ISophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi
ISophos: International Journal of Information, Technology and Philosophy

ISSN: 2651-463X *Yıl/Year: 2020 • Cilt/Vol: 3 • Sayı/Num: 5 • Güz/Autumn* **Çeviri Makale**

Gözetim ve Sansür: Teknolojinin İnsan Hakları Üzerine Etkisi*

Avrupa Parlamentosu

Çeviren: Mehmet Özoğul

*Bu eser, "European Union, European Parliament, Directorate – General for External Policies, Policy Department (2015, 16 April). Surveillance and censorship: The impact of technologies on human rights (Study). ISBN(pdf): 978-92-823-7024-7, doi(pdf): 10.2861/035360" adlı İngilizce belgenin "kısmi" çevirisidir.

Atıf/Citiation
Çev. Özoğul, M. (2020). Gözetim ve Sansür: Teknolojinin İnsan Hakları Üzerine Etkisi. ISophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi, Cilt: Cilt 3, Sayı 5, ss: 81-106.

Özet

İnsan hayatı çevrim içi dünyaya geçiş yaptığı gibi insan hakları da bu geçişi devam ettirmelidir. Avrupa Birliği ve diğer aktörlerin önündeki en büyük mücadele ise insan haklarına ait bütün yasaları dünyanın her bir noktasına yaymaktır. Bu rapor ise özünde güvenlik üzerine odaklanarak insan hakları temelli ve insana dair yaklaşımın ülke bazında yapılan güvenlik uygulamalarından daha iyi olacağını tartışır. Bu rapor aynı zamanda dijital çağda insan hakları üzerine sorun yaratan ülkeler ve şirketler hakkında genel bir değerlendirme ortaya koyar. Ayrıca insan haklarına ait çeşitli en bilinen uluslararası hukuk yasalarının ve standartlarının, teknik standartların, iş dünyasına ait yönlendirici ilkelerin, internet prensiplerinin ve politik anlamda girişimlerin listesini tutar ve bu listenin dijital çağdaki insan haklarını rejimi için dönüştürülmesinin son derece hayati olduğunu ortaya koyar. Bu rapor aynı zamanda internet ve insan hakları sorunu üzerine Avrupa Birliği tarafından yakın dönemde alınmış kararların etkilerini analiz eder. Bu rapor, teknolojinin insan hakları üzerine olumlu anlamda etkisini garanti altına almak için Avrupa Birliği içindeki insan hakları ve dijital politikalar üzerine çalışma yapan organların daha iyi bir şekilde birbirine entegre olması ve koordineli çalışmalıdır sonucuna varmaktadır. Aynı zamanda Avrupa Birliği kendi dijital stratejileri haricinde, dijital hakların üçüncü dünya ülkelerinin ulusal yasalarına girmesi için bunları teşvik etmelidir.

İdari Özet

İnsan hayatı çevrim içi dünyaya geçiş yaptığı gibi insan hakları da bu geçişi devam ettirmelidir. Avrupa Birliği ve diğer aktörlerin önündeki en büyük mücadele ise insan haklarına ait bütün yasaları dünyanın her bir noktasına yaymaktır.

Geçmiş yıllarda birçok hükümet teknolojik kapasitelerini sansür ve gözetimi rahat uygulamak için daha gelişmiş dijital araçlar ile güçlendirdiler ve geliştirdiler. Araştırmanın ikinci bölümünde dijital çağda insan haklarını ihlal eden hükümetler ve şirketler hakkında sonuçlar yer almaktadır. Genel anlamda bu bölüm ifade özgürlüğü ve özel yaşam üzerine yoğunlaşsa da aynı zamanda saldırgan uygulamalar ile geniş kapsamlı insan hakları arasındaki bağlantıyı göstermeye çalışır.

Araştırmanın üçüncü bölümü dijital çağda insan hakları rejiminin tam olarak dönüştürülüp uygulanabilmesi için hayati

olan ve Birleşmiş Milletler, Avrupa Konseyi gibi hükümet parlamentolarından daha üstün kurumlar tarafından geliştirilmiş yasalara ve standartlara dair bir genel bir bakış ortaya koyar. Bu bölüm aynı zamanda sıklıkla uluslararası aktivistler tarafından geliştirilen teknik standartları, iş dünyasına ait yönlendirici ilkeleri ve internet prensiplerini içerir.

Araştırmanın dördüncü bölümünde, dijital hakları korumak ve yaymak için potansiyele sahip olan çeşitli uluslararası politik girişimler irdelendi. Bu bölüm aynı zamanda ihracat kontrolü için ayarlanmış Wassenaar Antlaşmasını, WSIS Gelişimini, Özgür İnternet Koalisyonunu, teknik anlamda egemenlik tedbirlerini, ülke sınırları dışında insan hakları ve kriptolama gibi teknik çözümlere karşı yapılan uygulamaları içermektedir.

Avrupa Birliği var olan insan hakları esaslarını teknolojik gelişmelere adapte ederken sıklıkla aktif ve lider rolünü üstlenmektedir. Araştırmanın beşinci bölümü geçmiş yıllarda Avrupa Birliği tarafından internet ve insan hakları sorunu ile bağlantılı olarak dış politika ve dijital stratejiler bağlamında alınmış kararları irdelemektedir. Avrupa Birliği içindeki insan hakları ve dijital politikalar üzerine çalışma yapan organlar hedeflerine ulaşmak için daha iyi bir şekilde birbirine entegre olmalı ve koordineli çalışmalıdır.

Araştırmanın sonuç bölümünde Avrupa Birliği'nin dijital çağda insan haklarının teşvik edilmesi ve korunması için atması gereken adımlar irdelenmektedir. Avrupa Birliği kendi dijital stratejileri ve dış politikaları haricinde, dijital hakların üçüncü dünya ülkelerinin ulusal yasalarına girmesi için onları teşvik etmelidir. İnsan haklarına yönelik anlatımlar bu hedefe ulaşmaya yardımcı olabilir. Avrupa Birliği aynı zamanda teknoloji ve insan haklarına yönelik yapılan bağımsız araştırmaların yanında özel sektör ve hükümetlerin alması gereken sorumluluklarını ve sağlaması gereken şeffaflıklarını desteklemelidir.

1. Dijital Çağa Geçiş: İnsan Hakları ve Teknoloji

İnsan hayatı çevrim içi dünyaya geçiş yaptığı gibi insan hakları da bu geçişi devam ettirmelidir. Dijitalleşme çağının bu derece hızlanmasından önce insan hakları geliştirilirken temel hedefleri bireysel hakları aynı şekilde koruma altına almaktır. İnsan haklarını güvence altına almak ve teşvik etmek amacıyla devletlerin teminatı, bizim anlayışımız, sistem, farklı aktörlerin rolleri ve araçları tekrar rafine edilmeye, belirginleştirmeye ve güncellenmeye ihtiyaç duymaktadır. Bu araştırma temel olarak dijital çağda insan haklarının daha iyi anlaşılmasına katkı sağlamayı amaçlamaktadır.

Bu anlamda anahtar kelime değişimdir. İnsan haklarını koruma çalışmaları efektif bir şekilde dijital çağa geçirilmelidir. Ancak bu şekilde "insanların çevrim içi olduğu zamanlardaki insan hakları çevrim dışı oldukları durumdaki haklar ile aynıdır" sözü gerçek anlamda bir değer ifade eder. Enformasyon ve iletişim ağlarının geliştirilmesi sadece ekonomik, politik ve sosyal hayatı değiştirmemiştir, bu gelişim aynı zamanda yerküre üzerinden yaşayan her bir bireyin hayatını da değiştirmiştir. Beğenelim ya da beğenmeyelim bizim hayatlarımız geri döndürülmez bir şekilde bu değişim tarafından etkilenmiştir.

Çoğu durumda teknolojinin getirdiği olanaklar sayesinde birey, insan haklarını daha iyi kullanabilir hale gelmiştir. Bunun en büyük etkisini ise ifade özgürlüğü alanında görüyoruz. Teknolojinin kapsayıcı yeni formu sayesinde bireyler özgürlüklerini daha rahat kullanabilir hale gelmiş; "bilgiyi aramaya, almaya, yaymaya ve bunu ister sözlü ister basılı isterse herhangi bir ölçüde yaymaya vakıf olmuşlardır." İnsanlar bu teknolojik gelişim sayesinde enformasyonu yayma konusunda güçlenmişlerdir.

Enformasyon teknolojileri aynı zamanda insanları beklenmedik şekilde etkileşime sokarak iletişim modelini değiştirmiş ve değiştirmeye de devam etmektedir. Öyle ki bu gelişimlerden bazıları bize o kadar doğal gelmektedir ve teknoloji sayesinde sanki hep varmış gibi hissedilmektedir. Dünyanın çeşitli bölgelerinde yaşayan milyonlarca mülteci aileleriyle bağlantıda kalmak ve kazançlarını göndermek için eski nesil mektup göndermek yerine çeşitli çevrim içi araçlardan yardım almaktadır. Teknoloji aynı zamanda farklı yaşamsal kimliklere sahip insanların kimliklerini tanıtmak için onlara ~~da~~ güç vermekte, azınlıkların sesini duyurmasına yardımcı olmaktadır.

Teknoloji ön yargılı fakat kararsızdır (Feenberg, 1999; McCarthy, 2011); Teknoloji, nasıl kullanıldığına ve hangi etkilere sahip olduğuna dair çok fazla dikkate sahip değildir. Oysa bu önyargıların insan yaşamına ve onun ekonomik, politik, sosyal gelişimine dair sonuçları eğer insan hakları çevrim içi dünyada tam anlamıyla korunacaksa üzerinde durmaya ve ayrıntıya inmeye ihtiyaç duyar.

Çoğu durumda teknolojinin kullanımı aynı zamanda bireye ait insan haklarını yeni risklere açık hale getirir. İfade özgürlüğünün ürünü olan içeriklerin bu günlerde hükümet organları tarafından sıklıkla sansürlenmesi insan haklarının dijital çağda dönüşümünü ciddi şekilde görünür hale getirmektedir. Fakat bunun yanında verilen enformasyonu işleyen algoritmayı yaratan şirketler de bunun yanında ifade özgürlüğüne müdahale edebilirler. Bu yaratılan algoritmalar ve insan hakları standartları arasındaki dengeyi sağlamak önümüzdeki yıllarda karşımıza çıkacak mücadelelerden sadece biri olacak.

Geçtiğimiz yıllarda dijital çağda gizlilik hakkının ise özel datalara üçüncü taraf şirketlerce, hükümetlerce ve suçlularca kolayca erişilebilmesi olarak belirtilmesi ciddi şekilde dikkat çekmiştir. Özellikle Edward Snowden tarafından devlet gözetimine ve klasörlemesine dair ortaya çıkartılan deliller ve aynı zamanda büyük çok uluslu şirketlerce toplanan kişisel veriler, bu konu hakkındaki toplumun farkındalığını arttırmış ve birçok aktörü, gizlilik hakkının dijital çağa aktarılması üzerine çalışmaya motive etmiştir.

Bununla birlikte, insan haklarının çevrim içi alana taşınması ile alakalı sadece ifade özgürlüğü hakkı ve gizlilik hakkı olduğu düşünülemez. Özellikle fiziksel dünyada görülen haklar aynı zamanda çevrim içi dünyada da görülmelidir. Bunun için insan hakları analiz edilmeye ve geçici etkileri belirlenmeye ihtiyaç duymaktadır.

"Suçluluğu kanıtlana kadar herkes masumdur" diye adlandırabileceğimiz masumiyet karinesi, özellikle gözetim sağlamak amacı ile herhangi bir ön şüpheye dair delil olmadan toparlanan ve toparlanmaya devam eden devasa veriler ile çevrim içi alanda çarpışma içine girmektedir (Bauman et al., 2014). Eldeki güçlü bulgular eşliğinde ise özellikle anti-terör yasaları çerçevesinde masumiyet karinesi ortadan kaldırılabilir (Korff, 2014). İstanbul'daki Gezi Parkı protestoları ve Hong Kong'daki Şemsiye Devrimini dikkate aldığımızda Twitter, Facebook gibi dijital iletişim araçlarının bu eylemleri organize etmek için kullanımı bir kanıttır. Çünkü bu hükümetler kullanılan araçları engelleyerek ve internet hizmetini sekteye uğratarak protestocu insanların bir araya toparlanmalarını ve koordine olmalarını engellemeye ve durdurmaya çalışmışlardır. Bu durumda açık bir şekilde görülmektedir ki barışçıl toplanma ve örgütlenme hakkı dijital çağ içinde değerlendirilmelidir. Aynı şey ekonomik haklar ve sosyal hakların yanında ayrımcılıktan korunma içinde söylenebilir. Bu haklar özellikle dijital çağın artan ivmesinden ciddi derecede etkilenmektedir. Bu konuyu araştırmanın ikinci bölümünde daha detaylı ele alacağız.

Bu durumla aynı zamanda internet üzerinde ulusal güvenlik adına oluşan kaygılar siber güvenlik önlemlerini özellikle çevrim içi terörizm ile savaşmak boyutunda ciddi şekilde ileriye doğru itmiştir. Aynı zamanda Birleşik Devletler kendi ekonomilerine ve ulusal güvenliklerine dair en büyük tehlikenin "siber ataklar" olduğunu deklare etmiştir ve bu yükselen trend yakın zamanda değişecek gibi de gözükmüyor (Arce, 2015). Siber güvenlik yanlıları ve destekçileri ise ana amaç olarak güvenlik ölçeğini ele alma eğiliminde olup insan haklarına çok sınırlı bir bakış açısı ile bakma taraftarıdırlar. Örnek vermek gerekirse siber güvenlik yanlıları, odaklarını özel güvenlik güçlerini üzerine yoğunlaştırmakta ve var olan ilişkilendirilmiş yasal çerçevenin dışında alan tanımaktadır (Deibert, 2003; Tikk, 2010). Bu yaklaşım belki de siber saldırılara karşı ani ve hızlı bir reaksiyon olarak algılanabilir fakat aynı zamanda var olan anayasal korumaların azaltılması ve oluşan siber güvenlik politikası ile devlet kontrolünü sınırlandırmaktadır.

Sonuç olarak, Avrupa Birliğinin önündeki ana mücadele kendi üye ülkeleri ve dünyanın diğer bölgelerinde yer alan ülkelerin çevrim içi içerikteki insan hakları tanımını düzeltmesini sağlamaktır. Buna ek olarak bugün elimizde var olan insan haklarına ait yasal

düzenlemeler teknolojik gelişimin olası negatif etkileri öngörülerek tekrar bir geliştirmeye ihtiyaç duymaktadır. Avrupa Birliği önemli bir uluslararası aktör olarak ve uzun dönemli insan haklarına bağlı bir topluluk olarak, var olan insan haklarına ait prensiplerin teknoloji alanına uyarlanmasında son derece aktif ve lider bir yol oynayabilir ve oynuyor.

Avrupa Birliği'nin atması gereken bir diğer adım ise insan haklarının kendi iç ve dış politikaları ile bağlantılı olarak dijital çağa aktarılmasını desteklemek ve bundan emin olmaktır. Dijital çağ üzerinde uygulanan güç egemen devletlerin bölgesel yargıları üzerinde olduğu sürece Avrupa Birliği ve diğer aktörlerin etkisi sınırlandırılmış olacaktır. Bu nedenden ötürü birlikte karar alma ve ağ bağlantılı yaklaşımlar insan haklarının dijital çağa aktarılmasından ve korunmasında hayatidir. Özellikle çok uluslu şirketler ve teknik organizasyonların çok uzaklara bile etki gücüne sahip olması, uyguladığı politikalar ile daha da değer kazanmıştır. Aynı zamanda bu bağlam iç ve dış Avrupa Birliği politikaları ile bir uyum, ahenk içerisinde olmayı sağlamalıdır. Çünkü ancak bu sayede tüm Avrupa Birliği ülkeleri eşit ve uyum içinde çalışabilir ve üçüncü dünya ülkeleri tarafından üzerinde yapılan eleştirileri bertaraf edebilir.

Mevcut durumda, yapılan toplum münazaralarında askeri tabanlı siber güvenlik bağlamındaki düşünceler güç kazanıyor ve toplumun ilgisi çekiyor (Gilmor in LaFrance, 2015). İlgimizi ve dikkatimizi siber güvenlik konusunda insani bir yöne çekebilirsek bu dijital çağın küresel doğası için bir cevap içermiş olacak. Yapılan münazaralar sınırlar hakkında değil bireysel haklar üzerinde olmalıdır.

2. Dijital Çağda İnsan Hakları Üzerine Riskler ve Tehlikeler

Dünyanın çevresindeki birçok ülkede birey interneti ve diğer teknolojik gelişmeleri kullanımı ile bağlantılı olarak insan hakları ihlali riski ile yaşamaktadır. Aynı zamanda bu ihlaller sıklıkla insan haklarının çevrim içine uygulanması ile öğrenilmiştir.

Sınırsız gazeteciler örgütü tarafından bir araya getirilmiş olan "internete düşman ülkeler" listesi analize başlamak için kullanılabilecek bir örnek olarak ele alınabilir.[1] Bu liste, Bahreyn, Çin, Küba, Etiyopya, Hindistan, İran, Kuzey Kore, Pakistan, Rusya, Suudi Arabistan, Sudan, Suriye, Türkmenistan, Birleşik Krallık, Birleşik Arap Emirlikleri, Amerika Birleşik Devletleri, Özbekistan ve Vietnam'ı içermektedir.

Bu liste temel olarak odak noktasına ifade özgürlüğünü ve gizlilik hakkını almıştır, bunun nedeni ise bu hak ihlallerinin diğer hak ihlalleri yanında kolay bir biçimde dokümanlaştırılabilmesidir. Fakat bu araştırma aynı zamanda saldırgan uygulamalar ile geniş kapsamlı insan hakları arasındaki bağlantıyı göstermeye ve açıklamaya da çalışmaktadır.

2.1 İfade Özgürlüğü

İfade özgürlüğüne geçtiğimizde bu hakka yönelik ihlallerin genel olarak hükümetler tarafından yapıldığını görüyoruz. Bu ihlaller genel olarak muhalif sesleri engellemek, içeriği filtrelemek veya komple sansürlemek hatta bütün internet erişimini kesmek olarak görülebilmektedir.

Gazeteciler, hükümete muhalif olan insanlar ve kendi kişisel fikirlerini internet üzerinden paylaşan diğerleri, bireysel dünyanın her noktasında ciddi risklerle yüzleşiyorlar. Hükümetin vatandaşların internet aktivitesinin hangi etkilere sahip olduğunun an be an izlendiği ve rekor sayıda gazetecinin öldürüldüğü, hapis edildiği veya kaçırıldığı Suriye'de ifade özgürlüğüne yönelik tehlike ciddi şekilde yüksek gözükmekte. 2011 yılından beri "Gazetecileri Koruma" derneği tarafından toplanan belgelere göre Suriye Savaşı sırasında 89 gazeteci veya medya çalışanı öldürülmüştür ve bu oran aynı dönemde dünya üzerindeki gazeteci ölümlerindeki bütün oranlardan yüksektir.[2] Suriye gibi gazeteciler ve medya çalışanları için tehdit olarak görülebilecek bir diğer ülkede Pakistan'dır. 1992 yılından bugüne kadar toplam 81 gazeteci

1 http://12mars.rsf.org/2014-en/
2 https://cpj.org/killed/mideast/syria/

ve medya çalışanı öldürülmüştür.[3]

Bu ölümler ve ifade özgürlüğü ihlallerinin yanında Suriye rejimi geniş bir skalada askeri saldırı gerçekleştirebilmek için stratejik olarak internet sansürünü ve internetin komple kesilmesini kullanmaktadır. İnsan hakları üzerine yapılan politik ihlaller hakkında araştırmalarını yürüten Anita Gohdes'in gösterdiği gibi Suriye rejimi özellikle karşıt görüşten sahip direnişçilerle çatışılan bölgelerde internet karartması uygulamakta ve karşıt grupların iletişim yeteneğine sekte vurarak yapılan hak ihlallerini sistematik olarak kendilerine yönelik bağlantılanmasını engellemeye çalışmaktadır. Sonuç olarak "Suriye interneti, Suriye rejimi tarafından savaş sırasında bir silah olarak kullanılmaktadır" (Tanrıverdi, 2015).

İran'da ise bireyler hapis cezası riski altında yaşamaya devam etmektedir ve bu hapis cezası sadece rejimi eleştirmek ile alakalı değil aynı zamanda Sufi bölgesi ile alakalı bir yazı yayınlamak ya da "toplum ahlakına" zarar verici içerik olarak atfedilebilecek şeyleri yayınlamak ile de verilebilmektedir. Bu cezalardan en ünlüsü ise "Happy in Tehran"[4] ev yapım Youtube videosunun prodüksiyonu ve video içindeki dans hareketlerini yapan kişiye verilen 1 yıllık hapis cezası ve bu hapis cezasının yanında video içinde başörtüsü takmayan bir kadın görüldüğü için hapis cezasına ek olarak verilen 91 adet kırbaç cezasıdır.

Çin Halk Cumhuriyeti'nde ise Başbakan Xi Jinping'in seçim kampanyası sırasında çeşitli söylentiler yaratıldığı iddia edilerek sosyal medya kullanıcıları korkutulmuş ve gözaltına alınmıştır (RSF, 2014b).

Aynı zamanda kullanıcıların kendilerine ait internet sitesi ve blog açmasına karşılık olarak çaydırıcı bir önlem olsun diye internet üzerinden otoriteye sahip kamu kuruluşlarına zorunlu bir kayıt sistemi konulabilir. Suudi Arabistan'da blog veya bir internet sitesi kurmak için aranan şartlar şunlardır: En az 20 yaşını doldurmuş olmak, lise veya daha yüksek bir okuldan diplomaya sahip olmak ve sizin bu internet sitesi veya bloğunuzu düzgün kullanacağınıza dair geçmişe dönük iyi halinizi belli eden belgeler (RSF, 2014a). Konuşmaların ve duyguların ifade edilmesinin önüne geçmek için benzer bir sistem aynı zamanda Beyaz Rusya'da da kullanılmaktadır. Genel halka açık yayın yapan bir Beyaz Rusya web sitesi ".by" uzantılı bir alan adına sahip olmalı ve sunucu hizmetini Beyaz Rusya toprakları içinde barındırmalıdır (RSF, 2014a).

Telekomünikasyon endüstrisini kontrol etmek baskıcı rejimlerin internetteki içeriklere sansür ve kapatma uygulamak için kullandığı bir diğer stratejidir. İran halihazırda Facebook ve Twitter gibi sosyal medya araçlarına geniş anlamda ve ciddi şekilde filtreleme ve bloklama uygulamaktadır. Çin Halk Cumhuriyeti ise diğer önlemlerin dışında bütün ülkenin internet çıkışını ve girişini 6 geçiş kapısına indirdiği "Great Firewall" adını verdiği teknik çözümle bütün çevrim içi içeriği engelleyebilmektedir. Pakistan'da ise askeriye ve hükümet tarafında kontrol edilen web regülasyon ajansı ulusal çıkarları koruma amacının yanı sıra terörizm ile savaşmak, pornografiye engel olmak ve küfür gibi içeriklere engel olmak amacıyla hali hazırda binlerce web sitesine erişimi engellemektedir.

Online içeriği kontrol etmenin bir diğer yolu ise geçici bir şekilde bağlantıyı kesmek veya olan bağlantıyı kullanılmayacak kadar yavaşlatmak olarak görülmektedir. Örneğin İran hükümeti seçim gününe kadar gidilen bir hafta içinde çoğu uluslararası bağlantıları engellemiş ve şifreleme sistemi ile kurulan bağlantıları ise dramatik bir şekilde yavaşlatmıştır. Bu teknik aynı zamanda Suriye ve Pakistan'da farklı politik görüşten kampanyaları ve organizasyonları bozarak kullanılmıştır.

Devletler tarafından güçlü bir şekilde kontrol edilmeyen telekomünikasyon endüstrilerinde hükümetler çıkardıkları yeni mevzuatlar ile sansür kapasitelerini arttırmayı yollarını arayabilirler. Ukrayna Hükümeti'nin Avrupa Birliği ile ortaklık anlaşmasını imzalaması ile patlak veren Euromaiden protestoları sırasında Rusya Devlet Başkanı

3 https://cpj.org/killed/asia/pakistan/
4 http://youtu.be/tg5qdIxVcz8

Vladimir Putin, Ukrayna ve Kırım'da oluşan durumu rapor eden web sitelerinin yetkililerce kara listeye alınabilmesi için bir tasarı çıkartmıştır. Ayrıca ifade özgürlüğü üzerine ayrıntılı bir kısıtlama getiren yeni hukuk gerekliliği ile blog yazarları ve sosyal medya kullanıcıları telekomünikasyon kurumuna kayıt olmak durumunda bırakılmıştır. (…)

2.2 Gizlilik Hakkı

Geçmiş yıllarda birçok devlet gizlilik hakkı ile girdiği sayısız mücadelede kendi gözetim kapasitelerini artırmıştır. Çoğu baskıcı rejim hedef alma ve gözetim için genel olarak Avrupa ve Kuzey Amerika'da geliştirilmiş sofistike ve aynı zamanda etkili olan donanım ve yazılıma güvenmektedir. Hedefe doğru yapılan izleme ile kitleye yönelik yapılan izleme arasındaki ayrım önemlidir, ikisi de legal ve politik görüşe göre olabilmektedir. Kitlesel gözetim internet üzerinde mümkün olan bütün enformasyonun üzerine gelişigüzel odaklanmaktadır. Hedefe yönelik yapılan izleme ise temel olarak odağını bir bireye, birkaç bireye veya birkaç bölgeye koyabilir. Böylece en azından Uluslararası İnsan Hakları hukukuna uygun olabilmektedir (La Rue,2013).

Fransa'da Qosmos ve Almanya'da Ultimaco gibi birkaç Avrupa şirketinin de dahil olduğu şirketler, süren Suriye Savaşı'nda Suriye hükümetine gözetim teknolojisi sattıklarına dair iddialara karışmışlardır. Suriye savaşı sırasında hedef odaklı kötü yazılımlar sıklıkla ve yaygın olarak kullanılmış ve satın alınmışlardır (K. Lab, 2014; Scott-Railton-& Hardy, 2014). Suriye interneti üzerine yapılan zaman ayarlı saldırılar ile Suriye hükümeti tarafından yapılan bombalamalar, işkenceler ve askeri operasyonlar birbirleri ile paralellik göstermektedir. "İnternet aktif olduğu anlarda muhtemeldir ki bir aktivist hedef alınacak ve öldürülecektir; internetin bir bölgede aktif olmaması ise bu o bölgenin rejim güçleri tarafından bombalanacağının güçlü bir göstergesidir" (Tanrıverdi, 2015).

Etiyopya hükümeti ise İngiltere ve Almanya'da kolları bulunan Gamma Uluslararası şirketinin gözetim teknolojisi için ürettiği FinFisher ve FinSpy teknolojilerin birçok alıcısından biridir. Bu teknoloji özel olarak hükümetlere pazarlanmaktadır. FinFisher gözetim teknolojisi ile özellikle dijital hakların sistematik olarak ihlal edildiği Bahreyn, Pakistan (…), Birleşik Arap Emirlikleri ve Vietnam gibi ülkelerde kullanıcının internet davranışını takip etmek için kullanılmıştır (Citzen Lab 2013). Bu teknoloji aynı zamanda üç Bahreynli aktivistin yanında Birleşik Krallıkta yaşayan Etiyopyalı bir politik mülteci iletişimini hedef almak için de kullanılmıştır.

İran ise edinilen raporlara göre Avrupa Birliği tarafından ticaret yasağı olmasına rağmen gözetleme ekipmanlarını bir Alman şirketi olan Ultimaco'dan ve Çin'in telekomünikasyon alanındaki devlerinden olan ZTE ve Huawei'den sağlamaktadır. Azerbaycan Devleti'nin ise web siteleri ve sosyal medya araçları üzerinde sistematik veya geniş anlamda engelleme, sansürleme ile ilişkilendirilemiyorsa da HackingTeam olarak adlandırılan bir İtalyan ekibinden internet üzerine saldırı yapabilecek teknoloji satın aldığı iddia edilmektedir (Marczak, Guarnieri, Marquis-Boire, & Scott-Railton, 2014). İnternet üzerine sistematik bir gözetim uygulamasa da Azerbaycan hükümeti, 2014 yılı itibari ile çevrim içi takip edilen bireyleri gözaltına almanın, korkutmanın hatta cinsel tacizde bulunmanın daha geçerli bir yol olduğuna inanıyor. (…)

Öte yandan öyle anlaşlıyor ki yapılan büyük etkinlikler, hükümetlerin gözetim için yaptıkları ekstra harcamaları haklı hale getirmeye hizmet etmektedir. Bu durum, 2014 olimpiyatlarından önce Rusya'da aynı kaygılar güdülerek 2014 Dünya Kupasını düzenleyen Brezilya'da görülmüş, kitle gözetimi ve dijital komuta merkezi için ciddi bir yatırım yapılmıştır (Whitefield, 2014).

Tabi ki bu gözetim ekipmanları bu etkinliklerden sonra devre dışı bırakılmamıştır. Sportif aktiviteler üzerine yapılan araştırmalar göstermektedir ki aynı zamanda hükümetler bu etkinlikleri ellerinde olan son teknoloji gözetim aygıtlarını test etmek için bir fırsat olarak görmekte ve gelecekte standart hale getirmek istedikleri teknolojiyi bu küçük grupta denemektedirler (Bennett, Haggerty 2012). Devasa sportif aktiviteler ile kitlesel gözetimi

birbirine bağlayan bu trend, insan haklarına dair çok daha geniş ve iyi bir düşüncenin gerektiğini gösteriyor.

Aynı zamanda insan hakları üzerine Avrupa ve Kuzey Amerika'da not almaya değer ölçüde bir önemli bir endişe vardır. Edward Snowden'in çıkardığı belgelerin gösterdikleri eşliğinde "Beş Göz" olarak adlandırılan ABD, UK, Kanada, Avusturalya ve Yeni Zelanda, iç hukuk regülasyonlarını bypass ederek istihbarat ajansları aracılığı ile enformasyon topladığı ve paylaştığı ortaya çıkmıştır. Kullandıkları taktik ve yürüttükleri çok çeşitli işe alımlar en azından bu devletlerin uluslararası insan hakları yasaları eşliğinde tartışılabilir duruma getirmiştir. 2014 Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği raporunun sonucuna göre, "kitlesel" veya "toplu" gözetim programları, meşru bir amaca hizmet etseler ve erişilebilir bir yasal rejim temelinde kabul edilmiş olsalar bile, bu nedenle keyfi olarak kabul edilebilir" (Pillay, 2014).

2.3 Toplantı ve Gösteri Özgürlüğü, İnanç Özgürlüğü, Ayrımcılık, Ekonomik ve Sosyal Haklardan Yararlanma Özgürlüğü

Araştırmanın ilk bölümünün gösterdiği gibi dijital çağda ifade özgürlüğü ve mahremiyet hakkı sadece kontrol altında tutulan insan hakları değildir, diğer insan hakları da bu çağda kontrol altında tutulmaktadır. Teknoloji kullanıcıların aynı zamanda toplantı ve gösteri özgürlüğüne, etnisitiye, dine, cinsiyete veya cinsel tercihe yönelik özgürlük haklarına da çeşitli sansür ve baskılar uygulanmaktadır.

Çin Halk Cumhuriyeti'nde teknolojinin Falung Gong gibi dini gruplarda ve Tibetler ve Uygurlar gibi etnik unsurların hedef haline gelmesinde negatif bir etkisi olmuştur. 2014 yılı içerisinde önemli bir akademisyen ve web tasarımcısı olan Uygur kökenli Ilham Tohti ömür boyu hapis cezasına çarptırılmıştır (Bequelin, 2014).

Sudan, Suudi Arabistan, Yemen, Moritanya, Somali ve İran'da homoseksüelliğe referans olabilecek internet içeriklerine erişim, cinsel azıklıkların hak ihlalleri ile beraber ölüm ile cezalandırılabilmektedir. Daha geniş anlamda insanların kullanım alışkanlıklarının büyük veri havuzlarında toplanması ve firmalar ve devletler tarafından kişilerin seksüel profillerinin çıkartılması ya da daha hassas verilerinin profillenebiliyor olması ile beraber kurumsal sorumlukların tartışılmaya ihtiyaç duyduğu yeni bir insan hakları endişesini doğurmaktadır.

En önemlisi bütün hakların altında yatan temel prensibin altını çizmek gerekir: "Herkes; ırk, renk, cinsiyet, dil, din, siyasal veya başka bir görüş, ulusal veya sosyal köken, mülkiyet, doğuş veya herhangi başka bir ayrım gözetmeksizin bu Bildirge ile ilan olunan bütün haklardan ve bütün özgürlüklerden yararlanabilir" (Art.2, UDHR). Aynı zamanda bireyi korumak amacıyla insan haklarının çevrim içi dünyaya aktarılması sırasında söz konusu veri analiz edilip kullanılabilir. Gün geçtikçe bireyden elde edilen veri "Büyük Veri" olarak toplanmakta, depolanmakta ve işlenmektedir. Sigorta şirketleri ve medikal şirketler, arama motorları ayrımcı uygulamalar için önemli bir kapsam sunmaktadır (Pasquale, 2015; Tüfekci, 2015).

Son olarak not etmek gerekir ki teknolojinin ekonomik, sosyal ve kültürel haklar üzerine olan etkisine dair anlayışımız hala devam eden bir oluşum aşamasındadır. Bunlardan örnek vermek gerekirse "Tıbbi bakım altında bir standart dahilinde yaşama hakkı" daha geçiş odaklı bakış açışı ile araştırılmamıştır. Örneğin artan kullanıcı sayısı ile beraber kullanıcılar, sağlık ile bağlantılı verileri araştırırken interneti kullanmaktadır. Ancak bu veriler çoğu yargı organı tarafından sınırlandırılmış ve filtrelenmiştir. Bir örnek vermek gerekirse üreme sağlığı durumlarında bu yola başvurulmaktadır. Bir başka hassas alan ise kişisel sağlık bilgileridir. Sadece son dönemde kitlesel çevrim içi gözetimin tuttuğu arama motoru verilerine bakarsak kaç kullanıcının depresyonu, AIDS'i ve hatta kürtajı araştırdığını sayılarla görebiliyoruz. Dahası özgür bir hareket alanına sahip dijital uygulamalar ve avukat hakkı hala yetersizliğini korumaktadır.

İnsan hakları ihlallerine yönelik olarak hazırlanan bu liste yeteri kadar ayrıntılı

değildir çünkü teknolojinin geniş anlamda insan haklarına yönelik etkilerini anlamak ve değerlendirmek için daha fazla kanıt gerekmektedir. Devlet ve devlet dışı aktörler ise teknolojik kapasitelerini arttırmakta ve insan haklarının önünde yeni bir mücadele alanı yükselmektedir.

3 İnsan Haklarına Yönelik Yasal Düzenlemeler

İnsan hakları rejiminin doğduğu 1947 yılında dünya üzerindeki insan popülasyonunun sadece ufak bir kısmının telefon ve televizyon gibi en son teknolojilere erişimi vardı. Bugün ise dünya üzerindeki 3 milyar internet kullanıcısının yaklaşık %67'lik kısmı gelişmekte olan ülkelerden gelmektedir. Bu yaygın kullanımdan ötürü uluslararası yasalar ve standartlar sürekli olarak geliştirilmeye ve insan haklarını korumak için adapte edilmeye çalışılmaktadır fakat dijital alana yönelik sorunların hesaplanması için hala önümüzde uzun bir çalışma süreci vardır.

Araştırmanın bu bölümü Birleşmiş Milletler veya Avrupa Konseyi gibi hükümetler üstü kurumlar tarafından geliştirilmiş uluslararası yasalar ve standartlara yönelik bir genel değerlendirme olacaktır. Ayrıca bu araştırma, aynı zamanda sıklıkla hükümet dışı aktörler tarafından geliştirilen teknik standartları, iş yapma kurallarını ve ilkelerini de içerecektir. Bu araştırmanın ana hedefi, insan hakları ile alakalı tüm yasaları ve standartları içermek değil, daha ziyade dijital alana/çağa aktarılması hayati hale gelen insan hakları sistemine odaklanmaktadır.

3.1 Birleşmiş Milletler Tarafından Geliştirilmiş Yasalar ve Standartlar

İnsan Hakları Evrensel Beyannamesi[5] ile uluslararası düzeyde tanınan insan hakları, Birleşmiş Milletler Genel Kurulu tarafından 1948 yılı itibariyle Birleşmiş Milletler bünyesine adapte edilmiştir.[6] İnsan hakları ve yurttaş bildirgesinin vurguladığı ve üzerinde durduğu temel nokta şudur: Dünya üzerindeki her bir birey eşittir ve ayrımcılığa karşı eşit derecede korunmalıdır.

Enformasyon ve telekomünikasyon teknolojilerinin gelişimi bağlamına uygun olarak düşünülen 12 ve 19. maddelerde sırasıyla; "İnsanların özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz", "Herkesin düşüncesini özgürce açıklama ve yayma hakkı vardır" denilerek özgür irade sağlanmaya çalışılmıştır. Özellikle 19. madde; karşılıksız olarak verilen "herhangi bir müdahale olmaksızın fikirlerini savunma" ile "ülke sınırları söz konusu olmaksızın bilgi ve düşünceleri her yoldan araştırma, elde etme ve yayma" haklarının bir karmasından oluşmaktadır. Teknoloji geliştikçe yazışma gizliliğine olan anlayış, dijital iletişimin diğer formlarına dair anlayışı da ifade özgürlüğünü sağlamak için kapsamaktadır.

İnsan Hakları Evrensel Bildirgesi günümüz itibari ile 1976 yılında onaylayan devletler için geçerli olan "Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi" gibi insan hakları anlamında çok bilindik bağlayıcı antlaşmalara da ilham vermiştir. İnsan Haklarını Evrensel Beyannamesi'nin 17. maddesinde açıklanan mahremiyet hakkı "Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi"nde, kelimesi kelimesine aktarılmış ve korunmuştur. İnsan Hakları Ve Evrensel Bildirgesinin 19. maddesi olan düşünceleri yayma özgürlüğü ise "başkalarının hakları ve itibarı" ve "ulusal güvenliğin ve kamu düzeninin korunması" ile ilgili yapılan ekler ile genişletilmiştir. Gözden kaçmaması gereken nokta ise günümüzde de hala üzerinde derin tartışmalar, ifade özgürlüğü ile ulusal güvenlik arasındaki gerilimi ortaya çıkarmıştır. Mevcut politik anlatıcıların üzerinde sürekli olarak durduğu dijital çağda insan hakları temalı çarpışmanın fitili bu değişimdir.

Siber güvenliğin ötesinde, Birleşmiş Milletler İnsan Hakları Konseyi tarafından insan haklarının gelişimi için özellikle önemli olan, ülkelerin insan hakları durumlarını özel olarak araştırıp rapor edecek bağımsız uzmanlar görevlendirilmiştir. Birleşmiş Milletler tarafından

5 https://www.un.org/en/documents/udhr/index.shtml
6 1948'de, sekiz BM üye ülkesi oylamada çekimser kaldı, ancak hiçbiri muhalefet etmedi.

atanmış bu bağımsız araştırmacılar ise insan hakları sistemi üzerine yeni bir yorumlama şekli ve değişiklikler önermiştir. Bağımsız araştırmacıların yaptıkları bu yorumlar politik bir direnişle karşılaşıyorken onlar insan haklarının dijital alana dönüşümü için yeni bir yol açmışlardır.

Bu bağımsız araştırmacılar dijital teknolojilerin gelişmesine bağlantılı bir sorun olarak 1993 yılı itibariyle belirlenmiş insan hakları evrensel bildirgesinin "düşüncelerin özgürce ifade edilebilmesi" noktasını dijital alanda geliştirmek ve korumak noktasında direk mücadele etmek için son derece iyi donanımlıdırlar. Aynı zamanda bu bağımsız araştırmacıların bir diğer görevi de özgürlüklerin daha iyi korunması ve düşüncenin özgürce daha iyi ifade edilebilmesi için öneriler ve geliştirmeler sunmaktır.

Dijital zorlukların değerlendirilmesi, eski BM İfade Özgürlüğü Özel Raportörü Frank La Rue'nun mirasının önemli bir parçasıdır. Hem internet üzerinden uygulanan düşünce ve ifade özgürlüğü hakkı hakkında Genel Kurul'a sunduğu 2011 Raporu hem de Devletlerin etkileri hakkında İnsan Hakları Konseyi'ne sunduğu devletlerin iletişimleri gözetim altında tutmasının özel hayatın gizliliği ve düşünce ve ifade özgürlüğüne ilişkin insan haklarının uygulanması üzerindeki etkilerine dair 2013 Raporu, kapsamlı bir istişare süreci aracılığıyla dünyanın dört bir yanından gelen sesleri başarılı bir şekilde bütünleştirdi.[7] Her iki rapor da internetin insan hakları üzerine nasıl bir etkisi olduğu konusundaki anlayışımızı zenginleştirmiş ve bu alanda çok önemli olduğu düşünülen yaygın raporlar haline gelmiştir. Ağustos 2014 itibariyle onun yerine, ifade özgürlüğü ile işlem ve iletişimleri güvence altına almak için şifreleme kullanımı ve çevrimiçi olarak anonim olarak işlem yapmak ve iletişim kurmak için diğer teknolojiler arasındaki ilişkiyi yöneten yasal çerçeveye ilişkin raporunun Haziran 2015'te sunulması beklenen David Kaye geçti.[8]

Birleşmiş Milletler İnsan Hakları Konseyi 2012 yılında "*İnternet Üzerindeki İnsan Haklarının Yükseltilmesi, Korunması Ve Yararlanması Üzerime Çözüm*" başlıklı öneriyi oy birliği ile kabul etmiştir. Bu çözüm, "bireyler hangi medya organını kullanıyor olurlarsa olsunlar ifade özgürlüğünü kullanırlarken fiziki dünyada sahip oldukları koruma haklarına çevrim içi dünyada da sahip olmalıdır" ifadelerini önemli olumlamalarla beraber içermektedir. Bu doküman aynı zamanda internetin doğal ve dünya çapında yapısının, bulunan bu hataları da hesaba katarak büyüme ve gelişme evresinin devam etmesini önermektedir.

Geçtiğimiz birkaç yılda ciddi şekilde büyüyen bir sorun olan çevrim içi gizliliğe dair Birleşmiş Milletler İfade Özgürlüğü Raportörünün, İnsan Hakları Konseyi'nin 28. Oturumunda bu soruna dair bir çözüm önerilmesi beklenmektedir. İnsan hakları üzerine ve çevrim içi gizliliğe dair artan endişenin temel sebebi, Edward Snowden tarafından 2013 yılı itibariyle sızdırılan belgelerde ortaya çıkan iletişime dair izinsiz müdahaleler ve gözetim çabalarıdır. Oluşan bu sızıntılar, Birleşmiş Milletler Genel Kurulunu, "Dijital çağda mahremiyet hakkına dair çözümleri" adapte etmeye dair motive etmiştir. Aynı zamanda Birleşmiş Milletler tarafından yapılan bu çözüm önerisi, devletleri sadece mahremiyet hakkını sağlaması ve dijital iletişim üzerindeki ihlallerini sona erdirmesi konusunda teşvik etmemekte, aynı zamanda üye devletlerin iletişimin korunması üzerine yaptıkları yasal düzenlemeleri ve pratik uygulamaları, yaptıkları gözetime dair sonuçları da değerlendirme sürecine tabi tutmaktadır (A/RES/68/167).

Birleşmiş Milletler eski Yüksek Delegesi Navi Pillay'ın dijital çağda mahremiyet hakkı üzerine olan raporunda "bireyden izin alınmadan yapılan gözetim belli şartlar altında kabul edilebilir diyerek" görüşe önemli katkılarda bulunmaktadır. Bu gözetim şartlarının gerekli ve riskin adreslendiği yere göre orantılı olduğunu kanıtlamak ve göstermek ise hükümetin sorumluluğundadır. Navi Pillay'ın vardığı sonuca göre "Bu tarz gözetlemenin olduğu durumlarda kitlesel gözetimin olurluğunun önüne geçilmektedir."

7 Bkz. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290 ve http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40

8 Bkz. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Kaleme alınan bu rapor "Dijital çağda mahremiyet hakkına dair çözümleri" üzerine toplanan Birleşmiş Milletler Genel Meclisine bağlı üçüncü komitenin üye olan milletlere yaptığı genişletilmiş katılım ve onaylama çağrısına geliştirme ve revize etme yönünde çeşitli katkılarda bulunmuştur.

Çözüme yönelik maddeleri içeren bu öneri, dijital alanda mahremiyet hakkına getirilen yeni bir uluslararası standart olarak düşünülebilir. Bununla birlikte taslak metin üzerine oluşan konuşmalarda ortaya çıkan siyasi sürtüşmeler sırasında ortaya çıktı ki orantılılık ilkesi, yorumlamalar ve dokunulmazlık kavramı prensipleri üzerine daha dikkatli ve derinlemesine araştırma yapılmalıdır. Mahremiyet hakkına dair ise Birleşmiş Milletler özel raportörlerinin yaptıkları çalışmalar, yorumlamalar etrafındaki çatışmaları dağıtıp dijital çağdaki insan haklarına katkıda bulunabilir. Burada, düşüncelerin özgürce ifade edilmesi konusunda Birleşmiş Milletler İnsan Hakları Komitesi tarafında yapılan genel yorumlamanın 34. maddesi ve *Uluslararası Kişisel ve Siyasal Haklar Sözleşmesi'*nin 19. maddesindeki görüşler, bu çalışmalar açısından yararlı olabilir. *Birleşmiş milletler İnsan Hakları Komitesi* tarafında yapılan genel yorumlamalar, *Uluslararası Kişisel ve Siyasal Haklar Sözleşmes*i'nin 19. maddesindeki hakların korunmasıyla bağlantılı olarak "*Elektronik ve İnternet Tabanlı Ortamlardaki İfadeler*" başlığı altında değerli ek analizler ile güncellenmiştir. Ancak *Uluslararası Kişisel ve Siyasal Haklar Sözleşmesi*'nin 17. maddesine göre güncellenen mahremiyet hakkına dair genel yorumlamalarda hala bir şey eksiktir ve bahsedilmemiştir. Şu an kullanılan genel yorumlamanın 16 maddesinin kökenleri 1988 yılına kadar dayanmaktadır. Bu maddede sadece bilgisayar, veri bankaları ve diğer cihazlara değinilip geçilmiştir ve interneti bir yana bırakırsak dijital iletişime bile değinilmemiştir.

Birleşmiş Milletler Hükümet uzmanları grubu ayrıca devletlerin siber alandaki normlar ve hükümlülüklerini daha iyi bir şekilde tanımlamaya çalışmışlardır. Bu grup yoğun bir şekilde devlet güvenliği, hükümetler arasındaki anlaşmazlıklar ve devletlerin sorumlu oldukları normlar, prensipler ve kurallar üzerine yoğunlaşmışken aynı zamanda "çatışma sırasındaki enformasyon, iletişim teknolojileri ve bu enformasyon, iletişim teknolojilerinin savaş sırasındaki kullanımı için hangi uluslararası yasa uygulanır" konusunu da dikkate almışlardır. Bu grup, devletlerin internet üzerinde sorumsuzca davrandıklarını ima etmemektedir fakat klasik diplomatik anlayışlar üzerinden türetilmiş (silahsızlanma denemelerinden deneyimlediğimiz gibi) bir tarzda bu konunun üzerine gidilirse gözükmektedir ki oluşacak boşluk, kontrol edebilen herkes tarafından bir silah olarak kullanılabilecektir. Bu nedenle bu grup, bu koşullara özel genel normlar geliştirmeye ve güven arttırıcı önlemler alınırken ortaya çıkan belirsizlik içerindeki durumlara karşı azaltıcı önlemler almaya çalışmaktadır.

Teknoloji ve hukuk kuralları, benzer standartlar ve araçlarla evrimleşir ise ifade özgürlüğü ve mahremiyetin gizliliği dışında kalan insan haklarına dair diğer kurallar da Birleşmiş Milletler bünyesine entegre edilebilir. Fakat dijital alana uygulanabilir olan önemli hukuk kanunlarını ve prensiplerini sistemleştirerek insan haklarını korumaktan sorumlu tek uluslararası aktör Birleşmiş Milletler değildir.

3.2 Diğer Uluslararası Kuruluşlar Tarafından Geliştirilmiş Yasalar ve Standartlar

Geçtiğimiz yıllarda insan haklarının çevrim içi alana dönüştürülmesindeki önemli işler sadece Birleşmiş Milletler ve Avrupa Konseyi gibi hükümet üstü kurumlarda yapılmamış, aynı zamanda sivil toplum örgütleri, özel aktörler ve teknik organizasyonlar gibi çoklu paydaşlar tarafından da yapılmıştır. İnternet gibi insan aktivitesinin politik, sosyal ve ekonomik alanı ile kesişen bir teknoloji hakkında yasaların, prensiplerin ve standartların geliştirilmesi üzerine yapılan konuşmalar siber güvenlik, ticaret, teknik standartlar, kurumsal sorumluluk ve internet yönetişimi alanlarının tartışılması noktasında yapılmaktadır. Araştırmanın bu bölümü konuyla alakalı en çok bilinen uluslararası forumların önemli gelişmeleri üzerine genel bir bakış sağlamaktadır.

3.2.1 Avrupa Konseyi

Avrupa Konseyinin sadece 47 üyesi olmasına rağmen insan hakları düzeninin

gelişimi üzerine olan etkisi, üye sayısından çok daha ileriye ulaşmaktadır. İnsan hakları düzeninin önemli bir parçası olan Avrupa İnsan Hakları Mahkemesi, Avrupa İnsan hakları sözleşmesinde yer alan temel özgürlükleri ve insan haklarının koruyucusunun teminatı olmanın yanında aynı zamanda mevcut insan hakları düzeninin kurallarını dijital çağa aktarırken çıkan zorluklarla da mücadele etmede önemli bir rol oynamaktadır. Avrupa İnsan Hakları sözleşmesinin 8 ve 10. maddelerinde sırasıyla mahremiyet hakkı ve ifade özgürlüğü hakkı koruma altına alınmıştır. (…)

Avrupa İnsan Hakları Mahkemesinin yetki alanı içinde, çevrim içi alanda düşüncenin özgürce ifade edilebilmesi konusunda önemli bir emsal teşkil etmektedir. Mahkemenin belirttiği gibi "Günümüzde internet, bireylerin düşüncelerinin özgürce ifade edilebilmesi hakkı üzerine kullandığı temel araçlardan biri haline gelmiştir: İnternet; politika veya kamu yararı hakkında yapılan aktiviteler ve tartışmalarda ilgili gerekli araç ve gereci sağlamaktadır."[9]

Avrupa Konseyi "Kişisel verilerin işlenmesi ve korunması" üzerine olan maddeyi 1981 yılında kabul etmiş ve aynı maddeyi 2014 yılı itibariyle "kodlanmış veri koruması bu tarih itibariyle standarttır" düzenlemesi ile iyileştirmiştir. 2001 yılında Macaristan/Budapeşte'de belirlenmiş olan Siber Suç Sözleşmesi 44 ülke tarafından onaylanmış olsa da 100'den fazla ülke, ulusal mevzuatlarını bu sözleşme standartlarına çıkarmıştır. En önemlisi kabul edilen bu sözleşme günümüzde devletlerin siber suçlarla karşı iş birliği içinde adil olarak savaşmayı kabul ettikleri tek uluslararası sözleşmedir. Fakat aynı zamanda kendi yetki ve prosedürlerini içerisinde "ulusal yasaları altında, çeşitli koşullar ve güvenlik önlemleri altında insan hakları ve özgürlükler için yeterli korumayı sağlayacaktır" (Mad.15)

Son olarak vurgulanmalıdır ki Avrupa Konseyi uluslararası hukukun ayrılmaz bir parçası olarak insan haklarını teşvik etmek üzerine oldukça konuşkan bir tavır takınmaktadır. Konsey aynı zamanda çok farklı alanlarda yaptıkları çalışmalar ile insan hakları sorunu ve internet arasındaki ilişkiyi kaynaştırmaya çalışarak oldukça aktif bir çalışma yapmaktadır. Bu nedenle Avrupa Konseyi'nin rolü sadece hukuki değil, aynı zamanda internet üzerine yapılan uluslararası yasalar ve politikalarda insan haklarına dayalı yaklaşımı sağlamak için politik bir rol de üstlenmektedir.

3.2.2 Avrupa Güvenlik ve İş Birliği Teşkilatı

Avrupa Güvenlik ve İş Birliği Teşkilatı, insan haklarının dijital alana geçişinin yanında, var olan uluslararası insan hakları sistemine de katkıda bulunur. Katılan 57 ülke ile beraber bu dünyanın en büyük güvenlik odaklı hükümetler arası organizasyonu yasal olarak bağlayıcılığı olmayan fakat ülkelerarası iş birliğini teşvik edici önlemleri tanıtmıştır. Aralık 2013'de, Avrupa Güvenlik ve İş Birliği teşkilatı güven arttırıcı önlemler üzerinde "devletler arası iş birliğini, şeffaflığı, öngörülebilirliği, stabiliteyi geliştirmek ve yanlış anlama, gerginlik ve ICT'nin[10] kullanımında kaynaklı çatışma riskini azaltmak" hedefi ile anlaştı. Bu 11 önlem, bilgi paylaşımı, istişare ve diyalog halinde kalma ve ulusal yasaları yeterli teşvik içinde tutacak aday irtibat noktaları aralığında yer almaktadır. Açık bir şekilde temel özgürlükler ve insan haklarına saygı sorumluğu ile beraber güvenlik bağlantılı bu metin siber alana yönelik devlet davranışına dair önemli bir dönüm noktası olarak kabul edilmektedir. Siber güvenlik için güven arttırıcı önlemlere dair ikinci durum, halen Avrupa Güvenlik ve İş Birliği Teşkilatı'nın farklı üyeleri arasında tartışılmaktadır.

3.2.3 Teknik Organizasyonlar

Hükümetler arası düzeyde ilerleme elde edilirken devletlerin dijital alanda rollerinin ve sorumluluklarının yeniden tanımlanması ve internetin düzgün çalışmasından sorumlu teknik organizasyonların insan haklarına uygulanabilir standartlara yönelik sürekli revizyonlar içinde yeri önemlidir. Bu standartlara rağmen doğadaki teknik görülebilir ve

9 Konu ile alakalı bütün metin http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=001-115705#{"itemid":["001-115705"]}

10 Konu ile alakalı bütün metin http://www.osce.org/pc/109168?download=true

teknik standartlar, insan haklarına uygun olarak kabul edilmesi gereken önemli politik, sosyal ve ekonomik sonuçlara ve büyüyen bir tanıma sahip olmuştur.

İnternet Topluluğu, internet ile ilgili standartlara, eğitime ve "internetin dünya üzerindeki insanlar için inovasyon, ekonomik kalkınma ve sosyal gelişme platformu olma özelliğinin büyümesi ve evrimleşmesinin devam etmesinden emin olunması ile alakalı"[11] politikaya liderlik sağlamak amacı ile 1992 yılında kurulmuş, uluslararası ve kar amacı gütmeyen bir topluluktur. İnternet topluluğu himayesindeki İnternet Mühendisliği Özel Timi "ağ dizaynırlarının geniş ve açık internet topluluğunun, operatörlerin, sağlayıcıların ve araştırmacıların internet mimarisinin evrimi ve internetin düzgün çalışması ile ilgili endişelerini" etkilemektedir. Bu teknik topluluk, yapılması istenen taleplerle ilgili olarak internete uygulanabilir araştırmaları veya inovasyonları, davranışları, tanımlanan yöntemleri ortaya çıkartıp bunlara dair standartları ve protokolleri geliştirir.

Özel bilgilerin korunması üzerine yapılan açıklama isteği RCF 1984 olarak bilinir ve 1996 yılında yayınlanmıştır. Örneğin İnternet Mühendisliği Özel Timi tarafından geliştirilmekte olan ve tanınan güvenlik mekanizmaları, "kriptografik teknolojilerin uluslararası olarak yeterli oranda kullanımına bağlıdır ve ihtiyaç duymaktadır"[12]. Bu teknik topluluk, yakın zamanlarda mahremiyet hakkı ve düşüncenin özgürce ifadesi izlenimi altında büyüyen endişelerini yinelemiştir. Topluluk, şifrelemeyi internetin standardı yapmayı taahhüt eder. İnternet gizlilik beyanı vurguladığı "şifreleme mümkün olduğunda doğrulanmalıdır fakat doğrulama yapılmadan protokoller tarafından gizliliğin sağlanması bile yaygın gözetimle yüzleşmek için yararlıdır" açıklaması İnternet Mühendisliği Özel timi üzerinde gözetmen görevi gören İnternet Mimarisi Kurulu tarafından Kasım 2014'de kabul edilmiştir[13]

İnsan Hakları Protokolü Hususu Üzerine Araştırma Önerisi Taslağı'nda İnternet Mühendisliği Özel Timi, "İnsan haklarının temelini oluşturan ve internet altyapısını sağlayan standartlar ve protokoller" önermektedir. Teknik uzmanlardan oluşan grup bir yıllık ön araştırmada bu fikri daha fazla keşfedecek ve geliştirecektir.

Ayrıca Amerika merkezli ve kar amacı gütmeyen bir kuruluş olan *İnternet Tahsisli Sayılar ve İsimler Kurumu* (ICANN)'da Uluslararası İnsan hakları sistemine katkıda bulunmaktadır. Bu kuruluş, internet fonksiyonlarının çalışması için hayati olan IP adreslerinin ve alan adı isimlerini de içeren birkaç veri tabanı ile internet kaynaklarının bakımlarından sorumludur.

Yakın tarihli iki yayının işaret ettiği gibi, yeni alan adları atama sürecinde insan haklarını koruma sorumluluğu, hem ICANN'in karar alma sürecine Devlet Danışma Konseyi (GAC) aracılığıyla katılan hükümetlere hem de kurumsal bir aktör olarak ICANN'in kendisine aittir. Bu yayın, aynı zamanda ICANN'in ayrımcılıktan korunma ve özellikle düşüncenin özgürce ifade edilebilmesi gibi insan haklarını dikkate alarak kendi iç tüzüğünü değiştirmesinin zorunlu olduğunu öne sürmüştür. Bu tüzük değişimi özellikle devam eden ve iki binden fazla yeni alan adı kayıt isteği alınmış yeni genel üst düzey alan adları programı bağlamında önemlidir. Uzmanlara göre, ICANN'in yeni genel üst düzey alan adları programında ki şu an ki "duyarlı uygulamaları" düşüncenin özgürce ifade edilmesi noktasında tam bir uyum göstermemektedir. Bunun nedeni belli alan adlarının hassas olarak sınıflandırılmasıdır ve bu ".xxx" ".gay" veya ".amazon" gibi alan adı uzantılarının serbest bırakılması ICANN toplumunun üyelerinden farklı itirazlar almıştır. Bu araştırma birçok konuda kültürel, toplumsal ve/veya siyasi duyarlılıkları vurgularken aynı zamanda tescil alanının ihlali ile alakalı özgürce görüş bildirmektedir. Daha da önemlisi bu alan adlarından bazıları ayrımcılığa dayalı sebeplerce geri çevrilmiştir. Bu nedenle LGBT gibi potansiyel azınlık topluluklarını haklarını sınırlayıcı, insan haklarından tam anlamıyla yararlanmaları üzerinde kısıtlayıcı olmuştur.

3.2.4 Özel Sektör

İnsan hakları standartlarının korunması ile alakalı sorumluluğu olan tek özel kuruluş

11 http://www.internetsociety.org/who-we-are
12 https://tools.ietf.org/html/rfc1984
13 https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) değildir. Gerçekte insan hakları standartlarının korunmasında özel sektörün rolü hayatidir çünkü insan haklarının dijital çağa aktarılması ile bağlantılı zorluklar, hukuk ve teknik standartlar tarafından daha sistemleştirilmemiştir fakat sorumlu iş uygulamaları ile belli bir dereceye kadar giderilebilir. Ayrıca çoğu zaman çevrim içi şirketler ile onların müşterileri arasında bulunan tek yasal ilişki, kullanım şartlarını tartışmayla sınırlıdır ki bu şartlar, temel özgürlükler ve insan haklarını korumaya almış da olabilirler almamış da.

Özellikle çok uluslu büyük şirketler ile mücadele etmede sayısız zorluk vardır ve devletler, insan haklarını çevrim içi dünyada uygulamak ve korumak için giderek bu şirketlere bağımlı hale gelmektedir. Bir örnek olarak Facebook en büyük global sosyal ağ platformu olması sayesinde içeriği ve bunlardan birçoğunun da radikal olduğu düşünülen bütün içeriği platformu üzerinden sunmaktadır. Hükümetler radikal içeriği belirlemek amacıyla "internet şirketleri ile beraber çalışmaya ihtiyaç duyduklarını" (Watt & Wintour, 2015) tartışmaktadırlar.

Dahası çoğu zaman özel uygulamaların kendisi başlıca sayılamayan, şeffaf olmayan ve tahmin edilemeyen problemin parçasıdır (McNamee, 2014; York, 2010). İnsan haklarının dokunulmazlığına yapılan uygulamalar ile birlikte, ulusal devletler ve globalleşmiş küresel sektörler arasındaki karışık ilişki, insan haklarının çevrim içiyle ilgili başlıca mücadelelerinden biridir (Milton Mueller, 2010).

Birleşmiş Milletlerin iş ve insan hakları üzerine olan temel prensipleri, özel sektör şirketleri için insan haklarını kendi iş stratejileri ve uygulamalarında nasıl yeterince yansıtacaklarının davranış kodu olarak kabul edilebileceğin taslağını çizer. Birleşmiş Milletler' in iş ve insan hakları üzerine olan temel prensipleri, insan haklarına saygı ve diğer yasalara uymanın yanında özel işlevleri yerine toplumun organlarını üstün tutacağı noktasında işletmelerin rolünün tanınması temel alır. Birleşmiş Milletlerin iş ve insan hakları üzerine olan temel prensiplerinin altında, bilgi ve iletişim sektörleri üzerine faaliyet gösteren şirketlerden yaptıkları faaliyetler sürecinde insan haklarına saygı ve bağlılıklarını özetleyen açık politika beyanı ve ayrıca insan haklarına yönelik herhangi bir olumsuz etkiyi önlemek için yerinde değerlendirme ve tanıma yapacak uygun durum tespiti mekanizmalarını kurması beklenir[14].

Ekonomik Kalkınma ve İş Birliği Örgütü (OECD), çok uluslu şirketler için olan kuralları ayrıca açıklar: "İlişkili iç kanunların yürürlüğü ile ilgili ya da uluslararası insan hakları yükümlülüklerini uygulamak konusundaki devlet başarısızlıkları veya işin gerçeği devletlerin bu tür uluslararası yükümlülüklere/yasalara aykırı hareket edebilme potansiyelleri, işletmelerin insan haklarına saygılı olması konusunda oluşan beklentiyi azaltmaz. Yerel yasaların ve regülasyonların uluslararası anlamda tanınmış insan hakları regülasyonları ile çatışma içinde olduğu ülkelerde, işletmeler bu ülkelerdeki iç hukuku ihlal etmeden insan haklarını regülasyonlarını tam ölçüde sağlamak ve onurlandırmak için yollar aramalıdırlar"[15].

Küresel Ağ Girişimi'nin misyon ifadesine göre; girişim, insan hakları üzerinde çatışma sayılabilecek yerel yasalar ve politikalar üzerinde artan baskıdan beri bilgi ve iletişim sektöründe düşüncenin özgürce ifade edilebilmesini ve gizliliği korunabilmesi için iş birlikçi bir yaklaşımı yaratmayı hedeflemektedir.

Sonuç olarak dijital insan hakları mücadelesine yönelik sorunlar kaçınılmaz olarak bütün özel sektörü içermektedir. Bununla birlikte çözüme ulaşmak için kurumsal aktörlere olan bağlılık aynı zamanda probleminde bir parçasıdır. İnkar edilemez şekilde özel sektör insan haklarının yükseltilmesinde ve korunmasında katkıda bulunabilir. Aynı zamanda insan haklarının çevrim içindeki hakların merkezi parçalarından biri kabul edilmesi için şirketlerin yapmaya ihtiyaç duyduğu birçok durum da vardır.

14 http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf
15 http://www.oecd.org/daf/inv/mne/48004323.pdf

3.2.5 Çoklu Paydaş Toplantıları

Hükümetler, teknik topluluklar, özel sektör ve sivil toplumun her birinin çevrim içi insan haklarını korumak için özel bir rolü ve sorumluluğu varken "Sadece tüm bu aktörlerin tutumları ile geliştirilmiş ve adapte edilmiş normlar, teknoloji kullanıcılarının sorunlarına yeterli bir yanıt olabilir" şeklinde büyüyen bir anlayış vardır. Sonuç olarak çoklu paydaş toplantılarında gelişen yasalar, prensipler ve politika pratikleri, uluslararası münazaalarda önemli bir ivme kazanmıştır.

2014 yılının Nisan ayında Brezilya'nın Sao Paulo kentinde yapılan NETmundial Konferansı aşağıdan yukarıya, açık ve katılımcı bir süreç olarak örnek bir konferanstır. Çeşitli paydaşları temsil eden binlerce temsilcinin kararıyla onaylanan "NETmundial çoklu paydaş toplantıları ifadesi", internet yönetim prensipleri evrensel insan hakları tarafından desteklenmelidir, görüşünü tazeledi[16]. Birleşmiş Milletler'in 2012 yılındaki uluslararası insan hakları ifadesinde yer alan "İnsanların çevrim dışı olduğu anlardaki hakları, aynı zamanda çevrim içi olduğunda da korunmalıdır" beyanı, NETmundial beyanında yankılandı. Mahremiyetin korunması ile birlikte düşüncenin özgürce ifade edilebilmesi gibi spesifik olarak isimlendirilmiş haklar, keyfi veya hukuka aykırı gözetim, veri toplama, kişisel verileri kullanma gibi ihlallere maruz kalmayacak şeklinde beyan edildi.

NETmundial konferansı "Herkes, çevrim içi olarak sosyal ağlar ve platformlarda dahil olmak üzere, barışçıl bir şekilde toplanma hakkına sahiptir" gibi dijital alandan etkilenmiş diğer insan haklarını da anlamlı şekilde içermektedir. NETmundial beyanı enformasyon özgürlüğü ve veriye erişim konusunda oldukça özenlidir. "Herkes, yazarların ve yaratıcıların haklarına hukuken saygılı olarak internet üzerinden bilgiye ulaşabilmeli, onu paylaşabilmeli, üretebilmeli ve dağıtabilmelidir" maddesi beyanın içerisinde yer alır. Bu beyan, çevrim içi kaynaklara erişebilirliği teşvik ederek engelli kişilerin özel ihtiyaçlarına işaret eder. Son olarak internette insan haklarını geliştirmek için yapılan münazaralar "yoksulluk içinde yaşayan insanlara geliştirme süreçlerinde katılım imkanı vermek için hayati bir araçtır."

Düşüncenin özgürce ifade edilebilmesi ve mahremiyet hakkı gibi iki haktan daha ziyada NETmundial beyannamesinin yansıması, insan haklarına yönelik olarak kullandığımız ölçeği genişletmemiz ve bu iki haktan daha farklı haklara da ulaşmamız sonucuna varır. İnsan haklarını koruma önlemleri konusunu tanımlamak için sıklıkla kullanılan "internet kullanıcıları" ve "bireysel" kelimesi dikkat çekicidir. Bu bireysel etken çoklu paydaş toplantılarını insan haklarına yönelik doğrusal bir desteği tartışmaya soktu.

Mevcut insan hakları eğitimi sırasında normların hiçbir açık eksiğinin olmadığı görülmelidir. İnsan hakları zaman içerisinde evrim geçirmeye devam etmektedir ve çeşitli teknolojik gelişmeler insan haklarının korunmasının önünde kesinlikle bir problem yaratacaktır fakat bu problemler aşılmaz değildir. İnsan hakları standartlarının ve normlarının başarılı bir şekilde evrimleşmesini sağlamak amacı ile insan haklarının geleceğine yönelik geliştirmelerin genişçe tartışılması ve ilgili tüm aktörleri içermesi hayati gözükmektedir.

4. İnsan Haklarının Dönüşümünü Teşvik Eden Politika Girişimleri

Eninde sonunda, dijital geliştirmeler tarafından yaratılan bütün zorluklara karşı, hiçbir yasa veya yönerge tarafından komple hitap edilemez. Dijital hakların yeterince korunması amacı ile ülkeler, uluslararası yasalar ve standartları kendi iç hukuk yükümlülüklerinde uygulamak için kapsayıcı ve akıllı politikalar geliştirmeye ve iş birliği yapmaya ihtiyaç duymaktadır. Aynı zamanda insan haklarını korumak ve desteklemek için durum tespiti ve uyum mekanizmalarının kontrolünü sağlayacak kurumsal sektörde bir lidere ihtiyaç vardır. Bu bölüm çeşitli uluslararası politika girişimlerini ve bunların dijital hakları korumak ve desteklemek için sahip oldukları potansiyelleri değerlendirmeye çalışacak.

16 http://netmundial.br/netmundial-multistakeholder-statement/

4.1 Wassenaar Düzenlemesine Göre İhracat Kontrolleri

İhracat kontrolleri, insan hakları temelli yaklaşımın uluslararası politikaya uygulanmasında önemli bir mekanizma haline gelmektedir. Bununla birlikte uluslararası koordinasyon ve gözetim eksikliği nedeniyle mevcut önlemler, insan haklarını sistematik şekilde ihlal eden ülkelere yapılan gözetime ve sansüre yönelik teknoloji ihracatını engellemede yetersiz olmaya devam etmektedir.

Wassenaar düzenlemesi bu tür koordinasyonu gerçekleştiren bir forum olmasına rağmen odaklandığı nokta, uluslararası güvenlik ve stabilitedir. Bu forumda insan hakları sorunlarından açıkça bahsedilmemiştir. Wassenaar düzenlemesinin listeleri yıllık olarak güncellenmektedir ve teknolojinin sansür ve gözetim için kullanılması düzenlemesine yönelik olarak yapılacak güncelleme zaman alacaktır (Maurer, Omanovic vd., 2014). Wassenaar düzenlemesi, 2013 yılının Aralık ayında çeşitli gözetleme teknolojilerinin çift-kullanım listesinde yer almasını kabul etmiştir. Kitle gözetimi, hedefli gözetim ve telefon dinleme gözetimi gibi gözetim çeşitleri güncel Wassenaar listesinde yer almaktadır ancak tanımlar doğru teknolojilerin korunmasını sağlamak için hala adapte edilmeye ihtiyaç duymaktadır.

Wassenaar özelinde kullanılan gerçek kontrol listesi istişaresi endişe nedeni olmaktadır. Bu istişare karar mekanizmasını kontrol eden azınlık hükümet uzmanları ve aldıkları karar alma mekanizması çok az bir şeffaflığa sahiptir ve bu şeffaflık çekincesi bütün Wassenaar düzenlemesi için sorumluluktur. Sivil toplum ve araştırmacı gazeteciler lisanssız teknolojilerin satışının izlenmesinde önemli bir rol oynarken Wassenaar düzenlemesine imza koyan devletler, karar alma mekanizmalarını sivil topluma açarak ve sivil toplum aktörlerini ilgili uzman aktör olarak istişare süreçlerine dahil ederek kurumsal şeffaflıklarını arttırmaya ihtiyaç duymaktadırlar.

4.2 İnternet Yönetişimi ve Dünya Bilişim Toplumu Zirvesi (WSIS)

Cenevre'de 2003 yılında ve Tunus'ta 2005 yılında toplanan Dünya Bilişim Toplumu Zirvesi (WSIS), bilgi ve iletişim teknolojileri ve diğer teknolojik gelişmelere olan ilginin şehir merkezinde yaşayan kapsayıcı ve kalkınma odaklı bilgi toplumunu sağlamak için özellikle çok önemli olduğunu deklare etmiştir. Bu iki zirve, bilişim toplumu hedefine ulaşmak için farklı hatlardan sıkı bir eylem planının on yıllık bir süreç içerisinde uygulanmasını başlatmıştır. İnsan hakları temelli unsur, bireyin güçlendirilmesi odaklı yaklaşım ve ulaşılabilir, karşılanabilir ve kapsayıcı katılım için politikalar uygulanmasından süreç için nispeten güçlü bir unsurdur.

Amerika Birleşik Devletleri'nin New York kentinde 2015 yılı Aralık ayında Birleşmiş Milletler Genel Kurulu içerisinde gerçekleştirilecek olan "WSIS+10-İnceleme Zirvesi" kapsayıcı bir bağlılık yenilenmesine ve hak temelli internet yönetim rejimine yol açabilecektir. Bununla birlikte internet yönetişimi içerisindeki kayıp yönetişime yönelik olarak devam eden fikir ayrılıkları WSIS sürecinin yararı hakkındaki soruları arttırmıştır.

Buradaki zorluk, gelecekteki olması muhtemel zirveye yönelik her geliştirici çalışmanın insan haklarını yeterince hesaba kattığından emin olmaktır. Burada Birleşmiş Milletler ikinci komitesince 2015 yılı sonunda İnternet Yönetim Forumunda (IGF) genişletilen talimat aynı zamanda yararlı olabilir. Olası bütün eklemelerde IGF'in aslında onların çoğu eleştirilerine yanıt olduğundan emin olmalıdırlar (Milton Mueller & Wagner, 2014).

4.3 Çevrim içi Özgürlük Koalisyonu (FOC)

Çevrim içi Özgürlük Koalisyonu, 12'si Avrupa bölgesinden olmak üzere 26 gelişmiş veya gelişmekte olan ülke hükümetlerinden oluşan uluslararası bir koalisyondur. Bu koalisyon özgür ifade ve çevrim içi gizliliği desteklemek için diplomatik çabayı koordine eder. Bu çaba bilgilerin paylaşılmasını, çevrim içi insan haklarına karşı şüpheli ihlaller olması halinde ortak diplomatik girişimlerin ve diplomatik notların paylaşılmasını, uluslararası müzakereler içerisindeki deklarasyon ve pozisyon alma durumunu ortak açıklamalarda formüle etme noktasını içerir. 2014 yılının Ekim ayında 26 üye ülkeden oluşan koalisyon üye

ülkeleri ve üye ülkelerin işletmelerini, "Gözetim teknolojilerinin kullanımı ve ihracatı, uygun ve tutarlı ulusal yasalar içerisinde kontrol edilmelidir" (FOG, 2014) maddesini kabul ederek luslararası, çok paydaşlı olarak kullanılan gözetim teknolojilerini kullanmalarını frenlemek için kabul etmiştir. Bununla beraber Çevrim içi Özgürlük Koalisyonu, hükümetlerin karıştığı insan hakları ihlalleri için yapılan eleştirileri bertaraf etmek için bir koruma kalkanı olarak kullanılması fikri de ortaya atılmıştır. Moğolistan'ın FinFisher şirketinin müşterilerinden biri olduğu ileri sürülmektedir (Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2014), Birleşik Krallık ve ABD devletlerinin ikisi de "Beş Göz" istikbarat teşkilatı birliğinin üyelerindendir (Nyst & Crowe, 2014).

4.4 Teknolojik Egemenlik Önlemleri

Kendi vatandaşlarını kitlesel gözetim üzerinden gözetleyen hükümetler, bu görüşe kalkan olması için bu gözetimi **teknolojik egemenliği korumak üzerine alınan önlemler** olarak isimlendirmektedir. Pratikte bu görüş, özel servis sağlayıcılarını servislerini yerelleştirmek için zorlamak ve böylece hükümetin depolanan kişisel veriler üzerinde çok iyi bir kontrolün olanağına erişmesi anlamına geliyordu. Her ne kadar mahremiyetin korunması gibi insan hakkını sıklıkla bu tür önlemleri haklı göstermek için referans olarak gösteriyor olsalar da aynı zamanda milli güvenlik perspektifine dönmek için işaret vermektedirler. Devletlerin hassas veriler üzerinde kontrolünü arttırmayı deneyeceği aşikar olmakla beraber, insan hakları standartlarını aslında yalnızca devletler yükseltebilir.

Avrupalı farklı politikacılar ve şirketler, veri yerelleştirmenin gerekliliğini, internet trafiğine yönelik yerel yönlendirmeyi ve ulusal elektronik posta hizmetini önerdiler fakat şu ana kadar geniş kapsamlı bir destek bulamadılar (Maurer, Morgus, Skierka, & Hohmann, 2014). Ulusal yönlendirmeye yönelik tekliflerden biri Almanya'daki gizli ve açık aktörler tarafından yapılmıştır. Önerilene göre Avrupa Konseyi Başkanı Herman Van Rombuy tarafından **Avrupa ve Latin Amerika arasında,** deniz altından yeni bir bağlantı hattı çekilmesi önerisi getirilmiştir. Aynı zamanda "Finlandiya'nın veriler için güvenli bir liman" olmasını isteyen eğitimden ve iletişimden sorumlu Finlandiyalı bakan Krista Kiuru da bunu istemektedir. Avrupa'nın dışında Brezilya hükümeti, yabancı şirketler için ulusal sınırlar içerisinde veri depolama gereksinimini araştıran ilk hükümetlerden biriydi fakat sonuçta bu hüküm "Marco Civil da Internet" yasasının son oluşturulan teklifinden düştü. Rusya'daki **veri yerelleştirme önlemleri** Brezilya'daki önlemlerin son taslaktan çıkarılmasının aksine 2015'in Eylül ayında Rusya parlamentosu tarafından yürürlüğe sokulması planlanmaktadır. Benzer önlemler İran ve Çin hükümetleri tarafından olabildiğince çok verinin kendi ulusal sınırları içerisinde kalabilmesinin sağlanması için tarihsel olarak takip edilmiştir (Jiang, 2012; Rhoads & Fassihi, 2011).

Bu eylemler, dijital iletişimde güvenlik ve mahremiyeti korumanın arttırılması için söz vermesine karşın ters bir etkiyle vatandaşlarını izlemede ve kontrol altında tutmada hükümetlere genişleyen bir kapasiteye sahip olma alanı da yaratabilir (Maurer, Morgus vd., 2014). Otoriter rejimler, bir yandan vatandaşlarının dış dünya ile etkin iletişimini engellemişler, diğer yandan da dış dünya ile bağlantılarına izin vererek onların davranışlarını incelemek için uzun tedbirler almışlardır. Her zaman uygulanmamasına rağmen devlet kontrollü intranet (yerel internet) Cuba, İran ve Kuzey Kore gibi rejimlerde desteklenmiştir. Bu bölgelerde hükümetler uygunsuz gördükleri içerikleri engellemekte veya bağlantıyı tamamen kesmekte ve buna "ulusal internet" veya "Helal İnternet" gibi isimler vermektedirler (Hoffmann, 2012; Rahimi, 2011).

4.5 İnsan Hakları Dokunulmazlık Uygulaması

Hükümetlerin vatandaşların üzerindeki kontrolü artırmak ve onların verilerini kendi ülke toprakları içerisinde tutmayı aradığı gibi bilim insanları da insan hakları dokunulmazlık uygulamasının artan önemini işaret etmektedirler. Marko Milanoviç'in savunduğu "globalleşme çağında ülkeler artan bir şekilde kendi sınırları dışındaki insanların insan haklarına etkide bulunmaktadır ve bu etkileme ile beraber dokunulmazlığa yönelik

uygulamalara açılan davalardaki artışı ve genel konunun artan önemini açıklar" (Milanovic, 2011).

İnsan haklarına yönelik dokunulmazlık uygulaması, devletlerin kendi sınırlarının ötesinde de insan hakları olan yükümlülüklerini genişletmesini gerektiğini savunan bir konsepttir. Birçok ülke, insan hakları dokunulmazlık uygulaması yükümlüğüne direnirken hukuk bilginleri (Milanovic, 2011) ve Birleşmiş Milletler İnsan Hakları Konseyi (La Rue, 2013), dokunulmazlık uygulamasının bazı formlarını en azından kabul etme eğilimindedirler. Birleşmiş Milletler Özel Raportörü La Rue, kendi raporunda "Bir dizi devlet, dokunulmazlık uygulaması üzerinde yetki iddiasında bulunmak için ya da yabancı ülkelerdeki iletişimi kesmek için çıkartılan yasaları benimsemeye başlamıştır. Bu çıkartılan yasalar, insan hakları dokunulmazlık uygulaması ile ilgili ciddi kaygılara yol açmaktadır ve bireyin dış gözetiminin bir objesi olup olmadığını bilmesini olanaksız hale getirmektedir" (La Rue, 2013) noktasına değinmektedir. Sonuç olarak devletlerin ve özel sektörün kendi vatandaşlarının dijital haklarını diğer yabancı devletlerin bireylerinin dijital hakları ile eşit şekilde tamamıyla evrensel şekilde ele alacağına ummaktan başka bir çıkar yolu gözükmüyor (Bowden, 2013).

4.6 Uluslararası Politikalar Tarafından Organize Edilen Teknik Çözümler

Güçlü şifreleme aktivistleri, araştırmacı gazetecileri ve araştırmacıları, hassas iletişimi koruma olanağı sağlar. Ancak sıklıkla bu şifrelemeli iletişimin, geniş bir popülasyon tarafından kullanılabilmesi noktasında hantal kaldığı söylenmektedir. Şifrelemeyi dünyadaki tüm kullanıcılara ulaşılabilir hale getirmek, mühendisler ve özel sektörü bu şifrelemeyi internet protokollerinde, yazılımlarda ve donanımlarda standart hale getirmeye motive etmektedir.

Bununla birlikte istihbarat topluluğunun arasında endişeler olmuştur çünkü şifrelemenin kullanımındaki artış bazı durumlarda istihbarat çabalarına engel olabilir. Bu argüman şunu iddia etmektedir; güçlü uçtan uça şifrelemenin kamu tarafından fazla kullanılması istihbarat servislerinin işlerini yapma noktasında yeteneklerinin sınırlandırılması riskini doğurmaktadır (Yadron, 2015). Bu argümana rağmen, bununla benzer ulusal güvenlik politikaları hakkında yapılan birçok tartışmada bu iddiayı doğrulayacak çok az ampirik kanıt vardır. Buna karşılık yapılacak olan kamunun bu tarz şifreleme araçlarına erişimini kısıtlamak veya bu tarz teknolojilerin için bir arka kapı yerleştirmek eylemlerin kusurlu tasarımdan ötürü kaçınılmaz olarak istismar edilecektir (Bauman et al., 2014; Greenwald, 2014; Johnson, Maillart, & Chuang, 2014). Şifreleme sistemi kullanmaktan daha güzeli ise mutlak olarak hedeflenen gözetimin ortadan kalkması, gerekli olmamasıdır fakat bu şifrelemeler kitlesel gözetimi daha zor ve daha pahalı hale getirmektedir. Son olarak not edilmelidir ki, şifreleme üzerine olan tartışmalar yeni bir fenomen değildir fakat bu tartışmalar yıllardan beri devam etmektedir ve edecektir.[17]

5 Avrupa Birliği Eylemleri ve Politikaları ve Bunların Etkileri

Geçtiğimiz yıllarda Avrupa Birliği internet ve insan hakları sorunu ile ilişkili sayısız önlem almıştır. 2011 yılındaki Arap Baharı ve 2013 yılındaki Snowden sızıntıları ile beraber internet ve insan hakları sorununun önemi büyümüş, bu sorunlar artan bir şekilde siyasi ilgiye liderlik etmiştir.

5.1 Avrupa Birliği'nin Dış Politika Girişimleri

2014 yılında yayınlanmış olan *Düşüncenin Çevrim içi ve Çevrim dışı Dünyada Özgürce İfade Edilebilmesi Üzerine Avrupa Birliği İnsan Hakları Yönergeleri,* Avrupa Birliğinin dış politikasında dijital iletişimin öneminin farkında olduğuna dair bulguları gösteren önemli bir adımdı. Başlık, en açık ifade ile ifade özgürlüğüne odaklanırken içerisindeki yönergeler gizlilik, gözetim ve hatta AB kamu diplomasisi konularını genişletmiştir. Bu yönergelerde finansal araçlar üzerine olan bir husus özellikle önemlidir. Bu finansal araçlar üzerine olan husus açıkça "Avrupa Birliği'nin uygun olan tüm dış finansal araçları düşüncenin özgürce ifade edilebilmesinin daha fazla korumak ve teşvik etmek ve düşüncenin ifadesinin hem

17 http://openpgp.vie-privee.org/gilc-wass-fr.htm

çevrimdışı hem de çevrim içi alanda özgür, farklı, bağımsız medyanın ortaya çıkmasını destekleyen bir yapı"[18] içerisinde kullanılması gerektiğini söyler. Bir diğer önemli mekanizma ise Demokrasi ve İnsan Hakları İçin Avrupa Belgesi'dir (EIDHR) ve bu küçük bağış mekanizması önemli tehditlerle yüzleşen bireyler için kurulmuştur.

Daha da önemlisi Avrupa Parlamentosu 2012 yılında Avrupa Birliği dış politikası içindeki dijital özgürlük stratejisi kararını kabul etmiştir. Bu kararda "dijital özgürlüğe yönelik koruma ve teşvik etme ana akım olmalıdır" ve "otoriter rejimlere yönelik baskıcı teknolojilerin ihracatını ve hizmetini yasaklama"[19] fikirleri açıkça vurgulanmaktadır. Avrupa Parlamentosu tarafından dış ilişkileri şiddetli şekilde etkileyen bir başka kararda, NSA gözetlemesinin bir sonucu olarak alınan teröristlere ait finans verilerinin takibinin içeren SWIFT Antlaşmasının askıya alınmasıdır. Avrupa tarafından yapılan birçok güvenlik taahhüdü NSA'in geniş gözetim uygulamaları sonrasında sorgulanmaya başladı. Bu kararlar aynı zamanda Avrupa'nın Avrupa ile Amerika arasındaki veri paylaşımını sınırlamak için somut adımlar atmaya hazırlandığının önemli bir sinyalidir ve Avrupa parlamentosunun 4 Temmuz 2013'te ve 12 Mart 2014'te aldığı kararlar bu somut adımlar eşliğinde değerlendirilmelidir. Bu iki karar, NSA gözetlemesine ve bu gözetlemenin Avrupa Birliği vatandaşlarının bireysel haklarına yönelik etkisine odaklanmıştır.

Bu alınan kararlardan ikincisi özellikle Avrupa Birliği üyesi ülkelerdeki gözetim organlarına dikkat çekmeye ve bu organlara yönelik "Avrupa Dijital İhzar Emri" uygulamaya çağırmıştır. Bu kararlar aynı zamanda Avrupa Birliği tarafından yapılan "Güncel boşlukların giderildiğine yönelik tam bir inceleme yapılana kadar güvenli limanları kapatın" diyen geniş kapsamlı eylem planını da içerir. Bu karar ile "Avrupa Dijital İhzar Emri"nin hangi sonuca sahip olduğu görülecektir.

Avrupa Parlamentosu ayrıca kitlesel gözetimin verdiği zararların yanında gizliliği ve dijital hakları vurgulamak için düzenli olarak oturumlar ve etkinlikler organize etmektedir. Avrupa Parlamentosu gizlilik ve veri koruması üzerine güçlü bir vurgu koyarak gizliliğin Avrupa içinde ve dışında internet ve insan hakları üzerine tartışılması gereken anahtar konulardan biri olduğunu[20] noktasında kendisine pozisyon alır.

Mayıs 2015 yılından yayınlanan yeni *Avrupa Birliği Evrensel Dijital Stratejisi* nihayet an itibariyle Avrupa Komisyonu bünyesinde tartışılmaktadır. İnsan hakları temelli yaklaşıma sıkıca gömülmüş bir küresel strateji uygulanmasında önemli bir kök görevi görecektir.

Türkmenistan ve Çin gibi ülkeler Avrupa Birliği'nin insan hakları diyaloglarındaki dijital içerik üzerine insan haklarına endişelerine yönelik sıklıkla adres gösterdiği bir diğer alandır. Bu ülkelerin bu politikalarını sadece bu politik susturucu eşiğini sağlamak için kullanacağı gerçeğinin yanı sıra bu tarz mekanizmaların yararına hakkında bazı endişeler vardır (Boonstra & Laruelle, 2013; K. Hoffmann, 2010;Kinzelbach, 2014).

Avrupa Birliği Konseyi'nin internet yönetimi üzerindeki "insan hakları ve demokratik değerlerini" (16175/14) açıkça vurguladığı ve "İnsan haklarının evrensel anlamda teşvik edilmesi için internet bir araç olabilir" (16200/14) şeklindeki önerisinin yanı sıra "Çevrim içi insan haklarının korunması ve teşvik edilmesi" de aynı zamanda ABD ve AB arasındaki siber diyaloğun memnuniyet verici şekilde geniş kapsamlı bir parçasıdır. Bununla birlikte, *İnternet ve İnsan Hakları Bilgisi'*ni, Avrupa Dış Eylem Servisi (EEAS) çalışanları için kaynaştıran eğitim programının yanı sıra, yaklaşan diplomatik sonuçlara siber insan haklarını eklemek önemlidir.

Avrupa Birliğinin dış politika stratejisi için önemli bir buluşma yeri de Avrupa Komşuluk Politikası (ENP) ve genişleme müzakereleridir. Avrupa Komşuluk Politikasına yönelik

18 http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf

19 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//EN

20 http://www.europarl.europa.eu/news/en/news-room/content/20150116IPR09941/html/Committee-on-Human-Rights-meeting-21-01-2015-15001630

istişareler mevcut Avrupa Komisyonu tarafından komşu olan 16 ülkede insan temelli yaklaşımı dijital alanda teşvik etmek için bir fırsat olarak görülmüştür. 2014 ve 2020 yılları arasında 15,4 milyar bütçe ile Yeni Avrupa Komşuluk Aracı (ENI) demokrasi ve insan haklarına saygı yolunda ülkelerin ilerlemesini teşvik tabanlı yaklaşım ile sağlayacaktır. İnsan haklarının dijital alana uygulanması bu ilerlemenin ölçüsünde önemli bir kriter olabilir ve olmalıdır.

Bosna Hersek ve Kosova gibi Avrupa Birliğine girmek için müzakere sürecine aday olan ülkeler ve İzlanda, Arnavutluk, Makedonya, Sırbistan, Karadağ ve Türkiye gibi Avrupa Birliğine üye olmak için müzakere sürecinin devam ettiği ülkeler Avrupa Birliğinin insan hakları temelli yaklaşımı teşvik etmesi için potansiyel mekan olabilirler. Katılım öncesi yardım aracının ikinci sürümü (IPA II) 2014 ve 2020 yılları arasında demokrasi, yönetişim ve hukukun üstünlük alanlarının geliştirilmesi için sahip olduğu 11,7 milyar Euroluk bütçeyi dijital haklar bileşenlerini geliştirme alanını da dahil ederek kapsamalıdır.[21] Gelecek yıllarda müzakereler ortaya çıktıkça Avrupa Birliği, müzakerelerin çerçevesini ve bu müzakereci ülkelerde dijital alandaki insan haklarına yönelik sorunlarını adres göstermek için açıkça insan haklarını referans alan "Kopenhag Kriterlerini" kullanabilir.

5.2 Avrupa Birliği İçindeki Dijital Haklar Stratejileri

Avrupa içerisindeki dijital hakları yönetecek ana mevzuat, 2009 yılında imzalanan Lizbon Antlaşması ile devreye giren "Avrupa Birliği Temel Haklar Bildirgesi"dir. Bu bildirge Avrupa Birliği'nin dijital haklar dair pozisyonuna bir temel sağlar. Avrupa Adalet Divanı'nın 2014 yılında aldığı kararla "Avrupa Birliğinin Veri Saklama Direktifini"[22] geçersiz sayması alınan bu pozisyon sayesinde olmuştur. Bu bildirgenin ötesinde, örneğin Avrupa Komisyonu tarafından yayınlanmış "Avrupa Birliği Çevrim içi Haklar Kanunu" gibi yumuşak hukuksal önlemler de vardır. Bu haklar, Avrupa mevzuatında temel tüketici hakları odaklı iken, aynı zamanda Avrupa Birliği üye ülkeler arasındaki farklı politik alanları ve uyumu yönelik geçişi nasıl kolaylaştırabileceği meselesinde bir örnek olarak sunulmaktadır.[23]

Avrupa'daki dijital haklar sorunu üzerine en önemli, anahtar yasama girişimlerinden biri veri koruma çerçevesi reformudur. Bu reform hali hazırda hala tartışma aşamasındadır fakat sunduğu çözüm, Avrupa Parlamentosu'nun 12 Mart 2014 tarihinde aldığı kararla benimsenmiştir. Avrupa Parlamentosu'ndaki milletvekilleri, dijital alanda gizliliğin korunması için yasal çerçevenin adapte edilmesinde istekli rol oynamış ve karar alınmıştır. Yeni Avrupa Birliği Genel Veri Koruma Yönetmeliği içerisindeki bireyin kişisel verilerini kaldırma hakkı veya yönetmeliğin ihlalleri karşısında bireysel ve kolektif dava hakkı gibi spesifik öğeler hakkındaki kamu tartışması insan haklarına yönelik anlatının kaymasını desteklemektedir. Halihazırda bu tartışma, "gizliliğin ne olduğu ve veri koruma yönetmeliğinin dijital alandaki insan haklarını korumak için nasıl kullanılabileceğin" konusundaki uluslararası anlayışa önemli ölçüde katkıda bulunmuştur. Bununla birlikte düzenlemenin nihai şekli ve Avrupa dışındaki düzenleyici çerçeveler üzerindeki muhtemel etkisi henüz gözlenmeyi bekliyor.

Veri koruma reformunun çerçevesi üzerine olan tartışmalarla paralel olarak, ayrıca birlik genelinde bilgi güvenliği (NIS) ve ağ içerisindeki ortaklığın yüksek kalması konularında tedbir alınmasına sağlayacak yeni bir Avrupa Birliği yönergesi üzerine tartışmalar sürmektedir. Bu yeni direktifin hedefi özel ağlar ve bilgi sistemleri ile internetin güvenliğini geliştirmektir. Bu hedefle birlikte üye devletlerin operatör gerektiren kritik altyapılarındaki hazırlıklarını arttırmak ve birbirleri ile kurdukları iş birliğini geliştirmek, ulaşılmaya çalışılan şeydir.

Bu yeni direktifin önerisine Avrupa Komisyonu ve Yüksek Temsilci Catherine Ashton tarafından tasarlanmış Avrupa Birliği Siber Stratejisi eşlik etmektedir. Avrupa Birliği tarafından 2013 yılı içerisinde benimsenen "Avrupa Birliğinin Siber Güvenlik Stratejisi: Açık, Güvenli ve Sağlam Siber Alan" siber sorunların adalet, iç işleri ve dış politika yönlerini ele alan Avrupa Birliği içerisindeki ilk kapsamlı AB politika belgesidir.

21 http://ec.europa.eu/enlargement/instruments/overview/index_en.htm
22 http://www.loc.gov/law/help/eu-data-retention-directive/eu.php
23 http://ec.europa.eu/digital-agenda/en/code-eu-online-rights

Bireysel Haklar, Avrupa Birliği Temel Haklar Şartı'nda benimsenen hukukun üstünlüğü ve demokrasiyi vurgulayan strateji siber alanda korunmaya ihtiyaç duymaktadır. Bu strateji aynı zamanda "artan küresel bağlantının sansürü veya kitle gözetimini barındırmaması[24]" gerektiğini açıkça belirtmektedir. Ancak, "Siber" ve "Güvenlik" terminolojisi kelimelerin sivil bileşenini vurgulamak yerine dijital iletişimi militarize etmeye ve teminat altına almaya hizmet etmektedir. Dijital haklar ve ulusal güvenlik arasındaki görünür bir gerilim varken, Avrupa Parlamentosu, Komisyon, Konsey ve üye devletler mümkün olan her yerde bu terminolojiyi kullanmaktan kaçınmalıdır, çünkü bu terminoloji, internete yönelik "küresel ortak iyi" bakışını "askeri savaş alanı olarak internet" görüşüne kaydırır. Hatta internet hakkındaki bazı askeri söylemler dijital soğuk savaşa yol açabilir (Mueller, 2013)

Söylemlerden stratejilere doğru yola çıkarsak DG CNECT'deki emekli komiser Kroes tarafından geliştirilmiş *Bağlantıda Kalma Stratejisi,* "İnsan haklarını ve temel hakları güvence altına alacak AB taahhüdüne hem çevrim içi hem de çevrim dışı olarak saygı duymayı ve internet ile diğer iletişim ve enformasyon teknolojilerini siyasi özgürlüğün, demokratik gelişmenin ve ekonomik büyümenin sürücüsü olarak kalmasını desteklemeyi"[25] amaçlamıştı.

Strateji hakkında yapılan ilk tantananın aksine, strateji üzerinde çok az ilerleme kaydedilmiştir. Birkaç somut sonuçtan biri ise durum farkındalığına yönelik Avrupa'nın kapasitesini (ECSA) ölçmek için yapılan fizibilite çalışmasıdır. Bu fizibilite çalışması Avrupa Komisyonuna yapılan dijital hak ihlallerine hakkında daha iyi bilgi sağlamaya yönelik çalışma olarak görülebilir. Bu fizibilite çalışması halen devam ediyor olsa da böyle bir platformun gerçekten geliştirilebileceğine yönelik belirsizlik hala korunuyor.

Yeni bir Avrupa Komisyonunun geçtiğimiz günlerde atandığı göz önüne alındığında, yeni iki Başkan Vekili Andrus Ansip ve Federica Mogherini'nin bu konu hakkındaki nasıl bir iş birliği yapacaklarını görmek önemli olacaktır. İnsan hakları ve dijital politika üzerine Avrupa Birliğinin değişik stratejik elementleri, düşüncenin çevrim içi ve çevrimdışı dünyada özgürce ifade edilebilmesi üzerine Avrupa Birliği İnsan Hakları yönergeleri, bağlantıda kalma stratejisi, ECSA ve Avrupa İhracat Kontrol Politikasının incelemesi birbirlerine daha iyi entegre edilirler ise şüphesiz şekilde yararlı olacaktır.

Son olarak internete ve insan haklarına yönelik hakları sağlarken AB üyesi ülkeler, bu haklara yönelik yaptıkları ihlaller için eleştiriliyorken AB'nin güvenilirliğinden daha genel bir sorun vardır. Örneğin Macaristan'ın yeni medya yasalarını analiz edersek: İnsan Hakları İzleme Örgütü bu yasaları yargı ve medyaya zarar verici olarak nitelendirmiştir (HRW 2014). Diğer örnek ise "Beş Göz"ün ittifakında İngiltere'nin öne çıkan rolüdür (Nyst & Crowe, 2014). Burada Avrupa Birliği ve üye devletler için mücadele, iç politika ile dış politikalar arasındaki uyumun geliştirilmesi olmalıdır. AB üyesi ülkeler için AB dışındaki ülkelerde aynı eleştiriyi alıyorken önemli insan haklarını ihlal etmesi çok zor bir durumdur.

Avrupa Birliği, evdeki problemleri düşünerek bu alanlardaki güvenilirliğini geliştirmelidir. Yine de bazı üye devletlerin insan haklarına yönelik politikaları zorlu olabilir. Bu koşullar Avrupa Birliği'nin insan haklarının ileriye doğru geliştirilmesine yönelik çabasını engellememelidir. Avrupa Birliği bunun yerine, tutarlı bir dış politika altında yaşamak için dış politikada hak temelli bir gündemi takip etmeli ve bu amaca yönelik çabasını arttırdığından emin olmalıdır.

5.3 Avrupa Birliğinde İhracat Kontrolleri: Wassenaar Anlaşması ve Ötesi

Avrupa Birliği gözetim teknolojilerinin yönelik ihracat kontrolleri alanında özellikle aktiftir. Aralık 2011'de, Suriye gözetim teknolojisi ihraç eden bir Avrupa konsorsiyumuna yönelik medyada çıkan geniş rapor(Elgin & Silver, 2011) nedeniyle Avrupa Konseyi, internet ve telefon iletişimin izlenmesi ve kullanılması amaçlanan yazlım ve ekipmanların ticaretini önlemek için Suriye'ye yönelik mevcut yaptırımlarını güncelledi.

24 http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf
25 http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en

Bu tarihte Avrupa Birliği Suriye ve İran hedef alan yaptırımlarını sadece gözetleme teknolojisini dahil etmiştir, diğer kısıtlayıcı tedbirleri dışarda bırakmıştır. Avrupa Birliği ayrıca Belarus, Fildişi Sahili, Gine Cumhuriyeti, Libya, Myanmar ve Zimbabve gibi ülkelerin bu tarz teknolojik gözetim araçlarının iç baskı yöntemi olarak kullanılabileceği endişesi ile önlem olarak bu ülkelere bu ekipmanların ihracını yasaklamıştır.

Bu sorunların çoğuna cevaben, Avrupa Birliği üyesi ülkeler Wassenaar Düzenlemesi üzerindeki gözetim teknolojilerine yönelik güçlü yönetmeliğin ana savunucularından bazıları olmuşlardır. Bu değişiklikler hiçbir şekilde mükemmel olmamakla birlikte gözetim teknolojileri ihracatının düzenlenmesine yönelik önemli bir ilk adımdır (Maurer, Omanovic vd., 2014). Avrupa Birliği düzeyinde bu gelişmeler, "kitle gözetimi, izleme, takip etme ve engelleme için siber araçlar"ın açıkça tartışıldığı regülasyon olan *Avrupa İhracat Kontrol Politikasının İncelemesi'*nde desteklenmiştir.

5.4 Avrupa Birliği Ortakları ile Ticaret ve Yatırım Görüşmeleri

Avrupa Birliği açısından ticaret ve dijital haklar üzerine devam eden bir tartışma vardır ve bu tartışmalarda insan haklarına politikasına yönelik yapılması gereken güncelleme beklentileri ve fiili anlaşmalar arasındaki fikir ayrılıkları açıkça gözükmektedir. Bu durum özellikle Avrupa Birliği ve Amerika Birleşik Devletleri arasındaki güvenli liman antlaşması, Transatlantik Ticaret ve Yatırım Ortaklığı anlaşması ile Ticaret Hizmetleri Anlaşmasına yönelik saygıda kendini göstermektedir.

Yapılmış olan 50 ticaret antlaşması ile beraber şu anda çok daha fazla antlaşma anlaşma aşamasındadır, Avrupa Birliği, ortak ülkelerdeki insan haklarının korunmasını teşvik etmek için ikili yatırım anlaşmalarını kullanarak iyi konumlandırılmıştır. İnsan hakları üzerine esas temayüllerin uygulanması *Tercihlere Yönelik Avrupa Birliği Genelleştirilmiş Şema* (GSP+) altındaki ek ticaret teşvikleri ile ödüllendirilebilir. Bu şema, *Medeni ve Siyasal Haklar Uluslararası Sözleşmesi* ve 26 temel temayülün uygulanmasını içermektedir ve bu sayede Ermenistan, Bolivya, Yeşil Burun Adaları, Kosta Rika, Ekvator, El Salvador, Gürcistan, Guatemala, Moğolistan, Panama, Paraguay, Pakistan ve Peru gibi GPS+ ülkelerindeki dijital hakların güçlendirilmesine ve teşvik edilmesine önemli ölçüde katkıda bulunabilir. İnsan Haklarını korumak ve teşvik etmek için bir yöntem olarak sürdürülebilirlik ve iyi yönetişim kriterlerinin GSP+ sözleşmelerinde uygulandığından emin olmak gerekmektedir. Örneğin Pakistan internet ve telekomünikasyon ağlarının bağlantısını kesmede uzun bir geçmişe sahiptir ve Avrupa Birliği veya Avrupa Birliği'nin insan haklarına yönelik özel temsilcisinin GSP+ ile uyum açısından Pakistan hükümeti ile bu konunun konuşup konuşulmadığı henüz belli değildir.

İnsan Hakları aynı zamanda Avrupa Komşuluk Ortaklığı'nın (ENP) ve Afrika, Karayip ve Pasifik ülkeleri ile yapılan Cotonue Anlaşması'nın da temelini oluşturmaktadır. Sonuç olarak, AB ortaklığına şeffaflık ve halkın katılımı ve kamu istişareleri, sivil toplum diyaloğu ve sürdürülebilirlik etki değerlendirmesi yoluyla ticaret müzakereleri, ortak ülkelerdeki dijital hakların ihlalleriyle ilgili endişeleri dile getirmek için bir platform olarak kullanılmalıdır.

6. Fikirleri Tartışmak ve İleri Götürmek için Alan

Öncelikle belirtmek gerekir ki insan haklarına yönelik geniş bir yaklaşıma ihtiyaç vardır. Sansür ve gözetim üzerine yöneltilen açık odak, birbiriyle eşit alakalı birçok insan hakları yaklaşımını maskelemektedir. Biz insan hakları yaklaşımına ek örnekler sunmaya teşebbüs ederken bu çalışmada sansür ve gözetime yönelik açık odaktan etkilenmektedir. Tartışmanın odağını genişletme ve etkilenen diğer birçok insan hakkını göstermek hala devam eden bir sorundur ve mücadeledir. Dijital hakları bütün sektörlerde ana akım haline getirmek kaçınılmaz demektir çünkü gelişen dijital teknolojiler ile beraber bu gelişimden etkilenmeyen hiçbir insan hakları alanı kalmamıştır.

Önceki yaptığımız analizlerin ışığında Avrupa Parlamentosundaki insan hakları ile alakalı DROI alt komitesine şu önerilerde bulunuyoruz:

1. Avrupa Birliği üçüncü dünya ülkelerindeki insan haklarını koruma ve teşvik

etmeye yardımcı olmak için, ulusal mevzuatlarını geliştirmede teknik asistanlık ve kapasite inşası sunarak ilerlemeye teşvik etmelidir. İnsan haklarına yönelik olarak yapılan birçok tartışma uluslararası anlatmalara odaklanmışken, bu tartışmalar yasal ulusal çerçevenin yerine geçemez. Ayrıca, Avrupa Birliği üye ülkeleri yasal dinleme, mahremiyetin korunması ve siber alanda hukukun üstünlüğünün korunması gibi alanlarda insan hakları temelli mevzuat modeli geliştirmeli ve dünyanın çevresindeki partnerleri ile bu modelleri paylaşmalıdır.

2. Dijital hakların her alanına yönelik hesap verme sorumluluğunu güçlendirmelidir. Açık bir şekilde hesap sorulamaması anlamı, bireylerin kamu aktörlerinin yerine gizliliği korumak için sıklıkla yeni yollar araması gerekir. Maliyetleri ya da idari yükleri azaltmak için bastırmak insan hakları için ödün vermeyi haklı kılamaz. Avrupa Birliği, Avrupa İnsan Hakları Sözleşmesi (ECHR) ve Avrupa'nın içindeki veya dışındaki diğer ilgili adli yetkililerin önünde, gizlilik ihlali ve diğer dijital hak ihlalleri için daha iyi bireysel hata telafi ve temyiz mekanizmasını desteklemelidir.

3. Özel sektör şirketlerinin ve hükümetlerin şeffaflıkları geliştirilmelidir. Avrupa Birliği, algoritmalar ve kurumlar[26] için daha büyük şeffaflık talep etmeli ve dijital teknolojilerin insan haklarını nasıl şekillendirdiği hakkında önemli bilgilere erişimi olduğundan emin olmalıdır. Bu bilgilerin çoğu, akademilerde, gazetecilerde, genel kamuoyunda ve hatta ilgili kamu düzenleyicilerin elinde yoktur ve bu nedenden ötürü etkili bir şekilde değerlendirilemez.

4. Kapsamlı dijital politikaların ve stratejilerin taslağı çizilmelidir. Bu dijital politika ve stratejiler bazı kapsamları ile hali hazırda yürütülüyor olmasına rağmen, taslağın "dijital bileşeni" Avrupa Birliği'nin bütün ileriye dönük stratejilerine veya politikalarının içine kaynaştırılmalıdır. Böylece politikaların insan zihninde insan hakları temelli yaklaşım ile hizmete alındığından emin olunur. Avrupa Komşuluk Ortaklığı (ENP) ve Avrupa Birliği Kalkınma İş Birliği özelinde dijital haklar bir büyük odaktan yararlanabilir.

5. Avrupa Birliği ve Latin Amerika devletleri arasında dijital haklar konusundaki stratejik iş birliği derinleştirilmelidir. Brezilya, Almanya ve yeni Avrupa-Latin Amerika internet kablosunun "Gizlilik Çözümü" önemli bir ilk adım oluyorken, potansiyel iş birliğinin geliştirilmesi için araştırılması gereken birçok ek alan vardır. Bu alanlar iki kıta arasında ticaret ve araştırma yapılması için güçlü iş birliğini içermenin yanı sıra, Avrupa ve Latin Amerika ticaretin geliştirilmesi, veri koruma ajansları, diplomatik ilişkiler ve adli yetkililerde bu geliştirilmesi gereken iş birliğinin içindedir.

6. Dijital haklar sorunlarına dair Avrupa Birliğinin uluslararası politika oluşturma kurumsallığı ve özellikle Avrupa Birliğinin dünya çapındaki misyonu ile beraber daha fazla kurumsal bilgi birikimi üretin. Avrupa Birliği görevi içindeki insan hakları iletişim noktaları için düzenli dijital haklar eğitimi zorunlu hale getirilmelidir. Buna ek olarak görevler ve müdürlükler ülkelerdeki ve durumlardaki güvenli iletişime izin vermek için yetkili olmalıdır, bu yetki bireylerin güvenliği için hayati olabilir.

7. İnsan hakları ve teknoloji üzerine bağımsız kapsamlı araştırmaları teşvik etmek için bu alanlarda Avrupa araştırma iş birliğini daha da güçlendirmek. Özel sektör iş birliği memnuniyetle karşılanıyorken bu alandaki araştırmalar için kurumsal finansman üzerine mevcut muazzam güven üretilmekte olan araştırmaların kalitesi ve bütünlüğü ile mücadele etmektedir.

8. "Siber" kelimesini askeri anlamından arındırmak. İnsan haklarına yönelik anlatının kayması, Avrupa Birliğinin açık bir şekilde internet politikaları ve

26 https://cihr.eu/the-ethics-of-algorithms/

stratejilerini askeri boyuttan indirip sivil boyuta odaklaması ile sağlanabilir. Bu boyut, Avrupa Parlamentosunun insan haklarında siber güvenliğin ana merkez olmadığından emin olmak zorunda olacağı yaklaşan Avrupa Birliği Küresel Dijital Stratejisi için özellikle önemli olacaktır.

9. Ticaretteki insan hakları yönlerini, uluslararası ticaret anlaşmaları ve Avrupa Birliğinin ticaret politikasının kabulünü garantiye almak için anahtar mekanizma olarak ileriye sürmelidir. Bu ileri sürme, gözetim teknolojileri hakkında ince ayarlanmış mevcut ihracat kontrollerini içermektedir. Avrupa Birliği GSP+ ticaret çerçevesi ile beraber daha güçlü bir dijital haklar değerlendirme mekanizmasını teşvik etmenin yanı sıra insan haklarını vurgulayan başrol oyuncusu olmaya ihtiyaç duymalıdır.

10. İnsan haklarını arttırıcı teknolojileri, özellikle Wassenaar düzenlemesi içinde uluslararası ve ulusal seviyede şifreleme teknolojilerinin hükumet kontrolünden kurtulmasına yardım ederek desteklemelidir. Aynı zamanda Avrupa Birliği vatandaşları tarafında kullanılan güvenli iletişiminin fonksiyonel, kolay kullanılır ve daha iyi anlaşılır olmasını sağlamak için bu alana yönelik olarak daha fazla araştırmaya ve eğitime ihtiyaç vardır.

11. Avrupa Birliği, üye ülkelerini Birleşmiş Milletler İnsan Hakları Komitesindeki gizlilik hakkı ile alakalı olan 17. maddeye yeni bir genel yorum getirmek için çaba harcamaya teşvik etmelidir. Bu yeni yorumla beraber, uluslararası yasalara yönelik yorumların dijital çağ ile bağlantısı sağlanmaya çalışılacak ve gizlilik hakkı açısından sorumluluğun netleştirilmesine yardımcı olacaktır. Diğer bir yandan benzer bir unsur, Avrupa Birliği üye devletleri gizlilik hakkına ilişkin Birleşmiş Milletler Özel Raportörü kurulmasını da desteklemelidir.

Kaynakça

Abboud, L., & Maushagen, P., Germany wants a German Internet as spying scandal rankles, Reuters, 2013. Retrieved March 05, 2015, from http://www.reuters.com/article/2013/10/25/us-usa-spying- germany-idUSBRE99O09S20131025

Arce, N., Cyber Attack Bigger Threat Than ISIS, Says U.S. Spy Chief. Tech Times, 2015. Retrieved March 06, 2015, from http://www.techtimes.com/articles/35965/20150227/cyber-attack-bigger- threat-than-isis-says-u-s-spy-chief.htm

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J., After Snowden: Rethinking the Impact of Surveillance. International Political Sociology, 8(2), 121–144. doi:10.1111/ips.12048, 2014.

Bennett, Colin J. Haggerty, K., Security Games: Surveillance and Control at Mega-Events (p. 208). Routledge, 2012.

Bequelin, N., Jailing of Ilham Tohti Will Radicalize More Uighurs - NYTimes.com, 2014. Retrieved January 14, 2015, from http://www.nytimes.com/2014/09/26/opinion/nicholas-bequelin-china- jailing-of-ilham-tohti-will-radicalize-more-uighurs.html?_r=0

Birnbaum, M., Russian blogger law puts new restrictions on Internet freedoms. Washington Post, 2014. Retrieved February 15, 2015, from http://www.washingtonpost.com/world/russian-blogger- law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2- 6d08598c375b_story.html

Boonstra, J., & Laruelle, M., EU-US cooperation in Central Asia: parallel lines meet in infinity? EUCAM Policy Brief, 2013.

Bowden, C., The US surveillance programmes and their impact on EU citizens' fundamental rights. Brussels, Belgium, 2013.

Cavelty, M. D., From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review, 2014.

Ctizen Lab. Morgan Marquis-Boire, Marczak, Bill Claudio Guarnieri, and J. S.-R., You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab, 2013. Retrieved January 09, 2015, from https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Culzac, N., Iranians behind Tehran version of "Happy" sentenced to six months in prison and 91 lashes - Middle East - World - The Independent, The Independent, 2014. Retrieved January 14, 2015, from http://www.independent.co.uk/news/world/middle-east/iranians-behind-tehran-version-of- happy-sentenced-to-six-months-in-prison-and-91-lashes-9741014.html

Deibert, R. J., Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. Millennium - Journal of International Studies, 32(3), 501–530. doi:10.1177/03058298030320030801, 2003.

Dunn Cavelty, M., Cyber-security and threat politics: US efforts to secure the information age, 2007.

Elgin, B., & Silver, V., Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear - Bloomberg. Bloomberg, 2011.

Epstein, G., Online and Off, Information Control Persists in Turkey. Electronic Frontier Foundation, 2013. Retrieved June 24, 2014, from https://www.eff.org/deeplinks/2013/07/online-and- information-control-persists-turkey

Feenberg, A., Questioning Technology (p. 264). Routledge, 1999. FIDH, Surveillance Technologies "Made in Europe". Regulation Needed to Prevent Human Rights Abuses,

Finn, P., Cyber Assaults on Estonia Typify a New Battle Tactic. Washington: Washington Post, 2007. Retrieved from http://www.washingtonpost.com/wp- dyn/content/article/2007/05/18/AR2007051802122.html

FOC, Freedom Online Coalition: Statement on the Use and Export of Surveillance Technology, 2014. Retrieved January 14, 2015, from https://www.freedomonlinecoalition.com/wp- content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance- Technology-October-2014.pdf

Freedman, L., Censorship and manipulation of family planning information: an issue of human rights and women's health. Health and Human Rights: A Reader, 1999.

Greenwald, G., No place to hide: Edward Snowden, the NSA, and the US surveillance state, 2014.

Hoffmann, B., Civil society in the digital age: how the Internet changes state-society relations in authoritarian regimes. The case of Cuba. In Francesco Cavatorta (Ed.), Civil Society Activism under Authoritarian Rule. A comparative perspective (pp. 219–244). London, New York: Routledge, 2012.

Hoffmann, K., The EU in Central Asia: successful good governance promotion? Third World Quarterly, 2010.

HRW, Hungary. Human Rights Watch, 2014. Retrieved January 06, 2015, from http://www.hrw.org/europecentral-asia/hungary

Jenkins, P. N., Turkey Lifts Two-Month Block on YouTube | TIME, 2014. Jiang, M., Authoritarian informationalism: China's approach to Internet sovereignty. Forthcoming in P. O'Neil. & R. Rogowski (Eds.), … 30(2), 71–89. doi:10.1353/sais.2010.0006, 2012.

Johnson, P., Maillart, T., & Chuang, J., Government Surveillance and Incentives to Abuse Power. In Workshop on the Economics of Information Security (WEIS). Pennsylvania State University, 2014.

Kinzelbach, K., The EU's Human Rights Dialogue with China: Quiet Diplomacy and Its Limits

(p. 236).

Routledge, 2014. Korff, D., Expert Opinion prepared for the Committee of Inquiry of the Budestag into the SEYES global surveillance systems revealed by Edward Snowden. Berlin, Germany, 2014.

La Rue, F., Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40). Geneva, 2013.

Lab, C., You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab, 2013. Lab, K., Syrian Malware, the ever-evolving threat, 2014.

LaFrance, A., Where Design Choices and Civil Rights Overlap - The Atlantic. The Atlantic, 2015. Retrieved January 14, 2015, fromhttp://www.theatlantic.com/technology/archive/2015/01/where- design-choices-and-civil-rights-overlap/384142/

LGBT Technology Partnership, Homosexuality, Internet Censorship and Silence » LGBT Technology Partnership, 2013. Retrieved February 15, 2015, from http://lgbttechpartnership.org/homosexuality-internet-censorship-and-silence/

Livingstone, S., Digital Media and Children's Rights. LSE Media Policy Project, 2014. Retrieved from http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and- childrens-rights/

Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J., Mapping Hacking Team's "Untraceable" SpywareMapping Hacking Team's "Untraceable" Spyware, 2014.

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J., For Their Eyes Only: The Commercialization of Digital Spying, 2014. Retrieved January 14, 2015, from https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

Marthews, A., & Tucker, C., Government Surveillance and Internet Search Behavior. SSRN Electronic Journal. doi:10.2139/ssrn.2412564, 2014.

Maurer, T., Morgus, R., Skierka, I., & Hohmann, M., Technological Sovereignty: Missing the Point?, 2014. Retrieved January 14, 2015, from http://www.gppi.net/fileadmin/user_upload/media/pub/2014/Maurer-et-al_2014_Tech- Sovereignty-Europe.pdf

Maurer, T., Omanovic, E., & Wagner, B., Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age. Washington D.C., 2014.

McCarthy, D. R., Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet. Foreign Policy Analysis, 2011.

McNamee, J., ENDitorial: Turkish censorship - Swedish built, by royal appointment » EDRi. edri, 2014. Retrieved July 14, 2014, from http://edri.org/enditorial-turkish-censorship-built-sweden- royal-appointment/

Milanovic, M., Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy (p. 276). Oxford University Press, 2011.

Mueller, M., Networks and States: The Global Politics of Internet Governance (p. 280). MIT Press, 2010.

Mueller, M., Are we in a Digital Cold War. Internet Governance Project. Syracuse, N.Y., 2013.

Mueller, M., & Wagner, B., Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance (No. 1). Internet Policy Observatory Working Paper Series, University of Pennsylvania, Annenberg School, 2014.

Nyst, C., & Crowe, A., Unmasking the Five Eyes' global surveillance practices. GISWatch. Johannesberg, 2014.

Pasquale, F., The Black Box Society: The Secret Algorithms That Control Money and Information (p. 319). Harvard University Press, 2015.

Pillay, N., The right to privacy in the digital age Report of the Office of the United Nations High

Commissioner for Human Rights, 2014. Retrieved January 09, 2015, from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en. pdf

Rahimi, B., The agonistic social media: cyberspace in the formation of dissent and consolidation of state power in postelection Iran. The Communication Review, 2011.

Reporters Without Borders [RSF], Press Freedom Barometer 2014, 2014. Rhoads, C., & Fassihi, F., Iran Vows to Unplug Internet. Wall Street Journal, 2011.

RSF. (2014a). Enemies of the Internet. Retrieved February 15, 2015, from http://12mars.rsf.org/2014- en/#slide2

RSF. (2014b). Press Freedom Barometer 2014.

Scott-Railton, J., & Hardy, S., Malware Attacks Targeting Syrian ISIS Critics. Citizen Lab, 2014. Retrieved January 08, 2015, from https://citizenlab.org/2014/12/malware-attack-targeting-syrian- isis-critics/

Tanriverdi, H., Bürgerkrieg in Syrien: Das Internet als Kriegswaffe - Digital - Süddeutsche.de. sueddeutsche.de, 2015. Retrieved January 06, 2015, from http://www.sueddeutsche.de/digital/buergerkrieg-in-syrien-das-internet-wird-als-kriegswaffe-eingesetzt-1.2289887

Tikk, E., Global Cybersecurity–Thinking About the Niche for NATO. SAIS Review, 30(2), 105–119, 2010.

Tufekci, Z., Algorithms in our Midst: Information, Power and Choice when Software is Everywhere. Proceedings of the 18th ACM Conference on Computer ..., 2015.

Van Eeten, M. J., & Mueller, M., Where is the governance in Internet governance? New Media & Society, 15(5), 720–736. doi:10.1177/1461444812462850, 2012.

Wagner, A. Ben, Digital Rights in Turkey, 2014. Retrieved January 09, 2015, from https://cihr.eu/digital-rights-in-turkey/

Watt, N., & Wintour, P., Facebook and Twitter have "social responsibility" to help fight terrorism, says David Cameron | World news | The Guardian. The Guardian, 2015. Retrieved March 05, 2015, from http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity- cyberattack-threat

Whitefield, M., Security concerns could cast a shadow on 2014 World Cup in Brazil | The Miami Herald, 2014. Retrieved January 09, 2015, from http://www.miamiherald.com/news/nation- world/world/americas/article1952843.html

Yadron, D., Obama Sides with Cameron in Encryption Fight - Digits - WSJ. Wall Street Journal, 2015. Retrieved February 12, 2015, from http://blogs.wsj.com/digits/2015/01/16/obama-sides-with- cameron-in-encryption-fight/

York, J. C., Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University, 2010.

Zalnieriute, M., ICANN's Corporate Responsibility to Respect Human Rights. London, 2015. Zalnieriute, M., & Schneider, T., ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values (pp. 1–49). Strasbourg, 2014.