İnternet ve daha geniş dijital dünyada hukukun üstünlüğü

Özet ve Avrupa Konseyi İnsan Hakları Komiseri'nin tavsiyeleri

Tematik Belge

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

İnternet ve daha geniş dijital dünyada hukukun üstünlüğü

Avrupa Konseyi İnsan Hakları Komiseri tarafından yayımlanan tematik belge

Özet ve Komiser'in Tavsiyeleri

Avrupa Konseyi

Tematik Belgeler önemli güncel insan hakları meseleleri hakkında tartışmaya ve düşünmeye katkıda bulunmak amacıyla İnsan Hakları Komiserliği tarafından yayımlanır. Birçoğunda söz konusu meselelerle ilgili Komiser'in Tavsiyeleri de yer alır. Bu uzman raporlarındaki tüm fikirler Komiserliğin görüşünü yansıtmıyor olabilir.

Tematik belgelere Komiserliğin web sitesinden de ulaşılabilir: http://www.coe.int/en/web/commissioner/publications

Kapak fotoğrafı: Shutterstock
Kapak ve Tasarım: Avrupa Konseyi Belge ve Yayın Yapım Departmanı
Avrupa Konseyi

Teşekkür:

Bu Tematik Belge Profesör Douwe Korff (Visiting Fellow, Yale Üniversitesi (Information Society Project) ve Oxford Martin Associate, Oxford Martin School, Oxford Üniversitesi, Birleşik Krallık) tarafından hazırlanmıştır. Kendisi ve Komiser ayrıca EDRi'den (European Digital Rights) Joe McNamee'ye bu tematik belgenin taslak metnine, özellikle de kolluk hizmetlerinin özelleştirilmesi ile ilgili yaptığı çok faydalı yorumlar ve ilaveler için teşekkür eder.

Içerik

Özet

Bu tematik belge, giderek aciliyet kazanan bir sorunu ele almaktadır: internette ve onu içeren geniş dijital dünyada, hukukun üstünlüğünün yerleşmesini ve kalıcı hale gelmesini nasıl sağlayabiliriz? 1. bölüm çevrimiçi etkinliklerin kapsamını ve bu ortama yönelik tehditleri ele almaktadır; 2. bölüm yavaş yavaş oluşmakta olan "internet yönetişimi" ilkelerini tartışmakta ve ABD (ve Avrupa özelinde, Birleşik Krallık) tarafından dijital dünya üzerinde uygulanan özel denetime ve bu denetimin internette neden olabileceği bölünmeye dikkat çekmektedir. 3. bölüm hukukun egemenliğinin uluslararası standartlarının bir taslağını çıkarmakta ve hukukun bu yeni alanda uygulanmasında ortaya çıkan bazı sorunlara değinmektedir. 4. bölüm ise daha önceki bölümlerde ortaya çıkan temel konulara – ifade özgürlüğü, özel şirketlere devredilen kolluk görevi, verilerin korunması, bilişim suçları ve millî güvenlik – daha detaylı bir bakış getirmekte ve bu kavramların gerektirdiği hassas dengeleri tartışmaktadır.

Avrupa Konseyi İnsan Hakları Komiseri, bu tematik raporda ortaya atılan konularla ilgili bazı tavsiyeler oluşturmuştur; bunlar da Özet'in hemen arkasında yer almaktadır.

İnsan etkinlikleri için yeni bir ortam

Bugün yerel, bölgesel ve küresel etkinliklerimizde bize yeni araçlar sunan, küresel ve dijital bir ortamda yaşıyoruz. Bu etkinliklere siyasi aktivizm, kültürel alışveriş ve insan haklarının kullanımının yeni türleri de dâhil. Bu etkinlikler, "aslında gerçek değil" diyebileceğimiz anlamda sanal değiller. Tam tersine, gerçek vatandaşların yaşamlarının önemli bir bölümünü oluşturmaktalar. İnternete ve dijital medyaya ulaşımımızın kısıtlanması ve çevrimiçi etkinliklerimizin ya da elektronik iletişimlerimizin izlenmesine yönelik girişimler, bizim temel haklarımız olan ifade ve bilgi alma, örgütlenme, mahremiyet ve özel yaşam özgürlüklerimize (ve muhtemelen din ve inanç özgürlüğü ya da adil yargılanma hakkı gibi diğer haklarımıza da) bir müdahale oluşturmaktadır.

Yeni küresel dijital ortam, elbette aynı zamanda hukuksuz davranışlar için de yeni bir alan oluşturmaktadır. Örneğin nefret söylemi ya da çocuk pornografisinin yayılması, şiddete kışkırtma, telif hakkı ihlalleri ("korsanlık"), dolandırıcılık, kimlik hırsızlığı, kara para aklama ve zararlı yazılımlarla (mesela truva atı yazılımları ya da solucanlarla) elektronik iletişim altyapısının kendisine yapılan saldırılar ya da "hizmet reddi" ("denial of service") saldırılarını sıralayabiliriz. Bilişim suçları ve bilişim güvenliği önemli sorunlar haline gelmiştir.

Bu tehditler her geçen gün daha da ulusaşırı hale gelmektedir; dolayısıyla bilişim suçları, bilişim güvenliği ve terörle mücadele etme gerekliliği ile ilgili geniş bir uluslararası fikir birliği mevcut olmakla birlikte, ayrıntılar hakkında, neyin tehdit sayılacağı konusunda bile, pek bir mutabakat yoktur.

Burada dört mesele öne çıkmaktadır. Birinci olarak, bilişim suçlarını engellemeye yönelik devlet faaliyetleri, bilişim güvenliğine yönelik tehditler ve millî güvenliğe yönelik tehditler giderek birbirinin içine girmektedir; bu tip faaliyetler arasındaki sınırlar giderek bulanıklaşmakta ve bunlarla uğraşan kurumlar ve kuruluşlar giderek birbiriyle daha yakın çalışmaktadır. İkincisi; devletler artık tüm bu konulardaki eylemlerini koordine etmektedirler. Üçüncü olarak; millî güvenlik ve istihbarat kuruluşlarının çalışmaları giderek bireylerin ya da grupların dijital ortamdaki faaliyetlerinin izlenmesine dayalı hale gelmektedir. Dördüncü olarak; suç işlendikten sonra hukuki yaptırım uygulamaktansa, artık istihbarat ve önlemeye önem verilmektedir. Bu da, daha önce gizli servislere özgü olan teknikleri ve teknolojileri şimdi emniyet teşkilatlarının kullanması anlamına gelmektedir.

Dijital ortamın doğası

Tehlikeli veri

"Büyük Veri" (eylemlerimizle ilgili verilerin paylaşıldığı ve/veya bütün olarak birilerinin çıkarına kullanıldığı) ve "Eşyaların interneti"nin (giderek daha fazla fiziksel nesnenin – eşyaların – internet üzerinden tanıtıldığı) çağında, anonim kalmayı sağlamak giderek zorlaşmaktadır: Ortada ne kadar çok veri varsa, bir kişinin kimliğini tespit etmek de o kadar kolaylaşmaktadır. Dahası, Büyük Veri'nin daha da ince ve karmaşık şekillerde madenlenmesi, kullanıcı profillerinin oluşturulmasına yol açmaktadır. Her ne kadar bu profiller nadir durumları saptamakta kullanılsa da (örneğin geniş bir veri grubundan – diyelim Yolcu İsim Kayıtlarından – bir teröristi bulmak) güvenilir değildir ve istemsizce de olsa ırk, cinsiyet, din ya da milliyet üzerinden ayrımcılığa neden olabilir. Bu profiller öyle karmaşık şekillerde oluşturulmaktadır ki, bunlara dayalı kararlar fiilen sorgulanamaz hale gelmektedir, hatta bu kararları uygulayanlar bile altta yatan mantığı tamamen kavrayamamaktadır.

Dijital ortam tamamen kendi yapısı nedeniyle mahremiyete ve diğer temel haklara zarar verebilir ve kararların hesap verebilir şekilde alınmasını engelleyebilir. Bu nedenle mahremiyet haklarını zayıflatarak ya da yok ederek, iletişim ya da örgütlenme özgürlüğünü kısıtlayarak hukukun üstünlüğünü zayıflatma ve keyfi müdahalelere neden olma potansiyeli çok büyüktür.

Küresel ve özel fakat gökte değil

İnternetin açık yapısı nedeniyle (ki bu onun en büyük gücüdür) ağ üzerindeki herhangi bir uç nokta hemen hemen tüm diğer uç noktalarla iletişim kurabilir. Bunun için en verimli olarak hesaplanan yolu izler; veriler çeşit çeşit anahtarlardan, yönlendiricilerden ve kablolardan akarak geçer: Bu internetin fiziksel altyapısıdır. Elektronik iletişim sistemi kendi doğası nedeniyle ulusaşırıdır, hatta küreseldir; altyapısı ise, 'Bulut' tanımlamasına rağmen aslında fizikseldir ve gerçek mekanlara yerleştirilmiştir. Şu

anda bu fiziksel bileşenlerin pek çoğu ABD'dedir ve devlet kurumları tarafından değil özel kuruluşlar tarafından yönetilip denetlenmektedir.

İnternetin ana altyapısı, dünyanın okyanusları ve denizleri altından geçen yüksek kapasiteli fiber optik kablolardan ve onlara karadan bağlanan kablo ve yönlendiricilerden oluşur. Avrupa için en önemli kablolar, kıta Avrupa'sından Birleşik Krallık'a, oradan da Atlas Okyanusu'nun altından ABD'ye giden kablolardır.

Amerikan şirketlerinin İnternet ve Bulut'taki egemenliği göz önüne alındığında bu kabloların Avrupa'ya gelen ve Avrupa'dan çıkan verinin hemen hemen tamamı dâhil olmak üzere dünyanın tüm internet trafiğinin ve internet tabanlı iletişim verisinin büyük bir oranını taşıdığı görülür.

Denetim kimde?

İnternet denetimi

Avrupa Konseyi ve başka merciler tarafından, uluslararası kamu hukukunun ve uluslararası insan hakları hukukunun çevrimiçi ve çevrimdışı ortamlarda eşit uygulanması ve internette hukukun üstünlüğüne ve demokrasiye saygı gösterilmesi gerektiğini vurgulayan önemli internet yönetişimi ilkeleri ortaya konmuştur. Bu ilkeler internet yönetişiminin çok paydaşlı yapısını kabul etmekte ve desteklemektedir; ayrıca kamu ve özel sektörü yeni teknolojilerin, hizmetlerin ve uygulamaların tasarımı da dâhil olmak üzere tüm işlemlerinde ve etkinliklerinde insan haklarını ön plana almaya teşvik etmektedir. Devletleri de, başka milletlerin egemenliklerine saygı göstermeye ve kendi bölgesel yargı yetkilerinin dışında kalan kişilere ya da kurumlara zarar verecek faaliyetlerden kaçınmaya çağırmaktadır.

Fakat bu ilkeler hala büyük oranda sözde kalmakta ve bir iyi niyet ifadesinden öteye gidememektedir: Bu ilkelerin gerçekte uygulanmasını sağlayacak internet yönetimi düzenlemelerinde hala eksiklikler bulunmaktadır.

Aynı zamanda, internet yönetişiminin hesaba katması gereken bir gerçek – kısmen şirketlerinin baskınlığından, kısmen de geçmişten gelen düzenlemelerden dolayı – ABD'nin internet üzerinde dünyanın tüm devletlerinden daha fazla denetiminin olmasıdır. ABD'nin, yakın ortağı Birleşik Krallık ile birlikte, internet altyapısının büyük bölümüne erişimi vardır.

Daha önce ABD Millî Güvenlik Kurumu içerisinde bir yüklenici şirket hesabına çalışmış olan Edward Snowden, ABD ve Birleşik Krallık'ın bu denetim ve erişim kabiliyetlerini internetin, küresel elektronik iletişim sistemlerinin ve sosyal ağların kitlesel olarak gözetlemesi amacıyla kullandıklarını ifşa etmiştir. Devletlerin Snowden'in bu açıklamalarına internetin bölünmesi ile cevap verebileceğine dair korkular bulunmaktadır; ülkeler ya da bölgeler, kendi verilerinin sadece yerel yönlendiriciler ve kablolar aracılığıyla yönlendirilmesi ve yerel bulutlarda depolanmasını isteyebilirler. Bu, küresel ağa ulusal bariyerler yaratarak, bildiğimiz anlamıyla interneti yok etme riski taşımaktadır. Eğer ABD, interneti ve küresel iletişim sistemlerini etkileyen faaliyetlerini uluslararası insan hakları standartlarına daha uygun hale getirmezse, bu şekilde kesintili bir internet yaratmaya doğru ilerleyişi durdurmak zor olacaktır.

Özel sektör denetimi

İnternetin ve diğer dijital ortamların büyük bölümünün altyapısı özel kuruluşların elindedir, bunların çoğu da ABD şirketleridir. Bu sorunlu bir durumdur çünkü şirketler doğrudan uluslararası insan hakları hukukuna tabi değildir – uluslararası hukukun direk özneleri devletler ve hükümetlerdir – ve bu tip şirketlerden tazminat elde etmek çok daha zordur. Ayrıca, özel kuruluşlar kuruldukları ya da faaliyet gösterdikleri ülkelerin ulusal kanunlarına bağlıdır ve bu kanunlar her zaman uluslararası hukuk ya da uluslararası insan hakları standartlarına uygun değildir: internet üzerindeki faaliyetlere uluslararası insan hakları hukukuna aykırı kısıtlamalar (genelde ifade özgürlüğü anlamında) getirebilirler; ya da, örneğin internet faaliyetlerinin ya da elektronik iletişimin izlenmesi gibi konularda uluslararası insan hakları hukukuna aykırı müdahalelerde bulunabilir veya bu müdahalelere izin verebilirler; ve bu tip eylemler sınır ötesi şekilde, diğer devletlerin egemenliklerini ihlal edecek şekilde uygulanabilir.

Ulusal hukukun, dijital dünyanın önemli bir kısmının kontrolünü elinde bulunduran özel şirketlerin faaliyetlerine uygulanması son derece karmaşık ve hassas bir konudur. Tabii ki devletlerin interneti ya da elektronik iletişim sistemlerini kullanan suç faaliyetleriyle mücadele hakkı, hatta görevi vardır. Bu nedenle doğal olarak özel sektörün de işbirliğini isterler. Sorumlu şirketler de ürün ve hizmetlerinin suç amacıyla kullanılmasını engellemek isteyeceklerdir. Bununla birlikte, bu tip durumlarda devletler hem uluslararası insan hakları taahhütlerine bire bir uygun davranmalı hem de diğer devletlerin egemenliklerine tamamen saygı göstermelidir. Özellikle devletler, aracıların "gönüllü" olarak insan haklarını kısıtlamaya teşvik ederek anayasal ya da uluslararası yükümlülüklerinden kaçmaya çalışmamalı, şirketler de bireylerin insani haklarına saygı göstermelidir.

Dijital ortamda hukukun üstünlüğü

Hukukun üstünlüğü

Hukukun üstünlüğü, devletin kendisi de dâhil, kamu ve özel olmak üzere tüm kişi, kurum ve kuruluşların yasalar karşısında sorumlu olduğu bir yönetim ilkesidir. Söz konusu yasalar resmen açıklanmış olmalı, herkese eşit bir şekilde bağımsız bir yargı tarafından uygulanmalı, ve uluslararası insan hakları kuralları ve standartlarına uyumlu olmalıdır. Hukuk karşısında eşitlik, hukuki sorumluluk, hukukun uygulanmasında adalet, güçler ayrımı, karar verme sürecine katılım, hukuki kesinlik, keyfiyetten kaçınma ve yöntemsel ve yasal şeffaflık ilkelerine bağlılık ilkelerini de içinde barındırır.

Avrupa İnsan Hakları Mahkemesi tarafından geliştirilmiş temel "hukukun üstünlüğü" kriterleri

Avrupa İnsan Hakları Mahkemesi, kendi dava hukuku içinde, ayrıntılı "hukukun üstünlüğü" kriterleri geliştirmiş ve bu kriterler başka uluslararası insan hakları organları tarafından da benimsenmiştir. Bu kriterleri karşılayabilmek için temel haklar üzerindeki tüm kısıtlamalar net, kesin, kolay ulaşılır ve öngörülebilir yasal kurallara dayanmalıdır ve açık bir biçimde meşru amaçlara hizmet etmelidir; "gerekli" ve ilgili meşru amaçla

"orantılı" olmalıdır (belli bir "takdir payı" dâhilinde); ve bu şartların ihlal edildiği iddiasıyla başvurulabilecek "etkili bir [tercihan yargısal] hukuk yolu" bulunmalıdır.

Ayrım yapmadan "herkes"

İnsan haklarının "herkese", tüm insanlara uygulanması şartı, 1945'ten beri uluslararası insan hakları hukukunun en önemli özelliklerinden biridir: bunlar insan haklarıdır, sadece vatandaş hakları değildir.

Bu nedenle, çok sınırlı istisnalar dışında, tüm devletlerin, insan haklarını etkileyen ya da ona müdahale eden tüm kanunları, yaşanan yer ya da milliyete dayanan ayrımcılıklar da dâhil "hiçbir tür" ayrım yapmadan "herkese" uygulanmalıdır.

İnternetin işleyişinde ABD'nin ve ABD şirketlerinin özel konumu dolayısıyla, ABD'deki anayasal ve kurumsal yasal çerçeveler özel öneme sahiptir. Buna karşın, insan hakları hukukunun yukarıda bahsedilen ilkesine aykırı olarak, ABD Anayasasında ve dijital ortamı ilgilendiren çeşitli ABD yasalarında yer alan pek çok insan hakları güvencesi, sadece ABD vatandaşlarına ve ABD'de yaşayan ABD vatandaşı olmayan kişilere uygulanmaktadır ("ABD kişileri"). İfade özgürlüğü ve örgütlenme özgürlüğünü kapsayan Birinci Anayasa Değişikliği'nden, ABD vatandaşlarını "arama emri olmadan yapılan aramalara" karşı koruyan Dördüncü Anayasa Değişikliği'nden ve millî güvenlik ve istihbarat ile ilgili yasalarca (FISA Değişikliği ve Patriot Yasaları) sağlanan aşırı izlemelerden (sınırlı) korunma haklarının çoğundan sadece "ABD kişileri" yararlanabilmektedir.

"[Sözleşmeye taraf devletin] [toprakları ve] Yetki alanı dâhilinde"

Devletlerin uluslararası insan hakları hukuku altındaki sorumluluklarına sınır ötesi eylemlerinde de uyma görevi

Medeni ve Siyasi Haklara İlişkin Uluslararası Sözleşme (ICCPR) ve Avrupa İnsan Hakları Sözleşmesi (ECHR) de dâhil olmak üzere başlıca uluslararası insan hakları anlaşmaları, devletleri bu anlaşmalarla belirlenmiş insan haklarını "yargı yetkilerine tabi olan herkes için" "sağlamaya" ya da "güvence altına almaya" zorunlu kılar. Bu zorunluluğa, – yakın zamanda İnsan Hakları Komitesi ve Avrupa İnsan Hakları Mahkemesi tarafından yeniden doğrulandığı gibi – giderek daha fazla bölgesel değil, işlevsel bir anlam verilmektedir. Diğer bir deyişle, her bir devlet fiziksel denetimi altında olan ya da hakları kendisinin (ya da kurumlarının) eylemleri tarafından etkilenen herkes için bu hakları sağlama ya da güvence altına almak zorundadır.

Bu da demektir ki devletler, bireylerin insan haklarını etkileyebilecek her işlemlerinde – sınır ötesinde gerçekleşen ya da sınır ötesi tesiri olan eylemlerde bulunduklarında dahi – uluslararası insan hakları yükümlülüklerine uymalıdırlar.

Yaşadıkları yerden, milliyetlerinden ve diğer durumlarından bağımsız olarak, verileri Avrupalı denetleyiciler tarafından işlenen tüm bireyleri koruyan Avrupa veri koruma hukukunun takdir ettiği üzere, yukarıda bahsettiğimiz zorunluluğun –dijital dünyanın yapıtaşı olan– veri için, özellikle de kişisel veri için, özel sonuçları vardır. Fakat ABD, uluslararası insan hakları hukukunun bu şekilde uygulanmasını resmi olarak reddetmektedir. Dijital ortamda ABD'nin (ve bu ülkenin yargı yetkilerine tabi ABD

şirketlerinin) baskınlığı göz önünde bulundurulduğunda bu durum, bu yeni ortamda hukukun egemenliğine ciddi bir tehdit oluşturmaktadır.

Başta ifade özgürlüğü olmak üzere, rakip veya çelişen kanunların çevrimiçi etkinliklere eşzamanlı olarak uygulanmasının zorluğu

Birbiriyle rekabet eden – ve çelişen – farklı ulusal kanunların uygulanması sorunu, internet üzerinde hukukun üstünlüğünü güvence altına almak için acil olarak ele alınması gereken bir konudur.

Burada söz konusu olan, hükümetlerin uluslararası hukuka uygun ve demokratik bir toplumda gerekli ve orantılı tedbirleri alma hakkı değildir. Bu sınırlar dahilinde, hükümetler elbette yetki alanlarına giren düzenlemelerle ilgili kararlar vermekte özgür olmalıdır. Konu, hükümetlerin ya da mahkemelerin, bireylerin kendi yaşadıkları ülkenin kanunlarına uygun davrandıkları halde haklarının üçüncü ülkelerin kanunlarına dayanarak kısıtlanmasına yol açabilecek önlemler alabilme gücü ve hakkıdır. Bireyler, yabancı kanunların aksine, kendi ülkelerinin kanunlarını bilir ya da bilebilir ve bu kanunların nasıl uygulanacağını öngörebilir.

İlke olarak, yaşadıkları ya da kuruldukları ülkeden bilgiyi ulaşılabilir kılan kişi ve kuruluşlar, bu ülkenin kanunlarına uymak zorunda olmalıdır; yabancı web sitelerindeki materyallere, bu materyallerin yaşadıkları ülkede kanun dışı olduğunu bilebilecekken ve de bilmesi gerekirken ulaşan ya da indiren kişilerin ise, yaşadıkları ülkenin kurallarına uyması beklenebilir. Devletlerin uluslararası hukuka göre yasadışı olmayan yabancı materyaller üzerinde yargı yetkisi kullanması, materyaller ya da bunların yayıcısı ile tedbiri alan devlet arasında net ve yakın bir bağlantının bulunması gibi durumlar dışında, prensipte sınırlı kalmalıdır.

İnsan hakları ve özel kuruluşlar

İnsan hakları hukuku ve Ruggie ilkeleri ile Avrupa Konseyi ve diğer rehber ilkeler

Uluslararası insan hakları hukuku temelde yalnızca devletleri ve kamu yetkililerinin eylemlerini (ya da ihmallerini) bağlar. Fakat şimdi şirketler tarafından uygulanması planlanan yeni uluslararası standartlar ortaya çıkmaktadır. Bunların en önemlileri, Birleşmiş Milletler Genel Sekreterinin İş Dünyası ve İnsan Hakları Özel Temsilcisi John Ruggie tarafından tasarlanmış BM *İş Dünyası ve İnsan Hakları Rehber İlkeleri* (Ruggie İlkeleri)'dir. Fakat Ruggie İlkeleri hala ev sahibi devletlerin, şirketlerin yaptığı insan hakları ihlallerine karşı yapması gereken görevlere odaklanmaktadır. Bunun tersi olan durumla, yani devletlerin şirketlerden onların uluslararası insan hakları kanununu ihlal etmesine neden olacak taleplerde bulunması ile ayrıntılı olarak ilgilenmez.

Avrupa Konseyi ve diğer merciler tarafından, hükümetlerin ya da diğer özel kuruluşların uluslararası insan hakları kanununu ihlal edebilecek önlemleri destekleme taleplerini karşılamak durumunda kalan (ya da bu duruma düşme ihtimali olan) şirketlerin sorumlulukları hakkında daha fazla rehberliğin geliştirilmesi önemli görünmektedir.

İnternet ve e-iletişim şirketlerinin, devletlerin talimatıyla – ya da "teşvikine" dayanarak – filtreleme ya da engelleme yapması

İnternetteki materyalleri suç saymanın dışında –ki bu, materyaller başka bir ülkede üretildiğinde geriye dönük olarak, yani materyaller yayınlanıp erişildikten sonra, sıklıkla gerçekleşmekte–, devletlerin çevrimiçi belli materyallere ve bilgiye erişimi engelleme çabaları gittikçe artmaktadır. Bu tür engelleme ya da filtreleme, iletişimleri inceleyip daha önce belirlenmiş ölçütlere dayanarak bu materyalin talepte bulunan alıcıya (genelde interneti gezmekte olan birisine) iletilip iletilmeyeceğine karar veren bir yazılım ya da donanım tarafından gerçekleştirilmektedir.

Bu durumda, baskıcı devletlerin muhalif web sitelerini, ya da dine dayalı rejimlerin, dine hakaret olarak gördükleri web sitelerini engellemeye çalışması bir bakıma şaşırtıcı değildir. Fakat, hukukun egemenliğine saygı gösterdiği kabul edilen devletler de – Avrupa Konseyine üye devletler de dâhil – kabul edilemez buldukları materyallere erişimi her geçen gün daha fazla engellemeye çalışmaktadır. Ya da, daha sinsice ve kendilerini sorumluluktan soyutlayacak şekilde, internetin geçit denetçilerini (internet servis sağlayıcıları ve GSM operatörleri) bu işi açık ve net olan kamu hukuku yasal çerçevesinin dışında, "gönüllü" olarak yapmaya teşvik etmektedirler.

Genellikle, demokratik ülkelerde, engelleme ve filtreleme önlemleri, en azından başlangıçta resmi olarak, ırkçı ya da dinci "nefret söylemi" ya da çocuk pornografisi gibi meşru hedeflere yönelmekteydi. Fakat sistemlerin çalışma yöntemlerinde önemli kusurlar bulunmaktadır:

- engelleme, doğası gereği (kasıt olmaksızın) yanlış pozitifler (yasaklanan materyali içermeyen sitelerin engellenmesi) ve yanlış negatifler (yasaklanan materyali içeren sitelerin filtreye takılmadan geçmeyi başarması) yaratma ihtimali taşır;
- genellikle belli web sitelerini engellerken diğerlerini engellememeye yönelik ölçütler ve engellenmiş web sitelerinin listesi en iyi ihtimalle pek şeffaf değildir, en kötü ihtimalle ise gizlidir;
- neyin engellenip neyin engellenmeyeceği kararının – bilinçli olarak – özel kuruluşlara bırakıldığı durumlar başta olmak üzere, itiraz süreçleri külfetli olabilir, pek bilinmiyor olabilir ya da hiç bulunmayabilir;
- engelleme önlemlerini atlatmak, fazla teknik becerisi olmayan kişiler için bile oldukça kolaydır;
- en önemlisi, çocuk pornografisi ile ilişkisi özelinde, engelleme, asıl sorunun (yani söz konusu çocukların tacizinin) üzerine gitmekte tamamen başarısız kalır.

Yukarıdaki sorunlar, şu gerçekle birleşerek daha da büyümektedir: devletler çocuk pornografisi ve nefret söylemi gibi en ciddi konulara karşı site engellemeye bir kez başladıklarında, bunu hoşlarına gitmeyen başka alanlara doğru genişletme eğilimindedir. Küresel olarak, Avrupa da dâhil olmak üzere, devletler tarafından sadece nefret söylemi ve terörizm savunusu olan siteleri değil, örneğin cinsel haklar ya da azınlık hakları hakkında siyasi tartışmalar ya da bilgilerin bulunduğu siteleri de engellemeye yönelik girişimler olmuştur.

İçeriğin bir yasaya dayanarak engellendiği durumları, hukuki temeli olmayan engellemelerden ayırmak yararlı olacaktır. Engelleme önlemlerine meşru hedef

olan belli içeriklerin bulunduğu tartışılmaz bir gerçektir (yasa dışı içeriğin hukuki olarak engellenmesi). Fakat engelleme önleminin amacı ve onu gerçekleştirmek için kullanılan fiili teknik araçlar, önlemin orantılı ve dolayısıyla hukuki olup olmadığını belirlemedeki önemini hala korumaktadır – örneğin, eğer söz konusu içeriğe tesadüfen erişimin önemli düzeylerde olduğuna dair bir belirti yoksa ve engelleme önleminden sonra kasıtlı erişim hala kolaysa, engellemenin orantılılığı daha tartışmalıdır.

Eğer hangi sitelerin engelleneceği kararı, engelleme hakkında sorumluluğu üzerine almayan devletler tarafından "teşvik edilmiş" özel kuruluşlara bırakıldıysa (içeriğin hukuki temel olmaksızın engellenmesi), konu daha da karmaşık hale gelmektedir. Birleşik Krallık ve İsveç gibi bazı ülkeler, İnternet Servis Sağlayıcıları ile yapılan gönüllü düzenlemelere dayanan engelleme sistemleri başlatmıştır. Bu tip engelleme için, önlemin etkililiğine ya da orantılılığına dair kaygılar hala geçerliliğini korurken, bu durum yanıtlanması gereken daha genel ve temel bir sorunu ortaya çıkarmaktadır: Bu engelleme önlemlerinin ne kadarı gerçekten gönüllü veya devlet ne kadar sorumlu? AİHS (Avrupa İnsan Hakları Sözleşmesi)'nin 10. maddesinin sadece "kamu yetkilileri"nin bu hakka müdahalesinden bahsetmesi, devletleri böyle bir etkisi olan özel kuruluşların aldıkları önlemler karşısında temize çıkarmaz – özellikle de devletin bu önlemleri fiilen şiddetle teşvik ettiği durumlarda. Bu tür durumlarda, devlet bu tür bir sistemi yasama temeline oturtmadığı için sorumlu tutulabilir, çünkü bu tür bir temel olmaksızın kısıtlamaların yasalara dayandığı söylenemez.

Yakın tarihli bir kararında Avrupa İnsan Hakları Mahkemesi rastgele engelleme yapmanın tehlikelerine net olarak dikkat çekmiştir. Yıldırım – Türkiye vakasındaki hükmünde Mahkeme söz konusu önlemin – Atatürk'e saygısızlık olarak görülen bir Google sitesini engellemek için Google Sites tarafından barındırılan tüm web sitelerine Türkiye'den erişimin engellenmesinin – keyfi etkiler doğurduğu ve Google Sites tarafından sunulan tüm sitelerin toptan engellenmesine yol açtığı için, sadece rencide edici web sitesine erişimi engellemeye yönelik olduğunun iddia edilemeyeceğini ifade etmiştir. Dahası, internet sitelerini engellemeye yönelik adli inceleme süreçlerinin, kötüye kullanmayı önleme ile ilgili ölçütleri karşılamakta yetersiz kaldığı görülmüştür, çünkü iç hukuk, belirli bir siteye yönelik engelleme emrinin genel olarak erişimi engelleyecek bir araç olarak kullanılmamasını sağlayacak koruyucu tedbirler sunmamaktaydı. Bu nedenle Mahkeme AİHS'nin 10. maddesinin ihlal edildiğine hükmetmiştir.

Telif haklarının korunması amacıyla, şirketlerin talebi doğrultusunda ve mahkeme emriyle başka şirketlerin uyguladığı rastgele derin paket muayenesi (DPI)

Yukarıda anlatılana benzer şekilde, fikri mülkiyet hakkı sahipleri korsan içerik paylaşımını sağladığı ileri sürülen sitelere karşı uygulamak üzere her geçen gün daha fazla filtre ve engelleme isteğinde bulunmakta ve iddia edilen paylaşımla alakalı olarak internet kullanıcılarının bilgilerine ulaşmayı giderek artan şekilde talep etmektedir. Bunun yöntemlerine internet servis sağlayıcılarının zorunlu DPI kullanımını sağlamak ve bu yolla muhtemel (ya da olası) hak ihlalcilerini saptamak da dâhildir.

DPI, "denetçi"nin sadece "paket"in çıkış ya da varış noktalarına bağlı olarak kapsamlı üstveriyi değil, aynı zamanda bu iletişimlerin içeriğini de incelemesini gerektirmektedir.

"Paketler", belirli bir içerikle ilişkilendirilmiş bir model ya da algoritmaya göre seçilip ayrılmaktadır. Fikri mülkiyet hakkı sahipleri için bu, telif hakkı koruması altındaki belli bir video ya da fotoğraftır. Fakat aynı teknoloji, özünde herhangi bir şeyin aranmasını mümkün kılmaktadır: belli bir siyasi konuşma, belli bir devrimci şarkı, ya da bir sendikanın bayrağı gibi. Bu önlemler, telif hakkı ihlali yapması muhtemel (ya da olası) olan birkaç tanesi saptanmaya çalışılırken bir servis sağlayıcının (ya da cep telefonu ağının) tüm kullanıcılarının gözetlenmesini gerektirdiğinden oldukça tacizkar olup, bu nedenle de ciddi gereklilik ve orantılılık sorunları ortaya çıkarmaktadır.

Hem Avrupa İnsan Hakları Mahkemesi hem de Avrupa Birliği Adalet Divanı'nın kararları, bir İnternet Servis Sağlayıcı'nın (ya da cep telefonu operatörünün) yürüttüğü tüm iletişimlerin masum kullanıcılar kitlesi içindeki olası hak ihlalcilerini saptamak amacıyla rastgele filtrelenmesinin –yani genel izleme ve gözetleme yapılmasının– insan hakları kanununa aykırı olduğunu kuvvetle ima etmektedir.

Devletlerin sınır ötesi yargı yetkisi kullanımları

Yasama ve yürütme güçlerini, kendi fiziksel alanı üzerinde değil de başka bir devletin alanında tutulan veriyi ele geçirme ya da bu veri üzerinde denetim sağlamak için kullanan bir devlet, yargı yetkisini sınır ötesi olarak, başka bir devletin yetki alanında kullanıyor demektir. Bunu genel olarak, bu verileri diğer devlette bulunan sunuculardan çekmek için internetin fiziksel altyapısını ve küresel iletişim sistemlerini kullanarak, ya da yurtdışındaki bu tür veriye erişimi bulunan özel kuruluşları başka bir ülkedeki sunuculardan ya da cihazlardan bu veriyi çekip devlete vermeye zorlayarak yapar.

Genel uluslararası kamu hukukuna göre, yabancı makamlara sınır ötesi icra yetkisi veren anlaşmaların yokluğunda, ilk devletin bunu ikinci devletin rızası olmadan yapması yasal değildir.

Meseleler ve aralarındaki denge

Meseleler

İnternette ve daha geniş dijital dünyada hukuk düzenini kurmak ifade özgürlüğü, tüzel kişiler (özellikle anonim şirketler) ve insan hakları, veri korunması ve siber suçları etkileyen kuralların netleştirilmesini gerektirecektir. Buna bağlı alarak ele alınması gereken soru, bu yeni ortamda tüm bunlar arasındaki dengenin nasıl kurulması gerektiğidir.

İfade özgürlüğü

İnternette ve daha geniş dijital ortamda yapılanlara ilişkin ulusal yasalar, özellikle de ifade özgürlüğüne dair olanlar, çoğu kez aynı anda uygulanmaya çalışılmakta ve çelişmektedir: birçok devletin yasalarına göre kişiler, bir ülke içinde ya da ülkeden çevrimiçi ya da elektronik yazışmalarla gerçekleşen bir ifadede, bu ifade bulunulan ülkede yasaya uygun olsa bile bir başka ülkenin yasalarına aykırıysa, bu ikinci ülkenin yasalarına göre bundan sorumlu tutulabilirler. Bu durum, internetteki ve o ortamdaki hukuk düzenine temelden bir tehdit oluşturur. Bu konu henüz Avrupa İnsan Hakları Mahkemesi'nin içtihadında tam olarak ele alınmamıştır.

Yukarıda belirtildiği gibi, bu konuyu çözmenin tek yolu, devletler ve ulusal mahkemelerin, yurtdışından internet üzerinden dağılan ifade ve bilgiler uluslararası hukuka göre usulsüz olmadığı ya da devletin yargılama yetkisini kullanmasını haklı çıkaran bariz bağlantılar sunmadığı sürece, bu ifade ve bilgilere kendi yerel yasal standartlarını uygulamaktan kaçınacaklarını açık bir şekilde göstermeleri olabilir.

Bir diğer önemli mesele de bir internet sitesi, hatta İSS'ler yöneten birey ya da şirketlerin, internet sitesinde paylaşılan içeriğe dair yükümlülüğüdür. Burada da bugüne dek Avrupa düzeyindeki içtihat sınırlandırılmıştır. Halen özel şirketler açık yükümlülükler (ya içeriği kaldır ya da cezayı göze al) ile açık olmayan yükümlülükler (kullanıcıya yasaya uygun içeriğe erişmeyi garanti etmek) arasında kalmış görünmektedir. Sonuç olarak özel şirketler kurallara gereğinden fazla riayet etmeyi seçip tüm kullanıcıları yasaya gayet uygun olan içeriklere erişmekten alıkoyarken, aynı zamanda bundan etkilenen kullanıcılara geniş yorumlanabilecek hizmet şartları empoze ederek onlardan gelebilecek olası şikayetlerden kendilerini korumaya meyledebilir. Bunlar çözülmesi gereken temel meselelerdir.

Kolluk görevinin özelleştirilmesi

İnternetin ve küresel dijital ortamın büyük ölçüde tüzel kişiler (özellikle de, ama bununla sınırlı olmamakla birlikte ABD şirketleri) tarafından kontrol ediliyor oluşu da hukuk düzenine bir tehdit oluşturmaktadır. Bu gibi özel kuruluşlar, ifade özgürlüğü hakkının devlet tarafından sınırlandırılması için geçerli olan anayasal ya da uluslararası yasal kısıtlamalara tabi olmadan bilgiye erişime sınırlamalar getirebilir ya da getirmeye "teşvik" edilebilirler. Başka özel kuruluşların talebi üzerine yerel mahkemeler bu özel kuruluşlara muhtemel (ya da yalnızca olası) özel mülkiyet hakkı (genelde de fikrî mülkiyet hakkı) ihlallerini saptamak için verileri tacizkar bir biçimde inceleme emri verebilir. Kanun yürütme ya da millî güvenlik sebepleriyle, başka bir ülkenin – ya da bu başka ülkedeki şirketlerin ya da veri sahiplerinin – rızasını almadan, bu diğer ülkenin egemenliğini, şirketlerin hakkı olan ticarî mahremiyeti ve veri sahibinin insan haklarını ihlal edecek şekilde, resmî, ticari ve kişisel veriler dâhil, birtakım verileri başka ülkelerdeki sunuculardan "çekmeleri" emredilebilir.

Birleşmiş Milletler'in Ruggie İlkeleri bu meseleleri ele almanın önemine işaret etse de çözüm sunmamaktadır. Bahsedildiği gibi, bu yüzden yeni yaklaşım ve yönergelere ihtiyaç vardır. Vatandaşlarının insan haklarını özel kuruluşların ihlal etmesini engelleyemeyen devletlerin bundan sorumlu tutulabileceğini ve yine devletlerin, özel kuruluşların uluslararası insan hakları standartlarıyla uyumsuz genel hizmet şartlarının geçersiz sayılmasını sağlama yükümlülüğü olduğunu belirten Avrupa Konseyi, bu tartışmaya önemli katkılar yapmıştır.

Verilerin korunması

Avrupa veri koruma hukuku, Avrupa İnsan Hakları Mahkemesi tarafından geliştirilmiş genel "hukukun üstünlüğü" ilkelerinin özel yansımaları olan bir dizi temel ilke (adil işleme; amaç belirtme ve amaç sınırlaması; veriyi en aza indirme; veri niteliği; ve veri güvenliği) ve bir dizi hak (veriye konu olan kişinin hakları) ve başvuru yolları (bağımsız veri koruma yetkililerince yapılan kontrol) üzerine kuruludur. Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına

İlişkin Sözleşmesi (108 sayılı Sözleşme) ve bu konudaki AB kuralları, özel olarak kişisel verilerin işlenmesi bağlamında insan hakları hukukunun genel şartlarına riayetin nasıl sağlanması gerektiğini belirlemektedir. Avrupa veri koruma modeli giderek artan şekilde Avrupa Konseyi alanının dışında da benimsenmektedir: (halen bir yenilenme sürecinde olan) 108 sayılı Sözleşme, internet ve daha geniş dijital dünya için elzem olan, uluslararası hukuk düzenini bu açıdan güvenceye almada dünya çapında bir "altın standart" haline gelmektedir.

Avrupa'da veri koruma Avrupa Birliği Adalet Divanı'nın, zorunlu, şüpheye dayanmayan ve hedefi belirlenmemiş bir şekilde verilerin saklamasını reddettiği bir kararıyla daha da güçlendirilmiştir. Edward Snowden'in istihbarat ve güvenlik hizmeti uygulamaları hakkındaki ifşaatıyla başlayan tartışmayla bağlantılı olarak, gizli, büyük çaplı ve rastgele izleme programlarının Avrupa insan hakları hukukuyla uyumlu olmadığı ve terörle mücadele ya da millî güvenliğe yönelik başka önemli tehditlerle haklı çıkarılamayacağı giderek daha da belirgin hale gelmektedir. Bu tür müdahaleler ancak kesinlikle gerekliyse ve meşru bir amaçla orantılıysa kabul edilebilir.

Avrupa standartlarına uygun veri koruma, internette ve daha geniş dijital dünyada hukukun üstünlüğüne yönelik ilk ve en önemli temel taşını oluşturmaktadır. Sonuç olarak, 108 sayılı Sözleşme'nin halen sürmekte olan yenilenmesinin (çağa uydurulmasının) standartlarda herhangi bir düşüşe yol açmamasının sağlanması hayatî önem taşıyacaktır. ABD'nin 108 nolu Sözleşme'ye katılımı, yalnızca ABD vatandaşları için değil, temel veri koruma hakkına ve bunun sağladığı haklara riayete dair daha kapsamlı bir küresel yaklaşıma doğru bir hamle olarak özellikle değerli olacaktır.

Bilişim Suçları

Siber Suçlar Sözleşmesi taraf devletlerin ulusal mevzuatlarında –bilgisayar sistemlerine yasadışı erişim (hackleme), elektronik haberleşmelerin yasadışı olarak ele geçirilmesi, kötü amaçlı yazılım gönderilmesi, telif hakkı ihlalleri ve çocuk pornografisinin üretimi ya da dağıtımı gibi– belli eylemleri suç saymasını şart koşar; Ek Protokol'ü de taraf devletlerin, ırkçı ve yabancı düşmanı içeriğin (nefret söyleminin) dağıtımını suç haline getirmesini şart koşar. Ayrıca bu tür suçlarla mücadeleye ilişkin, kanıtların incelenmesi ve korunması, suçluların iadesi ve benzeri konularda karşılıklı hukuki yardım da dâhil olmak üzere uluslararası işbirliğine de kapsamlı biçimde imkan tanır. Sözleşme Avrupa dışındaki devletlere de açıktır ve ABD de dâhil böyle beş devlet tarafından onaylanmıştır.

Küresel dijital ortamdaki suçlara karşı çıkan bir sözleşmenin gerekliliği şüphe götürmez olmakla birlikte – Avrupa Konseyi de böyle bir süreci başlattığı için övgüye değerdir – Sözleşme taraf devletlerin onu uygulayışı açısından hukuk düzenine riayeti temin etmede henüz tamamen donanımlı değildir.

Bunun bir nedeni Sözleşme'nin kapsamlı bir insan hakları hükmü içermemesi, bu yüzden de devletlerin cezaya tabi suçları gereğinden geniş tanımlamasına, mevzuatlarında bu suçlara dair gerekli istisnalar veya savunma ilkelerini dâhil etmemesine (muhbirler için kamu yararı savunması gibi) karşı bir koruma sağlamadığı gibi, çifte yargılamaya veya taraf devletlere (resmî ya da gayriresmî) destek sağlanmasına (bunun insan haklarını ihlal edebileceği durumlarda) karşı da korumamaktadır.

Bir başka sebep de Sözleşme'nin, dijital veya ulusaşırı bağlamlarda hukuk düzenini destekleyen, Avrupa Konseyi tarafından geliştirilmiş diğer başlıca belgelere bağlı olmamasıdır. Sözleşme AİHS'ye taraf olmayan ya da Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin (UMSHS) benzer koşullarını tamamen kabul etmemiş devletlere de (ABD'nin kendi sınır ötesi faaliyetleri ve "ABD'li olmayan kişilerin" hakları açısından yapmış olduğu gibi) açık olduğu için, böyle bir bağlantı daha da gerekli görünmektedir. Avrupa hukuk düzeninin bakış açısından, Siber Suçlar Sözleşmesi'ne katılım hem devletlerin AİHS veya UMSHS gereği olan yükümlülüklerini tamamen kabul etmesini hem de Veri Koruma Sözleşmesi, Suçluların İadesine Dair Avrupa Sözleşmesi ve Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi'ni onaylamasını gerektirmelidir.

Son olarak Sözleşme'nin 26. ve 32. maddeleri emniyet teşkilatının sınır ötesinde bile bilgi toplamada, sarih koruyucu tedbirler belirlemeden "gayriresmî" yollara başvurma eğilimini destekler izlenimi vermektedir (örneğin normalde hukuk düzeniyle yönetilen bir ülkede mahkeme izni gerektirecek tacizkar bilgi toplama faaliyetleri için gayriresmî yöntemlerin uygulanması gibi). Ayrıca bu iki madde bu tür yetkililerin giderek artan biçimde doğrudan başka ülkelerdeki sunuculardan veri "çekme" ya da resmî, devletlerarası karşılıklı adlî yardım anlaşmalarına başvurmadan, muhtemelen verinin bulunduğu devletin egemenliğini ihlal eder şekilde bunu yetki alanlarındaki şirketlerden – özellikle de başlıca internet devlerinden – isteme eğilimini de destekler görünmektedir.

108 no.lu Sözleşme'nin 16. maddesinde belirlenmiş olan kişisel verilerin ulus aşırı faaliyetlerde hangi koşullarda toplanabileceğine veya iletilebileceğine ilişkin açık sınırlamaların olması ilkesi Siber Suçlar Sözleşmesi'ne de ilham vermelidir. Avrupa Konseyi Bakanlar Kurulu'nun bir dizi tavsiye ve tebliği, veri koruma ilkelerini muhafaza etmeyle gerekli hukukî yaptırıma izin verme arasında nasıl bir denge sağlanabileceği konusunda faydalı bir rehber olabilir. Siber Suçlar Sözleşmesi'ne taraf olan üye ülkelerin bu belgelere riayeti güçlendirilmelidir.

Siber Suçlar Sözleşmesi'ne eklenmesi önerilen yeni Ek Protokol'ün tasarlanması bu sorunlardan en azından bazılarını çözme imkanı sunabilir. Bu iyileştirmelerle Siber Suçlar Sözleşmesi internette ve daha geniş dijital dünyada hukukun üstünlüğü için ikinci bir temel taşı olabilir.

Millî güvenlik

Hem Avrupa İnsan Hakları Sözleşmesi hem de Avrupa Konseyi Veri Koruma Sözleşmesi prensipte, taraf devletlerin tüm faaliyetleri için geçerlidir: ikisi de bazı özel kural ve istisnalar içerse de millî güvenlik meseleleri açıkça hariç tutulmamıştır. Bu açıdan Avrupa Konseyi'nin görev ve yetki tanımı ve bu aygıtların kapsamı, millî güvenliği AB görev ve yetki alanının bilhassa dışında tutan AB hukukundan farklıdır. Bunun anlamı şudur: millî güvenlik ve istihbarat kurumlarının faaliyetlerinin uluslararası yasalarla düzenlenmesi söz konusu olduğunda, Avrupa Konseyi, en azından Avrupa'da başrolü üstlenmelidir.

Millî güvenlik ve istihbarat kurumlarının faaliyetlerine istinaden hukukun üstünlüğünü güvenceye alma gerekliliği, özellikle Edward Snowden'in ABD'nin Millî Güvenlik Kurumu (NSA), Birleşik Krallık'ın Devlet Haberleşme Merkezi (GCHQ) ve bunların 5EYES grubundaki ortaklarının (Avustralya, Kanada ve Yeni Zelanda) küresel izleme

işlemleri hakkındaki ifşaatı ışığında bariz hale gelmiştir. Bu ifşaat, bu kurumların düzenli olarak internetin belkemiğini oluşturan yüksek kapasiteli fiber optik kablolara bağlandıklarını, ayrıca dünya çapında devasa bir ölçekte cep telefonu ve diğer haberleşmeleri dinlemekte olduklarını, örneğin başlıca haberleşme sistemlerine kurdukları "arka kapıları" (back door) kullanıp bu tür sistemlerdeki güvenlik zaaflarını istismar ederek telsiz haberleşmelerine girip dinlediklerini göstermiştir.

Avrupa ve uluslararası insan hakları hukukunda millî güvenlik tüm diğer kaygılara baskın çıkan bir koz değildir. Nitekim "millî güvenlik" kavramı kapsamına neyin girmesinin meşru olacağı sorusunun kendisi yargıya tabidir; yani uluslararası insan hakları hukuku ışığında neyin meşru bir şekilde bu terimin kapsamına girdiğini – dolayısıyla neyin girmediğini – belirlemek mahkemelerin işi olmalıdır. 19. Madde (Article 19) adlı bir STK tarafından yazılmış ancak BM Düşünce ve İfade Özgürlüğü Özel Raportörü dâhil olmak üzere çeşitli uluslararası forumlar tarafından desteklenmiş *Millî Güvenlik, İfade Özgürlüğü ve Bilgiye Erişim Üzerine Johannesburg İlkeleri* bu konuda yararlı bir rehber olmuştur. Bu ilkeler, devletlerin insan haklarına müdahale etme sebebi olarak millî güvenliğe, ancak ülkenin bizzat yapısını ve temel kurumlarını tehdit eden konulara ilişkin olarak başvurabileceğini açıklığa kavuşturmaktadır. Bazen terör bu düzeye ulaşabilir ama çoğu durumda millî güvenlik paradigması içinde ele alınmaktansa hukuki yaptırımla başa çıkılması gereken bir olgudur. Bu, devletlerin internete ve e-haberleşmeye dair eylemleri için de geçerlidir.

Millî güvenlik ve istihbarat kurumlarının eylemlerine ve bunların arasındaki işbirliği ve bilgi alışverişine hukuki temel oluşturabilecek açık uluslararası anlaşmalar yoktur. Birçok ülkede bu kuruluşların çalışmalarını düzenleyen açık ve yayınlanmış mevzuat çok sınırlıdır. Bazılarında yayınlanmış hiçbir kural dahi yoktur. Bu kurum ve hizmet birimlerinin – yurtiçinde, sınır ötesinde ya da birbirleriyle işbirliği içinde – hangi kurallara göre çalıştığı bilinene dek faaliyetlerinin hukuk düzeniyle uyumlu olduğu söylenemez. Ciddi endişe kaynağı bir başka husus da birçok kontrol sisteminin açıkça etkisiz kalıyor olmasıdır.

Bir başka deyişle, her ne kadar evrensel insan hakları yapısının böylesi elzem bir parçasının temelini oluşturabilecek temel ilkeler mevcut olsa da, millî güvenlik açısından şu ana dek hukukun üstünlüğünü korumaya yönelik bir temel taşı bulunmamaktadır.

Emniyet teşkilatıyla istihbarat ve güvenlik kuruluşları arasındaki ortaklığın gittikçe arttığı göz önüne alındığında, hukukun üstünlüğünü düzeninin bu şekilde reddi, istihbarat ve güvenlik kuruluşlarından polis memurları ve savcılara sıçrama tehlikesi içermektedir. Bu konuda ulusal ve uluslararası düzeyde açık hukuki çerçevelerin yokluğu da internette ve küresel dijital ortamda hukukun üstünlüğüne yönelik bir tehdit oluşturmaktadır.

Komiser'in tavsiyeleri

Komiser bu tematik belgenin bulgularını ve sonuçlarını dikkate alarak, internette ve daha geniş dijital ortamda hukuk düzenine saygıyı geliştirme amacıyla aşağıdaki tavsiyelerde bulunmaktadır.

I. İnsan haklarının evrenselliğiyle çevrimiçi ve çevrimdışında eşit uygulanmaları üzerine

1. Hukukun üstünlüğünün temel gerekleri hem çevrimiçi hem de çevrimdışı ortamda eşit olarak geçerlidir ve uygulamada da öyle olması sağlanmalıdır. Bu özellikle şu anlama gelir:

- Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Avrupa Konseyi veri koruma kurallarının tümü bütün Avrupa Konseyi üye devletlerinin tüm kişisel veri işleme etkinlikleri için geçerlidir; üye devletlerin millî güvenlik ve istihbarat kurumları da buna dâhildir;
- interneti ve daha geniş dijital dünyayı denetleyen özel sektör özneleriyle yapılan özel amaçlı düzenlemelerle, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi (özel ve aile yaşamına saygı hakkı) ve 10. maddesi (ifade özgürlüğü) de dâhil olmak üzere, hukuk düzeni yükümlülüklerinden kaçınılamaz;
- Avrupa Konseyi üyesi devletler, Avrupa dışındaki devletlerin interneti kullanan ya da daha geniş dijital ortamda aktif olan bireyleri etkileyen her eylemlerinde uluslararası insan hakları yükümlülüklerine aynı şekilde uymalarını sağlamak için çaba göstermelidir; ve
- hiçbir devlet (ve emniyet teşkilatı, millî güvenlik ve istihbarat kurumları dâhil olmak üzere devlet organlarının hiçbiri), Avrupa ülkesi olsun ya da olmasın, başka bir ülkenin ya da ülkelerin açıkça ifade edilmiş rızası olmadan başka bir ülkede depolanmakta olan – ya da internetten ve elektronik iletişimlerin "belkemiği" kabloları aracılığıyla ülkeden ülkeye geçen – verilere erişememelidir. Bunun tek istisnası, böyle bir erişimin uluslararası hukukta açık, kesin ve sınırları belirlenmiş bir hukuki temelinin olduğu ve erişimin uluslararası veri koruma ve insan hakları standartlarıyla uyumlu olduğu durumlar olabilir.

II. Veri koruma üzerine

2. Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin Sözleşmesini (108 sayılı Sözleşme) henüz kabul etmemiş olan üye devletler bunu yapmalıdır. Bu sözleşme ayrıca üye olmayan devletlere de açıktır ve eğer geniş olarak benimsenirse, internet ve onu içine alan dijital ortamda hukukun üstünlüğünün en önemli temel taşı olabilir.

3. Bu sözleşmeyi kabul etmiş olan üye devletler, onun ulusal seviyede bütünüyle uygulanmasını sağlamalıdır.

4. Hali hazırda devam etmekte olan 108 sayılı Sözleşme'nin yenilenmesi süreci, Avrupa ya da küresel veri koruma standartlarında herhangi bir düşüşe yol açmamalıdır. Tam tersine, kuralların, özellikle de Internet ve onu da içine alan geniş dijital dünya ile ve millî güvenlik ve istihbarat amacıyla izlemeler ile bağlantılı olarak,daha net hale gelmesini ve daha iyi uygulanmasını sağlamalıdır;.

5. AB veri koruma kurallarının şu anda devam etmekte olan reformu bağlamında, hukukun üstünlüğünü olumsuz etkileyebilecek mevcut kurallar, örneğin rızayla, fişlemeyle ve yabancı emniyet güçlerinin kişisel veriye erişimiyle ilgili olanlar, netleştirilmeli ve 108 sayılı Sözleşme dahil olmak üzere uluslararası insan hakları yükümlülüklerine ve Avrupa Konseyi'nin ilgili tavsiyeleri ve rehber ilkelerine uyumlu hale getirilmelidir.

6. Şüpheye dayanmayan iletişim verilerinin toptan saklanması temel olarak hukukun üstünlüğüne aykırıdır, veri koruma prensiplerinin özü ile uyumsuzdur ve etkisizdir. Üye devletler buna başvurmamalı ya da verinin üçüncü kişiler tarafından zorunlu olarak saklanmasını dayatmamalıdır.

III. Bilişim suçları üzerine

7. Avrupa Konseyi Bilişim Suçları Sözleşmesi'ne taraf devletler, Sözleşme altında yaptıkları (ya da yapmaktan imtina ettikleri) her şeyde uluslararası insan hakları yükümlülüklerine uymalıdırlar; buna herhangi bir suç soruşturmasında ya da kovuşturmada ilgili suçların (ve onlarla alakalı unsurların, istisnaların ve savunmaların) tanımlanması, ve karşılıklı hukuki yardımlaşma ve suçluların iadesi de dahildir.

8. Eğer herhangi bir taraf devlet kendi sınırları dışındaki bireyleri etkileyecek eylemlerde bulunursa, bu o tarafı Bilişim Suçları Sözleşmesi altındaki ya da uluslararası insan hakları anlaşmaları (özellikle AİHS ve UMSHS) altındaki yükümlülüklerinden muaf tutmaz; tam tersine, bu yükümlülükler bu tür sınır ötesi eylemleri de eşit derecede bağlar.

9. Bilişim Suçları Sözleşmesine tüm taraf devletler aynı zamanda Veri Koruma Sözleşmesi, Suçluların İadesine Dair Avrupa Sözleşmesi ve Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesini de onaylamalı ve titizlikle uygulamalıdır.

10. Üye devletler, emniyet teşkilatları da dâhil olmak üzere, Avrupa Konseyi Bakanlar Komitesi'nin polis sektöründe kişisel verinin kullanımını düzenleyen R (1987) 15 sayhılı Tavsiye Kararı'nı, kişilerin fişlenmesi bağlamında kişisel verilerin otomatik işlemden geçirilme sürecinde bireylerin korunması ile ilgili Rec(2010)13 sayılı Tavsiye Kararı'nıve

2013 tarihli Temel Haklara Yönelik Dijital İzleme ve Diğer Gözetim Teknolojilerinden Kaynaklanan Tehlikeler Üzerine Bildirgesi'ni uygulamalıdır.

11. Üye devletler, emniyet teşkilatlarının başka bir ülkede yer alan sunuculardan ve altyapıdan resmi olmayan düzenlemeler altında veri elde etmemelerini, Bunun yerine Bilişim Suçları Sözleşmesi tarafından yaratılmış olan karşılıklı adli yardım düzenlemelerini ve kolaylaştırılmış veri muhafazası için özel düzenlemeleri kullanmalarını sağlamalıdır. Bir ülkedeki emniyet kurumları, başka bir ülkedeki internet servis sağlayıcıları, sosyal ağlar ve cep telefonu operatörleri gibi özel kuruluşların, müşterilerinin verilerini genel hizmet şartları altında açığa vurma yetkisini elde etmiş olmalarına bel bağlamamalıdır.

IV. Yargı yetkisi üzerine

12. Ulusal yargı yetkisinin ulusaşırı bilişim suçları ile ilgili sınır ötesi uygulamasında sınırlar olmalıdır. Bu sınırlar tanımlanırken, bireyin kendi ülkesinde (ya da bu fiillerin işlendiği ülkede) suçlara dair aslî sınırlamalar, istisnalar ya da savunmalar tanınıyorsa, bunlar bu tür sınırları, istisnaları ya da savunmaları kabul etmeyen diğer devletler tarafından hak iddia edilen yargı yetkisinin kullanımında da hesaba katılmalıdır.

13. Özelde ifade özgürlüğü hakkı bağlamında, yaşadıkları ya da kuruldukları ülkeden bilgiyi erişilir kılan bireyler ve şirketler, prensip olarak sadece o ülkenin kanunlarına uymak zorunda olmalı; aynı zamanda bu materyallere (onların kendi yaşadıkları ülkede yasadışı olduğunu bilebilecekken ve bilmeleri gerekirken) yabancı web sitelerinden ulaşan ya da onları indiren bireylerin ise, bulundukları ülkenin kanunlarına uymaları beklenmelidir. Uluslararası hukuka göre yasadışı olan içerik dışında, devletler yabancı dijital materyaller üzerinde sadece sınırlı durumlarda, özellikle materyal veya yayıcısı ile sözkonusu ülke arasında net ve yakın bir ilişki olduğu durumda, yargı yetkisi kullanmalıdır.

V. İnsan hakları ve tüzel kişiler üzerine

14. Üye ülkeler, devletin insan hakları yükümlülüklerini ihlal eden kısıtlamalar getirmek için, interneti ve daha geniş dijital ortamı kontrol eden özel şirketlere bel bağlamaktan vazgeçmelidir. Dolayısıyla özel şirketlerin, insan haklarını ihlal eden fiil ya da ihmallerinin devlete sorumluluk yüklediği durumlar hakkında daha fazla kılavuzluk gereklidir. Buna, devletin ihlale katılımı hangi düzeyi aştığında sorumluluğunun devreye gireceği ve devletin, özel şirketlerin genel hizmet şartlarının insan hakları standartlarıyla ihtilaf içinde olmamasını sağlama yükümlülüğü hakkında kılavuzluk da dâhildir. Devletin doğrudan katılımı olmadan gerçekleşen, tüzel kişilerin ticari amaçlı uygulamalarına ilişkin devletin sorumlulukları da incelenmelidir.

15. BM İş Dünyası ve İnsan Hakları Rehber İlkeleri'ni (Ruggie İlkeleri) geliştirerek ticari işletmelerin, interneti veya daha geniş dijital ortamı etkileyen faaliyetlerine dair sorumlulukları üzerine, özellikle de şirketlerin, hükümetlerden gelen, uluslararası insan hakları hukukunu çiğneyen isteklerle karşı karşıya kalabilecekleri veya böyle isteklerin muhtemel olduğu durumları kapsayacak şekilde daha fazla rehberlik geliştirilmelidir.

VI. Engelleme ve filtreleme üzerine

16. Üye devletler internet içeriğine erişim üzerindeki, kendi yetki alanlarındaki kullanıcıları etkileyen her türlü kısıtlamanın, bu tür tüm kısıtlamaların kapsamını düzenleyen ve olası istismarları önleyici adli gözetimi garanti eden, sıkı ve öngörülebilir bir yasal çerçeveye dayalı olmasını temin etmelidir. Buna ek olarak, yerel mahkemeler herhangi bir engelleme önleminin gerekli, etkili ve orantılı olup olmadığını, ve özellikle de sadece engellemeyi gerektiren spesifik içeriği etkileyecek şekilde yeterince hedeflenmiş olup olmadığını incelemelidir.

17. Üye devletler yukarıda tanımlanmış ölçütlere uygun bir çerçeve dışında engellemede bulunmakla ilgili olarak, interneti ve daha geniş dijital ortamı kontrol eden özel sektör tüzel kişilerine bel bağlamamalı veya onları teşvik etmemelidir.

VII. Millî güvenlik faaliyetleri üzerine

18. AİHS ve 108 sayılı Sözleşme, bu sözleşmelere taraf olan devletlerin, millî güvenlik ve istihbarat faaliyetleri de dâhil tüm faaliyetlerine uygulanmalıdır.

19. Spesifik olarak, internet ve daha geniş dijital ortamda hukuk düzenine riayeti sağlamak için:

- devletlerin insan haklarına müdahalelerini millî güvenliğe dayandırmasına, ancak ülkenin bizzat yapısına ve temel kurumlarına yönelik tehditler söz konusu olduğunda izin verilmelidir;
- millî güvenliğe tehdit iddiası üzerinden temel haklara müdahalede bulunmak isteyen devletler bu tehdidin ceza ve ceza muhakemesi ile ilgili uluslararası standartlarla uyumlu olağan ceza hukuku yoluyla önlenemeyeceğini ispat edebilmelidir;
- yukarıdaki ifade devletlerin internete ve elektronik haberleşmeye ilişkin eylemleri için de geçerlidir.

20. Üye devletler millî güvenlik ve istihbarat kurumlarının faaliyetlerini, kapsayıcı bir yasal çerçeve dâhiline çekmelidir. Bu kurumların ve hizmet birimlerinin – yurtiçinde, sınır ötesinde ya da birbirleriyle işbirliği içinde – hangi kurallara göre çalıştığı konusunda şeffaflık sağlanana kadar faaliyetlerinin hukukun üstünlüğüyle uyumlu olduğu varsayılamaz.

21. Üye devletler aynı zamanda millî güvenlik hizmetleri üzerinde etkin demokratik gözetimin yürürlükte olmasını temin etmelidir. Etkin demokratik gözetim için, özellikle de güvenlik hizmeti memurları arasında, insan haklarına ve hukuk düzenine riayet kültürü teşvik edilmelidir.

Günümüzde internet ve daha geniş kapsamlı dijital ortamlar, insan haklarımızın önemli bir bölümünü kullandığımız araçlardır. Ancak aynı araçlar insan haklarımızın ihlal edilmesine yol açacak şekilde de kullanılabilmektedir.

Çevrimiçi ortamda insan haklarının kullanımının çevrimdışı ortamdakiyle aynı düzeyde olması gerektiği konusunda genel bir görüş birliği vardır. Ancak uygulamada bunun gerçekleşmesini sağlayacak aktörler bu iki ortamda tam olarak birbirine karşılık gelmemektedir. Bu bağlamda dikkate değer bir konu, bazı devletlerin ve özel şirketlerin internet ve internetin fiziki altyapısı üzerindeki orantısız etkisi ve kontrolüdür.

Bu tematik belgede, söz konusu özel yönetişim konularının belirleyici olduğu bu ortamda hukukun üstünlüğünün nasıl sağlanabileceği ele alınmaktadır. Bu yapılırken özellikle insan hakları açısından önem taşıyan bazı politika alanlarına odaklanılmıştır. Bu alanlar ifade özgürlüğü, veri koruma ve özel hayatın gizliliğinden siber suçlar ve ulusal güvenliğe kadar uzanmaktadır. Belgede hukukun üstünlüğünün internetteki faaliyetlerimize uygulanmasını teminat altına almak için atılabilecek olası adımlar önerilmektedir.

www.commissioner.coe.int

PREMS 176414 TUR

TUR

www.coe.int

Avrupa Konseyi Kıta'nın öncü insan hakları örgütüdür. 28'i Avrupa Birliği üyesi olmak üzere, toplam 47 üyesi vardır.
Tüm Avrupa Konseyi üyesi devletler, insan hakları, demokrasi ve hukuk devletini korumak için hazırlanan bir anlaşma olan, Avrupa İnsan Hakları Sözleşmesi'ni imzalamıştır.
Avrupa İnsan Hakları Mahkemesi Sözleşme'nin üye devletlerde uygulanmasını denetler.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE