SİBER UZAY VE İNSAN HAKLARI

***Anıl Cumali ÇOKBİLDİK**

Özet

Siber uzayda insan hakları mevzuatının en önemli parçaları, ifade, görüş, kişi özgürlüğü ve mahremiyet hakkıdır. İfade özgürlüğü, kişi güvenliği ve özgürlüğü, özel yaşamın gizliliği ve kişisel verilerin korunması sık sık ihlal edilen hakların başında gelmektedir. İletişim ve bilişim alanındaki teknolojilerin artmasına paralel bir biçimde ortaya çıkan bu güvenlik sorunları geç te olsa bilişim hukukuna yönelik adımların atılmasını sağlamıştır. Bu çalışmada sırasıyla insan hakları ve siber uzayın tarihsel gelişimi, siber uzay ve insan hakları ilişkisinin boyutları, siber uzayda ihlal edilen insan hakları ve bu hakların korunmasına yönelik atılan ulusal, bölgesel ve uluslararası çalışmalar incelenmektedir.

Anahtar Kelimeler: Siber Uzay, İnsan Hakları, Hukuk.

CYBERSPACE AND HUMAN RIGHTS

Abstract

The most important parts of human rights legislation are the right to expression, opinion, personality and privacy in cyberspace. Freedom of statement, personal security and freedom, private life and the protection of personal data are often violated. These security issues, which emerged in parallel with the increasing technology in the field of communication and information technology, made it possible to take steps towards information law in the late stage. This study examines the historical development of human rights and cyber space, the dimensions of cyber space and human rights relation, human rights violations in cyberspace, and national, regional and international studies on the protection of these rights.

Keywords: Cyberspace, Human Rights, Law.

GİRİŞ

Tarih boyunca teknolojide meydana gelen gelişmeler, insan yaşantısı üzerinde birçok değişime ve dönüşüme neden olmuştur. Özellikle 80'li yıllardan itibaren küreselleşme faaliyetlerinin hız kazanması ve teknoloji alanında yaşanan gelişmeler bu değişim ve

* Selçuk Üniversitesi Uluslararası İlişkiler Bölümü Yüksek Lisans Öğrencisi. Ulaşmak İçin: cokbildikanilcumali@gmail.com

dönüşümün daha hızlı bir biçimde gerçekleşmesine neden olmuştur. Enformasyon çağı olarak adlandırabileceğimiz bu çağa girişi sağlayan en önemli faktör ise internetin ortaya çıkması olmuştur. Bilgi ve iletişim alanında baş döndürücü bir hıza kavuşmamızı sağlayan internet sayesinde (küreselleşmenin de bir uzantısı olarak) sınırlar ortadan kalkmış bireylerin istedikleri bilgiye ulaşabilme kapasitesi artmıştır (Kıvılcım, 2013: ss.222-223).

İnternetin yaygınlaşması ile siber uzay dediğimiz sanal dünyanın sınırları ise kestirilemeyecek ölçüde genişlemiştir. Bugün, gündelik yaşantımızda farkında olmadan gerçekleştirdiğimiz çoğu işlem teknolojik gelişmelere ve internete bağlı olarak karşımıza çıkmaktadır. İnternet yaygınlaştıkça hız ve yoğunluk onu kullanan bireylere paralel bir biçimde daha da artmıştır. Bugün dar bir perspektiften bakıldığında online bir şekilde gerçekleştirdiğimiz alışverişler, eğitim ve sağlık hizmetleri, haberleşme ve iletişim faaliyetleri internetin hayatımızı kolaylaştıran unsurları olarak karşımıza çıkmaktadır (Ünal, 2009: ss.132-134).

Bilgi ve iletişim alanında yaşanan teknolojik gelişmelerin insanlık açısından birçok fırsatı beraberinde getirdiği bir gerçektir. Ancak bu gelişmeler birçok riski ve tehdidi de bünyesinde barındırmaktadır. Özellikle internetin bu kadar yaygınlaşması siber uzay dediğimiz alanda güvenlik sorunlarının ortaya çıkmasına neden olmuştur. Siber uzay, bir anda ortaya çıkan ve sınırları belli olan bir kavram değildir. Bir benzetme yapılacak olursa, evren gibi genişlemeye devam eden ve genişledikçe içerisinde birçok aktörün yer aldığı/alacağı ve eksileceği bir alan olarak düşünülmektedir (Bryant, 2001, s.142).

İnternet ağlarının yayılması ile birlikte siber alanda faaliyette bulunan aktörlerde birbirine daha çok bağlanmıştır. Bu nedenle bu alan sadece fırsatlardan ve kolaylıklardan herkesin eşit bir biçimde yararlandığı bir ortam olarak düşünülmemelidir. Kişisel verilerin çalınması, dolandırıcılık ve sahtekârlık faaliyetleri, özel hayatın gizliliğine yönelik ihlaller, tehdit ve şantaj, siber zorbalık, çocuk pornografisi, ahlak kurallarının ihlali, kiralık katil ilanları, insan kaçakçılığı, uyuşturucu tacirliği, terörist faaliyetler, şirket ve devletlerin stratejik ve gizli olan belgelerinin çalınması ve satılması gibi faaliyetler bu alanda karşımıza çıkan tehditlerden ve suçlardan bazılarıdır (Malhotra, 2016: ss.145-148).

Bu çalışmada: Siber uzay ve insan hakları arasında ilişkinin boyutları nelerdir? Siber uzayda insan haklarını korumak mümkün müdür? Siber uzayda ihlal edilen insan hakları nelerdir? Siber uzayda sahip olduğumuz hak ve özgürlükler nelerdir? Siber uzayda insan haklarını

koruma mekanizmaları var mıdır? Gibi sorulara cevap verilecektir. Ayrıca çalışmada insan haklarını merkeze alan bir yaklaşımla siber uzayda yer alan aktörler arasındaki işbirliğinin kısıtlı olmasının nedenleri analiz edilecektir. Bu soruların cevaplanması kapsamlı bir literatür taramasına, çalışmada adı geçen anlaşmaların ve sözleşmelerin incelenmesine, güncel gelişmelerin dikkate alınmasına, kronolojik sıralamaya, örneklendirme ve karşılaştırmaya dayanmaktadır.

1. İnsan Hakları ve Siber Uzay İlişkisi

İnsan Hakları ve Siber Uzay alanları arasındaki ilişkilerin daha iyi analiz edilebilmesi için tarihsel arka planlarını ve gelişmelerini incelemek gerekmektedir. Bu iki alan birbirinden bağımsız bir gelişim süreci gösterse de özellikle 90'lı yıllardan itibaren internetin yaygınlaşması ile birlikte etkileşim içerisine girmiş ve birbirlerini yakından ilgilendiren alanlar olmuşlardır. İnsan haklarının kökenleri siber uzay alanına göre daha eskiye dayanmaktadır. Bu nedenle öncelikli olarak insan haklarının tarihsel gelişimi incelenecek sonrasında siber uzay alanı hakkında tarihsel arka plan gelişmeleri ele alınacaktır.

1.1. İnsan Haklarının Tarihsel Gelişim Süreci

Yaklaşık 2500 yıllık bir geçmişi bulunan insan hakları, tarihsel süreçte önce düşünsel alanda yani filozofların felsefi bakış açılarında ve tartışmalarında ortaya çıkan, sonrasında ise sözleşmelerde, anayasalarda ve uluslararası anlaşmalarda yer alan bir kavram olarak karşımıza çıkmaktadır. Temel olarak ve basit bir ifadeyle insanın korunması gerektiği konusunda ortak kanıya dayanan değerler bütünü olarak ifade edilmektedir. İnsan Hakları kavramının II. Dünya Savaşı'ndan sonra Birleşmiş Milletlerin kurulmasıyla ortaya çıktığı ifade edilse de köken olarak Doğal Hukuk teorisine dayanmaktadır (Küçükali ve Akbaş, 2016: s.71).

Doğal Hukuk Teorisi, kurallarını tanrısal bir güç ya da akıldan alan, toplumlar tarafından oluşturulmayan, doğada kendiliğinden yer alan haklar ve evrensel ilkelerden oluşan, zamandan ve mekândan bağımsız, herkes için geçerli olan ilkeleri ifade etmektedir (Toku, 2004: s.236). Bu teorinin ortaya çıkmasında ve gelişiminde katkıda bulunan kişiler arasında Platon, Aristo, Cicero, Seneca, Confucius, Aquinas, Grotius, Locke, Hobbes, Rousseau gibi ünlü düşünürler bulunmaktadır. Örneğin, Aristo doğa için haklı olan her şeyin yasalara göre

haklı olmayabileceğini ifade etmiştir. John Locke insanın bazı haklarının sırf insan olmasından kaynaklandığını ve bu durumun toplumsal sözleşme öncesindeki doğal durumunda da geçerli olduğunu ileri sürmüştür. Hobbes ise insanın yaşamla birlikte doğal haklara sahip olacağını söylemiştir. Grotius ise insanın doğasında yer alan bir takım temel hakların bulunduğunu ve bu hakların evrensel ve değiştirilemez olduğu görüşüne sahiptir (Kılıç, 2015: ss.99-101).

İnsan hakları bir mücadelenin ürünüdür ve bu mücadele boyunca özgürlük, kölelik, bireyin hak ve ödevleri, ahlak felsefesi, toplumsal sözleşmeler gibi konular tartışılmıştır. Bu tartışmalar köleliğe başkaldırıdan, günümüzde tartışılan siber güvenlik, barış hakkı, çevrenin korunması, vicdani ret gibi kavramlara doğru genişlemiştir. Elbette ki bu değişim ve gelişmeler, hem yukarıda ifade edilen felsefi ve entelektüel gelişmelere hem de aşağıda ifade edilecek olan dünya tarihindeki bazı önemli olaylara bağlı olarak şekillenmiştir (Ünal, 1994: ss.50-52).

1.2. Birinci Kuşak Haklar

Tarihsel olarak bakıldığında insan haklarının gelişiminin genel olarak üç aşamada gerçekleştiği görülmektedir. İlk aşama 17. ve 18. Yüzyıllardaki gelişmelere bağlı olarak gerçekleşmiştir. Bu dönemde özellikle Avrupa'da Rönesans, Reform ve Fransız Devrimi'nin etkisi ile bireysel haklar, özgürlük, adalet, eşitlik kavramlarının geliştiği ve daha sık kullanıldığı görülmektedir. Yine toplumsal sözleşme teorileri ile birlikte bireylerin vazgeçilmez ve devredilmez hak ve özgürlüklerini koruma görevi devlete yüklenmiştir. Devlet eğer bu görevini yerine getiremez ise yapılan sözleşmenin ve devletin meşruluğu ortadan kalkacaktır görüşü benimsenmiştir. Böyle bir durumda halk direnme hakkını kullanarak devlete itaat etmeyecektir (Engin, 2014: ss.206-207).

Fransız Devrimi bu anlamda verilebilecek en iyi örnek olarak karşımıza çıkmaktadır. Devrim ile birlikte ilan edilen 1789 Fransız İnsan ve Yurttaş Hakları Bildirisi insan hakları açısından son derece önemli anlamlar ifade etmektedir. İngiltere'de 1215 Magna Charta ve Amerika Birleşik Devletleri'nde 1776 Bağımsızlık Bildirisi ulusal nitelikli bildirilerdi. Ancak Fransız Bildirisi sadece Fransız yurttaşlarını değil tüm insanlığı kapsayan evrensel bir nitelik taşımaktadır. Bu bildirideki haklar insanın nerede ve ne zaman yaşarsa yaşasın sırf insan olmakla sahip olduğu haklar olarak karşımıza çıkmaktadır. Bu bildiride yer alan haklar daha

çok birincil kuşak haklar olarak nitelenen haklar (yaşama ve özgürlük hakkı, düşünce ve ifade özgürlüğü, kölelik yasağı vb.) olarak karşımıza çıkmaktadır. (Rude, 2015: ss.25-26).

1.3. İkinci Kuşak Haklar

İkinci aşama 19. Yüzyılın ikinci yarısında sosyalist akımların düşüncelerine paralel bir biçimde şekillenmiştir. Bu dönemde ekonomik, sosyal ve kültürel hakların öneminin dile getirilmesi, sadece bireyin özgürlüğünün yeterli olmadığının anlaşılması ikincil kuşak hakların ortaya çıkmasında etkili olmuştur. Bu haklar aynı zamanda pratik açıdan devletin bireye yönelik bir hizmette bulunmasını ve sorumluluk almasını gerekli kılan haklar olarak görülmektedir. Çalışma hakkı, sendikal özgürlükler, grev ve toplu sözleşme hakkı, sosyal güvenlik hakkı gibi haklar bu kategoride yer almaktadır (Cıngı, 2009: ss.11-12).

Özellikle Marksizm akımı zamanın özgürlük anlayışını eleştirerek sadece birincil kuşak hakların yetersiz olduğunu ve bu anlayışın değiştirilmesi gerektiğini savunmuştur. Örneğin bireyin konut dokunulmazlığı hakkının olmasına karşın bir konutunun olmaması bu hakkı işlevsiz bırakmaktadır. Sosyal ve ekonomik yetersizlikler insan hak ve özgürlüklerinin kullanılabilmesine engel olmaktadır. Bu nedenle bu hakların kullanılabilmesi için devlet üstüne düşen görevleri yerine getirmelidir (Algan, 2007: s.48).

1.4. Üçüncü ve Dördüncü Kuşak Haklar

Üçüncü aşama ise 20. Yüzyılın ikinci yarısında insanın yaşadığı çevreye uyumlu ve barışık, doğal, kültürel, sosyal ve ekonomik bir bütünlük içinde olması görüşüne dayanarak ortaya çıkmıştır. Üçüncül kuşak haklar olarak ta ifade edebileceğimiz haklar bu dönemde ortaya çıkmış böylece ulusların sosyal, kültürel, ekonomik kaynaklarını korumaya ve gelecek kuşaklara aktarılmasına yönelik haklar belirlenmiştir. Bunların içinde barış hakkı, tarihsel kalıntıları ait oldukları yerde görebilme hakkı, gelişme hakkı gibi haklar yer almaktadır (Kaboğlu, 2011: s.227).

İnsan haklarının tarihsel aşamaları incelendiğinde son yirmi yıllık dönemde ortaya çıkan dördüncü kuşak haklar tartışmalarına da ayrı bir parantez açmak gerekmektedir. Bazı araştırmacıların siber uzay hakkı, farklı olma hakkı, bilimin kötüye kullanılmaması hakkı, engelli çocukların özel eğitimden yararlanması hakkı, oyun hakkı gibi hakları dördüncü kuşak

haklar olarak değerlendirdiği görülmektedir. Bazı araştırmacılar ise bu hakların da üçüncü kuşak haklar içerisinde yer aldığı, ayrı bir kuşak içerisinde değerlendirilmesine gerek olmadığı görüşünü savunmaktadır. Bu noktada önemli olan husus çalışmanın odak noktası olan siber uzayın üçüncü kuşak haklar içerisinde ya da dördüncü kuşak haklar içerisinde değerlendirildiğinde insan hakları ile etkileşim halinde olduğunun anlaşılmasıdır (Turhan, 2013: s.369).

İnsan hak ve özgürlüklerinin belirlenmesine yönelik bu aşamalar ulusal ya da uluslararası koruma mekanizmalarının ortaya çıkması ile anlam bulmuştur. Bu hak ve özgürlüklerin teminat altına alınması, ihlal edilmemesi bazı standartların belirlenmesi ile mümkün olmuştur. Dünyada insan haklarını korumak ve geliştirmek için atılan adımlara bakıldığında Birleşmiş Milletler ve Avrupa Konseyi'nin yapmış oldukları çalışmalar ön plana çıkmaktadır. BM ve Avrupa Konseyi nezdinde hazırlanan sözleşmeler ve bildirilerden bazıları şunlardır:

Birleşmiş Milletlerin çalışmaları arasında İnsan Hakları Evrensel Beyannamesi, Ekonomik Sosyal ve Kültürel Haklar Sözleşmesi, Soykırım Suçunun Önlenmesine ve Cezalandırılmasına Dair Sözleşme, Çocuk Haklarına Dair Sözleşme, İşkence ve Diğer Zalimane, Gayri İnsani ve Küçültücü Muamele ve Cezaya Dair Sözleşme vb. sözleşmeler bulunmaktadır. Avrupa Konseyi'nin çalışmaları arasında ise Avrupa Sosyal Şartı, İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme, Çocuk Haklarının Kullanılmasına İlişkin Avrupa Sözleşmesi, Terörizmin Önlenmesine Dair Avrupa Sözleşmesi, Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi vb. sözleşmeler yer almaktadır. (TBMM Başkanlığı, https://www.tbmm.gov.tr/komisyon/insanhaklari/mevzuat_TIHB.htm, (Erişim Tarihi: 24.07.2018).

Çalışmanın bu kısmında detaya girilmeden insan haklarını ele alan hukuki metinlerin bir kısmına yer verilmiştir. Ancak görüldüğü gibi insan hakları ve siber uzay arasındaki etkileşimle birlikte ortaya çıkan sonuçların uluslararası hukuki karşılıklarına değinilmemiştir. Siber uzayda hak ve özgürlüklerin, yerine getirilmesi gereken ödev ve sorumlulukların hukuksal karşılıklarının anlaşmalarla ya da sözleşmelerle güvence altına alınıp alınmadığı çalışmanın sonraki kısımlarında incelenmektedir. Öncelikle siber uzayın ne olduğu, hangi alanları kapsadığı, aktörleri ve tarihsel gelişiminin açıklanması gerekmektedir. Böylece insan hakları ve siber uzayın hukuksal zeminde analizinin yapılması daha anlaşılır olacaktır.

2. Siber Uzayın Tarihsel Gelişim Süreci

İkinci Dünya Savaşı'nın hemen ardından başlayan Soğuk Savaş dönemi dünyayı iki kutuplu bir sistem haline getirmiştir. ABD ve SSCB'nin başını çektiği Batı ve Doğu Bloğu arasındaki mücadele, yaratmış olduğu rekabetçi ortam nedeniyle hem ABD hem de Sovyet Rusya'nın birbirlerini askeri ve psikolojik anlamda sürekli test etmelerine neden olmuştur. Böyle bir ortamda testlerden elde edilen yeni bulgularla hem kendilerinin hem de kendilerine bağlı olan devletlerin savunma sistemlerini güçlendirmeye yönelik adımlar atmışlardır. Hızlı bir silahlanma yarışı, füze sistemlerinin ortaya çıkması ve geliştirilmesi ve ardından uzaya taşınan rekabet siber uzay teknolojisinin altyapısının oluştuğu ve gelişmeye başladığı dönem olarak karşımıza çıkmaktadır (Darıcılı, 2017, ss.2-3).

Siber uzayın gelişimi özellikle internetin gelişimi ile birlikte ele alınmaktadır. 1957 yılında SSCB tarafından uzaya ilk yapay uydu olan Sputnik gönderilmiştir. Buna tepki olarak ABD Savunma Bakanlığı tarafından Arpa (Advanced Research Projects Agency) adında bir birim oluşturulmuştur (Bıçakçı, 2014: s.103). Birbirinden bağımsız bilgisayarların bir ağ üzerinden birbirine bağlanmasına yönelik araştırma birimine ise Arpanet adı verilmiştir. Daha çok askeri temele dayanarak kurulan bu birim ilk veri transferini 1969 yılında gerçekleştirmiştir. Araştırma amaçlı olarak 1974-1976 yılları arasında Intranet adıyla kullanılmıştır. Arpanet'in faaliyet alanı gittikçe genişlemiş ve askeri kanadı Mılnet olarak ayrılmıştır. Arpanet ise zamanla Internet adını almıştır (Bıçakçı, 2014: s.107).

Zamanla nükleer silahların, balistik füzelerin her iki devlet lehine de gelişim göstermesi ise dehşet dengesi olarak ifade edilen bir durumun ortaya çıkmasına neden olmuştur. Bu dengenin bozulmasını sağlayacak olan gelişme 23 Mart 1983 tarihinde ABD Başkanı Ronald Reagan'ın Stratejik Savunma Teklifi (Strategic Defence Initiative- SDI) ile gerçekleşmiştir. Bu teklif ABD'nin nihai hedefi olan caydırıcılığın gerçekleşmesi amacıyla savunma gücünü arttırmayı içermekteydi. Bu plan o dönemde Yıldız Savaşları olarak ifade edilmiştir (Darıcılı, s.11). SSCB bu durumun kendisi için son derece tehlikeli bir sonuç doğuracağının farkına varmıştır. Özellikle ekonomik açıdan bu hamleye karşılık verebilmenin maliyetinin de ülkeyi zor durumda bırakacağını görmüştür. SSCB 1980'lerde RMA (Revolution in Military Affairs) Programı ile silahlı kuvvetlerini modernize etmek istemiştir. Bu program Mareşal Nikolai Orgakov tarafından başlatılmıştır. Bu program ile birlikte ağ teknolojileri, teknolojik

altyapılar ve teknik operasyonlar ile eylem kapasitesi yüksek, daha stratejik ve etkin bir yapının oluşturulması sağlanmıştır (Chapman, 2003).

1983 yılına gelindiğinde TCP/IP (Transmission Control Protocol and İnternet Protocol) protokolüne geçilmiş ve internet ticari amaçlı olarak kullanılmaya başlanmıştır. TCP/IP karşılıklı olarak birbirine bağlı veri iletişimini sağlayan bilgisayar ağını ifade etmektedir. 1989 yılında internetin küreselleşmesinde ve geniş kitlelere sunulmasında öncülük eden isim olan İngiliz Fizikçi Tim Berners-Lee tarafından "World Wide Web" (www) ortaya çıkarılmıştır. Ayrıca "Hypertext" olarak bildiğimiz http sistemini geliştirmiştir. İnternetin kullanılmaya başlanması ve giderek yaygınlaşması denetimini zor bir hale getirmiştir. (Turhan, 2006: s.16).

1989 yılında Berlin Duvarı'nın yıkılması ile SSCB çöküş sürecine girmiştir. 1991 yılında ise kendisine bağlı devletlerin bağımsızlıklarını kazanmasıyla dağılmıştır. Soğuk Savaş'ın getirmiş olduğu rekabet ortamı sonraki yıllarda da devam etmiştir. Bunun nedenleri arasında 1980'lerden itibaren artan küreselleşme akımı, teknolojik gelişmeler ve bilgi toplumuna geçiş gösterilmektedir. Yeni teknolojik gelişmeler (cep telefonu, kredi kartı, internetin ortaya çıkması ve yaygınlaşması, online işlemler, robotik sanayi, ağ teknolojisi ve fiber optik, uydu teknolojilerinin yayılması ve yaygınlaşması vb.) aynı zamanda yeni ekonomik gelişmelerin de önünü açmıştır (Erendor, 2017: ss. 120-121). Küreselleşmenin de etkisiyle yeni ekonomik düzen ülkelerin birbirlerine eskisinden daha çok bağlanmasına ve rekabetin hemen her alanda artmasına neden olmuştur. Bu nedenle Soğuk Savaşın temel aktörleri olan ABD ve Rusya arasındaki rekabet günümüzde Çin, Almanya, İngiltere, Fransa, Japonya, Hindistan, Güney Kore, Kuzey Kore, Kanada gibi ülkelerinde içinde bulunduğu daha geniş bir perspektiften değerlendirilmektedir (Balay, 2004: ss.62-63).

2.1. Siber Uzay

Siber uzayın tarihsel gelişimi ise çok eskilere dayanmamakla birlikte daha çok 20. yüzyılın ikinci yarısındaki teknolojik gelişmelere paralel olarak ilerlemiştir. Siber teriminin kökeni incelendiğinde bu terimin sibernetik kavramından geldiği görülmektedir (Sezgin, 2016: s.562). Sibernetik kavramını ilk kullanan kişi makine-canlı iletişimini inceleyen ve bu alanda yapmış olduğu çalışmalarla sibernetik biliminin kurucu babası sayılan Louis Couffignal'dır. Siber uzay kavramı ise ilk kez William Gibson tarafından 1980'li yılların başında yazmış

olduğu "Neuromancer" adlı bilimkurgu romanında kullanılmıştır (Gibson, 1984). Siber uzayın tanımlanması konusunda farklı yorumlar bulunmaktadır. Bu tanımlamalardan bazıları şunlardır:

- Amerika Savunma Bakanlığı tarafından yapılan tanımlamada; telekomünikasyon ağları ve teknolojik altyapılar sayesinde birbirine bağlı bilgi teknolojilerinin bulunduğu (bilgisayar vs.) küresel bir alan olarak ifade edilmektedir (America Defence Ministry, https://www.defense.gov/portals/1/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, Erişim Tarihi 22.07.2018).
- Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortamdır (Ulaştırma Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf, Erişim Tarihi: 22.07.2018).

Bu tanımlamalardan yola çıkarak bir siber uzay tanımı yapacak olursak:
Siber uzay, bilgi ve iletişim ağlarıyla, dijital bir yaşam alanı olmasının yanı sıra, farklı amaçları olan çok sayıda aktörün yer aldığı, küresel ve bağlantısal bilgi teknolojilerinden oluşan bir alandır.

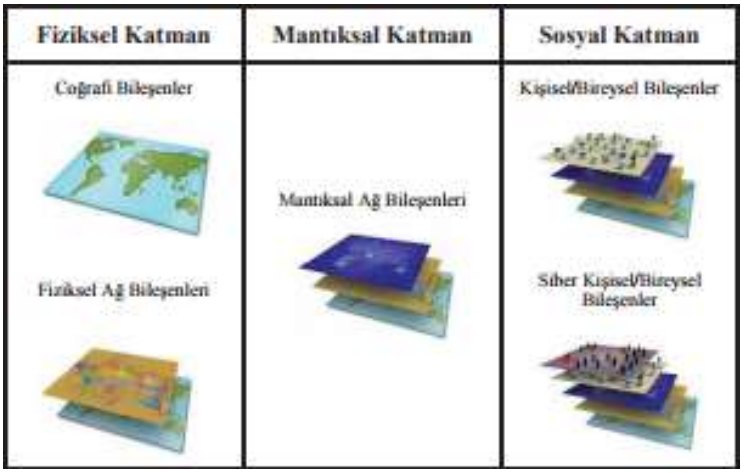
Bir alandaki terminoloji o alanın kavramsallaştırılması ve temel prensiplerinin anlaşılması açısından önemlidir. Bu nedenle siber uzay alanındaki terminolojik ihtiyaç her geçen gün artmaktadır. Çalışmada siber uzay ve insan hakları arasındaki ilişkinin bir uzantısı olarak bu alandaki aktörlerin kendi çıkarları doğrultusunda yapmış oldukları tanımlamaların yaratmış olduğu sorunlar ilerleyen kısımlarda değerlendirilmiştir. İnsan hakları ve siber uzay konusundaki tarihsel arka plan ve gelişim kısaca bu şekilde verilebilir.

2.2. Siber Uzayın Katmanları

Siber uzayın sınırlarını belirlemek oldukça zordur. Ancak siber uzay belirli katmanlardan oluşan boyutlara sahiptir. ABD Kara Kuvvetleri Komutanlığı Siber Uzay Operasyonları Konsept Kabiliyet Planı 2016-2028 isimli bildirisinde siber uzayı çeşitli katmanlara ayırmaktadır. Şekil 1'de görüleceği gibi 3 ana katman bulunmaktadır. Bu katmanlar fiziksel, mantıksal ve sosyal katmanlardır. Bu katmanlarda kendi içinde 5 farklı alt bileşenden

meydana gelmektedir. Fiziksel katman içerisinde coğrafi ve fiziksel ağ bileşenleri yer almaktadır. Ağlara bağlı olarak çalışan bilgi sistemleri coğrafi bileşenler içerisinde bulunmaktadır. Fiziksel ağ bileşenleri ise altyapılara erişimi sağlayan her türlü teknik bileşenleri ifade etmektedir. Mantıksal katman bilgisayar, telefon, modem gibi ağların bağlı bulundukları odak noktalarını ifade etmektedir. Sosyal katman ise kullanıcıların yer aldığı hem gerçek, hem de sanal bireylerden oluşan katmanı ifade etmektedir (US Army Cyberspace Operations Concept Capability Plan, (Erişim Tarihi: 18.07.2018) https://fas.org/irp/doddir/army/pam525-7-8.pdf).

Şekil 1. Siber Uzay'ın Katmanları



Kaynak: https://www.researchgate.net

David Clark'ın siber uzay modellemesinde ise dört katman bulunmaktadır. Bu katmanlar sırasıyla fiziksel iletişim altyapı katmanı, mantıksal katman, bilgi katmanı ve kullanıcıların bulunduğu katmandır. Fiziksel altyapı katmanı siber uzayın bir gerçekliğe dayandığına ve fiziki altyapısına gönderme yapmaktadır. Ancak siber uzayın daha çok sanal bir alan olarak görülmesi onun mantıksal alt bileşenlerinden kaynaklanmaktadır. İkinci katman olan mantıksal katman fiziksel temellerle desteklenmektedir. Hizmetleri oluşturan ve siber alanın temel özelliklerini destekleyen mantıksal katmanda sürekli yeni bileşenler oluşmaktadır. Bilgi katmanı ise siber ortamda saklanan, iletilen ve dönüştürülen bilgileri ifade etmektedir. Sonuncu katman olan kullanıcılar katmanı siber alanda faaliyette bulunan, katılan - iletişim kuran, bilgi alışverişinde bulunan, kararlar alıp planlar yapan, hizmet ve yetenekleriyle siber alanın kendisini dönüştüren kişileri ifade etmektedir (Almeida, 2016: ss.6-8).

2.3. Siber Uzay ve İnsan Haklarının İncelenmesi

Siber uzayda gerçekleştirdiğimiz faaliyetlerin olumlu ve olumsuz olmak üzere iki yönü bulunmaktadır. Bu alanda bilgiye erişim, fatura ödemeleri, bankacılık işlemleri, alışveriş, eğitim, sosyal medya kullanımı, iletişim gibi birçok fırsat bulunmaktadır. Ancak diğer taraftan bu alanda yer alan kullanıcılar açısından hak ihlalleri ortaya çıkmaktadır. Siber uzayda kullanabileceğimiz haklar ve bu hakların ihlallerine yönelik girişimler güvenlik yaklaşımı perspektifinde değerlendirilmektedir.

Teknolojik gelişmelere bağlı olarak değişen bu yeni güvenlik tehditleri siber uzayda karşımıza çıkmaktadır. Temel hak ve özgürlüklerin ihlal edilmesi bu alanda yer alan aktörlerin davranışlarına göre şekillenmektedir. Kimi zaman bireysel ihlaller gerçekleşirken kimi zaman bir grup, şirket, organizasyon ya da devlet tarafından gerçekleştirilen ihlaller söz konusu olmaktadır. Ancak bu noktada daha önemli olarak karşımıza çıkan durum bu ihlalcilerin çoğu zaman tespit edilememesidir. Sorumlular tespit edilse bile gerekli yaptırımları uygulayacak uluslararası mekanizmaların eksikliği göze çarpmaktadır (Ermiş, 2015).

Uluslararası sistemin aktörleri nasıl tarihsel süreç içerisinde değişime ve gelişime uğrayarak günümüze kadar çeşitlilik göstermekte ise siber uzay alanının da kendine has bazı aktörleri bulunmaktadır. Bu aktörler kimi zaman sistemin içindeki bir hatadan kaynaklanan ve durumdan haberi dahi olmayan bireylerden oluşuyorsa kimi zamanda sistematik bir biçimde bilinçli ve yaptıklarının ne gibi sonuçlar doğuracağını bilen kimselerden oluşmaktadır.

Bunlar sırasıyla sıradan kullanıcılar, ulusal menfaatleri göz önünde bulunduran ve politik, ekonomik, askeri, teknik motivasyonlara sahip ve devlet destekli yapılar, daha çok kişisel bilgileri ele geçirmeye ve bundan büyük menfaatler sağlamaya yönelik kurulmuş olan suç örgütleri, çeşitli ideolojilerin ve fikirlerin propagandasını yapma amacı güden haktivistler, daha çok eski çalışan ya da işten çıkarılan kişilerden oluşan ve intikam amacı güdenlerin oluşturduğu kişiler, hackerlar kadar bilgi sahibi olmasalar da sistemdeki açıklardan yararlanarak menfaat elde etme amacı güden script kiddie'ler, sistemde tam olarak nasıl hareket etmesi gerektiğini bilmeyen ve bu nedenle bir takım hatalara neden olanlar olarak ifade edilebilir (İbrahim Korucuoğlu, http://www.siberoloji.com, 15.07.2018)**.**

Dünyada yaklaşık dört milyar internet kullanıcısının olduğu göz önünde bulundurulduğunda ne kadar büyük bir kitlenin etkileşim halinde olduğu ortaya çıkmaktadır (Internet World Stats, https://www.internetworldstats.com/stats.htm, Erişim Tarihi: 15.07.2018). Böyle bir alanda meydana gelen iletişim ve etkileşim sonucunda insan haklarına yönelik ihlallerin de olağanüstü bir boyuta ulaştığı görülmektedir. Siber uzayın sanal olmanın ötesinde artık gündelik yaşamları kontrol eden, düzenleyen ve belirleyen bir işlevi bulunmaktadır. İnsanların büyük çoğunluğu günlük yaşantısının büyük bir kısmını siber alanda geçiriyor. İnsan hakları açısından bakıldığında siber uzayda karşımıza çıkan çok çeşitli hak ihlalleri bulunmaktadır. Kullanıcılar açısından yaşanan bu mağduriyetleri önlemek için siber alanda bir güvenlik ihtiyacı doğmuştur. Çalışmanın sonraki kısımlarında bu ihlaller incelenmiş ve siber güvenliğin sağlanması açısından geliştirilen bilişim hukukunun temel prensipleri ele alınmıştır.

2.4. Siber Uzayda İnsan Hakları İhlalleri

Siber uzayda yaşanan insan hakları ihlalleri çok geniş bir alana yayılmaktadır. İnsan hakları sadece temel hak ve özgürlüklerden oluşmamaktadır. Sosyal, ekonomik ve kültürel haklar ve üçüncül kuşak haklarda insan haklarının içerisinde yer almaktadır. Bu nedenle siber uzayda meydana gelen ihlaller bu çerçevede değerlendirilmelidir. Peki, bu ihlaller nelerdir? Bir ihlalin söz konusu olması için hem ulusal hem de uluslararası anlamda yaptırımları olan sözleşmeler, anlaşmalar, kanunların varlığı ve anayasalarda hukukun üstünlüğü ilkesine dayalı hakların belirlendiği kararların alınmış olması gerekmektedir.

Genel olarak bakıldığında siber uzayda karşımıza çıkan ihlaller şunlardır: Özel hayatın gizliliğini ihlal etmek, haberleşme ve iletişimin gizliliğini ihlal etmek, nitelikli hırsızlık, kredi kartı ve banka dolandırıcılığı, bilgisayar sabotajı, çocuk pornografisi, tehdit ve şantaj, siber zorbalık, siber terörizm, casusluk, insan kaçakçılığı, organ ticareti, fuhuş, kişisel verilere izinsiz erişim sağlamak, başka bir devletin verilerini ele geçirmek, hacking (hackleme), bilişim sistemine izinsiz girmek, sistemi engellemek veya bozmak, verilerin değiştirme ya da yok etmek, ifade, görüş özgürlüğünü ihlal etmek, nefret söylemi vb. olarak sıralanabilir (Bilgi Teknolojileri ve İletişim Kurumu, http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html, Erişim Tarihi: 17.07.2018).

Sanal ortamda insan hakları mevzuatının en önemli parçaları, ifade, görüş, kişi özgürlüğü ve mahremiyet hakkıdır. İnternetin de bu hakların kullanımı için vazgeçilmez bir araç haline geldiği görülmektedir. İfade özgürlüğü, kişi güvenliği ve özgürlüğü, özel yaşamın gizliliği ve kişisel verilerin korunması sık sık ihlal edilen hakların başında gelmektedir. İletişim ve bilişim alanındaki teknolojilerin artmasına paralel bir biçimde ortaya çıkan bu güvenlik sorunları geç te olsa bilişim hukukunun doğmasını sağlamıştır. İnsan hakları ve siber uzay alanında ortak bir güvenlik prensibi oluşturulacaksa bu erişilebilirlik, gizlilik ve bütünlük ilkeleri ile mümkün olacaktır (Can ve Akbaş, 2014: ss.17-18).

Bilişim yolları kullanılarak; terör örgütlerinin faaliyetlerini sanal dünyaya taşımaları, interaktif altyapının dolandırıcılık, hırsızlık amacı ile kullanılabilir hale gelmesi, çocuk pornografisinin yaygınlaşması, nefret söylemlerinin artması gibi nedenler bilişim hukukunun doğuşunu hızlandıran gelişmeler olmuştur. Ancak uluslararası bir bilişim hukukunun varlığından söz etmek oldukça zordur. Uluslararası çalışmalarda devletler daha çok çıkar odaklı hareket etmektedir. Bu nedenle bilişim hukuku alanında yapılan çalışmalar ulusal boyutta kalmaktadır. Uluslararası genel geçer bir bilişim hukukuna yönelik çalışmalarda ise devletler bu kararları daha çok tavsiye niteliğinde görmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Siber uzayda gerçekleşen faaliyetler interneti kullanan herkes açısından olumlu ya da olumsuz sonuçlar doğurabilmektedir. Örneğin bir nükleer tesisi hedef alan terör örgütünün o tesisi hacklemesi, etkileri açısından küresel bir nitelik taşımaktadır. İnternet üzerinden IP bilgilerinize sahip olan birisi illegal faaliyetlerde bu bilgileri kullanabilmektedir. Sosyal medya üzerinden paylaştığınız bir fotoğrafa sizi tanısın veya tanımasın yüz binlerce hakaret gelebilmektedir. Bilgisayarınıza ya da cep telefonunuza gelen bir e-postaya tıkladığınızda siz daha farkında bile olmadan kameranıza, kişisel bilgilerinize, fotoğraflarınıza, mesajlarınıza erişip özel hayatınızın gizliliği ihlal edilebilmektedir. Üstelik bununla kalmayıp bu bilgiler şantaj amaçlı kullanılabilmektedir (Arısoy, 2007: s. 167).

Siber uzayda gerçekleşen suçların, ihlal edilen hak ve özgürlüklerin kapsamı oldukça geniştir. Bu girişimler ise en çok internetin karanlık yüzü olarak adlandırılan DeepWeb'te karşımıza çıkmaktadır. Deep Web internet üzerinde normal web tarayıcılarımızla ulaşılamayan ve arama motorlarında görüntülenmeyen internet sitelerinin genel adıdır. Genelde içeriklerin illegal

olduğu bu ortama giriş yapabilmek için çoğunlukla TOR Browser kullanılmaktadır (Sui vd. 2015: ss. 6-7).

İnternet dünyasının çok geniş olduğu bilinse de bizim anladığımız ve bildiğimiz kısmı tüm internet dünyasının sadece %4'üdür. Kalanı ise Deepweb olarak ifade edilen boyutlardır. Tek bir boyut değil, boyutlar söz konusudur. Yani katman katman daha derine inmek mümkündür. Belli bir noktadan sonrası için özel cihazlar gerekir ve çok az insan bu boyuta erişebilmektedir. Deep Web kavramı için buzdağının görünmeyen yüzü tanımı yapılmaktadır. İllegal faaliyetlerin çoğunluğu ise Deepweb olarak değil Darkweb olarak adlandırılmaktadır. İnsan kaçakçılığı, fuhuş, uyuşturucu ticareti, kiralık katil ve hırsızlık ilanları, sadizm ve mazoşizme yönelik içerikler, çocuk pornografisi, stratejik ve gizli belgelerin yayınlanması veya satılması, sahte kimlik ve pasaport düzenleme faaliyetleri, patlayıcı madde yapımı içerikleri, insanlar ve hayvanlar üzerinde yasal olmayan tıbbi deneyler vs. gibi faaliyetler bulunmaktadır. (Zinnur Yeşilyurt, http://ab.org.tr/ab15/bildiri/249.pdf, Erişim Tarihi: 26.07.2018).

Bu durumun nedenleri arasında, Bilgisayar teknolojilerinin ve sistemlerinin yaygın bir şekilde kullanılması, siber alanda yüksek kazançların daha az riskle elde edilme imkânının bulunması, kanunlarda siber güvenlikle ilgili boşlukların olması, şikâyet bilincinin yaygınlaşmaması, siber alana yönelik yeterince bilgiye sahip olmadan faaliyetlerde bulunulması, suçları gerçekleştiren kişilerin eylemlerinin yaptırımsız kalacağını düşünerek rahat hareket etmesi, suçun işlendiği yer ve zamanın tespit edilmesinin çok zor olması, gerçekleştirilen eylemlerde kimliği gizlemenin kolay olması gibi faktörler sayılabilir (Bilgi Teknolojileri ve İletişim Kurumu, 2018).

Siber uzayda meydana gelen insan hakları ihlalleri ve bu ihlallerin boyutu tüm aktörler açısından değerlendirilmelidir. Örneğin sanal ortamda kişisel verilerin çoğunun özel şirketler tarafından depolanması, alınıp satılması haklarımızın ihlal edildiğini göstermektedir. Örneğin bilmediğimiz veya tanımadığımız firmalardan aldığımız kısa mesajlar, e-postalar, bilgilerimizin üçüncü kişilerle paylaşıldığını kanıtlar niteliktedir. Devletlerin de güvenlik kapsamında kişisel bilgilerimizi kullanması, hesaplarımızı kontrol etmesi, telefonlarımızı dinlemesi, internet üzerinde gerçekleştirmiş olduğumuz faaliyetlere izinsiz ulaşması yine ihlallere örnek olarak gösterilebilir. (International Telecommunication Union- ITU, 2006).

3. Siber Uzayda İnsan Haklarını Koruma Mekanizmaları

Siber uzayda meydana gelen ihlallerin çözüme kavuşturulması insan hakları kavramlarının siber güvenlik ile bütünleştirilmesi ile gerçekleştirilebilir. İnternetin kullanıcıları açısından sadece devletleri değil herkesi kapsayacak ortak bir siber güvenlik anlayışı ile insan hakları korunmalıdır.

Siber uzayda güvenlik açısından yaşanan problemler sadece bireyleri değil şirketleri ve devletleri de endişelendirmektedir. Siber alanda bir insan haklarından ve siber güvenlikten söz edilecekse her şeyden önce ortak ilkeler ve prensiplerin benimsenmesi ve internet etiğinin oluşturulması gerekmektedir. Etik kavramı günümüzde tanımlanması en zor alanlardan birisidir. Bu nedenle siber uzaydaki etik kurallarının oluşturulması son derece zor ve zahmetli bir iştir. Her ne kadar internet etiği ve hukuku alanında yapılan çalışmalar yeni bir süreç olup yavaş ilerlese de hem insan haklarını korunması hem de siber uzayda güvenliğin sağlanmasına yönelik olumlu gelişmeler olarak karşımıza çıkmaktadır (Weber, 2016: ss. 2-3). İnternet etiği kısaca internet vasıtasıyla gerçekleştirilen işlemlerde davranışları belirleyen kurallar olarak tanımlanmaktadır. İnternetin küresel çapta yönetilmesini sağlayacak bir mekanizma kurulması günümüzde oldukça zor olarak görülmektedir. İnternet Etiği, kontrol edilmesi son derece güç olan internet dünyası için uluslararası düzeyde alınacak önlemler ve ilkelerin belirlenmesi, ortaya çıkabilecek sorunların çözülmesine katkı sağlama amacıyla ortaya çıkmıştır. Çalışmanın bundan sonraki kısmında internet ya da diğer bir adıyla bilişim etiğine yönelik atılan adımlar incelenmektedir (Aydın, 2013: s.102).

İnternet olgusu hemen her yere sızmış olduğundan yarattığı risk ve zararlar etik tartışmalarının temelini oluşturmaktadır. Daha önce ifade edilen bu risk ve zararlar insan haklarına yönelik ihlallere neden olmaktadır. Devletlerin bile vatandaşlarının bilgilerine izinsiz erişim sağlayabildiği, verilere erişim yasağı koyduğu bir alanda haklarımız ne kadar güvence altında olabilir? İnternet etiği işte bu ve buna benzer durumlarda ihtiyaç duyduğumuz güvenlik ilkelerinin belirlenmesine katkı sağlayan bir kavram olarak karşımıza çıkmaktadır. Bu tarz sorunların çözülmesine yönelik girişimler gelişmiş ülkelerin, bölgesel ve uluslararası kuruluşların atmış olduğu adımlarla açıklanabilir. Birleşmiş Milletler, Avrupa Konseyi, G8, OECD bu örgütlerin başında gelmektedir.

İnternet Etiği konusundaki adımlardan ilki 1958 yılında Bilgisayar Etik Enstitüsü (Computer Ethics Institute) tarafından yayınlanan 10 ilke ile atılmıştır. Bilgisayar kullanımı konusunda etik prensipler ortaya koyan bu çalışma da başkalarının bilgisayarını izinsiz kullanmamak, bilgisayarı hırsızlık için kullanmamak, bilgisayara zarar vermemek, bedelini ödemediğimiz yazılımı kullanmamak ve kopyalamamak, bilgisayarı saygı duyulacak işlerde kullanmak gerektiği ifade edilmektedir. (Bilgisayar Etik Enstitüsü, http://computerethicsinstitute.org/publications/tencommandments.html, Erişim Tarihi: 29.07.2018).

Çalışmanın bundan sonraki kısmında internet etiği ve siber uzayda insan haklarını korumak için Avrupa Birliği ve Birleşmiş Milletlerin çalışmaları ile birlikte uluslararası örgütlerin çalışmaları ve ulusal eylem planları açısından öne çıkan çalışmalar incelenmektedir.

3.1. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Siber Suç Sözleşmesi (Council of Europe- Convention on Cybercrime) uluslararası açıdan siber güvenlik ve insan haklarını gözeten en önemli sözleşme olup 23 Kasım 2001 tarihinde imzalanmıştır. 1 Temmuz 2004 yılında yürürlüğe giren sözleşme Türkçe olarak "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde ifade edilmektedir. Türkiye'de bu sözleşmeyi 22 Nisan 2014 tarihinde TBMM'de kabul ederek yasalaştırmıştır. Sözleşme, özellikle telif hakkı, bilgisayarla ilgili dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlalleri, internet ve diğer bilgisayar ağları yoluyla işlenen suçlarla ilgili konuları ele almaktadır. Ayrıca bilgisayar ağlarının aranması ve durdurulması gibi bir dizi yetkiyi ve prosedürleri içermektedir (European Cybercrime Convention, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, Erişim Tarihi: 24.07.2018).

Sözleşmenin giriş kısmında öngörülen temel amacı, özellikle uygun yasaları benimseyerek ve uluslararası işbirliğini ilerleterek, toplumu siber suçlardan korumayı amaçlayan ortak bir ceza politikası izlemektir. Sözleşme siber güvenliğin sağlanması noktasında ulusal mevzuatların uyumlulaştırılması amacı gütmektedir. Sözleşme, taraf olan devletlere sözleşmede yer alan hukuki düzenlemeleri iç hukuklarına uyarlama yükümlülüğü getirmiştir (Önok, 2013: ss. 1242-1243).

3.2. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı

13 Mart 2004 yılında kurulan Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA) Avrupa Birliğine üye olan devletlerin ulusal ağ ve bilgi güvenliğine katkıda bulunmak, siber kültürün geliştirilmesini sağlamak, kritik altyapıların ve bilgi sistemlerinin siber saldırılardan korunmasını sağlamak amacıyla kurulmuştur. Temel hedefi ise bilgi güvenliği ve ağ güvenliğini sağlayarak AB iç pazarının düzenli bir biçimde işleyişine katkıda bulunmaktır (European Union Agency for Network and Information Security, https://www.enisa.europa.eu/about-enisa/mission-and-objectives, Erişim Tarihi: 22.07.2018).

3.3. İnternet Hakları ve İlkeleri Dinamik Koalisyonu

2005 yılında Tunis Zirvesi'nde internetin ve insan haklarının bir arada ele alınması gereken alanlar olduğu fikri ortaya atılmıştır. Bu alanda çalışma yapması için iki birim oluşturulmuştu. Bunlardan birisi olan İnternet Hakları Bildirgesi Dinamik Koalisyonu (Internet Rights and Principles Dynamic Coalition) internet üzerinde oluşturulacak kuralların ve yönetim ilkelerinin belirlenmesi için çalışmalara başlamıştır. 2009 yılına gelindiğinde yapılan çalışmalar sonucunda internette insan hakları ve ilkeleri şartı oluşturulmuştur. Bu şartın pratik bir biçimde kullanılabilmesi ve belirli bir insan hakları standardına ulaşabilmesi için alanında uzman kişiler tarafından ana hatları belirlenmiştir. Bu amaçla çeşitli taslak ve versiyonlar oluşturulmuş bunlar geniş katılımcılardan oluşan tartışmalarla geliştirilmiştir. 2011 yılında ise bu konuda yapılan çalışmalar nihayete erdirilmiş ve "10 Etkili İlke" adıyla yayınlanmıştır(The Charter of Human Rights and Principles for The Internet, https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf, Erişim Tarihi: 22.07.2018).

İnternet ortamında ya da sanal ortamda insan haklarına saygı konusunda temel prensipler ortaya koyan bu ilkeler, hakların eşitliği ve evrensel niteliğine vurgu yapmaktadır. Ayrıca herkes için güvenilir ve erişilebilir internet hakkı, fikir ve ifade özgürlüğü, internet aracılığıyla organize olabilme hakkı, bilgiye erişimin sağlanabilmesi için sansürün ortadan kaldırılması, kişisel verilerin korunması ve özel hayatın gizliliğinin ihlal edilmemesi, kültürel çeşitliliğin teşvik edilmesi, internetin tüm paydaşları için eşit fırsatlar sunması ve hukukun üstünlüğü prensibine dayalı açık ve şeffaf bir niteliğinin olması gibi konuları ifade etmektedir (Internet Rights and Principles Coalition, http://internetrightsandprinciples.org/site/about/, Erişim Tarihi: 26.07.2018).

İnternet Hakları ve İlkeleri Dinamik Koalisyonu, insan hakları standartlarını internet üzerinden yönetmek ve internet yönetimi süreçlerini ve sistemlerini geliştirmek için çalışmaktadır. Koalisyon üyeleri, Internet'te hakların çerçevelendirilmesi ve uygulanmasına yönelik süreçleri ve araçları tanıtmak için bireysel ve ortak olarak çalışmaktadırlar. Yayınlamış oldukları ilkeler farklı dillere çevrilmekte ve BM, Avrupa Birliği gibi organizasyonlarca desteklenmektedir (The Charter of Human Rights and Principles for The Internet, 2014).

3.3. Avrupa Siber Suç Merkezi (EC3)

Europol, Avrupa Siber Suçlar Merkezi'ni (European Cybercrime Center-EC3) 2013 yılında AB'deki siber suçlara karşı kanun uygulama sorumluluğunu güçlendirmek ve böylece Avrupalı vatandaşların, işletmelerin ve hükümetlerin çevrimiçi suçlardan korunmasına yardımcı olmak için kurmuştur. Kurulmasından bu yana, EC3 siber suçlarla mücadelede önemli bir katkı yapmıştır (Europol – European Cybercrime Center, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, Erişim Tarihi: 24.07.2018).

3.5. Birleşmiş Milletlerin Çalışmaları

Birleşmiş Milletler 1980'li yıllardan itibaren siber güvenlik çalışmaları yapmaktadır. BM Genel Kurulu "Küresel Siber Güvenlik Kültürünün Oluşturulması ve Kritik Bilgi Altyapılarının Korunması (Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures)", "Bilgi Teknolojilerinin Suç Amaçlı Kötüye Kullanımı İle Mücadele (Combating the Criminal Misuse of Information Technologies)" kararlarında üye ülkelere alması gereken tedbirleri açıklamıştır (United Nations General Assembly, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf, Erişim Tarihi: 29.07.2018).

Özellikle siber kültürün oluşturulması noktasında belirlemiş olduğu farkındalık, sorumluluk, etik, demokrasi, risk tasarımı, güvenlik yönetimi ilkeleri vs. önemlidir. Söz konusu olan bu ilkeler OECD tarafından da kabul edilmiş "Bilgi Sistemleri ve Ağların Güvenliğine İlişkin

OECD Rehber İlkeleri" (OECD Guidelines for the Security of Information Systems and Networks) olarak adlandırılmıştır (OECD, https://www.oecd.org/sti/ieconomy/15582260.pdf, Erişim Tarihi: 29.07.2018).

BM'ye bağlı Bilgi ve İletişim Teknolojileri Görev Gücü 2002 yılında yayınlamış olduğu "Bilgi Güvenliği- Siber Tehditlerin ve Siber Güvenliğin Keşfedilmemiş Bölgelerinde Hayatta Kalabilme Kılavuzu (Information Security: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security)" ile güvenlik olaylarına müdahale edecek mekanizmalarını, siber güvenlik sorunlarına yönelik çözüm önerilerini ortaya koyması bakımından önemlidir. BM, bilgi güvenliğinin sağlanması açısından Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT) adıyla faaliyet gösteren bir platform oluşturmuştur. Ayrıca BM'ye bağlı olarak faaliyet gösteren bir uzmanlık kuruluşu olan Uluslararası Telekomünikasyon Birliği (ITU) de bilgi güvenliği ile ilgili çalışmalar yürütmektedir. Bunların yanı sıra BM Genel Sekreterliği, İnternet Yönetişim Formunun düzenlenmesi görevinde bulunmaktadır (Güngör, 2015: ss.58-59).

Bu forumun amacı internet konusunda ilgili devletlerin altyapılarını geliştirmek, siber güvenlik sorunlarına yönelik tecrübe paylaşımında bulunmak, internetin güvenliğini sağlayacak politikaların hayata geçirilmesini sağlayacak çalışmalar yapmak olarak sıralanabilir. BM uluslararası bir sözleşme ortaya koyamamıştır ancak bu konuda yapılacak çalışmaları desteklemektedir. Özellikle Avrupa Siber Suç Sözleşmesini destekleyen bir tutum takınmaktadır (Ünver, 2011: ss.5-10).

Dünyada siber güvenlik ile ilgili çalışmalar yürüten diğer örgütler ve kurumlar şunlardır: Asya-Pasifik Ekonomik İşbirliği (APEC), Güneydoğu Asya Ülkeleri Birliği (ASEAN), Olay Müdahale ve Güvenlik Ekipleri Forumu (FIRST), Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE), Uluslararası Elektroteknik Komisyonu (IEC), Internet Mühendislik Görev Gücü (IETF), INTERPOL, Amerikan Devletleri Örgütü (OAS), Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD). (Network World, https://www.huffingtonpost.com/2010/08/05/most-influential-cybersec_n_671690.html, Erişim Tarihi: 01.08.2018).

Ulusal siber güvenlik stratejisi yayınlayan bazı ülkeler şunlardır: ABD, Almanya, Arnavutluk, Avusturya, Azerbaycan, Birleşik Krallık, Belçika, Çin Halk Cumhuriyeti, Çek Cumhuriyeti,

Danimarka, Estonya, Finlandiya, Fransa, Hırvatistan, Hindistan, Hollanda, İspanya, İsrail, İsviçre, İtalya, İzlanda, Japonya, Kanada, Katar, Letonya, Litvanya, Lüksemburg, Macaristan, Malezya, Norveç, Pakistan, Polonya, Portekiz, Romanya, Rusya, Slovakya, Slovenya, Suudi Arabistan, Türkiye, Ukrayna. (NATO Cooperative Cyber Defence Center of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, Erişim Tarihi: 01.08.2018)

Genel olarak bakıldığında siber uzayda insan haklarının korunmasına yönelik yapılan çalışmaların daha çok ulusal ya da bölgesel nitelikli olduğu görülmektedir. Özellikle uluslararası alanda işbirliğinin azlığı ve uluslararası bir koruma mekanizmasının oluşturulamaması devletlerin ulusal çıkarlarına öncelik veren tutumlarından kaynaklanmaktadır. Her devletin siber güvenlik kavramına farklı anlamlar ve tanımlamalar getirmesi, terminolojik ve teknik yetersizlikler bu sorunun derinleşmesine neden olan diğer faktörlerdir. Çalışmanın bu bölümünde siber uzayda insan haklarını korumak, dolayısıyla siber güvenliği sağlamak için yapılan çalışmaların ulusal ve uluslararası boyutları incelenmiştir. Çalışmanın bundan sonraki kısmında genel değerlendirmeler ışığında ulaşılan sonuçlar ve öneriler sunulacaktır.

SONUÇ

Bilgisayar ağlarının artması ve bilgi teknolojilerinin yayılması, dünyayı her zamankinden daha çok birbirine bağlamaktadır. 2030'da İnternet kullanıcılarının 5 milyar civarında olması beklenmektedir. O zamana kadar, dünya nüfusunun % 80'inin mobil bağlantıya sahip olacağı ve % 60'ının geniş bant erişimden yararlanacağı düşünülmektedir. Bu nedenle internet yaşadığımız dünyayı, tüketim hızını ve şeklini daha da geniş bir ölçüde şekillendirecektir (Council of Europe, http://www.consilium.europa.eu/en/policies/cyber-security/ Erişim Tarihi: 28.07.2018). Dijital çağ zenginlik, bilgi ve özgürlük açısından milyarlarca insana büyük fayda sağlamaktadır. Bu nedenle, internetin güvenliği ve istikrarı ve veri akışlarının bütünlüğü, devletler, şirketler, bireyler için giderek önem kazanmaktadır.

Siber uzay ve insan hakları birbirinden farklı alanlar olarak görülebilir. Ancak bu alanlar birbirini kapsamakta ve karşılıklı olarak etkileşim içerisinde bulunmaktadır. Siber alanın gün geçtikçe genişleyen yapısı insan hakları ihlallerinin de artmasına neden olmaktadır. Özellikle bu alana yönelik güvenlik anlayışı her aktör tarafından ayrı değerlendirilmektedir. Siber uzayda güvenlik nasıl sağlanacak? Siber uzayda barış tesis etmek mümkün müdür? Siber

uzayda insan hakları savunulabilir mi? Bu soruların cevabını vermek şu an için mümkün görünmese de yaşanılan gelişmeler ve atılan adımlar bize bazı ipuçları vermektedir. Bunlardan hareketle siber uzayda insan haklarının geliştirilmesi için şu sonuçlara ulaşabiliriz:

* Bilişim etiğinin geliştirilmesi için uluslararası işbirliğine yönelik çalışmalar arttırılmalıdır.
* Siber güvenlik ve türevleri (siber suç, siber zorbalık, siber uzay vs.) ile ilgili tanımlama sorunun çözümü için alanında uzman kişilerden oluşan ve herkes için ortak ilkelerin belirlendiği geniş kapsamlı konferanslar düzenlenmelidir.
* Siber uzay, insan hakları, bilişim etiği konusunda özellikle genç kuşağa yönelik eğitim politikalarının hayata geçirilmesini sağlamak. Bu konuda devletin girişimi olabileceği gibi özel sektöründe teşvik edilmesi önemlidir.
* Ulusal düzeyde alınacak güvenlik politikalarında ihmal ve ihlal edilen boşlukların düzenlenmesi sağlanmalıdır. Bu durum devlet ve yurttaşları arasındaki güven probleminin çözümüne de katkı sağlayacaktır.
* Teknolojik gelişmeler ve dijital çağa uyum sağlamak, toplumsal ve kültürel değerlerin zarar görmesini engellemek için siber kültür politikası oluşturmak,
* Siber uzayda insan haklarını korumak için teknik bilgi, altyapı çalışmaları ve risk analizlerini ölçecek birimlerin kurulmasını sağlamak
* Küresel ölçekte gerçekleştirilecek bu çalışmalar temelde insan haklarına, hukukun üstünlüğüne, uluslararası hukuk ilkelerine sıkı sıkıya bağlı bir şekilde hayata geçirilmelidir. Ayrıca siber politikalar özgürlük ve güvenlik arasında sürdürülebilir bir denge içerisinde hayata geçirilmelidir.

Sonuç olarak insan haklarının, ortaya çıkışından günümüze kadar olan tarihsel süreçte çeşitli aşamalardan geçtiği görülmektedir. Bu nedenle çalışmada insan haklarının dinamik bir kavram olarak değişim ve gelişim süreci ele alınmıştır. Diğer yandan siber uzay kavramının tarihsel arka planı verilerek açıklanmaya çalışılmış, siber uzayın aktörleri ve katmanları incelenmiştir. Siber uzay ve insan hakları arasındaki ilişkinin bağlantıları Soğuk Savaş ve sonrasındaki rekabetçi ortam bağlamında ele alınmıştır.

Teknolojik gelişmeler ve özellikle internetin ortaya çıkması, küreselleşme akımı, bilgi toplumuna geçiş gibi önemli noktalar siber uzayın sınırlarını daha da genişletmiştir. Siber uzay fırsatlar ve faydalarla birlikte, tehditler ve risklerin de yer aldığı bir alan olarak karşımıza çıkmaktadır. Bu durum bireylerin, grupların, şirketlerin, devletlerin güvenliğe bakış

açılarını da değişime uğratmıştır. Siber uzayın korunması temelde siber güvenliğin sağlanması ile mümkündür. Ancak siber uzayın başat aktörü olarak görülen devletlerin ve uluslararası örgütlerin evrensel bir siber güvenlik politikası oluşturmak için atacakları adımlarda ulusal çıkarları ve menfaatleri ön plana çıkarması nedeniyle başarısız bir girişim olarak karşımıza çıkmaktadır. Her geçen gün siber uzayda yeni tehdit türleri ortaya çıkmaktadır. Bu durum sadece bireyleri değil devletleri de zor durumda bırakmaktadır. Örneğin siber uzayda potansiyel tehditler içerisinde yer alan siber terör tehlikesi doğurabileceği sonuçlar düşünüldüğünde bile göz ardı edilmemesi gereken alanlardan biri olarak karşımıza çıkmaktadır. Önemli olan, işbirliği için atılacak olan adımların geç kalınmadan büyük felaketler yaşanmadan atılmasıdır. Büyük felaketlerin yaşanmaması açısından vatandaşlarının can ve mal güvenliğini düşünen devletler aynı hassasiyeti siber uzayda ihlal edilen ve göz ardı edilen diğer hak ve özgürlükler içinde göstermelidir.

KAYNAKÇA

ALGAN, Bülent, (2007) *Ekonomik, Sosyal ve Kültürel Hakların Korunması,* Ankara: Seçkin Yayıncılık.

ALMEIDA Virgilio, Cyberspace Governance Concept and Framework, Harward University,https://cyber.harvard.edu/~valmeida/pdf/Lecture2.pdf (20.12.2017)

ARISOY, Mine, (2007) "Hakaret", *Türkiye Barolar Birliği Dergisi*, Sayı 72.

AVRUPA KONSEYİ VE İNTERNET, https://edoc.coe.int/en/index.php?controller=get-file&freeid=6079 (12.12.2017)

AVRUPA KONSEYİ, https://europa.eu/globalstrategy/en/cyber-security (05.01.2018)

AYDIN, İnayet, Çocuk, İnternet ve Etik, https://www.researchgate.net/publication/316473196_Cocuk_Internet_ve_Etik, (18.12.2017)

BIÇAKÇI, Salih, (2014) "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler Dergisi*, Cilt 10, Sayı 40.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, Bilişim Hukuku, http://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu-detay-58.html (17.12.2017).

BİLGİSAYAR ETİK ENSTİTÜSÜ, http://computerethicsinstitute.org/publications/tencommandments.html (22.12.2017)

BRYANT, Rebecca, (2001) "What Kind of Space is Cyberspace?", *Minerva - An Internet Journal of Philosophy*, Vol. 5.

CAN, Özgü ve Fatih Akbaş, (2014) "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", *Tübav Bilim Dergisi*, Cilt: 7, Sayı: 2.

CHAPMAN, Garry, (2003) "An Introduction to the Revolution in Military Affairs", http://www.lincei.it (Erişim Tarihi: 24.07.2018).

CINGI, Aydın (2009) *Sora Sora Demokrasi*, İstanbul: Kalkedon Yayınları.

DARICILI, Ali Burak, (2017) "Demokrat Parti Hack Skandalı Bağlamında ABD ve RF'nin Siber Güvenlik Stratejilerinin Analizi", *Uluslararası Çalışmalar Dergisi*, Cilt 1, Sayı 1.

ENGİN, Zeynep Özlem Üskül, (2014) " Birey Kavramının Gelişimi ve İnsan Hakları", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt 72, Sayı 1.

ERENDOR, M.E., "Risk Toplumu ve Refleksif Modernleşme Çerçevesinde Siber Terörizm: Tanımlama ve Tipoloji Sorunu", *Cyberpolitik Journal*, vol.1, no.1, pp.114-133, 2017.

ERMİŞ, U. (2015) "Siber Caydırıcılık: Teoriği Kolay, Pratiği Zor", https://siberbulten.com/makale-analiz/siber-caydiricilik-teorigi-kolay-pratigi-zor/ (Erişim Tarihi: 28.07.2018).

EUROPOL – EUROPEAN CYBERCRIME CENTER, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (18.12.2017)

GIBSON, William, (1984) *Neuromancer*, Grafton Books - Collins Publishing Group, London, 1984.

GÜNGÖR, Murat, (2015) *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, T.C. Kalkınma Bakanlığı: Bilgi Toplumu Dairesi Başkanlığı, Uzmanlık Tezi, Ankara.

HUFFPOST, Most Influential Cyber Security Organizations in The World, https://www.huffingtonpost.com/2010/08/05/most-influential-cybersec_n_671690.html, (Erişim Tarihi: 01.08.2018)

INTERNET RIGHTS AND PRINCIPLES COALITION, http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_Booklet_Turkish_final.pdf (23.12.2017)

ITU- International Telecommunication Union, (2006), *Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CRIM-2006-PDF-E.pdf, (Erişim Tarihi 26.07.2018).

ITU- International Telecommunication Union, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (Erişim Tarihi: 29.07.2018).

KABOĞLU, İbrahim Ö., (2011) *Anayasa Hukuku Dersleri*, İstanbul: Legal Yayınları.

KILIÇ, Yavuz, (2015) " Hobbes, Locke ve Rousseau'da Doğa Durumu Düşüncesi", *Temaşa Erciyes Üniversitesi Felsefe Bölümü Dergisi*, Cilt 2, Sayı 2.

KIVILCIM, Fulya, (2013) "Küreselleşme Kavramı ve Küreselleşme Sürecinin Gelişmekte Olan Ülke Türkiye Açısından Değerlendirilmesi", *Sosyal ve Beşeri Bilimler Dergisi*, Cilt 5, Sayı 1.

KORUCUOĞLU, İbrahim, Siber Uzay Tanımı ve Aktörleri, https://siberoloji.github.io/siber-uzay-tanimi-aktorleri/ (16.12.2017).

KÜÇÜKALİ, Rıdvan, Hasibe Akbaş, (2016) "Bir Haklılaştırma Zemini Olarak Doğal Hukuk", *MSKU Eğitim Fakültesi Dergisi*, Sayı 3.

LEINER, M.Berry, *A Brief History of the Internet*, Internet Society, https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf (18.12.2017).

MALHOTRA, Sona, (2016) "Cyber Crime- Its Types, Analysis and Prevention Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6, Issue 5.

NATO Cooperative Cyber Defence Center of Excellence, https://ccdcoe.org/cyber-security-strategy-documents.html, (Erişim Tarihi: 01.08.2018).

OECD, Guidelines for the Security of Information Systems and Networks Towards a Culture of Security, https://www.oecd.org/sti/ieconomy/15582260.pdf, Erişim Tarihi: 29.07.2018).

ÖNOK, Murat, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadele ve İşbirliği, http://dergipark.gov.tr/download/issue-file/517 (18.12.2017).

RUDE George, (2015) *Fransız Devrimi,* İstanbul: İletişim Yayınları.

SEZGİN, Murat, (2016) "Bilişim Devrimi, Sibernetik İletişim ve Halkla İlişkiler", *Sosyal Bilimler Enstitüsü Dergisi*, Karabük, Cilt: 6, Sayı: 2.

SUI, Daniel, vd., (2015) "The Deepweb and The Darknet: A Look Inside Internet's Massive Black Box", *Wilson Center*, Stip 3.

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI, (2013). *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.*

TOKU, N. (2004) Felsefe Yazıları, İstanbul: Yeni Zamanlar Yayınları.

TURHAN, Aydın, (2013) "İnsan Hakkı Kuşakları Arasındaki Tamamlayıcılık İlişkisi", *İstanbul Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 4, Sayı 2.

TURHAN, Oğuz, (2006) *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)*, Devlet Planlama Teşkilatı: Planlama Uzmanlığı Tezi, Ankara.

ÜNAL Şeref, (1994) "İnsan Haklarının Tarihi, Felsefi ve Hukuki Temelleri", *Ankara Barosu Dergisi*, Ankara.

ÜNAL, Yenal, (2009), "Bilgi Toplumunun Tarihçesi", *Tarih Okulu Dergisi*, Sayı: 5.

ÜNAL, A. N., Milli Güç Unsurlarının Belirlenmesinde Siber Uzay Faktörü, https://www.researchgate.net/profile/Ahmet_Unal6/publication/321125904_Milli_Guc_Unsur

larinin_Belirlenmesinde_Siber_Uzay_Faktoru/links/5a0e74b00f7e9b7d4dba66fe/Milli-Guec-Unsurlarinin-Belirlenmesinde-Siber-Uzay-Faktoerue.pdf (20.12.2017).

ÜNVER, Mustafa vd., (2011) Uluslararası Kuruluşların Siber Güvenlik Faaliyetleri, Ankara.

WEBER, Rolf H., (2016) "Global Commission on Internet Governance", *Royal Institute of International Affairs*, No 39.

YEŞİLYURT, Zinnur, DeepWeb, Web'in Karanlık Yüzü, http://ab.org.tr/ab15/bildiri/249.pdf (15.12.2017).