü itiraz da koruma mekanizmalarının devreye sokulmasına rağmen, verileri kötüye kullanma riskinin çok büyük olmasıdır. Bu yüzden Parlamento, kişilerin DNA kayıtlarına erişim olanağını genişletme konusunda kısıtlayıcı davranmalıdır.

Hasta Dosyaları ve Sağlık Kayıtları

Güncellenmiş ve ulaşılabilir sağlık bilgileri, sağlık hizmetlerini en yüksek kaliteye çıkarma çalışmalarında büyük önem taşır. Halkın

---

* Emniyet Müdürlüğü bünyesinde görev yapan organize suçlar şubesi –çn.

sağlık verileri üzerine bilgiler kabaca iki türe ayrılır: Hastalık dosyaları ve sağlık kayıtları. Bunlar Hasta Dosyaları Yasası ve Sağlık Kayıtları Yasası'yla düzenlenmiştir.

Hasta dosyaları, vatandaşın sağlık hizmetleriyle ilişkisi hakkında bilgi toplar (teşhisler, hastalığın seyri, tedavi). Vatandaşa sağlık hizmetinde bulunan tüm kurumlar hasta dosyası oluşturmalıdır. Hizmetlerin en iyi düzeyde yapılabilmesine katkıda bulunacak bilgiler burada toplanır. Aynı zamanda, bu tür bilgiler güçlü mahremiyet koruması altına alınmalıdır; hasta dosyalarının amacı budur.

Sorun, güçlü bir kişisel bilgi koruması ile hasta dosyalarının büyük ölçüde dijitalleşmesinin nasıl birleştirileceğinde yatar. Hasta dosyalarını dijitalleştirmekten vazgeçmenin kişisel bilgileri korumayı güçlendirmesi şart değildir. Bunun nedeni, dijitalleşmenin hasta dosyalarına erişimi denetlemek için sunduğu olanakların, kâğıt dosyalarda olmamasıdır. Herhangi birinin erişimi kontrol edemediği kağıt dosyalar, kişisel bilgilere herkesin ulaşabilmesine izin verir. Buna karşın, dijital teknoloji, kendi dosyasını kimlerin gördüğü hakkında herkesin bilgi edinmesini çok daha iyi bir biçimde mümkün kılar.

Dijitalleşmenin avantajları büyüktür ve dijitalleşme kimlerin bilgiye ulaştığı hakkında daha iyi bir denetim olanağı sunar. Sağlık personelinin ihtiyaç duyduklarında bilgilere erişme olanağı yoksa, hastaya iyi bir şekilde yardımcı olmaları güçtür. Hükümet, 1 Ocak 2015 tarihi itibariyle yürürlüğe giren yeni hasta dosyası kanunuyla bu tutumu hayata geçirmeye çalıştıklarını savunur.

Bilgiyi farklı kurumlar arasında paylaştırmak, bilgilerin duyarlı yapısından dolayı eskiden zorken, şimdi bilginin paylaşımı kolaylaşmakla kalmayıp, kurum olarak bilgiyi başka kurumlarla paylaşmayı da kolaylaştırma yükümlülüğü gelmiştir. Yasanın getirdiği en büyük değişiklik budur. Gerekli erişim, tüm sağlık bilgilerine her zaman ulaşmak anlamına gelmemektedir. Gerekli bilgiye erişim mümkündür, ancak bu erişim, otomatik olarak *tüm* bilgiye ulaşılmasını sağlamaz. Buradaki anahtar sözcük *erişim yönetimli* bilgidir, yani erişim tamamen teknik önlemlerle sınırlandırılır. Bunu yapmak mahremiyeti korumak açısından çok önemlidir. Hastalara ait bilgi, size sağlık yardımında

bulunmak için bilgiye ihtiyacı olan sağlık personeline ulaştırılır ve tıbbi gerekçelerden dolayı personelin erişime ihtiyacı olduğu zaman bilgiler ulaşılabilir olacaktır.

Hassas bilgilere pek çok kişi ulaştığında, bunların kötüye kullanılma tehlikesi doğal bir sorundur. Veri Koruma Kurumu, bilgileri kendimiz kullanırken bile, mahremiyeti korumakta zorluklar çıkabileceğine dikkat çeker. [64]

Sorun, verilerin şifrelenmiş olmasına rağmen kişisel düzeyde tanımlanabilir olmasıdır. Daha önce de belirtildiği gibi, bireyleri tanımlayabilmek için üst veri düzeyinde çok fazla bilgi olması gerekli değildir. Bu konu, özellikle küçük belediyeleri ilgilendirir. Hasta dosyalarına oralarda kimlerin erişim sağlayabileceğini iyi değerlendirmek gerekir.

Veri Koruma Kurumu erişim yetkilerinin çok geniş tutulduğunu düşünse de hasta dosyalarıyla ilgili en büyük sorunun eksik mevzuat olduğu kesin değildir.[65] Kişiye ait hassas bilgileri güvenlik ihlalleri ve izinsiz erişimlere karşı güvence altına alan iyi bir bilişim sistemi kurmak belki de daha önemlidir. Halkın sağlık bilgilerini toplamak, hizmetlerin kalitesini artırmak için önemli bir araçtır. Yetkililer, bilgi toplayarak sağlık hizmetlerini daha rasyonel yürütmenin yanı sıra, halkın sağlık durumunu takip edebilir, tedavinin kalitesini değerlendirebilir ve hastalıkların nedenlerini tanımlayabilir.

Bundan dolayı yetkililer, hasta dosyalarının yanı sıra çeşitli sağlık kayıtları oluşturmuştur.[66] Sağlık kaydı, belirli bir bölgede yaşayan nüfusun sağlık bilgilerinin sistematik bir biçimde toplanmasından oluşur.[67] Norveç sağlık kayıtları kendine ait mevzuatla düzenlenir ve iki çeşit kayda ayrılır: *Merkezi sağlık kayıtları* ve *tıbbi kalite kayıtları.* Birincisi ülke çapındadır ve bazı durumlarda mevzuat, bireylerin tanımlanabilmesinden dolayı çok katıdır.[68]

Tıbbi kalite kayıtları, çeşitli hastalıklara yakalanmış hastaların rızasıyla sağlık verileri toplar. Amaç, tedavinin kalitesini güvence altına almak, hastalığın ortaya çıkışını incelemek ve araştırma yapmaktır. Yaklaşık 200 tıbbi kalite kaydı vardır, bunların 47'sinin resmi ulusal statüsü bulunmaktadır (Ağustos 2014 itibariyle). Bu kayıtların tümü

ülke çapında değildir, ancak ulusal tıbbi kalite kayıtlarının birkaç yıl içerisinde ülke çapına yayılması planlanmaktadır.

Sağlık kayıtlarının kullanımı, "Sağlık Kayıtları ve Tedavi Bilgileri Kanunu" (Sağlık Kayıtları Kanunu) ile düzenlenmiştir ve yasanın en önemli amacı mahremiyetin korunmasıdır:

> Sağlık kayıtlarının oluşturulması, hastalar için taşıdığı önemden dolayı tersine döndürülemez. Bu istenen bir şey de değildir ancak bu, sağlık kayıtlarının nasıl oluşturulduğunun bir önemi olmadığı anlamına gelmez. Tam tersi. Herkesin, kişisel bilginin sağlık kayıtları yasasına uygun bir biçimde korunması yönündeki talebinin dikkate alınması önemlidir. Yasa, tedavinin etik açıdan uygun bir biçimde yapılmasını güvence altına alır.

Mahremiyetin korunması açısından en büyük sorunlardan biri, farklı sağlık kayıtlarını birbirine bağlamanın getirdiği sorunlardır. Halk Sağlığı Enstitüsü (FHI) de, farklı kayıtlardaki verileri birbirine bağlamanın daha basit olması gerektiğini öne sürmektedir. Bu isteğin ardında yatan neden, Parlamento'nun, 2010-2020 döneminde yapılacak tıbbi kalite kayıtları ile merkezi sağlık kayıtlarının koordinasyonu ve modernleştirilmesi için sunulan planı Nisan 2011'de kabul etmesidir. FHI'nın internet sitesinde planın hedefi şöyle belirtilir: "*Norveç 2020'ye kadar, halkın sağlık durumuna ve tedavinin kalitesine dair sürekli güncellenen, güvenilir ve mahremiyetin korunması açısından güvenli bilgiye sahip olacaktır.*"[69] Bunun yanı sıra, FHI bünyesinde geleceğin dijital sağlık kayıtları şu şekilde geliştirilecektir:

- Kayıtlar bugün olduğundan daha hızlı güncellenecektir.

  Farklı kayıtlardan gelen bilgilere daha kolay bir biçimde bağlanılacaktır.

  Kalite artacaktır.

  Analiz kapasitesi büyüyecektir.

  Kayıtlar güçlü bir mahremiyet koruması ve yüksek bir bilgi güvenliğine sahip olacaktır.

FHI'nın argümanını anlamak zor değil; farklı sağlık kayıtlarından gelen bilgiler arasında bağ kurmanın, hastalığın seyri, önlenmesi ve tedavisine dair geniş bir bilgi sağlayacağı açıktır. Çekinceli nokta, farklı

kayıtlardan gelen bilgiler arasında bağlantı kurulduğunda, mahremiyetle ilgili sorunların ortaya çıkmasıdır. Bu tür çapraz bağlantılar, kişisel düzeyde kimlik tanımını kolaylaştırır. Ayrıca sağlık bilgilerinin giderek büyüyen depolanması, bilginin denetiminin yoldan çıkma olasılığını her zaman artırır.

2009 yılında Mahremiyet Komisyonu'nun altını çizdiği gibi, niyet iyi olsa da, bu tür bağlantılar sorunludur. Komisyon, Privacy International araştırmalarına dayanarak bunları ileri sürmüştür. Privacy International, Norveç'in mahremiyet korumasını kötü olarak değerlendirmektedir, çünkü Norveç'te, birbirine bağlanması mümkün çok sayıda tıbbi kayıt bulunmaktadır. [70]

Ancak sağlık kayıtlarının çapraz bağlantılarını kurmanın sağladığı fayda o kadar büyüktür ki, bunu yapmayı imkânsız kılmak önerilemez. Ama bu tür çapraz bağlantılar kurmak, sağlık kayıtlarına kimlerin erişebileceğinin değerlendirilmesini ve bu kayıtların kullanılma şekline çok sıkı bir düzenleme getirilmesini gerektirmektedir. Hükümetin Parlamento'ya sunduğu *Norveç'in Dijital Ajandası – Daha Kolay Bir Gündelik Hayat ve Artan Üretkenlik İçin Bilgi ve İletişim Teknolojisi* konulu ve 27 sayılı (2015-2016) bildirgede hükümet, resmi hizmetler ve özellikle sağlık hizmetleri verilirken vatandaşların mahremiyetlerinin korunmasının öneminin altını çizer. [71]

Bu iyi bir çıkış noktasıdır ancak belirleyici olan, mahremiyetin korunmasına dair düzenin nasıl uygulanacağıdır. Sıkı bir düzen, kişisel bilgileri kimin kullanacağını ve bu bilgilere kimlerin erişebileceğini denetlemenin yanı sıra, ihlallerin zorlaşması için bilgi ve iletişim teknolojisinin işlevselliği konusunda oldukça yüksek taleplerde bulunur.

Sağlık Teknolojisi

Nesnelerin internetinin (IoT) kullanımında, sağlık teknolojisiyle ilgili her alanda devrim yaşanacaktır. Sağlık teknolojisi kavramı, yardıma ihtiyacı olan kişilerin kendi kendilerine bakabilmelerini sağlayan teknolojilerden oluşan geniş bir yelpaze olarak tarif edilebilir basitçe. Sağlık teknolojisi, kullanıcılarına aktif katılım imkânı sunan teknik çözümler ve ürünler için kullanılan ortak bir kavramdır. Bu türden teknolojiye

pek çok örnek verilebilir; cep telefonu çözümleri, bağımsız araçlar ya da ürünler, resmi ve özel konutlara bağlı teknoloji.

Eskiden yardıma ve kontrol edilmeye ihtiyaç duyan insanlar, sağlık teknolojisi sayesinde, yaşlılar evi yerine kendi evlerinde yaşayabilirler. Öte yandan, sağlık teknolojisinin bazı türleri, mahremiyeti koruma açısından sorunlar doğurabilir.

Sorunu şöyle ifade edebiliriz: Bir kişiyi (çoğunlukla yaşlı birini) merkezden gözetleme sistemine bağlayarak önceden elle yapılan bir dizi şey otomatik olarak halledilebilir, örneğin demans hastaları kaybolmamaları için kontrol edilir. Belli başlı hastalıkları kontrol altında tutmak için tıbbi araçlar doğrudan bedene takılabilir ve bir makineye bağlanır. Vücut hastalık belirtileri gösterirse, makine anında bilgiyi alır. Çeşitli cep telefonu uygulamaları, vatandaşlara ne zaman ve hangi miktarda ilaç alacaklarını hatırlatabilir. İlaçların alındığı bilgisi internete de yüklenebilir. Bu yüzden sağlık teknolojisi, vatandaşın kendisinden başkalarının kaydettiği ve depoladığı çok hassas bilgileri içermektedir.

Bu teknolojinin sunduğu avantajlar göz önüne alındığında, kullanılan pek çok aracın orantılılık ilkesine uyduğu söylenebilir. Tüm bunların alternatifi, ya oldukça düşük bir hayat kalitesi ya da yaşlılar evinde yaşamanın beraberinde gelen cılız bir mahremiyet. Sağlık teknolojisini kullanmanın bir diğer önemli faydası, görevlilere günlük işlerinde yardımcı olmasıdır, böylelikle insani ilişkiler ve bakım için vakit kalır. Sorun yine, mevzuat tartışmasından önce, iyi bilgi teknolojileri rutinlerine sahip olmaktır.

Kişisel bilgiler hassas bilgiler oldukları için bunların işlenmesi, kayıt edilmesi güvenli bir şekilde yapılmalıdır ve bu işlemler için gerekli rutinler tatmin edici olmalıdır.

Geleceğin sağlık teknolojisinin insanlığın özel hayatını gerçekten gözetmesi için ilerideki teknolojik çözümlerin özel hayatı ciddiye alması gereklidir. Örneğin, teknolojiler, nerede ve nasıl sorusu hakkında sürekli bir izlemeye başvurmadan detaylı bilgiler verebilir. Teknoloji ve mahremiyet konusunda ülkenin ileri gelen uzmanlarından Doç. Dr. Espen Andersen (BI Üniversitesi), kendi blogunda,[72] Fredrik Øvergård tarafından geliştirilmiş *Smart113*[73] uygulamasından söz eder. Bu uygu-

lama, teknolojik çözümleri iyi mahremiyet çözümleriyle birleştirmiştir. Uygulama, yardım ekiplerinin (örneğin ciddi kazalar olduğunda) hızla ulaşması gereken konum bildirimini gerçek zamanlı paylaşmak üzere geliştirilmiştir. Böyle durumlarda GPS verileri çok faydalıdır, ancak GPS verileri kendi amaçlarına, bu durumda arama ekiplerinin yaralı kişileri bulması amacına, ulaştıklarında, başkaları için çok fazla değer taşımaz.

Bu tür uygulamaları ufak tefek işler için de kullanabiliriz. Çocukların bir yerden alınması ya da anne babalarına nerede olduklarını söylemeleri gerekiyorsa uygulama, kişinin nerede bulunduğu bilgisini, izlenmeden başkalarıyla paylaşmaya yarayabilir. Başka bir deyişle bu, uygulamanın içine gömülü bir özel hayat korumasıdır.

Ruter* uygulaması da, kullanıcı dostu bir hizmeti özel hayatın özenli bir şekilde korunmasıyla birleştirmeyi becererek, mahremiyet politikasını ölçülü kullanan uygulamaya çok güzel bir örnek oluşturur. Örneğin, kullanıcıları hakkında hassas kişisel bilgi depolayan Londra metrosunun seyahat kartıyla (Oyster Card) kıyaslandığında Ruter, kullanıcı hakkında önemli hiçbir veriyi saklamayan tekil, konum bildiren bir hizmettir.[74]

Yeni sağlık teknolojisinin sadece başındayız muhtemelen. Demografik değişimlerden ötürü dünyadaki nüfusun yaş bileşiminde büyük ölçüde yaşlılar ağır basıyor, özellikle de 80 yaş üzerindekiler. Bu grup, yardım ve bakım sektöründeki işgücününün yerini alabilecek bir teknolojiye ihtiyaç duyacaktır ve sağlık teknolojisinin çözümleri hayat kalitesinde büyük değişiklik yaratacaktır; en azından, bunu yapabilecek potansiyele sahiptir.

Öte yandan sağlık teknolojisi dengelenmelidir ki, yaşlıların özel hayatları da korunarak insani bütünlüğe sahip çıkılsın. Bunu da en iyi örneğin, Ruter uygulamalarının çalışma biçimlerinden esinlenip teknolojik çözümleri geliştirerek yapabiliriz.

---

* Oslo'daki toplu taşıma kurumunun adı –çn.

DOKUZUNCU BÖLÜM

Sonuç

Politik bir barometre olarak popüler kültürün rolü küçümsenemez. 1999'daki TV dizisi *Başkan*'da Aaron Sorkin, ABD toplumunun gelecek on yıl içerisindeki en temel sorununun dijital toplumdaki özel hayat olanakları olacağını söyleyerek tam hedefi tutturur. Dizinin 9. bölümünde ("The Short List") Sam Seaborn, 21. yüzyılda mahremiyetin neden en çarpıcı konu olacağına dair şu liberal görüşü aktarır:

> Önümüzdeki yirmi yılın meselesi kürtaj olmayacak. Yirmiler ve otuzlar devletin rolü hakkındaydı. Elliler ve altmışların meselesi sivil haklardı. Önümüzdeki yirmi yıl mahremiyet konuşulacak. İnternetten söz ediyorum. Cep telefonlarından söz ediyorum. Sağlık kayıtlarından, kimin eşcinsel olduğundan, kimin olmadığından söz ediyorum. Daha da ötesi, özgür olma iradesi zeminine kurulmuş bir ülkede bundan daha önemli ne olabilir?

11 Eylül 2001 tarihindeki terör saldırısı, terörizmin mahremiyet açısından olumsuz sonuçlar doğuran baskın bir sorun olmasına katkıda bulundu. Son 15 yıldaki gelişmeler, Sorkin'in zamanın ruhunu nasıl yakaladığını sergiler. Vatandaşların mahremiyeti, izlemenin dev teknolojik olanaklarıyla karşı karşıya kaldığında nasıl korunabilir?

Eskiden izleme, olası tehditleri izleyebilmeleri için otoritelere hangi yetkilerin verilebileceğiyle sınırlıyken, günümüzde mahremiyet kavramı ticari şirketlerin kişisel verileri işleyebilmesi için onlara hangi olanakların tanınacağı sorusuyla ilgilidir. Özel hayat bu yüzden iki yandan aynı anda baskı görür ve bu baskı süreklidir. Sorun pek küçüleceğe de benzemiyor.

Muhtemelen tam tersi olacaktır.

En büyük sorun, özel hayatı sonunda net bir şekilde yürürlükten kaldıran tek bir kararın olmamasıdır. Birlikte işleyen tüm olayların toplamı, özel hayatın konumuna önemli bir meydan okumadır. Tam da bu yüzden kritik sınırı aşmamıza sebep olan tek bir kararı göstermek zordur. Bir gün uyandığımızda özel hayat hakkının yok olduğunu keşfetme tehlikesi var mı?

Son onyıllar içerisindeki terör olayları yüzünden istihbaratın yetkilerini genişletme baskısı hiçbir şekilde son bulmayacaktır. Yeni terör olayları, politikacıların teröre karşı mücadelede sürekli olarak daha çok ve daha sert araçlar kullanılmasına razı olmaya direnmelerini zorlaştıracaktır. Liberal özgürlüğün soyut ilkeleri, çok somut teröre karşı beyhude çaba gibi görünse de işin esası şudur:

Açık, liberal toplumu korumalıyız.

Notlar

BİRİNCİ BÖLÜM

1 "The NSA Files", *The Guardian*, 5 Haziran 2013.

2 Angwin, 2014.

3 Clemet ve Egeland, 2010: s. 101-111

4 Turid Sylte, "Terrorfrykt gir ja til mer overvåkning", *Vårt Land*, 10 Nisan 2016.

5 Bygrave, 2014: s. 5.

İKİNCİ BÖLÜM

1 Larsen, 2010: s. 74.

2 Appelbaum, 2013.

3 Orwell, 1954.

4 Orwell, 1955.

5 Brandeis ve Warren, "The right to privacy", *Harvard Law Review*, 1890.

6 Newth, 2014: s. 58 ve 59.

7 Svendsen, 2010.

8 Richard Esguerra, "Google CEO Eric Schmidt Dismisses the Importance of Privacy", *Electronic Frontier Foundation*, 10 Aralık 2009.

9 Rob Colvile, "Eric Schmidt interview: You have to fight for your privacy or you will lose it", *The Telegraph*, 25 Mayıs 2013.

10 Svendsen, 2010.

11 NOU 2009:1, Birey ve Bütünlük: Dijital Toplumda Mahremiyet.

12 Agy.

13 NOU 1999:27, "İfade Özgürlüğü Gerçekleşmelidir" – Anayasa'nın yeni 100. maddesi için öneriler

14 NOU 2009:1, Birey ve Bütünlük: Dijital Toplumda Mahremiyet.

15 Agy.

ÜÇÜNCÜ BÖLÜM

1 "Arpanet", *Wikipedia*, erişim tarihi: 9 Temmuz 2016.

2 Odd Richard Valmot, "50 år med Moores lov", *Digi.no*, 17 Nisan 2015.

3 Steve Kovach, Lisa Eadicicco ve Steven Tweedie, "Samsung just unveiled Its Plan For The Future", *Business Insider*, 5 Ocak 2015.

4 Bkz. "The Internet of Things: Dr. John Barrett", *Ted Talk*, 12 Ekim 2012.

5 Daniel Ellsberg, "Pentagon Papers", National Archives 1971.

6 Sigmund Hovmoen, "USA ser deg overalt", *Aftenposten*, 13 Temmuz 2013.

7 Bamford, 2002.

8 Glenn Greenwald, "The crux of the NSA story in one phrase: collect it all", *The Guardian*, 15 Temmuz 2013.

9 James Ball, Julian Borger ve Glenn Greenwald, "Revealed: how US anda UK spy agencies defeat internet privacy and security", *The Guardian*, 5 Eylül 2013.

10 Agy.

11 Agy.

12 Matthew DeLuca, "Why are Apple and FBI battling over Iphone?", *NBC*, 16 Şubat 2016.

13 Martyn Williams, "DOJ cracks San Bernardino shooter's iPhone", *PC World*, 28 Mart 2016.

14 Neleri bilebileceğimiz söz konusu olduğunda, yöntem ve uygulamayı birbirinden ayırmakta fayda vardır. Tüm önemli kriptolama sistemleri, dünyanın her tarafındaki uzmanlar tarafından devamlı olarak incelenmektedir. Bu uzmanların hepsi, usulsüzlükleri ortaya çıkarma amacındadır. Bu yüzden, tüm yerleşik yöntemlerin kâfi olduğuna, güvenlik yetkilileri tarafından

öyle kolayca kırılamayacaklarına inanmak için yeterli nedenimiz var. Snowden'ın ifşaatları da bu görüşü destekler yönde. Buna karşın asıl sorun, sistemin pratikte uygulanması. Hain bir uygulamanın (*implementasyon*), dünyadaki en iyi yöntemin bile gizliliğini ihlal etmesini hiç kimse engelleyemez. Çok az sayıda uygulama, denetim (*audit*) dediğimiz şeye maruz kalmıştır ve pek çoğu da sınavı başarıyla geçmiştir. San Bernardino Davası FBI'ın sistemlere kolayca giremediğinin iyi bir örneğidir, aynı şey NSA için de geçerlidir.

15 Bård Standal, Facebook, erişim tarihi: 5 Nisan 2016.

16 NOU 2015: 13, Dijital Duyarlılık – dijitalize olmuş bir dünyada bireyleri ve toplumu korumak. Bölüm 23.8, Şifreleme üzerine.

17 Simon McCallum ve Mariusz Nowostawski, "Tillit satt i system", *Aftenposten*, 18 Nisan 2016.

18 Guardians US interaktif takımı, "Three degrees of separation: breaking down the NSA's 'hops' surveillance method", *The Guardian*, 28 Ekim 2013.

19 Mahremiyet 2014, Durum ve Eğilimler, Veri Koruma Kurumu ve Teknoloji Kurulu.

20 Amy Goodman, "We Don't Live in a Free Country: Jacob Appelbaum on Being Target of Widespread Gov't Surveillance", *Democracy Now*, 20 Nisan 2012.

21 "Mahremiyet 2014, Durum ve Eğilimler: Metadata ve Yeni İstihbarat" Veri Koruma Kurumu ve Teknoloji Kurulu.

22 Matt Blaze, "Phew it was just metadata", *Wired*, 19 Haziran 2013.

23 Agy.

24 James Ball, "NSA stores metadata of millions of web users for up to a year, secret files show", *The Guardian*, 30 Eylül 2013.

25 "Mahremiyet 2014, Koşullar ve Eğilimler: Üst Veri ve Yeni İstihbarat" Veri Koruma Kurumu ve Teknoloji Kurulu.

26 "Ağ tarafsızlığı", NKOM, 29 Aralık 2014.

27 Frode Bjerkestrand, "God natt, Internett", *Bergens Tidende*, 4 Kasım 2015.

28 AB Mahkemesi C13/12 sayılı karar, "*Unutulma hakkı*". Bu karar, Google ile İspanyol Veri Koruma Kurumu (Mario Costeja González'le birlikte) arasındaki davada alınmıştır.

29 Agy.

30 Samuel Gibbs, "Google to extend 'right to be forgotten' to all its domains accessed in EU", *The Guardian,* 11 Şubat 2016.

DÖRDÜNCÜ BÖLÜM

1 Newth, 2014.

2 Joseph McCarthy, "Enemies from within", 9 Şubat 1950'de yapılan konuşma.

3 Conservapedia'daki sayfadan alınmıştır.

4 Newth, 2014.

5 Wikipedia, Church Committee, erişim tarihi: 29 Haziran 2016.

6 15 no'lu belge (1995-1996), Lund Komisyonu Raporu adıyla anılır.

7 "Mahremiyet. Durum ve Eğilimler 2014", Veri Koruma Kurumu ve Teknoloji Kurulu.

8 Newth, 2014: s. 43-44

9 AB Yönergesi 2006/24/EF

10 AB Mahkemesi Kararı, C-293/12 ve C-594/12, 8 Nisan 2014.

11 Jan Arild Snoen, "Klart flertall for Datalagringsdirektivet", *Minervanettt*, 28 Nisan 2010.

12 "Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe", AB, 2015.

13 "Europeiske holdninger til overvåkning", teknologiradet.no, 24 Mart 2015.

14 Agy.

BEŞİNCİ BÖLÜM

1 Simon Rogers, "John Snow's data journalism: the cholera map that changed the world", *The Guardian*, 15 Mart 2015.

2 Bkz. "The Big Data Conundrum: How to Define It?", *MIT Technology Review*, 3 Ekim 2013.

3 Bkz. Gartner'deki Doug Laney'nin internet sayfası.

4 SAS Enstitüsü'nün Big Data sayfası.

5 "Zetabit", Wikipedia, erişim tarihi: 5 Mayıs 2016.

6 SAS Enstitüsü'nün Big Data sayfası.

7 David Lazer ve Ryan Kennedy, "What We Can Learn From the Epic Failure of Google Flu Trends", *Wired*, 1 Ekim 2015.

8 İlginç bir örnek de Telenor'un Pakistan'daki dang humması salgınına karşı mücadele etmek için Büyük Veri analizini kullanmasıdır. Abelia'nın 3 Mart 2015 yıllık konferansında sunuldu.

9 Tarayıcı, bilgisayar, işletim sistemi, telefon-ID, GPS'in sağladığı lokasyon verisinin izi, wifi ağına erişim sayesinde sürülebilir. Bu durum akıllı telefonlar, Ipad'ler ve tüm uygulamalarla dijital hizmetlerin kullanımından sonra daha normalleşmiştir. Ancak özellikle *çerez* kullanımı sorunludur çünkü çerezlerin kullanımının sağladığı olanaklar neredeyse sınırsızdır. Detaylı bilgi için bkz. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.

10 Beit Njarga ve Pål Joakim Olsen, "Fire av fem nettsider bryter cookie-bestemmelsene", dinside. no, 9 Haziran 2015.

11 "Cookies: regjeringen har valgt en dårlig løsning", datatilsynet.no, 5 Mart 2015.

12 Taylor Armerding, "The 5 worst Big Data privacy risks (and how to guard against them)", CSO Online, 12 Aralık 2014.

13 Finn Myrstad, "Datahamstring, formålsutglidning: Digitalt forbrukervern under press", *Vox Publica*, 31 Ağustos 2015.

14 "Big Data and privacy: A technological perspective", Başkan'ın Yürütme Ofisi, Başkan'ın Bilim ve Teknoloji Danışmanlar Konseyi, Mayıs 2014.

15 Agy.

16 Agy.

17 Agy.

18 Agy.

19 "Big Data: Seizing opportunities, preserving values", Başkan'ın Yürütme Ofisi, Mayıs 2014.

20 "Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy", Başkan'ın Yürütme Ofisi, 2012

21 Agy., bkz. s. 68

22 Catherine Nes, "Big Data – Personvernprinsipper under press", Veri Koruma Kurumu, Eylül 2013.

23 Agy., bkz. s. 5.

24 Agy.

25 Agy., bkz. s. 39.

ALTINCI BÖLÜM

1 Kavramın daha geniş bir tanımı için bkz. "Mahremiyet 2016: Koşullar ve Akımlar", Teknoloji Kurulu ve Veri Koruma Kurumu, 2016.

2 Agy.

3 Richard Waters, "Number crunch sees Alphabet enterprise value nudge ahead of Apple", *Financial Times*, 22 Ocak 2016.

4 *Forbes*'in en değerli şirketler listesi (2015).

5 2015 yılı *Forbes* listesinde Facebook 242. sırada ve Google 15. sırada yer almaktadır.

6 Adwords hakkında Google.com'dan daha fazla bilgi alabilirsiniz.

7 Tom DiChristopher, "Why Facebook ad-revenue can keep growing", CNBC, 5 Kasım 2015.

8 Morozov, 2013.

9 Bkz. Morozov'un açılış konuşması: "Datateknologien og politikkens død", Oslo, 13 Aralık 2014.

10 Alex Hern, "Facebook is making more and more money from you. Should you be paid for it?", *The Guardian*, 25 Eylül 2015.

11 Newth, 2014: s. 153.

12 Turrow, Hennessy ve Draper, 2015.

13 "Big Data and privacy: A technological perspective", Başkan'ın Yürütme Ofisi, Başkan'ın Bilim ve Teknoloji Danışma Konseyi, Mayıs 2014, bkz. s. 38.

14 Hoback, 2013.

15 Bkz. Snapchat kullanım şartları.

16 Astrid Dalen, "Forbrukerrådet med leseaksjon mot appvilkår", E24, 24 Mayıs 2016.

17 "7500 Online Shoppers Unknowingly Sold Their Souls", Fox News, 15 Nisan 2010.

18 Agy.

19 Agy.

20 Center for Responsive Politics.

21 Facebook ve Google'ın sürekli karşılaştığı bir diğer eleştiri de vergiden kaçmalarıdır. Bu, konuyla fazlasıyla ilgili önemli bir tartışmadır çünkü iş modelleri büyük ölçüde, Avrupalı vatandaşlardan veri toplamaya dayalıdır. Ancak sorunun karmaşıklığı ve büyüklüğünden dolayı, kitapta bu konuya daha fazla değinilmeyecektir.

22 Tetzscher, 2010.

23 Thaler ve Sunstein, 2008.

24 Kahneman, 2011.

25 Mark Milian, "Google to merge user data across its services", CNN, 25 Ocak 2012.

26 "Big Data and Privacy: A technological perspective", Başkan'ın Yürütme Ofisi, Başkan'ın Bilim ve Teknoloji Danışma Konseyi, Mayıs 2014, s. 38.

27 Hoback, 2013.

28 Google mahremiyet ilkeleri: 2000'den 2001'e yapılan değişiklikler

29 Program hakkındaki soru ve cevapları ACLU'nun internet sitesinde bulabilirsiniz.

30 AB Komisyonu, Güvenli Liman kararıyla ilgili internet sitelerinde etraflı bilgi sunmaktadır.

31 Avrupa Birliği Adalet Divan kararı, C-362/14, Maximillian Schrems Veri Koruma Komiserine karşı, "Güvenli Liman", 6 Ekim 2015.

32 Jon Wessel-Aas, "Europas øverste rettsinstanser har gitt tydelig beskjed til politikerne: Nå er det nok", *Aftenposten*, 7 Ekim 2015.

33 Eva Jarbekk ve Jarle Langeland, "Keep calm og fortsett overføringene av data til USA, men...", *Aftenposten*, 12 Ekim 2015.

34 Håkon Haugli ve Kristine Beitlan, "Privacy Shield skjermer norsk personvern", *Dagens Næringsliv*, 11 Temmuz 2016.

35 Ayrıntılı bilgi için bkz. AB Komisyonu'nun 29/2 2016 tarihli basın bülteni.

36 Madde 29 Grubu'nun basın bülteni, 1 Temmuz 2016.

37 Larry Downes, "The Business Implications of the EU-U.S. 'Privacy Shield'", *Harvard Business Review*, 10 Şubat 2016.

38 Tim Cook, EPIC konuşması, 1 Haziran 2015 (Techcrunch tarafından yeniden sunuldu).

39 Bkz. Apple'ın özel hayat yorumları: apple.com.

40 Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder", *The Guardian*, 11 Ocak 2010.

41 Richard Esguerra, "Google CEO Eric Schmidt Dismisses the Importance of Privacy", EFF, 10 Aralık 2009.

42 Finn Myrstad, "Forbruker- og personvern på nett", Tüketiciyi Koruma Kurumu yönetimindeki sunum, 9 Ekim 2015.

YEDİNCİ BÖLÜM

1 Hayek, 1994.

2 Agy: Hayek, "Keyfi devlet yönetimindeki ülke" ifadesini kullanır.

3 Avrupa Konseyi Parlamenterler Meclisi, Avrupa Konseyi'nin kurumlarından biridir ve üye ülkelerin ulusal parlamentolarının seçtiği temsilcilerden oluşur. Meclisin üyeleri somut konuları araştırır, önerilerde bulunur, salık verir. Parlamenter Meclis'in insan hakları konusundaki tavsiyelerinin, Avrupa'nın politikasında büyük ağırlığı vardır, çünkü Beyaz Rusya dışında tüm Avrupa devletleri mecliste temsil edilmektedir. Avrupa Konseyi

Parlamenterler Meclisi, Avrupa İnsan Hakları Mahkemesi'nin yargıçlarını ve Avrupa Konseyi'nin genel sekreterini seçer.

4 Mr. Peter Omtzigt (EPP), "Mass surveillance", Hukuk İşleri ve İnsan Hakları Komitesi, Avrupa Konseyi Parlamenterler Meclisi Taslak Karar, Ocak 2015.

5 Van der Hilst, 2013.

6 "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor", ABD Pen, 12 Kasım 2013.

7 Van der Hilst, 2013.

8 "Ny forordning for personvern gir flere rettigheter", datatilsynet.no, 16 Aralık 2015.

9 Jems Glanz ve Andrew W. Lehren, "N.S.A. Spied on Allies, Aid Groups and Businesses", *The New York Times*, 20 Aralık 2013.

10 İnsan Hakları Bildirgesi.

11 James Bamford, "They know much more than you think", *The New York Review of Books*, 15 Ağustos 2013.

12 Agy.

13 Agy.

14 ABD Vatanseverlik Yasası, kabul tarihi Ekim 2001.

15 Klaus Wivel, "Opgør med masseovervågningen", *Weekendavisen*, 4 Haziran 2015.

16 Oylama, Vatanseverlik Yasası, ABD Kongresi, 25 Ekim 2001.

17 Thomas Kean, "The 9/11 Commission Report", 22 Temmuz 2004.

18 Glenn Kessler, "Rice defends enhanced interrogations", *The Washington Post*, 30 Nisan 2009.

19 Richard Clarke, "Cheney and Rice Remember 9/11. I Do, Too", *The Washington Post*, 31 Mayıs 2009.

20 Agy.

21 Agy.

22 James Banford, "They know much more than you think", *The New York Review of Books*, 15 Ağustos 2013.

23 Klaus Wivel, "Opgør med masseovervågningen", *Weekendavisen*, 4 Haziran 2015.

24 Spense Ackerman, "James Clapper: Obama stands by intelligence chief as criticism mounts", *The Guardian*, 12 Haziran 2013.

25 James Banford, "They know much more than you think", *The New York Review of Books*, 15 Ağustos 2013.

26 Harald Brombach, "NSA-direktøren: Kryptering er grunnleggende for fremtiden", digi.no, 26 Ocak 2016.

27 Agy.

28 NSA izlemelerine karşı EFF'nin faaliyetlerine dair kronolojik ve tematik iyi bir incelemeyi kurumun web sitesinde bulabilirsiniz.

29 Dia Kayyali, "Section 215 Expires – For Now", EFF, 31 Mayıs 2015.

30 Jennifer Steinhauer ve Jonathan Weisman, "U.S. Surveillance in Place Since 9/11 Is Sharply Limited", *The New York Times*, 2 Haziran 2015.

31 Mark Jaycox ve Dia Kayyali, "The New Senate USA FREEDOM Act: A First Step Towards Reforming Mass Surveillance", EFF, 29 Temmuz 2014. Aşağıdakilere dikkat ediniz: Yasama, şüphe uyandıran izlemeye tamamen son veremeyebilir. Tüm ayrıntılı kayıtlara rağmen yasa, ilk belirli seçim dönemine "doğrudan bağlantılı olma" gibi belirsiz bir ifadeyle, NSA'nın ikinci bir tur (ikinci bir sekme) kayıtlar yapmasına izin veriyor. Çünkü, "doğrudan bağlantılı olma" standartı belirsizlik taşıdığından, hükümet bu ifadenin doğurduğu mantıklı şüpheyi gidermek zorundadır.

32 Klaus Wivel, "Opgør med masseovervågningen", *Weekend* gazetesi, 4 Haziran 2015.

33 James Bamford, "They know much more than you think", *The New York Review of Books*, 15 Agustos 2013.

SEKİZİNCİ BÖLÜM

1 İfade, İsveçli sanayi lideri Jan Stenbeck'ten alınmıştır.

2 NOU 2009:1, Birey ve Bütünlük – Dijital Toplumda Mahremiyet.

3 Busch, Tor Aksel, 2010.

4 Agy.

5 Wessel Aas, 2014.

6 NOU 2009:15, "Gizli bilgi – açık denetim."

7 Wessel Aas, 2014: Detaylı bilgi için bkz. s. 43-44

8 NOU 2012:14, raporunun incelenmesi: 22 Temmuz Komisyonu'ndan rapor.

9 Ceza Kanunu'nun 47. madde beşinci fıkrasında şöyle der: "Kişi, birinci ve ikinci fıkralarda belirtilen yasaları çiğneme niyetindeyse ve niyetini uygulama yönünde hareketler yaparsa, 51. madde gereği teşebbüs suçundan cezalandırılır." Daha yakından incelemek için bkz. Prop 131L (2012-2013) ve Öneri 442L (2012-2013).

10 Wessel Aas, 2014: s. 49.

11 Agy., bkz. s. 50.

12 Erling Johanne Husabø, "Demokratik hukuk devletinde hazırlık faaliyetlerinin suç kapsamına girmesinin sınırları ve teröre karşı gizli zorlayıcı tedbirlerin kullanımı", 22 Temmuz Komisyonu'na ait Tutanak: 6/12, 8 Mart 2012: s. 12.

13 Wessel Aas, 2014: s. 51.

14 Meşru Karar 87(2015-2016) *Ceza Hukuku Usulünde Değişiklikler vb. (gizli zorlayıcı tedbirler), Parlamento, 8 Haziran 2016.*

15 Öng. 68L (2015-2016).

16 NOU 2015:13, *Dijital Duyarlılık – Güvenli Toplum – Dijital Bir Dünyada Bireyleri ve Toplumu Koruma.*

17 Andreas Bakke Foss, "Anundsen om nye overvåkingsmetoder: På dette området skal man være ekstra påpasselig", *Aftenposten*, 28 Mayıs 2016.

18 Anders Anundsen, "Ingen snikinnføring av politimetoder i kampen mot alvorlig kriminalitet", *Nettavisen*, 26 Mayıs 2016.

19 Jon Wessel-Aas ve Erlen Balsvik, "Høringsuttalelse til forslag om utvidet overvåkning", Uluslararası Hukukçular Komisyonu, 6 Nisan 2016.

20 Johanne Hovland, Runar Henriksen Jørstad ve Anders Brekke, "Behandler omstridt overvåkingslov i dag", *NRK*, 8 Temmuz.

21 John Christian Elden, "Når vi lures inn i overvåknings-samfunnet", *Nettavisen*, 25 Mayıs.

22 Anayasa'nın 102. maddesi şöyle der: "Herkesin özel ve aile hayatına, konut ve yazışmalarına saygı gösterilmesi hakkı vardır. Konut aramaları, suç işleme durumları hariç yapılamaz. Devlet yetkilileri kişisel bütünlüğü korumayı gözetmelidir."

23 NOU 2009:15, "Zorlayıcı tedbirlerin kullanımına dair önleyici ve caydırıcı kurallar, Anayasa'nın 102. maddesindeki konut incelemeleri yasağına uymakta mıdır?" Alf Petter Høgberg ve Marius Stub, 31 Mart 2009.

24 NOU 2009:15, "Zorlayıcı tedbirlerin kullanımına dair önleyici ve caydırıcı kurallar, anayasanın 102. maddesindeki konut incelemeleri yasağına uymakta mıdır?", Denetim Metodu Kurulu tezi, Erling Johannes Husabø, 9 Nisan 2009.

25 Schartum, 2010: s. 8.

26 Christine Svendesen, "PST vil samle stordata", NRK, 22 Ağustos 2014.

27 Mahremiyet 2014, Koşullar ve Eğilimler, Veri Koruma Kurumu ve Teknoloji Kurulu.

28 *Aftenposten*, ortaya çıkanlar hakkındaki yazıları aftenposten.no sayfasında toplamıştır.

29 Andreas Slettholm ve Eivind Nicolai Lauritsen, "PST henlegger sak om falske basestasjoner", *Aftenposten*, 2 Temmuz 2015.

30 Jan Arild Snoen, "Anundsen har gått av", *Minervanett*, 10 Mart 2015.

31 "Oturum- Polis Yasası ve Elektronik Haberleşme (Cep Telefonu İzleme ve Sinyal Kesme Alanları Düzenlemesi) Yasa Teklifi", Hükümet, 4 Aralık 2014.

32 Andreas Bakke Foss ve Per Anders Johansen, "Svært omfattende og inngripende i den enkelte borgers personvern og rettssikkerhet", *Aftenposten*, 20 Ocak 2015.

33 PST'nin terör mevzuatıyla ilgili yasa değişikliği teklifi ve PST'nin kullandığı yöntemler, 13 Aralık 2011.

34 "Polisin güvenlik hizmetine ilişkin kurum dışı soruşturma", Traavik Komisyonu'nun raporu, Aralık 2012.

35 Osman Kibar, "INNBRUDDSALARAMEN", *DN Magasinet*, 20 Haziran 2015.

36 Agy.

37 Mahremiyet 2014, Koşullar ve Eğilimler, Veri Koruma Kurumu ve Teknoloji Kurulu 2014.

38 Agy.

39 "Ser på problemstillinger ved tilgang til den digitale informasjonsflyten inn og ut av Norge", Savunma Bakanlığı basın bülteni, 24 Şubat 2016.

40 Arild Færaas, "Regjeringen vurderer å la E-tjenesten få overvåke din internettbruk", *Aftenposten*, 25 Şubat 2016.

41 "Ser på problemstillinger ved tilgang til den digitale informasjonsflyten inn og ut av Norge", Savunma Bakanlığı basın bülteni, 24 Şubat 2016.

42 EOS Komisyonu'nun internet sayfasından.

43 Agy. Komisyon, denetim görevinden yola çıkarak, gerekli gördüğünde müdürlüğün başka bölümlerinde de inceleme yapabilir.

44 Sveinung Berg Bentzrød, "Etterretningstjenesten og PST får 150 millioner ekstra", *Aftenposten*, 10 Ekim 2014.

45 EOS Komisyonu'nun 2014 yıllık raporu.

46 Belge 16 (2015-2016), "Parlamento'nun İstihbarat– İzleme– ve Güvenlik Hizmetlerini Denetleme Komisyonu'nu (EOS Komisyonu) Değerlendirme Kurulu'nun Parlamento'ya sunduğu rapor", 29 Şubat 2016.

47 Agy.

48 Gunnar Kagge, Charlotte Karlsen ve Arild Færaas, "Krever opprydding i Oslos kamerajungel", *Aftenposten*, 24 Ağustos 2015.

49 Veri Koruma Kurumu'nun internet sayfasındaki giriş bölümüne bakınız.

50 Newth, 2014: s. 67.

51 Chris Francescani, "NYPD expands surveillance net to fight crime as well as terrorism", *Reuters*, 21 Haziran 2013.

52 Predpol.

53 Lev Grossman vd., "The 50 Best Inventions", *Time*, 28 Kasım 2011.

54 Newth, 2014: s. 72.

55 Agy.

56 Agy., s. 76

57 Redditt Hudson, "I'm a black ex-cop, and this is the real truth about race and policing", *Vox*, 7 Temmuz 2016.

58 AB Mahkemesi kararı, "C-293/12 ve C-594/12 Dijital Haklar İrlanda ve Seitlinger ve Diğerleri", 8 Nisan 2014.

59 Hans Petter Graver ve Henning Harborg, "DATALAGRING OG MENNESKERETTIGHETENE", 1 Ekim 2015.

60 Agy: s. 93-98.

61 Daha fazla bilgi için Brønnøysund Kayıtları'nın internet sitesine bakınız.

62 datatilsynet.no, 3 Nisan 2014.

63 Ingrid Spilde, "DNA-register - fordel eller fare?", forskning.no, 21 Haziran 2005.

64 "Kritisk til utvidet tilgang til helseopplysninger", Veri Koruma, 8 Aralık 2015.

65 Agy.

66 helseregister.no.

67 Daha fazla bilgi için bkz. Müdürlüğün e-sağlık internet sitesi.

68 Merkezi kayıtlar, öncelikle sağlık istatistiği ve hazırlıkları, sağlık hizmetlerinin kalitesinin artırılması, sigorta, yönetim ve idare ile ilgili sağlık izlemesi için kullanılır. Tıbbi Doğum Kayıtları, Kanser Kayıtları, Norveç Hasta Kayıtları ve Ölüm Sebebi Kayıtları bu tür merkezi sağlık kayıtlarına örnektir. Daha fazla bilgi için bkz. helseregistre.no.

69 FHI'nın internet sitesi.

70 NOU 2009:1, Birey ve Bütünlük - Dijital Toplumda Mahremiyetin Korunması.

71 Hükümetin Parlamento'ya sunduğu, *Norveç'in Dijital Ajandası – Daha Kolay Bir Gündelik Hayat ve Artan Üretkenlik İçin Bilgi ve İletişim Teknolojisi* başlıklı ve 27 sayılı bildirge (2015-2016).

72 Espen Andersen, "Smart113 – appen som finner deg", Espen Andersen'in blogu, 1 Ekim 2015.

73 Smart113 internet sayfası.

74 Ruter'in mahremiyet politikası.

Dizin

MAHREMİYET

DİJİTAL TOPLUMDA ÖZEL HAYAT

Eirik Løkke

teknoloji/hukuk

Bir gün uyandığımızda, özel yaşam hakkının yok olduğunu görme tehlikesi var mı? 5 Haziran 2013'te, NSA çalışanı Edward Snowden'ın sızdırdığı bilgilere dayanarak The Guardian'da yayımlanan bir makale, gözetleme toplumunun artık distopik bir gelecek olmaktan çıktığını gösteriyordu. Peki, biz bu gerçeğin ne kadar farkındayız? İçerdiği sorunların ve yol açtığı sonuçların bilincinde miyiz?

21. yüzyılda artık, devletlerin resmi kurumlarının, sosyal medya şirketlerinin, bankaların vb. sunduğu dijital hizmetlerin tüketicileriyiz. Uluslararası terörizm tehdidinin yol açtığı korkunun tehlikeli yoldaşlığı, ülke güvenliğini öne sürerek izleme yapılmasına anlayış gösterme tutumuna yol açmıştır. Üstelik, özel yaşam hakkınızı korumak amacıyla, yaşamın tüm devrelerine sızan bu dijital ağların dışında analog bir yaşam sürmeye kalkmanın sonucu daha fazla dikkat çekmek olabilir; çünkü elektronik iz bırakmamaya çalışmak bir dolu angaryayı göze almak demek.

Mahremiyet: Dijital Toplumda Özel Hayat, yeni teknolojilerin özel yaşamımızı nasıl doğrudan tehdit ettiğini açıklıyor. Kişisel verilerimizin kaydedilerek hem istihbarat örgütleriyle paylaşılması hem de ticari şirketlere pazarlanması sonucunda ihlal edilen özel yaşamımızı daha iyi koruyabilmek için ne tür yasal düzenlemelere ihtiyaç olduğunu; hem mahremiyetin önemseneceği hem de faydalı dijital araçların ve hizmetlerin gelişmesini sağlayacak bir dengenin nasıl kurulacağını ele alıyor.

Eirik Løkke, bağımsız bir think tank olan Civita'da danışman olarak çalışıyor.

Norveççeden çeviren: Dilek Başak

KÜY

THG 0805387 LDA

18 TL

ISBN 978-605-2116-46-3

9 786052 116463