

T.C.
SELÇUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER BİLİM DALI

SİBER UZAYDA ÖZEL HAYATIN GİZLİLİĞİ
HAKKINI YENİDEN TARTIŞMAK

Sezen Ceren YILMAZ

DOKTORA TEZİ

Danışman

Prof. Dr. Nezir AKYEŞİLMEN

KONYA-2023

TEŞEKKÜR

Bu tezin tamamlanması aşamasında değerli bilgi ve deneyimleriyle bana yol gösteren, hiçbir zaman desteğini esirgemeyen, en zorlu anlarda bile pozitif tutumu sayesinde devam etmemi sağlayan kıymetli danışmanım Prof. Dr. Nezir AKYEŞİLMEN'e katkılarından dolayı teşekkürü borç bilirim. Ayrıca Tez İzleme Komitesindeki değerli hocalarım Doç. Dr. Demet Şefika MANGIR ve Prof. Dr. Fatih MANGIR'a eleştiri ve dönütleriyle çalışmama katkı sağladıklarından dolayı çok teşekkür ederim.

Uzun süren çalışmam esnasında gece gündüz sabırla yanımda olan ve desteğini hep hissettiğim sevgili eşim Doç. Dr. Onur YILMAZ'a ve canım kızım İmge'ne ne kadar teşekkür etsem azdır.



ÖZET

Bu tez, bilgi iletişim teknolojilerinin gelişmesi ve dijitalleşmenin bir sonucu olarak siber uzayda özel hayatın gizliliği hakkının geleneksel uluslararası sistemde korunamadığını ileri sürmektedir. İnternet ve dijital teknolojilere olan bağımlılık toplumların sosyokültürel yapısının değişmesine neden olmuş bu da insan hakları bağlamında hem tehditleri hem de fırsatları beraberinde getirmiştir. Bu değişimden en çok etkilenen haklardan biri özel hayatın gizliliği olarak karşımıza çıkmaktadır. Siber uzayda aktörlerin çeşitlenmesi, bilgi iletişim teknolojilerin gelişmesiyle birlikte siber gözetim, siber istihbarat ve kişisel verilerin ihlal edilmesinde muazzam bir artış olmuş bunun bir sonucu olarak da özel hayatın gizliliği hakkı siber uzayda en çok ihlal edilen haklar arasında yer almıştır.

Siber uzay bağlamında özel hayatın gizliliği hakkının karmaşık ve çok yönlü olduğu ileri sürülmektedir. Bu hak, siber uzayda geleneksel olarak adlandırılan unsurlarını korumuş ancak hakkın kapsamı genişleyip çeşitlenmiştir. Bu genişleme karşısında da uluslararası ve bölgesel mekanizmaların bu hakkı korumada yetersiz kaldığı kabul edilmektedir. Konuyla ilgili mevcut bilgi birikimini ve tartışmaları ortaya koymak için literatür taraması yapılmış, farklı bakış açıları ortaya çıkarmak için kıyas yöntemi kullanılmış, belgelerin içeriği, amacı ve bulguları analiz etmek için ise belge inceleme yöntemlerine başvurulmuştur. Uluslararası hukukun siber uzayda gelişen teknolojilere ayak uyduramadığı ileri sürülmektedir. Söz konusu insan hakları olduğu için uluslararası hukuk anlayışının siber uzayı da ele alabilecek kadar genişlemesi gerektiği ve siber uzay bağlamında özel hayatın gizliliği hakkının tekrar tanımlanması ve tanımın kapsamının genişletilmesi gerektiği sonucuna varılmıştır.

Anahtar Kelimeler: Siber Uzay, Özel Hayat, Özel Hayatın Gizliliği Hakkı, İnsan Hakları, Bilgi İletişim Teknolojileri.

ABSTRACT

This thesis argues that as a result of the development of information communication technologies and digitalization, the right to privacy in cyberspace cannot be protected in the traditional international system. Dependence on the Internet and digital technologies has led to changes in the sociocultural structure of societies, which has brought about both threats and opportunities in the context of human rights. One of the rights most affected by this change was the right to privacy. With the diversification of actors in cyberspace and the development of information communication technologies, there has been a tremendous increase in cyber surveillance, cyber intelligence, and the violation of personal data, and the right to privacy has become one of the most violated rights in cyberspace.

It is argued that the right to privacy in cyberspace is complex and multifaceted. This right has preserved its traditional elements in cyberspace, but its scope has expanded and diversified. In the face of this expansion, it is accepted that international and regional mechanisms are insufficient for protecting this right. A literature review was conducted to reveal existing knowledge and debates on the subject. The syllogistic method was used to reveal different perspectives, and document analysis methods were used to analyze the content, purpose, and findings of the documents. It has been argued that international law has not kept pace with the development of technologies in cyberspace. It is concluded that since human rights are at stake, the understanding of international law should be broadened enough to address cyberspace, the right to privacy in the context of cyberspace should be redefined, and the scope of the definition should be expanded.

Keywords: Cyberspace, Privacy, the Right to Privacy, Human Rights, Information and Communication Technologies.

İÇİNDEKİLER

TEŞEKKÜR	i
ÖZET	ii
ABSTRACT.....	iii
KISALTMALAR	vi
GİRİŞ	1

BİRİNCİ BÖLÜM

1.SİBER UZAY VE İNSAN HAKLARI	19
1.1.Özel Hayat Bağlamında Siber Uzayın Kavramsal Çerçevesi	19
1.1.1 Siber Uzay	20
1.1.2. Siber Güvenlik	22
1.1.3. Siber Saldırıları	25
1.1.4. Siber Gözetim	28
1.1.5. Siber Şeffaflık	32
1.1.6. Siber İstihbarat	33
1.2. Bir İnsan Hakkı Olarak Özel Hayatın Gizliliği	39
1.2.1. Özel Hayatın Tanımı	39
1.2.2. Özel Hayatın Önemi	44
1.2.3.Özel Hayatın Kapsamı	46
1.2.3.1. Özel Alan	47
1.2.3.2. Kamusal Alan	49
1.2.4. Özel Hayatın Gizliliği Hakkının Boyutları	55
1.2.4.1 Kişisel Veri ve Kişisel Verilerin Korunması	55
1.2.4.2. Konuta Müdahale Etmeme	58
1.2.4.3. Ad Şöhret (İtibar) Hakkı	59
1.2.4.4. Yazışmalar	62
1.3. İnsan Haklarında Siber Uzayın Getirdiği Yeni Tartışmalar ve Özel Hayat 63	
1.3.1. Kuşak Hakları (İletişim Hakları)	63
1.3.1.1 İnternete Erişim Hakkı	64
1.3.1.2 Anonimlik Hakkı.....	68
1.3.1.3. Unutulma Hakkı	72

1.4 Özel Hayatın Gizliliğine Yönelik Teorik Yaklaşımlar	76
1.4.1 Özel Hayatın Gizliliği ve Özgürlük Teorisi	77
1.4.2. Özel Hayatın Gizliliğini Düzenleme Teorisi	79

İKİNCİ BÖLÜM

2.ULUSLARARASI DÜZENLEMELERDE ÖZEL HAYATIN GİZLİLİĞİ

HAKKI	83
2.1. Birleşmiş Milletler Düzenlemelerinde Özel Hayatın Gizliliği Hakkı	83
2.1.1. Evrensel İnsan Hakları Beyannamesi	89
2.1.2. Sivil ve Siyasal Haklar Konvansiyonu	90
2.2. Avrupa Konseyi Düzenlemelerinde Özel Hayatın Gizliliği Hakkı	93
2.2.1. Avrupa İnsan Hakları Sözleşmesi.....	96
2.2.2 Avrupa Konseyi Siber Suç Sözleşmesi	98
2.2.3. Biyotıp Sözleşmesi	101
2.3. Diğer Uluslararası Düzenlemeler	103
2.3.1. Amerikan İnsan Hakları Sözleşmesi	103
2.3.2. Avrupa Birliği Temel Haklar Şartı	105
2.3.3. Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi	107
2.3.4. Bilgi Teknolojileri Suçlarıyla Mücadeleye İlişkin Arap Sözleşmesi	110

ÜÇÜNCÜ BÖLÜM

3.SİBER UZAY ÖZEL HAYATIN GİZLİLİĞİ HAKKINI NASIL

ETKİLİYOR?	114
3.1. Siber Uzayın Özel Hayata Etkisi	114
3.1.1. Siber Gözetim	116
3.1.2. Siber İstihbarat.....	131
3.1.3. Kişisel Verilerin Korunması	140
3.2. Avrupa İnsan Hakları Mahkemesi Kararları	148
3.2.1. Elektronik Gözetim	148
3.2.2.Kişisel Veri ve Kişisel Verilerin Korunması	153
3.2.3. Yazışmalar (Haberleşme)	157
BULGULAR VE ANALİZ	164

SONUÇ	168
KAYNAKÇA	179



KISALTMALAR

AAİHK	:Amerikalılar Arası İnsan Hakları Komisyonu
AB	:Avrupa Birliği
ABD	:Amerika Birleşik Devletleri
ACCITO	:Arab Convention on Combating Information Technology Offences
ACoHR	:American Convention on Human Rights
AİHS	:Avrupa İnsan Hakları Sözleşmesi
AİHM	:Avrupa İnsan Hakları Mahkemesi Kararları
AKİHM	:Amerika Kıtası İnsan Hakları Mahkemesi
BİT	:Bilgi İletişim Teknolojileri
BM	:Birleşmiş Milletler
CCSPDP	:Convention on Cyber Security and Personal Data Protection
CCTV	:Closed-Circuit Television
CoC	:Convention on Cybercrime
CoFR	:Charter of Fundamental Rights of the European Union
CSEU	:Cybersecurity Strategy of the European Union
ECHR	:European Court of Human Rights
ESK	:Ekonomik ve Sosyal Konsey
EİHB	:Evrensel İnsan Hakları Beyannamesi
EUROPOL	:Avrupa Polis Teşkilatı
FBI	:Federal Bureau of Investigation
GDPR	:Avrupa Birliği Genel Veri Koruma Tüzüğü
GEOINT	:Coğrafi Konum İstihbaratı
GPS	:Global Positioning System
HUMINT	:İnsana Dayalı İstihbarat
IoT	:Nesnelerin İnterneti
İHK	:İnsan Hakları Komisyonu

KVKK	:Kişisel Verileri Koruma Kurumu
MASINT	:Ölçüm ve Akustik İstihbaratı
MİT	:Milli İstihbarat Teşkilatı
OECD	:Ekonomik İşbirliği ve Kalkınma Teşkilatı
OSINT	:Açık Kaynaklı İstihbaratı
SIGINT	:Sinyal İstihbaratı
SSHK	:Sivil ve Siyasal Haklar Konvansiyonu



GİRİŞ

Siber uzay tarihi elli yıl olmasına karşılık hayatımıza nüfuz etmesi yaklaşık otuz yıllık bir süreç olarak karşımıza çıkmaktadır. Yirminci yüzyılın ikinci yarısından itibaren, özellikle de 1990'lı yıllarda internetin günlük hayatımıza hızla girmeye başlaması ile birlikte siber alan küresel çapta yaygınlaşmış ve bu yeni alanda önemli sosyokültürel değişikliklerin oluşmasına neden olmuştur. Bireyler de bu alanın bir parçası olmuş ve bu da bireyler için hem tehditleri hem de fırsatları beraberinde getirmiştir. Bir yandan bireylerin kişisel gelişimi ve toplumsallaşması için muazzam bir fırsat yaratan siber uzay, diğer yandan da kişisel verilerin suiistimal edilmesinde açık hedef haline gelmiştir.

Bilgi iletişim teknolojilerindeki bu gelişme bireyi sanal ortamda güçlendirerek sosyalleşmesini sağlamış, bilgiye erişimini kolaylaştırmış, adeta global bir ortam oluşturarak dünyanın diğer ucundan haber alabilmesine olanak tanımıştır. Ancak aynı zamanda bu alan birey açısından mağduriyet yaratmış ve bireyin kendine ait olan dünyasını, bireyin rızası dışında bu sanal alana taşıyarak bireyin hayatını olumsuz etkilemiştir. Örneğin internet kullanımının yaygınlaşması sayesinde bilgi dolaşımı, toplanma ve ifade özgürlüğü haklarından yararlanma artmış ancak özel hayatın gizliliği hakkı da bir yandan kısıtlanmıştır. Hakkın bu sanal ortamda kısıtlanması ve ihlale açık hale gelmesi hakkın varolan doğasının da siber uzay bağlamında genişlemesine neden olmuş ve bu da birtakım değişiklikleri de beraberinde getirmiştir.

Devletler açısından zaten ihlale açık olan insan hakları, siber uzayda daha çok ihlal edilir hale gelmiştir. Fiziki ortamda hakkının ihlal edildiğini daha açık bir şekilde görebilen birey, siber uzayda bu hakkının devletler, şirketler veya bireyler tarafından ihlal edildiğinin farkında dahi ol(a)mamaktadır. Devletlerin güvenliği adına ihlal edilen insan haklarının, özel şirketler tarafından da yığın bilgi toplama uğruna suiistimal edildiği görülmektedir. Bu da genelde insan hakları özel de ise özel hayatın gizliliği hakkının siber uzayda korunması açısından sorun teşkil etmektedir.

Siber uzayda özel hayatın gizliliği hakkı bireyin en çok mağdur olduğu haklar içerisinde yer almaktadır. İnternette yapılan her türlü işlemin kayıt altına alınması, siber gözetimin hayatımızın bir parçası olması, sosyal medya sitelerinde veya

bloglarda yapılan paylaşımların kamusallaştırılması özel hayatın gizliliği hakkının daha kolay ihlal edilebilir hale getirmiştir. Bu gelişmelerin bir sonucu olarak “özel alan” ve “kamusal alan” kavramlarının siber uzayda içiçe geçmesi ve kavramlar arasındaki geçişkenliğin artması “hangi paylaşımın özel”, “hangi paylaşımın kamusal” olduğu tartışmalarını da bu sanal uzamda beraberinde getirmiştir. Bu içiçe geçen kamusal ve özel alanlar özel hayatın gizliliği hakkını nasıl etkilemektedir? Bu alanların sınırları siber uzayda tekrar tanımlanabilir mi? Bu ve buna benzer soruların cevaplarının tam olarak açıklanamaması da kavram kargaşasına ve karmaşıklığa neden olmaktadır. Bu bağlamda da siber uzayda özel hayatın gizliliği hakkının kavram karmaşasından etkilendiği görülmektedir.

Uluslararası hukuk belgelerinde özel hayatın gizliliği hakkı, ilk olarak Evrensel İnsan Hakları Beyannamesi’nin (EİHB) 12’nci maddesi’nde “özel hayatın korunması”, Avrupa İnsan Hakları Sözleşmesinde de “özel hayata saygı” olarak düzenlenmiştir. Özel hayatın gizliliği hakkı çok boyutlu bir kavram olarak karşımıza çıkmaktadır. Birey kendi hayatını bir giz perdesi içerisinde yaşamak isterken, devlet bazı durumlarda bu alana müdahale edebilmektedir. Hakkın çok boyutluluğu ve karmaşıklığı da aslında tam da bu noktada karşımıza çıkmaktadır. Örneğin, devletler henüz bir suç unsuru oluşmamışken terörizmi önlemek ve ulusal güvenliği sağlamak adına bireylerin haberi olmadan kişiyi gözetleyebilir, takip edebilir veya sanal ortamda kişi hakkında bilgi toplayabilir duruma gelmiştir. Bu kişinin rızası dışında olduğu için aslında özel hayatın gizliliği hakkının da ihlali anlamına gelmektedir.

Çalışmanın temelinde yer alan “Siber Uzayda Özel Hayatın Gizliliği Hakkı”, yukarıda saydığımız nedenlerden dolayı önem arz etmektedir. Çünkü ilk olarak siber uzayda yaşanan gelişmeler, haklar ve hatta kavramlar arasındaki çatışmayı da beraberinde getirmektedir. Özellikle uluslararası hukuk ve mahkeme kararlarında alana ilişkin net bir tanımlamanın yapılmaması bu kavram kargaşasını adeta içinden çıkılamaz bir hale sokmaktadır.

Tezin Amacı

Özellikle günümüzde, internetin yaygın kullanımı, dijitalleşme ve akıllı cihazların hayatımızın her alanına girmesi ile birlikte, siber uzayda özel hayatın

gizliliği hakkının korunması giderek daha önemli hale gelmiştir. Siber uzayda özel hayatın gizliliği hakkının ihlali, kişilerin mahremiyetinin ihlal edilmesine, kişilik haklarının zedelenmesine ve hatta suç mağduru olmasına neden olabilmektedir. Bu nedenle, siber uzayda özel hayatın gizliliği hakkının korunması için hukuki ve teknik önlemlerin geliştirilmesi ve uygulanması büyük önem taşımaktadır.

- Siber uzayda özel hayatın gizliliği hakkının kapsamını ve sınırlarını belirlemek. Bu amaç doğrultusunda tezin, siber uzayın tanımı, siber uzayda veri toplama ve işleme yöntemleri, siber uzayda özel hayatın gizliliği hakkının ihlali riskleri gibi konularda kapsamlı bir araştırma yapması gerekir.
- Siber uzayda özel hayatın gizliliği hakkının korunması için mevcut hukuki, siyasi ve teknik önlemleri değerlendirmek. Bu amaç doğrultusunda tezin, ulusal ve uluslararası hukukta özel hayatın gizliliği hakkının korunması için mevcut düzenlemeleri, siber uzayda özel hayatın gizliliği hakkının korunması için geliştirilen teknik önlemleri ve bu önlemlerin etkinliğini değerlendirmesi gerekir.
- Siber uzayda özel hayatın gizliliği hakkının korunması için yeni hukuki, siyasi ve teknik önlemler önermek. Bu amaç doğrultusunda tezin, siber uzayda özel hayatın gizliliği hakkının ihlali risklerini azaltmak için yeni hukuki ve teknik önlemler önermesi gerekir.

Siber uzayda özel hayatın gizliliği hakkı ile ilgili bu tez, bu alandaki hukuki ve teknik gelişmeleri takip etmek ve bu gelişmelere katkıda bulunmak için önemli bir fırsat sunmaktadır.

Tezin önemi

Literatürde siber uzayda özel hayatın gizliliği hakkı ile ilgili önemli çalışmalar bulunmaktadır. Bu çalışmalarda, siber uzayda özel hayatın gizliliği hakkının kapsamı, sınırları ve korunması gibi konular ele alınmıştır. Ancak, literatürde bu alanda hala bazı eksiklikler ve boşluklar bulunmaktadır.

Bu eksikliklerden ve boşluklardan bazıları şunlardır:

- Siber uzayda özel hayatın gizliliği hakkının kapsamının tam olarak tanımlanamamış olması: Siber uzayda özel hayatın gizliliği hakkı, geleneksel

anlamdaki özel hayatın gizliliği hakkının ötesine geçmektedir. Siber uzayda, bireylerin kişisel verileri, çevrimiçi etkinlikleri ve hatta düşünceleri bile özel hayat kapsamında değerlendirilebilir. Ancak, siber uzayda özel hayatın gizliliği hakkının kapsamının tam olarak tanımlanamaması, bu hakkın ihlallerinin tespit edilmesini ve önlenmesini zorlaştırmaktadır.

- Siber uzayda özel hayatın gizliliği hakkının sınırlarına ilişkin tartışmaların yetersiz olması: Siber uzayda özel hayatın gizliliği hakkı, diğer temel hak ve özgürlüklerle çatışabilir. Örneğin, suçun önlenmesi veya kamu güvenliğinin sağlanması gibi nedenlerle, devletlerin bireylerin özel hayatına müdahale etmesine ihtiyaç duyulabilir. Ancak, bu müdahalelerin özel hayatın gizliliği hakkını aşırı derecede ihlal etmemesi gerekir. Siber uzayda özel hayatın gizliliği hakkının sınırlarına ilişkin tartışmaların yetersiz olması, bu hakkın korunması için etkili önlemlerin alınmasını zorlaştırmaktadır.
- Siber uzayda özel hayatın gizliliği hakkının korunması için uluslararası hukukun yetersiz olması: Siber uzayda özel hayatın gizliliği hakkı, uluslararası hukukta henüz tam olarak güvence altına alınmamıştır. Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi, siber uzayda özel hayatın gizliliği hakkını korumak için bir temel oluşturmaktadır. Ancak, bu madde, siber uzayın kendine özgü özelliklerini dikkate almamaktadır. Siber uzayda özel hayatın gizliliği hakkının korunması için uluslararası hukukun geliştirilmesi gerekmektedir.

Bu eksiklikler ve boşluklar, siber uzayda özel hayatın gizliliği hakkının korunması için önemli zorluklar yaratmaktadır. Bu zorlukların giderilmesi için, literatürde yapılan çalışmaların kapsamının genişletilmesi ve bu alandaki tartışmaların derinleştirilmesi gerekmektedir. Bu tez bu noktalarda katkı yapmayı hedeflemektedir.

Tezin Soruları

Siber uzayda özel hayatın gizliliği hakkı ile ilgili bu tez, şu temel soruların cevaplarını arar:

- Siber uzayda özel hayatın gizliliği hakkının tanımı ve kapsamı nedir?
- Siber uzayda özel hayatın gizliliği hakkının ihlali nasıl gerçekleşebilir?

- Siber uzayda özel hayatın gizliliği hakkının korunması için hangi hukuki ve teknik önlemler alınabilir?

Bu temel soruların cevabını bulmak için tez, şu yardımcı sorulara da cevap vermeye çalışır:

- Siber uzayda özel hayatın gizliliği hakkının kapsamına giren alanlar nelerdir?
- Siber uzayda özel hayatın gizliliği hakkının ihlali hangi şekillerde gerçekleşebilir?
- Siber uzayda özel hayatın gizliliği hakkının korunması için hangi hukuki düzenlemeler mevcuttur?
- Siber uzayda özel hayatın gizliliği hakkının korunması için hangi teknik önlemler alınabilir?

Tez, bu sorulara cevap verirken, siber uzayın kendine özgü özelliklerini göz önünde bulundurmalıdır. Siber uzayda, fiziksel sınırlar ortadan kalktığı için, özel hayatın gizliliği hakkının ihlali daha kolay gerçekleşebilir. Ayrıca, siber uzayda, büyük miktarda veri depolandığı ve işlendiği için, bu verilerin gizliliğinin korunması daha zordur.

Tez, bu soruların cevaplarını verirken, uluslararası hukuk mevzuatını da incelemelidir. Uluslararası hukukta, özel hayatın gizliliği hakkı, EİHB, Avrupa İnsan Hakları Sözleşmesi (AİHS) ve Birleşmiş Milletler Siber Güvenlik İlkeleri gibi belgelerde düzenlenmiştir.

Tezin Metodolojisi ve Yaklaşımlar

Tez çalışması kapsamında çalışılan konunun içeriği gereği birden fazla bilimsel yöntem kullanılması öngörülmektedir. Bunlar arasında literatür taraması, belge analizi, söylem analizi ve gerektiğinde kıyasa başvurulacaktır.

İlk olarak; “Siber Uzay ve İnsan Hakları” ve “Özel Hayatın Gizliliği Hakkı” bölümleri ele alınırken literatür taraması yapılacaktır. Başka bir deyişle siber uzay ve insan haklarının ortaya çıkması bugüne kadar var olan kaynaklar bağlamında değerlendirilerek gelişimsel seyri ele alınacaktır. Literatür taraması, siber uzayda özel hayatın gizliliği hakkı ile ilgili tezde, konuyla ilgili mevcut bilgi birikimini ve

tartışmaları ortaya koymak için kullanılan bir yöntemdir. Bu yöntemde, konuyla ilgili kitaplar, makaleler, raporlar, tezler ve diğer kaynaklar incelenerek elde edilen bilgiler sistematik bir şekilde analiz edilir.

Literatür taraması yaparken dikkat edilmesi gereken şey kaynakların analizi gelir. Literatür taraması sırasında, elde edilen kaynaklar dikkatlice analiz edilmelidir. Bu analizde, kaynakların içeriği, yazarları, yayın tarihleri ve diğer önemli bilgiler göz önünde bulundurulmalıdır.

Kıyas ise, farklı kaynaklarda yer alan bilgilerin karşılaştırılması için kullanılan bir yöntemdir. Bu yöntemde, aynı konuda farklı kaynaklarda yer alan bilgiler bir araya getirilerek karşılaştırılır. Bu karşılaştırma sonucunda, konuyla ilgili farklı bakış açıları ve tartışmalar ortaya çıkar.

Belge inceleme, siber uzayda özel hayatın gizliliği hakkı ile ilgili bu tezde, belirli bir belgenin içeriğini ve amacını ortaya koymak için kullanılan bir yöntemdir. Bu yöntemde, incelenen belgenin metni, grafikleri, tabloları ve diğer unsurları dikkatlice analiz edilir. Bu çerçevede belgenin içeriği, amacı ve bulguları analiz edilir.

Siber uzayda özel hayatın gizliliği hakkı ile ilgili bu tezde, bu yöntemlerin birlikte kullanılması, daha kapsamlı ve derinlemesine bir araştırma yapılmasını sağlayacaktır.

Tezin Sayıtları

Tezin sayıtları aşağıda maddeler halinde yer almaktadır;

i) Günümüzde teknoloji baş döndürücü bir hızla ilerlemektedir. Bireyler, özel şirketler ve hükümetler bu yeni alanda aktif rol oynamaktadır. Ancak bireyler bir yandan teknolojik gelişmelerden fayda sağlarken diğer yandan da mağdur olmaktadır.

ii) İnsan hakları da bu gelişen teknolojiye olumlu ve olumsuz yönde etkilenmektedir. Ancak insan hakları durağan bir yapı olmadığı için dinamik bir şekilde ilerlemekte ve yeni kuşak insan haklarının bahsi geçmektedir.

iii) Siber uzay teknolojisinin gelişmesiyle birlikte özel ve kamusal alan kavramları birbirleriyle çelişmeye başlamış bu bağlamda genelde insan hakları özelde özel hayatın gizliliğine karşı siber uzayda yeni tehditler ortaya çıkmıştır,

iv)Siber uzayda, fiziksel dünyadaki gibi özel hayatın gizliliği hakkının korunması gerekir. Bu, kişilerin dijital ortamda da mahremiyetlerine saygı gösterilmesini isteme hakkının olduğu anlamına gelmektedir,

v) Uluslararası hukuk siber uzayda gelişen teknolojilere ayak uyduramamaktadır. Söz konusu insan hakları olduğu için uluslararası hukuğun ve mahkeme kararlarının daha dinamik bir yapı olması gerektiği ortadadır.

vi) Siber uzayda, özel hayatın gizliliği hakkının korunması için yeni hukuki düzenlemelere ihtiyaç vardır. Mevcut hukuki düzenlemeler, siber uzayın doğası gereği yeterli olmayabilir.

vii) Uluslararası hukuk anlayışının siber uzayı da ele alabilecek kadar genişlemesi gerektiği ortadadır.

viii) Siber uzay bağlamında özel hayatın gizliliği tekrar tanımlanmalı ve tanımın kapsamı genişletilmelidir.

Tezin Sınırlılıkları

Siber uzay ve insan hakları literatürü incelendiğinde, bahsi geçen kavramlar üzerinde oydaşma bulunmadığından dolayı kavramların her yazar tarafından farklı yorumlandığı görülmüştür. Dolayısıyla tezdeki bilgilerin bir yığın haline dönüşmemesi için birtakım kısıtlar belirlenmiştir. İlk olarak, çalışma kapsamında özel hayatın gizliliği bağlamında siber uzayın kavramsal çerçevesine yer verilecektir. İkinci olarak, siber uzay ve insan hakları kavramları açıklanırken özel hayat tanımlanacak ve bu bağlamda özel hayatın kapsamı ve özel hayatla ilgili kavramlar ele alınacaktır. Üçüncü olarak, uluslararası ve bölgesel sözleşmelere yer verilirken özel hayatın gizliliği hakkının yer aldığı belgeler çalışmada ele alınacaktır. Böylece bu hakkın bölgesel ve uluslararası sözleşmelerde nasıl tanımlandığı ve ele alındığı görülebilecek, ilgili belgeler hakkın tanımını açısından kıyaslanabilecektir. Dördüncü ve son olarak ise, siber uzayda özel hayatın gizliliğini en çok ihlal eden alanlar siber gözetim, siber istihbarat ve kişisel verilerin korunması olarak belirlenmiştir. Dolayısıyla son bölümde yapılacak tartışmanın sınırları bu alanlar içerisinde olacaktır. Ayrıca yine aynı alanların Avrupa İnsan Hakları Mahkemesi kararları çerçevesinde nasıl ele alındığına

yer verilecektir. Böylece kavram sadece teorik olarak değil, pratiklerden de yola çıkılarak tanımlanacaktır.

Literatür Taraması

Siber uzayda özel hayatın gizliliği hakkı, son yıllarda giderek daha önemli hale gelen bir konudur. İnternet ve diğer dijital teknolojilerin yaygınlaşmasıyla birlikte, bireylerin özel hayatları daha da görünür hale gelmiştir. Bu durum, özel hayatın gizliliği hakkının ihlallerine yol açabilecek yeni riskler yaratmıştır. Tezin bu bölümünde konu ile ilgili özgün makaleler ve kitaplara yer verilmiştir. İlgili literatür taraması ele alındığında;

- i. Siber uzayda özel hayatın gizliliği hakkının ihlalini ele alan çalışmalar,
- ii. Çevrim içi ihlali korumaya yönelik norm ve standartlar geliştirilmesi gerekliliğini öneren çalışmalar,
- iii. Siber uzayda özel hayatın gizliliği hakkını korumak için uluslararası işbirliği yapılması gerektiğini ele alan çalışmalar,
- iv. Siber güvenlikte teknik yaklaşımdan ziyade insan unsurunun temel alınması gerektiğini ifade eden çalışmalar yer almaktadır.

Siber uzayda özel hayatın gizliliği hakkının ihlaline değinen çalışmalardan ilki Mbanaso ve Dandaura “The Cyberspace and Intensification of Privacy Invasion” (2015) isimli makalesidir. Soyut bir kavram olan mahremiyetin, bir yandan kullanıcılara hizmetleri ve kaynakları daha erişilebilir hale getirirken diğer taraftan kullanıcıların bu tür hizmete güvenilip güvenilmeyeceğini sorguladığından bahsetmektedir. Makalede ayrıca gelişmekte olan teknolojilerin kullanıcıların mahremiyetini gizlice nasıl ihlal ettiğini ve mevcut özel hayatın gizliliğinin yetersizliklerini ortaya çıkarmaktadır. Ayrıca siber uzayın bireyin mahremiyetini koruma konusunda daha fazla araştırılması gerektiğini de dile getirmektedir. Sonuç olarak yazara göre, siber uzay ortamında özel hayatın korunmasına dair mahremiyet, gizlilik ve güvenliği sağlayabilen bütünleşik bir yaklaşımın sorunun çözümünde önemli bir rol alacağını belirtmektedir (Mbanaso ve Dandaura; 2015, s. 24-31).

Debatin ise “Ethics, privacy, and self-restraint in social networking. In Privacy online” isimli makalesinde sosyal ağlarda özel hayatın gizliliği ilkesinin ancak

bireyleri bu konuda eğitmekle mümkün olabileceğini, bu konuda çalışan tüm paydaşların (sistem geliştirici, eğitimci vb.) bir bütün olarak toplumda mahremiyet okuryazarlığını teşvik eden bir ortam yaratmaktan da sorumlu olduğuna vurgu yapmıştır (Debatin, 2011, s. 47-60).

Barrett-Maitland ve Lynch, “Social Media, Ethics and the Privacy Paradox”, isimli çalışmalarında siber uzayda özel hayatın gizliliğini sosyal medya üzerinden anlatmaktadır. Özel hayatın gizliliğinin evrensel bir hak olduğunu savunanlarla birlikte, mahremiyetin “iklim, din, teknolojik ilerleme ve siyasi düzenlemeler” gibi çeşitli faktörlere bağlı olarak farklılık gösterebileceğinden, aynı zamanda göreceli olarak da görülebileceğinden bahsetmiştir. Teknolojik gelişmelerle birlikte mahremiyetin yeniden tanımlandığı dünyada sosyal medya ancak etik ve ahlaki ilkeler çerçevesinde kullanıldığı takdirde mahremiyet ihlallerinin sayısının düşürebileceğinden ve bununda ancak kullanıcıların siber uzay konusunda eğitilmeleri ile mümkün olabileceğinden bahsetmektedir (Barrett-Maitland ve Lynch, 2020, s. 1-11).

Jørgensen, “The right to privacy under pressure” isimli makalesinde siber uzayda özel şirketlerin ve yetkililerin özel hayatın gizliliği konusunda şeffaf olmadığından ve kullanıcıların çoğu zaman nette sunulan hizmetleri kullanabilmesi için çeşitli sözleşmeleri onay vermek zorunda kaldıklarından bahsetmektedir. Bunun yanı sıra uluslararası düzeyde verilerin korunması için ortak bağlayıcı standartlar olmadığını dile getiren yazar aynı zamanda internetteki altyapı ve temel hizmetlerin çoğunun özel şirketler tarafından yönetilmesini de risk unsuru olarak göstermektedir. (Jørgensen, 2020, s. 165-170).

Vilić ve Radenković, “The Right to Privacy, Informational Privacy and the Right to Information in the Cyberspace” isimli makalesinde, Özel hayatın gizliliği hakkı ve bilgi edinme hakkının siber uzayda çatışan iki hak olduğunu belirtmişlerdir. Bu iki hakkın yasal olarak düzenlenmesi, onların dengesi ve uyumunun sağlanması gerektiğini ifade etmektedir. Özellikle kamu yararının gözetildiği bazı durumlarda belirli bilgilere erişime sahip olma ve özel hayatın gizliliği çatıştığında, özel hayatın gizliliği ilkesine öncelik verilmesi suretiyle hakların yasal uyumu ve dengesinin sağlanması gerektiğinden bahsedilmektedir (Vilić ve Radenković, 2017, s.74-78).

Daniel Solove tarafından kaleme alınan "A Taxonomy of Privacy" isimli makalenin temel argümanı, hukuk sisteminin özel hayatın gizliliğini ne şekilde sınıflandırabileceğine ilişkin bir çerçeve sunmaktır. Makalesini William Prosser'ın çalışmalarına dayandıran Solove bugüne kadar iyi bir şekilde tanımlanmamış ve muğlak olan özel hayatın gizliliğinin sorunlarını analiz etmek için bir çerçeve sağlamaktadır (Solove, 2006, s.477-564).

Rona ve Aarons, "State responsibility to respect, protect and fulfill human rights obligations in cyberspace" isimli makalesinde, uluslararası insan hakları hukukunun içeriğini siber uzay kapsamında ele almaktadır. İnsan hakları hukukunun siber uzaya uygulanması gerektiğini dile getiren yazar, devletlerin de siber uzayda bu haklara saygı göstermesi ve hakları koruması gerektiğini belirtmektedir. Varolan uluslararası hukukun siber uzaya uygulanmasının zor olduğunu, devletlerin insan haklarına yalnızca saygı göstermekle kalmayıp aynı zamanda bu haklara saygı göstermeyi de sağlama yükümlülüğü olduğuna dikkat çekmektedir. Bu bağlamda devletlerin, insan hakları ihlali teşkil edecek davranışlarda bulunmasını engelleyen yasal tedbirler almaları istenmiştir (Rona ve Aarons, 2016, s. 503-530).

Çevrim içi ihlali korumaya yönelik norm ve standartlar geliştirilmesi gerekliliğini öneren çalışmalar ise aşağıda yer almaktadır.

Yao, "Self-protection of online privacy: A behavioral approach", makalesinde siber uzayda özel hayatın gizliliğinin korunması, bireyin sanal ortamdaki risklerin farkında olup kendini koruma stratejileri benimsemesi sayesinde olabileceğinden bahsetmektedir. Bireyin çevrimiçi mahremiyet konusunda endişeli olmasına rağmen, mahremiyetini ihlal edebilecek uygulamalar hakkında çok az bilgiye sahip veya birey bunun farkında olsa dahi interneti kullanırken buna dikkat etmediğine vurgu yapmaktadır. Tüm bu nedenlerden dolayı, yazara göre çevrimiçi özel hayatın gizliliğinin korunmasına yönelik davranışsal bir yaklaşım, normatif bakış açısına göre daha tercih edilebilir olduğunu dile getirmektedir (Yao, 2011, s. 111-125).

Nissenbaum, "A Contextual Approach to Privacy Online" genel olarak çevrimiçi mahremiyeti korumak için İnternet'in ticari olmayan kullanımlarını da içeren yeni öneriler sunmaktadır. Örneğin kanun koyucular toplumda var olan sosyal değerleri

İnternet'teki benzer uygulamalara adapte etmeli ve çevrimiçi yaşamın çeşitli yönleri için uygun bilgi akışına dayalı normlar geliştirmelidir. Bu bağlamda teknolojik şirketler ve yasa koyucular, özgürlük veya mahremiyet gibi temel demokratik değerlere bağlı ve bu değerlerle tutarlı çevrimiçi normlar oluşturmalı ve teknolojik olanların aksine (var olan düzen) "ahlaki zorunlulukları" (moral imperative) güçlendirmelidir (Nissenbaum, 2011, s. 32-48).

Jørgensen ve Desai “Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google” makalelerinde Amerika Birleşik Devletleri ve Avrupa sistemlerini kullanıcıların özel hayatının gizliliği ve veri koruma hakları ile Google ve Facebook gibi çevrimiçi platformların uygulamaları arasındaki çatışmayı araştırmaktadır. Her iki sistem de bu platformlar veri toplama ve verilerin yeniden düzenlenmesi, online ticaret modelinin merkezinde yer aldığından, bu platformlar, kullanıcılarına iyileştirilmiş bilgi sağlama talebini yerine getirmekte ancak maksimum kişisel veri toplamaya devam ettiklerinden bahsetmektedir. Çevrimiçi özel hayatın gizliliği hakkı tartışılan makalede, özel hayatın gizliliği hakkını koruyacak norm ve standartların geliştirilmesi gerektiği ifade edilmektedir (Jørgensen ve Desai, 2017, s.106-126).

Rengel, “Privacy as an International Human Right and the Right to Obscurity in Cyberspace” çevrimiçi teknolojiler bağlamında özel hayatın gizliliğinin korunmasının mevcut yasal çerçevenin belirsiz olduğundan ve bu alandaki mevcut teknolojiyle, bu hakların ihlal edilme potansiyeli ile başa çıkmak için yetersiz olduğundan bahsetmektedir. Bireyi siber uzayda korumak için ‘right to obscurity’ nı önerir. Yazara göre bu hak, siber uzayda kullanıcılarla ilgili tanımlayıcı bilgilere erişimin korunmasıyla elde edilmektedir. Erişim koruması, içeriğe erişimi yönetmek için çeşitli teknoloji ve yöntemleri kapsamaktadır. Bir kullanıcının özel kalmasını istediği bilgilerin korunması ve erişime kapatılması ile bireyin bilgilerini koruyan düzenleme ile de elde edilebileceğinden söz eden yazar “Obscurity” kavramının yakın gelecekte internetin geçtiği sözleşmelerde “özel hayat” kavramı yerine kullanılabileceğini dile getirmektedir (Rengel, 2014, s.37-42).

David Lyon’ın Gözetim Çalışmaları isimli kitabı, gözetim tarihi, gözetim ve güç arasındaki ilişki, yeni teknolojilerin gözetim üzerine etkisini kapsayan kapsamlı bir

alıřma olarak karřımıza ıkmaktadır. Gemiřten gnmze gzetimin ne řekilde deėiřtiėini rneklendirerek bireylerin ve grupların hkmetler, zel řirketler ve diėer kuruluřlar tarafından ne řekilde gzetlendiėini incelemektedir. Gzetim ve iktidar arasındaki iliřkiye de deėinen Lyon, bireylerin sosyal medya, teknolojik cihazlar ve mobil cihazları kullanımı sayesinde gzetimde pasif olarak yer almadıklarını, aynı zamanda veri retimine de aktif olarak katıldıklarını savunmaktadır (Lyon, 2013).

Boyd, “Networked Privacy. Surveillance & Society” isimli makalesinde zel hayatın gizliliėi sorununun sosyal medya ve teknoloji kullanımının artmasıyla ivme kazandıėını dile getirirken bireylerin siber uzayda sayısız ekseninde birbirine baėlandıėını ve insanların, hayatları bu kadar birbirine baėlıyken siber uzayda bireysel kontrol saėlayabilmelerinin zorluėunu dile getirmektedir. Dolayısıyla siber uzayda zel hayatın gizliliėinin korunmasının merkezine aėları, grupları ve toplulukları konumlandıran modeller geliřtirmemiz gerektiėi ve kullanıcıların, bařkalarının hayatlarının yorumlama řeklini olumsuz etkilemeyecek řekillerde paylařmaya zgrleřtirerek glendirmenin bir yolunu bulmasının gereklilik olarak grmektedir (Boyd, 2012, s. 348-350).

Rao, “Human rights and Cyberspace: Use and Misuse” isimli makalesinde, siber alan ve insan hakları baėlantısını hem uluslararası szleřmelerden hem de Hindistan da var olan yasalar zerinden aıklamıřtır. Yazara gre, siber uzay iyi ve kt ynde kullanılabilir ancak siber uzayın anonim yapısı gnmzde internetin faydalarını baltalamaktadır. Her gn insan hakları ihlallerinin ve bir bireyin mahremiyetinin siber alandaki son geliřmelerle tehlikede olduėunu savunmaktadır. Makalesinde her bir insan hakkı iin zm reten yazar, siber uzayda zel hayatın gizliliėi hakkının korunabilmesi iin ynetiřim, bilgi iletiřim teknolojileri, yasalar ve yasaların uygulama alanlarının etik bir řekilde ele alınması gerekliliėini vurgulamaktadır (Rao, 2016, s. 5-31).

nnc bařlık olan siber uzayda zel hayatın gizliliėi hakkını korumak iin uluslararası iřbirliėi yapılması gerektiėini ele alan alıřmaların diėer alıřmalardan daha fazla olduėu grlmektedir. Bu alıřmalardan ilki, Donedo ve Almeida’nın “Privacy governance in cyberspace” isimli makalesidir. Bu makalede zel hayatın heterojen (znel) bir yapıya sahip olduėunu ve bunun da zel hayat kavramı ele

alınırken oydaşmanın zorluğunu ortaya koyduğunu belirtmektedirler. Bu yüzden özel hayatın gizliliği, her ülkenin kendi hukuk sistemi içerisinde o ülkeye özgü yasal çerçevede çizilmesine neden olmakta ve evrensel koordinasyon için gerekli tanımlamalar atlanmaktadır. Siber uzayda özel hayatın korunması konusu küresel bir sorun olarak yaklaşan yazarlar özel hayatın gizliliğine yönelik yeni bir yaklaşımın, sadece mahremiyet ve veri korumayla ilgili düzenlemeleri değil, aynı zamanda birey ve dünya arasında etkileşim sağlamaya yardımcı olan tüm faktörleri birbirine bağlayarak ortaya çıkarabileceğini ifade etmektedirler. Dolayısıyla küresel siber uzayda veri koruma ve özel hayatın gizliliği ile ilgili çok paydaşlı mekanizmalar oluşturma fırsatı, farklı aktörleri ve çıkarları müzakere masasına oturtan alternatif yollar ışığında araştırılması gerektiğini dile getirmişlerdir (Doneda ve Almeida, 2015, s. 50-53).

Goldstein, Tov ve Prazeres (2018) yılında yayımladığı “Report Privacy in Digital Age” isimli raporda; siber uzayda özel hayatın gizliliğinin şirketler, çıkar grupları ve hükümetler tarafından suistimal edildiğinden bahsetmektedir. Dijital ortamlarda meydana gelen insan hakları ihlallerini kabul etmeli ve özel hayatın gizliliği hakkını sağlamak için uluslararası bir toplum olarak pragmatik adımlar atmamız gerektiğinden ve bunun da ancak çok uluslu bir ittifakla sağlanabileceğinden bahsetmektedir (Goldstein, Tov ve Prazeres, 2018).

Joseph Nye; “The regime complex for managing global cyber activities” (2014) isimli raporunda, siber faaliyetlere yönelik yönetim modeli sunmaktadır. Siber güvenlik ve insan haklarına da değinen Nye siber uzaydaki teknolojinin değişkenliği, ekonomik ve siyasal çıkarların hızlıca dönüştüğünü ve dolayısıyla siber uzayda yer alan aktörlerin çıkarlarını nasıl tanımladıklarını ile ilgili olarak siber uzayda yer alan sorunları yönetecek normatif yapıların geleceğini tahmin etmenin mümkün olmadığını dile getirmektedir. Ayrıca diğer yazarların yanı sıra Nye, küresel anlaşmalardan ziyade aynı tutumda olan devletlerin siber uzayda istikrarı bozan davranışları önlemek için öncelikli olarak birlikte hareket edebileceğinden ve daha sonrasında geniş bir aktör grubuna genelleştirmeye çalışabileceğinden bahsetmektedir (Nye, 2014, s. 5-15).

Fischer-Hübner; “Privacy at risk in the global information society” isimli çalışmasında siber uzayda ekonomik fırsatlar vurgulanırken sosyal etkilerin ihmal

edildiğinden bahsetmektedir. Teknoloji temelli programların çoğunun temel olarak ekonomik çıkarlar tarafından motive edildiğini dile getirmektedir. Dolayısıyla bilgi iletişim altyapısı tasarlanırken özel hayatın gizliliğinin kabul edilebilir olması için minimum gereksinimler belirleyen yazar, bir direktif veya kural belirlenecekse öncelikle pilot projelerde test edilmesi gerektiği ve özel hayatın gizliliğine yönelik kabul edilemez riskler taşıyorsa bu kural ya da direktiflerin uygulanmaması gerektiğini belirtmektedir. Bunun yanı sıra yazara göre, güvenlik ve mahremiyet konuları baştan düşünülmeli ve sistem tasarımına entegre edilmelidir. Bunun yanısıra özel hayatın gizliliğinin uluslararası olarak tanımlanmasının bir ihtiyaç olduğunu vurgulamaktadır (Fischer-Hübner, 1997, s. 261-274).

Mbanaso “Personal Data Privacy and Security–Who, What, When, Why, Where and How” isimli çalışmasında ise özel hayatın gizliliğinin işlenmesi ve korunmasının hala karmaşık ve sorunlu olduğu söylemektedir. Özel hayatın gizliliği ele alınırken teknoloji, hukuk ve politikanın göz ardı edilmemesi gerektiğini ve bunların kanunlar, yönergeler ve ilkeler tarafından yönlendirilen güçlü yerel ve uluslararası desteğe sahip olması gerektiğini dile getirmektedir. Özel hayatın gizliliğini ancak esnek ve sağlam yapılandırılabilir bir politika mimarisi ile sağlanabileceğini vurgulamaktadır (Mbanaso, 2018, s.1-8).

Bernal “Internet Privacy Rights: Rights to Protect Autonomy” isimli çalışmasında özel hayatın gizliliği ile ilgili yasalar arasında birtakım çatışmalar bulunduğunu dile getirmektedir. Bu çatışmalar hem ilgili yasaların kendi içerisindeki çelişme (daha önce kabul edilen uluslararası sözleşmeler veya ülkelerin kendi iç hukuklarıyla çelişme) hem de ilgili grupların ihtiyaç ve hakları arasındaki çatışmadan doğduğuna değinmektedir. Bazı yasaların hükümetler tarafından zor kabul edilirken bazılarının da kabul edildikten sonra uygulamada sorunlar yaşandığını tespit eden Bernal, siber uzay teknolojisinin ayrıntılı bir analiz için çok karmaşık, değişken ve hızlı bir yapıya sahip olduğunu vurgulamaktadır. Dolayısıyla anlık olarak duruma müdahale ederek bu duruma yönelik önlemler almak yanıltıcı olabileceğine değinen Bernal, dijital çağda özel hayatın gizliliğine yönelik daha güçlü yasal korumaların olması gerektiğini ifade etmektedir (Bernal, 2014, s. 82-117).

PoKempner; “Cyberspace and State Obligations in the Area of Human Rights” isimli makalesinde diğer yazarlardan farklı olarak ilk önce siber uzayın avantajları üzerinden durmuş ve özellikle ekonomik, sosyal ve kültürel hakların çevrimiçi iletişimden büyük faydalar elde ettiğine değinmiştir. Her ne kadar siber uzay teknolojileri birçok hakkın gerçekleştirilerek daha çok insana ulaşmasını sağlasa da özel hayatın gizliliği hakkını devlet gözetiminden korumak için kapsamlı bir uluslararası çerçevenin bulunmamasından dolayı devletler arasında daha fazla iş birliğine duyulan ihtiyacı tartışmaktadır (PoKempner, 2013, s.239-260).

Damen, Köhler ve Woodard “The Human Right of Privacy in the Digital Age” makalelerinde, dijital çağda özel hayatın gizliliğine yönelik birtakım çözüm önerileri sunmaktadır. Bu bağlamda özel hayatın gizliliği tanımının evrensel olarak açıklığa kavuşturulması gerektiğini ve Birleşmiş Milletler gibi uluslararası organların daha güçlü uygulama mekanizmaları geliştirmeye gerek duyulduğunu vurgulamışlardır. Siyasi aktivist ve sivil toplumun da kamu ve özel sektöre baskı yapması gerektiğini dile getiren yazarlar ayrıca özel hayatın gizliliği hakkının ihlali ile ilgili tüm konuların kamuya açık olması ve verilen bilgilerin yeterli, şeffaf, erişilebilir ve hesaplanabilir olması gerektiği söylemektedirler (Damen vd. , 2017, s.3-14).

Moise “Cybersecurity and Human Rights” adlı çalışmasında, internetin, insan haklarının uygulanması için benzeri görülmemiş fırsatlar sunduğundan ancak bu fırsatları sunarken bir yandan da bazı şirketlerin, müşterilerinden büyük miktarda kişisel veriler elde ettiğine değinmektedir. Böylelikle bu şirketler ve suç örgütleri kullanıcıların özgürce gönderdiği veya bilgisi olmadan toplanan kişisel verileri alıp satarak büyük karlar elde etmektedir. İnternet alanında faaliyet gösteren özel sektör, dijital alanda kişisel verilerin ve özel hayatın gizliliğinin korunmasını internette yapılan ticari faaliyetleri olumsuz etkileyen bir kısıt olarak gördüğünü vurgulamaktadır. Bu yüzden siber güvenlik kullanıcılarına hem ulusal hem de uluslararası düzeyde mücadele için uygulanabilir çözümler sunmak zorunda olduğunu belirtmektedir (Moise, 2016, s.160-164).

Son başlık olan siber güvenlikte teknik yaklaşımdan ziyade insan unsurunun temel olarak alınması gerekliliğini dile getiren çalışmalardan ilki, Deibert’in “Toward a Human-Centric Approach to Cybersecurity” isimli makalesidir. İlgili makalede

devletlerin kendi vatandaşlarının güvenliğine tehdit oluşturabileceği birçok yolu olduğunu ve bilgi iletişim teknolojilerinin hükümetlere bu tehditler konusunda nasıl yardım edebileceğini açıklamaktadır. Savaş zamanı durumlarının dışında bile devletler, gözetleme yoluyla ve hem siyasi muhaliflerin baskı altına alınmasını hem de diğer devletlerin işlerine karışmayı kolaylaştıran diğer araçlarla insanları tehdit edebilmektedir. Bununla birlikte, daha büyük bir topluluğu korumak adına bireysel haklar ne olacağı konusunda bir miktar devletin uzlaşmasını haklı çıkaran uzun süredir devam eden etik tartışmaların da olduğunu dile getirmektedir. Bireysel ve devlet güvenliği arasındaki bu ödünleşimin tahkim edilmesi, devletlerin ahlaki konumu ve devletlerin ve vatandaşların birbirlerine karşı hakları ve görevleri hakkındaki daha büyük tartışmalara neden olacağını belirtmektedir (Deibert, 2018, s.411-424).

Cavelty, “Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and engineering ethics” makalesinde sorunu hem güvenlik hem de esas olarak devlet aktörlerinin uygulamalarına odaklanarak ele almıştır. Siber uzayın insan güvenliğine olan etkilerini tanımlayan yazar, mevcut sistemle ilgili sorunun, güvenliğin hem geleneksel devlet odaklı ulusal güvenlik hem de insan güvenliği açısından yetersiz üretilmesi olduğundan bahsetmektedir. Üretilen siber güvenlik türünün ekonomik ilkelere dayandığını ve ulusal güvenlik kavramınının siber uzaya genişletilmeye çalışılmasının özellikle özel hayatın gizliliği ve ifade özgürlüğü üzerinde bir etkiye sahip olduğunu dile getirmektedir. Çözümün sadece devletlerarası işbirliğinde bulunamayacağını aktaran yazar güvenlikle ilgilenen tüm paydaşlar için ortak bir ilgi konusuna odaklanılması gerektiğini savunmaktadır (Cavelty, 2014, s. 701-715).

Liaropoulos, “Reconceptualising cyber security: Safeguarding human rights in the era of cyber surveillance” makalesinde güvenliğin odağını siber uzaydaki insan haklarına kaydırarak siber güvenlik ikileminin paradoksları, siber uzaydaki tehditlerin doğası ve güvenliğin referans nesnesine ilişkin yanlış algılamaları bizlere sunmaktadır. İnsan unsurunun temelde yer alması gerektiği alternatif bir siber güvenlik görüşüne duyulan ihtiyaçtan bahsederken, devletlerin ise siber uzayda insan haklarını onaylama konusundaki isteksizliği ve küresel bir yönetim rejiminin olmaması, siber uzaydaki

insan haklarının geleceği için oldukça kasvetli bir çizdiğinden bahsetmektedir (Liaropoulos, 2016, s. 32-40).

Hollis ve Ohlin “What if Cyberspace Were for Fighting?” isimli makalesinde ise diğer makalelerden farklı olarak siber uzayda açıkça devletçi bir yönelim sergiledikleri görülmektedir. Ulusal savunma ve ulusal güvenliğin etik açıdan sorunsuz kavramlar olduğunu kabul eden yazarlar, hem hukukta hem de çatışma durumlarında devletlerin hakları ve görevlerinin en önde geldiği düşüncesini benimsemektedirler (Hollis ve Ohlin, 2018, s. 441-456).

Bu çerçevede literatürde var olan bazı eksiklikleri giderecek önemli çalışmalar yapılmıştır. Bu çalışmalara göz atıldığında hem mevcut literatür hem de gerekli olan çalışmalara ihtiyaç daha da net anlaşılabacaktır.

Tezin Akışı

Tezin çatısını belirleyen tezin akışına bakıldığında, tezin birinci bölümü “Siber Uzay ve İnsan hakları” başlığı altında ele alınmaktadır. Bu başlık altında öncelikle özel hayat bağlamında siber uzayın kavramsal çerçevesi çizilecek, kavramsal çerçeve çizilirken de siber uzay, siber güvenlik, siber saldırılar, siber suçlar, siber gözetim, siber şeffaflık ve siber istihbarat kavramlarının tanımlamalarına yer verilecektir. Bir diğer genel başlık olan “Bir İnsan Hakkı Olarak Özel Hayatın Gizliliği” başlığı altında ise özel hayatın tanımı, önemi, kapsamı ve özel hayatın gizliliği hakkının boyutları farklı tanımlar çerçevesinde ele alınacaktır. Özel hayatın kapsamı ele alınırken özel alan ve kamusal alan tartışmalarına yer verilecek, özel hayatın gizliliği hakkının boyutlarında ise kişisel veri ve kişilerin korunması, konuta müdahale etmeme, ad ve şöhret hakkı ve yazışmalar ele alınarak bu hakların nasıl tanımlandıkları ve içeriklerinin ne olduğuna değinilecektir. Bir diğer üst başlık ise “İnsan Haklarında Siber Uzayın Getirdiği Yeni Tartışmalar ve Özel Hayat” olarak adlandırılmaktadır. İlgili bölümde siber uzayın hayatımıza kattığı yeni haklara yer verilerek bu haklar özel hayatın gizliliği bağlamında tartışılacaktır. Yeni haklar; internete erişim hakkı, anonimlik hakkı ve unutulma hakkı olarak ele alınmıştır. Birinci bölümün son başlığı olan “Özel Hayatın Gizliliğine Yönelik Teorik Yaklaşımlar” bölümünde ise Alan Westin’in ve Irwin Altman’ın özel hayatın gizliliğine yönelik teorilerine yer verilecek

ve bu teorilerin benzer farklı yönleri irdelenirken, aynı zamanda özel hayatın gizliliğine yaptıkları katkılar ele alınacaktır.

Çalışmanın ikinci bölümü “Uluslararası Düzenlemelerde Özel Hayatın Gizliliği Hakkı” başlığını taşımaktadır. Bu bölümde öncelikle Birleşmiş Milletler (BM) düzenlemelerindeki uluslararası sözleşmeler ele alınacaktır. Özel hayatın gizliliği hakkının hangi aşamalardan geçerek uluslararası sistemde nihai halini aldığına yer verilecek, sonrasında ise “Evrensel İnsan Hakları Beyannamesi” ve “Sivil ve Siyasal Haklar Konvansiyonu (SSHK)”’nda bu hakkın nasıl ele alındığı açıklanacaktır. Çalışmanın ikinci alt başlığı olan “Avrupa Konseyi Düzenlemelerinde Özel Hayatın Gizliliği Hakkı” bölümünde ise Avrupa Konseyi nezdinde yapılan bölgesel sözleşmelere yer verilecektir. Bu bağlamda “Avrupa İnsan Hakları Sözleşmesi”, “Avrupa Konseyi Siber Suçlarla Mücadele Konvansiyonu” ve Biyotıp Sözleşmeleri’nde özel hayatın gizliliği hakkının nasıl ele alındığı açıklanacak ve sözleşmelerin benzer ve farklı noktaları vurgulanacaktır. “Diğer Uluslararası Düzenlemeler” başlığı adı altında ise yine bölgesel sözleşmelere yer verilerek farklı kıtalarda özel hayatın gizliliği hakkının nasıl tanımlandığına yer verilecektir. Bu kapsamda da “Amerikan İnsan Hakları Sözleşmesi”, “Avrupa Birliği Temel Haklar Bildirgesi”, “Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi” ve “Arap Ligi Siber Güvenlik Konvansiyonu” ele alınacaktır.

Çalışmanın üçüncü ve son bölümünde ise “Siber Uzay Özel Hayatın Gizliliği Hakkını Nasıl Etkiliyor” sorusuna cevap aramaya çalışılacaktır. Cevaplar aranırken öncelikle özel hayatın gizliliği hakkını en çok ihlal eden siber gözetim, siber istihbarat ve kişisel verilerin korunması alanları ele alınacaktır. İlgili bölümlerde bu alanların özel hayatın gizliliği hakkını hangi yönden ve ne şekilde etkilediği ayrıntılı bir şekilde tartışılacaktır. “Avrupa İnsan Hakları Mahkemesi Kararları (AİHM)” alt başlığında ise “Elektronik Gözetim”, “Kişisel Veri ve Kişisel Verilerin Korunması” ve “Yazışmalar” başlıklarında AİHM’nin kararları incelenerek teknolojiye dair güncel tartışmaların yargıya ne şekilde yansıdığı ele alınacaktır.

BİRİNCİ BÖLÜM

1.SİBER UZAY VE İNSAN HAKLARI

1990lı yıllarda internet kullanımının yaygınlaşması ve bilgi iletişim teknolojilerine olan bağımlılığın artması, yeni bir alanın ortaya çıkmasına neden olmuştur. Siber uzay olarak adlandırılan bu yeni alan fiziksel sınırları aşarak toplumları ve bireylerin yaşamlarını derinden etkilemiştir. Bireylerin birbirleri ve toplumla etkileşimi değişmiş, iletişim ve bilgi paylaşımı da biçim değiştirerek sanal ortamlara taşınmıştır. Bireyler bu dijital teknolojileri gündelik hayatlarının bir parçası haline getirdikçe, siber uzay fiziksel dünyanın adeta bir bağlantısı olarak günümüzde yerini almış ve yaşantımızın ayrılmaz bir parçasını oluşturmuştur. Bununla birlikte, fiziksel ve sanal alanın birbirine bağlanması ile başlayan bu dönüşümün insan haklarını da derinden etkilediği görülmektedir. Daha önce yüzyüze ilişkiler üzerine kurulan insan hakları da siber uzaya taşınarak bireyler için birtakım fırsatları ve zorlukları da beraberinde getirmiştir.

Bu bölümde öncelikle özel hayat bağlamında siber uzayın kavramsal çerçevesi ele alınacaktır. Daha sonra bu çalışmanın temelini oluşturan özel hayatın gizliliği farklı çerçevelerde tanımlanacak, özel hayatın önemi ve bu hakkının unsurlarına yer verilerek, dijital teknolojilerle birlikte hayatımıza giren yeni haklar tartışılacaktır. Son aşamada ise özel hayatın gizliliği hakkını ele alan teorilere değinilecektir. Böylece siber uzay ve özel hayatın gizliliği hakkı arasındaki ilişkinin tanımlanması amaçlamaktadır.

1.1. Özel Hayat Bağlamında Siber Uzayın Kavramsal Çerçevesi

Özel hayat bağlamında siber uzayın kavramsal çerçevesi ele alınırken siber uzayın özel hayatın gizliliğini etkileyen kavramlarına yer verilecektir. Bu minvalde öncelikle siber uzay kavramı tanımlanacak, sonrasında ise güvenlik, saldırılar, suçlar, gözetim, şeffaflık ve istihbarat kavramları siber uzay kapsamında ele alınarak açıklanacaktır.

1.1.1 Siber Uzay

Felsefi temellerini Platon'un "Mağara Alegorisi"nden alan siber uzay kelimesinin günümüzdeki semantik kimliği "sibernetik" teriminden türetilmiştir (Choucri, 2012, s. 7). Sibernetik terimi öncelikle 1834 yılında André-Marie Ampère tarafından Fransızca yayımlanan "Essai sur la philosophie" isimli eserinde, daha sonra ise Norbert Wiener'in 1948 yılında yazdığı "Cybernetics, or Control and Communication in the Animal and the Machine" kitabında yer almıştır. "Sibernetik, otomatik makinelerin ve insan sinir sisteminin işleyişindeki ortak unsurları bulmaya ve makinelerde ve canlı organizmalarda tüm kontrol ve iletişim alanını kapsayacak bir teori geliştirmeye çalışmaktadır" (Wiener, 1948, s.14). Wiener, ister makinede ister hayvanda olsun, kontrol ve iletişim teorisinin tüm bu alanını sibernetik olarak isimlendirmiştir (Wiener, 1948, s.12).

Weiner iletişim kavramını kontrol kavramıyla ilişkilendirerek, mesaj alışverişinin araçlara çevreleri üzerinde belirli bir kontrol imkanı sağladığını iddia etmiştir (Hildebrandt, 2014, s.34). Wiener'ın sibernetik kavramı, insanların makinelerle ara yüz oluşturabildiği ve bu ortaya çıkan sistemin etkileşim için alternatif ortam sağlayabileceği fikri de siber uzay kavramının temelini oluşturmaktadır (Ottis ve Lorents, 2010, s.267). Wiener'ın kitabında geliştirilen ve siber uzayın da temellerinden birini oluşturan olgulardan biri de "geri bildirim" olarak karşımıza çıkmaktadır. Bu geri bildirim döngüsü de makinelerin denetiminde devrime yol açacak ve böylece girdi-çıkı arasındaki süreçler ayarlanarak, bu yeni teknolojilerin kendilerini geliştirmeleri sağlanmaya çalışılacaktır. Bunu yaparken, insandan insana, insandan makineye ve makineden makineye iletişimin bilimsel olarak daha iyi anlaşılmasını amaçlamaktadır (Hildebrandt, 2014, s.34).

Sibernetik ve uzay kelimelerini birbirine bağlayarak, kelimenin bugünkü ismini veren ise William Gibson'dır. 1984 yılında "Neuromancer" isimli bilim kurgu kitabında siber uzay terimini ilk defa kullanan Gibson'a göre siber uzay;

Her gün milyarlarca meşru operatör tarafından, her ulusta, matematiksel kavramlar öğretilen çocuklar tarafından deneyimlenen rızaya dayalı bir halüsinasyon... İnsan sistemindeki her bilgisayarın bankalarından soyutlanmış verilerin grafiksel bir

temsili. Akıl almaz bir karmaşıklık. Zihnin uzay boşluğunda sıralanan ışık çizgileri, veri kümeleri ve takımyıldızları. Uzaklaşan şehir ışıkları gibi...(s.69)

Gibson'ın siberuzay kavramını açık bir şekilde tanımlamadığı görülmektedir. Ancak siber uzayı teknik karmaşıklık olarak ele almaktadır. Bu teknik karmaşıklık şu şekilde oluşmaktadır. Bilgisayarlar tarafından oluşturulan veri gösterimleri ağlar arasında aktarılmakta ancak aynı zamanda da psikoloji, epistemoloji, hukuki ve sosyal sistemler tarafından da çerçevelenmektedir (Whittaker; 2004, s. 21). Bu bağlamda da siber uzay tamamen insan yapımı, her zaman ekonomik ve siyasi güçler tarafından şekillendirilen bir yapı olarak karşımıza çıkmaktadır.

Ploug'un siber uzay için iki tanım yapmıştır. Bu tanımların ilkinde siberuzay'ı, birbirine bağlı bilgisayar ağları üzerinden sürdürülen ve erişilen sanal bir yer, oda veya alan olarak tanımlarken diğerinde birbirine bağlı bilgisayar ağları tarafından erişilebilen bir etkileşim yeri olarak ifade etmiştir (Ploug, 2009, s. 69-70). Bir başka tanıma göre ise; siber uzay bilgisayar ağları kullanarak veri depolamak, değiştirmek ve paylaşmak için bilgisayarların ve elektromanyetik spektrumun kullanımı ile tanımlanan fiziksel ve fiziksel olmayan bileşenlerin oluşturduğu ortam tanımlanmıştır (Schmitt, 2017, s.2011).

Buraya kadar yapılan tanımlardan da görüldüğü üzere siberuzay'ın teknik yönünün ağır bastığı, bilgisayar ve ağ donanımlarına dayanan tanımlar yapıldığı görülmektedir. Bu teknik tanımların eksikliğine vurgu yapan Asquith ve Morgan, bu tanımlara kullanıcı olarak "insan"ın dahil edilmesi gerekliliğini çünkü insanın siber uzayın örtülü olarak ayrılmaz ve aktif bir parçası olduğunu dile getirmektedirler (2020, s. 122). Ancak bilgisayar donanımları yanına kullanıcı olarak insan'ın eklenmesinin de yeterli olmadığını dile getiren Ottis ve Lorent bu tanımların içerisinde mutlaka "zaman" kavramının da yer alması gerektiğini belirtmektedir. Zaman bağımlılığının siber uzayın gözden kaçan bir yönü olduğunu belirten yazarlar yeni bir siber uzay tanımı yapmaktadır. Bu bağlamda siber uzay, zamana bağlı olarak birbirine bağlı bilgi sistemleri ve bu sistemlerle etkileşime giren insan kullanıcıları kümesidir (Ottis ve Lorent, 2010, s. 267). Tüm bu tanımlar çerçevesinde de görülebileceği gibi siber uzay tanımında da fikir birliği yoktur. Unutulmaması gereken nokta, siber uzayı sadece

teknolojinin bir bileşeni gibi değil, bireyin de hem kodlayıcı hem de nihai kullanıcı olarak sürece dahil olduğu bir uzam gibi tanımlanması gerekliliğidir.

Bilgi iletişim teknolojilerinin son otuz yılda hayatımıza girmesiyle birlikte bizler de siber uzayın birer parçası olmuş durumdayız. Bireyler açısından siber uzay, online alışveriş yapabildiğimiz, bilgiye erişim için kullandığımız, diğer insanlarla e-mail, sosyal medya veya çeşitli uygulamalar üzerinden iletişim kurabildiğimiz veya bilgilerimizi depolayabildiğimiz hatta sakladığımız bir ortam olarak karşımıza çıkmaktadır. Tabi ki bu örnekleri çeşitlendirmekte mümkündür. Bunların hepsini günümüzde internet aracılığı ile yapabilmekteyiz. İnternet günlük hayatımızın bir parçası haline gelmiş durumdadır. Cep telefonlarımız, televizyonlarımız, oyun konsollarımız hatta evimizde kullandığımız beyaz eşyalar bile artık internete bağlanabilmekte. Siber uzay karşımıza bir metafor olarak çıkarken, internet kurumların veya bireylerin iletişim kurmak amacıyla standart protokolleri kullanan küresel bir bilgisayar ağı olarak tanımlanmaktadır. Dolayısıyla internet, siber uzayın sadece bir yönü olarak karşımıza çıkmaktadır. World Wide Web veya İnternet'i siber uzay terimiyle aynı anlamda ele alınmaması gerekmektedir.

Fiziksel ve sanal alanların birbirine bağlanması, bireylerin lehine olan gelişmeler gibi görülmektedir. Siber uzayın mesafeleri ortadan kaldırdığı, iletişimin maliyetini düşürdüğü, daha fazla bireyin birbiriyle iletişim kurduğu (bir bakıma sınırların ortadan kalktığı) bireyler için daha çok zaman yarattığı (çevrimiçi alışveriş), hatta yeni iş alanları oluşturduğu yadsınmamaktadır. Ancak bu uzam bir takım sorun ve tehditleri de beraberinde getirmektedir. Bu tehditler siber uzayda karşımıza siber saldırılar olarak karşımıza çıkmaktadır. En çok görüldüğü alanlar kişisel bilgilerin çalınması, siber zorbalık, siber gözetim gibi alanlardır. Bir sonraki siber güvenlik başlığında ise siber uzayda siber güvenlik tanımlarına değinilecek ve kavramın çerçevesi oluşturulmaya çalışılacaktır.

1.1.2. Siber Güvenlik

Siber uzayın anarşik yapısı, kritik alt yapılar ve bilgi iletişim teknolojilerinin bazı özellikleri siber uzamda güvensizliğe neden olmaktadır (Akyeşilmen, 2018, s. 109). Siber güvenlik teriminin ilk defa 1990'lı yıllarda bilgisayar mühendisleri

tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanıldığı görülmektedir (Hansen ve Nissenbaum, 2009, s. 1155). Nissenbaum siber güvenliği kısaca “bilgisayar güvenliği” ve “güvenlikleştirme (securitization) birleşimi olarak tanımlamaktadır (2005, s. 65). Bir başka tanım ise bilgisayar ve iletişim teknolojilerine aynı zamanda bağlı olarak işleyen sistemlerin güvenliği olarak ifade etmektedir (Baybutt, 2004, s. 285). Moise ise, “kritik bilgi altyapısının yanı sıra küçük ve orta ölçekli işletmelerin bilgi ağları veya kişisel bilgisayarlar gibi kritik bilgi altyapıları olarak kabul edilen unsurların korunmasını içeren geniş bir terim” olarak tanımlamaktadır (2016, s. 160). Tanımlardan da anlaşılacağı üzere siber güvenlik aslında daha çok internet altyapısı, hizmet ve uygulama güvenliği olarak anılmaktadır (Deibert, 2018, s. 412). Bilgi iletişim teknolojilerinin (BİT) ekonomik rolü ve yararlarını en üst düzeye çıkarma ve fırsatlarından faydalanma amacı; siber netik saldırıların, (özellikle de kritik bilgi altyapısına karşı işlenen) ulusal güvenliğe yönelik bir tehdit oluşturabileceği gerçeği ile devletlerin karşı karşıya kalmasını beraberinde getirmiştir (Moise, 2016, s. 160). Bu bağlamda da devletlerin ulusal çıkarlara öncelik verip bu alanı güvenlikleştirmeye çalışarak bireysel kullanıcıları gözardı etmeye çalıştıkları görülmektedir.

Siber güvenlik aslında teknolojik, hukuki, sosyolojik, ekonomik ve politik alanların kesiştiği disiplinlerarası bir alan olarak karşımıza çıkmaktadır (Moise, 2016, s.160). Bu bağlamda siber güvenlik Tablo 1’de (Goldsmith, 2021) görüleceği üzere üç sütundan oluşmaktadır. Bunlar teknoloji, süreçler ve insanlardır.

Tablo 1. Siber Güvenlik

Teknoloji	Süreçler	İnsanlar
•Antivirüs •Güvenlik Duvarı İhlali •Saldırı Tespiti •Yazılım Güncellemeleri..vb.	•Yönetim Sistemleri •Politikalar-Prosedürler •Denetim •Yönetim Çerçevesi	•Eğitim-Farkındalık •Beceriler-Sertifikalar •Siber Hijyen

Yukarıdaki tablodanda görüleceği üzere ilk sütun teknoloji ayağından oluşmaktadır. Teknoloji sütunu daha çok altyapı bir başka deyişle teknikle ilgili kısımdan oluşmaktadır. Altyapı siber güvenliğin olmazsa olmaz unsurudur. Ancak diğer iki sütün olmadan tek başına teknoloji siber güvenliği sınırlı bir şekilde sağlayabilmektedir. İkinci sütun süreçlerden oluşmaktadır. Süreçler, daha çok kurum ve kuruluşlarla ilgilidir. Burada kurum ya da kuruluşların faaliyetlerinin, rollerinin ve belgelerinin veri güvenliği risklerini azaltmak için nasıl kullanıldığının tanımlanması önem arz etmektedir. Son sütun ise insanlardan oluşmaktadır. Bu grup en fazla riske sahip grup olarak kabul edilmektedir. Bunun nedeni ise bireylerin siber uzayın en zayıf halkasını oluşturmasıdır. Dolayısıyla etkili bir siber güvenlik isteniyorsa bireyler bu konuda eğitilerek farkındalık yaratılmalıdır. Siber güvenliği sadece ulusal güvenlik bazında ön plana almak güvenliğe yönelik bütüncül yaklaşımı sektöre ugratmaktadır. İnsanlar açısından siber güvenlik kavramını biraz daha açacak olursak son yıllarda siber uzayın bireyler açısından tehdit oluşturmaya başladığı söylenebilmektedir (Akyeşilmen, 2018, s. 107). Bilgisayarlarda, cep telefonlarında, uygulamalarda hatta çevrimiçi alışveriş yaparken dahi siber güvenlik terimiyle karşı karşıya kalmaktayız. Kullanılan sitelerdeki alt yapı sorunları, güvenlik açıkları ve kullanıcı bilgilerinin ihlal edilmesi de son günlerde medyada sıklıkla dile getirilmektedir. Bireysel ihlalin bu kadar çoğalması uluslararası toplum bazında ses getirmekte ve son yıllarda da siber güvenliğin insan merkezli yaklaşımının tanımlanmaya başlandığını görülmektedir. Bu yaklaşıma göre siber güvenlik, ağları bilgiye erişim, düşünce özgürlüğü ve örgütlenme özgürlüğü gibi modern insan haklarının uygulanması için gerekli temelin bir parçası olarak görülmektedir (Deibert, 2018, s. 412). 2013 yılında yayımlanan Avrupa Komisyonu (European Commission) “Cybersecurity Strategy of the European Union (CSEU)” belgesi de siber güvenlikte insan haklarını temel almıştır. Belgeye göre; “...Siber Güvenlik Stratejisi'nde belirlenen eylemlerin, AB'nin temel değerlerine saygı ve AB Temel Haklar Şartı'nda yer alan temel hak ve özgürlüklerin, özellikle de kişisel veriler ve özel hayatın gizliliği hakkının korunmasıyla yönlendirileceği belirtilmektedir” (CSEU, 2013, s.2).

Akyeşilmen'e göre ise, insan hakları ve siber güvenlik arasındaki ilişki iki yönlü olarak karşımıza çıkmaktadır; tüm kullanıcılar için güvenli bir siber alan yaratmak ve

siber alanda insan hakları için güvenli bir ortam yaratmak... (2016, s.34). Bu iki unsur aslında birbirleri içerisine geçmiş sarmal gibidir. Bu unsurlardan birini sağlamadan diğerinin sağlanması söz konusu değildir. İnsan hakları açısından güvenlik, devletlere yalnızca negatif yükümlülük getirmemektedir. Devletlerin siber güvenlik politikaları, insanların güçlendirilmesini ve refahını etkili bir şekilde merkeze koyarak yalnızca savunmacı değil, aynı zamanda kolaylaştırıcı bir rol oynamalıdır (Kovacks ve Hawtin, 2013, s. 7). Ancak bu sayede birey güvenli ve sürdürülebilir bilgi edinim, kullanım ihtiyacını karşılayacak, internetin faydalarından yararlanabilecek ve kendisi açısından riskleri en aza indirebilecektir.

Tüm bu hususlara siber güvenlik çerçevesinde bakacak olursak devletlerin artık vatandaşlarını siber uzayda tam olarak koruyamadığı görülmektedir. Her ne kadar devletler ulusal siber güvenlik politikaları geliştirseler de, siber uzayın sınırının olmayışı ve uluslararası iş birliğinin tam olarak yapılamaması siber güvenliğin tam olarak sağlanamamasına neden olmaktadır. Bir başka unsur ise bu noktada siber güvenliğe bütüncül bakış açısından yaklaşılması gerekliliğidir. Sadece teknik bir bakış açısıyla insan unsuru gözardı edilmekte bu da siber uzayda bireylerin özellikle özel hayatın gizliliği hakkı, ifade özgürlüğü hakkı ve kişisel verileri koruma hakkının ihlaline neden olmaktadır. Dolayısıyla siber güvenlikte bütüncül yaklaşım benimsenmeli devletlerin politikaları bireylerin özel güvenlik ihtiyaçlarına da cevap verebilecek şekilde belirlenmelidir.

1.1.3. Siber Saldırıları

Siber uzay, hiçbir savunmanın mükemmel olmayacağı dinamik bir ortam olarak karşımıza çıkmaktadır. Bilgi iletişim teknolojilerinin bu dinamik yapısı siber uzayı da günden güne değiştirmekte ve kapasitesini geliştirmektedir. İnternette eş zamanlı olarak siber saldırıların dahi takip edilebildiği bir dönemde yaşamaktayız. Bilgi iletişim teknolojilerindeki bu yenilikler bilgi güvenliğinin sağlanması açısından tam koruma sağlayamamakta ve siber güvenliğe karşı klasik ama etkisiz bir söylem olan, bilgisayarlara anti-virüs programlarının kurulması da bireyleri siber saldırılardan ve zararlı yazılımlardan koruyamamaktadır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı belgesinde siber saldırı, “Siber uzaydaki bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler” olarak tanımlanmıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020, s. 10). Bu kasıtlı olarak yapılan işlemlerin bir kısmı bireyler tarafından gerçekleştirilirken, bir kısmı da devletler veya suç örgütleri tarafından yapılabilmektedir (Akyeşilmen, 2018, s. 74). Siber saldırıların çok çeşitli amaçları bulunmaktadır. Saldırganlar sadece bilgiyi hedef alabileceği gibi bazen sadece kullanıcıyı da hedef alabilmektedir. Saldırının amacı, gizli bilgilerin elde edilmesi, bilgiye zarar verilerek değiştirilmesi bu bağlamda da bilginin bütünlüğünün bozulması ve kullanıcıların bilgiye erişiminin engellenmesi olarak karşımıza çıkmaktadır (Şenol, 2018, s. 194). Dolayısıyla siber saldırıların aslında bilgiye yönelik olduğunu söyleyebiliriz. Burada önemli olan hatta siber güvenliğin de önemli bir unsuru olarak karşımıza çıkan, bilgi bütünlüğünün, gizliliğinin ve erişilebilirliğinin korunmasıdır.

Siber saldırılar esnasında kullanılan yöntem ve teknikler çok çeşitli olarak karşımıza çıkmaktadır. Kullanılan yöntemlerin bazıları sistemleri yani bilgiyi temel alırken bazıları da kullanıcıları hedef olarak almaktadır. Tablo 2’de siber saldırılar esnasında kullanılan yöntemler yer almaktadır.

Tablo hazırlanırken kullanılan yöntem ve teknikler iki grupta incelenmiştir. Birinci grupta yer alan siber ortamdaki saldırı tekniklerini “araçlar” oluşturmaktadır. Virüs, solucanlar, Truva atı, ara bellek taşıma siber saldırı araçları olarak isimlendirilebilir. İkinci grubu ise insana odaklanan teknolojik araçlar oluşturmaktadır. Bu durumda teknik araçlar ve insana dayalı teknikler birlikte kullanılmaktadır (Lin, 2013, s. 477-478). Siber casusluk, siber suçlar, haktivizm ve hibrit savaş insan odaklı grup içerisinde yer almaktadır. İlk grupta sadece teknik araçlar söz konusuysen, insan odaklı grupta siber uzayın aktörleri de saldırı esnasında yer almaktadırlar. Siber saldırılar esnasında kullanılan teknik ve yöntemler Tablo 2’de (Meyers, Powers, Faissol, 2009, s. 15) gösterilmektedir.

Tablo 2:Siber Saldırılar Esnasında Kullanılan Teknik ve Yöntemler

Saldırı Türü	Alt Kategoriler	Açıklama
Virüs	Sistem Virüsleri, Dosya Virüsleri, Makrolar	Mevcut bir programa ekli olup, virüslü dosyalarla çoğalan kendi kendini kopyalayan program.
Truva Atı (Trojan)	Uzaktan erişim, veri yok etme	Kötü niyetli bir amaca hizmet eden iyi huylu görünen program
Solucan (Worms)	Botnet'lerle toplu posta gönderme, ağdan haberdar olma	Şebekeler veya e-posta yoluyla çoğaltan kendini çoğaltan program; Kullanıcı etkileşimi gerekli değil
Butter Overflows (Arabellek Taşımı)	Aşırı Veri Atanması	Arabellek taşmasıyla kontrolü ele geçiren veya başka bir işlemi çökerten süreç
Denial of Service/Distributed Denial of Service (DDoS/DoS Saldırısı)	Ara bellek aşımı, SYN, Teardrop, Smurf, Servislere Aşırı Yüklenme ve Message Flooding Saldırıları	Meşru kullanıcıların bir ana bilgisayara veya ağa erişmesini engelleyen saldırı
Network Attacks (Ağ Saldırıları)	Sızdırma, web / e-posta kimlik avı, oturum kaçırma, kablosuz WEP çatlaması, web uygulama saldırıları	Kullanıcılara veya ağlara karşı ağ protokollerini manipüle etmeye dayalı saldırı
Physical Attacks	Enerji silahı (HERF tabancası, EMP / T bombası, LERF), Van Eck Saldırıları	Bir ağın veya bilgisayarın fiziksel bileşenlerine zarar veren saldırılar
Password Attacks/ User Compromise (Şifre Saldırıları)	Tahmin etmek (kaba kuvvet, sözlük saldırıları), Uygulamayı istismar etmek	Bir şifre veya giriş kimlik bilgisi edinmeyi amaçlayan saldırılar
Information Gathering(Bilgi Toplama)	Paket koklama (packet sniffing) , ana makine haritalama, güvenlik tarama, port tarama, OS parmak izi	Saldırgan tarafından bilgi toplanır. Zarar vermeyen saldırılardır.
Siber Casusluk	Ekonomik/Endüstriyel Casusluk, Askeri Casusluk ve Siyasal Casusluk	Bilgisayar yoluyla kullanıcının haberi olmadan veri toplama
Siber Suçlar	Hedef Olarak Bilişim Sistemler (Yetkisiz Erişim, Servis Dışı Bırakma vb.), Bilişim Bağlantılı Suçlar (Kredi Kartı Dolandırıcılığı vb), Bilişim Bağlantılı Normal Suçlar (Uyuşturucu Trafığı, Kara Para Aklama, Terör Propagandası yapma vb)	Bilgisayar ağ sistemine yasadışı erişimdir. Herhangi bir zarara neden olmayacağı gibi, hasara ve bilgisayar korsanlığına kadar gidebilir.
Haktivizm	Siyasi Haktivizm	Siyasi olaylara tepkilerini siber ortamı kullanarak gösteren sanal protestolardır
Hibrit Çatışmalar	Virüs, askeri komuta kontrol ağları, DDoS, saturation (ping doygunluğu)	Silahlı güçlerin ve siber saldırıların birlikte kullanılması sonucu yıkıcı ve uzun vadeli hasar verilmesi

Yukarıdaki tablodan da görüleceği üzere her bir saldırı türü farklı alt kategorileri etkilemektedir. Siber uzayın en zayıf halkası olan bireye yönelik olarak gerçekleştirilen en sık karşımıza çıkan saldırı türü siber suçlardır. Bireylere yönelik siber suçlar işlenirken tabloda yer alan birçok yöntem birarada kullanılabilir. Kullanıcılar çoğunlukla siber saldırı sonrasında herhangi bir saldırıya uğradığının bilincinde değillerdir. Örneğin, Türkiye’de 2016 yılında Sağlık Bakanlığı hastanelerine yönelik siber saldırılar gerçekleşmiş ve saldırı esnasında bireylerin veri tabanındaki bilgileri çalınmış ve bazıları silinmiştir. Bu siber saldırı kamuoyunda paylaşıldığından dolayı birçok kullanıcı bu durumdan haberdar olmuştur aksi takdirde bireylerin verilerinin çalındığından haberi olması söz konusu olmamaktadır.

Bilgi iletişim teknolojilerinde yaşanan değişimden dolayı siber uzayda gerçekleştirilen saldırılar için hem hükümetler hem bireyler tarafından alınan önlemler yetersiz kalmaktadır. Siber alanın özelliklerinden biri olan “anındalık” bir başka deyişle beklenmeyen bir zamanda ortaya çıkma, bu alanın kontrol edilememesine neden olmaktadır. Teknolojik alanda yaşanan bu gelişmelerin bir yandan devletlerin güvenliğini etkilerken diğer yandan da bireyleri dolaylı ve/veya doğrudan olarak etkilediği görülmektedir. Siber saldırı araçlarının çeşitliliği, saldırıların nereden olduğunun bilinemeyişi, saldırıların maliyetsiz olması ve siber uzayda kullanılan tekniklere internet ortamından rahatça erişilmesi bireylerin ne tür bir tehditle karşı karşıya kaldığını her geçen gün daha da açık bir şekilde göstermektedir. Tüm bu nedenlerden dolayı kullanıcıyı bilinçlendirmek büyük önem arz etmektedir (Akyeşilmen, 2018, s. 81). Kullanıcıyı bilinçlendirmek her ne kadar kesin bir çözüm oluşturmaya da en azından siber saldırıların bir kısmının önlenmesinde etkili olacağı düşünülmektedir.

1.1.4. Siber Gözetim

Gözetim kavramının en ilkel toplumlarda bile var olduğu bir dizi etnografik çalışmada gösterilmiştir. Gözetim, davranışları, faaliyetleri ve diğer değişen bilgileri belirlemek için kişilerin veya konumların izlenmesini içermektedir (Shimonski, 2014, s.3). Lyon’un söylemiyle aslında gözetim insanlık tarihi kadar eskidir ve daima muğlaktır (Lyon, 2013, s. 113). Fransızca ‘surveiller’ fiilinden

türetilen “gözetim” fiili, denetlemek ve izlemek anlamının yanı sıra, belirli insan davranışlarının dikkate alındığı süreç anlamına gelmektedir (Watt, 2021, s.60). Lyon gözetimi, “etkileme, yönetme, koruma, yönlendirme gibi amaçlar doğrultusunda kişisel bilgilere dönük odaklı, sistemli ve düzenli ilgi” olarak tanımlamaktadır (Lyon, 2013, s.31). Gözetim, bilgi toplamak için bir kişiyi veya yeri yakından gözlemlemeyi veya dinlemeyi içerir. Fuchs’a göre ise gözetim rekabet mantığına dayanır. İnsanlarla ilgili verileri toplayarak, depolayarak, işleyerek, dağıtarak, değerlendirerek ve kullanarak grupların veya bireylerin belirli davranışlarını ortaya çıkarmaya veya önlemeye çalışır, böylece davranışlarını etkilemek için insanlara karşı potansiyel veya gerçek fiziksel, ideolojik veya yapısal şiddet yönlendirilebilir (2014, s.158). Tanımlardan da anlaşılacağı üzere gözetim tek taraflı bir faaliyet olarak karşımıza çıkmamaktadır. Gözetlenen birey de aslında bu sürecin doğal bir parçasıdır.

Gözetimde kullanılan teknikler açısından gözetimi; modern öncesi, modernite ve post modern dönem olarak ayırmak yerinde olacaktır. Bu ayrımı yapmamızın nedeni siber uzayda kullanılan gözetim tekniklerinin modern dönemde kullanılan tekniklerden ne şekilde farklı olduğunu belirtmek ve özel hayatın gizliliğine ne derece müdahil olduğunun kavranmasının sağlanması gerekliliğidir. Bu bağlamda yola çıkacak olursak, modern öncesi dönemde gerçekleştirilen gözetim daha çok doğrudandır ve belirli bir mekan içerisinde gerçekleştirilmektedir. Gözetim teknikleri ise yüz yüze ve dinleme olarak karşımıza çıkmaktadır. Dedikodu, gözetleme, gizlice dinleme, Engizisyon mahkemesi kayıtları, nüfus sayımları gibi örneklerle çoğaltılabilir. Ulus-devletin kurulması, modernitenin ve merkezileşmiş bürokratik devletin yükselişi modern gözetim çalışmalarını teşvik eden ve önemli unsurlardandır (Manokha, 2018, s. 226-227). Modernitenin vazgeçilmez bir parçası olan bürokrasi aslında gözetimin en önemli unsurlarından biridir çünkü kimliklendirme, sayım, kayıt tutma, sınıflandırma gözetim için veri oluşmasını sağlamaktadır (Lyon, 2013, s. 19-120). Moderniteyle birlikte aslında tüm bu veriler iktidarda tek elde toplanmaya başlamıştır. Bunun yanı sıra kapitalist üretim biçiminin de ortaya çıkmasıyla birlikte yoğun bir iş yeri gözetimi yine bu dönemin mihenk taşı olarak karşımıza çıkmaktadır. Demokrasinin de kapsayıcılığı ile gözetim toplum içerisinde daha yaygın hale gelmiş (demokrasi bağlamında tüm vatandaşlar sisteme dahil edilmeye çalışılmış) ve

sonrasında ise gündelik hayatımıza müdahil olmuştur. Kısacası modern devletin yükselişiyle birlikte gözetimin önemi artmış ve onu karakterize eden olağan idari aygıtın (iktidarın) bir parçası haline gelmiştir (Watt, 2021, s. 60). Tüm bu pratikler akademik çalışmalarla ve edebi eserlerle de desteklenmiştir.

George Orwell'ın "Bin Dokuz Yüz Seksen Dört" isimli edebi eserinde totaliterlik ve devlet idaresinde yapılan gözetimin sonuçlarının neler olabileceğini gözler önüne sermiştir. İktidarın merkezileşmesi, her köşe başının tele-kameralarla donatılması, hatta evlerin dahi dinlenmesi ve izlenmesi Orwell'ın eserinde devlet merkezli gözetimi özel hayatının anlamını kavramamızı sağlamıştır (Orwell,2008). Orwell'ın kitabında yer alan meşhur "Big Brother is Watching You" (Büyük Birader Seni İzliyor) metaforu, vatandaşların sürekli olarak izlenme veya kulak misafiri olma korkusu altında olduğunu ve insanların yaptığı her şeyin hükümet tarafından katı bir şekilde kontrol edildiğini dile getirerek, modern gözetim çalışmalarını derinden etkilemiştir. Yine Franz Kafka'nın "Dava" isimli eserinde "gözetim altında tutulan, her hareketi başkaları tarafından izlenen bir karakter olan" (Yılmaz, 2020, s.427) Joseph K.'nin kendisine herhangi bir neden söylenmeden tutuklanması ve sonrasında çıkmaza giren bürokratik süreçlerini anlatmaktadır. Bürokrasi, baskı ve toplumun kurumlarıyla çevrelenen karakter, iktidara direnmenin çaresizliği içerisinde bilmediği suçunu kabul etmiş ve erke teslimiyetin önemli bir sembolü olmuştur (Kafka, 2017).

18. yüzyıl İngiliz filozofu ve sosyal teorisyeni Jeremy Bentham tarafından kurgulanan Panoptik Hapishane modeli modern gözetim teorilerinin temeli olarak ele alınmaktadır. Panoptikon, hapishanelere, fabrikalara, çalışma evlerine ve akıl hastanelerine uygulanabilen bir sosyal disiplin mimari sistemi için yazılmış öneri olarak karşımıza çıkmaktadır. Panoptikon yapısının merkezinde bir gözetleme kulesi bulunan dairesel bir hücre dizisinden oluşmaktadır. Böylece gardiyanlar, mahkûmlar tarafından görülmeden her mahkûmu her an gözlemleyebiliyordu. Mahkûmlar, ne zaman gözlemlendiklerini bilmeden otoritenin sürekli varlığının farkında olduklarından dolayı disiplinlerini kendileri sağlayacak ve böylece çok az sayıda gardiyan çok sayıda mahkum üzerinde düzeni sağlayabilecekti. Lyon'a göre Panoptikon, "mimari yapının tek bir görünmez gözcünün aynı anda pek çok insanı gözetlemesini olanaklı kıldığı otomatik bir gözetleme biçimidir (2013, s. 57).

Michel Foucault, 1975 tarihli “Discipline and Punish” adlı kitabında Bentham’ın Panoptikon modelini tekrar ele alarak analiz etmiştir. Foucault, panoptikonu, disipliner toplumların yurttaşlarına boyun eğdirme eğilimini göstermenin bir yolu olarak kullanmıştır (McMullan, 2015). Aynı zamanda modernizmde temel bir mekansal figürü ve modern öznelliğin yaratılmasında, başka bir deyişle insanların (ve toplumun) modernite imgesinde yeniden inşasında kilit bir aracı temsil etmekteydi (Wood, 2003, s. 235). Foucault, panoptisizmi “...bireylerin belirli normlara göre modellenmesi ve dönüştürülmesi biçiminde bireylere uygulanan bir iktidar türü” olarak tanımlar (2019, s.70). Bir başka deyişle Panoptikon figürü tarafından temsil edilen toplumsal yörünge olan panoptisizm, kişinin sürekli inceleme altında olduğu inancı yoluyla kendi kendini denetleme dürtüsüdür, böylece modernist projenin hem itici gücü hem de kilit sembolü haline gelmektedir (Wood, 2003, s. 235).

Gözetimin modern devlette merkezi bir konumda olduğunu savunan yazarlardan biri de Anthony Giddens’tır. Giddens’a göre gözetim, enformasyonun kodlanması ve toplumsal denetime doğrudan atıfta bulunmaktadır (Lyon, 2013, s. 83). Bir başka deyişle gözetimi hem bilgilerin toplanması, hem de üstlerin astların faaliyetini denetlemesi olarak tanımlamaktadır. Gözetim, nüfus idaresi ile ilgili bilgilerin kodlanması (doğumlar, evlilikler, ölümler, demografik ve mali istatistikler, intihar, boşanma, suçluluk vb.) ve bunların her türden memurlar ve idareciler tarafından doğrudan denetlenmesidir” (Giddens, 1984, s. 183). Bu da bilgi toplama çerçevesinde modern ulus devlette gözetimin genişletilmesi anlamına gelmektedir. Giddens'a göre örgütlenme ve gözetleme ayrılmaz bir şekilde bağlantılıdır ve modern ulus devlette sistematik bir biçimde yer almaktadır. Bu nedenle Giddens, tüm modern toplumların bilgi toplumu olduğunu da savunmaktadır (Giddens, 1987, s.27). Böylece modern ulus devlet gözetim sayesinde bir yandan bilgiyi kayıt altına alırken, diğer yandan da sosyal denetime olanak sağlamaktadır.

Modern gözetim teorilerine baktığımızda daha çok toplumun disipline edilmesi, verilerin kayıt altına alınması ve bu bağlamda da gözetim yapıldığı gözlenmektedir. Orwell, Kafka gibi yazarlar modern gözetim teorilerinin edebi ve kurgusal yanını bizlere sunarken, Bentham, Foucault, Giddens’ta gözetimin teorik çerçevesini sağlamaktadır. Bu minvalde, modern gözetim teorileri bürokratik yapı, şirketler, ulus-

devlet gibi yapıların teknolojik büyüme biçimlerinin gelişmesi olarak düşünülürken, postmodern gözetim teknoloji tabanlı, bedeni nesneleştiren, gündelik evrensel gözetim biçimleriyle ilgilenir (Lyon, 2001, s.109) Modern ve postmodern ayrımı yapıldığında bunları birbirinden farklı kavramlar gibi düşünmemek gerekmektedir. Postmodern dönem, modern dönemi de kapsamaktadır ve birbirlerine eklemlenerek oluşan bir süreç olarak karşımıza çıkmaktadır. Tezin son bölümünde post modern gözetime ayrıntılı olarak yer verileceğinden dolayı burada değinilmemiştir.

1.1.5. Siber Şeffaflık

İletişim ve bilgi denetiminin internet ortamına taşınmasıyla birlikte, önceleri daha çok fiziksel alanda kamu kurumlarında anılan şeffaflık kavramı siber uzayın önemli bir bileşeni haline gelmiştir. Şeffaflık genellikle “daha fazla açıklık” olarak karşımıza çıkmaktadır. Şeffaflık kavramı, çeşitli kamu idarelerini, özel sektörü ve günümüzde bireyleri etkilediğinden dolayı tek bir tanımı yoktur. Ancak tüm tanımların ortak bir unsuru vardır. Bunlar; bilgiye erişme, onu anlama ve yorumlama ihtiyacıdır (Gandía vd., 2016, s. 28). Siber uzayda şeffaflığı birçok yazar kamu otoriteleri bağlamında ele almıştır. Ancak şeffaflık aynı zamanda uluslararası insan hakları hukukun da temelini oluşturmaktadır. Birleşmiş Milletler İnsan Hakları Komitesi'nin de dile getirdiği gibi, "şeffaflık ve hesap verebilirlik ilkelerinin gerçekleştirilmesi", "insan haklarının geliştirilmesi ve korunması için esastır" (Aktaran: Moorehead, 2017, s. 110). Dolayısıyla şeffaflık insan haklarının korunması ve geliştirilmesi için asli bir unsur olarak da karşımıza çıkmaktadır.

West'e göre, farklı şeffaflık kavramlarında ortak olan üç özellik vardır: i) “bilginin zamanında erişilebilir olması ihtiyacı; ii) açıklanan, kesin ve alakalı olarak anlaşılan bilgilerin kalitesi ve iii) bilgiye erişilebilirliktir” (Aktaran: Gandia vd.,2016, s.29). İnternet ortamından bireylerin beklentisi ise bu bağlamda eksiksiz bilgiye ve şeffaflığa ulaşılabilmesidir. Dijital teknolojilerdeki bu gelişmeler aynı zamanda günlük hayatımızı hatta yaşamımıza da şekillendirmektedir. Çünkü internet, aynı zamanda idarelerdeki yönetim süreçlerini modernize etmek, vatandaş katılımını sağlamak, şeffaflığı teşvik etmek ve bilgiye daha kolay erişim sağlamak için de kullanılmaktadır (Gandía vd. , 2016, s. 28). Dijital teknolojilere ve internete olan

bağımlılığının günden güne artması, yapay zekâ'nın ortaya çıkması, ekonomik, kültürel, politik ve sosyal faaliyetlerin de siber uzam üzerinden gerçekleştirilmesi, bu alandaki şeffaflık ihtiyacını da beraberinde getirmiştir. Örneğin, seçmenler internet aracılığıyla bir adayın konuşmalarına, makalelerine, muhalif adayların görüşlerine, hatta siyasi partilerin çevrimiçi mali tablolarına anında erişebilmektedir (Noveck, 1999, s. 484). Dolayısıyla siber uzayın şeffaf olması hem demokratik katılım yönünden, hem de bireylerin de sürece daha fazla müdahil olarak herşeyi gerçekte olduğu gibi görmelerini açısından önem arz etmektedir. Bu örnekler dijital teknolojilerin, şeffaflığın toplumsal ve bireysel davranış üzerindeki olumlu etkilerini göstermektedir.

Siber uzayın şeffaf olmaması, siber güvenlik ikilemine yol açabilmektedir. Bu nedenle, istihbarat toplama ve kitlesel gözetimle ilgili sürecin şeffaf olarak yürütülmemesi, siber uzayın kalıcı gelişimini sekteye uğratabilmektedir (Popa, 2015, s. 61). Hem devletler hem de özel şirketler bireyler hakkında veri toplarken, hükümetler siber gözetim yaparken şeffaf değillerdir. Dolayısıyla siber uzaydaki aktörler, kullanıcıların siber özgürlüklerine ve siber teknolojilerin tarafsızlığına zarar vermektedir (Popa, 2015, s. 60-61).

Siber uzayda şeffaflık bireyin kendini güvende hissetmesi, rahat hareket edebilmesi, bilgi edinmesi çerçevesinde önem arz etmektedir. Teknoloji ve bilgi çağında yaşarken verilerin gizli tutulmaya çalışılması bireylerin güvensizliğini arttırmakta, zaten anarşik olan siber uzayın içerisinde bireyin daha da savunmasız hale gelmesini sağlamaktadır. Siber uzayda bilgiyi erişilebilir kılmak ve birey açısından kullanılabilir hale gelmesi bireyin kendini geliştirmesinin bir ön koşulu olarak görülebilir. Devletin ve çok uluslu şirketlerin görevi ise, çevrimiçi içeriklerle ilgili yasal önlemleri alarak, bilgileri internet kullanıcıları için kolay anlaşılabilir, açık bir şekilde sunması ve siber şeffaflığın bu uzamda sağlanması olarak karşımıza çıkmaktadır.

1.1.6. Siber İstihbarat

Siber saldırıların çeşitliliği ve miktarındaki artış devletleri, şirketleri ve hatta bireyleri teknolojiye ayak uydurmak zorunda bıraktığı görülmektedir. Önceden kapınızı kilitleyerek aldığınız önlemler artık siber uzayda aktörlere güvenli bir ortam

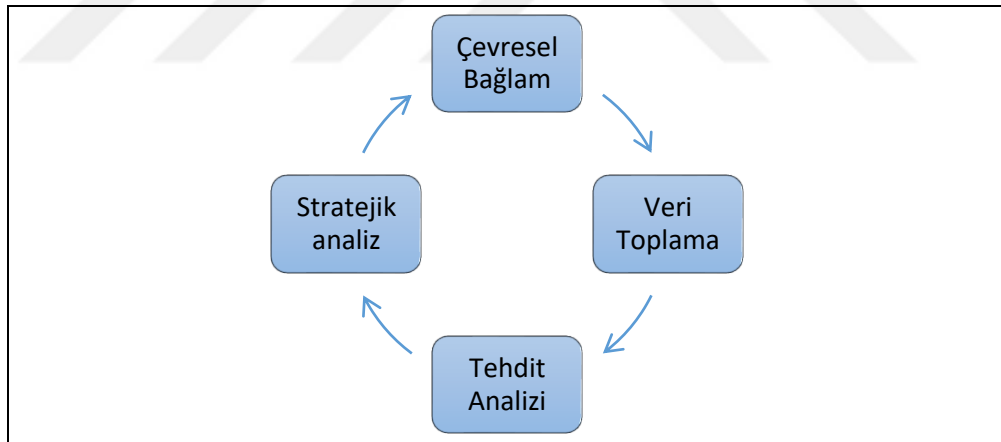
sağlayamamaktadır. İnternette yer alan muazzam bilgi yığını geleneksel istihbarat faaliyetlerini de etkilemiş ve siber istihbaratın, siber tehditlerden biri olarak karşımıza çıkmasına yol açmıştır. Siber istihbarat'ı tanımlamadan önce istihbarat kelimesinin tanımlanması gerekmektedir. Milli İstihbarat Teşkilatı (MİT)'na göre istihbarat; “devlet tarafından belirlenen ihtiyaçlara karşılık olarak çeşitli kaynaklardan derlenen haber, bilgi ve dökümanların işlenmesi sonucu elde edilen ürün” olarak tanımlanmaktadır (“MİT”, t.y.). Federal Bureau of Investigation (FBI) ise istihbaratı şu şekilde tanımlamaktadır; “politika yapıcılar için karar vermede, özellikle de ulusal güvenliğimize yönelik potansiyel tehditlerle ilgili kararlarda faydalı olacak şekilde analiz edilmiş ve rafine edilmiş bilgilerdir” (“FBI”, t.y.). Tanımlardan da anlaşılacağı üzere istihbaratın temeli bilgidir. Ancak bir bilginin istihbarat olabilmesi için elde edilen bilginin işlenmesi gerekmektedir. İhtiyaç duyulan bilgi de akılcı yöntemlerle toplanıp, analiz edildikten sonra değerlendirilir ve gerekli olduğu zamanda kullanıma sunulur bu da istihbaratın temel hedefi olarak karşımıza çıkmaktadır (Şenol, 2018, s. 199). İstihbarat çoğu zaman casuslukla aynı anlamda kullanılsa da, casusluk gibi gizli yöntemlerle bilgi elde etmekten ziyade, erişilebilen ve varolan bilgilerin çeşitli tekniklerle toplanması, toplanılan bilgilerin işlenmesi ve analiz edilmesine odaklanmaktadır (Ünver, 2018, s.1). İstihbaratta bilgilerin tanımlanmasından kullanılmasına kadar geçen süreç döngüden (cycle) oluşmaktadır.

Günümüzde istihbaratın dijitalleşmesi eski istihbarat tanımlarını ortadan kaldırmamakta ancak geleneksel istihbarat tanımını da genişletmektedir. Geleneksel istihbaratta insan temelli olarak yapılan bilginin işlenmesi, siber uzaya taşındığında daha mekanik bir yapıya dönüşmektedir (Mangır ve Küçükırlı, 2019, s. 299). Bir başka deyişle bilgi teknolojisi ile güçlendirilmiş ve ağ bağlantılı bir organizasyon haline gelmektedir (Castagna, 1997, s. 184). ABD Siber Güvenlik ve Altyapı Güvenliği Dairesi (CISA) ise siber istihbaratı; “Karar vermeyi geliştiren eylem planları sunmak için siber alandaki tehditleri, riskleri ve fırsatları tanımlayan, izleyen ve tahmin eden bilgileri edinme, işleme, analiz etme ve yayma” olarak ifade etmiştir (2019, s.3). Avrupa Polis Teşkilatı (EUROPOL) siber istihbarı, “çeşitli kamu, özel ve açık kaynaklardan siber suçlar hakkında bilgi toplama ve sonrasında bu bilgileri işleme ve analiz etme” şeklinde belirtmiştir (“EUROPOL”, t.y.). Tanımlardan yola çıkarak

siber istihbaratın iki yönü olduğunu söylemek mümkün olmaktadır. Bunlardan ilki herhangi bir saldırı olmadan önce olası saldırıyı önleme olarak karşımıza çıkarken ikincisi ise saldırı esnasında olası tehditi azaltmadır. Bu bağlamda siber istihbarat, başka ülkelerden bilgi toplama, bu bilgiler sayesinde dış aktörlerin amaçlarını anlama, şüpheli etkileşimleri bulma gibi konularda siyasi aktörleri güçlendirmektedir (Mangır ve Küçükırlı, 2019, s. 300). Siber istihbarat sadece devletleri kapsamamaktadır. Dolayısıyla siber istihbaratı gerçekleştiren siber uzay aktörleri şirketler, devletler ve bireyler olarak karşımıza çıkmaktadır (Akyeşilmen, 2018, s. 231). Ancak madur olan aktörlerin (bireylerin) aynı zamanda bu süreçte siber saldırı istihbaratını yaptığını da gözden kaçırmamız gerekmektedir.

Siber istihbaratta geleneksel istihbarata benzer bir döngüden oluşmaktadır. Bu döngü süreci Tablo 3’de (Townsend, Ludwick, McAllister, Mellinger ve Sereno, 2013, s.6) görüleceği üzere “siber ihtihbarat çerçevesi” olarak tanımlanmaktadır.

Tablo 3:Siber İstihbarat Çerçevesi



Döngünün birinci basamağını çevresel bağlam oluşturmaktadır. Bu süreçte kuruluş ve sektörleri hedef alan tehditler, riskler ve fırsatlar, kuruluşların iç/dış ağı ve operasyonları yer almaktadır. Siber istihbaratı gerçekleştirmek için hangi verilen gerekli olduğu bu basamakta belirlenmektedir. Veri Toplama aşamasında ise, analistlerin kurumsal gereksinimlerine yanıt vermek üzere analiz etmesi için çok sayıda dâhili ve harici kaynaktan veri ve bilgi toplanmaktadır. Tehdit analizi süreci ise

operasyonel ve taktiksel analiz üzerine kurulmaktadır. Siber güvenlik operasyonlarını/eylemlerini ve stratejik analizi bilgilendirmek için kuruluş ve sektöre yönelik belirli tehditlere ilişkin teknik ve teknik olmayan verilerin değerlendirilmesi süreci olarak karşımıza çıkmaktadır. Son aşama olan stratejik analiz sürecinde ise istihbarat değerlendirilmeleri teknik analizden gelen raporları bütünsel olarak ele alınmasıdır. Stratejik tehditler, tehdit aktörleri, riskler ve fırsatlarla ilgilidir ve karar vericiler için kuruluşun hayati çıkarlarına ilişkin bilgi sağlamaktadır (Townsend vd. , 2013, s. 5-18). Tüm bu döngü süreci siber istihbaratın tamamlanması açısından önem arz etmektedir ancak konumuz itibarıyla verilerin hangi kaynaklardan, ne şekilde elde edildiğini gösteren veri toplama aşaması özel hayatın gizliliğini ihlal etmesi yönünden muazzam bir öneme sahiptir.

Literatürde gruplandırmada farklılıklar bulunsada beş geleneksel istihbarat toplama disiplini kabul edilmektedir: Bunlar; İnsana Dayalı İstihbarat (HUMINT), Açık Kaynaklı İstihbaratı (OSINT), Sinyal İstihbaratı (SIGINT), Coğrafi Konum İstihbaratı (GEOINT) ve Ölçüm ve Akustik İstihbaratıdır (MASINT). HUMINT, "İnsanlar tarafından toplanan ve sağlanan bilgilerden türetilen bir istihbarat kategorisi" olarak tanımlanmakta (Stottlemyre, 2015, s.585) ve geleneksel istihbarat türünü oluşturmaktadır. Temel olarak HUMINT, sızma, görüşmeler yoluyla bilgi toplamaktan (kişilerden ve kurumlardan veri toplamaktan) ve stratejik değeri olan herhangi bir bilgiyi elde etmeye çalışmaktan oluşmaktadır (Sebeny, 2013, s. 662). Bu süreç, İnsan Temelli Sosyal Mühendislik Teknikleri, Mülakat, Sorgulama ve Sosyal Mühendislik Araçları aracılığıyla veri toplamayı içermektedir. GEOINT, "Dünya üzerindeki güvenlikle ilgili faaliyetlerin analizi ve görsel temsildir. Görüntü, görüntü zekâsı ve jeo-uzamsal bilginin entegrasyonu yoluyla üretilmektedir (Clark, 2020, s. 5). SIGINT ise terörle mücadele en çok kullanılan istihbarat toplama şekli olarak karşımıza çıkmaktadır. SIGINT, belirlenmiş hedefin elektronik sinyal ve iletişim bilgilerinin toplanması ve analiz edilmesi sonucunda elde edilen bilgidir (TechTarget, 2015). MASINT, radar gibi teknik donanımlar aracılığıyla verilerin toplanması ve analizidir (Stottlemyre, 2015, s.586). Bu yöntemlerden HUMINT ve OSINT insanlar tarafından toplanan bilgilerin analizi yoluyla elde edilmekte ve bu nedenle de tamamen bireylerin

veya grupların faaliyetlerine dayanan bilgileri içermektedir (Stottlemyre, 2015, s. 584).

OSINT özel hayatın gizliliğinin ihlali açısından diğer istihbarat yöntemlerinden ayrılmaktadır. Kamuya açık kaynaklardan bilgi arama ve bilgiyi elde etme ile kullanılan teknikleri ve araçları tanımlamak için kullanılan kavram olarak karşımıza çıkmaktadır (Evangelista vd., 2021, s. 346). OSINT istihbaratında, sosyal medya, hükümet raporları, coğrafi konumlar, kod siteleri, sosyal ağlar, uydu görüntüleri, akademik yayınlar, güvenlik açıkları veri tabanı gibi çok çeşitli açık kaynaklar ve ayrıca internet üzerinden erişilebilen bir dizi başka bilgide kullanılabilir. Günümüzde istihbaratın yüzde seksenden fazlası açık kaynaklı istihbarat bilgisinden oluşmaktadır (Miller, 2018, s. 703). Açık kaynaklı istihbaratta veriler kamuya açık olan her türlü bilgiden oluşmaktadır. Ancak her bilgi istihbarat kaynağı değildir. Elde edilen bilgiler ancak işlendikten sonra istihbarat haline gelmektedir.

Açık kaynaklı istihbarat gerçekten kamuya açık bilgilerden oluşuyorsa burada özel hayatın gizliliği hakkı ihlal edilerek veri toplanıyor mu? sorusu karşımıza çıkmaktadır. Genel kanıya göre bu sorunun cevabı evettir. Örneğin sosyal medyada kişisel bilgiler, konum bilgileri, fotoğraflar ve durum bilgileri kullanıcılar tarafından paylaşılmaktadır. Paylaşım sonrası bu kişisel bilgiler bir şirket tarafından kopyalanıp, analiz edildikten sonra veri haline getirilebilmektedir. Ancak bu bilgiler bireyin rızası dışında bir başka deyişle kullanıcıdan habersiz olarak toplanmaktadır. Kullanıcı aslında sadece yakın çevresiyle paylaştığını sandığı bilgilerini genellikle özel şirketlere adeta sunmaktadır. Her ne kadar kullanıcılar sosyal medya hesabı açarken gizlilik sözleşmesi imzalsın ve bu minvalde de verilerinin korunup, üçüncü taraflarla paylaşılmasına yasal çerçevede engel olunacağı kanısında olsa dahi günümüzde süreç bu şekilde işlememektedir. Bahsi geçen yasal çerçeve özel şirketler, devletler ve hatta bireyler tarafından ihlal edilebilmektedir. Tam bu noktada da bireyin özel hayatın gizliliği hakkı ihlal edilmektedir. Miller'ın da belirttiği gibi OSINT arenasında her zaman var olan bir siber güvenlik sorunu olan kimlik avı, bilgisayar korsanlığı, sahte veriler, dolandırıcılık ve benzerleri söz konusudur (2018, s. 710). Bireylerin tüm bu durumlardan dolayı teknolojiye güveninin günden güne azalmakta olduğunu görülmektedir. New York Times Magazine'de bu konuda makalesi olan Hess durumu

şu şekilde özetlemektedir: “Özel hayatın gizliliği hakkı çevrimiçi yaşamda önemli bir para birimi haline geldi- uygun hizmetler ve ucuz heyecanlar karşılığında alınıp satıldı. ... Giderek bir hak olarak değil, lüks bir mal olarak görülüyor. ... Veri madenciliği şirketleri bizim hakkımızda her şeyi biliyor ama biz onların bildikleri hakkında çok az şey biliyoruz.” (Aktaran: Miller, 2018, s. 716). Gerçekten de özel hayatın gizliliğinin nasıl ve ne derecede ihlal edildiği kullanıcılar tarafından tam olarak bilinmemektedir. Birey ancak kendisi hakkında olumsuz bir durum söz konusu olduğunda veya internette gezinirken verilerinin nasıl çalındığını ve kullanıldığını görebilmekte veya bu durumun farkında dahi olmadan yaşamını idame ettirmektedir.

Özel hayatın gizliliğini ihlal eden bir diğer yöntem ise siber istihbaratta yapay zekânın kullanılmasıdır. Günümüzde siber istihbarat toplayıp, analiz eden kişiler ve şirketler, yapay zekâ ile birlikte çalışmaktadır (“Teknolojik Düşünce Merkezi-STMthinktech”, t.y). Spesifik olarak da çoğu analiste, veri toplama, analiz etme ve rapor oluşturma konusunda yardımcı olmak için makine öğrenimini tekniklerinden biri olan yapay zekânın öğretildiği görülmektedir (Ettinger, 2019, s. 8). Siber istihbaratta yapay zekâ kullanımının özellikle özel hayatın gizliliğinin gözetim ve kişisel verilerin korunması hakkını ihlal ettiği görülmektedir. Wachter ve Mittelstadt, "algoritmik sorumlulukla ilgili endişeler, genellikle bu teknolojilerin bizim hakkımızda tahmin edemeyeceğimiz, anlayamayacağımız veya çürütemeyeceğimiz, özel hayatın gizliliğini istila eden ve doğrulanamayan çıkarımlar yapma biçimiyle ilgili" olduğunu dile getirmektedir (Aktaran: Warso, 2019, s. 20).

Özel hayatın gizliliğini siber uzayda en çok ihlal eden teknikler OSINT ve SIGINT olarak karşımıza çıkmaktadır. Yapay zeka destekli bu istihbarat toplama teknikleri özellikle kamuya açık bilgiler ve bireylerin iletişimi üzerinden verileri toplamakta, analiz etmekte ve bu bilgileri kategorize etmektedir. Ancak hem verilerin izinsiz toplanması hem de Wachter ve Mittelstadt'ın da dile getirdiği gibi hem verilerin elde edilme yönteminde hem de yapay zekanın bireyleri kategorize ederken de yaptığı çıkarımlarda birtakım sorunlar yer almaktadır. Bu konunun ayrıntılarına üçüncü bölümde detaylı olarak değinilecektir.

1.2. Bir İnsan Hakkı Olarak Özel Hayatın Gizliliği

Özel hayatın gizliliği hakkını anlayabilmemiz ve yorumlayabilmemiz için öncelikle özel hayat kavramının tanımına, önemine, hangi alanların özel hayat kapsamına girip hangilerinin bu bağlamda olmadığına tanımlanması ve hangi alanları etkileyip etkileşimde bulunduğuna bakmamız gerekir.

1.2.1. Özel Hayatın Tanımı

Özel hayatın tanımının uluslararası anlaşmalarda ve anayasalarda yer almadığını görmekteyiz. Özel hayatın birden çok alanı kapsaması, tanımı yapılırsa kapsamının daraltılabileceği endişesi kavram için tanım yapılmamasına neden olmaktadır. Solove tanım sorununa, yazarların özel hayatı kavramsallaştırmada geleneksel bir yöntem kullanmaları ve sonuç olarak, tanımlarının özel hayatın sadece bazı yönlerini vurgulaması veya çok geniş olması ve tanımlamaması olarak yaklaşmaktadır (Solove 2002, s.1094). Uluslararası belgeler özel hayat hakkında tanım sağlamadığından dolayı, özel hayatın içeriği, kapsamı günümüzde AIHM içtihatlarında tanımlanmaktadır.

Solove'un bahsettiği geleneksel yöntem özel hayatın ilk defa uluslararası sözleşmeler veya anayasalarda hak olarak tanımlandığı süreci içermektedir. Örneğin Amerika Birleşik Devletlerinde özel hayat öncelikle mülkiyet hakkı olarak karşımıza çıkmaktadır. Bu geleneksel özel hayat kavramı daha çok sözleşmelere, federal yasalara, mülkiyet haklarına ve iş geleneklerine bağlıdır (Singleton, 1999, s. 296). Ancak Avrupa Birliği'ne baktığımızda özel hayatın daha çok insan onuru çerçevesinde ele alındığını görülmektedir. Özellikle kitle iletişim araçlarının gelişmesi sayesinde özel hayatın tanımının değiştiğini ve kavramın genişlediğini söylemek mümkün olmaktadır. Günümüzde ise kavram tanımının daha çok insanların kendileri hakkındaki bilgileri kontrol etme hakkına sahip olması ve veri gizliliği ile ilintilendirildiği görülmektedir.

Özel hayat tanımlarına bakmadan önce özel hayatın unsurlarına bakmamız tanımları kavramıza yardımcı olacaktır. Banisar ve Davies özel hayatın dört yönünü şu şekilde tanımlamıştır (1999, s. 6-7):

1. Bilgi Gizliliği; Bireyin tıbbi kayıtları, kredi kartı bilgileri gibi kişisel verilerin toplanması ve işlenmesini içeren kuralları oluşturulan veri koruma,
2. Bedensel Gizlilik; Genetik testler, uyuşturucu testi gibi yasal prosedürlere karşı insanların fiziksel benliklerinin korunması;
3. İletişim Gizliliği; Posta, telefon, e-posta ve diğer iletişim biçimlerinin güvenliğini ve gizliliğinin korunması,
4. Bölgesel Gizlilik; Ev içi ve iş yeri veya kamusal alan gibi diğer ortamlara izinsiz girişe ilişkin sınırların belirlenmesiyle ilgili olan mahremiyet.

Tüm bu maddeler çerçevesinde özel hayatın gizliliğinin kişisel verilerin korunması, beden bütünlüğü, iletişimin gizliliği ve konut dokunulmazlığı çerçevesinde ele aldığı görülmektedir. Aslında neredeyse bütün uluslararası anlaşmalarda özel hayatın gizliliği hakkı beden bütünlüğü dışında bu çerçevede ele aldığı görülmektedir.

Solove özel hayatın gizliliğinin çok çeşitli tanımları olduğunu ifade etmiş ve bu tanımları altı kategoriye ayırmıştır. Solove’a göre özel hayatın gizliliği tanımları ya altı kategorinin içerisinde tanımlanmıştır ya da altı kategorinin kombinasyonundan oluşmaktadır. Bu kategoriler, yalnız bırakılma hakkı, kendine sınırlı erişim, gizlilik, kişisel bilgilerin kontrolü, kişilik ve yakınlık “samimiyet”tir (Solove, 2002, s. 1094).

Bunlardan ilki “*yalnız bırakılma hakkı*”dır. Modern anlamda özel hayatın gizliliğinin tanımlanması Warren ve Brandeis’in 1890 yılında “Harvard Law Review”de yayımlanan “Özel Hayatın Gizliliği” isimli makalesi olarak kabul edilmektedir. Yargıç Cooley’e atıf yaparak bu hakkı şu şekilde tanımlamışlardır (Warren ve Brandeis, 1890).

Son icatlar ve iş yöntemleri, kişinin korunması ve bireyin ‘yalnız bırakılma hakkı’nın güvence altına alınması için atılması gereken bir sonraki adıma dikkat çekiyor...İlerleyen uygarlığa eşlik eden yaşamın yoğunluğu ve karmaşıklığı, dünyadan biraz uzaklaşmayı gerekli kılmıştır.... böylece yalnızlık ve özel hayatın gizliliği birey için daha önemli hale geldi; ancak modern girişim ve icatlar, özel hayata yapılan saldırılar yoluyla onu... yalnızca bedensel yaralanmanın verebileceğinden çok daha büyük zihinsel acı ve sıkıntıya maruz bıraktı... (s. 195-196).

İlk defa tanımlanan özel hayatın gizliliği hakkının, insanların istemedikleri müdahalelerden uzak ve yalnız kalması yoluyla özel hayatını yaşama hakkına sahip olduğunu ifade etmektedir. Bu bakış açısı, bireyin dışarıdan müdahalelere uzak kalarak özel hayatlarını muhafaza edebilmelerinin önemini vurgulamaktadır.

Özel hayatın gizliliği kavramının bir başka tanımı, "*kendine sınırlı erişim*" kavramı olarak adlandırılmaktadır. Gavison (1980), "Mahremiyete olan ilgimizin, başkalarına erişilebilirliğimizle ilgili endişelerimizle ilgili olduğunu savunuyorum: başkaları tarafından ne ölçüde tanındığımız, başkalarının bize ne ölçüde fiziksel erişimi olduğu ve ne ölçüde başkalarının dikkatine maruz kaldığımızdır" (s.423) şeklinde tanımlamıştır.

Sissela Bok ise "fiziksel erişim, kişisel bilgiler veya dikkat nedeniyle başkaları tarafından istenmeyen erişime karşı korunma durumu" olarak tanımladığı görülmektedir (Aktaran: Wacks, 1987, s.126) Ernest Van Den Haag'e göre ise, "Bir kişinin (veya başka bir tüzel kişinin) kendisine ait bir alana münhasır erişimidir. Özel hayatın gizliliği hakkı, kişiye başkalarını (a) izlemekten, (b) kullanmaktan, (c) özel alanını işgal etmekten (istila etmekten veya başka şekillerde etkilemekten) men etme yetkisi verir" (Aktaran: Solove, 2008, s. 19). Tanımların ortak noktası bireyin kendi sınırlarını kontrol etmesi ve özel bilgilerini hangi ölçüde paylaşmak istediğiyle ilgili olarak karşımıza çıkmaktadır. Bu bakış açısında birey kendisi hakkındaki bilgileri belirleme yetki ve özerkliğine sahiptir.

Bazı yazarlar da özel hayatı *gizlilik* üzerinden tanımlamışlardır. Bu yazarlardan biri de Richard Posner'dir. Posner her ne kadar özel hayatın tanımını yapmaktan kaçınsa da özel hayatın bir yönünün de bilgilerin saklanması ve gizlenmesi olduğunu belirtmektedir. Posner'e göre özel hayat; herkesin kendisi hakkındaki bilgileri kamuya açık yerlerde kısıtlama hakkına sahip olduğu ve dışarıdakilerin bundan yararlanmaya teşvik edilmemesi gerektiğinden dolayı gizliliğin bir seçeneği olarak sunmaktadır" (Posner, 1983, s. 271). Sidney Jourard'ın da özel hayatın tanımını yaparken özellikle gizliliğe vurgu yaptığı görülmektedir: "Özel hayatın gizliliği, bir kişinin geçmiş ve şimdiki deneyimleri, eylemleri ve gelecekle ilgili niyetleri hakkındaki belirli bilgileri başkalarından saklama arzusunun bir sonucu" olarak tanımlamaktadır (Aktaran: Solove, 2008, s. 21-22). Bu görüşe göre, üçüncü taraflarla paylaşmak istenilmeyen

bilgilerin gizliliğinin önemi ve bu bilgilerin paylaşılmasının önlenmesi gerekliliğine vurgu yapmaktadır. Birey hangi noktada özel hayatının hangi yönünü paylaşacağına kendisi karar vermekte ve bu bilgi üzerinde kontrol sahibi olması gerektiğine inanmaktadır.

Yakınlık (Samimiyet) tanımlamasına göre ise, özel hayat kişisel ilişkilerin geliştirilmesi çerçevesinde tanımlanmaktadır (Solove, 2008, s. 34).

Buradaki yakınlık, samimiyetin anlamı ise kişinin yakın çevresi ve bireyin yakın çevresiyle kurduğu ilişki olarak karşımıza çıkmaktadır. Bu anlamda ki özel hayat, günümüz toplumunda da kabul edilen ideal bir özel hayat biçimi olarak görülmektedir. Rachels özel hayatın gizliliğini şu şekilde dile getirmektedir: “Çevremizdeki insanlarla olan ilişki türlerine göre davranışlarımızı düzenleriz. Bize kimlerin erişebileceğini kontrol edemezsek (örneğin bazen çeşitli insanları hayatımıza alıp bazen de hayatımızdan çıkarabiliriz), o zaman benimsememiz gereken davranış kalıplarını veya diğer insanlarla ilişki türlerini kontrol edemeyiz” (1975, s.331). Rachels özel hayatın gizliliğini burada bireyin kendisi hakkındaki bilgilerine erişimi sınırlayabilme ve kontrol edebilme bağlamında ele almıştır. Bir başka deyişle toplum içerisinde bireylerle nasıl ilişki kurduğumuz, bireyleri kendimize yakın gördüğümüzde özel hayatımızı ne ölçüde paylaştığımız ile ilgili olarak görülmektedir. Özel hayatın kişisel ilişkileri ve deneyimleri koruduğu anlayışını vurgulamaktadır.

Özel hayat “*kişisel bilgilerin kontrolü*” olarak da ele alınmaktadır. Bu kavramın özünde kişinin kendisiyle ilgili bilgiler üzerinde kontrol uygulama yeteneği ile ilgilidir. Fried özel hayatı şu şekilde tanımlamıştır: “özel hayatın gizliliği, kişinin kendi hakkındaki bilgisi üzerindeki kontrolüdür (Fried, 1968, s. 483). Bu aynı zamanda kişilerin bilgiye erişimini kontrol ettiği sosyal düzenin bir yönü olarak karşımıza çıkmaktadır (Fried, 1968, s. 493). Özel hayatı kişisel bilgilerin kontrolü olarak tanımlayan bir diğer yazar ve teorisyen ise Alan Westin’dir. Alan Westin’in bu teorisi bu alandaki ilk en kapsamlı teori olarak ele alınmaktadır. Westin’e göre özel hayat; “başkalarının kafasında bizim hakkımızda bilgi olmaması değildir; daha ziyade kendimizle ilgili bilgiler üzerinde sahip olduğumuz kontroldür” (1967, s. 7). Hiranandani’nin özel hayatı, kişinin kişisel yaşamıyla ilgili bilgilerin edinilmesi, kullanılması, saklanması, iletilmesi ve yayılması ile ilgili olduğu ve aynı zamanda

'bilginin kendi kaderini tayin etmesi' olarak da ifade ettiğini görülmektedir (Hiranandani, 2011, s. 1092). Yazarlara baktığımız zaman özel hayatın gizliliğini sadece bireyin kendisine ait kişisel veri ve bilgileri üzerindeki kontrolü olarak ele alındığı görülmektedir. Bireyler kişisel bilgilerinin ne şekilde kullanılacağını kararını verme yetkisine sahip olmalarının yanısıra bu bilgilerin korunmasının önemini de vurgulamaktadır. Günümüzde direktifler ve bölgesel sözleşmelerde de özel hayatın bu yön ve şekilde ele alındığı görülmektedir.

Kahn özel hayatı “*Personhood (Kişilik)*” kavramından yola çıkarak tanımlamıştır. Kahn’a göre özel hayat; bireyin kişiliğini tam olarak gerçekleştirmesi için gerekli koşulların tanınması ve bunlara saygı gösterilmesi gerektiği inancına dayanan bireyin haysiyetini dolaylı yoldan ifade etmektedir (2003, s. 378). Hakların bütününün bir parçası olan özel hayatın gizliliği, “kimlik ve haysiyet kavramları arasında hareket etmekte özgür olan bir çizgi boyunca bir noktadır”. Özel hayat, sadece mülkiyeti koruma aracı olarak ele alınmamalı aynı zamanda kimliği formüle etmek için bir araç olarak kavramsallaştırılmalıdır (Kahn, 2003, s. 410). Bir başka kişilik bağlamında tanımlayan ise BM Mahremiyet Hakkı Özel Raportörü Cannataci’dir. Cannataci’ye göre özel hayat kavramı, “bireyin 'kişisel faaliyetlerinden bağımsız olma arzusu, bir tür özerklik' anlamına gelir... 'temel bir haysiyet hakkının ve bireyin kişiliğinin özgür, engelsiz gelişiminin korunması ve geliştirilmesine ilişkin bir tartışma bağlamında çerçevelenmesini' tavsiye ettiği görülmektedir (Cannataci, 2016, s. 10-11). Bu bağlamda da özel hayatın esas olarak bireysel özerklik ve kendi kaderin tayin etme ile ilgili olduğunu belirtmiştir. Bu görüş, özel hayatın gizliliğini bireyin onuru, kimliği ve bağımsızlığı bağlamında el almaktadır. Özel hayat kavramı bireyin onurunun bir parçası olarak tanımlanmakta ve bireyin kendisini gerçekleştirebilmesi açısından da elzem olduğu vurgulanmaktadır.

Özel hayatın gizliliğinin çok uzun geçmişine rağmen, bu kavramın tanımı hala güncel bir sorun olarak karşımıza çıkmaktadır. Literatürde de tanım üzerinde tartışmaların sürdüğü görülmektedir. Özel hayat tanımı üzerinde oydaşma olmadığından dolayı günümüzde tanımlar özel hayatın unsurları çerçevesinde yapılmakta bu da kavram kargaşasına neden olmaktadır. Özel hayatın gizliliğinin kapsamının geniş olması, kesin sınırlarının olmayışı, kültürden kültüre değişiklik

göstermesi ortak bir tanım oluşturulamamasının nedenlerinden sayılabilmektedir. Bunun yanı sıra bireyin biricikliğinin (benzersiz olması) beraberinde getirdiği farklılık, bireyin özel hayata (hayatına) atfettiği önem ve değer de bu tanımların farklı şekillerde yapılmasına neden olduğu görülmektedir.

1.2.2. Özel Hayatın Önemi

Bireyin özel hayatının ve gizliliğinin korunmasının temelinde kişinin insana yaraşır bir şekilde hayatını devam ettirmesi yatmaktadır. Bireyler, insan ilişkilerini sürdürmek, kapasitelerini ve duyarlılıklarını geliştirmek, yaratmak, büyümek ve hatta hayatta kalmak için özel hayat ve sosyalleşme arasında bir denge içinde olmalıdır (Gavison, 1980, s. 440). Birey eğer bu dengeyi sağlayamazsa toplum içerisinde özerkliğini ve onurunu korumayacak dolayısıyla kendisini gerçekleştiremeyecektir. Bu yüzden özel hayat bireysel özerkliğin temelini oluşturmaktadır.

Literatüre baktığımızda özel hayatın önemine ilişkin birçok farklı bakış açısı görülmektedir. Moreham, özel hayatın önemini insan onuru bağlamında ele aldığı almaktadır. Moreham'a göre özel hayatın gizliliği, bireyin onuruyla ayrılmaz bir şekilde bağlantılıdır (Moreham, 2008, s. 234). Başkaları bireyin onurunu ancak iki şekilde ihlal edebilmektedir. Bunlardan ilki, bireyin onuruna saygı göstermemek, ikincisi ise, özel hayatın gizliliğine yapılacak müdahalenin bireyin iç huzuru üzerindeki etkisini göz ardı etmektir. Bireye karşı bu şekilde bir tutumun sergilenmesinin birey üzerindeki etkisi derin olmaktadır. Bu tutumla yaklaşan kişiler, bireye ve genel olarak da dünyaya, "bireyin duygularının ve seçimlerinin önemli olmadığını iletmektedirler" (Moreham, 2008, s.236). Bu da bireyin kendisi ile çelişerek iç huzurunun bozulmasına ve kendisini değersiz hissetmesine neden olmaktadır. Tüm bu nedenlerden dolayı da özel hayatın önemi temel olarak insan onuruna saygı ile bağlantılı olarak tanımlanmalıdır (Moreham, 2008, s.236-238).

Gavison, özel hayatın gizliliğinin önemini bireyin özerkliğini korumak ve kendisini geliştirmesi olarak ele almaktadır. Bu bağlamda Gavison şunları dile getirmektedir (1980):

Özel hayatın önemi iki tür endişeden kaynaklanmaktadır. İlk olarak, bazı alanlarda özel hayatın gizliliği bireyler için yeterli değildir. İkincisi, özel hayatın

gizliliğinin eşitsiz dağılımı, manipölasyona, aldatmaya, özerklik ve demokrasiye yönelik tehditlere yol açabilmektedir. Birincisi, bizim birey kavramımızla ve insanların tam olarak farkına varmaları için yapmalarına izin verilmesi gerektiğini düşündüğümüz eylem türleri ile ilgilidir... Örneğin özel hayatın gizliliğini akıl sağlığına, özerkliğe, büyümeye, yaratıcılığa ve anlamlı insan ilişkileri kurma ve yaratma kapasitesine bağlayan argümanlar bu kümeye aittir. İkincisi ise, istediğimiz toplum türüyle ilgilidir... Bunun için toplumun liberal ve çoğulcu olması gerekir... (s. 444).

Bu bağlamda Gavison'ın özel hayatın önemini hem birey hem de toplum temelinde ele almaktadır. Birey açısından bireyin bahsi geçen eylem türlerinin gerçekleştirmesinin elzem olduğuna değinirken, bireyin bu eylem türlerini gerçekleştirebileceği toplumun da tanımlamasını yaptığı görölmektedir.

Rachels ise özel hayatın önemini "korunması gereken bir değer" olarak ele almaktadır. Hakkımızdaki bilgilere kimin erişebileceğini kontrol etme, farklı şekillerde sosyal ilişkiler oluşturma ve sürdürme becerisi arasındaki yakın ilinti özel hayatın önemini vurgulamaktadır (s. 326). Ayrıca Rachels'in özel hayatın önemini göstermek amacıyla dört argüman öne sürdüğü görölmektedir (1975, s. 323-324). Bu argümanlar;

1-Rekabet durumlarında insanların çıkarlarını korumak için özel hayatın gizliliği bazen gereklidir.

2- Özel hayatın gizliliği gereklidir, çünkü birisi sırf başkalarının bilmesi utanç verici olacağı için hayatının veya davranışının bazı yönlerini gizli tutmak isteyebilir.

3- Tıbbi kayıtlar gizli tutulmalıdır, çünkü bunların ifşası iş kaybına, sigortaya elverişliliğe ve çeşitli sosyal yardımlardan yararlanamayışa neden olabilir.

4-Bir kredi soruşturmasında özel bilgilerin ifşa edilmesi, kredinin reddedilmesine neden olabilir. Bir kişinin kredi başvurusunun, başvuru sahibinin cinsel hayatı, siyasi görüşleri vb. kişisel detaylarından etkilenmesi haksızlıktır.

Rachels'in bu argümanları dile getirmesinin nedeni, birey toplumla ilişkisini yürütürken veya çok çeşitli nedenlerle sosyalleşirken bireyin tatmin edici bir hayata sahip olmasının bireyin özel hayatı açısından önemini vurgulamaktır. Daniel Solove

ise özel hayatın önemini “toplumsal fayda” çerçevesinde tanımlamaktadır. Solove’a göre; “Özel hayatın değeri, topluma katkılarına göre değerlendirilmelidir. Bireysel olarak özel hayatın korunması toplumun pahasına olmak zorunda değildir. İnsanların özel hayatını korumanın değeri, sosyal faydalarıyla gerekçelendirilmelidir. Tek başımıza değil, diğer insanlarla bir arada yaşıyoruz ve sosyal katılım yaşamın gerekli bir parçasıdır” (Solove, 2008, s. 91). Solove'un bu bakış açısı, özel hayat ve sosyal yaşamın birbirini dışlamadığı aksine özel bilgilerin ve bireyin kişisel sınırlarını korumasının daha geniş sosyal etkileri olduğu fikrinin altını çizmektedir.

Özel hayatın gizliği kavramının nasıl net bir tanımı yoksa, yukarıda verilen örneklerden de görüleceği üzere özel hayatın önemi de net bir şekilde açıklanamamakta, bireylerin özel hayatı ele alış şekline göre değişiklik gösterdiği görülmektedir. Literatüre baktığımızda yazarların özel hayatın önemini genellikle kendi tanımları çerçevesinde bir kavramlaştırmaya tabi tuttukları görülmektedir. Kimi yazarın özel hayatın gizliliğinin önemini bireysel olarak ele alırken, kimi yazarın da toplumsal bir süreç olarak ele aldığı görülmektedir. Yapılan açıklamaların çoğunda vurgu, özel hayatın içsel değerini açıklamaktan ziyade, kişinin özel hayatı ihlal edildiğinde ortaya çıkan sonuçları değerlendirmede yatmaktadır. Bu bağlamda özel hayatın değeri, özel hayatın ihlali durumunda diğer özgürlük ve hakların da tehdit altında olması anlamına gelmektedir. Bu yüzden özel hayatın değerini öncelikle bireysel anlamda ele almak gerekir. Çünkü toplumun temelini bireyler oluşturmaktadır. Bu yüzden bireyler özel hayatın önemini algılar ve buna saygı gösterip içselleştirirse, özel hayatın değeri ancak o zaman toplumun kültürel bir unsuru haline gelecektir.

1.2.3.Özel Hayatın Kapsamı

Günümüzde hala gelişmekte olan ve çok yönlü bir kavram olarak ele alınan özel hayat, teknolojik gelişme, kişisel özerklik ve toplumsal ilerlemenin çetrefilli ilişkisi içerisinde kendi bağlamını oluşturmaya devam etmektedir. Kamusal ve özel alanlar arasındaki ayrımı açıklığa kavuşturmak, özel hayatın kapsamını anlamak için temel bir çerçeve oluşturmaktadır.

1.2.3.1. Özel Alan

Toplum içinde bireyler, özerk olarak ve bir topluluğun üyesi olarak ikili bir rolle yaşamlarını idame ettirirler. Bireyin kendi sınırlarını belirlediği kişisel alanın yanısıra toplumla sosyalleşme veya vatandaş olarak hak ve ödevlerini yerine getirdiği kamusal hayatı bulunmaktadır. Bu yüzden kamusal ve özel alanı tanımlamak özel hayatın gizliliği hakkının çerçevesinin çizilmesi açısından önem arz etmektedir. Özel alan ve kamusal alan zıt kavramlar olarak tanımlansa da aslında birbirleri ile ilintili kavramlar olarak karşımıza çıkmaktadır. Örneğin kamusal alan tanımı yapılmadan özel alan tanımı yapılamayacağı gibi, özel alanın tanımı yapılmadan da kamusal alan tanımlanamamaktadır. Kamusal alan liberal düşünce temelinde devlete/topluma tekabül ederken, özel alan, ev alanı/ev dışı alanı sembolize etmektedir.

Özel alan en basit haliyle bireyin evi, yakın çevresi ve ailesi çerçevesinde tanımlanmaktadır. Özel alanda bireyin özel hayatı başkalarının müdahalesine kapalı olup, bunun korunmasını isteme hakkı bireye tanınmaktadır (Tezcan, 1991, s. 385). Zafer ise özel alanı, bir kişinin izni olmadan kimsenin giremeyeceği, başkasının bilinmesinin arzu etmediği ve toplumun iyi ya da kötü değerlendirmesiyle karşılaşmak istemediği tamamen özerk bir alan olarak tanımlamaktadır (Aktaran: Bozlak, 2013, s.31). Dolayısıyla bireyin özel alanı bireyin izni çerçevesinde, paylaşmak istedikleri veya gizlemek istedikleri çerçevesinde şekillenmektedir. Bir başka deyişle özel alan, bireyin rızası ile kamu ile paylaşmak istemediği konu, alan, durumlar bütünü olarak karşımıza çıkmaktadır. Bu alana hukuk düzeni haricinde müdahale edilememektedir. Bu durumun tek istisnası topluma mal olmuş kişiler olarak karşımıza çıkmaktadır. Topluma mal olmuş kişilerin örneğin siyasetçilerin özel alanları daha sınırlı yapıya sahiptir. Bu kişilerin olaylar ve durumlar karşısında görüntülerinin yayınlanması ve kaydının alınmasında rıza şartından feragat ettikleri kabul edilmektedir (Bozlak, 2013, s.32).

Özel ve kamusal alanların birbiriyle ilintili olduğunu savunan yazarlar olduğu gibi, bu alanların birbirlerinin alternatifi olduğunu dile getiren yazarlar da bulunmaktadır. Richard Sennett kamusal ve özel alan arasındaki bağlantıyı şu şekilde tanımlamaktadır:

Kamusal ve özel ifade tarzları birbiriyle çelişen şeyler olmaktan çok birbirlerinin alternatifiydiler. Kamusal alanda toplumsal düzen sorunu işaretlerin yaratılmasıyla çözülürken, özel alanda bakıp büyütme sorunu aşkın ilkelere bağlanarak, çözülme bile çözülmeye çalışıldı. Kamusal alanı yöneten itkiler istenç ve yapıntı, özel alanı yönetenler ise kısıtlamalar ve yapıntının silinip gitmesiydi. Kamusal alan insan yaratımıydı; özel alan ise insanlık durumuydu (Sennett, 2013, s.138).

Görüldüğü üzere Sennett kamusal ve özel alanı zıt kavramlar olarak değil, aksine içiçe geçmiş ve birbirini etkileyen alanlar olduğunu dile getirmektedir. Alexander Kluge ise kamusal ve özel alanın ilişkisini aşağıdaki şekilde tanımlamaktadır:

Kamusal alan değerler için bir tür pazardır. Söyleyebileceğim şeyler ve utandığım için asla söyleyemeyeceğim şeylerin pazarıdır. Böylece kamusal alan, bir kendine güvenin işaretidir. Eğer ne hissettiğimi yada tecrübelerimi başkalarına anlaşılabilir kılabilirdiğimi inanmıyorsam, işte bu mahremdir. Kendimi kamusal olarak ifade edemem mahremiyetin tiranlığıdır. Kamusal alan, ancak özel alanın özgür ve gelişmiş olması oranında özgürdür. Bu yüzden kamusal yaşamın ne manaya geldiğini anlamak için, örneğin aile politikası gibi mahremiyet alanındaki patikaları incelemek zorundasınız (Aktaran: Özbek, 2004, s.443).

Kamusal ve özel alanın birbirlerine zıt kavramlar olduğundan bahseden yazarlar da bulunmaktadır. Bu yazarlardan biri de Weintraub'dur. Weintraub, kamusal ve özel alanların eşleştirilmiş bir karşıtlıktaki bir unsur olarak anlamlı olduğunu vurgulamaktadır. Kamusal ve özel kavramlarının sıklıkla tartışıldığı iki ölçüt sunmaktadır. Bu iki ölçütü de "görülebilirlik" ve "kolektivite" olarak adlandırmaktadır. Bu iki ölçütün bazı durumlarda birbirlerine karışabileceği ancak özünde farkın yeterince açık olduğundan bahsetmektedir (Weintraub, 1997, s.4-5). Örneğin, oy vermek kolektivite bir eylem iken, kime oy verdiğiniz görülemediğinden dolayı özel alan içerisinde tanımlanmaktadır.

Kamusal alan ve özel alan kavramları tartışmalı konular olarak karşımıza çıkmaktadır. Özel alan kavramı, bireyin yabancıların dış müdahalesinden ve kamusal alandan ayrı, bireyin kendi sınırlarını çizdiği özel bir alanı ifade etmektedir. Bu kişisel alan, dışarıdan kimsenin müdahalesi olmadan bireyin toplum içerisinde kendini

gerçekleştirmesine olanak tanıyarak adeta birey için sığınak görevi görmektedir. Bireyin ilişkileri, duyguları, düşünceleri, evi kısaca başkasıyla veya toplumla paylaşmak istemediği faaliyetlerini kapsamaktadır. Bireyin özel alanı, bireyi toplumsal müdahale ve baskılardan koruyarak, özgür seçimler yapmasına ve biricikliğini gerçekleştirmesine olanak tanımaktadır.

Teknolojinin gelişmesiyle birlikte kamusal ve özel alan arasındaki sınırlar belirsizleşmeye başlamış ve günümüzde bu alanların yeniden tanımlanmaya çalışılmakta olduğu görülmektedir. Siber uzayın bireysel ve kolektif kullanımının bu alanların yeniden tanımlanması için uygun bir zemin oluşturduğu gözlemlenmektedir. Ayrıca alanlar arasında keskin sınırların olmaması, devletlerin, özel şirketlerin ve bireylerin siber uzayda özel hayatına yönelik müdahalelerin de artmasıyla birlikte bu tartışmanın güncel konular arasında yer aldığını ifade etmek gerekmektedir.

1.2.3.2. Kamusal Alan

Bugünkü anlamıyla Batı tarihinde 17. yüzyılın sonlarından itibaren olan “kamu/kamusal” kavramı, burjuva topluma ait bir terim olarak karşımıza çıkmaktadır (Özbek, 2004, s.43). 'Kamu' terimi, vatandaşlık, müşterek olan ancak özel olmayan, herkes tarafından erişilebilir ve gözlemlenebilir şeyler hakkındaki fikirleri ifade etmektedir (Papacharissi, 2002, s.10). Bir başka deyişle kamu, vatandaşların kamu işlerine katılımını gerektiren demokratik ideallerle yakından bağlantılıdır. Bu kamular aleniyet (publicity) aracılığıyla devleti topluma karşı sorumlu tutarak, toplumla devlet arasında aracı olmayı amaçlamaktadır (Fraser, 2004, s.106). Böylelikle kamu otoritesi olarak nitelendirilen devlet'in direk dahil olmadığı ancak dolaylı olarak var olduğu, vatandaşların ise herhangi bir kısıtlamaya tabii olmadan kamuya ilişkin meseleleri tartışabildiği bir alan olarak “kamusal alan” tarihsel süreç içerisinde karşımıza çıkmaktadır.

1962 yılında Almanca yayınlanan “Kamusal Alanın Yapısal Dönüşümü” (Strukturwandel der Öffentlichkeit) isimli kitabıyla, Habermas burjuva kamusal alanının tarihsel süreç içerisindeki oluşumunu ve yapısal dönüşümünü anlatarak modern anlamda kamusal alan fikrini kavramsallaştırmıştır. Burada kamusal alan kavramını modern olarak nitelendirmemizin sebebi, kamusal alan kavramının

köklerinin Antik Yunan'a kadar dayandırılmasıdır¹. XVIII. yüzyılda Avrupa'nın siyasi yapısındaki, kapitalist üretim tarzlarında meydana gelen değişiklikler, aydınlanma felsefesi ve feodalizmin çöküşüyle birlikte burjuvazi yükselmeye başlamıştır. Devlet ile toplum, kamu ile özel arasında hiçbir ayrım olmayan feodal sistemin aksine, yeni bir toplumsal düzen oluşmuştur. Bu yeni toplumsal düzende devlet ile özel alan arasında konumlandırılmaktadır. Kamusal alan olarak adlandırılan bu alan mülk sahibi, eğitilmiş bir okur kitlesinin üyelerinin öncelikle edebiyat ve siyasetle ilgili konularda rasyonel-eleştirel tartışmalara katıldığı bir "burjuva kamusal alanı" olarak karşımıza çıkmaktadır (Kazi, 2011, s.173-174). "Kamusal Alan" kavramıyla, toplumsal yaşam içinde, kamuoyuna benzer bir şeyin oluşturulabildiği ve politik sorunları çözmeye yönelik rasyonel-eleştirel etkileşim olan ahlaki-pratik söylemler ifade edilmektedir (Habermas, 2004, s. 95; Dahlberg, 2001). Fraser ise Habermas'ın kamusal alanını; vatandaşların ortak meseleler hakkında müzakere edebildikleri söylemsel etkileşim alanı olarak tanımlamaktadır. Bu alan politik katılımın müzakere ile sağlandığı, ilke olarak devlete karşı söylemlerin üretildiği ve dolaştığı bir alan olmakla birlikte, kavramsal olarak da devletten ayrı bir alanı simgelemektedir (Fraser, 2004, s. 104-105).

Habermas kamusal alanı, vatandaşların bir araya gelerek kısıtlanmamış bir şekilde genel yarara ilişkin meseleleri müzakere edebildikleri kamusal alandaki söylemlerin muhataplarına aktarılması ve onları etkilemesini mümkün kılacak araçlar olarak dergi, gazete, televizyon ve radyoyu iletişim araçları olarak tanımlamaktadır (Habermas, 2004, s.95). Yazılı medyanın, o günlerde burjuva kamusal alanının tanımlanmasında önemli bir rol oynadığı görülmektedir. Günümüzde ise bilgi iletişim teknolojilerinin gelişmesi sonucu internet, en çok kullanılan iletişim aracı olarak karşımıza çıkmaktadır (Kazi, 2011, s.174). Bu yeni teknoloji ve demokrasinin savunucuları, ana akım medya ve politikadan dışlanmış bireylere, muhalif fikir ve gruplara kapalı tutulan tartışma ortamına katılma imkanı sunmaktadır. Bu görüşe göre internet, kamunun erişimine açık bilgi ve fikirler kümesini zenginleştirerek, daha

¹ Daha detaylı bilgi için bakınız; Hylen, S. (2020). Public and Private Space and Action in the Early Roman Period. *New Testament Studies*, 66(4), 534-553.

bilgili ve donanımlı seçmen kitlesinin var olmasını sağlayarak, politik katılımdan dışlanan grup ve bireyleri de kapsayarak demokrasinin gelişmesinde katkıda bulunmaktadır (Kellner, 2004, s. 715). Bu sayede internet demokrasiyi yaymak ve daha önce dışlanmış olanları da kapsayan, güçlü bir katılım temelinde demokrasiyi yaymada yardımcı olmaktadır. İnternetin kapsayıcılığı, tek taraflı olmaması bir başka deyişle siber uzayın iki yönlü, merkezi olmayan iletişiminin herkesçe erişilebilir olması, bireylerin özgürce fikir beyan etmesi açısından rasyonel ve eleştirel söylemi kolaylaştırdığı görülmektedir. Bu bağlamda da internetin devlet iktidarını sorumlu tutabilecek kamusal alanı geliştirmeye temel sunduğu bazı yazarlar tarafından kabul edilmekte ve siber uzayın yeni bir kamusal olup olmadığı da tartışılmaktadır.

Siber uzayda dijital platformlar aracılığıyla yeni bir kamusal alan oluştuğunu savunan yazarlar öncelikle bunu çevrimiçi medyanın sağladığı bilgilere nispeten açık, kolay ve hızlı erişime dikkat çekmektedirler. Jones, siber uzayı insanlar tarafından yapıldığı için sosyal alan olarak tanımlamakta ve "yeni kamusal alan" olarak da bireyin kendini gerçekleştirme ve kişisel gelişime yönelik güçlü yanını vurgulamaktadır (1997, s. 22,25). Çevrimiçi kamusal alanın her vatandaşa kendini kamusal olarak ifade etme fırsatı sunması, katılımcıların hayatlarında başka türlü karşılaşamayacakları ve kendilerine yeni, etkileşimli ve potansiyel olarak daha erişilebilir yollarla sunulan bu bilgi zenginliğinin, kendilerinin ve başkalarının bakış açıları hakkında daha fazla düşünmeye, eleştirmeye, tartışmaya daha fazla özen göstermelerine yol açtığını ileri sürmektedirler (Schäfer, 2015, s.3-4, Mahlouly, 2013, s.10). Dolayısıyla bireyler burada fikirlerini beyan etme, özgür bir şekilde dile getirme ve sorgulama hakkına sahiptir. Bu da siber uzaydaki söylemlerin birkaç kişi tarafından tekelleştirilmesini sınırlarken, müzakereler bağlamında tartışmaya açık olan konuların çerçevesinde eleştirel tartışmaların yapılmasına olanak tanımaktadır.

İkinci olarak siber uzayın yeni bir kamusal alan oluşturduğunu ileri süren akademisyenler, çevrimiçi medyanın toplumda daha fazla insanın sesini duyurmasını sağladığını vurgulamışlardır. Geleneksel medya hükümetler tarafından kısıtlanabilmekte, baskılanabilmekte veya kontrol altına alınabilmektedir. Ancak çevrimiçi medyanın adem-i merkeziyetçi yapısı bu kontrol mekanizmalarını nispeten daha zor bir eylem olarak karşımıza çıkarmaktadır. Bu görüşe göre, yeni bilgisayar

teknolojileri ve internet daha fazla bilgiyle donanmış seçmen kitlesinin üretilmesine yardımcı olarak, siyasi tartışmalardan genel olarak dışlanmış grup ve bireylerin kamusal alana katılım olanaklarını genişleterek demokrasiye katkıda bulunmaktadır (Kellner, 2004, s.715; Schäfer, 2015, s. 4). Örneğin kurumlar karşısında bireyler, daha güçlü örgütler veya otoriter hükümetler karşısında muhalifler veya “Batı” karşısında çevre ülkelerden veya kalkınmakta olan ülkelerin vatandaşlarının da çevrimiçi kamusal alana herhangi bir müdahale olmadan fikirlerinin kolay bir şekilde yayınlanabildiği görülmektedir (Schäfer, 2015, s. 4). Dolayısıyla internet erişimine sahip olan her birey herhangi bir kısıtlamaya maruz kalmadan tartışmalara katılabilmektedir.

Son olarak ise akademisyenler çevrimiçi kamusal alanın yeni iletişim türlerinin tamamen üretilmesine yardımcı olabileceğini savunmuşlardır. Özellikle sosyal medya, yeni, merkezi olmayan, ağ bağlantılı bir iletişim ve içerik üretiminin kolaylaştırıcıları olarak görülmektedir (Benkler, 2006, s.213). Bu üretimin piyasa dışı kitle iletişim araçlarını kullanarak, piyasada olmayan ürünleri hedeflediği düşünüldüğünde, geleneksel medya iletişimini etkileyen ticari mantığın üstesinden gelmenin etkili bir yolu olarak tasvir edilmektedir (Schäfer, 2015, s.3-4). Bu minvalde yeni iletişim türlerinin sermayenin yukarıdan aşağıya küreselleşmesine karşı, dayanışma ağları geliştirerek ve bu mücadelelerini tüm evrende sürdürerek tabandan küreselleşmeyi örgütlemeye çalıştıkları söylenebilmektedir (Kellner, 2004, s.728). Dijital kamusal alanın tüm bu olumlu yönlerine baktığımızda aslında gelenekselleşen bir yapının internet aracılığıyla kırılmaya başlandığını söylenebilmektedir. İnternete erişimi olan her bireyin bu platformda sesini rahatça duyurabilmesi, kendisini ifade edebilmesi, kitle iletişim araçlarının kemikleşmiş ticari yapısına karşın âdem-i merkezîyetçi yeni platformların özellikle sosyal medyanın yaygınlaşması dijital kamusal alanın olumlu yönleri olarak karşımıza çıkmaktadır.

Ancak bazı yazarlar çevrimiçi kamusal alan’a daha eleştirel yaklaşmaktadırlar. Bu eleştirilerin ilki bireylerin dijital alana katılımı konusunda karşımıza çıkmaktadır. Bu yazarlar internetten hala belirli bir grubun faydalandığını (büyük oranda genç, beyaz ırktan, orta ya da üst sınıftan erkekler) (Kellner, 2004, s. 724), internet erişimi hiç olmayan bireylerin hatta ülkelerin olduğunu dolayısıyla herkesin çevrimiçi olarak

eşit bir şekilde bu alanlara katılmayacağını ileri sürmektedirler. Bu yüzden de sadece internete erişen gruplar bu alanda seslerini duyururken, internete erişimi olmayan bireylerin ise bu bağlamda dışlanacağını savunmuşlardır (Papacharissi, 2002, s.13; Khan, M., Gilani, I., & Nawaz, A., 2012, s.117).

Ocak 2022 yılı itibariyle küresel internet kullanıcıları, 4.95 milyara yükselmiş ve internetin nüfuz ettiği oran şu anda toplam dünya nüfusunun yüzde 62,5'ini oluşturmaktadır. Bu açıdan bakıldığında hala internet erişimi olmayan ciddi bir kitle karşımıza çıkmaktadır. Dolayısıyla siber uzayda bireylerin ve grupların tam katılımdan mahrum bırakan çevrimdışı sosyal eşitsizlikler, kapsayıcı bir çevrimiçi müzakerelerin geliştirilmesinin zorluğunu gözler önüne sermektedir.

İkinci olarak sorgulanan ise çevrimiçi kamusal alanda yapılan tartışmaların çeşitliliğidir. Çevrimiçi kamusal alanda benzer düşünen insanlar arasında dahi küçük topluluklara bölünme tehlikesi bulunmaktadır (Schäfer, 2015, s. 5; Mahloully, 2013, s.11). Bu görüşe göre; arama motoru algoritmaları bireylerin geçmişte girdikleri sayfaları kayıt altına alarak ve geçmiş aramaları da göz önünde bulundurarak bireylere uygun görülen bilgileri sağlamaktadır. Bu da bireylerin internette sadece benzer sayfalarda gezmelerine ve karşıt görüşlerle karşılaşmamasına yol açmaktadır. Mahloully bireyin davranışlarından yola çıkarak, internet ortamında farklı ideolojilerin karşı karşıya gelmesinin pek olası olmadığından bahsetmektedir. Buna göre kullanıcılar, kendi görüşlerini destekleyen web sitelerini ziyaret etme veya ağlarla bağlantı kurma eğilimindedir. Bu nedenle de, çeşitlendirilmiş ve dağınık olarak var olan kamusal alanlar, karşıt görüşlerle yüzleşmeye ve argümanlarını geliştirmeye yönlendirilmedikleri görülmektedir (Mahloully, 2013, s.12). Karşıt görüşlerle yüzleşmeyen bir kamusal alan modelinde ise bireyler kendi bakış açılarını yansıtmada daha az motive olabilmektedirler.

Son görüş ise bireylerin çevrimiçi ortamlarda anonim kimlik kullanmasıyla ilgilidir. Yüz yüze iletişimin olmadığı çevrimiçi kamusal alanda iletişim sanal olarak gerçekleştirilmekte ve bireylerin gerçek kimliklerini paylaşp paylaşmadığı dahi sorgulanmaktadır. Bu noktada karşımıza iki durum çıkmaktadır. Bunlardan ilki, bireylerin kimlik iddialarını ve öne sürülen bilgilerini doğrulamanın zorluğudur. İkincisi ise yüz yüze iletişimin olmadığı birçok çevrimiçi forum makul bir düzeyde

katılımcıyı saygı çerçevesinde dinleme veya farklı görüşlerle çalışma taahhüdünün elde edilememesidir (Khan vd, 2012, s.117). Bu da görüşler açısından çatışma yaratmaktan ziyade rasyonel bir iletişim şekli kurulamamasına neden olabilmektedir. Katılımcıların kimliklerini gizlemesi veya takma ad kullanması bireyleri her ne kadar iktidarın polislerine karşı koruyup özgürce fikirlerini beyan etmelerine olanak tanısa da çevrimiçi müzakerelerde karşılıklı saygı ve empatiyi gözden kaçırmalarına neden olabilmektedir.

Günümüzde siber uzayın yeni bir kamusal alan olup olmadığı hala tartışma konusudur. Bilgi sirkülasyonu hatta yığınları göz önüne alındığında genellikle karşımıza bloglar, çevrimiçi tartışma alanları ve çeşitli sohbet odaları çıkmaktadır. Çevrimiçi odalarda genellikle ticari ürün tanıtımı, eğlence ve kültür gibi konuların ön plana çıktığı görülmektedir. Bu alanların az bir kısmında siyaset konuşulduğu gözlemlenmektedir. Var olan siyasi tartışmalar da birden çok çevrim içi odalara bölündüğünden dolayı hem siyaseten internette bir bütünlük sağlanamamakta hem de bilgilerin doğruluğu ve kalitesinden şüphe edilmektedir. Bu bağlamda Habermas'ın kamusal alanının kapsayıcılığı, geniş bir vatandaş yelpazesinin müzakerelere katılımını internet her ne kadar sağlasa da siber uzayda sohbet odalarında bir otoritenin olmaması, bilgi yığınlarının parçalı bir şekilde sunulması kısacası bir bütün oluşturulamaması bu çevrimiçi kamusal alanda üretilen bilginin doğruluğunun sorgulanmasına hem de hükümetleri önemli bir ölçüde etkileyememesine neden olmaktadır.

Bunun yanı sıra Habermasçı kamusal alanda olduğu gibi çevrimiçi kamusal alan yerelleştirilememektedir. Bunun nedeni Habermas'ın kamusal alanının ideal olarak devletin vatandaşları ve kamu otoritelerinin arasında konumlandırmasıdır. Bir diğer nedeni ise Habermas kamusal alanı, başta ulusal basın olmak üzere geleneksel medyanın etrafına tanımlamıştır. Ancak günümüzde siber uzayın, internetin sınırları bulunmamakta ve yazılı medyada da büyük ölçüde işlevini yitirmektedir. İnternet, bu bağlamda kamusal alanın kurumsallaşma araçlarından yoksundur, çünkü siyasal iletişimin kamusallığını düzenleyebilecek ve koruyabilecek bir üst otorite bulunmamaktadır. Bu da internette kamusal alanın giderek küreselleşen, dijitalleşen ve parçalanmış bir ortamda rasyonel eleştirel söylemleri üretmesine engel olarak

görülmektedir. Ancak bireylerin bu ortamlarda bir araya gelerek ifadelerini özgürce savunmaları, tartışmaları bakımından da Habermasçı kamusal alandan ziyade, siber uzaya özgü küresel yeni bir kamusal alanın ortaya çıktığı görülmektedir.

1.2.4. Özel Hayatın Gizliliği Hakkının Boyutları

Özel hayatın gizliliği hakkının boyutlarını tanımlamak özel hayatın gizliliği hakkının unsurlarının ne şekilde ele alındığının gösterilmesi adına önem arz etmektedir. Bu hak sınırları çizilmiş tek bir bağlamdan oluşmamakta ve birden çok unsuru bünyesinde barındırmaktadır. Bu sınırlar olmadığından dolayı da kavram karmaşımıza çok boyutlu ve karmaşık olarak çıkmaktadır. Kaya özel hayatın gizliliği hakkının boyutlarını dört başlıkta ele almıştır (2022, s.10-14). Bunlar; kişisel veri ve kişilerin korunması, konuta müdahale etmeme, ad, şöhret (itibar) hakkı ve yazışmalarıdır.

1.2.4.1 Kişisel Veri ve Kişisel Verilerin Korunması

Günümüzde veri tabanlarında milyonlarca kişinin bilgileri tutulmaktadır. Tutulan her bilginin kritik öneme sahip olmasına da gerek olmadığı görülmektedir. Günlük harcama alışkanlıklarınız, hangi web sayfalarında sörf yaptığınız, alışveriş yaparken hangi marketten ne aldığınıza kadar gündelik rutin veriler ama bir o kadar da detaylı veriler depolanmaktadır. Depolanan veriler de çeşitli şekillerde kodlanarak bilgi haline getirilip sanal olarak dosyalanmaktadır. Bu bilgiler genellikle bireyin haberi olmadan özel şirketler, devletler veya bireyler tarafından elde edilmektedir. Bilgiler elde edilirken de bireyler hem paylaşmak istemediği kişisel verilerin üçüncü taraflarca ele geçirilmesine hem de siber gözetime maruz kalmaktadır. Siber uzayın en güçlü aktörü konumundaki büyük çok uluslu şirketler bu verilerin toplanmasını teşvik ederek bu verileri ticari olarak kullanmaktadır. Bilgileri bireyin haberi olmadan ele geçirilen birey ise çoğunlukla bu durumun farkında dahi değildir.

Kişisel verilerin korunması yeni bir kavram değildir. Ancak 1970li yıllar sonrasında bilgisayarın da kullanımının artmasıyla birlikte daha da önem kazanmıştır. 1990'lar sonrasında özellikle yapay zeka teknoloji sayesinde verilere erişim daha kolay ve ucuz hale gelmiştir. Böylece bilgi işleme, depolama gibi tekniklerin gelişmesi sayesinde devletler ve özel şirketler bilgi yığınlarını daha etkin kullanma

yeteneğini arttırırken, bireylerin özel hayatı da aynı oranda ihlal edilmeye başlanmıştır.

Kişisel veri kavramına baktığımızda özel hayatın gizliliği gibi tam olarak muğlak bir kavram olmadığını ve rehber ilkeler, protokollerde tanımının açıkça yapıldığını görmekteyiz. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) 23 Eylül 1980 tarihinde yayımlanan, 2013 yılında revize edilen “Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkeler” de "kişisel veriler, kimliği belirli veya belirlenebilir bir kişiyle (veri sahibi) ilgili herhangi bir bilgi anlamına gelir“ şeklinde tanımlandığı görülmektedir (OECD, 2013). Aynı tanımın “Avrupa Konseyi (Council of Europe) Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi”nde (108 no’lu Sözleşme olarak da anılmaktadır) sözleşmede kullanıldığı görülmektedir (2018, s. 7). Teknolojinin muazzam bir seviyede ilerlemesi, kişisel veri kavramının artık tanımlanmasının genişlemesiyle birlikte rehber ilkelerin ve sözleşmelerdeki kişisel veri kavramının daha da detaylandırıldığı söylemek yanlış olmayacaktır. Bu açıkça “95/46EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi ” (1998) ve “2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü” (GDPR) ,de karşımıza çıkmaktadır. Buna göre;

95/46EC Sayılı Direktif 2(a) Maddesi: “Kişisel veriler', kimliği belirli veya belirlenebilir bir gerçek kişiyle ('veri sahibi') ilgili herhangi bir bilgi anlamına gelir; Kimliği belirlenebilir kişi, özellikle bir kimlik numarasına veya fiziksel, fizyolojik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktöre atıfta bulunularak doğrudan veya dolaylı olarak kimliği belirlenebilen kişidir.

GDPR Madde 4(1): 'kişisel veriler', kimliği belirli veya belirlenebilir bir gerçek kişiyle ('veri sahibi') ilgili herhangi bir bilgi anlamına gelir; Kimliği belirlenebilir gerçek kişi, özellikle ad, kimlik numarası, konum verileri, çevrimiçi tanımlayıcı gibi bir tanımlayıcı veya fiziksel, fizyolojik, söz konusu gerçek kişinin genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğidir.

Bahsi geçen maddelere baktığımızda isim, konum bilgisi, çevrimiçi tanımlayıcı ve genetik kimlik bilgilerinin de kişisel bilgilere eklendiği görülmektedir. Özellikle siber uzayın da etkisiyle çevrimiçi tanımlamanın dahil edilmesi bu belgelerin dinamik yapısının bir göstergesi olarak karşımıza çıkmaktadır.

Yukarıda bahsi geçen rehber ilkeler ve sözleşmeler kişisel veriler bağlamında ele alınmıştır. Ancak literatüre ve uluslararası anlaşmalarda kişisel veri kavramının sıklıkla özel hayatın gizliliği bağlamında ele alındığı görülmektedir. Evrensel İnsan Hakları Beyannamesi, Sivil ve Siyasal Haklar Konvansiyonu, Avrupa İnsan Hakları Sözleşmesinde kişisel veriler direk olarak tanımlanmamış ancak Avrupa İnsan Hakları Mahkemesinde, kişisel verilerin ihlali ile ilgili davalar özel hayatın gizliliği ile ilgili maddeye atıf yapılarak tanımlanmıştır. Ancak Avrupa Birliği Temel Haklar Şartında (2009) 7. maddede Özel Hayatın Gizliliği hakkının yer aldığı, 8. maddede ise Kişisel Verilerin Korunması'nın ayrıca tanımlandığı görülmektedir.

Kişisel Verilerin Korunması özel hayatın gizliliği açısından büyük önem arz etmekle birlikte, bu iki kavramın birbirinin yerine kullanılmasının özel hayatın gizliliği açısından sorun yaratacağı düşünülmektedir. Bir yandan kişisel verilerin korunması özel hayatın gizliliği ile birebir ilişkiliyken, hatta özel hayatın gizliliği kavramının tanımı kişisel verilerin korunması üzerinden yapılırken, diğer yandan özel hayatın gizliliğini sadece kişisel verilerin korunması olarak ele alınması, özel hayat kavramını dar bir çerçeveden tanımlanmasına neden olmaktadır. Oysa ki özel hayatın gizliliği bireysel özerklik, mahremiyet, yalnız kalma vb. gibi birçok kavramı daha bünyesinde barındırmaktadır. Ancak bu durum özel hayatın gizliliğinin en çok ihlal edildiği alan olarak devletlerin güvenlik uygulaması bağlamında kişisel veri toplaması, gözetim yoluyla ve algoritmalar aracılığıyla kişisel bilgilerimizin toplanması ve işlenmesi gerçeğini değiştirmemektedir. Siber uzayda yer alan her bilgi kişisel bilgi olmayabilir ancak (Gür, 2018, s.857) bireylerden elde edilen verilerin bir çoğunun bireyi özel hayatı bağlamında etkilediği görülmektedir. Örneğin kredi kartı başvurusu sırasında veya çok basit bir örnek olarak uçağa binerken bile bireylerin güvenlik adı altında kişisel bilgileri araştırılmakta ve depolanmaktadır. Elde edilen bilgiler daha sonra devletler tarafından kodlanarak ayrıştırılabilmekte bu da bireylerin ırk, cinsiyet, etnik kimlik vb. konularda kodlanmasına neden olabilmektedir. Bu örnekleri DNA

analizinden, siyasi tercihlerinize, alışveriş alışkanlıklarınızdan, hangi gazeteleri okuduğunuza kadar uzun uzadıya uzatmak mümkündür. Dolayısıyla kişisel verilerin korunmasının özel hayatın gizliliğinin temel yapı taşlarından biri olduğunu belirtmek bu minvalde yanlış olmayacaktır.

1.2.4.2. Konuta Müdahale Etmeme

Özel hayatın gizliliğinin korunan bir diğer unsuru da konuta müdahale etmeme olarak karşımıza çıkmaktadır. Konut genel anlamıyla, bireyin yaşadığı yer anlamına gelmektedir. Bu tanım bağlamında konut dediğimizde aklımızda ev imgesi oluşmaktadır. Ancak AİHM konut kavramını daha geniş şekilde tanımlamıştır. AİHM'ne (European Court of Human Rights-ECHR) göre konut; Kişinin sahibi veya kiracısı olduğu mülkle sınırlı değildir. Bu, bir akrabaya ait bir evde, yıllık bazda veya uzun süreli oturmayı da kapsayabilir (Menteş vd Davası, 1997), İkincil bir konut veya tatil evleri (Demades vd Davası, 2003) de konut kapsamındadır, Karavanlar ve diğer sabit olmayan meskenleri de içerir (Chapman Davası, 2001), İş yerleri (Niemiets Davası, 1992) ,İşletmenin binası, ofisi ve şubeleri (Buckley Davası, 1996)de konut olarak tanımlanmaktadır (Roagna, 2012, s. 31).

AİHM kararlarında konut kavramının mesken bağlamında da tanımlandığını görülmektedir. Ancak literatürde konut kavramı özellikle özel hayat bağlamında çok farklı şekillerde tanımlanmaktadır. Solve'a göre, konut genellikle özel hayatın en önemli yeri olarak görülmektedir (Solove, 2008, s. 58). Camden konutu, bir kişinin kalesi (Aktaran: Akyürek, 2014, s. 81) olarak tanımlarken; Othman ise, barınak, güvenlik ve diğer birçok işlevin yanı sıra insanın özel hayatının somutlaşmış hali olarak dile getirmiştir (Othman, 2013, s. 1). Othman'ın konut tanımına benzer bir konut tanımı yapan Hayward ise konutu, barınak, sığınak, sosyal bağlılık, etkinlik, kişiselleştirme ve öz-kimlik, süreklilik ve özel hayat için bir yer olarak işlev gördüğünü öne sürmektedir (Aktaran: Othman, 2013, s. 1). Bu tanımlar bağlamında yazarların konut kavramını ifade ederken hep özel hayata atıf yaptığı görülmektedir. Konut dokunulmazlığı hakkı uluslararası sözleşmelerde de özel hayatın gizliliği hakkının kapsamında yer almaktadır. EİHB'nin 12. Maddesinde, AİHS'nin 8. Maddesinde, Medeni ve Siyasi Haklara İlişkin Sözleşmenin 17. Maddesinde konut

dokunulmazlığına özel hayat ile ilgili maddelerde açıkça tanımlanmıştır. İlgili sözleşmelerde konut bağlamında ele alınan bir diğer husus ise, konut dokunulmazlığının ihlalidir. Dolayısıyla konut dokunulmazlığının iki yönü bulunmaktadır. Bunlardan ilki bireyin özel hayatını yaşadığı yer olarak karşımıza çıkarken, ikincisi ise bireyin konutuna izinsiz olarak girmemeyi içermektedir. Kaboğlu bunu, bireyin konut içerisinde yaşamını istediği şekilde düzenleme ve dış müdahalelerden korunma hakkına sahip olduğunu belirterek dile getirmiştir (Kaboğlu, s.167). Olcay ise “Konut Dokunulmazlığı kişinin, özel yaşam alanı olan ve bu itibarla mekan kavramıyla bağlantılı olarak dışarıya karşı korunan konut’un içerisinde huzur ve güven duygusuyla yaşamını sürdürme hakkı olarak tanımlanmalıdır” şeklinde ifade ederek konut dokunulmazlığının iki yönünü de tanımlamıştır (Olcay, 2019, s. 225).

Bu minvalde konut dokunulmazlığı hakkı hem özel hayatın gizliliği bağlamında, hem de kişiye saygı olarak ele alınmaktadır. Konut dokunulmazlığı hakkının ele alındığı bir başka bağlam ise özel alan ve kamusal alan ayrımı olarak karşımıza çıkmaktadır. Hareven, “Kentleşme ve sanayileşmenin bir sonucu olarak iş yerinin evden uzaklaştırılmasının ardından, konut, ailenin özel inziva yeri olarak yeniden şekillendi ve ev, yeni bir kavram ve varoluş olarak ortaya çıktı” şeklinde görüşünü ifade etmektedir (Aktaran: Solove, 2008, s. 61). Bu ifade tarzında konut kişinin özel alanı bağlamında ele alınmakta ve mahkeme kararlarında da bu kapsamda değerlendirilmektedir. Fransız yargıtayında ele alınan bir davada bir kişinin izinsiz olarak fotoğrafının çekildiği bir davada “herkesin özel hayatına saygı hakkı, yaşam alanını oluşturan yerlerin sunumu da içerir” demektedir (Aktaran: Akyürek, 2014, s. 81). Bu da konut dokunulmazlığı kavramının kişinin özel alanı bağlamında ele alındığını, bireyin yaşam alanının kamusal alandan ayrıldığını ve bireyin öznelliğine katkıda bulunduğunu dile getirmektedir.

1.2.4.3. Ad Şöhret (İtibar) Hakkı

Özel hayat kapsamında korunan bir diğer unsur da kişinin ismi olarak karşımıza çıkmaktadır. Bir kişinin adı kimliğinin temel bileşenidir. Kişi doğumuyla birlikte aile içerisinde, sonrasında ise sosyalleşmenin bir süreci olarak toplum içerisinde bu isim ile anılmaktadır. İsim, kişinin yasal ilişkilere katılımı için gerekli bir koşul olarak

kabul edilir (Ulbashev, 2020, s.45). Götting'e göre isim, toplumdaki her insanın özdeşleşmesini sağlar ve bir dereceye kadar kişisel temsil amacına hizmet etmektedir (Aktaran: Ulbashev, 2020, s.44). O halde bireyin isminin hem bireysel hem de toplumsal yönü bulunmaktadır. Bunun yanısıra eğer bireyin bir ismi yoksa, dolayısıyla bireyin isim hakkı da olamamaktadır. Ulbashev bunu şu şekilde dile getirmektedir: "isim hakkı olmadan isimden kaynaklanan hak yoktur", başka bir deyişle, "isimden kaynaklanan haklar, bir isim hakkını takip eder"(2020, s. 44).

İsim hakkı uluslararası hukukta ilk defa BM Sivil ve Siyasal Haklar Konvansiyonunun 24. maddesinin 2. fıkrasında tanımlanmıştır (Salihpaşaoğlu, 2013, s. 238). İlgili maddeye göre "Her çocuk, doğumundan hemen sonra nüfus kütüğüne kaydedilecek ve bir isme sahip olacaktır". İsim hakkının yer aldığı bir diğer sözleşme ise BM Çocuk Haklarına Dair Sözleşmedir. Sözleşmenin 7. maddesinde "Çocuk doğumdan hemen sonra derhal nüfus kütüğüne kaydedilecek ve doğumdan itibaren bir isim hakkına, bir vatandaşlık kazanma... hakkına sahip olacaktır" denilmektedir. Avrupa İnsan Hakları Sözleşmesinde isim hakkı tanımlanmamıştır ancak bu eksiklik AİHM kararları ile kapatılmıştır. İsim hakkı AİHM kararlarında AİHS 8. Madde, özel hayatın gizliliği bağlamında ele alınmaktadır (Guillot Davası, 1993) Mahkeme, sadece isimlerin değil ön adların da "özel hayat" kapsamına girdiğine karar vermiştir (Garnaga Davası, 2013).

İsim hakkına konu olan geleneksel davalar genellikle isim değiştirme, evlendikten sonra soyadı alma gibi davalar olarak karşımıza çıkmaktadır. Ancak teknolojinin gelişmesiyle birlikte isim hakkı siber uzaya taşınmıştır. Buna göre bir kişinin isminin alan ismi (Domain Name) olarak izinsiz alınması ve başkalarına sunulması da isim hakkının ihlali olarak değerlendirilebilmektedir (Fırat, 2015, s.110). Ayrıca yine sosyal medya kullanılmasıyla birlikte görünür hale gelen takma ad "nickname" kişinin ismi kapsamında korunmaktadır. Özellikle sosyal medyada "fenomen" olarak tabir edilen ve ünlü olan kullanıcılar bulunmaktadır. Kişiler bu isimle ünlü olduklarından dolayı bu kişilerin isimlerinin başka sosyal medya kullanıcıları tarafından izinsiz kullanılması isim hakkının ihlali olarak kabul edilmektedir (Aka, 2017, s. 245). Sosyal medya da bir diğer isim ihlali (hatta en sık karşılaşılan) ihlal ise sahte hesaplar olarak karşımıza çıkmaktadır. Bireyin haberi

olmadan adına başka bir hesap açılması, yine isim hakkı bağlamında değerlendirilebilmektedir (Aka, 2017, s. 245). Örneklerden de görüleceği üzere teknolojik gelişmeler geleneksel hakları siber uzaya da entegre etmiş görünmektedir. Geleneksel bağlamda isim hakkında daha çok ad-soyad değiştirme gibi davalar görülürken, artık siber uzayda daha çok isim ihlalleri üzerinden davaların yürüyeceği düşünülmektedir.

Özel hayat bağlamında korunan bir diğer hukuki değer ise şöhrettir. Şöhret, bir kişinin başkaları tarafından algılanması veya toplumda sahip olduğu saygı ile bağlantılıdır (Leto ve Dean, 2011, s.2). Robert Post ise şöhret kavramının gizemli bir kavram olduğunu dile getirerek, kavramın üç şekilde anlaşılabileceğini savunur. Birincisi, mülk kapsamında şöhret olarak tanımlanmaktadır. Buna göre şöhret, sıkı çalışma, çaba ve erdemli yaşamın bir sonucu olarak bir birey tarafından inşa edilir ve sahiplenilir. İkinci olarak, onur olarak şöhret kavramını tanımlamaktadır. Bu kavram mülk temelli şöhretin tam tersi olup, bireyin sosyal rütbe veya konumuyla ilgili olmaktadır. Üçüncü olarak ve özel hayatın gizliliği bağlamında ele aldığımız, şeref olarak itibar anlayışıdır. Bu anlayışta insan onurunun veya kişiliğinin temel bir yönü olarak olarak tanımlanmaktadır (Post, 1986, s. 693-719). Post'un tanımlarından da görüleceği üzere şöhret tek bir kavramdır ancak bireyin yaşamının toplum içerisinde farklı yönlerini etkilemektedir.

EİHB'nin 12. Maddesinde, SSHK'nin de 17. Maddesinde korunan kişinin şöhreti özel hayatın gizliliği kapsamında ele alınırken, AİHS'de ifade özgürlüğü içerisinde tanımlanmıştır. AİHS'nin 10. Maddenin 2. fıkrasına göre;

Görev ve sorumluluklar da yükleyen bu özgürlüklerin kullanılması, yasayla öngörülen ve demokratik bir toplumda ulusal güvenliğin, toprak bütünlüğünün veya kamu güvenliğinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması, gizli bilgilerin yayılmasının önlenmesi veya yargı erkinin yetki ve tarafsızlığının güvence altına alınması için gerekli olan bazı formaliteler, koşullar, sınırlamalar veya yaptırımlara tabi tutulabilir...denilmektedir.

AIHM şöhret davalarına bakarken özel hayatın gizliliği bağlamında AIHS'nin 8. Maddesi çerçevesinde değerlendirmektedir.

İfade özgürlüğü ve kişinin şöhretinin çatıştığı durumlar bulunmaktadır. Özellikle basın alanında bu çatışmaların olduğu görülmektedir. İfade özgürlüğü kapsamında yapılan bazı haberler, kişi hakkında gerçeği yansıtmayan bilgilerin verilmesi ve bunun gerçekmiş gibi toplumla paylaşılması bireyin şöhreti ve itibarını toplum ve özel hayatı çerçevesinde zedeleyebilmekte, bunun doğrudan bir sonucu olarak da bireye zarar verebilmektedir. Bu yüzden ifade özgürlüğü ve bireyin şöhreti ayrı ayrı korunurken, bu iki kavramın dengede tutulmasına özen gösterilmesi gerekmektedir.

1.2.4.4. Yazışmalar

Kişinin yazışmaları haberleşme hürriyeti çerçevesinde ele alınmaktadır. Haberleşme hakkında AIHM geniş bir yorumu benimseyerek haberleşmeyi şu şekilde tanımlamıştır: “Özel veya profesyonel nitelikteki mektuplar” (Niemietz Davası, 1992), “gümrük memurları tarafından el konulan paketler”(X Davası, 1978), “aile üyeleri arasında (Margareta ve Roger Andersson Davası, 1992) veya başkalarıyla yapılan telefon görüşmeleri” (Ludi Davası, 1992), “elektronik mesajlar (e-mailler), internet kullanımı” (Copland Davası, 2007), “bilgisayar sunucularında saklanan veri” (Wieser ve Bicos Beteiligungen GmbH Davası, 2007), “hard diskler” (Petri Sallinen ve Diğerleri Davası, 2005) ve “disketler” (Iliya Stefanov Davası, 2008), “teleksler” (Campbell Christie Davası, 1994) ve “çağrı cihazları” (Taylor-Sabori Davası, 2003) ve “özel radyo yayınları” (X ve Y Davası, 1982). Tanımlardan da görüleceği üzere AIHM sadece mektup, telgraf, teleks ve telefon gibi geleneksel haberleşme tanımlara bağlı kalmayıp, teknolojik gelişmelere de ayak uydurarak, e-postalar veya İnternet kullanımı dahil olmak üzere elektronik iletişimi de kapsayacak şekilde yorumlamıştır.

Haberleşmeye saygı gösterilmesi hakkının amacı, bireyin haberleşmesinin kesintiye ve sansüre uğramadan başka kişilerle iletişim kurmasını sağlama olarak yorumlanmaktadır (Roagna, 2012, s. 32). Bu nedenle haberleşme hakkı, özel hayatın gizliliği bağlamında ele alınmaktadır. Uluslararası sözleşmelerde de özel hayatın gizliliği kapsamında ele alındığı görülmektedir. AIHM kararlarına bakıldığında AIHS'nin 8. maddesi kapsamında değerlendirme yapıldığı görülmektedir. Hakkın

içeriğine baktığımızda ise, hakkın ihlal edilmemesinin, bireyin korunmasının ön plana çıkarıldığı görülmektedir.

Haberleşmenin korunması AİHM kararlarına göre sadece özel yerlerde geçen iletişimi değil aynı zamanda iş yerlerinde geçen iletişimi de kapsamaktadır. Bunun yanı sıra haberleşmenin önemli bir ölçüde ihlal edildiği alan olarak karşımıza ceza evindeki tutuklular olarak karşımıza çıkmaktadır. Bu kişiler haberleşme özgürlüğünden mahrum oldukları için, kontrollü olarak yaptıkları haberleşmelerin de ihlal edilmesi bireyin kişisel alanına zarar verebilmektedir (Roagna, 2012, s. 39). Teknolojinin gelişmesinin haberleşmenin gizliliğine de yansıdığı görülmektedir. Son zamanlarda “gizli gözetim tedbirleri” adı altında açılan davalarda artış olduğu vurgulanmaktadır. AİHM’ne göre eğer bir kişi izlenecekse, bu mutlaka gerçeğin açığa çıkarılmasını sağlamalıdır. “İzleme faaliyetleri haberleşmeye saygı hakkına ciddi bir müdahale teşkil ettiğinden, bilhassa açık olan bir “kanuna” dayanmalıdır” (Huvig Davası, 1990). Örneklerden de görüldüğü üzere haberleşmenin gizliliği çok farklı alanlarda karşımıza çıkmaktadır. Bireyi doğrudan etkilediği için de özel hayat içerisinde değerlendirilmektedir. Haberleşmenin gizliliği hakkında haberin içeriğinden ziyade, dışarıdan bir müdahale olup olmadığına bakılmaktadır. Bu hak kapsamında bireyin özerk alanının korunması ve dışarıdan bu alana herhangi bir müdahale olmaksızın bireyin bu alanını kontrol etmesine olanak tanınması anlayışını yansıtmaktadır.

1.3. İnsan Haklarında Siber Uzayın Getirdiği Yeni Tartışmalar ve Özel Hayat

Dijital dünyanın gelişmesi ile birlikte insan haklarının unsurları ve bileşenleri de çeşitlenmiş ve bunun bir sonucu olarak da yeni haklar doktrinde tartışılmaya başlanmıştır. Bu yeni hakların daha çok bilgi iletişim teknolojilerinin gelişmesi sonucu ortaya çıktığı görülmektedir.

1.3.1. Kuşak Haklar (İletişim Hakları)

Günlük hayatımızın daha çok internete ve teknolojik gelişmelere dayandığı bir çağda yaşamaktayız. Bu da bireyler açısından daha önceleri hayal dahi edilemeyecek birtakım sorunları beraberinde getirmektedir. Sorunlar büyüdükçe ve siber uzayda

insan hakları ihlalleri de daha fazla dile geldikçe siber uzay ve teknolojik gelişimle ilgili yeni haklar tartışılmaya başlanmıştır. Dördüncü kuşak haklar konusunda henüz akademide bir oydaşma olmasa da siber teknolojinin insan hakları literatüründe yeni tartışmalara yol açtığı görülmektedir. Bu haklar internete erişim hakkı, anonimlik hakkı ve unutulma hakkı olarak karşımıza çıkmaktadır (Akyeşilmen, 2021, s.312).

İnsan haklarının tarihsel süreç içerisinde ihlaller sonucu ortaya çıktığı görülmektedir. Günümüzde varolan insan hakları açısından da iki önemli sorun bulunmaktadır. Bunlardan ilki, siber uzayda geleneksel haklara saygı gösterilmemesi durumudur. Bir diğeri ise, dijital ortamla birlikte yeni kavramların hayatımıza girmesi, geleneksel hakların da bu kavramları kapsamaması olarak karşımıza çıkmaktadır.

1.3.1.1 İnternete Erişim Hakkı

Siber uzay öncesinde hayal dahi edemeyeceğimiz internet günümüzde insan hakkı tartışmaları içerisinde yer almaktadır. İnsan hakları ebedi gerçekler ya da insan türünün varlıkları olmaktan çok, toplumdaki gelişmeleri yansıttıkları için evrimleşmektedir (De Hert ve Kloza, 2012, s. 3). Ayrıca, tüm haklar, insan haklarını ifade etme ve bilgi edinme haklarıyla desteklenmektedir. İnsan hakları hakkında iletişim kurma hakkı, kişilere bu hakları talep etme yetkisi vermekte, böylece hakları standart manipölasyon veya zorlama tehdidine karşı korumaktadır (Nickel, 2008, s. 988). Bu bağlamda internetin hayati bir altyapı parçası ve küresel iletişim, topluluk oluşumu ve yönetim için önemli bir yol haline geldiği görülmektedir (Joyce, 2015, s. 494). İnternet erişimini temel bir hak haline getirme fikri, son zamanlardaki dijital dönüşüm, kontrol, sansür ve pandemiye yönelik gelişmeler nedeniyle yerinde bir talep olarak karşımıza çıkmaktadır. Siber uzayda ortaya çıkan bazı sınırlar yasal ve hukuka aykırı olarak bilgi akışını kısıtlamaktadır. İnternet ve web kullanımının yaygınlaşmasıyla, hükümetlerin ve şirketlerin onu kontrol etmeye, sınırlamaya veya ele geçirmeye çalışma isteği de artmaktadır (Akyeşilmen, 2018, s.286). Yakın geçmişte olduğundan daha fazla, İnternet'in doğasını korumaya ve sürdürmeye yönelik artan bir ihtiyaç günümüzde vurgulanmaktadır (De Hert ve Kloza, 2012, s. 3). 16 Mayıs 2011'de, Birleşmiş Milletler Düşünce ve İfade Özgürlüğü Hakkının Geliştirilmesi ve Korunması Özel Raportörü Frank La Rue, BM'ye sunduğu raporda,

içeriğin engellenmesi ve filtrelenmesi, aracılık sorumluluğu, siber saldırılar, özel hayat ve veri koruma, internete erişim ve gerekli altyapı gibi konuları dikkate alarak ifade özgürlüğü ve internete erişim hakkı hakkında genel ilkeler geliştirmiştir. Söz konusu raporda La Rue, İnternet'in "bir dizi insan haklarını gerçekleştirmek için vazgeçilmez bir araç haline geldiğini" ilan etmiştir (2011, s. 22). İlgili raporda İnternet'e erişim insan hakkı olarak tanımlanmasa dahi La Rue'nun açık bir şekilde bunu ima etmesi devletlerin bu konu üzerinde düşünmesini sağlamıştır. Ayrıca internet'e evrensel erişimin sağlanmasının bir zorunluluk olması gerektiğini öne sürmesi ise internete erişimin bir insan hakkı olarak tanımlanmasının farkındalığını arttırmaktadır.

İnternet erişiminin bir dizi politik, ekonomik, sosyal ve kültürel boyutu bulunmaktadır. Bireyler tarafından pandemi döneminde özellikle eğitim, sağlık, toplum hizmetleri, ticaret ve eğlence dahil olmak üzere birçok amaç için internetin yaygın olarak kullanıldığı görülmüştür. Bu geniş kapsam açısından bakıldığında internet, insan haklarının gerçekleşmesini kolaylaştıran bir katalizör görevi de görmektedir (Tully, 2014, s. 185-194). İnternetin hem içeriği hem de bağlantısı bakımından belirli bir düzeyde korunması, ifade özgürlüğüne ilişkin olarak karşımıza çıkmaktadır. Ancak internet erişiminin başka haklarla da ilişkili olduğu gözden kaçırılmamalıdır. İnternet erişiminin, İnsan Hakları Evrensel Beyannamesin de yer alan” ifade ve bilgi edinme hakkı (İHEB Madde 19)”, “toplanma hakkı (İHEB Madde 21)” ve “kültür hakkı (İHEB Madde 27(1)) kapsamında korunan bir dizi iletişim faaliyetine olanak tanıdığını da vurgulamak gerekir. Avrupa İnsan Hakları Sözleşmesinde ise, özel hayatın gizliliği hakkı (Madde 8), düşünce, vicdan ve din özgürlüğü (Madde 9) ve toplanma ve örgütlenme özgürlüğü (Madde 11) haklarıyla ilintili olduğu görülmektedir. Bu hakların ifade özgürlüğü hakkıyla pek çok ortak noktası vardır, bir başka deyişle bunların gerçekleştirilme araçlarını korurlar, üçü de negatif haklardır ve çok benzer sınırlama kriterlerine tabi bulunmaktadırlar. Ek olarak, eğitim hakkı (AİHS Ek Protokolünün 2. Maddesi), kültürel yaşama katılma hakkı (MSHS 15. Madde) yeterli yaşam standardı (Ekonomik, Sosyal ve Kültürel Haklara İlişkin Uluslararası Uygunluk Madde 11 (De Hert ve Kloza, 2012, s. 23) hakları da bu bağlam içerisinde değerlendirilebilmektedir. Dolayısıyla ifade özgürlüğünün diğer haklardan yararlanmanın temelini oluşturduğunu söylemek yanlış olmayacaktır. Bu

bağlamda özellikle kamusal alan boyutunda erişim ve katılım sorunlarının önemi açısından ifade özgürlüğünün yeniden değerlendirilmesini gerektirmektedir.

İfade özgürlüğü hakkı, genel olarak, evrensel olarak tanınan ve diğer hakların savunulması ve korunması için temel oluşturan merkezi ve kolaylaştırıcı bir insan hakkı olarak düşünülmektedir (Joyce, 2015, s. 498). İnternet erişimi şu anda, özellikle ifade özgürlüğü hakkı olmak üzere önceden var olan birçok haktan yararlanmanın bir yönü olarak ele alınmaktadır. Mathiesen, İnternete erişimi “birincil” bir hak olmamakla birlikte, birincil iletişim hakkından türetilebileceğini dile getirmektedir. Ayrıca, iletişim hakkı insanlara haklarını kullanma ve sorumluluklarını yerine getirme yetkisi veren bir temel hak olduğundan, devletlerin insanların internet teknolojisine erişimini sağlama yükümlülüğü bulunmaktadır. İnsan hakları ihlalleri vatandaşlar adına gerçekleştirilebileceğinden, vatandaşlar ahlaki yükümlülüklerinin (ve hükümetlerinin) yerine getirilmesini sağlamak için gerekli bilgilere sahip olmalıdır (Mathiesen, 2012, s. 15-20).

Reglitz, ücretsiz internet erişiminin evrensel bir ahlaki ve insan hakkı olarak görülmesi gerektiğini, dijital çağda diğer yerleşik insan haklarının korunması ve geliştirilmesi için gerekli olduğundan bahsetmektedir. İnternet erişimi kendine özgü bir haktır, çünkü başka herhangi bir hakka indirgenemez veya başka bir hak tarafından kapsanamaz. İnternet erişimi, bu haklara dijital olarak erişime izin vermesine rağmen, konuşma özgürlüğü, toplanma veya ücretsiz bilgi gibi diğer hakların basit bir versiyonu değildir. Bu haklar, sanal bir küresel bağlamda İnternet erişimi olmadan tam olarak gerçekleştirilemez. Aynı şekilde, İnternet erişimi, ifade özgürlüğü ve toplanma gibi temel insan haklarını gerçekleştirmenin benzersiz ve ikame edilemez bir yolu olarak ele alınmalıdır (Reglitz, 2020, s. 5-6)

Literatürde bu konu üzerine tartışmalar devam etmektedir. İnternet erişiminin insan hakkı olduğunu savunan yazarların yanı sıra bunun bir hak olmadığını dile getiren yazarlar da bulunmaktadır. Amerika’da, internetin babası olarak tanımlanan Cerf, internete erişimin insan hakkı olmadığı, interneti iyileştirmenin, insanlık durumunu iyileştirmek için önemli olsa da sadece bir araç olduğunu dile getirmektedir (Cerf, 2012). Bu görüşünü şu sözleriyle desteklemektedir: "Herhangi bir teknolojiyi (insan haklarının) bu yüce kategorisine yerleştirmek bir hatadır, çünkü zamanla yanlış

şeylere değer vermeye başlayacağız." (2012). Cerf bu görüşünde internet erişimini sadece bir araç olabileceğini ancak bunun bir hak olarak tanımlanamayacağını vurgulamaktadır.

Cerf'in bu köşe yazısıyla başlayan tartışmaya Skepys'de destek vermiştir. Skepys'e göre; değer verdiğimiz şeyleri insan hakları olarak adlandırmayı bırakmalı ve bunun yerine onları siyasi bir topluluğa üyelik için araçsal olarak gerekli olan daha temel insan haklarına yönelik acil tehditler olarak görmeliyiz (Skepys, 2012, s.25). Bu görüşlere bir diğer katkı sağlayan kişi ise Michael O'Rielly'dir. Rielly'de internet erişimini gereklilik kapsamında ele almaktadır. Rielly'e göre, insanlar teknoloji olmadan da yaşayabilecek ve çalışabileceklerdir. Bu yüzden internete erişimin bir insan hakkı veya gereklilik olarak ele alınmasının mantıksız olduğunu dile getirmektedir. "Bunun yerine, 'ihtiyaç' terimi, yiyecek, barınak ve su gibi insanların onsuz yaşayamayacağı şeyler için ayrılmalıdır"(Aktaran: Rajpari, 2020). İnternet erişimini bir insan hakkı haline getirmemenin temel argümanlarından biri, hayatta kalmak için gerekli olmadığı veya insan olmanın doğasında olmadığı fikri olarak karşımıza çıkmaktadır. Ayrıca internet erişimi gibi değer verdiğimiz her bir yapıyı insan hakları bağlamında ele alınmaması gerekliliği de ifade edilmektedir. Pandemi dönemine bakıldığında bir çok kurum evden çalışma sistemine geçmiştir. Ayrıca yine aynı dönemde interneti olmayan öğrencilerin eğitim haklarından yararlanamadığı görülmüştür. Yaşanılan COVID 19 pandemisi internetin önemini bir kez daha göstermektedir. Pandemi sonrası toplumda ise, insanların temel ihtiyaçlara erişmek için bir araç olarak internete bağımlı oldukları ve iş, eğitim, eşitlik, sağlık, iletişim ve benzeri alanlarda internet erişiminin insan haklarını koruma adına çok önemli işlevi olduğu düşünülmektedir.

İnternet kesintilerinin yıldan yıla arttığı bir dünyada, hükümetler ve vatandaşlar arasındaki ilişkiyi geliştirmek ve tüm insan haklarını korumak için doğru adımların atılması önem arz etmektedir. BM İnsan Hakları Konseyi, ifade özgürlüğü hakkı ve barışçıl toplanma hakkı gibi çevrimdışı hakların çevrimiçi olarak da uygulanması gerektiğini giderek daha fazla kabul etmesine rağmen, insan hakları hukuku çevrimiçi haklara karşı açık korumalar içermemektedir. İnternet erişiminin ifade özgürlüğü, sağlıklı bir demokrasi ve diğer birçok haktan yararlanmak için temel yapı taşı olduğu

artık bilinen bir gerçektir. Bu minvalde internete erişim bir hak olarak tanınmalıdır. Bu hak negatif bir hak olmamalı, bunun yanısıra internete erişimi olmayan bireylere internet erişimini de içeren pozitif yükümlülükler getiren bir hak olarak tanımlanmalıdır (Akyeşilmen, 2018, s.285). İnternete erişim ancak bu şekilde bir hak olarak tanımlandığında, bireylerin bilgiye ulaşacağı, bilgiyi yayabileceği, kullanabileceği ve kapsayıcı bir hak olarak karşımıza çıkabilir.

1.3.1.2 Anonimlik Hakkı

Siber alanın insan haklarına getirdiği bir diğer tartışma ise anonimlik hakkı olarak karşımıza çıkmaktadır. Çevrimiçi etkinliklerin artmasıyla birlikte, günlük hayatımızda varolan “anonimlik” terimi dijital platforma taşınmıştır. Anonimlik, kamuya açık olarak bilinmeyen anlamına gelmektedir (Ziolkowski; 2013, s.40). Anonim eylemler/anonimlik uzun bir geçmişe sahiptir ve “anonim eserler, şarkılar, broşürler ve hatta kitaplar insanlığın ilerlemesinde önemli bir rol oynamıştır” (Solove, 2007, s. 139). Anonimlik, özne olarak kişinin bilinmemesi durumunda kullanılabildiği gibi, bir sanat eserinin ya da bir eserin kimin tarafından yazıldığı/yapıldığının bilinmemesi anlamında da kullanılmaktadır. Konumuz açısından burada özne olarak kişinin bilinmemesi tanımı ele alınacaktır. Dijital çağ öncesinde de var olan bu kavram klasik anonimlik olarak adlandırılabilir. Birçok kavramın dijital dünyaya taşınmasıyla birlikte anonimlik kavramının da bu uzamda yer edindiği görülmektedir.

Litearatürde siber uzayda anonimlik teriminin kullanımının çeşitli anlamlar içerdiği görülmektedir. Levine, anonimliği “görünen anonimlik” ve “gerçek anonimlik” iki farklı şekilde tanımlamıştır (Levine, 1996, s.1528-1529). Du Pont ise yine Levin gibi anonimliği kategorilere ayırıp, anonimlik türlerini “gerçek anonimlik” ve “sahte anonimlik” olarak isimlendirmiştir (2001, s.196). Aslında iki yazarın da burada belirtmek istediği kategorizasyon aynı noktaya ulaşmaktadır. İsimlerinden de anlaşılacağı gibi görünen anonimlik ya da sahte anonimlik bireyin çevrimiçi ortamda tam olarak anonim olmamasını sağlamamaktadır. Bu anonimlik türü takma ad (nickname) gibi, bilgisayar kullanıcılarına elektronik sohbet tartışmaları veya elektronik posta amacıyla kendi adlarından başka adları kullanma fırsatı sunmaktadır (Levine, 1996, s.1529). Mesajı gönderenin kimliği, kolayca açığa çıkarılmadığı veya

kolayca erişilebilir olmadığı için gerçekten anonim gibi görünse de, aslında gönderenin kimliğini bir şekilde bulmak mümkün olmaktadır (Du Pont, 2001, s.196). Bunun nedeni bu tür kullanıcıların genellikle internet servis sağlayıcılarına gerçek kimliği ile kayıt olmalarıdır (Levine, 1996, s.1529). World Wide Web'de gezinmek, sonuçları olmayan anonim bir etkinlik olmaktan uzakta görünmektedir (Weber & Heinrich, 2012, s. VII). Dolayısıyla bu tür anonimlik yetkili merciler tarafından izlenebilmektedir. Pek çok internet kullanıcısı, isimlerini, adreslerini veya banka bilgilerini girerek kimliklerini açıklamadıkları sürece İnternet'in anonimliğine ve kişisel verilerinin korunmasına hala inanmaktadır (Schwartz ve Solove, 2011, s.590). Bu nedenle de bireylerin internette anonim olma durumları aslında tam da sözde anonimlik ile ilintili olarak karşımıza çıkmaktadır. Bu anonimlik çeşidi bireylerin/vatandaşların ifade etmek istedikleri bir duyguyu veya bir düşüncüyü sanal ortamda dile getirmelerini kolaylaştırmaktadır.

28 Mayıs 2003 tarihinde “Avrupa Konseyi Bakanlar Komitesi İnternette İletişim Özgürlüğü Bildirisinde” (Declaration on Freedom of Communication on the Internet) anonimlik bir hak olarak tanımlanmıştır. Bildiride yer alan maddede anonimlik şu şekilde belirtilmiştir: “Çevrimiçi gözetime karşı korumayı garantiye almak ve bilgi ve düşüncelerin özgür ifadesini çoğaltmak amacıyla üye devletler, internet kullanıcılarının kimliklerini ifşa etmeme isteklerine saygı göstermelidirler”.

Mayıs 2015'te ise, düşünce ve ifade özgürlüğünün desteklenmesi ve korunmasına ilişkin BM Özel Raportörü çevrimiçi anonimlik hakkında çok önemli bir rapor yayımlamıştır. Raporda çevrimiçi anonimliğin korunması özel hayatın gizliliği hakkı ile birlikte ele alınmıştır. İlgili raporda; “Şifreleme (Encryption) ve anonimlik, güçlü bir şekilde korunmalı ve teşvik edilmelidir çünkü bunlar, dijital çağda düşüncüyü ifade etme özgürlüğü hakkının anlamlı bir şekilde kullanılması için gerekli olan özel hayatın gizliliğini ve güvenliği sağlar” (Human Rights Council, 2015).

Her iki belgeye baktığımızda ifadelerden de anlaşılacağı üzere siber uzayda anonimlik, özel hayatın gizliliği hakkının ve ifade özgürlüğünün bir bileşeni olarak karşımıza çıkmaktadır. Bunun yanı sıra devletlerin siber gözetimine karşı, bireyi korumak adına, bireylerin siber uzayda anonim olma hakkına saygı duyulması gerektiği de dolaylı olarak ifade edilmektedir.

Siber uzayın anonimliği insanlara daha özgür ve açık bir şekilde davranmaları için eşsiz bir ortam sağlamaktadır (Hu, Kumar vd; 2017, s. 1). İnternette bireyler anonim olarak iletişim kurduklarında, kendilerini güvende hissederler. Bu da demokratik ülkelerde vatandaşların kişisel itibarlarına karşı misilleme korkusu olmadan görüşlerini dile getirmelerini de olanak tanımaktadır (Du Pont, 2001, s.196). Bir başka deyişle iletişim kurulan kişi ya da mercilerle yüz yüze etkileşim olmadığından dolayı bireyler söylemleri yüzünden çekinmemekte ve gerçekten söylemek istediklerini hiçbir baskı olmadan ya da herhangi bir kaygı gütmeden ifade edebilmektedirler. Çevrimiçi anonimliğin özellikle ifade özgürlüğü konusunda bireylere sağladığı avantaj ve sosyal fayda yadsınamayacak derece büyüktür (Akyeşilmen, 2021, s.318) . İfade özgürlüğünü kolaylaştırmanın yanı sıra, kullanıcıların İnternet'teki faaliyetlerinin ticari şirketler ve devlet tarafından gözetlenmesini ve izlenmesini önlemelerini de sağlamaktadır.

Çevrimiçi anonimlik özel hayatın gizliliği konusunda da bireylere birtakım avantajlar sunmaktadır. Anonim iletişim, bireylerin kimliklerini sanal ortamda açıklamak istemediği zaman en güçlü araçlardan biri olarak karşımıza çıkmaktadır. Kişiler, herhangi bir kurumdan veya kişiden bilgi talep ederken gerçek kimliklerini gizlemek için takma adlar da kullanabilmektedirler. Kadınlar, cinsiyet ayrımcılığı veya tacizden kaçınmak için internette iletişim kurmak için takma adı kullanmayı tercih edebilmektedir (Kling, Lee, Teich ve Frankel, 1999, s. 83). Bu tür örnekleri çoğaltmak mümkündür. Ziolkowski ise siber uzayda anonimliğin, özel hayatın gizliliği kapsamında bireye sağladığı fayda açısından kullanılabildiği alanları aşağıda şu şekilde dile getirmiştir; “özel bilgilerin korunması(örn. şifreler, sosyal güvenlik ve kredi kartı numaraları),ticari işlemlerin yürütülmesi, ifade özgürlüğü (siyasi ve siyasi olmayan iddialar açısından), çevrimiçi suç faaliyetlerini tespit etmede kolluk kuvvetlerinin çabaları (örn. polis yasadışı faaliyetler için sohbet odalarını ve forumları anonim olarak gözlemler)” (2013, s.41).

Tüm bu nedenlerden dolayı, bireylerin kimliklerini ifşa etmeden interneti anonim olarak kullanma motivasyonları çok çeşitlidir. Çevrimiçi anonim iletişim bireylere ifade özgürlüğü sunarken, diğer yandan da bireyin özel hayatının ihlal

edilmesi, gözetlenmesi ve bireye özgü bilgilerin çalınması gibi riskleri de beraberinde getirmektedir.

Çevrimiçi anonim iletişim, insanların bilgi alışverişinde bulunma ve iletişim kurma biçimleriyle ilgili fırsatlar sunduğu gibi bazen de suç teşkil eden amaçlar uğruna kullanılabilir. Aslında günümüzde siber uzayda anonimliği tartışmalı kılan nokta da tam olarak budur. Anonimlik, bireylerin çevrimiçi kendisini ifade etmesini sağlayan bir kavram olarak karşımıza çıksa da bazen de bireyleri tehdit etmek, bilgileri çalmak, kötüye kullanmak ve siber zorbalık için kullanılan bir araç olarak da karşımıza çıkmaktadır. Aynı zamanda, bir başkasının kimliğine bürünerek anonim olma, insanlara yabancı bir kimliğin arkasına saklanma olanağı sunmakta ve böylelikle kişinin kendi adına olası sonuçlar doğurmadan fikir verme avantajını da bahşetmektedir (Weber & Heinrich, 2012, s. 3). Bu yönlerin yanı sıra, internete yüklenen bilgilerin World Wide Web’den mahkeme kararı olmaksızın kaldırılmaması her türlü bilginin herkese açık hale gelmesini sağlamaktadır ki bu da özel hayatın gizliliğini suiistimal eden bir başka nokta olarak karşımıza çıkmaktadır. İnternette anonimliğin olası suiistimal edilmesinden endişe eden bireyler, interneti kullanan kişilerin özel hayatını suiistimal ettiği ve bireye zarar verdiği gerekçesiyle, anonimliği yasaklayan veya sıkı bir şekilde düzenleyen bir politikayı desteklemektedir. Taciz, nefret söylemi, kişisel bilgilerin çalınması, başka bir bireyin kimliğini çalarak o kişiymiş gibi davranma ve ırkçılık çevrimiçi dünyamızda bireylere zarar vermektedir. Ancak çevrimiçi anonimliği yasaklamak, internetin olumlu yanını baltalarken bunları ortadan kaldırmak için de çok az şey yapabilir. Çünkü siber uzay anarşik bir yapıdadır ve sınırları yoktur. Dolayısıyla hükümetlerin burayı kontrol altına alması ve siber uzayda her bir suçlunun failinin bulunup yargılanması mümkün olmamaktadır. Bunun yanı sıra anonimliğin kısıtlanması, siber uzayda ifade özgürlüğü ve özel hayatın gizliliği üzerinde ciddi olumsuz sonuçlara yol açacaktır. Bu noktada gözetilmesi gereken husus anonimliğin bireyin özel hayatının gizliliği ve ifade özgürlüğü açısından bir hak olduğudur. Ancak bu hak sonsuz olarak anlaşılmamalıdır. Anonimlik hakkı ancak diğer bireylerin haklarına da saygı duyulacak şekilde kullanılırsa gerçek işlevini yerini getirecek ve bireye siber uzayda daha özgür bir ortam yaratılmasını sağlayacaktır.

1.3.1.3. Unutulma Hakkı

Yeni kuşak haklar arasında tartışılan bir diğer hak ise unutulma hakkıdır. İnternetin günlük hayatımızın bir parçası olması, bu platformda kişisel verilerin paylaşılması, saklanması ve depolanması bilgi yığınlarına yol açmaktadır. Çevrimiçi ortamda depolanan bilgilere, bireyin istediği zaman müdahale edememesi, hangi bilgilerinin çevrim içi ortamda yayımlandığını bilememesi de bireyleri kişisel verileri koruma anlamında korku ve paniğe sevk etmektedir.

Bu anlamda bireyin kişisel verilerine, üçüncü kişiler tarafından erişimin (kısmen) kısıtlanması sağlanarak; onurlu yaşamının güvence altına alınması, toplumdan dışlanmasının engellenmesi ve geçmişinden bağımsız bir şekilde yeni bir başlangıç yapabilmesi adına kişisel verilerin korunması hakkının bir görünümü olarak “Unutulma Hakkı” gündeme gelmektedir (Kişisel Verileri Koruma Kurumu (KVKK), 2021, s. 9).

Silme hakkı olarak da bilinen “Right to Erasure,” Unutulma hakkı, İnternet arama motorlarının belirli sonuçları kaldırmasını talep ederek bireylerin çevrimiçi kimlikleri üzerinde kontrol sahibi olmalarını sağlayan, yeni ortaya çıkan bir yasal kavramdır (Carter, 2016). Bu hakkın amacı, bireylere kişisel bilgileri üzerinde, özellikle de bu bilgilerin sıklıkla rızaları olmaksızın yayılabildiği sanal dünyada, daha fazla söz hakkı vermek ve verileri üzerindeki kontrolü bir nebze de olsa sağlayabilmektedir.

Avrupa'da, unutulma hakkı tartışmasının ana odak noktası, 2010 yılında açılan ve 2014 yılında nihai sonuca ulaşan Mario Costeja Gonzales davasıdır (Mario Costeja Gonzales Davası, 2014) . İlgili dava, Gonzalez isimli bir İspanyol'un, ödenmemiş borcu nedeniyle el konulan evi ile ilgili, açık artırma duyurusunu içeren bir çevrimiçi arama motorunda kendisi hakkında çıkan sonucunun kaldırılmasını talep etmesiyle ilgilidir. Söz konusu duyuru onaltı yıl önce bir İspanyol gazetesinde yayınlanmış ve daha sonra dijital ortama aktarılarak çevrimiçi erişime açılmıştır. Gonzales de ilgili durum ortadan kalktığından dolayı bu haberin ilgili arama motorundan kaldırılmasını talep etmektedir. Avrupa Birliği Adalet Divanı (Court of Justice of the European Union), bilgilerin yetersiz, ilgisiz veya artık alakalı olmaması ve bağlantıların

sürdürülmesinde kamu yararı bulunmaması koşuluyla, bireylerin arama sonuçlarından belirli web sayfalarına bağlantıların kaldırılmasını talep etme hakkına sahip olduğuna karar vermiştir. Mahkeme ayrıca Google gibi arama motorlarının 95/46/EC sayılı veri koruma direktifi kapsamında "veri denetleyicisi" olarak kabul edildiğini ve AB veri koruma direktifine tabi olduğunu tespit etmiştir (Hijmans, 2014, s. 555-560).

Böylece Avrupa'da tartışılan bu hak, kişisel verileri koruma kapsamında ele alınarak 2012 yılında Genel Veri Koruma Yönetmeliği'nin taslağında yer almıştır. GDPR, 2016 yılında tamamlanmış ve 25 Mayıs 2018 tarihinde yürürlüğe girerek 95/46/EC sayılı veri koruma direktifinin yerini almıştır. GDPR'nin 17. Maddesinde ise "veri sahibinin, bir başka deyişle öznenin unutulma hakkını hangi durumlarda talep edeceğine ve bu hakkın istisnalarına yer verilmiştir. İlgili maddeye göre;

"Veri sahibi, denetleyiciden kendisiyle ilgili kişisel verilerin gereksiz bir gecikme olmaksızın silinmesini talep etme hakkına sahip olacaktır ve denetleyici, aşağıdaki gerekçelerden birinin geçerli olduğu durumlarda kişisel verileri bir gecikme olmaksızın silme yükümlülüğüne sahip olacaktır:

- a) kişisel verilerin toplanma veya başka bir şekilde işlenme amaçlarıyla ilgili olarak artık gerekli olmaması;
- b) veri sahibi, Madde 6 (1)'in (a)² bendine veya Madde 9 (2)'nin (a)³ bendine göre işlemenin dayandığı ve işleme için başka bir yasal dayanağın olmadığı durumlarda rızasını geri çeker;
- c) veri öznesi Madde 21 (1)⁴ uyarınca işlemeye itiraz ediyorsa ve işleme için ağır basan meşru gerekçeler yoksa veya veri öznesi Madde 21 (2)⁵ uyarınca işlemeye itiraz ediyorsa;

² Madde 6(1)-a bendi: "veri sahibinin, kişisel verilerinin bir veya daha fazla özel amaç için işlenmesine izin vermesi;"

³ Madde 9 (2)-a bendi: "Birlik veya Üye Devlet yasalarının 1. paragrafta atıfta bulunulan yasağın veri sahibi tarafından kaldırılamayacağını öngördüğü durumlar dışında, veri öznesi bu kişisel verilerin bir veya daha fazla belirli amaç için işlenmesine açık rıza vermiştir"

⁴ Madde 21 (1): "Veri öznesi, 6(1) maddesinin (e) veya (f) bendi temelinde, kendisiyle ilgili kişisel verilerin işlenmesine, kendi özel durumuna ilişkin gerekçelerle her zaman itiraz etme hakkına sahip olacaktır. , bu hükümlere dayalı profil oluşturma dahil. Kontrolör, veri konusunun çıkarlarını, haklarını ve özgürlüklerini geçersiz kılan veya yasal iddiaların oluşturulması, kullanılması veya savunulması için işleme için zorlayıcı meşru gerekçeler göstermediği sürece kişisel verileri artık işlemeyecektir".

⁵ Madde 21 (2) : "Kişisel verilerin doğrudan pazarlama amacıyla işlendiği durumlarda, veri sahibi, kendisiyle ilgili kişisel verilerin, bu tür doğrudan pazarlama ile ilgili olduğu ölçüde profil

- d) kişisel verilerin hukuka aykırı olarak işlenmiş olması;
- e) Veri sorumlusunun tabi olduğu Birlik veya Üye Devlet hukukundaki yasal bir yükümlülüğe uymak için kişisel verilerin silinmesi gerekiyor;
- f) kişisel veriler, Madde 8 (1)⁶ 'de atıfta bulunulan bilgi toplumu hizmetlerinin sunumu ile ilgili olarak toplanmıştır”.

Yukarıdaki şartların sağlanması halinde veri sorumlusu “kişisel verileri haklı bir gecikme olmaksızın silme yükümlülüğüne” sahiptir. Unutulma hakkı dört farklı şekilde gerçekleştirilebilir. Bunlar; başvurunun kaldırılması, anonim hale getirilmesi, silinmesi ve erişimin sınırlandırılmasıdır (s. 156-157). Ancak unutulma hakkının mutlak bir hak olarak tanımlanmadığını ve bu bağlamda da istisnaları olduğunu belirtmemiz gereklidir. Unutulma hakkının istisnaları yine ilgili belgenin 17. Maddenin 3. fıkrasında tanımlandığı görülmektedir. Buna göre istisnalar şu şekilde dile getirilmiştir; ifade ve haber alma özgürlüğü söz konusu olduğunda, yasal yükümlülüğe uyum veya kamu yararı veya resmi yetkinin kullanılması durumunda, halk sağlığı ve arşivleme, bilimsel, tarihsel ve istatistiksel amaçlı kamu yararı söz konusu olduğunda ve yasal taleplerin oluşturulması, kullanılması ve savunulması için söz konusu hakkın istisnaları olarak kabul edilmektedir (GDPR, 2018).

Unutulma hakkının istisnalarının belirtilmesi ve mutlak hak olarak tanımlanmaması aslında bu hakkın diğer haklarla çatışması durumunda hangi bağlamda ele alınacağını belirtmektedir. Dolayısıyla kamuoyunda en çok tartışılan unutulma hakkının ifade özgürlüğü ve bilgiye erişim hakkıyla çatıştığıdır. Örneğin Rosen, unutulma hakkının sansüre yol açabileceğini ve halkın önemli bilgilere erişimini sınırlayabileceğini ileri sürmüştür (2012, s.88). Løkke ise, bu hakkın ifade özgürlüğü ve özel hayatın gizliliği hakkı arasındaki gerilimi tırmandıracağını, özellikle otoriter toplumlarda bu durumun daha da sorunlu olduğunu, dolayısıyla unutulma hakkında esas olanın hem şeffaflığa duyulan ihtiyaç hem de sürecin rastgele kararlar

oluşturma dahil olmak üzere, bu tür pazarlama için işlenmesine herhangi bir zamanda itiraz etme hakkına sahip olacaktır”.

⁶ Madde 8 (1): “6(1) maddesinin (a) bendinin geçerli olduğu durumlarda, doğrudan bir çocuğa bilgi toplumu hizmetlerinin sunulmasıyla ilgili olarak, çocuğun en az 16 yaşında olması durumunda çocuğun kişisel verilerinin işlenmesi yasal olacaktır. Çocuğun 16 yaşından küçük olduğu durumlarda, bu tür işlemler yalnızca çocuk üzerinde ebeveyn sorumluluğu sahibi tarafından izin verildiği veya izin verildiği ölçüde ve ölçüde yasal olacaktır. Üye Devletler, 13 yaşından küçük olmamak koşuluyla, bu amaçlar için yasayla daha düşük bir yaş sağlayabilir”.

bütününden ziyade bütüncül bir şekilde ele alınması gerektiriliğini savunmuştur (2018, s.46-47). Ancak bu GDPR'nin 17. Maddesinin 3. Fıkrasında belirtilen istisnalar tam da bu iki hakkı dengede tutmak için belirtilmiştir. Silinmesi veya kaldırılması talep edilen bilgilerde öncelikle kamu yararı aranmaktadır. Kamu yararının olduğu durumda ise mutlak bir hak olmadığından dolayı unutulma hakkı bireyin aleyhine sonuçlanabilmektedir.

Unutulma hakkı çerçevesinde karşımıza kıtalar arası iki farklı bakış açısı da çıkmaktadır. Avrupa özel hayatın gizliliği çerçevesinde ve buna bağlı olarak unutulma hakkı özelinde bireyin onur ve şöhretini temel alırken, Amerika ifade özgürlüğünü öncelemektedir. Avrupa'da, unutulma hakkının fikri kökleri; cezasını çekmiş ve ıslah olmuş bir suçlunun mahkumiyetine ve hapsedilmesine ilişkin gerçeklerin yayınlanmasına itiraz etmesine izin veren ve bunu bir hak olarak tanıyan Fransız hukukunda bulunmaktadır (Rosen, 2012, s.88). Amerika Birleşik Devletlerinde ise, Birinci Değişiklikte (First Amendment) ifade özgürlüğü hakkı, hüküm giymiş kişiler hakkında kamu yararını ilgilendiren doğru bilgilerin yayılması lehine uygulanmaktadır (Weber, 2011, s.122). Böyle bir hakkın pratikte uygulanması sansür anlamına gelmekte ve köklü bir yasa olan ABD Birinci Değişiklik haklarına ters düşmektedir (Royston, 2016, s.273). Bu bağlamda da unutulma hakkı, ifade özgürlüğünün önceliğinden dolayı ABD mahkemelerinde büyük ölçüde reddedilmiş veya dar çerçevede tanımlanmıştır.

Unutulma hakkı özel hayatın gizliliği hakkının temel unsurlarından biri olan ad, şan ve şöhret hakkı ve bireyin onuru gibi kavramlarla doğrudan ilintili olduğundan özel hayat açısından büyük önem arz etmektedir. Bu hak her ne kadar belirli bir zaman diliminde kamuya açık bilgileri içerse de dijital ortamda birey hakkında yer alan birçok bilgi, bireyin rızası dışında ve haberi olmadan çevrimiçi ortamlara aktarılabilmektedir. Ayrıca bireyle ilgisiz veya bireye dair güncelliğini yitirmiş bilgiler, birey hakkında yanıltıcı ve utandırıcı olabilmektedir. Bu durumlar bireyin toplum içerisinde itibarının zedelenmesine neden olmaktadır. Bu minvalde bu hakkı sadece bilgilerin silinmesi düzeyine indirgememek gerekmektedir. Hala tartışılmakta olan unutulma hakkı ifade özgürlüğü ile çeliştiği düşünülmekten dolayı tartışılmaya da devam etmektedir. Ancak burada hatırlatmanması gereken önemli bir detay karşımıza çıkmaktadır.

Unutulma hakkı mutlak bir hak değildir ve bu yüzden hakkın istisnaları belirtilmektedir. Bununla birlikte verilerin arama motorlarından kaldırılması verilere hiç ulaşamama anlamını taşımamaktadır. Sadece kamu yararı olmadığı sürece herkesin bu bilgilere erişemeyeceği anlamına gelmektedir. Adli yargı sürecinde olan verilere hukuki bir şekilde erişmenin mümkün olduğu göz ardı edilmemelidir. Dolayısıyla dava örnekleri çoğalıp içtihatlar çeşitlendikçe ilerleyen zamanlarda ifade özgürlüğü ve unutulma hakkı arasındaki dengenin korunabileceği düşünülmektedir.

1.4 Özel Hayatın Gizliliğine Yönelik Teorik Yaklaşımlar

Özel hayatın gizliliği, Samuel Warren ve Louis Brandeis'in (1890) mahremiyet hakkı isimli makalesinin yayınlamasıyla önemi anlaşılmış ve uluslararası toplum tarafından da farkına varılmıştır. O dönemden beri kavram farklı disiplinler tarafından tartışılmış, uluslararası anlaşmalarla içeriği tanımlanmaya çalışılmıştır. Alan Westin 1967 yılında yazdığı "*Privacy and Freedom*" isimli eserinde, Irwin Altman'ın ise 1975 yılında yayınladığı "*The environment and social behavior: privacy, personal space, territory, and crowding*" kitabında daha geniş bir çerçevede ele alınmıştır. Her iki teorisyenin çalışmaları, literatürde önerilen kavramlar olmuş ve özel hayatın gizliliği konusundaki temel çalışmalar arasında yer almıştır. Ayrıca bu eserler, çağdaş teorilerin de özü olarak kabul edilmektedir.

Alan Westin'in çalışmasının yayınlanmasının akabinde Fransa, Birleşik Krallık, Kanada, Amerika Birleşik Devletleri (ABD) ve İsveç'te bir dizi araştırma yapılmış ve bu ülkelerin her biri daha sonra Westin'in bilgi kontrolü olarak özel hayatın gizliliği tanımına dayanan veri koruma yasaları kabul edilmiştir. Günümüzde de kırktan fazla ülke tarafından özel hayatın gizliliği ile ilgili, yasal rejimlerini uyumlu hale getirmek için devam eden uluslararası çabaların bir parçası olarak benzer yasalar çıkarılmıştır (Bennett ve Raab, 2002, s. 102).

Altman ise Westin'in teorisini geliştirerek yine dönemin en önemli ve temel yapıtları arasında yer almıştır. Altman'ın çalışmaları birçok yazarın çalışmalarının temelini oluşturmuş (Margulis, 1977, Sundstrom, 1986 ve Newell, 1995) ve özel hayat ile ilgili olarak (Margulis, 2003, s. 411) önemli analizlerde yer almıştır. Tüm bu

nedenlerden dolayı, bu iki yazarın da çalışmalarının özel hayatın gizliliğinin kavranması ve kapsamlı açıklanmasından dolayı çalışmamızda bu iki teori seçilmiştir.

1.4.1 Özel Hayatın Gizliliği ve Özgürlük Teorisi

Alan Westin'in "özel hayatın gizliliği ve özgürlük" teorisi temelde bireysel özgürlük, özel hayatın gizliliği ve toplumsal normlar arasındaki ilintiyi açıklamayı amaçlamaktadır.

Westin özel hayatın gizliliğini şu şekilde tanımlamıştır;

Özel Hayatın Gizliliği, bireylerin, grupların veya kurumların, kendileri hakkındaki bilgilerin başkalarına ne zaman, nasıl ve ne ölçüde iletileceğini kendileri belirleme iddiasıdır. Bireyin toplumsal katılımı ilişkisi açısından bakıldığında, mahremiyet, bir kişinin ya yalnızlık durumunda ya da küçük grup içinde ya da daha büyük gruplar arasında, fiziksel ya da psikolojik yollarla toplumdan gönüllü ve geçici olarak geri çekilmesidir.

Westin tanımında insanların özel hayatın gizliliğine ihtiyacı olduğundan bahsetmektedir. Birey bu istemini ne zaman ve hangi koşullar altında istediğine de kendisi özgürce karar vermektedir. Burada özel hayat hem psikolojik hem de fiziksel olarak tanımlanmıştır. Bir başka deyişle gereken hususta bu süreci „geçici“ olarak tanımlamasıdır. Westin’e göre birey sosyal bir varlık olduğundan dolayı mahremiyet arzusu mutlak değildir. Dolayısıyla birey sosyal çevresi ve özel hayatı arasında bir denge kurarak yaşamaya devam eder (Westin, 1968, s. 7). Özel hayatın gizliliği bireyin kendisi için amaç olarak değil, toplumda yaşamasının koşulu sonucu kendini gerçekleştirmesi için bir araç olarak karşımıza çıkmaktadır.

Dinamik bir süreç olarak karşımıza çıkan özel hayatın gizliliğinde Westin dört durum tanımlamıştır. Bunlar, yakınlık, yalnızlık, anonimlik ve kendini sakınmadır. Durumlar, özel hayatın gizliliğinin işlevlerinin, bir başka deyişle amaçlarının gerçekleştirildiği araçlardır.

Yalnızlık, bireylerin diğerlerinin gözleminden kurtulduğu ve bireyin ulaşabileceği en eksiksiz mahremiyet hali olarak görülmektedir. Yakınlık ise, bireyin rahat ve samimi bir ilişki kurması, hareket etmesi amacıyla küçük bir grubun üyesi

olarak hareket etmesidir. Anonimlik, kamuya açık yerlerde veya kamusal eylemlerde kimlik ve gözetimden uzak olmayı ifade ederken; kendini sakınma, kendinizle ilgili bilgileri başkalarına ifşa etmeme özgürlüğü ile ilgilidir. Hayatımızın çoğu yalnızlık veya anonimlik içinde değil, yakınlık durumlarında ve başkaları tarafından tanındığımız grup ortamlarında geçmektedir.

Durumlar amacı gerçekleştirmek için kullanılan araçlar olarak karşımıza çıkar demiştik. Peki Westin'e göre özel hayatın gizliliğinin amacı nedir? Araçlar nasıl kullanılır? Bu soruların cevaplarına bakıldığında Westin'in özel yaşamın gizliliği için dört amaç tanımladığını görmekteyiz. Bunlardan ilki kişisel özerklik ihtiyacıdır. Westin yalnızlığı öz benlik olarak tanımlamakta ve öz benliği de eşmerkezli sarmal örneğinden yola çıkarak açıklamaktadır. Buna göre; çemberin en içinde birey "nihai sırlarını" ("ultimate secrets") barındırmaktadır. Eğer birey baskı altında değilse bu sırlarını kimseyle paylaşmamaktadır. Bir sonraki halkada ise yakın akrabaları veya bireyin tanımadığı yabancılarla paylaşacağı mahrem sırlar yer almaktadır. Sarmalın en dış halkası ise bireyin arkadaşlarına açıktır ve tüm herkese açık olan bireyin gündelik hayattaki ilişkilerine ulaşana kadar devam etmektedir. Westin bu sarmalda bireyin başkaları tarafından manipüle edilmekten, hükmedilmekten veya ifşa edilmekten kaçınma arzusunu ifade etmektedir. İkinci amaç duygusal rahatlama. Bireyler toplum içerisinde hem fiziksel hem de psikolojik gerilimler yaşayabilirler. Bu gibi durumlarda bireyler gündelik yaşamın karmaşasından çıkarak duygusal rahatlama, dinlenme ihtiyacı duymaktadırlar. Rahatlamak, kişinin kendisi olmak, günlük hayatın streslerinden kaçmak ve öfke, hayal kırıklığı, keder veya diğer güçlü duyguları tepki veya alay korkusu olmadan ifade etmek için gerekli fırsatları sağlayarak bireyin sağlıklı bir şekilde hayatını devam ettirmesini desteklemektedir. Bireyin duygusal rahatlama yaşamaması bireyi psikolojik çöküş ve intihara kadar sürükleyebilmektedir. Üçüncü bir işlev, öz değerlendirme ve karar vermedir. Her bireyin kişisel deneyimlerini analiz etmesi ve olaylarla bağdaştırması gerekmektedir. Yalnızlık ve düşünme fırsatı yaratıcılık için çok önemlidir. Bireyler deneyimlerinden edindikleri bilgiyi işlemek için yer ve zamana ihtiyaç duymaktadırlar. Bu da bireyin tutarlı olmasını ve olaylara uygun hareket etmek için alternatifleri değerlendirmesi ve sonuçları öngörme fırsatı sunmaktadır. Nihai işlev olan ve dördüncü amaç olarak

karşımıza çıkan sınırlı ve korumalı iletişimin iki yönü bulunmaktadır: Sınırlı iletişim kişilerarası sınırları belirlerken, korumalı iletişim ise, kişisel bilgilerin güvenilir kişilerle paylaşılmasını sağlamaktadır (Westin, 1967, s. 39-44).

Westin'in teorisine baktığımızda bireyin sosyal, psikolojik ve fiziksel durumlarını da ele alarak özel hayatın gizliliğinin detaylı olarak açıklamaya çalıştığı görülmektedir. Westin özel hayatı bilgi çerçevesinde bir başka deyişle iletişim çerçevesinde tanımlamıştır. Birey burada özel hayatını sadece kendi içerisinde değil, toplumsal süreçlerden, çevresinden de etkilenerek ve bu süreçlere göre davranışlarını belirleyerek toplum ile ilişkisini şekillendirmektedir. Bu süreç, bireyin sürekli içerisinde yer aldığı dinamik bir süreç olarak karşımıza çıkmaktadır. Birey hangi durum ve koşullarda özel hayatıyla ilgili olan bilgilerinin ne kadarını, kimlerle ne açıdan paylaşacağına karar vermektedir. Bir başka deyişle birey kendisi ile ilgili bilgileri ya kendisini gözetimden koruyarak (yalnızlık ve yakınlık durumu), ya kimliğini paylaşmayarak (anonimlik) ya da ifşadan korunarak (sakınma) kendisini toplum içerisinde gerçekleştirebilmektedir. Bu teoride esas vurgulanmak istenen bireyin özel hayatın gizliliği ile toplumsal dengenin sağlanmasının gerekliliğidir.

1.4.2. Özel Hayatın Gizliliğini Düzenleme Teorisi

Westin'in özel hayatın gizliliği ve özgürlük teorisinden etkilenen Irvin Altman ise 1975 yılında yayımladığı kitabında Westin teorisine katkılar yaptığı görülmektedir. Westin gibi, özel hayatın gizliliğini kültürel bir evrensel değer olarak görmüş ve çeşitli sosyal ortamları baz alarak terosini açıklamaya çalışmıştır. Ancak Altman, Westin'in bireyin özel hayatın gizliliğini ve sosyal etkileşimini zıt kutuplara yerleştirmek yerine, bireyin iletişimi yan yana getirerek, ikisi arasında müzakere edilen çizgi olarak ele almaktadır. Bir başka deyişle bireyin özel hayatın gizliliği ve sosyal etkileşimini ne şekilde yönettiğini açıklamaktadır. Altman buna göre özel hayatı şu şekilde tanımlar: (Altman, 1975).

Bir kişinin veya bir grubun başkalarıyla etkileşimini düzenlediği kişilerarası bir sınır süreci. Benliğin başkalarına açıklık derecesini değiştirerek, varsayımsal bir kişisel sınır, başkalarıyla sosyal etkileşime az ya da çok açıktır. Bu nedenle özel hayat,

bir birey veya bir grup tarafından bir öz-sınır üzerinde seçici kontrolü içeren dinamik süreçtir (s. 6).

Altman'a göre, özel hayatın gizliliğinin düzenlenmesi, iki temel psikolojik ihtiyaçtan etkilenen dinamik bir optimizasyon sürecidir: Bir yandan, bireyin özel hayatını koruma, kişisel bilgilere erişimi ve paylaşımını kontrol etme ihtiyacı vardır, diğer yandan da sosyal olarak etkileşime girme ve böylece kişisel bilgileri paylaşma ihtiyacı doğmaktadır. Zamanla kişi veya grup değişen koşullara tepki olarak kendini veya grubu başkalarına açar ya da kapatır. Bu bağlamda da özel hayatın gizliliği aslında "benliğe erişimin seçici kontrolü" olarak karşımıza çıkmaktadır (1975, s. 22-24). Bireyi başkalarından ayırmak için etrafımızdaki bir tür bölge veya aura olan "kişisel alana" ihtiyacımız var. Bu mekânsal mesafe de "bireye konfor alanı, kolaylık ve rahatlama" sağlamaktadır (Altman, 1975, s. 54-96).

Altman'ın teorisinde özel hayatın gizliliği ile ilgili beş özellik vardır; ilk özellik, özel hayatın gizliliğinin işlediği bireysel ve grup seviyeleridir; 2) özel hayatın gizliliğinde istenen ve mevcut seviyeleri arasındaki fark (burada istenen bir kişinin ihtiyaçlarına ve gereksinimleri için olması gerekeni belirtirken, mevcut seviye ise bir kişinin sahip olduğu olarak tanımlanır); 3)Optimal (arzu edilen ve gerçekleşen eşit olması durumu) bir özel hayatın gizliliğinin tanımlamanın imkânsızlığı; 4) kişilerarası sınır kontrolünün dinamik süreci (diğer bireylerle olan iletişimimizi hızlandıran veya düzenleyen bir süreç, bireyin iç dünyası ve dış koşullar karşısında tepki olarak kendisini karşısındakine veya topluma ne kadar ifade ettiği ve son olarak 5) özel hayatın gizliliğinin iki yönlü karakteri (özel hayatın gizliliği diğer kişilerden ya da çevreden gelen girdileri ve çıktıları içermesi nedeniyle iki yönlüdür) bulunmaktadır (Margulis, s.418-419).

Margulis, Altman ve Westin teorisinin birçok ortak özelliği olduğunu hatta Altman'ın Westin'in teorisini temel alarak yeni teori ürettiğini ileri sürmektedir. Buna göre, her iki teoride psikolojik bir kavram olarak özel hayatın gizliliği üzerine teoriye katkıda bulunmaktadır. Özel hayatın gizliliği için her ikisi de bireyin kendini kontrol ettiğini ve bu sürecin nasıl düzenlenmesi gerektiğini vurgulamaktadır. Bir başka ortak noktaları ise özel hayatın gizliliğini dinamik bir süreç olarak tanımlamaları ve hem bireysel hem de grup düzeyinde tanımlamalar yapmalarıdır. Her ikisi de özel hayatın

gizliliğinin bir bütün olarak veya kısmen kültürel evrensel (cultural universal) olduğu konusunda hemfikirlerdir. Altman'a göre, özel hayatın psikolojik ifadeleri kültüre özgü iken Westin'e göre, özel hayat durumları ve işlevleri, altta yatan sosyopolitik değerlerinden dolayı siyasi sistemlere özgüdür (Margulis, 2003, s. 423).

Westin ve Altman teorisi arasındaki temel fark, Altman'ın daha kapsayıcı bir özel hayatın anlayışına yol açan, sosyal etkileşimlere yaptığı vurgudan kaynaklanmaktadır (Margulis, 2003, s. 418-419). Bir başka deyişle, Altman insan ve çevre etkileşimine yeni bir bakış açısı kazandırmıştır. Genel kanının aksine özel hayatın gizliliğinin bireysel bir süreç değil, doğası gereği sosyal bir süreç olduğunu öne sürmüştür. Westin teorisinden bir başka farkı ise, özel hayatın gizliliğinin sadece bireyin bilgileri paylaşma kontrolüne bağlı olmaması, bu süreci hem girdisi hem de çıktısı olan çift yönlü bir süreç olarak ele almasıdır.

Bölüm Değerlendirmesi

Yaklaşık otuz yıllık geçmişe sahip ve yeni bir alan olarak karşımıza çıkan siber uzayın fiziki dünyada var olan birçok kavramı bu alan kapsamında dönüştürdüğü görülmektedir. Yüzyüze ilişkilerimizde de var olan güvenlik, istihbarat, saldırılar, gözetim, suç ve şeffaflık gibi kavramlar siber uzayla birlikte bu sanal uzama da aktarılmıştır. Siber uzayda bu kavramların çeşitlenip genişlemesi devletleri, özel şirketleri ve bireyleri de etkilemektedir. Genel olarak siber uzay devletlere ve özel şirketlere veri kontrolü, güvenlik, fayda-maliyet gibi konularda avantaj sunarken, bireylerin siber güvenlik, siber suç, siber gözetim, siber istihbarat ve siber saldırılara maruz kaldığı görülmektedir. Ayrıca devletler ve özel şirketler tarafından yapılan faaliyetlerin siber uzayda şeffaf olarak paylaşılmaması da özel hayatın ihlal edilmesine neden olmaktadır.

Özel hayatın tanımı konusunda uluslararası alanda henüz fikir birliği yoktur. Bu yüzden çok çeşitli tanımlarının yapıldığı görülmektedir. Çalışma kapsamında özel hayatın tanımı “yalnız bırakılma hakkı, kendine sınırlı erişim, gizlilik, kişisel bilgilerin kontrolü, kişilik ve yakınlık “samimiyet”” olarak ele alınmıştır. Özel hayatın önemi kapsamının da bu tanımlar çerçevesinde şekillendiği görülmektedir. Örneğin kişisel verilerin kontrolü tanımı, kişinin kendi bilgisi üzerinde kontrol sahibi olmasının

önemini vurgularken, gizlilik tanımı kişisel verilerin gizlenmesi, saklanması vurgu yapmaktadır.

Bireyler toplum içerisinde iki yönlü ilişkide bulunmaktadır. Bunlardan ilki, bireysel sınırların çizildiği bireyin özel alanının oluştururken, diğeri ise bireyin toplumla etkileşimde olduğu kamusal alanını oluşturmaktadır. Kamusal ve özel alanının sınırları da özellikle internet ve sosyal medya sitelerinin kullanılmasıyla birlikte bulanıklaşmış, bireyin özel alanı (bireyin bilgisinin rızası dışında paylaşılması, yayılması ve bu alana müdahale edilmesi) tartışılan bir konu haline gelmiştir. Ayrıca internetin yeni dijital kamusal alanlar oluşturmaya başladığı da bu tartışmalar içerisinde yerini almıştır.

Özel hayatın gizliliği hakkının birçok tanımı ve kapsamı olduğu gibi, kişisel veri ve kişisel verilerin korunması, konuta müdahale etmeme, ad ve şöhret hakkı ve yazışmalar'ın özel hayatın gizliliği hakkının boyutlarını oluşturduğu görülmektedir. Bu hakkın ayrıca bilgi iletişim teknolojilerinden etkilenmesinin insan hakları alanında yeni tartışmaları da beraberinde getirdiği gözlenmiştir. Bu bağlamda internete erişim hakkı, anonimlik hakkı ve unutulma hakkının çeşitli raporlarda ve direktifler de hak olarak tanımlandığı görülmektedir.

Son olarak özel hayatın gizliliğine yönelik teorik yaklaşımlar, doktrinde bu hakkın hangi açılardan ele alındığının görülmesi adına önem arz etmektedir. Bu kapsamda da özel hayatın gizliliği açısından çağdaş teorilerin özü kabul edilen Alan Westin'in "Özel Hayatın Gizliliği ve Özgürlük Teorisi" ve Irwin Altman'ın "Özel Hayatın Gizliliğini Düzenleme Teorisi" ele alınarak, iki teorinin özüne değinilmiş ve sonrasında bu iki teori arasındaki farklara yer verilmiştir.

İKİNCİ BÖLÜM:

2.ULUSLARARASI DÜZENLEMELERDE ÖZEL HAYATIN GİZLİLİĞİ HAKKI

Bu bölümde öncelikle özel hayatın gizliliği hakkının uluslararası hukuk bağlamında ilk defa tanımlanırken hangi aşamalardan geçip nihai halini aldığından bahsedilecektir. Ardından özel hayatın gizliliği hakkının hem uluslararası insan hakları sözleşmelerinde hem de bölgesel insan hakları sözleşmelerinde ne şekilde ele alındığı incelenecektir. Son olarak ise bu hakkın bölgesel siber güvenlik sözleşmelerinde hangi bağlam içerisinde ele alındığı gösterilecektir.

2.1. Birleşmiş Milletler Düzenlemelerinde Özel Hayatın Gizliliği Hakkı

Bu bölümde BM Sisteminde, EİHB hazırlanırken Özel Hayatın Gizliliği Hakkının tanımlanması görevli komisyonlar ve yazım sürecine bağlamında ele alınacaktır. Böylece özel hayatın gizliliği hakkının EİHB’de nihai halinin nasıl yazıldığı süreç içerisinde tanımlanmaya çalışılacaktır.

EİHB, 1946 ve 1948 yılları arasında iki yıllık bir süreçte hazırlandığı görülmektedir. BM Şartının 68. maddesinde, Ekonomik ve Sosyal Konsey (ESK) insan haklarının geliştirilmesi için komisyon kurmakla görevlendirilmiştir. Bu bağlamda da İnsan Hakları Komisyonu -İHK (Commission on Human Rights) 23 Ocak 1946 yılında kurulmuştur. Dokuz kişiden oluşan komisyonun üyeleri bir yıllığına komisyona seçilmişlerdir. Rene Cassin ve Roosevelt’in de görevli olduğu bu komisyonun görevi; uluslararası bir insan hakları beyannamesinin hazırlanması, sözleşmelerin hazırlanması ve dünya çapında insan haklarına uyulmasına izlemektir. Bunun yanı sıra devletlere, sivil toplum kuruluşlarına insan hakları ihlalleriyle ilgili forum sağlama görevi de bulunmaktadır. Ancak komisyonun insan hakları ihlallerini ele alma yetkisi bulunmamaktadır (İHK, t.y). Bu görevler doğrultusunda komisyonun, ESK’nın önerileri doğrultusunda çalışmalar yapması, öneriler sunması ve bilgi vermesi beklenmektedir. Ayrıca İnsan Hakları Komisyonu bünyesinde “Taslak Hazırlama Komitesi” (Commission on Human Rights Drafting Committee -Drafting Committee) kurulmuştur. Bu komitenin de İHK gibi çeşitli ülke temsilcilerinden oluştuğu görülmektedir. Komitenin amacı ise, önerilen maddelerin gözden geçirilmesi

ve birleştirilmesi olarak tanımlanmaktadır. Beyanname hazırlık aşamasında kurulan bir diğer grup ise “Çalışma Grubu (Working Group)”dur. İnsan Hakları Komisyonu Belçika delegesinin teklifiyle kurulmuştur. Çalışma grubunun amacı, Genel Kurul (General Assembly)’a rapor sunulması ve Genel Kurul’un da oturumlar esnasında ki önerilerine uygun göreceği kararları alabilmesi olarak karşımıza çıkmaktadır (Working Group Report, 1947, s. 2).

Winter, İHK’nin misyonunu, barış zamanında insan haklarına ve onuruna yönelik her saldırıyı püskürtmek ve BM Şartı ilkelerine göre tüm engelleri aşmaya yetecek kadar güçlü bir uluslararası insan hakları bildirgesi hazırlamak için savaş zamanında başlatılan halk mücadelesi olarak tanımlamaktadır (2013, s. 243). Milletler Cemiyetinin başarısız oluşu, iki dünya savaşı ve çeşitli anlaşmalarla sürdürülmeye çalışılan barış çabalarının, uluslararası hukuk yoluyla savaştan barışa geçme konusundaki başarısızlığı uluslararası arenada o dönemde açıkça görülmektedir. Aynı zamanda uluslararası ilişkilerde o dönem, devletin gücünün ve bunun için gerekli sınırların da yeniden düşünülmesi gereken bir dönemin başlangıcı olarak karşımıza çıkmaktadır. Böyle bir uluslararası ortamda bir yandan devletin egemenliğini sınırlandırma için uluslararası anlaşma hazırlamak, bir yandan da devletlerin buna taahhüt etmelerini sağlamak zorlu ve karmaşık bir süreç olarak görülmektedir. Bu yüzden de beyannamenin oluşturulma aşamasında devletlerin kavramlar üzerinde fikir ayrılıklarına düştüğü, ortak bir standart oluşturulmaya çalışılırken uzun tartışmaların yaşandığı göz ardı edilmemelidir.

Beyannamenin oluşturulması aşamasında, özel hayatın gizliliğine ilişkin bir hüküm getirilip getirilmeyeceği konusunda taraflarca herhangi bir tartışma yapılmamıştır (Diggelmann ve Cleis, 2014, s. 443). Bunun yanı sıra beyanname hazırlanırken “özel hayat” ve “özel hayatın gizliliği” kavramlarının kimi zaman birbirlerinin yerine kullanıldığı kimi zaman da farklı kavramlar olarak ele alındığı görülmektedir. Bu yüzden beyannamenin yazım sürecine değinirken “private life” kelimesi “özel hayat”, “privacy” terimi ise “özel hayatın gizliliği” olarak ele alınacaktır.

Beyanname taslağının hazırlanış sürecine bakıldığında, ilk oturumun Taslak Hazırlama Komitesi tarafından 9 Haziran- 25 Haziran 1947 tarihlerinde yapıldığını

görülmektedir. Komite öncesinde BM İnsan Hakları Direktörü John P. Humprey tarafından taslak bir metin hazırlanmış (secreteriat outline) ve komite bu metin üzerinden çalışmalarını sürdürmüştür. Humprey bu taslağı oluştururken sırasıyla, İnsan Hakları Komisyonu üyelerinin birinci oturumdaki gözlemleri, toplantı kayıtları; hükümetler tarafından İnsan Hakları Komisyonuna sunulan taslak uluslararası beyannameler veya öneriler (Şili, Küba, Panama, Hindistan ve Amerika Birleşik Devletleri'nden beş belge değerlendirilmiş; Fransa ve Birleşik Krallık'tan gelen teklifler çok geç geldiği için dahil edilmemiştir) ve ulusal anayasalardan⁷ yararlanmıştır (Schabas, 2013, s. Lxxxviii). Taslak bir metin hazırlanmasının nedeni komisyonun çalışmalarını kolaylaştırmak olarak karşımıza çıkmaktadır.

Özel hayatın gizliliğinin, birinci oturumda nasıl tanımlandığına geçmeden önce sekreteryaya tarafından hazırlanan taslak metine genel kurul karar taslağında ne şekilde yer verildiğini değinmek Kurul'un bakış açısını anlamamızı sağlayacaktır. Genel Kurul, "...konut dokunulmazlığı ve iletişimin gizliliğine saygı gösterilmediği sürece.... hakların güvence altına alınamayacağını" görüşünü ifade etmiştir (Drafting Committee, 1947a, s.27). Humprey tarafından oluşturulan taslak metin köklerini Amerika Birleşik Devletleri Anayasasının 4. değişikliğinden⁸ (The Fourth Amendment), ABD'nin Şili⁹ ve Panama'nın¹⁰ da taslak metinlerini gözden geçirerek hazırladığı¹¹ görülmektedir. İlgili madde şu şekilde taslak metinde yer almaktadır. "Hiç kimse keyfi aramalara veya el koymalara veya şahsına, meskenine, aile ilişkilerine, itibarına, özel hayatın gizliliğine, faaliyetlerine veya kişisel mülküne

⁷ Beyaz Rusya, Sovyetler Birliği, Ukrayna ve Yugoslavya'dan dört sosyalist anayasa da dahil olmak üzere yaklaşık on sekiz Avrupa anayasası değerlendirildi. Latin Amerika on sekiz anayasadan sorumluydu. Asya'dan (Afganistan, Çin, Hindistan, Filipinler ve Siam) sadece beşi, Orta Doğu'dan (İran, Irak, Lübnan, Suudi Arabistan ve Suriye) beşi daha vardı. Sadece dört Afrika anayasası dikkate alındı (Mısır, Etiyopya, Liberya ve Güney Afrika). (Schabas, 2013, s. Lxxxix).

⁸ "İnsanların, makul olmayan arama ve el koymalara karşı kişilerin, evlerinde, belgelerinde ve eşyalarında güvende olma hakkı ihlal edilmeyecektir"

⁹ Şili taslak metninde "aile ilişkileri özgürlüğü hakkı" na vurgu yapmıştır. "right to freedom of family relations,"

¹⁰ Panama Taslak metninde, Bir kişinin "kendisini evini, itibarını, mahremiyetini, faaliyetlerini ve mülkünü" kapsayan "yanlış müdahaleden kurtulmak" şeklinde tanımlamıştır. ("to freedom from wrongful interference" that covered a person's "person, home, reputation, privacy, activities, and property")

¹¹ "Hiç kimse keyfi veya yetkisiz olarak kişiyi, evi, evrakları ve eşyaları üzerinde aranamaz veya şahsına, meskenine, ailesine, başkalarıyla olan ilişkilerine, itibarına, mahremiyetine, faaliyetlerine veya mülküne makul olmayan müdahalelere tabi tutulamaz. Yazışmaların gizliliğine saygı gösterilecektir."

makul olmayan müdahalelere tabi tutulamaz. Yazışmaların gizliliğine saygı gösterilecektir” (Drafting Committee, 1947b, s.4).

Bu bağlamda Genel Kurul özel hayatın gizliliğini “konut dokunulmazlığı” ve “iletişimin gizliliği” ile sınırlandırırken, Sekreteryaya tarafından hazırlanan metinde özel hayatın gizliliği “konut”, “aile” ve “itibar” çerçevesinde tanımlandığı görülmektedir. Cassin ise bu belgetyi daha sonra revize etmiş ve Sekreteriat Outline belgesinde iki önemli değişiklik yapmıştır. Bunlardan ilkinde yapılan değişiklikte ilgili madde “özel hayat” kavramı çerçevesinde ele alınmıştır. “Özel hayat, konut, iletişim ve itibar dokunulmazdır ve kanunla korunmaktadır” (Drafting Committee, 1974a, s.53) Cassin’in önerdiği ikinci değişiklikte ise karşımıza “özel hayatın gizliliği” kavramı çıkmaktadır. “Konutun ve iletişimin mahremiyeti ve itibara saygı kanunla korunur.” (Drafting Committee, 1974a, s.75).

Cassin’in birinci taslağı çerçevesinde, Birleşik Krallık ilkeye katıldığını ancak “konut dokunulmazlığına” ve “yazışmaların mahremine” dokunulmazlık (inviolable) kelimesini değil “saygı gösterileceği” şeklinde ifade edilebileceği önerisini getirmiştir. Fransa ise, maddenin “özel hayatın dokunulmazlığı kanunla gözetilir ve düzenlenir” şeklinde değiştirilebileceğini dile getirirken, Avusturya, “"Konut ve yazışmaların mahremiyeti ve itibara saygı, kanunla korunmalıdır." önerisini getirmiştir. Ancak Birleşik Krallık, “hukuk tarafından korunur” ibaresi yerine “saygı duyulur” kelimesini tercih ettiğini belirtmiştir (Diggelmann ve Cleis, 2014, s. 445; Morsink, 1990, s. 135-136). Bu tartışmaların bir sonucu olarak ve Humphrey’nin hazırladığı metinde "dokunulmazlık" terimi yer almadığından dolayı, Taslak Komitesi Birinci Oturumunda "Konutun mahremiyeti, iletişim ve itibara saygı kanunla korunur" şeklinde kabul edildiği görülmektedir (Drafting Committee, 1974a, s.75).

Taslak Komitesinin çalışmasını tamamlamasının ardından “Çalışma Grubu” son taslak üzerinde çalışmaya başlamıştır. Taslak Komitesi'nin önerilerinden yola çıkarak ve Panama tarafından yapılan bir öneriyi¹² dâhil ederek, özel hayatın gizliliği ile ilgili hüküm yeniden düzenlenmiştir. Bundan sonraki tartışmalar “kişi, konut ve belge

¹² "Makul olmayan müdahaleye karşı özgürlük şahsı, evi, itibarı, mahremiyeti, faaliyetleri ve mülkiyeti ile herkesin hakkıdır. Devlet bu özgürlüğü korumakla yükümlüdür" <https://digitallibrary.un.org/record/631107>, 26 April 1946, E/HR/3.

(iletiřim) konuları üzerine odaklanmıřtır. Kiřisel mülkiyet kavramı beyanname taslağında 17. maddede yer aldığı için çıkartılmıřtır. Aynı řekilde bireyin řahsi dokunulmazlığı da 3. maddeyle örtüřtüğü için özel hayatın gizliliğı “bireyin özgürlüğü üzerinden değıl, konutun özgürlüğü üzerine tartıřılmaya bařlanmıř (Morsink, 1990, s. 136) ve řu řekilde kabul edilmiřtir: “Herkes, itibarına, özel hayatına ve ailesine makul olmayan müdahalelerden kanunen korunma hakkına sahiptir. Evi ve yazıřmaları dokunulmazdır”(Working Group Report, 1947, s.8).

İnsan Hakları Komisyonu bu formdaki ön taslağı 1947 sonlarında ESK'ya sunmuřtur. Eř zamanlı olarak ise üye devletlerden ESK'ya sunulan taslak metnin üzerinde çalıřma yapılması istenmiřtir. Üye devletlerin yine daha önceki oturumlarda olduğı gibi “dokunulmazlık” ibaresine karřı çıktığı görölmektedir. Bunun nedeni, dokunulmazlığın mutlak olmadığını ve istisnaların belirtilmesi gerektiğinin üzerinde durulmasıdır (Morsink, 1990, s.136-137). Bu bağlamda Taslak Komitesi, Üye Devletlerin yorumlarını değılendirmiş ve ardından, "özel hayat" veya "özel hayatın gizliliğı" kelimelerinin tamamen kaldırıldığı bir taslak önerdiği görölmektedir: “Herkesin, itibara, aileye, meskene veya yazıřmaya makul olmayan müdahalelere karřı kanunen korunma hakkı vardır” (Drafting Committee, 1948, s.7) .

Komisyonun üçüncü oturumunda ise bir önceki oturumda kabul edilen metinde yer alan “kanunen korunma” ibaresi üzerine müzakerelerde bulunulmuřtur. Kanunen korunma ibaresinin metinde yer almasına gerek olmadığı, bunun zaten öncelikle devlet mekanizmanın görevi olduğı tartıřılmış ve sonrasında bu ibare taslaktan çıkartılmıřtır (Morsink, 1990, s. 137). Üçüncü oturumun en temel değıřikliğinin İnsan Hakları Komisyonu tarafından “Taslak Komitesinin” raporunu değılendirirken yaptığı görölmektedir. Bir önceki oturumda ilgili maddeden çıkartılan “özel hayatın gizliliğı” ibaresi yeniden gündeme alınmış ve taslak beyannamenin 10. maddesinin en bařına getirilmiřtir. Sonrasında ise Çin'in önerisi kabul edilerek öncelikle Ekonomik ve Sosyal Konsey'e daha sonrasında ise Genel Kurul'a sunulmuřtur (Diggelman ve Cleis, 2015, s. 447). Genel Kurul'un ilgili madde üzerinde iki değıřiklik yaptığı görölmektedir. Bunlardan ilki “makul olmayan” ibaresinin ilgili maddeden çıkartılması, ikincisi ise makul olmayan ibaresinin yerine “keyfi” ibaresinin getirilmesidir. Uzun süren müzakerelerin ardından ise Genel Kurul'un önerisi" řu

şekilde değiştirilmiş ve nihai halini almıştır. “Hiç kimse özel hayatına, ailesine, evine veya yazışmalarına keyfî müdahaleye, şeref ve itibarına yönelik saldırılara maruz bırakılamaz. Herkes, bu tür müdahale veya saldırılara karşı kanunun korumasından yararlanma hakkına sahiptir” (General Assembly,1948, s.4).

BM sisteminde özel hayatın gizliliği hükmünün son halini almadan önce hangi aşamalardan geçtiği, genel hatlarıyla itiraz edilen yönleri bu hakkın ne şekilde tanımlandığının bilinmesi açısından önem arz etmektedir. Genel çerçeve içerisinde bu sürece bakarsak özel hayatın gizliliği hakkının EİHB hazırlanmadan önce devletlerin anayasasında yer almadığı görülmektedir. Bu yüzden özel hayatın gizliliği öncelikle uluslararası hukuk çerçevesinde tanımlanmış, daha sonra devletlerin anayasaların da yer almıştır denilebilmektedir. Özel hayatın gizliliği sadece belirli eyaletlerde “konut ve iletişim” çerçevesinde tanımlandığı ve dolayısıyla ilgili madde nihai halini almadan önce tartışmaların ve tanımların konut, aile ve iletişim çerçevesinde yapıldığı görülmektedir.

Bir diğer değinilmesi gereken husus da özel hayatın gizliliği kavramının tam olarak tanımlanmamasından ileri gelmektedir. Aslında bu sorun günümüzde de hala devam etmektedir. Kavramın geniş olması birden çok unsuru bünyesinde barındırması (konut, aile, iletişim vb) değişen koşullar altında ve somut olaylar çerçevesinde yorumlanabilmesini sağlamak nedeniyle literatürde hiçbir zaman tek bir tanım yapılamadığı dile getirilmektedir (Gözübüyük ve Gölcüklü, 2011, s. 330). Ayrıca hem genel tanım eksikliği hem de beyanname yazılırken İngilizce ve Fransızca dillerinin bir arada kullanılması, temelde metin üzerinde asıl vurgulanmak istenen ifadelerin verilememesine neden olduğu vurgulanmaktadır. Özellikle Cassin'in Fransızca taslaklarının İngilizce'ye yeniden çevrilmesi, 'aslında olduğundan çok daha uzak' görünen bir metnin üretilmesine neden olduğu ifade edilmektedir (Diggelmann ve Cleis, 2014, s. 448). Özel hayat, özel hayatın gizliliği ve bazen de gizlilik (secrecy) kelimelerinin ilgili maddede yer alması, çıkarılması ve ne şekilde ifade edilmesi gerektiği tartışmalarının kökeninde de bu iki dilin kullanılmasının neden olduğu görülmektedir. Beyanname maddeleri oluşturulurken özün bir başka deyişle asıl dile getirilmek istenen kavramın tam olarak karşılığı aranırken “kelimeler” üzerinde birçok tartışma yapıldığı gözlemlenmektedir. Bu da kültürlerarası ortak bir payda bulmanın

dil üzerinde nasıl etkili olduđu ve zorluđunu bizlere göstermektedir. Tüm bunlara rağmen, EİHB sayesinde “şemsiye” bir kavram olarak özel hayatın gizliliđi tanımı yapılmış, daha sonra bu tanımdan yola çıkarak gerek anayasaların gerekse yeni uluslararası belgelerin oluşturulduđu görölmektedir.

2.1.1. Evrensel İnsan Hakları Beyannamesi

Evrensel İnsan Hakları Beyannamesi (Universal Declaration of Human Rights) 10 Aralık 1948 tarihinde 217 A(III) sayılı kararla Pariste toplanan Genel Kurulda sadece sekiz ülkenin çekimser kalmasına karşın kırksekiz ülkenin kabul etmesiyle ilan edilmiştir. Uluslararası anlamda insan haklarını ilk düzenleyen belge olması açısından bu belge diđer belgelere emsal teşkil etmektedir. Türkiye’de 6 Nisan 1949 yılında Bakanlar Kurulu kararıyla bu belgeyi onaylamış ve beyanname 27 Mayıs 1949 yılında yürürlüğe girmiştir. Beyannameye baktığımızda 30 maddeden oluştuđunu görmekteyiz. 1-21. madde temel haklara değinirken, 22-27 arasındaki maddelerde “Sosyal Ekonomik ve Kültürel Haklara” yer verilmektedir. Beyannamenin 12. maddesinde ise “özel hayatın gizliliđi hakkı” düzenlemiştir. İlgili madde beyannameye şu şekilde yer almaktadır: “Hiç kimse, özel yaşamına, ailesine, konutuna ya da haberleşmesine yönelik keyfi müdahalelere ya da onur ve şöhretine yönelik saldırılara maruz bırakılmayacaktır. Herkesin, bu tür müdahale ya da saldırılara karşı yasa ile korunma hakkı vardır”.

Beyanname, hukuki açıdan bağlayıcı olmayan bir belge olarak karşımıza çıkmaktadır. Bu bakımdan, imzalayan veya onaylayan devletler için evrensel bir ahlak kodu olarak tanımlanabilmektedir (Erdoğan, 2011, s.132).

EİHB’de tanımlanan, özel hayatın gizliliđi hakkı birinci kuşak haklar kategorisinde “kişi” hakkı olarak yer almaktadır. Bir başka deyişle, özel hayatın gizliliđi hakkı, 1789 yılında gerçekleşen Fransız Devrimi’nden sonra kişi hak ve özgürlüklerini öngören birinci kategoriye dahil edilmiştir (Şen, 1989, s. 117). Bu hakkın birinci kategoriye dahil edilmesinin nedeni hakların birbirleriyle olan bağlantısıdır. Diđer haklardan yararlanabilmek için öncelikle bu hakkın korunması gerekmektedir.

Özel hayın gizliğı hakkına baktığımızda, ilk satırında hakkın negatif statüsü görölmektedir. Negatif haklar söyleminde, devlet iktidarı üzerindeki yasal ve anayasal kısıtlamalarla garanti edilen devlet müdahalesine ve düzenlemesine karşı, doğal kendi çıkarlarını sürdürme özgürlüğünün korunması amaçlanmaktadır (Karppinen ve Puukko; 2020, s.314). Bir başka deyişle hakkın gerçekleştirilmesi için devletin herhangi bir müdahalesi olmaması anlamına gelmektedir.

İlgili maddenin birinci cümlesine baktığımızda kişinin iletişiminden kişiye müdahaleye ve saldırıya kadar geniş bir kapsam içerisinde ele alındığı görölmektedir. Kişinin özel hayatı, ailesi, meskeni ve iletişim çerçevesinde tanımlanmış ve bu alanlara karşı keyfi müdahale ve kişinin onur ve şöhretine saldırıda bulunulamayacağı dile getirilmiştir. Bireyin özgürlüğü de bu bağlamda korunmaktadır.

İlgili maddenin ikinci satırında da “kanun ile korunma” ibaresi bulunduğundan aynı zamanda devlete pozitif yükümlölük yüklediğı (Üzeltürk, 2004, s. 66) de belirtilmektedir. Devlet, bu hakkın korunması için ve elverişli koşulların sağlanması için birincil sorumluluğına sahip olarak karşımıza çıkmaktadır.

Yirminci yüzyılın benzersiz siyasi projesi (Waltz, 2002 s. 438) olarak adlandırılan EİHB, insan haklarının savunulmasında hem ulusal hem de evrensel bir standardın getirilmesini amaçlamıştır. Belge insan haklarının devletlerarasında sınırlı bir şey olarak değil, bireylerin birbiriyle ve kendi çıkarları için oluşturdukları gruplarla ilişkilerini tanımlamıştır (Winter, 2013, s.250). EİHB insan haklarının yapı taşı olarak karşımıza çıkmaktadır. Bu beyanname sayesinde devletler ilk defa özgürlük, eşitlik ve haklarını savunan bir belge üzerinde uzlaşmışlardır. Ayrıca bu beyanname ile birçok uluslararası anlaşma hazırlanmış ve temel olarak ele alınmıştır. Bu belgelerden bir diğeri ikiz sözleşmelerden biri olan BM Sivil ve Siyasal Haklar Konvansiyonu’dur.

2.1.2. Sivil ve Siyasal Haklar Konvansiyonu

EİHB’nin kabul edilmesinden sonra, beyannamede yer alan hakların hukuki bağlayıcılık kazandırılmasına yönelik çalışmalar yapılmış, temel hak ve özgürlükler ihlal edildiğinde ise bunu belirleyecek bir mekanizma ve yaptırım sistemine ihtiyaç duyulmuştur (Erdoğan, 2011, s. 132). İnsan Hakları Komisyonu, EİHB’ye paralel olarak bir sözleşme yazımına 1947 yılında başlamış 1950 yılında tamamladığı

sözleşmeyi Genel Kurul'a sunmuştur. Sözleşme nihai halini 16 Kasım 1966 yılında olarak, 2200 A(XXI) sayılı karar ile imzaya açılmıştır. Sivil ve Siyasal Haklar Konvansiyonu (SSHK) 35 ülkenin onaylaması sonucu 23 Mart 1976 tarihinde yürürlüğe girmiştir.

SSHK'ye genel olarak baktığımızda giriş bölümünde EİHB'ne ve BM Şartına atıfta bulunduğunu görülmektedir. EİHB'de tanımlanan Medeni ve Sosyal Haklar'ın, SSHK'de daha ayrıntılı olarak tanımlandığı görülmektedir. Ayrıca bu konvansiyonun EİHB'nin aksine bağlayıcılığı¹³ bulunmaktadır. Özel hayatın gizliliği hakkına sözleşmede 17. Madde de yer verilmiştir. İlgili madde; "1. Hiç kimsenin özel hayatına, ailesine, evine ya da haberleşmesine keyfi ya da yasadışı olarak müdahale edilemez; hiç kimsenin şeref ve itibarına yasal olmayan tecavüzlerde bulunulamaz. 2- Herkesin, bu gibi müdahalelere ya da tecavüzlere karşı yasalarca korunma hakkı vardır" (SSHK, 1976).

İlgili maddeye bakıldığında EİHB'deki tanımla paralellik gösterdiği, ancak hakkın daha kapsamlı olarak ele alındığı görülmektedir. İki madde arasındaki fark, SSHK'nin 17. maddesinin yalnızca kişinin özel yaşamına ve özel alanına daha spesifik yönlerine 'keyfi' müdahaleleri yasaklamakla kalmayıp, aynı zamanda 'yasadışı' olanların da bu kapsama eklenmesi olarak karşımıza çıkmaktadır (Diggelman ve Cleis, 2014, s. 449).

Sözleşmede özel hayatın gizliliği hakkı mutlak bir hak olarak tanımlanmamıştır. Mutlak hak¹⁴ tanımı şu açıdan önemlidir. Sözleşme içerisinde mutlak hak olarak tanımlanan haklar herhangi bir sınırlamaya tabi olmadan gerçekleştirilebilmektedir. Ancak mutlak olmayan haklar ulusal güvenlik, kamu düzenini sağlamak ve ayrıca başkalarının hak ve özgürlüklerini korumak adına sınırlandırılabilir.

¹³ Sözleşmenin bağlayıcılığı 2. Madde kapsamında tanımlanmıştır. Buna göre; "Mevcut mevzuatta ve diğer yasal tedbirlerde henüz düzenleme bulunmayan durumlarda, bu Sözleşme'ye Taraf her Devlet, kendi anayasal kurallarına ve bu Sözleşme'nin hükümlerine uygun olarak, bu Sözleşme'de tanınan hakların uygulanmasını sağlamak bakımından gerekli olan yasama ve diğer tedbirleri almakla yükümlüdür."

¹⁴ Mutlak hak olarak tanımlanan haklar; yaşam hakkı, işkence, zalimane ve insanlık dışı veya aşağılayıcı muamele veya ceza yasağı, kölelik ve zorla çalıştırma yasağı, borç nedeniyle hapis yasağı, kanunsuz suç ve ceza olmaz ilkesi, kişi olarak tanınma hakkı ve düşünce, vicdan ve din hürriyeti olarak belirlenmiştir.

belirtilmektedir. Özel hayatın gizliliği hakkı bağlamında, ulusal güvenlik gibi nedenlerle bazı durumlarda devletlerin bu hakkı aşmasına başka bir deyişle müdahale etmesine izin verilmektedir. Devletin müdahalesi, bu tür kısıtlamaların yasada öngörüldüğü anlamda “hukuki” olması ve izin verilen müdahalenin kapsamıyla orantılı olması bakımından “keyfi olmaması” anlamına gelmektedir. Dolayısıyla mesele, devletlerin kendi vatandaşlarını korumak için 17. maddeyi göz ardı etmesi değil, daha çok, gayri meşru koşullar altında göz ardı edilen özel hayatın korumasının nasıl uygulanacağın vurgusudur (Barbaro, 2017, s. 143).

1988 yılında BM İnsan Hakları Komiserliği tarafından SSHK Madde 17’ye ilişkin Genel Yorum No 16’da daha da geliştirilmiştir. 16 no’lu yorumun teknolojik gelişmelerin bir sonucu olarak yayımlanıp kabul edildiği görülmektedir. Bağlayıcı özelliği olmayan genel yorum belgesinde özel hayatın gizliliğinin bir unsuru olan kişisel verilerin korunmasına yer verilmektedir. İlgili madde aşağıda yer almaktadır:

İster kamu makamları ister özel kişi veya kurumlar tarafından olsun, kişisel bilgilerin bilgisayarlarda, veri bankalarında ve diğer cihazlarda toplanması ve tutulması kanunla düzenlenmelidir. Devletler, bir kişinin özel hayatına ilişkin bilgilerin, bu bilgileri almaya, işlemeye ve kullanmaya kanunen yetkili olmayan kişilerin eline geçmemesini ve asla Sözleşme ile bağdaşmayan amaçlar için kullanılmamasını sağlamak için etkili tedbirler almalıdır. Özel hayatının en etkili şekilde korunabilmesi için her birey, otomatik veri dosyalarında hangi kişisel verilerin saklanıp saklanmadığını ve saklanıyorsa hangi amaçlarla saklandığını anlaşılabilir bir biçimde öğrenme hakkına sahip olmalıdır. Her birey aynı zamanda dosyalarını hangi kamu makamlarının veya özel kişi ya da kurumların kontrol ettiğini veya edebileceğini de öğrenebilmelidir. Bu tür dosyalar yanlış kişisel veriler içeriyorsa veya kanun hükümlerine aykırı olarak toplanmış veya işlenmişse, her birey düzeltme veya silme talebinde bulunma hakkına sahip olmalıdır (UN Human Rights Committee, 1988, 10. paragraf).

İlgili madde ile birlikte devletlere kişisel verileri koruma hakkı kapsamında pozitif yükümlülük getirildiği görülmektedir. Ayrıca devletlerin kişisel verileri yetkisiz olarak ele geçirme ve kullanılmasını önlemek amacıyla etkili tedbirler

alınması gerektiğini vurgulamaktadır. Bir başka vurgulanan kavram ise siber şeffaflık ve hesap verilebilirlik ilkesi olarak karşımıza çıkmaktadır. Böylece bireyin kişisel bilgileri üzerinde kontrol yetkisine sahip olması amaçlanmaktadır.

EİHB ve SSHK'nin temel uluslararası insan hakları belgeleri olarak karşımıza çıkmaktadır. Ancak belgeler yasal statüleri ve kapsamı bakımından farklılık göstermektedir. EİHB siyasi, sosyal, sivil, ekonomik ve kültürel hakları içeren geniş kapsamlı bir belge olarak karşımıza çıkarken, SSHK'nin sivil ve sosyal haklar gibi daha kısıtlı hak grubunu ele aldığı görülmektedir. Ayrıca EİHB bağlayıcı olmadan evrensel etik standartları ortaya koyarken, SSHK ise devletlere yasal olarak bağlayıcı yükümlülükler sunduğu görülmektedir.

2.2. Avrupa Konseyi Düzenlemelerinde Özel Hayatın Gizliliği Hakkı

Avrupa nezdinde insan haklarının benimsenmesi Avrupa Konseyi'nin kurulması ile başlamıştır. Avrupa Konseyi kurulmadan önce devletlerin iç işi olarak benimsenen insan hakları anlayışı, Konseyin kurulmasıyla birlikte devlet sınırlarını aşmıştır. Avrupa'nın bütünleşmesi fikri yüzyıllar öncesine dayansa¹⁵ da savaşlar arası dönemde, Avrupa siyasi federasyonunu teşvik etme girişimleri, hâlâ güçlü olan Avrupa milliyetçiliği tarafından engellenmiştir (Weil, 1963, s. 804). İkinci Dünya Savaşı sonrası Avrupa'da oluşan iki ayrı blok da Avrupa'nın bütünleşmesi önünde önemli bir engel teşkil etmemiştir. 19 Eylül 1946 yılında Winston Churchill'in "Avrupa Devletler Birliği"nin oluşturulması gerektiğini söyleyen konuşması Avrupa bütünleşmesinin temel adımı olarak görülmektedir (Akdemir, 2014, s. 45-46).

Churchill'in bu fikrini somutlaştıran adım ise 7-10 Mayıs 1948 tarihleri arasında gerçekleştirilen Lahey'de düzenlenen Avrupa Kongresi olmuştur. Kongreye 16 ülkeden¹⁶ 713 delege, diğer on ülkeden ise gözlemciler katılmıştır. İki gün süren kongrenin amacı, Avrupa Birliği fikrine geniş desteği göstermek, harekete yeni bir

¹⁵ La Rochefoucauld, Saint Simon, Due de Sully, Emile de Girardin, Agustin Thierry, William Penn, Victor Hugo, De Gasperi gibi düşünürler Avrupa'da bir birlik kurulmasına inanmışlardır (Karluk Rıdvan, Avrupa Birliği ve Türkiye, İstanbul, Beta Yayınları, 2007, s. 1).

¹⁶ Temsil edilen ülkeler Avusturya (12), Belçika (18), İngiltere (140), Danimarka (32), İrlanda (5), Fransa (185), Almanya (51), Yunanistan (18), İtalya (57), Lihtenştayn (3), Lüksemburg (8), Hollanda (59), Norveç (12) Saar (5), İsveç (19), İsviçre (39). Ayrıca Bulgaristan, Kanada, Çekoslovakya, Finlandiya, Macaristan, Polonya, Romanya, İspanya, ABD ve Yugoslavya'dan bazıları mülteci veya sürgün olan elli kadar gözlemci bulunmaktadır.

ivme kazandırmak ve birlik fikrinin hedeflerine ulaşması için pratik önerilerde bulunmak olmuştur (Robertson, 1965, s. 24). Churchill yaptığı açılış konuşmasında insan hakları bağlamında şunları dile getirmiştir;“Avrupa Birliği hareketi, gücünü ortak manevi değerlerimizden alan olumlu bir güç olmalıdır. Ahlaki kavramlara dayanan ve bir misyon duygusundan ilham alan demokratik inancın dinamik bir ifadesidir. Hareketimizin merkezinde, özgürlükle korunan ve yasalarla desteklenen bir İnsan Hakları Sözleşmesi fikri yer almaktadır” (Bates,2010, s. 47).

Bu bağlamda Churchill’in açılış konuşmasında insan haklarını merkeze koyduğu görülmektedir. Simpson’a göre ise; böyle bir konuşmanın amacı, Batı’ya özgürlüğü geri getirmek değil, amaç zaten var olanı totaliter tehditten korumak, yani muhafaza etmektir (Simpson, 2004, s. 605).

Hague kongresinin gerçekleştirildiği döneme bakıldığında ise insan haklarının kesin bir çerçevesinin çizilmemiş olduğu bilinmektedir. Bu durum, Birleşmiş Milletler İnsan Hakları Komisyonu tarafından kurulan taslak hazırlama komitesi toplantısını henüz yapılmamış olmasından ve Komisyonun da aynı ay içerisinde toplanmamasından görülmektedir (Simpson, 2004, s. 605). Bu duruma aciliyet kazandıran gelişme olarak 1940’ların sonlarında, Birleşmiş Milletler EİHB oluşturma çabalarına ve bu çabalarda karşılaşılan zorluklara işaret edilebilmektedir. Bu dönemde daha iyi bir örnek oluşturmak ve etkili bir bölgesel insan hakları garantisi bulmak için Avrupalılara çevrildiği görülmektedir (Bates, 2010, s. 6).

Avrupa neden böyle bir oluşuma ihtiyaç duymuştu? Avrupa’nın böyle bir oluşuma ihtiyaç duymasının en büyük nedeni 1940’ların sonlarında tek tek sosyalist devletlerin kurulması olarak görülmektedir (Bates, 2010, s.5). Ayrıca, Batı Almanya’nın o dönemlerde, yakın zamanda topluluğa katılması beklentisi ve kabul için belirli şartların oluşturulmasının öncelik kazandığı görülmektedir. Bu topluluk sayesinde böylece kurallar belirlenecek ve ülkeler bu ilkeleri kabul ederek yüzlerini tekrar demokrasiye dönmüş olacaktı. Bir başka etken ise, her Avrupa ülkesinde insan haklarının korunması ve bu bağlamda da demokrasinin güvence altına alınmasıydı. Çünkü demokrasi birleşik Avrupa için olmazsa olmaz bir koşul olarak ön plana çıkmaktaydı (Weil, 1963, s.804).

Kongre boyunca özgürlüğün temel olduğu, Avrupa’da barışın tahsis edilebileceği, devletlerin egemenliği doktrinin Nazi Almanyası’nda olduğu gibi bireysel özgürlükleri engelleyebileceği ve dolayısıyla insan haklarının gerekli ve uluslararası boyutta garanti altına alınabileceği dile getirilmiştir (Weil, 1963, s. 804-805). Kongrenin bir diğer özelliği ise kongre sonunda “Message to Europeans” başlığı altında kongre delegeleri tarafından hazırlanan metindir. Metne göre (Aktaran: Robertson, 1965) aşağıdaki hükümler kabul edilmiştir;

- Alanında kişilerin, fikirlerin ve malların serbest dolaşımının yeniden sağlandığı birleşik bir Avrupa arzu ediyoruz;
- Düşünce, toplanma ve ifade özgürlüğünün yanı sıra siyasi muhalefet oluşturma hakkını güvence altına alan bir İnsan Hakları Beyannamesi istiyoruz;
- Bu Şartın uygulanması için yeterli yaptırımlara sahip bir Adalet Divanı istiyoruz;
- Bütün milletlerimizin güçlerinin temsil edileceği bir Avrupa Meclisi arzu ediyoruz;
- Evimizde ve kamuoyunda, siyasi ve dini hayatımızda, meslek ve sendika çevremizde, barışın ve barışın son şansını sunan bu yüce dava için çalışan tüm kişi ve hükümetlere tam desteğimizi vermeye söz veriyoruz (s.25).

Yukarıda sayılan maddeler çerçevesinde Kongre sonunda iki temel öneri kabul edilmiştir. Bunlardan ilki, üyeleri parlamentolar tarafından seçilecek olan Avrupa Parlamenter Meclisini kurmaktır. Yasama ve yürütme yetkili olmayan meclisin işlevi ise, Avrupa Federasyonu için plan üretmeye yönelik adımları atması olarak tanımlanmıştır (Simpson, 2004, s.607). Bir diğer öneri ise, Meclisin Avrupa İnsan Hakları şartı oluşturması gerektiği idi. Her üye devletin dışişleri bakanından oluşan Bakanlar Komitesi ve her üye devlette hem hükümet hem de muhalefet partilerinin parlamenterlerinden oluşan Danışma Meclisi¹⁷, Sözleşme'nin hazırlanmasında yer alan organlar olarak görev yapacaktı (Weil, 1963, s. 805). Bu bağlamda uluslararası bir yargı bölümü kurularak bu bölümün başına Pierre-Henri Teitgen,¹⁸ getirilmiştir. Sir

¹⁷ Danışma Meclisi üye devletlerin ulusal parlamentolarının temsilcilerinden oluşmaktadır.

¹⁸ Fransada 1945-1946 yılları arasında Adalet Bakanlığı yapmıştır.

David Maxwell-Fyfe,¹⁹ ve Fernand Dehousse,²⁰ ise raportör olarak görev aldığı görülmektedir. Temmuz 1949'da Avrupa Hareketi, basitçe "Avrupa İnsan Hakları Sözleşmesi" başlıklı yayın çıkarılmış ve Avrupa Konseyi Bakanlarına gönderilmiştir. Belge, "Avrupa İnsan Hakları Sözleşmesi" taslağının yanısıra, Avrupa İnsan Hakları Mahkemesi için de bir Tüzük Taslağı içermektedir (Bates, 2010, s. 51-52). Kongre sonuçları, Belçika ve Fransız dışişleri bakanları tarafından yeni oluşturulan Brüksel Antlaşması Örgütü Danışma Konseyi'ne sunulmuş ve 5 Mayıs 1949'da Avrupa Konseyi Statüsü imzalanmıştır²¹ (Robertson, 1965, s. 25). Böylece Avrupa İnsan Hakları sözleşmesinin temelleri de resmi olarak atılmış ve bu bağlamda da insan haklarının bölgesel olarak korunması Avrupa Konseyi çerçevesine yerleştirilmiştir.

2.2.1. Avrupa İnsan Hakları Sözleşmesi

1950 yılında imzalanan ve 1953 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesinin (AİHS), sözleşmedeki haliyle tam adı “İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme”dir. Sözleşmeye genel olarak bakıldığında sözleşmenin temel olarak üç kaynaktan esinlendiği görülmektedir: İHEB, Avrupa Hareketi Uluslararası Komitesi'nin tavsiyeleri ve söz konusu hareketin Uluslararası Yargı Bölümü tarafından hazırlanan AİHS taslağıdır (Westlund, 2018, s. 12). Sözleşmenin başlangıç kısmına bakıldığında EİHB'ne atıfta bulunduğu görülmektedir. Evrensel Beyanname aynı zamanda bölgesel kuruluşlar tarafından uluslararası standartların yetkili beyanı olarak görülmektedir. Kasım 1950'de kabul edilen Avrupa İnsan Hakları Sözleşmesi, önsözünde²² Bildirge'nin önemini kabul etmektedir (Schabas, s. cxiv). Sözleşmenin bir diğer gözümüze çarpan hususu ise EİHB'nin aksine, AİHS'de SSHK gibi sadece medeni ve siyasi hakları kapsadığı, ekonomik ve sosyal hakların yer almadığı görülmektedir.

¹⁹ İngiliz politikacı ve avukat.

²⁰ Belçika temsilcisi.

²¹İmzalayan ülkeler; Belçika, Danimarka, Fransa, İrlanda, İtalya, Lüksemburg, Hollanda, Norveç, İsveç ve Birleşik Krallıktır.

²² “Aşağıda imzası bulunan Avrupa Konseyi üyesi hükümetler, Birleşmiş Milletler Genel Kurulu tarafından 10 Aralık 1948'de ilan edilen İnsan Hakları Evrensel Bildirisi'ni, bu bildirinin, açıkladığı hakların evrensel ve etkin olarak tanınmalarını ve uygulanmalarını sağlamayı hedef aldığını, ...Evrensel Bildiri'de yer alan bazı hakların ortak güvenceye bağlanmasını sağlama yolunda ilk adımları atmaya kararlı olarak, ... aşağıdaki konularda anlaşmışlardır”(https://www.echr.coe.int/documents/convention_tur.pdf)

Sözleşmenin bir diğer önemi ise, uluslararası hukuk açısından önemli bir dönüm noktası olmasıdır. Sözleşme bağlamında oluşturulan insan hakları koruma mekanizması sayesinde, devletlerin insan haklarına karşı yükümlülükleri denetlenmektedir. Bu bağlamda sözleşme ile üye devletlerin yalnızca insan haklarını koruma yükümlülüklerini kabul etmelerini değil, aynı zamanda bireylerin uluslararası hukuk uyarınca hakları olduğunu kabul etmelerini de güvence altına alınmaktadır (Naankiel, 2014, s. 8). Bu çerçevede öncelikle 1954 yılında Avrupa İnsan Hakları Komisyonu ve 1959 yılında Avrupa İnsan Hakları Mahkemesi kurulmuştur.

Sözleşmeyi genel çerçevede tanımladıktan sonra, özel hayatın gizliliği bağlamında bakacak olursak, AİHS’de, özel hayatın gizliliği hakkı 8. madde içerisinde “Özel ve Aile Hayatına Saygı Hakkı” başlığı altında düzenlenmiştir. İlgili madde;

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir (AİHS, 1950, s.10-11).

Birleşmiş Milletler Sisteminde özel hayatın gizliliği hakkı “privacy” terimi ile tanımlanırken, Avrupa Konseyi bünyesinde “private life” (özel hayat) olarak tanımlanmıştır. Özel hayat (private life) ve özel hayatın gizliliği (privacy) terimlerinin “şemsiye” bir terim olarak komisyon tarafından tartışılıp tartışılmadığı da tutanaklarda belirtilmemiştir (Diggelmann ve Cleis, 2014, s. 457). Westlund’a göre, sözleşme taslağı hazırlanırken Fransızcanın öne çıkması ve sadece Fransızcada yer alan “vie privée” kelimesinin bir çevirisi olarak özel hayat kavramının kullanılmış olabileceği fikri öne sürülmektedir (2018, s. 25). Her ne kadar bu terimler arasında farklılık bulunsa da AİHS’de özel hayat kavramı “özel hayatın gizliliği” olarak yorumlanmalıdır.

8. madde kapsamında yer alan bir diğer değişiklik ise EİHB’de yer alan “kişinin şeref ve itibarı” kelimelerinin kaldırıldığı görülmektedir. Burbergs’e göre, kişinin şeref

ve itibarının korunması kasten devre dışı bırakıldığı dile getirilmektedir. Özel hayatın gizliliğinin özünde zaten “kişinin şeref ve itibarı” yer aldığından dolayı bu kavramların kapsam dışı bırakılamayacağı dile getirilmiştir (Aktaran: Westlund, 2018, s. 26).

Sözleşmenin 8.maddesinin 1.fikrasına bakıldığında özel hayatın gizliliği kavramının aile, konut ve yazışmalara saygı haklarıyla birlikte tanımlandığı görülmektedir. Aile, konut ve yazışmalar ile ilgili bilgilerin hepsi özel hayatın gizliliği kavramına dahildir (Erdoğan, 2011, s. 194-195). Devletin yükümlülüğü, hem bu hakka yönelik müdahaleleri önlemek, hem de bu hakları güvence altına almak için pozitif koruyucu önlemler alması olarak görülmektedir (Tezcan, 2006, s. 270). 8. maddenin 2.fikrasına baktığımızda ise Birleşmiş Milletler SSHK gibi yine devletin belirli durumlarda bu hakka müdahale edebileceği tanımlanmıştır. Ancak birey özel hayatını kamuya kendisi açmışsa, bu durumda özel hayata müdahaleden bahsedilememektedir (Tezcan, 2006, s. 271).

Bu hakkın amacı, özel hayat bağlamında bireylerin kamu makamlarına karşı keyfi müdahaleden korumak olarak tanımlanabilmektedir. Sözleşme bireyler için bağlayıcı değildir, ancak devlet bireyleri diğer bireylere karşı korumakla yükümlüdür (Westlund, 2018, s. 4). AİHS’nin bölgesel sözleşmeler arasında en etkin sözleşme olduğunu söylemek yanlış olmayacaktır. Getirdiği denetim mekanizması sayesinde sözleşme “bağlayıcı” niteliktedir. EİHB bağlayıcı olmayan evrensel bir beyanname iken, AİHS bölgesel ve bağlayıcıdır. Sözleşme hükümlerinin uygulanması Avrupa İnsan Hakları Mahkemesi tarafından denetlenmektedir.

2.2.2 Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Siber Suç Sözleşmesi (Convention on Cybercrime-CoC) teknolojinin gelişmesi sonucu uluslararası iş birliğini arttırmak, sınır ötesi iş birliği yapmak ve ülkelerin ulusal yasaları arasında bir standart oluşturarak siber suçlara karşı birlikte hareket etmek amacıyla hazırlanmıştır. Sözleşme, Haziran 2001’de imzalanmış ve 8 Kasım 2001’de Avrupa Konseyi Bakanlar Komitesi tarafından kabul edilmiştir. Kasım 2001 tarihinde de Macaristan’ın Budapeşte kentinde üye devletler ve gözlemci devletlerin imzasına sunulduğundan dolayı aynı zamanda “Budapeşte Sözleşmesi” olarak da isimlendirilmektedir. 1 Temmuz 2014 tarihinde yürürlüğe giren sözleşme,

bilgisayar ile dolandırıcılık, ağ güvenliği ihlali, İnternet ve diğer bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası anlaşma olarak karşımıza çıkmaktadır.

Dört bölümden oluşan sözleşmenin ilk bölümünde siber suç alanına özgü terimlerin tanımları yer almaktadır. İkinci bölümün ise iki başlık altında ele alındığı görülmektedir. Birinci başlığın amacı, ulusal ve uluslararası düzeyde suçlarla mücadele için ilgili suçlar çerçevesinde asgari standart oluşturmak, bilgisayar ve bilgisayarlarla ilgili suçları önlemek için de önleyici araçlar geliştirme olarak tanımlanmıştır (Council of Europe, 2001, s.7). İkinci başlıkta ise birinci başlıkta tanımlanan suçların hangi hükümlere göre uygulanacağı belirtilmiştir. Sözleşmenin üçüncü bölümünde uluslararası iş birliğine yönelik hükümler yer alırken, dördüncü bölümde ise sözleşmeye katılım, çekince, beyanlar vb. hükümlerin yer aldığı görülmektedir.

Özel hayatın gizliliği hakkı çerçevesinde sözleşmeye baktığımız zaman ise, sözleşmenin sadece giriş kısmında bu hakka atıf yapıldığı görülmektedir. İlgili madde;

Kolluk kuvvetlerinin menfaatleri ile 1950 tarihli Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi, 1966 tarihli Birleşmiş Milletler Sivil ve Siyasal Haklar Konvansiyonu ve diğer uygulanabilir uluslararası insan hakları anlaşmalarında yer alan ve herkesin herhangi bir müdahale olmaksızın kanaat sahibi olma hakkının yanı sıra, sınırlara bakılmaksızın her türlü bilgi ve düşüncüyü arama, alma ve verme özgürlüğü de dahil olmak üzere ifade özgürlüğü hakkı ile özel hayatın gizliliğine saygı gösterilmesine ilişkin hakları teyit eden temel insan haklarına saygı arasında uygun bir denge sağlanması ...olarak tanımlanmıştır (CoC, 2001, s.2).

Sözleşmenin giriş metninde yer alan bu metinden kolluk kuvvetlerine tanınan geniş yetkilerin, uluslararası iş birliğinin özel hayatın gizliliği hakkına müdahale etmeyeceği ve uluslararası insan hakları çerçevesinde sözleşme maddelerinin düzenlendiği anlaşılmaktadır. Ayrıca sözleşme içerisinde açıkça yazmasa dahi sözleşmenin 3. Maddesinde özel hayatın gizliliği hakkına “Yasadışı Dinleme” başlığı altında dolaylı atıf yapıldığı görülmektedir. İlgili madde;

Taraflardan her biri, kasıtlı olarak işlendiğinde, bu tür bilgisayar verilerini taşıyan bir bilgisayar sisteminden elektromanyetik emisyonlar da dahil olmak üzere, bir bilgisayar sistemine, bir bilgisayar sisteminden veya bir bilgisayar sistemi içinden yapılan kamuya açık olmayan bilgisayar veri iletimlerinin teknik araçlarla haksız olarak dinlenmesini iç hukukunda suç olarak tanımlamak için gerekli olabilecek yasal ve diğer tedbirleri alır. Bir taraf, suçun dürüst olmayan bir niyetle veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilgili olarak işlenmesini şart koşabilir (CoC, 2001, s.3).

Görüldüğü üzere sözleşmenin 3. Maddesinde öncelikle iletişimin gizliliği, iç hukukta güvenceye altına alınması gerektiği bir başka deyişle ülkelerin bu verilerin gizliliğini sağlamakla mükellef olduğu belirtilmiştir. Avrupa Komisyonunun açıklayıcı raporuna göre ise; komisyonun yasadışı dinlemeyi özel hayatın gizliliği hakkının bölünmez bir parçası olan iletişimin gizliliği çerçevesinde yorumladığı görülmektedir. Açıklayıcı rapora göre;

Bu hüküm, veri iletişiminin gizliliği hakkını korumayı amaçlamaktadır. Bu suç, kişiler arasındaki sözlü telefon konuşmalarının geleneksel olarak dinlenmesi ve kaydedilmesi ile aynı şekilde haberleşmenin gizliliğinin ihlalini temsil etmektedir. Haberleşmenin gizliliği hakkı Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinde yer almaktadır. Madde 3 kapsamında oluşturulan suç, bu ilkeyi telefon, faks, e-posta veya dosya transferi gibi her türlü elektronik veri transferine uygulamaktadır (Council of Europe, 2001, s.10).

Açıklayıcı rapor ise, iletişimin gizliliğinin hangi araçlar çerçevesinde tanımlayacağını ve AİHS'nin hangi maddesine dayandırıldığını belirtmektedir. Ancak özel hayatın gizliliği hakkı sadece iletişimin gizliliğinden oluşmamaktadır. Bu durumda ilgili maddenin özel hayatın gizliliği hakkının sadece bir yönüne değindiğinden dolayı, hakkın bütünü için koruma sağlayamadığı görülmektedir.

Sözleşmenin geneline bakıldığında kişisel verilerin korunması çerçevesinde özel hayatın gizliliği hakkını dolaylı olarak kapsadığı görülmektedir. Sözleşme içerisinde uluslararası insan hakları belgelerine her ne kadar atıf yapılsa da, özel hayatın gizliliğinin sözleşme içerisinde doğrudan yer almaması ve hatta detaylandırılmaması

sözleşmenin eksik bir yönü olarak karşımıza çıkmaktadır. Ancak yine de bağlayıcı olan bu sözleşme, bu alanda yeni oluşturulacak sözleşmelere temel teşkil ettiği ve bu alanda yapılan ilk uluslararası sözleşme olduğu için önemini korumaktadır. Sözleşmenin sadece Avrupa Konseyi üyelerine değil, sözleşmeye katılmak isteyen tüm ülkelere açık olması uluslararası arenada işbirliğinin güçlendirilmesine hem de sözleşmeye taraf olan ülke sayısı arttıkça, bu alanda uluslararası bir standart oluşmasına olanak sağlayacağı öngörülmektedir.

2.2.3. Biyotıp Sözleşmesi

Avrupa Konseyi tarafından hazırlanan bir diğer sözleşme Biyotıp Sözleşmesi'dir. Sözleşmenin tam adı ise "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Haklarının ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi"dir. 4/4/1997 yılında Oviedo'da imzaya açılan sözleşme, 1/12/1999 yılında yürürlüğe girmiştir. Oviedo'da imzalandığı için "Oviedo Sözleşmesi" olarak da anılmaktadır.

Sözleşmenin genel çerçevesine baktığımızda Oviedo Sözleşmesi insan biyoetiğinin tüm alanını kapsamayı amaçlamaktadır. Bu sözleşme ile ilk defa çok taraflı bir anlaşmanın, insan hakları ve biyotıp arasındaki bağlantıyı kapsamlı bir şekilde ele alındığı görülmektedir. Ayrıca tamamen biyolojik hukuka ayrılmış ilk çok taraflı bağlayıcı belge olma niteliği de taşımaktadır (Andorno, 2005, s. 134-143). Sözleşmeye taraf olabileceklerin sözleşme çerçevesinde geniş tutulduğu görülmektedir. Bir başka deyişle, devletler ilgili uluslararası örgütün üyesi olmasa dahi (Avrupa Konseyi ve Avrupa Birliği), eğer söz konusu devlet sözleşmenin hazırlık aşamasında bulunduyorsa veya Avrupa Konseyi Bakanlar Kurulu tarafından davet alıyorsa sözleşmeye katılabilmektedir (Gemalmaz, 2012, s. 291). Bu da uluslararası sözleşmelerde ilk defa karşımıza çıkan bir özellik olarak görülmektedir.

Sözleşmenin başlangıç kısmına baktığımızda EİHB, AİHS, Avrupa Sosyal Şartı SSHK, Kişisel Verilerin Otomatik İşlenmesinde Bireysel Verilerin Korunması Sözleşmesi ve Çocuk Hakları Sözleşmesini'ni göz önüne alarak, biyoloji ve tıp alanında teknolojik geliştirmelere de atıfta bulunarak, insan haysiyeti, hak ve hürriyetleri korumak adına sözleşmenin yapıldığı belirtilmiştir.

Biyotıp Sözleşmesinin 3. Bölümünde “Özel Yaşam ve Bilgi Edinme Hakkı” başlığı altında 10. maddede özel hayata yer verilmiştir:

1. Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir.
2. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir.
3. İstisnai durumlarda, 2nci paragrafta belirtilen hakların kullanılmasında hastanın yararları bakımından kanun tarafından kısıtlamalar öngörülebilir. (Council of Europe, 1996, s. 4).

Callard’a göre ilgili maddeler, Avrupa İnsan Hakları Sözleşmesi’nde belirtilen daha genel özel hayatın gizliliği hakkını, kişisel sağlık bilgilerinin özel alanına uygulamaktadır (2010, s. 82). 10. Maddenin 1. Fıkrasına göre, birey kendisiyle ilgili bilgilerin paylaşılıp paylaşılmayacağına kendisi karar verme hakkına sahiptir. Bir başka deyişle bireyin özerkliği ve kişisel bilgilerin kontrolü ön plana çıkmaktadır. 2.fıkrasında ise, bireyin kendi sağlığı hakkında “bilgiye erişim hakkı”na sahip olduğu beyan edilmektedir. Bu fıkrada bilgiye erişim hakkı olduğu kadar bilgiyi reddetme hakkı da görülmektedir. Ancak bilgiyi reddetme hakkı yine bireyin kendisiyle kısıtlanmaktadır. 3.fıkrasında ise bu hakkın hastanın yararına olabilecek durumlarda kısıtlanabileceğinden bahsedilmiştir. Gemalmaz’a göre, bu madde ile 2. fıkrada yer alan “bilgiye erişim hakkı” ile “bilgiyi reddetme hakkı” birlikte anılmaktadır. İstisnai durum olarak belirtilenin aslında “bilgiye erişim hakkı”nın sınırlandırması olarak yorumlanması gerekmektedir. Ayrıca Gemalmaz, bu fıkranın “istisnai haller” ve “hastanın menfaatleri” ibarelerinin sözleşme çerçevesinde tanımlanmamasından dolayı geniş bir yoruma sahip olduğunu dile getirmektedir (Gemalmaz, 2012, s. 297). İlgili ifadelerin tam olarak tanımlanmaması ise ilgili hükümler yorumlanırken muğlaklığa neden olabilmektedir. Ancak yine de Oviedo sözleşmesiyle birlikte genelde biyotıp alanındaki etik ilkelerin özelde de özel hayatın gizliliği ilkesinin uluslararası insan hakları çerçevesinde yasal bir biçime dönüştürüldüğü söylenebilmektedir.

2.3. Diğer Uluslararası Düzenlemeler

Özel hayatın gizliliği hakkının uluslararası sözleşmeler ve Avrupa Komisyonu dışında da, sözleşmeler ile koruma altına alındığı görülmektedir. Bu bölümde Amerikan İnsan Hakları Sözleşmesi, Avrupa Birliği Temel Haklar Şartı, Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi ve Bilgi Teknolojileri Suçlarıyla Mücadeleye İlişkin Arap Sözleşmesi ele alınacaktır.

2.3.1. Amerikan İnsan Hakları Sözleşmesi

Amerikan İnsan Hakları Sözleşmesi (American Convention on Human Rights - ACoHR), 22 Kasım 1969'da San Jose, Kosta Rika'da düzenlenen “Amerikalıların İnsan Hakları İhtisas Konferansı” sonrasında doğmuştur. Bu nedenle “San Jose Paketi” olarak da anılmaktadır. Sözleşme, bahsi geçen konferans sonrası imzaya açılmış ve yaklaşık on yıl sonra 18 Temmuz 1978 yılında yürürlüğe girmiştir.

Goldman, Amerikan İnsan Hakları Sözleşmesi(Amerikan Sözleşmesi) asli garantileri ve kurumsal mekanizmasıyla belki de uluslararası bir organ tarafından şimdiye kadar geliştirilen türünün en iddialı ve geniş kapsamlı belgesi olarak tanımlamaktadır. Kapsamlı olarak anılmasının nedeni ise 1948 yılında ilan edilen Amerikan Haklar Bildirgesinin kapsamını ve içeriğini önemli ölçüde genişletmesine bağlamaktadır (2009, s. 865-866). Sözleşmeye baktığımızda sözleşmenin 82 maddelik kapsamlı bir belge olduğunu görmekteyiz. Sözleşmenin II. Bölümünde Medeni ve Siyasi Haklara²³ değinilmektedir. Ekonomik, Sosyal ve Kültürel Hakların ise sözleşmede sadece madde 26²⁴'da yer aldığı görülmektedir. Bunun nedeni, insan hakları konusunda asgari standart belirlemek yerine devletleri kendi iç ekonomik ve sosyal politikalarında yenilikçi değişiklikler için çaba göstermeye teşvik etmek olarak karşımıza çıkmaktadır (Cabra, 1980, s. 60). Craven bunu, Amerikan Sözleşmesinin Ekonomik, Sosyal ve Kültürel Hakları, Medeni ve Siyasal Haklar çerçevesinde dolaylı olarak korunması olarak yorumlamaktadır (Aktaran: Gemalmaz, 2012, s. 352).

²³ Medeni ve siyasi haklara ilişkin II. Bölüm, 3 ila 25. Maddelerde yer almaktadır.

²⁴ Madde 26. Aşamalı Gelişim, “Taraf Devletler, Buenaos Aires Protokolüyle değişik Amerikan Devletleri Örgütü Şartında öngörülen ekonomik, sosyal, eğitimsel, bilimsel ve kültürel standartların içerdiği hakların, mevzuat çıkartılması ya da diğer uygun yollarla, tam olarak gerçekleştirilmesini aşamalı biçimde sağlamak amacıyla, hem ulusal düzeyde hem de uluslararası işbirliği yaparak, özellikle ekonomik ve teknik nitelikler olmak üzere, önlemler almayı taahhüt ederler/üstlenirler”.

Sözleşmenin bir diğer özelliği ise, düzenlenen hakların öznesinin “kişi²⁵” (person) olmasıdır. Bu bağlamda sözleşmede yer alan haklar tüzel kişilerden ziyade bireyler içindir. Ayrıca, sözleşmeye taraf devletler için hem pozitif hem de negatif yükümlülükler bulunmaktadır. Buna göre, sözleşmede yer alan haklara²⁶ hem “saygı gösterme” hem de bu hakların tam olarak ve özgürce kullanılmasını “temin etmek” yükümlülüğü devletindir (Gemalmaz, 2012, s. 347). Böylece devletler bireylerin haklarını özgürce kullanmaları için gerekli ortamı sağlarken, diğer yandan da bu hakların korunmasını garanti altına almakla yükümlü olacaklardır.

Özel hayatın gizliliği hakkının sözleşmenin 1. Kısım “Devletin Yükümlülükleri ve Korunan Haklar” başlığı altında 11. madde ele alındığı görülmektedir. İlgili madde:

1. Herkesin onuruna saygı gösterilmesi ve haysiyetinin tanınması hakkı vardır.
2. Hiç kimse, özel yaşamına, ailesine, evine ya da yazışmalarına keyfi ya da kötü niyetli müdahalelerin ya da onur ve itibarına yönelik yasadışı saldırıların hedefi olamaz.
3. Herkes, bu tür müdahale ve saldırılara karşı hukukun korumasından yararlanma hakkına sahiptir (ACoHR, 1969).

Sözleşmenin 11. Madde 1. fıkrasında bireyin onuru ve haysasiyetinin korunmasına diğer sözleşmelere nazaran vurgu yapıldığı görülmektedir. 2.ve 3. fıkraların diğer insan hakları belgeleriyle aynı şekilde özel hayatın gizliliği hakkını koruduğu görülmektedir.

Amerikan İnsan Hakları Sözleşmesinin, sözleşmeye taraf devletlerin yükümlülüklerini sağlamak adına iki ana mekanizması olduğu görülmektedir. Bunlardan ilki “Amerikalılar Arası İnsan Hakları Komisyonu (AAİHK)” “dur ve komisyonun merkezi Washington D.C Amerika’da yer almaktadır. Bir diğer yetkili organı ise Amerika Kıtası İnsan Hakları Mahkemesi (AKİHM)’dir ve merkezi Kosta Rika’da bulunmaktadır.

²⁵ Madde 1.2. “Bu Sözleşmenin amaçları bakımından “kişi” terimi, her bir insan anlamına gelir”.

²⁶ Madde 1.1. “Bu Sözleşmenin tarafı Devletler, burada tanınan haklara ve özgürlüklere saygı göstermeyi ve kendi yargı yetkilerine tabi tüm kişilerin, söz konusu haklar ve özgürlükleri, ırk, renk, cinsiyet, dil, din, siyasal ya da diğer görüş ulusal ya da sosyal köken, ekonomik statü, doğum ya da herhangi bir başka sosyal koşul gerekçeleriyle hiçbir ayrımcılık yapılmaksızın, özgürce ve tam olarak kullanabilmelerini temin etmeyi, üstlenirler.”

AAİHK sözleşmeye taraf olan devletlerin insan haklarına ilişkin bireysel şikayetleri üzerinde çalışmaktadır. AKİHM'nin ise yetkilerinin AAİHK'dan daha dar kapsamda olduğu görülmektedir. Sadece AAİHK tarafından sevk edilen davalara ve sözleşmeye taraf devletlerarasındaki çekişmeli davalara bakmakla yükümlü olduğu görülmektedir. Mahkemenin kararları bağlayıcı olarak karşımıza çıkmaktadır.

Kapsamlı bir bölgesel sözleşme olarak karşımıza çıkan Amerikan sözleşmesinin hükümleri izleme ve uygulama mekanizmalarında farklılık görülmektedir. AİHS'de tüm şikayet ve başvurular doğrudan AİHM'ne yapılırken, Amerikan sözleşmesinde başvuruların AAİHK'ya yapıldığı görülmektedir (Gemalmaz, 2012, s.364). Amerikan Sözleşmesinin, birçok insan hakları belgeleriyle ortak noktası olsa da sözleşmenin Amerika kıtasının kültürünü yansıttığı görülmektedir. Örneğin Avrupa kıtasında ve uluslararası belgelerde daha çok “birey“ kelimesi kullanılırken, bu sözleşmede “kişi“ üzerinden tanım yapıldığı görülmektedir.

2.3.2. Avrupa Birliği Temel Haklar Şartı

Avrupa Birliği Temel Haklar Şartı (Charter of Fundamental Rights of The European Union-CoFR) AB için önemli bir dönüm noktası olarak görülmektedir. AB kurucu anlaşmalarında yer alan tüm temel hak ve özgürlüklerin belirli bir katalogta bulunmamasının birlik için tartışmalara neden olduğu görülmektedir. Temel haklar konusunda olan bu eksiklik, insan hakları konusuna da açıklık getirilmesi taleplerini beraberinde getirmiştir. Avrupa Topluluğu Adalet Divanı bu eksikliği her ne kadar içtihatlar ile gidermeye çalışsa da (üye devletlerin anayasalarını ve AİHS'ni temel alsada), herhangi bir hukuki metin ile bağlı ve bağlayıcı olmadığından dolayı bir başka deyişle somut bir ölçüt bulunmadığından dolayı yazılı bir metin ihtiyacı doğmuştur (Özcan, 2014, s. 720; Yüksel, 2002, s.39). Bu çerçevede de 17 Aralık 1999 tarihinde Brüksel'de Temel Haklar Şartı'nı hazırlamak için çalışmalar başlamış ve 7 Aralık 2000 tarihinde Nice Zirvesinde ilan edilmiştir (Metin, 2011, s. 133). Temel Haklar Şartı'nın, “üye devletlerin anayasal gelenekleri ve uluslararası yükümlülükleri, Avrupa Birliği Antlaşması, Topluluk Antlaşmaları, Avrupa İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi, Topluluk ve Avrupa Konseyi tarafından kabul edilen Sosyal Şartlar ile Avrupa Toplulukları Adalet Divanı ve Avrupa İnsan Hakları

Mahkemesi içtihadından kaynaklanan hakları yeniden teyit ettiği” ilgili belgede dile getirilmiştir (CoFR, 2000, s.8). Birey’i temel alan Şartın oluşturulma amacına giriş kısmında şu şekilde yer verilmiştir;“Toplumdaki değişimler, sosyal ilerleme ve bilimsel ve teknolojik gelişmeler ışığında temel hakların korunmasını güçlendirmek ve bu hakları bir Şartta daha görünür kılmak gerekmektedir” (CoFR, 2000, s.8).

Toplamda 54 maddeden oluşan Şart yedi bölümden oluşmaktadır. Özel hayatın gizliliği hakkına ikinci kısımda “Özgürlükler” başlığı altında yer verilmiştir. 7. maddede ele alınan özel hayatın gizliliği hakkı “Özel Hayata ve Aile Hayatına Saygı” üst başlığı ile ele alınmaktadır. İlgili maddeye göre; “Herkes özel ve aile hayatına, evine ve iletişimine saygı gösterilmesi hakkına sahiptir” (CoFR, 2000, s.10). İlgili maddenin AİHS’nin 8. maddesi ile paralellik gösterdiği görülmektedir. Bunun en büyük nedeni, şart oluşturulurken hakların birçoğunun AİHS’nden alınması olarak karşımıza çıkmaktadır. Ancak burada önemli bir fark ortaya çıkmıştır. AİHS’nin 8. maddesinde bahsi geçen “haberleşme” sözcüğü yerine bilimsel ve teknolojik gelişmelerin baz alınarak “iletişim” kelimesi kullanıldığı görülmektedir. Bu da şartın giriş kısmında yer alan “toplumdaki değişimler, sosyal ilerleme ve bilimsel ve teknolojik gelişmeler ışığında temel hakların korunmasını güçlendirmek...” amacıyla paralel olarak hakkın tanımlanmasını beraberinde getirmiştir.

Avrupa Birliği Temel Haklar Şartı’nın oluşturulmasında büyük ölçüde AİHS’nden yararlanıldığı görülmektedir (Metin, 2002, s.47) Ancak Şart ve AİHS’nin benzer ve farklı olduğu yönler bulunmaktadır. En önemli benzerlikleri iki belgenin de Avrupa kıtasında temelde insan haklarını koruyan iki farklı yasal belge olmasıdır. Farklılıklarına değinecek olursak en önemli farklılık; AİHS Avrupa Konseyi’nin tüm imzacı devletleri için geçerliyken, AB Şartı sadece Avrupa Birliği’nin yargı yetkisi dahilinde geçerlidir. Bir diğer fark AB Temel Haklar Şartı, AB hukukunun bir parçası olarak karşımıza çıkmaktadır, ancak Avrupa Birliği AİHS’ne taraf değildir. Dolayısıyla AB hukukunun bir parçası değildir ancak insan haklarını korumada önemli belgeler arasında yer almaktadır. Bir diğer farklılık ise kapsam konusunda karşımıza çıkmaktadır. Şart, Avrupa Birliğindeki insan hakları için kapsamlı bir çerçeve sunmaktadır, ancak AİHS bu çerçevenin yalnızca bir kısmını oluşturmaktadır. Son olarak ise Şart, AB tarafından hazırlanmış ve ABAD tarafından yorumlanmıştır, ancak

AIHS Avrupa Komisyonu tarafından hazırlanarak, AIHM tarafından yorumlandığı görülmektedir. Ayrıca Şart, AB Anayasası oluşturulması adına atılan ilk somut belge niteliğine sahiptir. Birlik içerisinde anayasa oluşturulmaması da o dönemde bu şartın oluşturulması önemli bir adım olarak görülmektedir.

2.3.3. Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi

Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Sözleşme (Convention on Cyber Security and Personal Data Protection-CCSPDP), 27 Haziran 2014 tarihinde Afrika Birliği Zirvesinde kabul edilmiştir. Sözleşmenin kabul edildiği yer Malabo olduğu için “Malabo Sözleşmesi” olarak da adlandırılmaktadır. Sözleşmenin yürürlüğe girmesi için gerekli olan 15 devletin onay süreci ancak 9 yıl sonra tamamlanabilmiş ve sözleşme 8 Haziran 2023 tarihinde yürürlüğe girmiştir.

Sözleşme temelde elektronik ticaret, siber güvenlik, siber suçlar ve kişisel verilerin korunmasını sağlamak ve Afrika Birliği Üye Devletlerinde siber güvenlik alanında iş birliğini geliştirmek için gerekli ortak mevzuat ihtiyacını ele almayı amaçlamaktadır. Bunun yanı sıra tüketicileri, fikri mülkiyet haklarını, kişisel verileri ve bilgi sistemlerini ve çevrimiçi özel hayatın gizliliği gibi konularda da yasal boşluğun doldurulması sözleşmenin bir diğer amacı olarak görülmektedir.

Sözleşmenin önsöz bölümünde özel hayatın gizliliğine kapsamlı bir şekilde atıf yapıldığı görülmektedir. Önsözde vurgulanmak istenen husus, bilgi iletişim teknolojilerinin gelişiminden oluşabilecek ve özel hayatın gizliliği hakkını ihlal edebilecek tehlikeler için kapsamlı bir koruma mekanizması geliştirilmesi, teknolojiye gelişmeler karşısında ise teknoloji ve özel hayatın gizliliği arasındaki dengenin korunması gerekliliği vurgulanmaktadır. Sözleşmenin geneline bakıldığında ise dört bölümden oluştuğu görülmektedir. Bu bölümler sırasıyla; “Elektronik Ticaretin Organizasyonu”, “Kişisel Verilerin Korunması”, “Siber Güvenliğin Teşviki ve Siber Suçlarla Mücadele” ve “Ortak ve Nihai Hükümler” dir. Özel hayatın gizliliği hakkına sözleşmenin ikinci bölümünün 8. maddesinde yer verilmektedir.

- 1- Her bir Taraf Devlet, başta fiziksel verilerin korunması olmak üzere temel hakların ve kamu özgürlüklerinin güçlendirilmesini amaçlayan yasal bir

çerçeve oluşturmayı ve kişisel verilerin serbest dolaşımı ilkesine halel getirmeksizin özel hayatın gizliliğine yönelik her türlü ihlali cezalandırmayı taahhüt eder.

- 2- Bu şekilde oluşturulan mekanizma, her türlü veri işlemenin gerçek kişilerin temel özgürlüklerine ve haklarına saygı göstermesini sağlarken, Devletin ayrıcalıklarını, yerel toplulukların haklarını ve işletmelerin kuruluş amaçlarını tanır (CCSPDP, 2014, s.14).

8.maddede özel hayatın gizliliğinin bir çerçeve mekanizma oluşturularak sağlanması amaçlanmaktadır. Bu çerçeve mekanizma oluşturulurken, özel hayat ve fiziksel verileri koruma ön plana çıkmaktadır. Aynı zamanda da tüm paydaşların çıkarları göz önüne alınarak ortak bir bileşende buluşmanın önemi vurgulanmaktadır. Bu yaklaşım ile özel hayatın gizliliği, kamu kurumları, aynı zamanda da topluluk hakları ve işletmeler arasında denge kurmaya çalışıldığı görülmektedir.



Kişisel verilerin korunması sözleşmenin 9. Maddesi ve 23. Maddeleri arasında açıklanmaktadır. Bura da önemli olan nokta Malabo Sözleşmesinin veri sahiplerini bilgi edinme hakkı²⁷, erişim hakkı²⁸, itiraz hakkı²⁹ ve unutulma hakkı³⁰ gibi çok çeşitli hakları detaylarıyla ortaya koymasındır. Böylece özel hayatın gizliliği hakkına sahip olan kişisel veri sahiplerinin de detaylı olarak tanımlanan haklar ile güvence altına alındığı görülmektedir.

Genel olarak sözleşme hem içeriği hem de kapsadığı konular açısından geniş bir yelpaze sunmaktadır. Sözleşme de sadece kişisel verilerin korunması değil, elektronik ticaret, özel hayat, siber güvenlik ve siber suçlar gibi çok bileşenli konuların yer aldığı görülmektedir. Yelpazenin bu kadar geniş olması uygulamada birtakım sorunları beraberinde getirebilir. Ayrıca 2014 yılından 2023 yılına kadar sadece 15 üye devletin sözleşmeyi imzalaması, sözleşmenin Afrika kıtasında uygulanabilirliğini

²⁷ Madde 16: Bilgi edinme hakkı

Veri sorumlusu, verileri işlenecek olan gerçek kişiye aşağıdaki bilgileri sağlayacaktır aşağıdaki bilgileri, verilerin toplandığı zamandan daha geç olmamak kaydıyla ve kullanılan araç ve imkanlara bakılmaksızın, aşağıdaki bilgilerle birlikte:

- a) Kendisinin ve varsa temsilcisinin kimliği;
- b) Verilerin hangi amaçlarla işleneceği;
- c) İlgili veri kategorileri;
- d) Verilerin ifşa edilebileceği alıcı(lar);
- e) Dosyadan çıkarılmayı talep etme kapasitesi;
- f) Verilere erişim ve düzeltme hakkının varlığı kendisi ile ilgili;
- g) Verilerin saklandığı süre;
- h) Verilerin üçüncü ülkelere önerilen aktarımları.

²⁸ Madde 17: Erişim hakkı

Kişisel verileri işlenecek olan herhangi bir gerçek kişi, kontrolörden sorular şeklinde aşağıdakileri talep edebilir:

- a) Değerlendirmesine ve işlemeye itiraz etmesine olanak tanıyacak türden bilgiler;
- b) Kendisiyle ilgili verilerin işlenip işlenmediğine dair teyit;
- c) İşlenmekte olan kişisel verilerin ve bunların kaynağına ilişkin mevcut her türlü bilginin kendisine iletilmesi;
- d) İşlemenin amacı, ilgili kişisel veri kategorileri ve verilerin ifşa edildiği alıcılar veya alıcı kategorileri hakkında bilgi.

²⁹ Madde 18: İtiraz hakkı

Herhangi bir gerçek kişi, meşru gerekçelerle, kendisiyle ilgili verilerin işlenmesine itiraz etme hakkına sahiptir. Kendisiyle ilgili kişisel veriler üçüncü taraflara ilk kez ifşa edilmeden veya onlar adına pazarlama amacıyla kullanılmadan önce bilgilendirilme ve bu tür ifşa veya kullanımlara ücretsiz olarak itiraz etme hakkının açıkça sunulması hakkına sahiptir.

³⁰ Madde 19: Düzeltme veya silme (unutulma) hakkı

Herhangi bir gerçek kişi, veri sorumlusundan, duruma göre, kendisiyle ilgili yanlış, eksik, belirsiz veya güncel olmayan veya toplanması, kullanılması, ifşa edilmesi veya saklanması yasak olan kişisel verilerin düzeltilmesini, tamamlanmasını, güncellenmesini, engellenmesini veya silinmesini talep edebilir.

sorgulamaktadır. Sözleşmenin az sayıda ülke tarafından imzalanması sözleşmenin amaçlarından biri olan ortak mevzuatın oluşturulması da sekteye uğratabilir.

Son olarak sözleşmeyi Budapeşte sözleşmesi ile karşılaştırdığımızda, öncelikle sözleşmenin kapsamı açısından farklılıklar görülmektedir. Avrupa Konseyi tarafından oluşturulan Budapeşte sözleşmesi küresel bir kapsama sahipken, Malabo sözleşmesinin kapsamının Afrika kıtası olduğu görülmektedir. Ayrıca Budapeşte sözleşmesi her ne kadar özel hayatın gizliliği hakkına vurgu yapsa da sözleşmenin önceliğinin siber suçlarla uluslararası işbirliği olduğu görülmektedir. Ancak Malabo sözleşmesi kişisel veriler ve özel hayatın gizliliğinin korunması için kapsamlı bir çerçeve sağlamayı amaçladığı söylenebilir. Sözleşmeler kapsamı bakımından farklı olsa da Malabo sözleşmesi Budapeşte sözleşmesinden sonra yapılan ilk bölgesel sözleşme olarak önemini korumaktadır. Bu bağlamda da özel bir öneme sahiptir. Temelde her iki sözleşmenin de amacı bölgesel ve/veya küresel olarak siber suçlarla mücadele ederken siber tehditlerden korunmayı ve işbirliğini geliştirmeyi amaçlamaktadır.

2.3.4. Bilgi Teknolojileri Suçlarıyla Mücadeleye İlişkin Arap Sözleşmesi

Bir başka bölgesel sözleşme Bilgi Teknolojileri Suçlarıyla Mücadeleye İlişkin Arap Sözleşmesi (Arab Convention on Combating Information Technology Offences- ACCITO) dir. Eski adıyla Arap Devletler Ligi, yeni adıyla ise Arap Ligi 2010 yılında sözleşmeyi kabul etmiştir. Sadece Arap Ligi üyelerine özel olan bu sözleşme Arap Ligi'nin yedi üyesinin onaylaması ardından 7 Şubat 2014 tarihinde yürürlüğe girmiştir. Sözleşmenin amacı sözleşmenin 1. maddesinde şu şekilde dile getirilmiştir: “Bu sözleşmenin amacı, Arap Devletlerinin güvenlik ve çıkarları ile toplumlarının ve bireylerin güvenliğini korumak amacıyla bu tür suçların tehditlerini bertaraf etmek için bilgi teknolojisi suçlarıyla mücadele alanında Arap Devletleri arasındaki iş birliğini geliştirmek ve güçlendirmektir” (ACCITO, 2010, s.2).

Bir başka deyişle bölgesel bir sözleşme oluşturulmasının temel amacı Arap Ligi üyeleri arasındaki iş birliğini güçlendirerek devletlerin varlıklarını, halklarını ve çıkarlarını siber suçlara karşı savunmalarını ve korumalarını sağlamaktır. Sözleşme 43 maddeden ve beş ana bölümden oluşmaktadır. Anlaşmanın genel hükümlerinin

belirlendiği I. bölümde terminoloji tanımı yapılmış ve Yasadışı Erişim Suçu, Yasadışı Dinleme Suçu, Verilerin Bütünlüğüne Karşı Suç, Bilgi Teknolojisi Araçlarının Kötüye Kullanılması Suçu, Sahtecilik Suçu, Dolandırıcılık Suçu, Özel Hayata Karşı Suçlar, Bilgi Teknolojisi Yoluyla İşlenen Terörizmle İlgili Suçlar gibi bilgi teknolojileri gibi suçlar tanımlanmıştır. İkinci bölümde Prosedürel hükümler yer alırken üçüncü bölümde Bilgi Teknolojilerinde Saklanan Verilerin Saklanması, Usul Hükümlerinin Uygulama Alanı, Kullanıcıların Takip Bilgilerinin İvedi Saklanması ve Kısmen Açıklanması, Bilgi Verme Emri, Saklanan Bilgilerin İncelenmesi gibi usule uygun hükümlere yer verilmiştir. Dördüncü bölüm üye devletlerin hukuki ve adli işbirliğine yer verirken son bölümde ise sözleşmenin yürürlüğe girmesinin koşulları nihai hükümler başlığı altında ele alınmıştır.

Sözleşmenin birinci bölümünde Madde 14’de “Özel Hayatın Gizliliğine Karşı Suçlar” adı altında özel hayatın gizliliğine yer verilmiştir. İlgili madde: “Bilgi teknolojisi yoluyla özel hayatın gizliliğine karşı suç.” şeklinde tanımlanmıştır (ACCITO, 2010, s.7).

Sözleşmede özel hayatın gizliliği giriş bölümü de dahil olmak üzere ilgili madde dışında ele alınmadığı ve vurgulanmadığı görülmektedir. İlgili maddenin de içerik ve kapsam bakımından yetersiz olduğu görülmekte hangi koşulların özel hayatın gizliliğini ihlal ettiği açıkça belirtilmediği görülmektedir. Bir başka deyişle özel hayatın gizliliğini korumakla yükümlü kılacak herhangi bir katı düzenleme getirmeden özel hayatın gizliliği hakkına üstünlük bir şekilde atıfta bulunmaktadır (Hassib ve Shires, 2022, s.100-101). Dolayısıyla sözleşme içerisinde özel hayatın gizliliği muğlak kalmıştır denilebilir. Bu da ilgili hükmün istenildiği gibi yorumlanması riskini beraberinde getirebilmektedir. Genel itibarıyla sözleşmedeki maddeler geniş olarak tanımlansa da tanımların net olmaması sözleşmede belirsizliğe yol açtığı görülmektedir.

Bölüm Değerlendirmesi

Özel hayatın gizliliği hakkının uluslararası ve bölgesel insan hakları belgelerinde yer aldığı görülmektedir. Bunun nedeni sözleşmelerde de belirtildiği üzere insan onur

ve haysiyetinin herşeyden üstün olması ve insanın biricikliği olarak karşımıza çıkmaktadır.

EİHB uluslararası hukukta ilk defa tanınan insan hakları belgesi olması nedeniyle diğer sözleşmelerden ayrı bir öneme sahiptir. Özel hayatın gizliliği hakkının tanımının yine ilk defa bu sözleşmede uzun tartışmalar ve oturumlar sonucunda ortaya çıktığı görülmektedir. Ayrıca EİHB'nin bu alanda öncü belge olması nedeniyle birçok uluslararası sözleşmenin hazırlık aşamasında beyannamenin temel belge olarak alındığı görülmektedir. EİHB'den sonra hazırlanan insan hakları belgelerinde özel hayatın gizliliği daha kapsamlı olarak ele alınmakla birlikte, temelde sözleşmelerde yapılan tanımların benzerlik taşıdığı görülmektedir.

EİHB uluslararası alanda insan haklarına dair etik kuralları belirleyen belge olarak karşımıza çıkmaktadır. Bu yüzden beyannamenin bağlayıcılığı bulunmamaktadır. Ancak EİHB'den sonra ortaya çıkan neredeyse tüm insan hakları belgelerinin bağlayıcı olduğu ve yargı mekanizmalarının bulunduğu görülmektedir.

Uluslararası insan hakları belgelerinin yanısıra bölgesel nitelikte de özel hayatın gizliliği hakkının korunmaya çalışıldığı görülmüştür. Bölgesel düzeyde insan hakları belgelerinin düzenlenmesinin amacı EİHB ve BM Sivil ve Siyasal Haklar Konvansiyonu gibi uluslararası belgeleri güçlendirmek, komşu devletlerarasındaki işbirliğini arttırmak ve her bölgenin kültürüne özgü düzenlenerek bölgesel ihtiyaçlara göre uyarlama olarak karşımıza çıkmaktadır. Ancak özel hayatın gizliliği hakkı evrensel bir hak olduğundan dolayı bölgesel sözleşmelerde herhangi bir fark gözetilmeden tanımlandığı görülmektedir.

İnsan hakları sözleşmelerinde değinilmesi gereken bir diğer husus özel hayatın gizliliği hakkının mutlak bir olarak tanımlanmamış olmasıdır. Sözleşmelerde hakkın belirli istisnalarının bulunduğu görülmektedir.

Gelişen teknolojiler sonucu özel hayatın gizliliği hakkının bölgesel siber suç sözleşmelerinde de çeşitli bağlamlarda yer aldığı görülmektedir. Avrupa Konseyi Siber suç sözleşmesinde yasadışı dinleme bir başka deyişle iletişimin gizliliği temel alınırken, Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesinde kişisel verilerin korunması, Bilgi Teknolojileri Suçlarıyla Mücadeleye

İlişkin Arap Sözleşmesinde ise bilgi teknolojisi adı altında ele alındığı görülmektedir. İnsan hakları sözleşmelerinde özel hayatın gizliliği hakkının tanımlanmasında büyük farklılıklar bulunmazken, siber suç sözleşmelerinde bölgesel farklılıkların ön plana çıktığı görülmektedir.



ÜÇÜNCÜ BÖLÜM:

3.SİBER UZAY ÖZEL HAYATIN GİZLİLİĞİ HAKKINI NASIL ETKİLİYOR?

Bilgi teknolojilerinin durmaksızın gelişmesi ve bireylerin interneti daha fazla alanda kullanmasıyla birlikte, bireyin özel hayatın gizliliği hakkının ihlali konusunda birtakım endişeler ortaya çıkmaktadır. Teknolojik gelişmelerin kendi ekonomisini yaratmasıyla birlikte kullanıcı verileri daha önemli hale gelmiş bu da çok uluslu şirketler, devletler ve üçüncü tarafların bu verileri kendi çıkarları doğrultusunda kullanmasına neden olmuştur. Kişisel bilgilere yetkisiz erişim ayrıca bu verilerin kötü niyetli amaçlarla kullanılma riski ve istismar edilebilme potansiyeli de bireyleri doğrudan etkilemektedir.

Siber uzay bireye hem fırsatlar sunarak hem de doğrudan birtakım zorlukları beraberinde getirerek özel hayatın gizliliği hakkını doğrudan etkilemektedir. Dijital toplumun ortaya çıkması kullanıcılara birtakım faydalar sağlasa da diğer yandan bireyin özel hayatını koruma arzusunu da beraberinde getirmektedir. Genel olarak bakıldığında siber uzayın özel hayatın gizliliği hakkına etkisi karmaşık ve çok yönlü olarak tanımlanabilmektedir. Siber uzayın öngörülemez yapısı, bireyin bilgilerinin ele geçirilme esnasında farkında olmaması durumu veya tehditin nereden geleceğinin bilinmemesi bu karmaşık yapıyı desteklemektedir.

Siber uzayda özel hayatın gizliliği hakkı en çok siber gözetim, siber istihbarat ve kişisel verilerin konusunda konuşulmaktadır. Bu bölümde öncelikle bahsi geçen konulara yer verilecektir. Daha sonra ise bu konuların AIHM kararlarında ne şekilde ele alındığı dava örnekleriyle açıklanmaya çalışılacaktır.

3.1. Siber Uzayın Özel Hayata Etkisi

Bilgisayarların ve internetin gelişmesi sonucu ortaya çıkan siber uzay özel hayatlarımızda köklü bir devrim yaratmıştır. Öncelikle internetin hızla yaygınlaşması sayesinde günlük rutinlerin fiziksel dünyadan sanal dünyaya kaydığı görülmektedir. Bunun nedeni aslında teknolojik yeniliklerin hayatımızı kolaylaştırması, fiziksel alanda yapılan birçok eylemin sanal alana taşınması olarak açıklanabilmektedir. Bu

durum beraberinde yeni iletişim şekillerinin ortaya çıkmasına ve bireyin hem özel hem de kamusal hayat dinamiklerinin değişmesine yol açmaktadır. Mesafe ve zaman dinamiklerinin ortadan kalkması ile birey fiziksel sınırlarını aşarak hem tüm dünya ile hızlı iletişim kurmuş hem de maliyet ve fayda açısından belirli bir doygunluk hissine ulaşmıştır. Bireyin daha önce satın alarak okuduğu bir gazete, çevrimiçi ortamda ücretsiz hale gelmiş, birey bir gazete yerine istediği kadar gazete okuyabilir olmuştur. Aynı zamanda sosyal medya platformlarının da yükselişiyle birey anonim olarak daha önce ifade edemediği birçok şeyi ifade eder olmuş ve sosyalleşme için yeni platformlarda yer almıştır. Bireyler fiziksel sınırları aşarak kendine siber uzayda yeni kamusal alanlar oluşturmaya başlamıştır. Ancak bu benzeri görülmemiş teknolojik devrimin özel hayatın gizliliği ile ilgili endişeleri de beraberinde getirdiği görülmektedir.

Bilgi iletişim teknolojilerinde olan gelişme, bireyin özel alanı ve kamusal hayatı arasındaki çizgiyi belirsiz hale getirmiş ve bireyin özel hayatı giderek artan bir şekilde dijital ortamla iç içe geçmiştir. Birey günlük hayatında belki de yakın çevresiyle bile paylaşmayacağı bilgilerini sanal ortamda paylaşır hale gelmiştir. Kişisel bilgilerin siber uzayda paylaşılması, saklanması ve toplanması ile birlikte özel hayatın gizliliği hakkı da siber uzayda ihlal edilir hale gelmiştir. Bunun yanısıra çok uluslu şirketlerin bireylerin verilerini kayıt altına alması ve/veya özel şirketlerin, devletlerin vatandaşlarını Orwell’cı bir yaklaşımla bireyi her alanda izlemesi, yine birçok devlet kurumunun istihbarat yöntemiyle bireylerin verilerini toplu olarak ele geçirmesi özel hayatın gizliliği ile ilgili endişeleri arttırmaktadır.

Siber uzayda gerçekleştirdiğimiz her işlemde dijital izlerimizi bırakmaktayız. Ancak siber uzayda bu bıraktığımız izlerin kimler tarafından ne amaçla ve ne zaman kullanılacağını çoğunlukla farkında değiliz. Kişisel verileri korumanın zorluğu tam da bu noktada karşımıza çıkmaktadır. Kapalı devre televizyon (Closed-Circuit Television-CCTV) kameraları ile çevrimiçi gözetim, ortam sesi dinleme, Global Konum Belirleme Sistemi (Global Positioning System-GPS) teknolojisi sayesinde konum belirlemenin de yaygın varlığı birey açısından siber uzayda bir takım ihlalleri beraberinde getirmektedir.

Bauman'ın deyimiyle bilgilerin büyük bir çoğunluğu aslında kişilerin kendileri tarafından cep telefonları kullanarak, alışveriş merkezlerine giderek, tatillerde seyahat ederek, eğlenerek veya internette gezinerek sağlanmaktadır. Düzenli olarak, kendiliğimizden ve hatta isteyerek her gün kartlarımızı kullanıyor, posta kodlarımızı söylüyor ve kimliklerimizi gösteriyoruz“ (Bauman ve Lyon, 2016, s.24). Bir taraftan siber uzayda mutlu olduğumuz anları paylaşma arzusu, bir taraftan da paylaştığımız her bilginin veri olarak kayıt altına alınması bireyi paradoksal bir durumun içerisine sokmaktadır.

Sonuç olarak, siber uzay, bireylere fırsatlar ve zorluklarla dolu bir dijital sınır sunarak, özel hayatın tanımının kapsamını değiştirmiştir. Bireyin özel hayatın sosyalleşme, eğitim, ifade özgürlüğü, bilgiye erişim ve toplanma özgürlüğü gibi alanlarda olumlu olarak etkilemektedir. Ancak özellikle siber gözetim, siber istihbarat ve kişisel verilerin korunması konusunda da kontrol edilemez bir şekilde özel hayatın gizliliğinin ihlal edildiği görülmektedir.

3.1.1. Siber Gözetim

Modernitenin yükselişi, 20. yüzyılın totaliter rejimleri ve ardından süregelen soğuk savaş nedeniyle gözetim, ulus-devletlerin ayrılmaz bir parçası haline gelmiştir. Bürokrasinin yükselişiyle birlikte devletler, kendi sınırları içerisinde vatandaşları hakkında bilgi toplamış, işlemiş, toplanan bilgileri de kategorize edip depolamışlardır. Bürokrasi, bilgi toplama kapasitesi ve denetleyiciliğiyle temel bir gözetim biçimi olarak tanımlanmaktadır (Lyon, 2013, s. 120). Bu sürecin günümüzde de sadece devlet sınırları içerisinde olmasa dahi devam ettiği görülmektedir.

Modern ulus devletteki gözetim Foucault'un Panoptikon kavramına benzetilmektedir. Foucault Panopticon'u şu şekilde tanımlamaktadır:

Panopticon'u düşsel bir yapı olarak anlamamak gerekir: O, ideal biçime getirilmiş olan bir iktidar mekanizmasının diyagramıdır, her tür engelden, dirençten veya sürtüşmeden arınmış olan işleyişi saf bir mimari ve optik sistem olarak sunabilir: O fiili durumda, her tür özel kullanımdan kopartılabilen ve kopartılması gereken siyasal bir teknoloji biçimidir (Foucault,1992, s. 258).

Panoptikon'un aynı ulus-devlette olduđu gibi sınırları vardır. Gözetim fiziksel alandadır ve belirli bir mekanı bulunmaktadır. Gözetleyen devlettir ve gözetlenen birey bunun farkındadır ancak kim tarafından gözetlendiğini hiçbir zaman bilememektedir.

Foucault gözetimi tanımlarken esas vurguladığı modern toplumların “disiplin” toplumu olarak tanımlanabileceğidir. “Panopticon, nesnesi ve amacı hükümlerlik ilişkisi değil de, disiplin ilişkileri olan yeni bir "siyasal anatomi"nin genel ilkesidir” (Foucault, 1992, s. 262). Ancak “bu disiplin herhangi bir kurum veya aygıtla özdeşleştirilemez çünkü bütün aygıtlar ve kurumları birbirine bağlamak, sürdürmek, kesiştirmek ve yeni bir işleyiş kazandırmak suretiyle kateden bir tür iktidar veya bir tür teknolojidir” (Deleuze, 2013, s.45) “İktidar... gözetim tekniklerinin sayesinde, ...ilke olarak aşırılığa, güce, şiddete başvurmadan icra edilmektedir” (Foucault, 1992, s. 222-223). İktidar şiddete başvurmayacaktır, çünkü panoptikonda mahkumlar, ne zaman gözlemlendiklerini bilmeden otoritenin sürekli varlığının farkında olacaklardır. Bu nedenle de, mahkumlar kendi kendini disipline edecek ve az sayıda gardiyan çok sayıda mahkum üzerinde düzeni sağlayabilecektir.

Foucault'un Bentham'dan ödünç alarak geliştirdiği Panoptik yapılar, gözetimin fiziksel ve mekansal olduđu ve gözetimin merkezi yapılar tarafından yapıldığı bir model sunmaktadır. Panopticon modelinin en önemli katkılarından biri, gözetimin bireyin davranışının şekillendirilmesine yaptığı vurgudur. Foucault, okul, hapisane, işyerleri gibi mekanlarda bireylerin izleniyor olma ihtimalinin bile bireylerde öz disiplin duygusunu geliştirdiğini savunmuştur.

Birçok araştırmacı, günümüz gözetimini anlamak için panoptikon metaforunu hapisane alanından çıkarmış ve devletin sosyal davranış kontrol etmeye ve etkilemeye çalıştığı diğer alanları tanımlamak için kullanmıştır. Bu aynı zamanda moderniteden post modernliğe geçişi de temsil etmektedir. Bu düşünürlerden biri Deleuze'dir. Deleuze birçok açıdan Foucault ile aynı görüşü paylaşmakla birlikte, Foucault tarafından tanımlanan disiplin toplumunu eleştirmiştir. Panopticon'un amacı, bireyleri sürekli gözetim ve kontrole tabi tutarak disiplinli ve uysal bir nüfus yaratmaktır. Deleuze'e göre bireyler artık okul, hapisane ve hastane gibi kurumlar tarafından sürekli fiziksel gözetime tabi değil, daha çok veri dolaşımına dayalı bir

elektronik kontrol sistemine tabidir. Artık disiplin toplumları yerini kontrol toplumlarına bırakmıştır. Deleuze, disiplini "yönetmenin" bir amacı veya itici gücü olduğunu özellikle reddetmektedir; bunun yerine disiplinin denetim biçimlerinde bulunması gerektiğini ifade etmektedir (Galič vd.,2017, s. 19). Çünkü denetim toplumları, bireylerin davranışlarını düzenlemek için bilgi ve teknolojiyi kullanmaktadır. Bireyler bürokrasinin ön planda olduğu üretim toplumundan tüketim toplumuna geçiş yapmışlardır. Deleuze bunu şu şekilde ifade etmektedir;

Disiplin toplumlarının iki kutbu vardır: bireyi belirleyen imza ve onun bir kitle içindeki konumunu gösteren sayı ya da idari numaralandırma...Öte yandan, denetim toplumlarında önemli olan artık bir imza ya da sayı değil, bir koddur: kod bir paroladır, öte yandan disiplin toplumları parolalarla düzenlenir (1992, s.5).

Bireyler kapalı devre kameraları, sosyal medya, büyük veri gibi teknolojiler aracılığıyla sürekli gözetim ve izlemeye tabi tutulmaktadır. Dolayısıyla modernite de karşımıza çıkan fiziksel gözetim postmodern dönemde soyut ve sayısal hale gelmektedir. Bireyler sadece kapalı mekanlarda değil, gündelik hayatlarının her yönünde gözetimde tabi olmaktadır.

Moderniteyi Foucault'un Panoptikonunu "disiplin toplumu" olarak tanımlarsak, Post modern dönemi ise Deleuze'nin deyişiyle "denetim toplumu" (Deleuze, 1992, s. 4) olarak tanımlayabiliriz (Lyon, 2013, s. 131). Disiplin toplumunda gözetim bireysel imza ile topluluk içerisinde yürütülürken, denetim toplumunda algoritmalar, kodlar bunların ikisini de kapsayarak yürütülmektedir (Lyon, 2013, s. 130).

Foucault ve Orwell'ı eleştirerek yeni bir gözetim metaforu ileri süren Haggerty ve Ericson'dur. Haggerty ve Ericson'a göre Orwell, tüm vatandaşların gözetlendiği bir kurgu değil sadece orta ve üst sınıf vatandaşların gözetlendiği, alt sınıfların ise kendi hallerine bırakıldığını dile getirmektedir. Ancak bu toplumun bütününün gözetlendiği fikrini gözden kaçırmak anlamına gelmektedir (2000, s. 606). Foucault ise, onsekizinci ve ondokuzuncu yüzyıl toplum dönüşümlerine odaklanarak çağdaş gözetim teknolojilerini gözardı ettiğinden dolayı yazarlar tarafından eleştirilmiştir (2000, s. 607).

Haggerty ve Ericson'ın "The surveillant assemblage" makalesinde, çağdaş gözetim gelişmelerini analiz etmek için Gilles Deleuze ve Felix Guattari'nin çalışmalarından aldıkları "gözetim topluluğu" kavramını kullanmaktadır (2000, s.605). Gözetim topluluğu, insan bedenlerini kendi bölgesel ortamlarından soyutlayarak parçalanmasından ve sonrasında bir dizi veri akışı sayesinde tekrar birleştirilmesiyle oluşturulmaktadır. Böylece bedenler fiziki özelliklerinin yanısıra "veri çifti" de oluşturmaktadırlar (2000, s.611).

Haggerty ve Ericson Orwell ve/veya Foucault gibi belirli durumlara odaklanmak yerine genel bir gözetim topluluğu ve teknolojilerin birleşimi ile ilgilenmektedir. Çağdaş gözetimin disipliner güçten ziyade yeni teknolojiyle varolan sistemlerin bir bütün halinde bir araya getirme arzusundan kaynaklandığını savunurlar (2000, s. 610). Gözetim teknolojileri Foucault'daki gibi dikey bir hiyerarşiye sahip değildir. Dikey hiyerarşiden ziyade günümüzde gözetim artık çok yönlü ve yatay olarak yapılmaktadır. Tek tek kurumların gözetlenmesinden ziyade tüm toplum bütün olarak gözetlenmektedir.

Haggerty ve Ericson'a göre post panoptik gözetim aşağıdaki bileşenlerden oluşmaktadır;

- 1-Daha önce ayrı olan sistemleri bir araya getirme arzusu tarafından yönlendirilir, bu da gözetim kapasitesinde üstel bir artışa yol açar. Ayrı olan sistemlerin biraraya getirilmesinin bir sonucu olarak da bu sistem hem devlette hem de devlet dışı kurumlarda çalışmaktadır.
- 2-Kontrol, yönetim, güvenlik, kâr ve eğlence gözetimci topluluğu biraraya getirmekte ve harekete geçirmektedir.
- 3- Gözetleme, "işitsel, kokusal, kimyasal, görsel, ultraviyole ve enformasyonel" uyaranların görsel olarak kayıt altına alınmasıyla oluşmaktadır. Tüm bunlar çerçevesinde gözetim makineler aracılığıyla yapılmaktadır.
- 4- Gözetim, insan bedeninin artık fiziksel olarak yer değiştirmesinden ziyade bedeni saf enformasyona dönüştürmekle ilgilenir (2000, s. 609-613).

Genel olarak, Haggerty ve Ericson, gözetimin postmodern toplumlarda nasıl olduğuna dair bir bakış açısı sunmaktadır. Gözetimin artık belirli sınırlar ve kalıplar içerisinde olmadığını dile getiren çalışmalarında, gözetimin artık yeni teknolojiler sayesinde sınırları aştığı, sosyal, kültürel ve ekonomik faktörlerin de etkisiyle sürece çok sayıda aktörün de dahil olduğu bir dinamik bir sistemin parçası olarak görmektedirler. Günümüzde bireylerin bedenlerinin de siber uzayda saf enformasyon olarak yer aldığını vurgulamaktadırlar.

Bir diğer panoptikon sonrası kavram ise Thomas Mathiesen'in Foucault'un disipliner iktidar kavramını tanımlayan panoptikon modeline dayanmaktadır. Mathiesen Foucault'un panoptikonundaki gibi "azınlığın" çoğunluğu izlediği değil, "çoğunluğun" azınlığı izlediği "Sinoptikon" metaforunu tanımlamıştır. Foucault'un panoptikon çizgisinden ayrılmayan Mathiesen gözetimin hem panoptik hem de sinoptik olduğunu dile getirmiştir.

Mathiesen hapisane ile aynı zamanda modern basının da doğduğunu, bu nedenle de hem panoptikonun hem de sinoptikonun 'birbirleriyle yakın etkileşim, hatta kaynaşma içinde nasıl geliştiğini' vurgulamaktadır (Mathiesen, 1997, s.219-223). Modern kitle iletişim araçlarına özellikle de televizyona vurgu yapan Mathiesen televizyonu sinoptikonla özdeşleştirmiştir. Mathiesen'e göre "Modern televizyon, sinoptikon, bizi sessizleştirir..." (1997, s.231). Bir başka deyişle, "çoğunluk, azınlığı izleyip takip etmeye, azınlığın yaşamını kendine göre içselleştirmeye ve onun kontrolünde, onun doğrularını "olması gereken" olarak görerek eylemde bulunmaya başlamaktadır (Demir, 2017, s.60). Böylece; "Ruhun' (Soul) kontrolü ve disiplini, yani özdenetim yoluyla kendini kontrol eden ve böylece sözde demokratik kapitalist topluma düzgün bir şekilde uyan insanların yaratılması, aslında modern sinoptikon tarafından yerine getirilen bir görevdir..."(Mathiesen, 1997, s. 215).

Mathiesen modern kitle iletişim araçlarının bilincimizi nasıl etkilediğini ve yönlendirdiğini vurgulamaya çalışmıştır. Kitle iletişim araçlarına maruz kalmanın bir sonucu olarak bireyler pasifize edilmekte, kapitalist topluma adapte edilmekte ve gözetimi içselleştirmeye koşullandırılmaktadır. Bu nedenle Mathiesen, sinoptikon modelini anlayanın, gözetimin çağdaş toplum üzerindeki etkisini kavramak için çok önemli olduğunu iddia etmektedir.

Doyle, Mathiesen'in internetten ziyade televizyona vurgu yaptığını dile getirmektedir. Bunun nedeni o dönemlerde internetin henüz yaygın olarak kullanılmayışı olarak açıklanmaktadır (2011, s. 286).

Gözetim teknolojileri için geliştirilen bir diğer kavram ise “Süperpanoptikon”dur. Mark Poster tarafından geliştirilen bu kavram, post modern gözetimin modern gözetim biçimlerinden daha kapsayıcı ve karmaşık olduğunu tanımlamak için kullanılmıştır. Süperpanoptikon kavramı da aynı Bentham'ın panoptikon kavramı gibi sürekli gözetim içermektedir ancak gözetim hapishane gibi fiziksel sınırlar içerisinde değil, hem iktidarın önceki teknolojisiyle hem de dijital teknolojinin olduğu her yerde yapılmaktadır. Bu yüzden süperpanoptikon diğer postmodern gözetim teorileri gibi mekandan bağımsız olarak tasarlanmıştır. Bentham/Foucault'un panoptikon kavramını veri tabanı ile birleştiren Poster'a göre;

Gözetlenen kişi, gözetleme için gerekli bilgiyi sağlar. Dikkatle tasarlanmış bir yapıya ihtiyaç yoktur, kriminoloji gibi bir bilim kullanılmaz ve karmaşık bir idari ağıta başvurulmaz, bürokratik bir örgüt kurulmasına gerek yoktur. Süperpanoptikonda, bireyin eylemi telefon hattı aracılığıyla bilgisayarlı veri tabanına iletilindiğinde gözetim sağlanmış olur (1990, s.184).

Süperpanoptikon, veri tabanları aracılığı ile bireyleri gözetlediğinden dolayı, birey Panoptikonun aksine gözetlendiğinin farkında değildir. Süperpanoptikon'da gözetim iki şekilde yapılabilmektedir. Bunlardan ilki, sosyalist devletler tarafından tehdit ve korku unsuru olarak etkin şekilde kullanılan kapsamlı veri tabanı kaydının tutulmasıdır. İkincisi ve günümüzde sıklıkla kullanılan, yetkililerin bireyin kişisel bilgilerinin, faaliyetlerinin ve konumlarının kaydını tutması ve bu verilerin gerektiğinde kurumlarla paylaşması, bu bağlamda kişileri tespit etme ve bulunmasını sağlamaktadır (Badenhoop, 2021, s. 953; Poster, 2018, s. 549).

Bilgisayarlar aracılığı ile işlenen veritabanları bireyi “bölünebilir” hale getirerek, bireye tek bedene dayalı ikincil bir benlik oluşturmaktadır. Poster'e göre, birey denetim toplumlarında etkin ve istekli bir şekilde gözetim sürecine katılmaktadır. Böylece bireyin her hareketi devlet ve kapitalist şirketler tarafından kayıt altına alınmaktadır (2018, s.549). Poster'de Foucault'dan tam bir kopuş görülmemektedir.

Aksine Poster denetim toplumunun disiplin topluluğunun bir devamı olduğunu ancak aynı zamanda değişimi de içerdiğini belirtmektedir.

Panoptikon'un post modern gözetim toplumu için uygun bir metafor olarak yıkıldığını söylenen şey kapatma, tecrit ve eğitim koşullarının değişmesi olarak görülmektedir. Modern dünyada bireyler artık hem ülke içerisinde hem de ülke dışında daha fazla hareket halindedir ve bunun sonucu olarak da bireyler panoptikondaki gibi izole bir yaşam sürmemektedirler. Bu noktada Bauman bütün toplumsal biçimlerin büyük bir hızla çözüldüğünü ve dolayısıyla daha önce sabit sınırlı ve yapısal olan şeylerin akışkanlığını dile getirmektedir (Bauman ve Lyon, 2016 s. 13-14). Lyon'ın "Akışkan Gözetim" olarak nitelendirdiği bu durum eskinin görece katı kurumları yumuşamış, ağların ve yazılımın hakim olduğu bir dünyada şekillenebilir ve hızla o günün koşullarına ayarlanabilir hale gelmiştir (Lyon, 2010, s. 325). Modernitenin de yerinde durmadığını ve akışkanlaştığını belirten Bauman'a göre günümüzde;

Bu katı sabitlik çözülmüş durumda; zira "belki de, her şeyin ötesinde panoptik-sonrası bir dönemdeyiz". Bugünün güç ilişkileri içinde iktidar mekanizmalarını elinde bulunduranlar "herhangi bir anda, bütünüyle ulaşılmaz hale gelebilir, hatta hiç ortalıkta görünmeyebilirler (2016, s. 22-23).

Bauman'ın burada dile getirdiği artık yönetilenlerle iktidarın hiçbir şekilde yüzyüze gelmeyiştir. Mahkumlar ve denetmenlerin karşılıklı bağımlılığı duvarların ortadan kalkmasıyla sona ermiş, iktidar artık değişik teknolojiler sayesinde panoptikonun sınırlarından sıyrılmış ve birçok farklı gözetim teknolojisi ortaya çıkmıştır (Bauman ve Lyon, 2016, s.15). Kontrol ve düzenin sağlanması için ortaya çıkan gözetimin özellikle 1980'lerden sonra şekil değiştirmeye başladığı gözlemlenmektedir. Simetri, izleyen ve izlenenler arasında kurulu olan ve aynı zamanda dağınık ve değiştirilebilir olmayan gözetim, artık panoptikonun sınırlarında çıkıp gündelik hayatlarımızın içerisinde yer almaktadır (Lyon, 2010, s. 327). Gözetim artık, elektronik bir hale gelmiştir. Panoptikon'da oturanlar sürekli olarak izlenme tehdidinin farkındayken internetteki devlet gözetimi artık görünmez olmuştur.

Bauman'ın bir diğer tezi ise, aynı Poster'in savunduğu gibi gözetime bireylerin birer tüketici olarak gönüllü katıldıklarıdır. Bireyler, disiplin edici gözetime maruz

kalmak yerine, giderek daha fazla tüketici olarak oluşturulmakta ve piyasa ekonomisine dahil edilmektedir (Haggerty ve Ericson, 2000, s. 615). Bireyler piyasanın onlara sunduğu birtakım avantajlardan yararlanmak adına tüketici profillerini gönüllü olarak piyasaya vermektedirler. Tüketici pazarlarının cazibesiyle bireyler artık Bentham/Foucault panoptikonunu gerektirmeyecek şekilde kendi bedenlerinin bekçiliğini yapmak üzere eğitilmişlerdir. Nasıl ki salyangozlar evlerini sırtlarında taşıyorsa, modern çağın insanı da kendi kişisel panoptikonlarını sırtında taşımak zorundadır (Bauman ve Lyon, 2016, s. 73-74). Bu postmodern çağın bir gerekliliği olarak sunulmuş ve bu bağlamda da bireylerin bunu içselleştirmesi sağlanmıştır. Bir başka deyişle günümüz dünyasında gözetime birey gönüllü olarak katılmaktadır. Çağın koşullarına ayak uydurmak için birey tüketime yönlendirilmektedir. Ancak birey her gönüllü tüketim yaptığında aslında gözetim sayesinde kayıt altına da alınmaktadır. Dolayısıyla, birey tüketim yaptıkça gözetlenmekte, gözetlendikçe de yeni tüketime yönlendirilmektedir. Sosyal medyada da buna benzer şekilde karşımıza çıkmaktadır. Birey sosyal çevresi tarafından kişisel bilgilerini paylaşmaya teşvik edilmekte, paylaşım yaptıkça da, paylaştığı bilgiler üzerinden daha fazla gözetlenmektedir.

Post modern gözetim teorilerini çoğaltmak mümkündür. Teknoloji, veri akışı, bilgiye ulaşma kolaylaştıkça yeni gözetim teorileri de karşımıza çıkmaktadır/çıkacaktır. Buraya kadar incelediğimiz gözetim teorilerin ortak noktası, Bentham'ın mimarisinden yola çıkarak Foucault'un geliştirdiği Panoptikon modeline dayanmalarındır. Günümüzde gözetim okul, hastane, havaalanları, alışveriş merkezleri gibi yerlerde fiziki olarak devam etmekle birlikte, birbirine bağlı ağlar ve dolayısıyla veriler sayesinde sanal olarak da gerçekleştirilmektedir. Post panoptik teorilerin bir diğer ortak noktaları ise, fiziksel gözetimden ziyade veri gözetimine odaklanmalarındır. Veri artık bireyin olduğu her yerdedir. Yüksek duvarlar veya sınırlardan sıyrılmıştır. Veri gözetimi görece daha soyut olarak karşımıza çıkmaktadır. Dolayısıyla birey gözetlenirken gözetlendiğinin dahi farkında değildir. Ayrıca modern gözetim teorilerinde iktidar merkezde yer alırken, post modern gözetim teorilerinde aktörler çeşitlenmiştir. Devlet modern gözetim teorilerinde merkezi bir konumdayken, günümüzde ve siber uzayda özel şirketler, devlet ve bireyler üzerinden gözetim

yapılmaktadır. Aktörlerin çeşitlenmesinin getirdiği bir diğer sonuç ise gözetimin post modern teorilerde gücün toplum içerisinde çeşitli aktörler arasında nasıl dağıldığına odaklanarak aşağıdan yukarı bir yaklaşım benimsenmektedir.

Modernizmde sistematik olarak ortaya çıkan ve sonrası post modern dönemde de artarak devam eden gözetim olgusu ve gözetim metaforlarını anlamak ve açıklamak bireylerin özel hayatının gizliliğinin nasıl ve ne şekilde ihlal edildiğini kavramamız bakımından önem arz etmektedir. Çağın gerekliliğine ve kullanılan teknolojileri de ele alarak geliştirilen gözetim metaforları günün koşullarına yönelik detaylı bir toplumsal analiz yaparken, aynı zamanda da bireyin bu toplum içerisinde yaşadığı gözetim sarmalını bizlere açıklamaktadır. Gözetimi tanımlamak için kullanılan metaforların, bireyi izleme ve kontrole yönelik toplumsal tutumları hem yansıttığı hem de şekillendirdiği görülmektedir. Ayrıca, bu teknikler insanların günlük yaşamlarında nasıl gözetim altında tutulduklarına dair perspektifler sunabilmektedir.

Modernizmde yüzyüze veya fiziksel ortamlarda yapılan gözetim, post modernizmle birlikte siber gözetimi de beraberinde getirmiştir. Bu sebeple yüzyüze veya fiziksel gözetim terkedilmemiş aksine siber gözetim teknolojileriyle birleşerek bireyler hatta gruplar açısından daha geniş gözetim uygulamalarına yol açmıştır. Siber gözetim artık sınırları ortadan kaldırmış ve bilgi işlem ve yazılımı kullanılarak dijital bilgileri bir başka deyişle verileri toplayarak bireyin hayatına müdahil olmuştur. Siber gözetimin yükselişiyle birlikte, fiziksel alanın geleneksel sınırları bulanıklaşmış ve bireylerin özel hayatın gizliliği hakkını, ifade özgürlüğünü ve gözetim korkusu olmadan bilgiye erişme ve bilgiyi paylaşma becerisini etkilemeye başlamıştır.

Siber gözetimi yeni olarak karşımıza çıkaran şey ise, teknolojinin gelişimi dolayısıyla bireylerin interneti kullanma şeklidir. Özellikle hayatımızın her alanına nüfuz eden internet sadece iletişim aracı olmaktan çıkmış, eğlence, sağlık, iş başvurusu, alışveriş, tüketim ve hatta coğrafi konumumuzu bile bildirdiğimiz bir alan olarak hayatımızın bir parçası olmuştur. Tüm bu gelişmeler çerçevesinde de gözetim ile elde veriler çoğalmış ve çeşitlenmişlerdir (Bernal, 2016, s. 244-247). Tıpkı Haggerty, Ericson, Deleuze ve Guattari'nin bahsettiği gibi bireylerin, toplulukların attıkları her adım bireylerle birlikte adeta veri çiftine dönüşmüştür. Gözetim hem niteliksel olarak hem de niceliksel olarak değişmiştir. Yıldız'a göre; "Gözlenebilir

olanın ve fiziki gözetimin ötesine geçen, insanların daha az sorguladığı daha derinlemesine “deri altı” bir gözetim ve takip süreci hız kazanmıştır (2022, s.16). Bedenlerimiz bir taraftan fiziki olarak gözetlenirken, diğer taraftan bedenlerimiz üzerinden sanal veriler oluşturulmuştur.

Oluşturulan veri çiftleri veya sanal bedenler her zaman hayatımızı olumsuz şekilde mi etkilemektedir? Bu konuda iki farklı görüş karşımıza çıkmadır. Bu görüşlerden ilki güvenlik-özgürlük ikilemi bağlamında gözetimin özelde bireyler genelde toplum için yararlı olduğu, bir diğeri ise gözetimin özel hayatın gizliliğinin sonunu getirdiği görüşüdür. Dolayısıyla birinci tezde gözetim toplum tarafından meşru olarak kabul edilirken, ikinci tez de bireyin bilgisi olmadan birey hakkında veri toplamak özel hayatının gizliliği hakkının ihlali veya sonu olarak tanımlanmaktadır.

Özellikle 11 Eylül saldırıları, zaten varolan gözetim uygulamalarına yasal dayanak hazırlamıştır. Bu meşrulaştırma eyleminin en büyük nedeni güvenlik olarak karşımıza çıkmaktadır. Mathiesen’in belirttiği gibi çoğunluğun azınlığı izlemesi bir başka deyişle halka 11 Eylül saldırılarını bildirmek için medyanın kullanılması sinoptikon etkisi doğurmuş ve bireylerin bu ikilemi içselleştirilmesi sağlanmıştır. Bireyler bir taraftan güven içerisinde hayatlarını idame etmek isterken, diğer taraftan da özel hayatlarının gizliliğinin bir kısmından gönüllü olarak vazgeçmektedirler. “Birinden ne kadar çok varsa diğerinden o kadar az vardır” (Bauman ve Lyon, 2016, s. 53). Ancak bu özgürlük-güvenlik ikilemi bağlamında siber gözetimi meşrulaştırmayı sadece 11 Eylül saldırılarına bağlamak Bauman ve Lyon’a göre yanlış olur. Bu durumu şu şekilde dile getirmişlerdir;

...güvenlik mekanizmalarını "birbirine bağlayan" şey "Öteki'ne duyulan korku"dur...Öteki komşumuzdur, yanımızdan geçen biridir, aylaktır veya bizi takip eden biridir; sonuçta her yabancı Öteki'dir. Ama bu durumda, hepimizin de bildiği gibi şehirde yaşayanlar birbirine yabancıdır ve hepimizin tehlikeli olduğundan şüphelenilebilir; bu yüzden de hepimiz uçuşan, dağılan ve bilinmeyen tehlikelerin, bir "olağan şüpheliler" kümesi altında toplanıp sıkıştırılmasını bir dereceye kadar istiyoruz. Bu toplama sayesinde tehlikenin uzakta tutulacağını ve aynı zamanda da bu toplamanın bizi tehlikenin bir parçası olarak sınıflandırılma tehlikesinden koruyacağını umuyoruz (Bauman ve Lyon, 2016, s.118).

Bauman ve Lyon'un söylemlerinden de görüldüğü üzere, siber gözetim aslında sadece 11 Eylül terör saldırısından sonra meşrulaştırılmamış, aslında varolan ancak gizliden gizliye yapılan gözetimi meşrulaştırmıştır. Toplumdaki bireylerin öteki hakkında duyduğu şüphe, ötekinin bilinmemesi ve tehlikelerden korunma arzusu bireyin güvenlik adına kendi haklarının bir kısmından feragat etmesini beraberinde getirir. Hobbes'un Toplum sözleşmesi gibi birey yine kendi güvenliği için birtakım haklarından feragat ederek bunu iktidara gönüllü olarak devretmek zorunda kalmıştır. Dolayısıyla güvenlik için gözetim uygulamalarını kabul eder hale gelmiştir. Bunun en büyük örneğini kapalı devre televizyon kameralarını içselleştirerek ve olağanmış gibi kabul ederek yaşadığımız toplumlarda görmekteyiz. Sokaklarda, caddelerde, okullarda ve hatta kamusal alanların büyük bir çoğunluğu bu kameralarla donatılmıştır. Ancak birçoğumuz bu kameraların bizim güvenliğimiz için olduğunu düşünerek sorgulama ihtiyacı duymayız. Bu veriler bireylerin güvenliği ve toplumda olası terör saldırılarına yönelik önleyici olarak mı kullanılmaktadır? Yoksa her bir bireyi gözetim altında tutarak bireyler hakkında veriler mi toplamaktadır? sorularını aklımıza getirebiliriz. Her ne koşulda olursa olsun bu iki sorunun da cevabı evet olarak karşımıza çıkmaktadır. CCTV kameraları kolluk kuvvetleri tarafından toplumun huzuru ve düzenini sağlama açısından hem denetimi kolaylaştırmaktadır hem de şüpheli görülen davranışlar sayesinde kolluk kuvvetlerinin olaya anında müdahale etmesini sağlamaktadır. CCTV kameraları sayesinde suç oranının belirli bir oranda düşürülmesi (panoptikon etkisi) sağlansa da, aynı zamanda bu kameralar sayesinde kitlesel gözetim yapıldığı da görülmektedir. Kitlesel gözetim sadece otorite ülkeler tarafından değil, İngiltere gibi gelişmiş ülkelerde de karşımıza çıkmaktadır. Örneğin, CCTV kameralarının en yoğun olarak kullanıldığı şehirlerden biri olan Londra'da 942.000 CCTV kamerası bulunmaktadır. Dünya geneline baktığımızda ise özel işletmelerin kendi CCTV kameraları hariç bu sayının sekiz yüz milyon olduğu belirtilmektedir (Wise, 2022). Sekiz yüz milyon kamera büyük veriyi de beraberinde getirmektedir. Toplumu sürekli olarak CCTV kameraları sayesinde izleyen bir Büyük Birader metaforu, bireyi uygunluk, dahil etme, erişim, şüphe ve ayrıcalığı belirleyen belirli kriterlere göre kategorize etmekte ve düzenlemektedir (Henschke ve vd., 2021, s.108). Böylece bireyler çeşitli kodlar altında kategorilere bölünüp sınıflandırılmaktadırlar.

Sonuç olarak, özel hayatın gizliliğinin ihlali de kişisel güvenlik açısından ödenmesi gereken adil bir bedel olarak kabul edilmektedir (Lichinitzer ve Snir, 2022, s. 1190).

CCTV kameralarının yaygın olarak kullanımının yanısıra, CCTV kameralarına ses eklenmesi hem görsel hem de işitsel gözetimi karşımıza çıkarmaktadır. Görsel gözetim çerçevesinde günlük hayatımız içerisinde maruz kaldığımız biyometrik gözetimin özellikle kolluk kuvvetleri tarafından kullanıldığı görülmektedir. Biyometri, kimlik belirleme aracı olarak insan vücudunun farklı bileşenlerinin (Ses, DNA, vb.) ölçümlerini kullanmaktadır (Akt: Nunn, 2001, s. 262). Biyometrik gözetim ise, bireylerin parmak izleri, yüzler, iris desenleri veya sesler gibi fiziksel ve/veya davranışsal özelliklerine dayalı olarak gerçekleştirilmektedir (Kloppenburger, S., & Van der Ploeg, 2020, s. 57). Biyometrik gözetim Haggerty ve Ericson'un da ifade ettiği gibi bedeni saf enformasyona dönüştürmektedir. Çünkü bu tür bir gözetim bireyin fiziksel bir temsilinin dijital bir ortama 'aktarmak' için dijitalleştirilmiş şablonu olarak karşımıza çıkmaktadır.

Günümüzde biyometrik gözetim sınır kapıları, bankalar, Avrupa'da Schengen Vize Sistemi ve Vize Bilgi Sistemleri gibi alanlarda oldukça yoğun olarak kullanılmaktadır. Ayrıca akıllı telefonlar için biyometrik özelliklerinin geliştirilmesiyle bu gözetim türünün ivme kazandığı görülmektedir. Klasik biyometrik yöntemlerin (ses, yüz tanıma, iris, vb.) kullanılmasının yanısıra cep telefonlarında kullanılan ekran kaydırma şekli, dinamik imza ve yürüyüş tanıma gibi insanların siber uzaydaki davranışlarını da içeren yöntemleri kapsamaktadır (Snijder, 2016, s.6).

Gözetim başlı başına tartışmalı bir alanken biyolojik gözetimin hayatımıza bu kadar entegre olması özel hayatın gizliliği hakkı açısından da tartışmaları beraberinde getirmektedir. Biyolojik gözetimde bireyler yürüyüşleri, yüz şekilleri gibi fiziksel özellikleri kullanılarak veya din, dil, ırk olarak kategorilere ayrıştırılabilmektedir. Bireylerin bu şekilde belirli fiziksel özelliklerinin kullanılıp ayrıştırılması özünde insan haklarına aykırıdır. EİHB'nin 2. Maddesi: "Herkes; ırk, renk, cinsiyet, dil, din, siyasi ya da başka inançlarına bakılmaksızın eşit haklara sahiptir" demektedir. Dolayısıyla bu gözetim türü ile bireyin kategorilere ayrılması, bireyin kamusal alanlarda ayrıştırılmasına, azınlıklar bağlamında veya kişinin fiziksel özellikleri çerçevesinde ayrımcılığa hatta dışlanmaya neden olabilmektedir. Bunun yanısıra yüz

tanıma sistemlerinde görülen hatalar da bu gözetim türündeki endişeleri arttırmaktadır. Veri tabanının bireyleri yanlış şekilde eşleştirilmesi ve kodlanması geri dönülemez hatalara neden olabilmektedir. Örneğin, “İngiltere’de Londra Polisi 2018 ve 2019 boyunca yüz tanıma denemeleri yapmış, polis kontrollerinde durdurulan 42 kişiden sadece sekizi’nin arandığı doğru olarak belirlenebilmiştir” (Aktaran: STM Teknolojik Düşünce Merkezi, 2021, s. 9).

Dolayısıyla yanlış eşleştirme yüzünden yapılan hatalar masum olan kişinin itibarını zedelemekte ve hatta özgürlüğünü de elinden alabilmektedir. Bir diğer tartışmalı alan ise bu tür bilginin bireyin anonimliğini kaldırmasıdır. Bu da bireyin kişisel verilerine erişilebilir olup, birey adına birçok işlem yapılabilmesine neden olmaktadır. Dahası özellikle bankacılık sektöründe biyometrik verilerin kullanılması bireyler açısından risk oluşturabilmektedir. Örneğin; “Yapılan araştırmalarda genellikle güvenli bulunan bu sistemlerin, canlı bir yüz yerine yüzün basılı bir görüntüsünün veya çalıntı biyometrik özellik dosyalarının kullanılması gibi yöntemlerle yanıltılabileceğini göstermektedir (Aktaran:STM Teknolojik Düşünce Merkezi, 2021, s. 10). Örneklerden de görüldüğü üzere biyometrik gözetim ile elde edilen verilerin bireyin rızası dışında alınması, üçüncü tarafların eline geçme olasılığı ve ne amaçla kullanıldığı şeffaf olmadığından dolayı özel hayatın gizliliği hakkı açısından ihlalleri de beraberinde getirmektedir.

İşitsel gözetim, güvenlik, soruşturma veya istihbarat toplama amacıyla elektronik cihazlar kullanılarak ses dalgalarının izlenmesi ve kaydedilmesi süreci olarak ifade edilebilir. Bu tür bir gözetim telefon dinleme (telefonlara takılan mikrofonlar), internet üzerinden ses protokolü ve odalara yerleştirilen dinleme cihazları (mikrofon, böcek vb) gibi araçlar aracılığıyla yapılmaktadır. Birey dinlendiğinin farkında değildir. Diğer gözetim türleri gibi gizli olarak yapılan bu gözetim bireyin özel hayatın gizliliği hakkına tehdit oluşturmaktadır. William Blackstone, işitsel olarak yapılan gizli gözetimin bir genel hukuk suçu olduğunu belirtmiş ve bunu "duvarların veya pencerelerin altını ya da bir evin saçaklarını dinlemek, konuşmalara kulak kabartmak ve bunun üzerine iftira ve tehlikeli hikayeler uydurmak" olarak tanımlamıştır (Aktaran: Solove,2006, s.492). Bu gözetim tekniği, üçüncü şahıslar tarafından kötüye kullanılmaya açık olabilecek, kişiler veya kuruluşlar

hakkında onların bilgisi dışında hassas ve gizli bilgiler toplamak için kullanılabilir. Blackstone'un da "iftira ve tehlike hikayeler uydurmak" diyerek vurgulamak istediği budur. Örneğin; bireylerin özel konuşmalarının geniş çapta izlenmesine yol açarak potansiyel olarak kişisel ve profesyonel ilişkilerini tehlikeye atabilir veya bireyi çeşitli sınıflandırmalar içerisine sokarak kategorize edip fişleyebilmektedir. Dahası bireylerin iletişimini keserek özel hayatın gizliliği hakkının bir parçası olan haberleşmeyi ihlal edebilmektedir.

Görsel ve işitsel gözetimin yanısıra internet gözetiminin yükselişi, siber gözetim alanını daha da genişletmiş ve siber gözetimi kapsamlı bir veri toplama alanına dönüştürmüştür. İnternet tabanlı gözetimin yaygınlığı, internetin sunduğu küresel erişilebilirlik, internete kolay müdahale, düşük maliyet ve geniş veri toplama kapasitesinin bir sonucu olarak artmıştır. İnternet üzerinden gözetleme, içeriğe bakılmaksızın bir bireyin iletişim faaliyetleri hakkında daha fazla bilgi toplama potansiyeline sahiptir. Bu tür bir gözetim aynı zamanda içeriğe erişim sağlayabilen geleneksel telefon dinleme yöntemlerine göre daha kolay erişilebilirdir (Bernal, 2016, s.252).

Teknolojik cihazlar gelişmekle ve çeşitlenmekle kalmamış aynı zamanda gözetim yapmak isteyen aktör sayısı da çoğalmaktadır (Richards, 2013, s.1936). Büyük ve küçük ölçekli özel şirketler, kişisel verilerin toplanması, kullanılması ve satılmasından büyük gelirler elde etmektedir. Örneğin, görünüşte ücretsiz olarak bize sunulan reklamlar, İnternet kullanıcılarının aslında tüketici davranışlarını okuma ve tüketim davranışlarını kategorize etmektedirler (Richards, 2013, s.1938). Bu durumun bir sonucu, istihbarat örgütlerinin bireysel hedeflerden tüm topluluklara kadar tüm dijital iletişim düzeylerinde kapsamlı izleme yapabilmelerine olanak sağlaması olarak karşımıza çıkmaktadır. Bir diğer sonucu ise, hükümetler ya da şirketler gibi büyük ve güçlü kurumlar tarafından kullanılan aynı ağın çok daha az güce sahip bireyler ya da gruplar tarafından da kullanılabilmesidir. (Lyon, 1997, s.36). Günümüzde yaygın olarak kullanılan sosyal medya platformlarında kullanıcıların eğilimleri, tercihleri ve davranışlarını ortaya çıkarmak için büyük miktarda verinin toplanmasını ve analiz edilmesini içeren veri madenciliği kullanılmaktadır. Örneğin sosyal medya siteleri, kullanıcıların profillerini oluşturmak ve kullanıcıları ilgili reklamlar veya içeriklerle

potansiyel bir tüketime yönlendirmek için kullanıcıya yönelik gönderiler, beğeniler, paylaşımlar ve kişisel veriler gibi muazzam miktarda kullanıcı verisi toplamaktadır. Bunun yanı sıra özel şirketler ve hükümetler olası riskleri belirlemek, istihbarat toplamak veya ilgili kişileri izlemek için bireyin sosyal medya platformunda paylaştığı gönderileri, yorumları ve mesajları izleyebilir. Toplanan verilerin üçüncü şahısların eline geçmesi veya büyük ölçekli şirketler tarafından kötüye kullanılması veya satılması özellikle özel hayatın gizliliği hakkını derinden etkilemektedir. 2018 yılında yaşanan Cambride Analytica Skandalı bu duruma örnek oluşturmaktadır. Cambridge Üniversitesi araştırmacısı Aleksandr Kogan tarafından yazılan "This Is Your Digital Life" isimli kişilik testi uygulaması sayesinde teste katılanların ve teste katılan bireylerin Facebook'taki arkadaşlarının kişisel bilgileri bireylerin haberi olmadan toplanmış ve ilgili şirket tarafından Donald Trump'ın seçim kampanyasında kullanılmak üzere toplanmıştır. Aslında 270.000 kullanıcı sadece testi çözerken, Facebooktaki arkadaşlarının da verilerine erişmesi söz konusu olunca bu sayının elli milyon kişiyi bulduğu görülmektedir (Tüfekçi, 2018). Görüldüğü üzere internette çözülen basit bir test, özel hayatın gizliliği hakkının ne şekilde ihlal edildiğine dair kapsamlı örnek oluşturabilmektedir.

Modernizmle birlikte yükselişe geçen ancak postmodern dünyadaki teknolojik gelişmelerle birlikte doruk noktasına ulaşan siber gözetim özel hayatın gizliliği hakkını açıkça ihlal etmektedir. Bireylerin siber gözetimle birlikte veri çiftleri ve enformasyon bağlamında kodlanıp, kategorilere ayrılması, bu tür bilgilere yetkisiz erişim veya yetkili kurumlar tarafından bireyin özel hayatına yapılan ihlaller açıkça görülmektedir. Gözetim sürecinin doğası gereği şeffaf olmaması, özel şirketlerin ve bireysel aktörlerin de bu alana dahil olması birey açısından riskleri de beraberinde getirmiştir. Öncelikle birey kategorilere ayrılarak kodlanmış ve siber uzayda insani özelliklerini yitirmiştir. Kodlar üzerinden konuşulan bireyler artık algoritmalar aracılığıyla kodlanan, istenildiğinde parçalanan, istendiği zamanda alt kodlara ayrılan sanal kimlikler haline dönüşmüştür. Özgürlük-güvenlik ikilemi çerçevesinde aynı Deleuze'un dediği gibi günümüz toplumları artık "disiplin toplumlarından" denetim toplumlarına geçiş yapmıştır.

3.1.2. Siber İstihbarat

Teknolojinin gelişmesi ve eklenerek büyümesi sonucu siber tehditlerin hem miktarında hem de çeşitliliğinde büyük bir artış olduğu görülmektedir. Bu da devletleri kendi önlemlerini almaya yöneltmiştir. Saldırıların ne zaman ne şekilde olduğu veya olacağı bilinmediğinden dolayı devletlere yönelik potansiyel tehlikeleri önleme veya bir sonraki adımı tahmin etme adına devletler siber istihbaratı etkili şekilde kullanma yoluna gitmişlerdir. Devlet bu yolla hem bekasını hem de vatandaşlarının güvenliğini korumak amacı gütmektedir. Bu yönden bakıldığında siber istihbarat etik bir olgu olarak karşımıza çıkmaktadır. Ancak uygulamadaki orantısızlık, gerekli olmadığı halde birçok verinin toplanması ve kategorize etme, istihbaratın oynayabileceği önemli ve etik rol ile sınırsız kullanımının gereksiz zarara yol açma potansiyeli insan hakları bağlamında ihlalleri de beraberinde getirmektedir.

Bir süreç olarak istihbarat verilerin toplandığı, işlendiği ve nihai olarak gerekli mercilere iletildiği bir döngüden oluşmaktadır. Veriler için herhangi bir ücret ödenmesine gerek yoktur. Çünkü devletler ve şirketler için veri bireylerdir. Bu veriler kaçınılmaz olarak bireylerin günlük hayatından beslenmektedir. Dünya üzerinde online platform kullanan her bireyin veri çifti veya dijital parmak izi bulunmaktadır. Bu parmak izleri sayısız veri noktası aracılığıyla kullanıcıyı tanımlamakta ve teknoloji ile her etkileşime girdiğimizde daha ayrıntılı hale gelmektedir. Örneğin web sitelerinden alışveriş yaptığımızda, okullarda, havaalanında, cep telefonu kullandığımızda ve hatta yüz yüze alışveriş yaptığımızda dahi bu verilere kolaylıkla erişilmesi mümkündür. Bu tür verilerin yeterli sayıda kişiden toplanması ve aranabilir bir veri tabanında çapraz referanslandırılmasıyla, bir bireyin hem ne yaptığını hem de ne yapmaya niyetli olduğunu anlamak ve bunun bir tehdit olup olmadığını belirlemek de olasıdır (Bellaby, 2016, s.302). Ayrıca Facebook, TikTok ve Twitter gibi sosyal medya platformlarının çoğunun mobil uygulamaları, coğrafi konum verilerini, fotoğraf ve videoları, kişileri, cihaz ve tarayıcı türünü, beğenileri, tweetleri ve hatta kullanıcıların akışlarında gezinirken reklamlarda veya karşımıza çıkan gönderilerde ne kadar süre durakladıklarını toplamak için kullanılmaktadır. Özellikle TikTok platformu Facebook ve Twitterdan kullanıcıya dair daha fazla bilgi topladığı bilinmektedir. Örneğin biyometri ve diğer uygulamalardan kullanıcı adları ve şifreler

de dahil olmak üzere bir cihazın panosuna kopyalanan her şeyi toplamaktadır. Google ise bir Gmail kullanıcısının gönderdiği ve aldığı her e-postanın içeriğini taramaktadır (McLaughlin, 2023).

İletişim ağlarının küresel olarak yayılımı hem devletlere hem de şirketlere coğrafi olarak daha kapsamlı siber istihbarat için yeni olanaklar sunmuştur. Ayrıca siber istihbarat esnasında yapay zekanın kullanılması küresel ağlar çağında istihbarat servislerinin giderek daha fazla verinin toplanmasına ve veri kategorizasyonuna olanak sağlamaktadır. ABD Ulusal Güvenlik Ajansının (NSA) bireyler hakkında gizlice topladığı bilgiler 2013 yılında Edward Snowden tarafından ortaya çıkarılınca siber istihbaratın aslında ne kadar büyük ve kapsamlı şekilde yapıldığı da ortaya çıkmıştır. Bir başka deyişle bireyin başkaları ile paylaşmak istemediği bilgilerin özel şirketler tarafından devlet kurumuna ne şekilde aktarıldığı alenen ortaya çıkmıştır.

11 Eylül saldırılarından bu yana ABD istihbarat teşkilatları hem kendi vatandaşları hem de yabancı uyruklular hakkında bilgi toplama ve araştırmayı önemli ölçüde artırmıştır. İstihbarat faaliyetleri her ne kadar 11 Eylül saldırıları ardından hız kazanmış gibi gösterilse de temeli Soğuk Savaş dönemine kadar uzanmaktadır. Kamuoyu tarafından en yaygın olarak bilineni ve en eskisi ise ECHELON sistemidir. Devletlerin baş harflerinden oluşan “UKUSA” olarak da bilinen gizli anlaşma kapsamında kurulmuş olan ECHELON’a taraf devletler Birleşik Krallık, ABD, Kanada, Avustralya ve Yeni Zelanda ittifakı aynı zamanda “Beş Gözler İttifakı” olarak da bilinmektedir. 1996 yılından bu yana, küresel telekomünikasyon sistemlerinin otomatik olarak gözetimi öncelikle Amerika Birleşik Devletleri ve İngilizce konuşan müttefiklerinin sinyal istihbarat kurumları tarafından gerçekleştirilmektedir (Campbell, 2000, s.149). ECHELON istihbarat operasyonu çok büyük miktarda iletişim bilgilerini ele geçirerek ve ayırım gözetmeksizin hepsini toplayarak, Memex gibi yapay zeka yardımcılarını kullanarak değerli olanları ayıklayarak çalışmaktadır. Bunu yaparken de Sinyal İstihbarat tekniğinin bir alt bileşeni olan COMINT (Communication Intelligence) istihbarat toplama tekniğinden yararlanmaktadır (Mombelli,2014, s.10).

ECHELON istihbarat operasyonunun özel hayatın gizliliği hakkını ihlal ettiği kaçınılmaz bir gerçektir. Çünkü bireyin bilgileri hiçbir kıstas gözetilmeden

toplanmaktadır. Burada ne kamu yararı ne orantılılık gibi ölçütler yer almaktadır. ECHELON istihbaratının nasıl ihlalde bulunduğunu ve durumun vehametini Kanada “İletişim Güvenliği Kuruluşu” eski çalışanı Mike Frost şu sözlerle dile getirmiştir:

Bir kadın bir gece önce okulun düzenlediği gitmişti ve oğlu da gösteride yer almaktaydı. Oğlunun gösteride başarısız olduğunu düşünüyordu. Ertesi sabah arkadaşıyla telefonda konuşurken arkadaşına şöyle bir şey söyledi: 'Danny dün gece gerçekten bombalandı'. Bilgisayar bu konuşmayı çıkardı. Bilgisayarı inceleyen analist konuşmanın neyi kastettiğinden pek emin değildi, bu yüzden de ihtiyatlı davranarak o kadını ve telefon numarasını olası bir terörist olarak veri tabanına kaydetti (Matney, 2015).

Görüldüğü üzere bir anne kullandığı tek bir kelimeden dolayı uluslararası istihbarat ağında terörist olarak kodlanmıştır. Bu duruma yönelik bir çalışma Raso vd.’nin 2018 yılında “Yapay Zeka ve İnsan Hakları: Fırsatlar ve Riskler” isimli araştırmalarında da ele alınmıştır. Çalışmada altı başlık belirlenmiş “Ceza Adaleti (risk değerlendirmeleri), Finans (kredi puanları), Sağlık hizmetleri(teşhis), İçerik Moderasyonu (standartların uygulanması), İnsan Kaynakları (işe alma ve işe yerleştirme) ve Eğitim (deneme puanlaması)” ve bu alanların insan hakları üzerine etkisini değerlendirilmiştir. Araştırma sonucunda ise altı başlıktan olumsuz olarak etkilenen tek hakkın olarak özel hayatın gizliliği hakkı olduğu görülmüştür. Bunun nedeni; yapay zeka teknolojilerin gerçek kişiyi tanımlamadan bireye ait verileri topladıktan sonra bireyin özel hayatı ile ilgili tahminlerde bulunması ve bunlara göre hareket etmek için kullanılan öngörüler üretebilmesi olarak karşımıza çıkmaktadır.

Yukarıda annenin uluslararası arenada “terörist” olarak kodlanması da bu çalışmayı destekler niteliktedir. Yanlış kodlanma sonucu birey doğrudan gözetime maruz bırakılarak, iletişim verileri dinlenerek özel hayatı büyük ihtimalle ihlal edilecektir. Bu durum bireyin seyahat özgürlüğüne bir kısıtlama getirebileceği gibi, herhangi bir yasal işlem yaparken karşısına çıkması muhtemel olarak görünmektedir. Görüleceği üzere algoritmaların bireyi yanlış kategorize etmesi bireyin özel hayatının büyük ölçüde ihlal edilebileceği anlamını taşımaktadır.

ECHELON istihbaratını sadece genel kitlesel gözetim bağlamında ele almak da eksik değerlendirmeye neden olabilir. Bunun nedeni, ECHELON istihbaratının NSA'nın Amerikan vatandaşları üzerinde casusluk yapmasına izin verilmemesidir. NSA'nın temel önceliği, yabancı güçlerden ve ülkenin güvenliğine tehdit oluşturan kişilerden sinyal istihbaratı toplamaktır (Brown, 2003, s.198). Bu noktada da karşımıza özel hayat bağlamında ikinci bir risk çıkmaktadır. ECHELON aynı zamanda ulusal ve uluslararası mevzuattan bağımsız olduğu için bireyleri tehdit etmektedir. Örneğin vatandaşı olunmayan bir ülkede birey hangi yasal koruma altında olacaktır? Birey tutuklansa onu koruyacak kanunlar var mıdır? Az önce de belirttiğimiz gibi ECHELON ulusal ve uluslararası mevzuattan bağımsız olduğu için bu iki sorunun da cevabı hayır olarak karşımıza gelmektedir. Bu durumda da birey, sistemin o durumdaki hatta o günkü insafına kalmış görünmektedir.

NSA'nın belirli verileri toplamak ve depolamak için iki ayrı program kullandığı görülmektedir. Bunlardan ilki XKeystore programı diğeri ise PRISM programıdır. XKeystore programı özellikle e-postaları ve internette yapılan neredeyse her şeyi toplayıp saklamaktadır. NSA, XKeystore adlı programın internetten istihbarat geliştirmeye yönelik "en geniş kapsamlı" sistemi olduğunu belirtmektedir. SIGINT tekniği ile verileri toplayan bu program hedef kişisi yalnızca ABD vatandaşı ise, Yabancı İstihbarat Gözetim Yasası (Foreign Intelligence Surveillance Act-FISA) kapsamında izin alması gerekmektedir. Ancak ABD vatandaşı olmayan bireyler için bu izin gerekli değildir (Greenwald, 2013). Ancak bu izin alınmadan dahi birçok bireyin verilerinin alındığı Snowden tarafından dile getirilmiştir. Snowden 2014 yılında yayımlanan bir televizyon röportajında XKeystore programını şu şekilde tanımlamıştır.

Diyelim ki büyük bir Alman şirketine çalışıyorsunuz ve ben bu ağa erişmek istiyorum, bir forumdaki bir web sitesindeki kullanıcı adınızı takip edebilirim, gerçek adınızı takip edebilirim, arkadaşlarınızla olan ilişkilerinizi takip edebilirim ve parmak izi adı verilen, size özgü bir ağ etkinliği oluşturabilirim, yani dünyanın neresine giderseniz gidin, kimliğinizi gizlemek isterseniz dahi her yerde size erişebilirim (Hubert,2014).

Snowden'ın açıklamaları XKeystore programının dünyanın neresinde olursanız olun verilerinize internet üzerinden her şekilde erişilebildiğinin göstergesi olarak karşımıza çıkmaktadır. Bu kadar muazzam şekilde yapılan siber istihbarat faaliyetinin istisnasız özel hayatı ihlal ettiğini söylemek yanlış olmayacaktır.

İkinci bir program olan PRISM ise Facebook gibi sosyal medya sitelerini izleyerek ve e-postaları toplayarak istihbarat verileri toplamaktadır. Bahsi geçen program verileri e-posta, sohbet, videolar, fotoğraflar, depolanan veriler, VOIP, video konferans ve çevrimiçi sosyal ağ ayrıntıları gibi verileri dokuz ABD şirketinin (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube ve Apple - "Prism Sağlayıcıları") internet sunucularından sağlamaktadır (Anderson, 2015, s. 330) PRISM programı da aynı XKeystore gibi daha çok ABD vatandaşı olmayan bireyleri hedef almaktadır. Bireylerden PRISM programı tarafından toplanan veri türleri daha sonra otomatik olarak kategorilere ayrılarak, ihtiyaç duyulduğu anda kullanılmak üzere depolandığı bilinmektedir. Her şirketten toplanan verilerin kapsamı ve niteliği farklı olduğu da görülmektedir. PRISM istihbarat programının bireyler açısından taşıdığı risk, şirketlerin sunucularına doğrudan erişmesine izin vermesinden kaynaklanmaktadır. Dolayısıyla tarafların rızasına veya iznine gerek yoktur. Bu da programın NSA destekli olduğunu bizlere göstermektedir. Snowden ifşaatından sonra Eski ABD başkanı Obama NSA destekli bu istihbarat programlarının ABD vatandaşları için gerekli olduğunu şu sözlerle dile getirmektedir: "Yüzde yüz güvenliğe sahip olup aynı zamanda yüzde yüz mahremiyete ve sıfır rahatsızlığa sahip olamazsınız," (Kleinman, 2013). Daha önceki bölümlerde dile getirdiğimiz üzere birey burada özgürlük ve güvenlik ikilemi arasında tercih yapmak zorunda bırakılmış ve devletin güvenliği yine bireyin özel hayatının önünde tutulmuştur. Aslında Edward Snowden tarafından da gün ışığına çıkarılan özel hayatın gizliliğini koruyan kapsamlı bir mekanizma olmadığı ve devletlerin ulusal güvenlik politikalarının insan hakkından üstün tutulduğudur. Özel hayatın gizliliğini koruyan mekanizmalar yetersiz olduğundan dolayı da istihbarat örgütleri özel şirketlerle iş birliği yaparak bireylerin haklarını kolaylıkla ihlal etmektedirler.

Günümüzde siber istihbaratta devletler veya özel şirketler yapay zekadan da yararlanmaktadır. Açık kaynak istihbaratı veya OSINT, belirli bir işleve hizmet etmek

için halka açık, yasal veri kaynaklarından bilgi toplama işlemlerini ifade eder. Bu açık kaynaklardan bazıları sosyal medya, bloglar veya haberler olabilmektedir. Bir başka deyişle aslında bir Google araması yapmak basit bir OSINT biçimi olarak karşımıza çıkmaktadır. OSINT sıradan bir internet kullanıcısı tarafından yapılabildiği gibi profesyoneller tarafından da yapılabilmektedir. Bunun nedeni binlerce çevrimiçi kaynağın kolaylıkla ve aynı anda taranabilmesidir. Ancak teknolojinin gelişmesiyle birlikte OSINT’te gelişmiştir. OSINT sadece veri tabanlarından bilgi aramakla sınırlı değildir. Bunun yerine OSINT için özel yazılımlar geliştirildiği görülmektedir. Bu yazılımlardan bazıları 'SpiderFoot', 'Recon-ng', 'Maltego' ve 'Spyse'dir. Örneğin SpiderFoot, web sitesinde kendisini " IP adresleri, alan adları, e-posta adresleri, adlar ve daha fazlası hakkında istihbarat toplamak için 100'den fazla genel veri kaynağını (OSINT) otomatik olarak sorgulayan bir keşif aracı" olarak pazarlamaktadır (Oerlamans, 2022). Ayrıca bireylerden toplanan veriler daha sonra kategorize edilerek başka özel şirketlere satılabilmekte veya devletlerle iş birliği yapılabilmektedir.

OSINT istihbaratının kamuya açık bilgilerden elde edildiğini daha önce dile getirilmişti. Kamu ile paylaşılan bilgiler yine de bireyin özel hayatı ile ilgili olabilmekte ve birey bunun sadece kendi çevresinde paylaşmak isteyebilmektedir. Bu bilgiler alınıp veri haline dönüştürüldükten sonra ancak bireyin özel hayatına müdahale söz konusu olmaktadır. Yine aynı şekilde kamuya açık ses dosyaları ve/veya videoların kullanımı da telif hakkı kapsamında ihlallere yol açabilmektedir (Koops, 2013, s. 677).

OSINT kaynaklı bir başka ihlal edilen alan sosyal medya sitelerinin gözetlenmesi ile ilgilidir. Örneğin 2012 yılında iki İngiliz turistin ABD’yi yok edeceklerine dair Tweet atmaları ve ardından ABD’den sınır dışı edilmeleri sosyal medya sitelerinin takip edildiğinin bir göstergesi olarak karşımıza çıkmaktadır (Eijkman ve Weggemans, 2012, s.290) Görüldüğü üzere verileri yanlış bir şekilde analiz etmek bireylere zarar verebilmektedir. Özel hayatın gizliliği kavramı verilerin erişilebilir olmasıyla ilgili olsa da, o bilgileri hangi bağlamda kullandığınız da önem arz etmektedir. Örneğin Danah Boyd’a göre, “kamu” kelimesini "herkes tarafından, her koşulda, her zaman ve her amaçla erişilebilir" anlamında saptırılmıştır demektedir (Boyd, 2010). Kullanılan istihbarat programları sayesinde içerik bağlamdan

çıkarılmış, veri olarak etiketlenmiş ve bireyin eylemleri en başta ona erişimimiz olduğu gerçeğiyle gerekçelendirilmiştir”. Helen Nissenbaum bu durumu “Verinin erişilebilir olması, onu kullanmanın etik olduğu anlamına gelmez” diyerek özetlemektedir (Nissenbaum, 2004, s.119). Bu noktada siber uzayın doğası gereği iç içe geçen kamusal alan ve özel alan kavramları arasındaki sınırların ortadan kalktığı görülmektedir. Birey sosyal medya hesabındaki bilgileri her ne kadar kendi kişisel sayfasında paylaşıyor olsa da bu bilgilerin istihbarat programları sayesinde geri dönülemez şekilde kamulaştığı gözlemlenmektedir. Ayrıca bireyin bir bilgiyi paylaşması bu bilgilerin devletler, özel şirketler tarafından bireyin rızası olmadan kullanılması hakkını beraberinde getirmemektedir.

ECHELON, PRISM veya XKEYSTORE gibi istihbarat programlarının kullanımı büyük ölçüde yapay zeka kullanımına dayanmaktadır. 2013 Snowden ifşaatlarından sonra bu konu özel hayatın gizliliği çerçevesinde uluslararası arenada da büyük yankı uyandırmıştır. Örneğin NSA destekli bu sistemler sayesinde; iletişimin toplu olarak dinlendiği ve internet ve uluslararası iletişim verilerinin toplandığı ortaya çıkmış, dinlenen verilerin ileri düzeyde aranması ve analizi için araçlar geliştirildiği görülmüş, hükümetler ve telekomünikasyon hizmet sağlayıcıları arasındaki iş birliği ilişkileri ve ülkeler arası istihbarat paylaşımı da dahil olmak üzere bir dizi faaliyet gözler önüne serilmiştir (Watt, 2021, s.6). Bu konu aynı zamanda Birleşmiş Milletler İnsan Hakları Yüksek Komiserliği’nin A/HRC/48/31 numaralı “The right to privacy in the digital age” raporunda da açık bir şekilde ele alınmıştır. Belgede siber istihbarat esnasında yapay zekânın kullanılmasının sakıncaları 12. ve 20. Maddeler arasında düzenlenmiştir. Buna göre ilgili maddeler;

12-kişisel verilerin artan şekilde toplanması ve kullanılması yoluyla özel hayatın gizliliği hakkına müdahaleyi genişleten, yoğunlaştıran veya teşvik eden yapay zeka sistemlerinin özellikleridir.

13- Yapay zeka sistemleri, genellikle kişisel veriler de dahil olmak üzere büyük veri kümelerine dayanır... Veri simsarları kişisel verileri toplar, birleştirir, analiz eder ve sayısız alıcıyla paylaşır....

14- Bu veri kümeleri, insanların özel hayatlarını şirketlere ve devletlere ifşa etmenin yanı sıra, bireyleri başka şekillerde de savunmasız hale getiriyor...

Büyük veri kümeleri, sayısız analiz biçimine ve verilerin üçüncü taraflarla paylaşılmasına olanak tanıyor;

15- kişisel veriler söz konusu olmadığında bile, özel hayatın gizliliği hakkı da dahil olmak üzere insan hakları, ...bunların kullanımından olumsuz etkilenebilir.

16- „... Yapay zeka araçları, zihinsel ve fiziksel durumları da dahil olmak üzere bireyler hakkında geniş kapsamlı çıkarımlar yapabilir ve belirli siyasi veya kişisel eğilimleri olan insanlar gibi grupların tanımlanmasını sağlayabilir“

17- Pek çok çıkarım ve tahmin, insanların özerkliği ve kimliklerinin ayrıntılarını oluşturma hakları da dahil olmak üzere, özel hayatın gizliliği hakkından yararlanmayı derinden etkiler....

18-Yapay zeka tabanlı kararlar hatasız değildir. Aslında, yapay zeka çözümlerinin ölçeklenebilirliği, görünüşte küçük olan hata oranlarının olumsuz etkilerini önemli ölçüde artırabilir...

19- Hatalı verilere dayanan yapay zeka sistemlerinden elde edilen çıktılar, örneğin bir kişiyi yanlışlıkla olası bir terörist veya refah dolandırıcılığı işlemiş olarak işaretlemek gibi birçok şekilde insan hakları ihlallerine katkıda bulunabilir...

20- Birçok yapay zeka sisteminin karar verme süreçleri şeffaf değildir. Veri ortamının karmaşıklığı, yapay zeka sistemlerinin geliştirilmesi ve işletilmesinin altında yatan algoritmalar ve modellerin yanı sıra devlet ve özel aktörlerin kasıtlı gizliliği, kamunun yapay zeka sistemlerinin insan hakları üzerindeki etkilerini anlamasını anlamlı hale getiren faktörlerdir (s. 4-6).

Yukarıda maddelerden de anlaşılacağı üzere siber istihbaratta veri toplama esnasında kullanılan yapay zeka özel hayatın gizliliği hakkını olumsuz yönde etkilemektedir. Yapay zeka sistemleri, büyük miktarlarda verinin toplanmasına, depolanmasına, birleştirilmesine ve analizine dayanmaktadır. Yapay zeka sistemlerini besleyen bilgiler ya kişisel olarak tanımlanabilir ya da anonimleştirilmesi durumunda bir algoritma kullanılarak yeniden tanımlanma olasılığı olabilen bilgilerden oluşmaktadır (Raso vd., 2018, s. 18-19). Bu bağlamda kişisel verilerin bireyin bilgisi

dışında toplanması ve bu bilgilerin kamusallaştırılması bireyin özeline müdahil olarak ihlal edilme anlamını taşımaktadır.

Bir diğer etki ise, birey hakkında veri toplama ve bireyi kodlama bir başka deyişle bireye sanal profil oluşturma esnasında karşımıza çıkmaktadır. Bireyin rızası dışında toplanan veriler yapay zeka desteği sayesinde bireye yeni bir profil oluşturmak veya bireyler hakkında çeşitli çıkarımlarda bulunmak amacıyla kullanılabilir. Kişisel bilgilerin kullanılarak algoritmalarla çıkarımda bulunulması bireyin daha sonraki davranışı öngörmesiyle bireyin gerçek kimliğini yansıtmayabilir. Ayrıca yapay zekanın bireyi suçlu ya da yanlış kodlaması durumunda (suçlu veya terörist gibi) birey detaylı bir takip sürecine girmekte, bireyin sürekli gözetim altında tutulmasına olanak sağlamakta ve onur ve haysiyetini etkileyebilecek telafisi olmayan süreçlerle mücadele etmesi sonucunu doğurabilmektedir.

Siber istihbaratın bir diğer sonucu ise veri ihlalleri olarak karşımıza çıkmaktadır. Siber istihbarat sürecinin bir parçası olan veri ihlali ve bireyin verilerine yetkisiz erişim üçüncü tarafların eline geçtiği takdirde birey açısından büyük bir risk ortaya çıkmaktadır. Örneğin kişisel sağlık kayıtlarınıza yetkisiz erişim bireyin başkalarıyla paylaşmak istemediği bilgilerinin ifşasına neden olabilmektedir. Bir başka açıdan, bireysel bilgilerinizin yine kötü niyetli kişiler tarafından ele geçirilmesi, kişisel bilgilerinizin başka amaçlarla kullanımına yol açabilmekte ve bu minvalde birey kişisel veriler üzerindeki kontrolünü kaybedebilmektedir. Bu durum genellikle banka hesap bilgilerinin çalınması, kimlik bilgilerinin kopyalanıp başka amaçlar için kullanılması ve/veya sosyal medya platformlarında yer alan bireyin bilgi ve fotoğraflarının rızası dışında kullanılmasını içermektedir. Ancak bu durum bireyin güvenliği ve özel hayatı çerçevesinde kapsamlı sonuçlara yol açabilmektedir.

Bir başka riste siber gözetim olarak karşımıza çıkmaktadır. Siber istihbarat faaliyetleri bireylerin verilerini kullandığından dolayı bireyin sosyal medya hesapları, telefonu, bilgisayar gibi çok çeşitli kaynaklardan beslenmektedir. Bireyin her bir ayak izinden birey izlenerek büyük miktarda veriler toplanmaktadır. Bu şekilde yapılan bir gözetim bir önceki bölümde de değindiğimiz üzere yasal güvenceden yoksun olduğundan dolayı bireyin özel hayatını ihlal etmektedir. Ayrıca birey gözlemlendiği veya analiz edildiğinin farkına varırsa, bu bireyin davranışını değiştirmesine neden

olabilmektedir. Bu durum da “panoptik etki” olarak adlandırılmaktadır (Leslie vd., 2021, s. 16). Panoptik etki de bireyin özel hayatında istediği gibi davranamamasına ve özellikle ifade özgürlüğü kapsamında kendisini gerçekleştirememesine neden olabilmektedir.

Devletlerin bekası için siber tehditlere yönelik yaptığı siber istihbarat faaliyetleri ile özel hayatın gizliliği hakkı arasında denge kurmak esas olarak karşımıza çıkmaktadır. Siber istihbarat devletlerin, özel şirketlerin ve bireylerin güvenliği söz konusu olduğunda büyük avantajlar sağlarken, özel hayatın gizliliği hakkında verilerin izinsiz kullanılması, anonimleştirilmesi, özel şirketler tarafından bu verilerin satılması, bireylerin gruplandırılması ve etiketlenmesi (siyasi parti, din, dil, ırk vb.) bağlamında özel hayatın gizliliği hakkını olumsuz etkilediği gözlemlenmektedir. OSINT ve SIGINT gibi özel hayatın gizliliğini en çok ihlal eden siber istihbarat tekniklerinin ve kullanılan programların bireylerin özel hayatı ihlal edilmeden yasal çerçeve içerisinde tanımlanması ve etik güvenceleri de içerecek şekilde şeffaflık, hesap verilebilirlik, orantılılık ilkeleri de göz önüne alınarak hukuk sınırları içerisinde bir bütün olarak sunulması gerekmektedir.

3.1.3. Kişisel Verilerin Korunması

Teknolojik gelişmelerin durmaksızın geliştiği çağda siber uzayda kişisel verilerin korunması büyük önem kazanmıştır. Bireylerin internet üzerinden gerçekleştirdiği her adım faaliyet türüne bakmaksızın veri üretmektedir. Üretilen verilerin nasıl korunacağı, kimlerle paylaşılacağı, üçüncü tarafların erişimi ve verilerin ne şekilde kullanılacağı siber uzayda yapılan tartışmaların önemli bir basamağını oluşturmaktadır. Özellikle yapay zeka kullanımının artmasıyla birlikte kişisel veriler çok daha rahat bir şekilde ele geçirilip kategorize edilir hale gelmiştir. Veriler dijital çağda internet ekonomisinin temelini oluşturmaktadır. Veriler söz konusu olduğunda, kişisel veriler neredeyse her zaman tamamen otomatik bir şekilde toplanmakta ve analiz edilmektedir. Kişisel veri ve özel hayatın gizliliği hakkında en büyük endişelerden biri bilginin nasıl elde edildiği ve ne amaçla kullanıldığıdır. Birçok işletme uluslararası alanda yer alabilmek için verileri ticarileştirerek paraya çevirmekte ve böylece büyük kazançlar elde etmektedir. Mobil teknolojilerin, bulut

bilişim sistemlerinin, öğrenme algoritmalarının ve büyük veri teknolojilerinin ortaya çıkması şirketler için yeni fırsatlar yaratmış ve verilerin dijitalleşmesini de artırmıştır (Pereira, vd., 2022, s. 1). Örneğin Amazon, Google, Tesla, Apple, Netflix, Uber ve Airbnb en yeni teknolojileri nesnelerin interneti ve büyük veri analitiğini kullanmaktadır.

Kişisel verilerin korunması, bireyin kişisel bilgilerinin yetkisiz erişim, kullanım veya ifşadan korunması olarak karşımıza çıkmaktadır. Ayrıca bireysel özerkliği koruyarak bireyin toplum içerisinde rahatça yaşamasına olanak sağlamaktadır. Bir başka deyişle Alan Westin'in tanımıyla kişinin kendi bilgileri üzerinde kontrol hakkına sahip olmasıyla ilişkilidir. Ancak çalışmanın birinci bölümünde vurgulandığı gibi kişisel veri ve kişisel verilerin korunması farklı anlamlara gelmektedir. İnsan Hakları sözleşmeleri kişisel verilere saygıyı vurgularken, kişisel verinin korunması bireye ait verilerin muhafaza edilmesi anlamını taşımaktadır. Kişisel verilerin korunması özel hayatın gizliliği hakkından kaynaklanmaktadır. Ayrıca sadece özel hayatın gizliliği hakkını değil, ifade özgürlüğü hakkı veya toplanma özgürlüğü hakkı açısından da büyük önem arz etmektedir.

Avrupa Birliği 2016 yılı Nisan ayında Kişisel Verilerin Korunması Kanunu'nu kabul etmiştir. 2018 yılında yürürlüğe giren “Genel Veri Koruma Direktifi” dijital teknolojilerin birey üzerindeki etkileriyle başa çıkmak için geliştirilmiştir ve şu an dünyadaki en kapsamlı ve ilercici veri koruma mevzuatı olarak yer almaktadır (European Data Protection Supervisor, t.y.). GDPR'ın 3. Bölümünde 12 ve 23. maddeler arasında “Veri Sahibinin Hakları” düzenlenmektedir. Bu haklar maddeler halinde şu şekilde yer almaktadır;

Veri konusunun haklarının kullanılmasına yönelik şeffaf bilgi, iletişim ve yöntemler (Madde 12), Veri sahibinden kişisel verilerin toplandığı durumlarda sağlanacak bilgiler (Madde 13), Veri sahibinden kişisel verilerin alınmadığı durumlarda sağlanacak bilgiler (Madde 14), Veri sahibinin erişim hakkı (Madde 15), Düzeltme hakkı (Madde 16), Silme hakkı- 'unutulma hakkı' (Madde 17), İşlemeyi kısıtlama hakkı (Madde 18), Kişisel verilerin düzeltilmesi veya silinmesi veya işlemenin kısıtlanması ile ilgili bildirim yükümlülüğü (Madde 19), Veri taşınabilirliği

hakkı (Madde 20), İtiraz hakkı (Madde 21), Profil çıkarma da dahil olmak üzere otomatik bireysel karar verme (Madde 22), Kısıtlamalar (Madde 23)dır (GDPR,2020).

GDPR'nin 12. maddesi kişisel verilerinin işlenmesiyle ilgili olarak bireyler için kısa, şeffaf, açık, sade ve erişilebilir bilgilerin önemini vurgulamaktadır. 13. maddesinde ise kişisel veri bireyin kendisinden toplandığında kişilere sağlanması gereken bilgileri, 14. madde de verinin kişi üzerinden elde edilmediği zaman bireye verilecek bilgiler yer almaktadır. 15 ve 22. maddeler arasında erişim, düzeltme, unutulma, işlemeyi kısıtlama, veri taşınabilirliği, nesne ve otomatik bireysel karar verme hakkını içeren veri konularının kişisel haklarını özetlemektedir. Son madde de ise bu hakların hangi durumlarda kısıtlanabileceğinin ele alındığı görülmektedir. Bu maddelerin amacı, AB'de bireylere kişisel verileri üzerinde daha fazla kontrol yetkisi vermek ve bireyin verileri işlenirken şeffaflık ve adaleti sağlamaktır. Ayrıca bireylerin özel hayatın gizliliğini ve kişisel verilerini kontrol altına almak için belirli haklar ve bilgiler sağlamaya odaklanarak veri işleyen tarafları da hesap verebilir ve sorumlu hale getirdiği görülmektedir. Ancak her ne kadar veri toplama, işleme, analiz ve depolama GDPR'da tanımlanırsa tanımlansın, kişisel verilerimiz siber uzayda yine de ihlal edilmeye devam ettiği görülmektedir.

Büyük Veri ve Nesnelerin İnterneti açısından GDPR'ın ilgili maddelerine baktığımızda; kişisel verilerin işlenmesine ilişkin ilkeler (Madde 5), Veri depolama, erişim, düzeltme ve silme (Madde 5, 15-17), Onay Koşulları (Madde 7) dahil olmak üzere belirli hükümleri içerdiği söylenebilmektedir. Ayrıca veri sahibinin bilgilendirilmesi ve veri ihlalinin denetim bakanlığına iletilmesi, ihlalin veri sahibine iletilmesi (Madde 13-14 ve 33-34), otomatik karar verme ve profil oluşturma (Madde 21-22), tasarım gereği ve varsayılan olarak veri koruması (Madde 25) ve veri koruma etki değerlendirmesi de (Madde 35-36) bu kapsamda ele alınabilmektedir (Watcher, 2018, s. 269).

Gelişen teknolojinin bir sonucu olarak kişisel veriler en çok Büyük Veri analitiği ve Nesnelerin İnterneti kullanımı sonucunda ihlale uğradığı görülmektedir. Büyük veri "yüksek hızda yakalama, keşif ve analiz sağlayarak çok çeşitli verilerden çok büyük hacimlerde değeri ekonomik olarak ayırmak için tasarlanmış yeni nesil teknolojiler ve

mimariler" olarak tanımlanmaktadır (Jain, vd., 2016, s. 1). Kişisel veriler açısından, büyük veri kullanıcıların dijital izlerinin yansıması olarak karşımıza çıkmaktadır.

Böylesi gelişen teknolojiler genel açıdan devletlere ve özel işletmelere muazzam kolaylık sağlarken, bireyler bu teknolojilerden olumsuz şekilde etkilenmektedir. Teknolojinin bu denli geliştiği bir ortamda birey açısından kişisel verilerine saygı hakkı kolayca ihlal edilebilir hale gelmiş ve kişisel verilerinin kontrolünü adeta kaybetmiştir. Bu açıdan da büyük veri özel hayatın gizliliği hakkı açısından risk teşkil etmektedir. Verilerin çeşitlenip çoğalması, internetin günlük alışkanlıklarımızın bir parçası haline gelmesi, sağlık dahil bütün kayıtlarımızın çevrimiçi platforma taşınması ve bahsi geçen verilerin ve uluslararası paylaşımı özel hayatın gizliliği hakkını siber uzayda korumanın daha da zorlaşacağı düşünülmektedir.

Günümüzde birçok sektörde bilginin toplanması, analiz edilmesi ve depolanması Büyük Verinin kullanımı sayesinde şekil değiştirmiştir. Rubinstein'a göre Büyük Veri'nin üç ana özelliği bulunmaktadır. Bunlardan ilki; veriler çevrimiçi platformlar, konum izleme özelliklerine sahip mobil cihazları, veri paylaşım uygulamaları, akıllı ortamlar, izleme sistemleri ve hatta genetik test ve biyometrik kimlik doğrulama için insan vücudunu kapsamadadır. Böylelikle çok sayıda kaynaktan toplanan verilerin geniş çaplı kullanım alanı olmaktadır. İkinci özelliği; büyük depolama kapasiteleriyle (Petabayt- PB) donatılmış yüksek hızlı bilgisayarların kullanılmasıdır. Üçüncü ve son tanımlayıcı özelliği ise bu devasa veri hacmini depolamak ve analiz etmek için yeni hesaplama sistemlerinin kullanılmasıdır (2013, s. 77).

Görülebileceği üzere kişisel bilgiler neredeyse her şekilde elde edilmektedir. Ayrıca verilerin depolama alanının yükselmesi sayesinde, uygun maliyetli ve verimli bir şekilde işlenmesini mümkün kılmaktadır. 1 Petabyte (PB) 1000 Terabyte'a (TB) eşittir. Araştırmalar insan beyninin yaklaşık 2,5 PB kapasiteye sahip olduğunu göstermektedir. Örnek vermek gerekirse, tek bir PB yaklaşık 3,5 yıllık kesintisiz 1080p kalitesinde video içeriğini barındırabilmektedir. Başka bir senaryoda ise insanlar yaşamları boyunca günde 4.000 fotoğraf çekecek olsaydı, yine de yalnızca 1PB depolama kapasitesini doldurabileceği öngörülmektedir (Reber, 2010).

Veri ihlalleri, büyük veri analitiği bağlamında kişisel verilerin korunmasına yönelik önemli bir tehdit oluşturmaktadır. Kişisel verilerin en çok ihlal edildiği alanlardan biri “veri ihlali” olarak karşımıza çıkmaktadır. Veri ihlalleri, bilgisayar korsanlarının bireyin kullandığı ağlara erişerek bilgisayar veya diğer mobil cihazlara erişmesi veya kuruluşların kişisel bilgileri güvenli bir şekilde imha etmemesi gibi güvenlik olaylarından kaynaklı olarak kişisel verilere yetkisiz erişimi içermektedir (Culnan, 2009, s. 678). Çevrim içi olarak gerçekleştirdiğimiz her şeyde kişisel bilgilerimizin çalınması ihmalî bulunmaktadır. Bu bilgiler adımız, ev adresimiz, e-postalarımız olabileceği gibi banka hesaplarımız veya sağlık verilerimiz de olabilmektedir. Bireysel verilerimiz genellikle kurumsal web sitelerinden, şirketlerden veya kişisel bilgisayarlardan sızdırılabilmektedir. Kimlik Hırsızlığı Veri Merkezi (Identity Theft Resource Center) ’nin 2022 Yıllık Veri İhlali Raporu’na (Annual Data Breach Report-ADBR) göre, Amerika Birleşik Devletlerinde 422.143.312 kişi, kişisel verileri çalındığı için mağdur olmuştur. İzinsiz erişilen verilerde ilk üç sıraya baktığımız zaman ise kişinin isminin, sosyal güvenlik numarasının ve doğum tarihlerinin çalındığı görülmektedir (ADBR, 2022).

İzinsiz şekilde elde edilen kişisel “verilerin kötüye kullanılması” özel hayatın gizliliği hakkının bir diğer ihlal boyutunu oluşturmaktadır. Günümüzde de sıklıkla karşılaştığımız bu ihlal türü, yetkisiz erişilen kişisel bilgilerin özel şirketlere satılması veya bireysel kullanıcıların paylaşması sonucunda oluşmaktadır. Örneğin e-maillere düşen otomatik spam mailleri, kişisel verilerimizin paylaşılması sonucu her gün onlarca aldığımız reklam mailleri veya ticari işletmeler tarafından yapılan telefon aramaları kişisel verilerimizin üçüncü taraflara satılması örneğini oluşturmaktadır. Ayrıca kredi kartı dolandırıcılığı veya adınıza sahte hesaplar açılması yine bireyi bu konuda mağdur eden örnekler olarak karşımıza çıkmaktadır. Bunların yanı sıra Dark Web’de çalınan kişisel bilgilerin satılması veya çocuk ve/veya bireylerin haberi dahi olmadan Dark Web’e pornografi materyali olarak yüklenmesi bireyin toplum içerisinde şan, şöhret ve onurunu zedelemekte ve bireyin toplum içerisinde huzur içerisinde yaşamasına engel teşkil etmektedir.

Büyük Verinin kullanımının bir başka ihlal yönünü ise otomatik karar alma süreçleri oluşturmaktadır. Bireyin kişisel verilerinden yola çıkarak bireylerin

kategorize edilip sınıflandırılması özel hayatın gizliliği açısından birtakım endişeleri de beraberinde getirmektedir. Bu da insanların dijital ve çevrimiçi faaliyetlerinin bir sonucu olduğu ve bireysel kişisel profiller oluşturmak için kullanabileceği gerçeğini ifade etmektedir (Daniels, 2023).

Otomatik karar alma ile ilgili iki büyük sorun bulunmaktadır. Birincisi, bu sistem geçmiş verileri kullanır ve dolayısıyla önyargılı tahminler üretmektedir. İkinci olarak, bu sistemin tahminleri sorgulanamaz veya itiraz edilemez çünkü algoritmalar özeldir ve ticari sır perdesi altında korunmaktadır (McCarroll, 2019, s. 708). Dolayısıyla bireyin kaderi büyük verinin atadığı kategoriye göre şekillenmektedir. Bu da bireyin bilgisi dahi olmadan belirli bir sınıfa ya da belirli bir kategori altına tanımlanmasını içerebilmektedir. Bu durumun bir sonucu bireyin eşit olmayan bir muameleye maruz kalması veya ayrımcılık şeklinde karşımıza çıkabilmektedir. Bir başka deyişle birey kendi kaderini tayin edemez çünkü zaten birey hangi kategori altında değerlendirildiğini bilememektedir. Toplanan bilgilerin bireylerle paylaşılmaması aynı zamanda hakkında işlem yapılan bireyin sistemden dışlanması anlamına gelmektedir. Bu da bir ironi olarak karşımıza çıkmaktadır.

Büyük Veri kişisel verileri toplayıp analiz ederken veriler üzerinden tahmine dayalı analiz yapmaktadır. Bu durum devletler için güvenliği sağlamak amacıyla kullanıldığında muazzam bir fayda sağlamaktadır. Hatta özel şirketlere de müşterileri kategorize ederek hangi ürünün kime nasıl pazarlanacağı konusunda işlerini kolaylaştırdığı görülmektedir. Ancak bireyler açısından bu durum avantajdan ziyade dezavantaja neden olmaktadır. New York Times'ın Target Inc. Firması hakkında yaptığı haberde bu durum daha açıkça anlaşılmaktadır. Habere göre; Target Inc.firması müşterilerin satın alma alışkanlıklarına göre “hamilelik tahmin puanı” hesaplamaktadır. Buna göre bir vakada genç bir kızın babası; kızının sürekli hamilelikle ilgili reklamlar ve kupon aldığı için Target Inc. Mağazasına şikayette bulunmak için gitmiştir. Ancak birkaç gün sonra mağaza yetkililerini arayan baba, kızının hamile olduğunu ve Ağustos'ta doğum yapacağını söyleyerek mağaza yetkililerinden özür dilemiştir (Aktaran; Tene ve Polonetsky, 2013, s.253). Görüleceği üzere insanların en özel durumları dahi yaptıkları alışverişler sayesinde tahmin edilebilmektedir. Ancak buradaki durum bireyin özel hayatın gizliliği hakkının bir

pazarlama stratejisi olarak ihlal edilmesidir. Alışveriş alışkanlıklarının kategorize edilip sizlere sunulması farklı bir şey, bireyin hassas verilerinin normalleştirilerek pazarlama aracı olarak sunulması farklı bir şeydir. Biri sadece metalden oluşurken, diğeri değerlerden oluşur. Bireyin henüz paylaşmadığı hassas kişisel bir durum ifşa edilerek etik dışı bir yol takip ettiği görülmektedir. Dolayısıyla kişisel veriler rastgele bir şekilde toplanırken etik ilkelerden bahsetmek mümkün müdür? Belki de cevaplanması gereken ilk soru bu olmalıdır.

Birçok işletme ve devlet kuruluşları gerek serbest piyasada üstünlük elde etmek amacıyla gerekse güvenlik amacıyla ihtiyacı olan veriyi değil, erişebildiği tüm veriyi toplayıp depoladığı görülmektedir. Oysaki kuruluşlar kişisel verilerin toplanmasını meşru hedeflerine ulaşmak için gerekli olan asgari ölçüde sınırlandırmaları gerekmektedir. Ayrıca, toplandıkları amaçlar için artık kullanılmayan verileri silmeleri ve kişisel verilerin tanımlanabilir biçimde tutulmasına ilişkin kısıtlayıcı politikalar uygulamaları gerekmektedir. Büyük veri, veri minimasyonundan ziyade maksimum veriyi elde etmeye çalışır. Daha uzun süreler için daha fazla veri toplanmasını teşvik etmektedir (Tene ve Polonetsky, 2013, s.259). Kişisel verilerin ihlali de tam da bu alanda çıkmaktadır. Veriler toplanırken mutlaka belirli bir amacı olmalı ve belirli bir süre için toplanması gerekir. Böylesine rastgele toplanan bilgilerin orantılılık, şeffaflık, hesap verilebilirlik ve etik ilkelerden yoksun olduğu görülmektedir.

Büyük Verinin yanı sıra kişisel verilerimize doğrudan etki eden bir başka teknoloji ise Nesnelerin İnterneti (Internet of Things) 'tur. Günümüzde sağlık sisteminde, ticarete, araçlarımızda, şehirlerde, evlerimizde veya kişisel olarak kullandığımız birçok araç nesnelerin interneti (IoT) teknolojisi ile çalışmaktadır. Örneğin akıllı evler, kendimizde ve çocuklarımızda kullandığımız akıllı saatler, buzdolapları, robot süpürgelerimiz, akıllı çay, kahve makinalarımız IoT teknolojilerine örnek oluşturmaktadır. IoT teknolojisinin özelliği, insan müdahalesi olmadan nesnelerin internete bağlanması olarak karşımıza çıkmaktadır (Akyeşilmen, 2018, s. 312). Sensörlerle birleştirilmiş ve verileri ileten ve işleyen, diğer makineler veya insanlarla iletişim kuran, genellikle otomatikleştirilmiş fiziksel nesnelerin ağı olarak tanımlanmaktadır (Pereira, vd., 2022, s. 4-5). IoT, tıp, akıllı ulaşım, şehir planlama, akıllı tarım, enerji ve benzeri birçok alanda dönüşüm sağlama konusunda umut verici

görülmektedir. Örneğin, bir hastanın vücudundaki kablosuz vücut sensörleri sayesinde sağlık uzmanlarının hastalarını her yerde izlemelerine yardımcı olabilmektedir (Ogundoyin, 2020, s.315). Ancak konu birey olduğunda birtakım olumsuz gelişmeleri de beraberinde getirdiği görülmektedir.

IoT cihazları, sürekli dinleme, izleme ve veriyi toplama nedeniyle büyük miktarda hem hassas hem de kişisel bilgiler biriktirmektedir. Elde edilen verilere aynı büyük veri de olduğu gibi üçüncü tarafların yetkisiz erişimi, veri ihlalleri ve verilerin kötüye kullanımı risklerini de beraberinde getirmekte bu da bireye zarar verme potansiyelini arttırmaktadır. Ayrıca IoT cihazlarında anonim kullanımın olmaması bir başka deyişle kullanılan cihazların direkt bireylere tanımlanması, kontrol mekanizmasının olmaması özel hayatın gizliliğine dair endişeleri daha da çok arttırmaktadır.

IoT, internete bağlı robot süpürgeci daha fazlasını temsil etmektedir. Hayatımızda yer alan birçok nesnenin ağa bağlanmasını işaret etmektedir. Bu da çevrimiçi kaynaklar kullanıldıkça daha fazla verinin oluşması anlamına gelmektedir. Örneğin çocukların kullandıkları akıllı saatler sayesinde ebeveynler çocuklarının nerede olduklarına ve konum bilgilerine ulaşabilmektedir. Ancak arka planda bu konum bilgileri veri sahipleriyle de paylaşılmakta hatta ortam sesi çevrimiçi olarak dinlenebilmektedir. Bu da yabancılar tarafından çocuğun izlenmesi, konumunun takip edilmesi ve hatta çocuk ile iletişim kurulması için kullanılabileceğinin bir göstergesi olarak karşımıza çıkmaktadır. Bir başka durumda evlerimizde kullandığımız araçlar için geçerlidir. Bu araçların her biri potansiyel olarak siber tehdite açıktır. Bu kullandığımız akıllı cihazların üçüncü tarafların eline geçirilmesi durumunda yine özel alanımızı ihlal edebilmektedir. Ayrıca kötü niyetli bir hacker akıllı cihazlarımızdan kişisel bilgilerimizi ele geçirerek, örneğin evinizde güvenlik sistemi varsa bunu devre dışı bırakabilmektedir. Bu ve buna benzer örnekleri çoğaltmak mümkündür.

Büyük veri ve nesnelerin internetinin özel hayatın gizliliği hakkını birçok yönden ihlal ettiği görülmektedir. Teknolojinin durmadan gelişmeye devam etmesi bu ihlallerin yanında gelecekte farklı ihlalleri de beraberinde getireceğini göstermektedir. GDPR her ne kadar bu riskleri minimize etmeye çalışsa da tanımlamalardaki muğlaklık kişisel verilerin korunması aşamasında belirsizlik yaratmaktadır. Örneğin

veri ihlalleri söz konusu olduğunda veri sahiplerini bilgilendirme gereklilikleri (Madde 34), yalnızca 'gerçek kişilerin hak ve özgürlüklerine yüksek risk' olduğu zaman geçerlidir. Ancak GDPR içerisinde 'yüksek risk' tanımlanmadığı görülmektedir (Watcher, 2018, s. 270). Bu ve buna benzer muğlaklıkların yeni teknolojiler geliştikçe, yaygın bir kişisel veri koruma kültürü geliştikçe ve AİHM'de davalar çeşitlendikçe giderilmeye çalışılacağı düşünülmektedir. Ayrıca özellikle AB sınırları dışında da kişisel verilerin korunması hususunda fikir birliği ve iş birliği oluşturularak ortak bir direktifin tanımlanması kişisel verilerin daha etkin bir şekilde korunmasını sağlayacaktır.

3.2. Avrupa İnsan Hakları Mahkemesi Kararları

AİHM kararları özel hayatın gizliliği hakkının teknoloji bağlamında yeniden yorumlanması konusunda önem arz etmektedir. Bu bölümde AİHM kararları elektronik gözetim, kişisel veri ve kişisel verilerin korunması ve yazışmalar başlıkları altında ele alınacaktır.

3.2.1. Elektronik Gözetim

AİHM'nin siber gözetim davalarını elektronik gözetim adı altında ele aldığı görülmektedir. Dolayısıyla bu bölümde elektronik gözetim başlığı altında ele alınan davalar siber gözetim davalarına örnek teşkil etmektedir.

Szabó and Vissy v. Hungary Davası (2016); Dava, Macaristan'ın 2011 yılında yürürlüğe koyduğu terörle mücadele amaçlı gizli gözetim yasası ile ilgilidir. Başvuranlar, AİHS'nin 8, 13 ve 6. Maddeleri uyarınca Macar Hükümeti aleyhine şikayette bulunmuş ve yasaların izin verdiği gözetleme biçiminin haksız ve orantısız müdahaleci tedbirlere maruz kalabileceklerinden şikâyetçi olmuşlardır.

Bu davada önem arz eden mahkemenin gerçekleşmesi muhtemel terör olayları için önceden haber almak amacıyla iletişimin yoğun bir biçimde izlenmesinin günümüz terör olayları yüzünden doğal bir sonuç olduğunu kabul etmesi olarak karşımıza çıkmasıdır. Ancak mahkeme, söz konusu mevzuatın operasyon alanı dışındaki kişiler hakkında da kitlesel verileri ele geçirebileceğin ve ulusal yasaların

bireylere yeterli güvence sağlamadığından dolayı AİHS'nin 8. Maddesinin ihlal edildiğine karar vermiştir.

Ben Faiza v. France Davası (2018); Dava büyük çaplı bir uyuşturucu kaçakçılığına karıştığı düşünülen şüphelinin gözetim tedbirleri ile ilgilir. Başvuran için üç gözetim tedbirleri alınmıştır; (i) bir telefon operatörüne, dört telefon hattından gelen ve giden aramaların kayıtlarını ve baz istasyonlarının listesini elde etmesi için bir mahkeme emri verilmiştir. (ii) polis, başvuran tarafından kullanılan bir araca bir izleme cihazı takmak için soruşturma hakiminden sözlü izin almıştır; ve (iii) soruşturma hakimi, aracı kullanan kişilerin konuşmalarını alacak, düzeltecek, iletecek ve kaydedecek bir cihazın ve araca bir ay süreyle coğrafi konum belirleme cihazının takılmasına karar vermiştir. Başvuran tüm bu gözetim önlemlerinin özel hayatına bir müdahale teşkil ettiğinden şikâyetçi olmuştur.

Mahkeme, Fransız hukukunda GPS cihazı aracılığıyla dinlemenin açık bir şekilde gösterilmediği, bu yüzden de başvuranın demokratik toplumda hukukun üstünlüğünün sağladığı asgari korumadan yararlanamaması nedeniyle Sözleşme'nin 8. maddesinin (özel hayata saygı hakkı) ihlal edildiğine karar vermiştir.

Cep telefonu operatörü için ise mahkeme, telefonunun sinyal gönderdiği baz istasyonlarının listesini elde etmesi ve daha sonra hareketlerini takip etmesi için verilen mahkeme kararında, bu eylemin yasalara uygun ve meşru amacı olduğu için 8. maddenin ihlal edilmediğine karar vermiştir.

Antovic and Mirkovic v. Montenegro Davası (2018); İlgili dava, Karadağda üniversitede görev yapan iki profesörün ders verdikleri alanlara video gözetimi yerleştirilmesi ile ilgilidir. Başvuranlar toplanan bilgiler üzerinde etkili bir kontrole sahip olmadıklarını ve gözetimin hukuka aykırı olduğunu belirterek 8. Madde kapsamında haklarının ihlal edildiğini öne sürmüşlerdir.

Mahkeme daha önceki kararlarında özel hayat kavramının mesleki faaliyetleri veya kamusal bağlamda gerçekleşen faaliyetleri içerebileceğine hükmettiğini ve üniversite amfityatrolarının akademisyenlerin işyerleri olduğunu, burada sadece ders vermekle kalmayıp öğrencilerle etkileşime girdiklerini, sosyal hayat içerisinde etkileşime girdiklerini ve sosyal kimliklerini inşa ettiklerini belirtmiştir. Ayrıca

AIHM'nin önceki kararlarında işyerinde yapılan gizli video gözetimini bir çalışanın özel hayatına müdahale olarak değerlendirmiş ve işyerinde gizli olmayan gözetimin de aynı çerçevede değerlendirilmesi gerektiğine kanaat getirerek akademisyenlerin 8. maddeye istinaden özel hayatın gizliliğinin ihlal edildiği kararını vermiştir (Antovic ve Mirkovic, 2018, paragraf 44-45).

Gorlov and Others v. Russia Davası (2019); Dava, mahkumların mahkeme öncesinde odalarında kapalı devre televizyon kameraları tarafından sürekli olarak izlenmesi ile ilgilidir. Başvuranlar kadın gardiyanlar tarafından odalarında sürekli olarak gözetlenmesinin, özel hayatlarına saygı gösterilmesi haklarını ihlal ettiğinden şikâyetçi olmuşlardır. Mahkeme davayı değerlendirirken aşağıda yer alan görüşü sunmuştur:

...Bir kişiyi özgürlüğünden mahrum bırakan diğer tüm tedbirler gibi, tutukluluk da kişinin hak ve özgürlüklerine çeşitli sınırlamalar getirirse de, bu kişi, Sözleşme'nin 8. maddesi ile güvence altına alınan haklar da dâhil olmak üzere, yalnızca tutuklu statüsü nedeniyle Sözleşme'deki haklarını kaybetmez; dolayısıyla, bu haklara getirilen kısıtlamaların her davada gerekçelendirilmesi gerekir... (Gorlov and Others, 2019, Paragraf 81).

Yukarıda maddenin yanısıra mahkeme, mahkumların gözaltındayken sürekli video gözetimi altına alınmasının, kişinin özel yaşamına saygı hakkına ciddi bir müdahale olarak kabul edilmesi gerektiğini, ayrıca Rusyanın gözetimle ilgili ulusal hukukunun, açık, kesin veya ayrıntılı olarak değerlendirilemeyeceği sonucuna vardığından dolayı 8.maddenin ihal edildiğine karar vermiştir.

Big Brother Watch and Others- The United Kingdom Davası (2021); Dava, Kar Amacı Gütmeyen Kuruluşlar, Çeşitli Sivil Toplum Kuruluşları, Akademisyenler ve Gazeteciler tarafından Büyük Britanya ve Kuzey İrlanda Birleşik Krallığı aleyhine Mahkeme'ye yapılan üç başvurudan oluşmaktadır. Taraflar üç farklı gözetleme rejimine ilişkin AIHM'ye başvuruda bulunmuşlardır. Bunlar; “iletişimin toplu olarak dinlenmesi, yabancı hükümetlerden ve istihbarat kurumlarından dinleme materyallerinin alınması ve iletişim hizmeti sağlayıcılarından iletişim verilerinin elde edilmesi”dir (ECHR,2022). Dava, ABD ve Birleşik Krallık elektronik gözetim

rejimleri hakkındaki 2013 Snowden açıklamalarından bu yana İngiltere'nin toplu gözetim programlarına karşı ilk AİHM kararı olmasından ve uluslararası istihbarat servisleriyle istihbarat paylaşımına dair ilk dava olması açısından önem arz etmektedir.

Mahkeme öncelikle gözetim programları için iç hukukta olması gereken asgari sekiz şart belirlemiştir. Bunlar;

- 1.Toplu dinlemeye hangi gerekçelerle izin verilebileceği;
- 2.bir bireyin iletişiminin dinlenebileceği durumlar;
- 3.izin verilmesi için izlenecek prosedür;
- 4.önleme malzemesinin seçilmesi, incelenmesi ve kullanılması için izlenecek prosedürler;
- 5.materyali diğer taraflara iletirken alınması gereken önlemler;
- 6.dinleme süresinin sınırları, dinleme malzemesinin saklanması ve bu tür malzemenin silinmesi ve imha edilmesi gereken koşullar;
- 7.bağımsız bir makamın yukarıdaki güvencelere uygunluğu denetleme prosedürleri ve usulleri ve bu makamın uyumsuzluğu ele alma yetkileri;
- 8.bu tür uyumun bağımsız ex post facto incelemesi için prosedürler ve uygunsuzluk durumlarını ele alma konusunda yetkili organa verilen yetkiler (Big Brother Watch ve Others,2021, paragraf 361).

İç hukuk için bu çerçevenin belirlenmesi mahkemenin gereklilik ve hukuka uygunluğu birlikte ele aldığıın göstergesi olarak karşımıza çıkmaktadır. Dava sonucunda iletişimin toplu olarak dinlenmesiyle ilgili olarak AİHS'nin 8. Maddesinin, özel ve aile hayatına saygı hakkı ve iletişimin ihlal edildiğine; iletişim hizmeti sağlayıcılarından iletişim verilerinin elde edilmesi ile ilgili olarak 8. maddenin ihlal edildiğine; beşe karşı on iki oyla, Birleşik Krallık'ın yabancı Hükümetlerden ve istihbarat kurumlarından dinlenen materyalleri talep etme rejimiyle ilgili olarak 8. maddenin ihlal edilmediğine karar vermiştir.

Centrum för Rättvisa v. Sweden Davası (2021); davada başvuru, kar amacı gütmeyen İsveçli bir insan hakları kuruluşu olan Centrum för Rättvisa'dır. İlgili kurum yaptığı şikayette, sinyal istihbaratı ve gizli gözetim alanındaki İsveç mevzuatının ve uygulamasının AİHS'nin 8. Maddesi kapsamındaki özel hayatın gizliliğini ihlal ettiğini

öne sürmektedir. Mahkemenin, toplu dinlemeyi, süreç ilerledikçe bireylerin 8. Madde kapsamında bireyin haklarına müdahale derecesinin arttığı kademeli bir süreç olarak ele aldığı görülmektedir.

Grand Chamber (Büyük Daire), İsveç toplu dinleme hukukunun üç eksiklikliğini tespit etmiştir. Bunlar; “kişisel veri içermeyen dinlenen materyallerin imha edilmesine ilişkin açık bir kuralın bulunmaması; Sinyal İstihbarat Yasası'nda veya diğer ilgili mevzuatta, istihbarat materyallerinin yabancı ortaklara iletilmesine karar verilirken, bireylerin özel hayatın gizliliğinin çıkarlarının dikkate alınmasına ilişkin bir gerekliliğin bulunmaması; ve etkili bir ex post facto incelemenin bulunmamasıdır“ (ECHR, 2022, s.9).

Tüm bu eksikliklerin bir sonucu olarak AİHM, ikiye karşı on beş oyla, Sözleşme'nin 8. maddesinin (özel ve aile hayatına, konuta ve haberleşmeye saygı hakkı) ihlal edildiğine karar vermiştir.

AİHM'nin gözetim ile ilgili kararları da teknolojinin gelişmesi, kullanılan cihaz ve yöntemlerin çeşitlenmesi sonucu kapsamının genişlediği görülmektedir. Geçmişte de özellikle kolluk kuvvetleri tarafından, suçluların ele geçirilmesi veya casusluk faaliyetlerinde gözetim tekniğine başvurulduğu ve bu tekniğin de suçluyu yakalamadaki önemi bilinmektedir. Nitekim AİHM eski davalarına göz atıldığında örneğin 1978 yılında ele alınan Klass ve diğerleri/Almanya davasında mevzu bahis haberleşmenin kayda alınması veya 1984 yılında Malone/Birleşik Krallık davasında iletişimin dinlenmesi iken günümüzde GPS ile konum izleme, internet üzerindeki verilerin izlenmesi, yüz tanıma teknolojileri veya araçlara yerleştirilen kameralar gibi çok farklı teknik ve yöntemler karşımıza çıkmaktadır.

AİHM kararları da bu gelişmelere ayak uydurmuş kullanılan teknikler doğrultusunda farklılaşmıştır. Örneğin yukarıda bahsi geçen Ben Faiza France davası araca takılan GPS konum izleme ile veya Big Brother Watch Birleşik Krallık davası kitle gözetimi ile ilgilidir. Özellikle Big Brother Watch davası hem konunun güncel olması hem de uluslararası istihbarat paylaşımına dair ilk dava olması açısından hem klasik gözetim davalarından hem de elektronik gözetim davalarından ayrılmaktadır.

Ayrıca dava yapay zeka kullanımı ile ilgili iken AIHM'nin bu konuya hiç değinmemesi de dikkat çekmektedir.

Davalarla ilgili göze çarpan husus AIHM'nin elektronik gözetimi değerlendirirken iki yola başvurduğu görülmektedir. Bunlardan ilki, iç hukukta yürürlükte olan kanunun niteliği olarak karşımıza çıkmaktadır. Örneğin mevcut iç hukukta kanun detaylı olarak tanımlanmış mı veya hukukun üstünlüğü ilkesi gözetilmiş mi? İkincisi ise hem alınan tedbirlerin kapsamı, uygulamaki açık ve detaylı kurallar, elde edilen bilginin ne kadar süre ile saklanacağı veya ne zaman imha edileceği gibi veri gizliliğini korumayı amaçlayan prosedürlerden oluşmaktadır. Böylece mahkemenin verilere üçüncü tarafların erişimini, verileri kötüye kullanma ve keyfiyetin önüne geçmeyi engellemeyi amaçladığı görülmektedir.

3.2.2. Kişisel Veri ve Kişisel Verilerin Korunması

Kişisel Veri ve Kişisel Verilerin Korunması özel hayatın gizliliği hakkında en çok müdahale edilen alanlardan biri olarak karşımıza çıkmaktadır. Gerek yapay zeka teknolojisinin gelişmesi gerekse bilgi iletişim teknolojileri kişisel verilerin bireyin rızası dışında hem hükümetler hem de özel şirketler tarafından kolaylıkla elde edilmesine olanak tanımaktadır. Yeni teknolojilerle ilgili dava örneklerinden bazıları aşağıda yer almaktadır.

MD and Others v. Spain Davası (2022) ; Dava, Katalonya polisinin, Katalonya'nın İspanya'dan bağımsızlığı konusunda belirli görüşler ifade eden yargıçlar hakkında bilgi toplayıp dosyalamasıyla ilgilidir. Aynı yılın mart ayında La Razón gazetesi, yargıçların bildirileri hakkında "otuz üç ayrılıkçı yargıcın komplosu" başlıklı bir makale yayımlamıştır. Makale, başvuruçuların polis veri tabanından alınan kişisel bilgilerini (adlarını, fotoğraflarını, çalıştıkları mahkemeleri ve bazı durumlarda siyasi görüşlerini) içermektedir. Ayrıca kişisel bilgilerin yanısıra başvuruçuların siyasi görüşlerinin de yine ilgili veri tabanında yer aldığı görülmektedir. Başvuranlar özel hayata ve aile hayatına saygı, ifade özgürlüğü ve adil yargılanma haklarının ihlal edildiğini ileri sürerek, AIHS'nin 8, 10 ve 6. maddelerine dayanarak, şikayetçi olmuşlardır.

Yerel makamların kişisel bilgilerin sızdırılması ile ilgili olarak veritabanlarından sorumlu kişinin ifadesini almamasından dolayı da devletin kişisel verileri koruma konusunda sorumluluğunu yerine getirmediği tespit edilmiştir. Bu bağlamda da AİHM'ne göre devletin, bu soruşturma adımını yerine getirmemesi nedeniyle Sözleşme'nin 8. maddesi kapsamındaki yükümlülüklerini yerine getirmemiş olduğu ve 8. maddede yer alan kişilerin verilerin korunması hakkını ihlal ettiği mahkeme tarafından belirlenmiştir.

Volodina v. Russia Davası (2021); Dava, Rus makamlarının, başvuran adına sahte profiller oluşturan, özel hayatı ile ilgili fotoğraflarını yayınlayan, hareketlerini takip eden ve sosyal medya aracılığıyla ölüm tehditleri gönderen eski partnerinin tekrarlayan siber şiddetine karşı, onu korumadığı iddiasıyla ilgilidir. Başvuran, özellikle Rus yasalarının çevrimiçi takip veya başvuranın çevrimiçi ortamda kimliğine bürünme gibi aile içi şiddetin siber uzayda alabileceği tezahürleri açıkça hedef almamasını Sözleşme'nin 8. maddesine (özel hayata saygı hakkı) dayanarak ihlal edildiğini iddia etmiştir.

Failin cezasız kalması, Devlet mekanizmasının kadınları siber şiddetten korumak için yeterince caydırıcı bir etki yaratma kabiliyetinden şüphe duyulmasına neden olmuştur. Mahkeme, Rus makamlarının Sözleşme'nin 8. Maddesinin ihlal edildiğine karar vermiş ve Rus makamlarının başvuranı ağır istismardan korumak için bu hüküm kapsamındaki pozitif yükümlülüklerini yerine getirmediğini tespit etmiştir.

S. and Marper v. The United Kingdom Davası (2008); Büyük Britanya ve Kuzey İrlanda Birleşik Krallıklarına karşı, iki Britanya vatandaşı parmak izlerinin, DNA örneklerinin ve DNA profillerinin, haklarındaki cezai takibatın sona ermesinden sonra belirsiz süre için saklanması AİHS'nin 8. Maddesi kapsamındaki haklarının ihlali olduğunu iddia etmiştir. Bu davada önemli olan nokta Mahkeme'nin teknolojinin gelişimini dikkate almasıdır: "Genetik ve bilgi teknolojisi alanındaki gelişmelerin hızlı temposunu göz önünde bulunduran Mahkeme, gelecekte genetik bilgilerle bağlantılı özel hayat menfaatlerinin yeni şekillerde veya bugün kesin olarak öngörülemeyen bir şekilde olumsuz etkilenebileceği ihtimalini göz ardı edemez "(S. and Marper, 2008, paragraf 71) demektedir.

Ayrıca Mahkeme DNA verileri depolamanın muhtemel etnik kökene dair bilgi verdiğini belirtmektedir. Davanın başvuruçuları, kendileri hakkında depolanan verilerin sadece ulusal polis için değil, bunun dışında elli altı kuruluşun daha bu bilgilere erişebildiğini beyan etmişlerdir (S. and Harper, 2008, paragraf 87). Mahkeme DNA örneklerinin ve DNA profillerinin muhafaza edilmesinin başvuranların “özel yaşamlarına saygı gösterilmesi haklarına orantısız şekilde saldırı oluşturduğuna ve demokratik bir toplumda gerekli olmadığına” kanaat getirerek AİHS 8. Madde kapsamında ihlalin olduğuna karar vermiştir(S. and Harper, 2008, paragraf 125-126).

Gaughran v. the United Kingdom Davası (2020); Bu dava, aşırı alkol kullanan bir kişinin tutuklandıktan sonra fotoğrafı, parmak izi ve DNA örneğinin alınması ve bu örneklerin polis teşkilatının kayıtlarında süresiz olarak tutumayı amaçlamasıyla ilgilidir. Mahkeme sadece alıkoyma süresinin sınırsızlığına değil, aynı zamanda sistemdeki denetim eksikliğine de odaklanmıştır (Gaughran,2020, paragraf 96).

Mahkemenin fotoğrafların saklanması başvuranın 8. Madde kapsamındaki hakkına bir müdahale olarak değerlendirilmiştir:

Başvuranın gözetiminde çekilen fotoğrafının yakalandıktan sonra çekildiği ve polis tarafından kullanılmak üzere yerel bir veri tabanında süresiz olarak tutulacağı ve polisin muhtemelen fotoğrafa yüz tanıma ve yüz haritalama teknikleri de uygulayacağı göz önüne alındığında, başvuranın fotoğrafının çekilmesi ve saklanması özel yaşam hakkına bir müdahale teşkil etmiştir (Gaughran,2020, paragraf 70).

Mahkeme başvuranın verilerinin saklanması, belirli güvencelerden yoksun olduğu ve çatışan kamu ve özel çıkarlar arasında adil bir denge kuramadığından dolayı 8.maddenin ihlal edildiğine karar vermiştir.

Aycaquer v. France Davası (2017); Gösteticiler ve jandarma arasında çıkan arbede sonucu tutuklanan başvuranın, ulusal DNA veri tabanına dahil edilmek üzere DNA örneği istenmiş ancak başvuran DNA örneğini vermeyi reddetmiş ve bunun bir sonucu olarak da tutuklanmıştır. Başvuran özel hayata saygı hakkının ihlal edildiği gerekçesiyle mahkemeye başvurmuştur.

Mahkeme ilk olarak "saklanan dosyanın amacına ve söz konusu suçların niteliğine ve/veya ciddiyetine bağlı olarak bu tür kişisel verilerin saklanma süresinin belirlenmesi" şartının kurum tarafından belirtilmediğini dile getirmiştir (Aycaguer, 2017, paragraf, 43). İkinci olarak saklanan DNA profillerinin saklama süresinin ilişkin mevcut düzenleme olmadığı ve silinemediğinden dolayı veri sahiplerine yeterli koruma sağlamadığını karar vermiştir (Aycaguer, 2017, paragraf, 45). Bu nedenlerden dolayı da yönetmeliklerin kamu ve özel çıkarlar arasında adil denge kuramadığından, başvuranın özel hayata saygı hakkının ihlal edildiğine karar vermiştir.

AİHM kararlarına baktığımızda ise kişisel verilerin özel hayatın gizliliği hakkı çerçevesinde yorumlandığı dava sonuçlarında görülmektedir. Bu kişisel verilerin bireyin özel hayatıyla ve bireyin kimliğinin belirlenebilmesine ve/veya belirlenebilir olması ile ilgili bir durum olarak karşımıza çıkmaktadır.

Mahkeme özel hayat terimini geniş yorumladığı gibi, teknolojinin gelişmesinden dolayı kişisel veri kavramını da geniş bir şekilde yorumladığı görülmektedir. Teknolojinin gelişmesi ile birlikte kişisel veriler ad, soyad, ev adresi, doğum tarihi gibi verilerin kapsamını da genişleterek IP adresleri, DNA, GPS verileri gibi verilerin de eklendiği görülmektedir. IP adresi, GPS gibi verilerin bireyin yer tespitini yaparak bireyin kimliğinin belirlenmesine neden olmaktadır. DNA verileri ise bireyin genetik bilgileri ve hassas bilgileri arasında yer almakta ve üçüncü tarafların eline geçmesi durumunda birey genetik olarak kodlanabilmekte ve ayrımcılığa maruz kalabilmektedir. DNA verileri değiştirilemez ve sabit olduğundan dolayı özellikle bireysel özerklik açısından büyük önem arz etmektedir.

Mahkemenin ilgili davalarda bir diğer göz önüne aldığı husus kişilerin verilerin ne kadar süre ile saklanabileceğidir. Genellikle yasalarda kişisel verilerin güvenlik amacıyla bireyden alınabileceği belirtilmiş ancak bireyden elde edilen verilerin ne kadar süre ile saklanacağı belirtilmemiştir. Verilerin sınırsız süre ile saklanması ve silinememesi de mahkeme tarafından özel hayatın gizliliğinin ihlali olarak değerlendirilmektedir.

Bir başka göz önünde bulundurulacak husus kişisel verilerin toplanmasında belirli meşru amaçların gözetilmesi gerekliliğidir. Bu da devletlerin keyfi müdahalesine karşı

bireyin haklarının korunması anlamına gelmektedir. Mahkeme kişisel verilerin toplanması, depolanması ve işlenmesi sürecinde adil, şeffaf ve hukuka uygun olunması, doğruluğu ve ilgililiği ile de karar verdiği görülmektedir. Bu da devletlerin iç hukukunun tekrar gözden geçirilip, bu kriterlerin eklenmesinde önemli rol oynadığı görülmektedir.

3.2.3. Yazışmalar (Haberleşme)

Siber uzayda özel hayatın gizliliği hakkının en çok suistimale uğradığı bir diğer alan yazışmalar olarak karşımıza çıkmaktadır.

Copland v. United Kingdom Davası (2007); Dava, Birleşik Krallık Hükümetinin sorumluluğu altında yönetilen bir kolej, bir çalışanın 1991-1999 yılları arasında telefon, e-posta ve internet kullanımının izlenmesiyle ilgilidir. Copland, yapılan bu izlemenin Avrupa İnsan Hakları Sözleşmesi'nin 8(1) maddesi ile güvence altına alınan özel hayatın gizliliği ve yazışma haklarını ihlal ettiğini iddia etmiştir. Mahkeme içtihadına göre;

İş yerinden yapılan telefon görüşmeleri, 8 (1) maddesinin amaçları doğrultusunda "özel hayat" ve "yazışma" kavramları kapsamındadır... Mantıksal olarak, kişisel internet kullanımının izlenmesinden elde edilen bilgiler gibi, iş yerinden gönderilen e-postaların da benzer şekilde 8. Madde kapsamında korunması gerektiği sonucuna varılmaktadır (Copland, 2007, paragraf 41).

“Mevcut davada başvurana, aramalarının izlenebileceğine dair herhangi bir uyarı yapılmamıştır, bu nedenle iş telefonundan yapılan aramaların gizliliğine ilişkin makul bir beklentisi vardır. Aynı beklenti başvuranın e-posta ve internet kullanımı için de geçerli olmalıdır (Copland, 2007, paragraf 42) ”.

Bu kararın AIHS 8(1) fıkrasının sadece işyerinden yapılan telefon görüşmelerini değil, aynı zamanda e-posta ve internet kullanımı için de geçerli olduğunu teyit etmektedir. Mahkeme, 8. madde kapsamında kişinin özel hayatına ve haberleşmesine saygı gösterilmesi hakkına bir müdahale teşkil ettiği kanaatindedir.

Roman Zakharov v. Russia Davası (2015); Aralık 2003'te, gazeteci ve Glasnost Savunma Vakfı'nın bir şubesinin başkanı Roman Zakharov, telefon görüşmelerinin

adli bir izin almaksızın gizli dinlenmesi sisteminin özel hayatına ve yazışmalarına saygı gösterilmesi hakkını ihlal ettiğini iddia etmiştir.

Mahkeme Rus hukuku tarafından izin verilen izleme tedbirlerinin, ulusal güvenlik ve kamu güvenliğinin korunması, suçun önlenmesi ve ülkenin ekonomik refahının korunması gibi meşru amaçlar güttüğünü dile getirmektedir (Zakharov, 2015, paragraf 237). Ancak Mahkeme, Rus kamu makamlarının hangi koşullarda gizli izleme tedbirlerine başvurma yetkisine sahip olduğu, bu tür eylemlerin süresi, özellikle de hangi koşullar altında sonlandırılmaları gerektiği, dinlemeye izin verilmesi ve dinlenen verilerin saklanması ve imha edilmesine ilişkin usullerin eksikliği ve dinleme denetiminin olmaması nedeniyle AIHS 8. Maddesinin ihlal edildiğine karar vermiştir (Zakharov, 2015, paragraf 302-304).

Robathin v. Austria Davası (2012); 2006 yılında davacı olan avukatın hakkında hırsızlık, ağırlaştırılmış dolandırıcılık ve zimmete para geçirme şüphesiyle ceza davası açılmıştır. Dava esnasında avukatlık bürosunda yapılan aramadan ve belgelerin yanı sıra tüm elektronik verilerine el konulmasının AIHS 8. Maddesi kapsamında yazışmalara hakkını ihlal ettiğini belirtmiştir.

Mahkeme, arama emrinde yalnızca kısa ve oldukça genel gerekçeler verildiğini, dolayısıyla tüm elektronik verilerin genel ve sınırsız bir şekilde aranmasına ve el konulmasına izin verildiğini kaydetmiştir. Bu koşullar altında Mahkeme, arama izninin kapsamı makul bir şekilde sınırlandırılmamış olduğunu ve tüm verilere el konulmasının ve incelenmesinin meşru amaca ulaşmak için gerekli olanın dışına çıktığını (orantısız) tespit ederek yazışmalar saygı hakkının ihlal edildiğini kabul etmiştir.

Buturugă v. Romania Davası (2020); Bu dava, başvuranın eski kocası tarafından aile içi şiddet uygulandığı ve elektronik yazışmaların gizliliğinin ihlal edildiği iddialarıyla ilgilidir. Buturugă, özellikle 3. Madde (işkence ve insanlık dışı veya aşağılayıcı muamele yasağı) ve 8. Maddeye (özel ve aile hayatına ve haberleşmeye saygı hakkı) dayanarak AIHM'ye başvuru yapmıştır. Mahkeme'nin aile içi istismarın bir yönü olarak siber zorbalığa ilişkin yorumları önem arz etmektedir.

...siber zorbalık řu anda kadınlara ve kız çocuklarına yönelik řiddetin bir yönü olarak kabul edilmektedir ve siber gizliliğin ihlali, mağdurun bilgisayarına izinsiz girilmesi ve özel veriler de dahil olmak üzere veri ve görüntülerin ele geçirilmesi, paylaşılması ve manipüle edilmesi gibi çeşitli şekillerde olabilir. Aile içi řiddet bağlamında, siber gözetleme genellikle kişinin yakın partneri tarafından gerçekleştirilmektedir... (Buturugă, 2020, paragraf 74).

Bu davada siber zorbalığın yalnızca 8.madde kapsamında değil, AİHS'nin 3. Maddesi ve 8.maddesi ile birlikte ele alındığı görölmektedir. Sonuç olarak ilgili davada devletin pozitif yükümlölüklerini yerine getirmediğı ilgili maddelerin ihlal edildiğine karar verilmiştir.

Bărbulescu v. Romania Davası (2017); Dava özel bir řirketin çalışanı olan Bărbulescu'nun, elektronik haberleşmelerini izledikten ve bu haberleşmenin içeriklerine ulaştıktıktan sonra işverenin çalışanın sözleşmesini feshederek işten çıkartılmasıyla ilgilidir. Bay Bărbulescu sözleşmesinin feshedilmesini AİHS'nin 8. maddesine (özel ve aile hayatına, konuta ve haberleşmeye saygı hakkı) dayanarak hayatının gizliliğinin ihlaline dayandığından ve yerel mahkemelerin özel hayatına ve haberleşmesine saygı hakkını korumadığından şikayetçi olmuştur.

Mahkeme ilgili davada iletişimin 8. madde tarafından korunup korunmadığının değerlendirilmesinde belirleyici olmayan ancak önemli bir faktör olarak "makul özel hayat beklentisi" ilkesinin altını çizmiştir (Bărbulescu, 2017, paragraf 56). Buna göre, işverenin talimatları doğrultusunda işyerindeki özel sosyal hayatın sıfırlanamaz olduğu belirtilmiştir (Bărbulescu, 2017, paragraf 80). Özel hayata ve yazışmaların gizliliğine saygı, gerekli olduğu ölçüde kısıtlansa bile, varlığını sürdürmektedir.

Ayrıca, "bir kişinin internet kullanımının izlenmesinden elde edilen bilgiler gibi, 8. madde kapsamında benzer korumadan yararlanan işyerinden gönderilen e-postalar için de geçerlidir (Bărbulescu, 2017, paragraf 72). Bir başka deyişle, bir kişinin işyerinden gönderilse bile anlık iletişimlari "yazışma" olarak nitelendirilmektedir.

Sonuç olarak Mahkeme, ulusal makamların Bay Bărbulescu'nun özel hayatına ve haberleşmesine saygı hakkına yeterli koruma sağlamadığı ve söz konusu menfaatler

arasında adil bir denge kurmadığı kanatine vardığından dolayı yazışmalara saygı hakkının ihlal edildiği sonucuna varmıştır.

Yeni teknolojilerin kullanılmasının haberleşmesinin gizliliğini hangi açılardan ihlal ettiğini örnek davalar ile gösterilmeye çalışılmıştır. AİHS’de yazışmaların kapsamının genel bir tanımı olmadığı ve yazışmaları dava özelinde bir başka deyişle bireysel olarak değerlendirdiği görülmektedir. Her ne kadar bu durum yazışmayı oluşturulan çerçevenin sınırlarının belirlenmesine zorluk oluştursa da bu durum aynı zamanda mahkeme içtihatlarının daha kapsamlı ve teknolojik gelişmeler ışığında daha esnek bir şekilde değerlendirilmesine olanak tanımaktadır.

Dava örneklerine bakıldığında yeni teknolojiler olarak, elektronik yazışmaların, e-postaların, internetten haberleşmenin izlenmesi, elektronik yazışmalarının gizliliğinin ihlali veya elektronik verilere el koyma yöntemiyle haberleşmenin AİHS kapsamında ihlal edildiği görülmektedir.

AİHM kararlarına bakıldığında, mahkemenin verdiği kararların da teknolojinin gelişmesi ile birlikte teknolojiye ayak uyduracak şekilde kapsamının kademeli olarak geliştirildiği görülmektedir. Örneğin, Klass and Others v. Germany Davasında (1978) ilk defa telefon konuşmaları özel hayatın gizliliği hakkının bir bütünü olarak tanımlanmıştır. “Her ne kadar telefon görüşmeleri 8. maddenin 1. paragrafında (madde 8-1) açıkça belirtilmemiş olsa da, Mahkeme, Komisyon gibi, bu tür görüşmelerin bu hükümde atıfta bulunulan "özel hayat" ve "yazışma" kavramlarının kapsamına girdiğini düşünmektedir“ (1978, paragraf 41).

Mahkeme daha sonra 2007 yılında Copland v Birleşik Krallık davasında 8.maddenin kapsamını genişleterek, başvuranın e-posta ve internet kullanımına ilişkin kişisel bilgilerin toplanması ve saklanması yazışma ve özel hayata saygı hakkıyla ilgili sorunları gündeme getirdiğine karar vermiştir. Böylece e-posta ve internet tabanlı yazışmalar da artık 8.maddenin bir başka yönü olarak karşımıza çıkmaktadır. Bu minvalde artık yazışmaların içeriğine bakılmazsınız, iş yerlerinde gerçekleşen yazışmaların yanı sıra şahsi yazışmalar da bu kapsam içerisine girmektedir.

AIHM kararlarının bilgi iletişim teknolojisindeki yeniliklere ayak uydurmaya çalıştığı görülmektedir. Yazışma teriminin klasik kapsamı olan mektup, telgraf, teleks ve telefon konuşmalarının kapsamının genişletilerek, e-posta ve internette yapılan tüm yazışmaları da içerecek şekilde yorumlandığı ifade edilebilir. Ayrıca klasik kapsamda olan yazışmalar ev sınırlarından çıkarılarak, bireyin iş yerinde yaptığı yazışmaların da bu kapsama dahil edildiği örnek kararlardan çıkarılabilmektedir.

Ayrıca ilgili davalarda AIHS'nin 8.maddesinin 2.paragrafına atıfta bulunularak yazışmaların „hukukun üstünlüğü“ ilkesine uygun olarak, iç hukukta tanımlanıp tanımlanmadığına bakılmış ve bireyin hangi durumlarda yazışmalarına el konacağıının veya hangi durumda bu yazışmaların izlenebileceğinin belirlenmesinin de gerekli olduğunu vurgulamıştır.

Sonuç olarak AIHM, 8. maddenin kapsamı ile ilgili olarak, telefon, faks, e-posta ve diğer gizli iletişimlerle kişisel internet kullanımının "yazışma" kavramları kapsamında olduğuna karar vermiştir. Bunun yanı sıra evlerin gizlice aranması ve gözetlenmesi, posta ve paketlerin kontrol edilmesi, elektronik iletişim ve elektronik verilerin incelenmesi veya kayıt altına alınmasında "yazışma" bağlamında değerlendirilebileceği görülmektedir.

Bölüm Değerlendirmesi

Siber gözetim, siber istihbarat ve kişisel veriler özel hayatın gizliliği hakkını siber uzayda en çok ihlal eden yöntemler olarak karşımıza çıkmaktadır. Fiziki alanda zaten varolan bu yöntemler dijital teknolojilerin gelişmesi sonucu siber uzay'a taşınarak kapsamlarını genişlettikleri görülmektedir. Siber gözetim günümüzde CCTV kameraları, biyometrik gözetim, işitsel gözetim, internet gözetimi ve özelde de sosyal medya gözetimi olarak karşımıza çıkmaktadır.

Siber istihbaratta ise ön planda olan aktörler özel şirketler ve devletlerdir. Devletlerin ve özel şirketlerin özellikle ECHELON, PRISM veya XKEYSTORE gibi istihbarat sistemlerini kullanması ve elde edilen verileri yapay zeka aracılığı ile ayrıştırıp veri haline getirmesi hem kitlesel gözetime neden olmakta hem de verilerin yanlış kodlanma sonucunu doğurabilmektedir. Ayrıca bu sistemlerin yanı sıra açık

kaynak istihbaratı ve sinyal istihbaratı kullanımı da özel hayatın gizliliğini hakkını ihlal etmektedir.

Bireyin bilgilerine yetkisiz erişim ve bu bilgilerin üçüncü taraflar tarafından bireyin rızası olmadan kullanımı kişisel verilerin ihlali anlamına gelmektedir. İnternette attığımız her adımın veri olarak kodlandığı bir dünyada, kişisel veriler en çok Büyük Veri analitiği ve Nesnelerin İnterneti kullanımı sonucunda ihlale uğradığı görülmektedir. Büyük verinin, herhangi bir amaç olmadan tüm verileri elde etme amacı gütmesi ve tahmine dayalı çıkarımlar yapması nedeniyle özel hayatın gizliliği hakkını ihlal ederken, nesnelerin interneti izleme, dinleme ve veri toplama nedeniyle bu hakkı ihlal ettiği görülmektedir.

Siber gözetim, siber istihbarat ve kişisel verilerin ihlalinin en büyük ortak noktası ise bireyin haberi ve rızası olmadan bu eylemlerin gerçekleştirilmesi olarak karşımıza çıkmaktadır.

AIHM'nin kararları genel olarak incelendiğinde, kararların teknolojik gelişmeler çerçevesinde alındığı görülmektedir. Ancak davalar ve mahkemenin hızının yine de teknolojinin gerisinde kaldığını da ayrıca belirtmek gerekmektedir. AIHM bilgi iletişim teknolojilerinde olan gelişmeler çerçevesinde verdiği kararları “Yeni Teknolojiler (New Technologies)” olarak isimlendirmektedir (ECHR,2022). En son 2022 yılında Yeni Teknolojiler dava kararlarını yayımladığı görülmektedir. Ancak belgede yeni teknolojilerin tanımının yapılmadığı bunun yerine kullanılan yöntemler ele alınarak kategorizasyona gidildiği görülmektedir. İlgili belge incelendiğinde yeni teknolojileri 12 kategoriye ayırdığı görülmektedir. Bu kategoriler; elektronik veri (Electronic Data), E-mail, GPS (Global Positioning System), İnternet, Cep Telefonu (Mobile Telephone), Kitap ve müzik eserlerinin telif hakları (Copyright of books and musical work), Çevrimiçi Taciz (Online harassment), Kablosuz iletişim (Radio communications), Uydu Anteni (Satellite dish), Uzaktan iletişim (Telecommunications), Gizli Kamera Kullanımı (Use of hidden cameras) ve Video Gözetimi (Video surveillance)dir (ECHR, 2022, s. 1-29)

Davalara bakıldığında ise en çok davanın özel hayatın gizliliği hakkı kapsamında olduğu görülmektedir. Bu kapsamda açılan 38 davadan 27 tanesi bu hakkın ihlal

edildiği kararına bağlanmış, onbir davada da ihlal olmadığına kanaat getirilmiştir. Özel hayatın gizliliğinden sonra en çok açılan dava ifade özgürlüğü kapsamında karşımıza çıkmaktadır. İfade özgürlüğü bağlamında ise toplam 20 dava açılmış ve 13 davada ihlal olduğu, 7 dava da ise ihlal olmadığı karara bağlanmıştır. Davalardan da görüleceği üzere yeni teknolojilerin kullanımı en çok özel hayatı olumsuz olarak etkilemektedir.

Siber uzayda yeni teknolojilerin kullanımında yapay zekanın neredeyse her alanda kullanımı söz konusudur. Ancak dava kararlarında yapay zekaya değinilmediği görülmektedir. Oysaki yapay zeka kullanımı gözetim, istihbarat ve veri toplama konularında aktif olarak kullanıldığı bilinmektedir. Bir başka değinilmesi gereken husus ise özel hayatın bileşenleri olan “konuta müdahale etmeme” ve “ad, şan, şöhret (bireyin itibarı)” ile ilgilidir. Konuta müdahale etmeme hakkı teknolojik gelişmeler çerçevesinde daha geniş olarak tanımlanmış ancak dava kararlarında bu hakka değinilmediği görülmektedir. Aynı şekilde bireyin itibarı, bireyin toplum içerisinde yaşaması için elzemdir ve yeni teknolojinin kullanılmasından doğrudan etkilenmektedir. Ancak bireyin itibarının zedelenmesi yönünde dava kararı olmadığı görülmektedir.

Bir başka göze çarpan husus ise özellikle kişisel verilerin toplanmasında büyük bir paya sahip olan nesnelerin internetine değinilmemiş olmasıdır. Oysaki nesnelerin interneti büyük bir hızla gelişmekte elektronik verinin, cep telefonunun vb. cihazların kullanımı sonucunda verileri kaydedip depolamaktadır. Günümüzde de siber uzayda önemli bir yere sahip olan bu teknolojinin gelecekte de daha çok ihlale neden olabileceği tahmin edilmektedir.

AİHM kararlarını yeni teknolojiler açısından genel olarak değerlendirdiğimizde kararların teknoloji bağlamında genişletilip, sözleşmeden doğan hakların daha kapsamlı tanımlandığı görülmektedir. Ancak yine de bu kararlar teknolojinin gelişme hızına ayak uyduramadığı da göz ardı edilemeyecek bir gerçek olarak karşımıza çıkmaktadır.

BULGULAR VE ANALİZ

1948 yılında EİHB'nin kabul edilmesinden günümüze toplumların BİT'lerin gelişmesi sonucu hızlı bir ilerleme kaydettiği görülmektedir. BİT'ler bir yandan bireylerin hak ve haklara erişim olanaklarını geliştirerek bilgiye kolayca ulaşmayı sağlamış, bir yandan da sınırları aşarak bireyi ulusal düzeyden küresel düzeye taşımıştır. Teknolojik gelişmelerdeki bu değişimin kaçınılmaz olarak insan haklarını etkilediği bu çalışmada tespit edilmiştir. Etki iki yönlü olarak görülmektedir. İlk olarak teknolojik gelişimin, insan hakları ve insan haklarıyla ilgili olguları daha ileriye taşıdığı gözlemlenmektedir. Örneğin, internet kullanımının 1990lardan sonra yaygınlaşmasıyla birlikte, bilgiye erişim ve iletişim konusunda ulusal sınırlar kalkmış, her bir birey böylece eğitim, ifade özgürlüğü, toplanma ve örgütlenme özgürlüğü haklarından daha kolay faydalanabilir hale gelmiştir. Ayrıca yine BİT'lerin gelişmesi sayesinde sanal kamusal alanlar oluşturularak, devlet temelli ihlallere karşı kamuoyu oluşturulmuş ve böylece demokratik ortamların oluşturulmasının sağlandığı görülmektedir. İkinci yönü ise, gelişen teknolojilerin insan hakları ihlallerini de beraberinde getirmesi olarak karşımıza çıkmaktadır. Siber uzayda aktörlerin çoğalıp çeşitlenmesi özellikle çok uluslu şirketlerin alana hakimiyeti veri gizliliği, gözetim ve istihbarat çalışmalarını da beraberinde getirmektedir. Devletler ve çok uluslu şirketler kişisel verilere kolaylıkla erişebilmekte, bu da insan hakları, dijital bilgi güvenliği ve özel hayata saygı hakkı ile ilgili sorunları gündeme getirmektedir.

Yapılan çalışma sonucunda BİT'nin insan hakları arasında en çok özel hayatın gizliliği hakkını olumsuz yönde etkilediği görülmüştür. Günümüzde teknolojik gelişmeler ve özellikle büyük veri, yapay zeka kullanımı, nesnelerin interneti, siber gözetim ve siber istihbarat teknolojilerinin çok uluslu şirketler ve devlet kurumları tarafından kullanımının yaygınlaşması sonucu özel hayatın gizliliği hakkına büyük tehdit oluşturduğu tespit edilmiştir. Bireyin rızası dışında kişisel verilerin kolayca toplanabilmesi, depolanması ve sınırsız süre ile saklanması bireyin en mahrem verilerinin üçüncü tarafların eline geçmesi riski bireyi siber uzayda tehdit eder hale gelmiştir. Örneğin, GPS verileri sayesinde suçluların konumu belirlenebilmekte, yapay zeka sayesinde bireylerin biyometrik verileri kullanılarak suçluların sistemle eşleştirip kimlik tespiti yapılabilmekte ve hatta adli tıp DNA sayesinde suçlu bireylerin

kimliğini kolayca bulabilmektedir. Ancak yukarıda belirtilen tüm örnekler aynı zamanda özel hayatı da tehdit etmektedir. GPS verileri sayesinde devletler vatandaşlarını kolayca gözetlemekte, yapay zeka sayesinde bireyin biyometrik verisi başka bir kişi ile eşleştirilebilmekte ve bireyin DNA örneğinin kötüye kullanım amacıyla başka kişilerin eline geçmesi, bireyin benzeri görülmemiş risklere de maruz kalması anlamına gelmektedir.

Özel hayatın gizliliği hakkına uluslararası belgelerde yer verildiği tespit edilmiştir. Bu hakkın “Evrensel İnsan Hakları Beyannamesi”nin 12. Maddesi, “Sivil ve Siyasal Haklar Konvansiyonu”nun 17. Maddesi, “Avrupa İnsan Hakları Sözleşmesi”nin 8. Maddesi, “Avrupa Konseyi Siber Suç Sözleşmesi”nin 3.maddesi, “Biyotıp Sözleşmesi”nin 10. Maddesi, “Amerikan İnsan Hakları Sözleşmesi”nin 11.maddesi, “Avrupa Birliği Temel Haklar Şartı”nın 7.maddesi, “Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi”nin 8.maddesi ve “Bilgi Teknolojileri Suçlarıyla Mücadeleye İlişkin Arap Sözleşmesi”nin 14.maddesinde ele alındığı görülmektedir.

Bahsi geçen tüm anlaşmalar özel hayatın gizliliği hakkını temel bir insan hakkı olarak tanımakta ve korumaktadır. Ayrıca ulusal sınırlar içerisinde devletlere bu hakka saygı gösterme, koruma ve gerekli görüldüğü taktirde pozitif yükümlülükleri uygulama ana hatlarıyla belirlenmektedir. İnsan hakları sözleşmeleri bireyin ailesine, iletişimine, özel hayatına, evine keyfi ve yasadışı müdahaleyi yasaklarken, Biyotıp ve siber güvenlikle ilgili olan sözleşmeler daha çok tıbbi ve kişisel verilerin korunmasına odaklanmaktadır.

Özel hayatın gizliliği hakkının temel bir insan hakkı olduğu ve korunması gerekliliği konusunda uluslararası bir oydaşma olsa da, bu hakkın bölgesel ve uluslararası sözleşmelerde tanımının açıkça yapılmadığı görülmektedir. Bu hak yalnız kalma hakkı, özel hayat, iletişimin gizliliği, kişisel özerklik ve keyfi müdahaleden korunmayı gibi unsurları da kapsayan çok yönlü ve karmaşık bir hak olarak karşımıza çıkmaktadır. Uluslararası ve bölgesel sözleşmelerde özel hayatın gizliliği hakkı için birçok unsuru kapsayacak şekilde geniş ve açık uçlu bir dil kullanılmaktadır. Bu da hakkın daha geniş kapsamlı olarak farklı bağlamlarla ilintili olarak yorumlanabilmesi ve uyarlanabilmesine olanak sağlamaktadır.

Toplumların sosyal ve kültürel çeşitlilikleri de bu hakkın tanımlanması ve uygulanmasında farklılık gösterebilmektedir. Birtakım farklılıklara rağmen sözleşmelerde bu hakkın temelinde etik ve yasal çerçevenin korunmasının gerekliliğinin vurgulandığı görülmektedir. Bu çerçevenin genel kapsamda devletlere hakka müdahale etmeme gibi negatif ve hakkı koruma bağlamında pozitif yükümlülükler getirdiği görülmektedir.

Özel hayatın gizliliği hakkının kapsamı, ele alınış biçimi konusunda anlaşmalar arasındaki farklılıklar bulunmaktadır. EİHB, SSHK, AİHS, Avrupa Temel Haklar Şartı, Amerikan Sözleşmesi ve Biyotıp Sözleşmesi bu haktan doğrudan bahsederken, siber güvenlikle ilgili sözleşmelerde kişisel verilerin korunması gibi ilgili hükümler aracılığıyla dolaylı olarak bahsedildiği görülmektedir.

Özel hayatın gizliliği hakkının bağlayıcıyı sözleşmeden sözleşmeye farklılık göstermektedir. Örneğin bu hak EİHB’de bağlayıcı değilken SSHK’de bağlayıcı olarak karşımıza çıkmaktadır. Ancak yine de bir ülke uluslararası veya bölgesel sözleşmeye taraf olduktan sonra bu hakkı korumak ve saygı göstermekle yükümlü hale gelmektedir. Bölgesel insan hakları sözleşmelerinde bireylerin hakları devlet yetkilileri veya diğer kişiler tarafından ihlal edildiğinde, bireyler Avrupa İnsan Hakları Mahkemesi veya Amerikalılar Arası İnsan Hakları Komisyonuna başvurarak çözüm arayabilmektedir. Bu mahkemelerin kararları bağlayıcıdır. Yine AİHS ve Amerikan sözleşmesi gibi uluslararası bir sözleşme olan SSHK’da bağlayıcı özelliğe sahiptir. Bireyin hakları ihlal edildiğinde birey İnsan Hakları Komitesi gibi uluslararası kurumlara yasal yollarla başvuru yapabilmektedir. Görüldüğü üzere bu hakkın uygulamasının uluslararası sistem ve bölgesel sistemlerde farklılık göstermektedir. Bu bağlamda özel hayatın gizliliği hakkının korunması da bu sistemler çerçevesinde oluşturulan mekanizmalara ve uygulama süreçlerine bağlı olmaktadır.

Bölgesel olarak yapılan siber güvenlik sözleşmelerinin siber uzayda özel hayatın gizliliği hakkının büyük ölçüde ihlal edildiği ve ihmale açık olduğundan dolayı yapıldığı görülmektedir. Özellikle bilgi iletişim teknolojilerindeki gelişme, siber uzayda özel hayatın gizliliği hakkını etkileyerek hem birtakım yeni fırsatları hem de zorlukları beraberinde getirmiştir. Bir yandan internete, bilgiye erişim ve iletişim kolaylaşmış diğer yandan da siber gözetim, istihbarat ve kişisel verilerin toplanması

yaygınlaşmıştır. Bireye ait bilgilerin bireyin rızası dışında toplanması ve depolanıp kullanılması bireyin özel hayatın gizliliği hakkını çoğu zaman ihlal edebilmektedir. Ayrıca bunların yanı sıra bireyler çevrimiçi dünyada gezinirken veya akıllı telefon/ ev eşyalarını kullanırken de bu ihlallere maruz kalmaktadırlar. Bu teknolojik gelişmenin bir sonucu olarak da siber uzayda özel hayatın gizliliği hakkı en çok ihlal edilen hak olarak karşımıza çıkmaktadır.

Uluslararası antlaşmalarda yer alan özel hayatın gizliliği hakkının unsurları, bu hakkın temel bir insan hakkı olarak tanımlanması ve korunması konusunda sağlam bir temel oluşturmuş olsa da, siber uzayın kendine özgü karmaşık ve çok yönlü yapısından dolayı uygulama kısmında birtakım zorlukları da beraberinde getirmektedir.

Uluslararası anlaşmaların hazırlanma süreci internetin ve hatta dijital teknolojilerin henüz yaygın olarak kullanılmadığı XX. yüzyıla dayanmaktadır. Bu yüzden bu belgeler hazırlanırken o dönemin siyasi ve toplumsal bağlamlarında ele alındıkları görülmektedir. Ancak günümüzde teknolojinin gelişmesiyle birlikte siber istihbarat, siber gözetim, veri ihlali, kişisel verilerin özel şirketler ve devletler tarafından toplanıp kayıt altına alınması ve depolanması gibi, uluslararası anlaşmalarda öngörülemeyen birtakım yeni ihlal türlerini de beraberinde getirmiştir.

Uluslararası anlaşmalarda yer alan özel hayatın gizliliği hakkının unsurları günümüzde “geleneksel” olarak isimlendirilmekte ve geçerliliğini hala korumaktadır. Ancak bu unsurların siber uzayda bu hakkı korumak için yeterli olmadığı görülmektedir. Sürekli değişen ve kendini yenileyen dijital ortamda teknolojinin doğasına uygun olarak bu hakkın kapsamı ve uygulama alanlarının geliştirilmesi ve hatta yeniden tanımlanması ve yorumlanması gerekmektedir.

SONUÇ

Elektronik cihazlar, cep telefonları, bilgisayarlar, kamera sistemleri, sosyal medya ve akıllı cihaz teknolojileri günümüzde baş döndürücü bir hızla gelişmektedir. Toplumun ve gündelik yaşamın bir parçası haline gelen yeni teknolojiler iletişim kurma, ticaret, ekonomi, siyaset gibi bireyin etkileşimde olduğu birçok alanı etkilemektedir. Özellikle internetin yaygın kullanımı ile birlikte bilgi iletişimin teknolojilerinin topluma entegrasyonunun, bireye yadsınamaz fayda sağladığı görülmektedir. İnsan hakları da bu gelişen teknolojilerden hem olumlu hem de olumsuz yönde etkilenmektedir. Geleneksel iletişim yöntemlerinin aksine siber uzayın bireylere çevrimiçi ortamda herhangi bir kısıtlama ve sınırlama olmadan fikirlerini açıkça beyan etme, uluslararası toplum nezdinde önemli bir bilgiyi paylaşma ve global olarak bilgiye erişim ve eğitim konusunda fırsatlar sunduğu görülmektedir. Bir başka deyişle bu dijital ortamın bilgiye erişim, bilgiyi kullanma ve paylaşma biçimlerimizi de dönüştürerek insan haklarını etkilediği gözlemlenmektedir.

İnternet bireylere güç verdiği gibi devletlere de bireyler üzerinde güç vermektedir. Özgürlüklerimiz ve kimliklerimiz verilerimizin seyahat ettiği yerlerde bulunmaktadır, bireylerin de velayetini alan hükümetler, bireylerin düşüncelerini, inançlarını, geçmişini, geçim kaynaklarını, hareketlerini ve itibarlarını da kontrol altına almaktadır (PoKempner, 2013, s.260). Bireyler toplum içerisinde bir taraftan bu yeni teknolojilere adapte olurken diğer taraftan da hızla gelişen teknolojinin bir sonucu olarak verileri kontrol etme ve yoğun bilgi akışı konusunda bilgi iletişim teknolojilerine ayak uyduramamaktadır. Siber uzayın ortaya çıkışı hükümetlerin ve çok uluslu şirketlerin bireyin özel alanına daha fazla müdahil olmasına neden olmaktadır. Bu durumun bir sonucu olarak da siber uzay bilginin gizliliği, güvenliği ve bütünlüğü açısından yeni tehditleri de beraberinde getirmiş ve bu durum da insan hakları ihlallerine yol açmıştır. Çevrimiçi ortamda bireylerin siber tehditlere daha açık ve hedefli bir şekilde maruz kalması birey açısından önemli güvenlik sorunları da beraberinde getirmektedir.

Siber uzayda devlet kurumlarından ziyade özel sektör alt yapı ve bilgilerin büyük bir kısmını kontrol etmektedir. Bu ortamda iletişim kurulduğu anda bireyin verileri altyapı sahibi olan ve bunları işleten özel şirketlere emanet edilmektedir. Özel

şirketlerin siber uzaydaki bu avantajlı konumu birtakım endişeleri de beraberinde getirmektedir. Öncelikle özel şirketler veri toplarken bireylerin özel hayatın gizliliği hakkı göz önüne alınmamakta ve sadece veri toplanmaktadır. İkincisi, özel olarak kabul edilen bilgilerin şirketler tarafından toplanması hukuk kurallarına aykırıdır. Bunun nedeni özel şirketlerin kolluk kuvveti olmak için gerekli donanımına sahip olmaması ve hesap verilebilirlik ilkesine tabi olmamalarından kaynaklanmaktadır (Souter, 2012, s. 22). Bu durum göz önünde bulundurulduğunda, bireyin özel ve kamusal alanı arasındaki sınırların da artık eskisi gibi kesin bir netlikle ayrıl(a)maması karşımıza çıkmaktadır. Önceden bireyin özel alanı olarak tanımlanan her bir unsur günümüzde kamusal veya yarı kamusal hale gelmiş bu da bireyi siber uzayda ihlale açık en zayıf aktör haline getirmiştir. Özellikle sosyal medya platformları sayesinde öncelikle özel şirketler bireyin bu özel alanına müdahil olmuş ve bu alanda bireyin var olan bilgilerini toplayıp kaydederek ve hatta özel şirketlere ve hükümetlere satarak muazzam bir kazanç elde etmişlerdir. 2010 yılında Facebook'un kurucusu Mark Zuckerberg'in "çevrimiçi sosyal ağların yükselişi, insanların artık özel hayatın gizliliği beklentisi olmadığı anlamına geliyor" (Johnson, 2010) demesi ve yine 2013 yılında "İnternet'in babası" olarak tabir edilen Vinton Cerf'in, "özel hayatın gizliliğinin bir anormallik olabileceğini" ve "özel hayata ulaşmanın bizim için giderek zorlaşacağını" (Edwards, 2013) ifade etmeleri özel hayatın aslında özel şirketler tarafından ihlal edildiğinin en büyük göstergesi olarak karşımıza çıkmaktadır. Tüm bu örnekleri dile getirirken 1999 yılında SUN Microsystems'in CEO'su Scott McNealy ünlü sözü olan "Zaten sıfır özel hayatınız var. Aş bunu..." (Hadas, 2019) söylemini de es geçmemek gereklidir. Bu örnekler her ne kadar tek bir söz olarak görünse de siber uzayda özel hayatın gizliliği hakkının teknoloji devleri tarafından ne şekilde ele alındığının en büyük göstergelerinden biri olarak karşımıza çıkmaktadır. Bu örnekleri biraz daha derinleştirmek gerekirse cep telefonu kullanımı ele almamız gerekmektedir. 2023 yılının ilk verilerine göre dünya çapında 6.925 milyar insan akıllı cep telefonu kullanmaktadır (Wise, 2023). Önümüzdeki bir iki yıl içerisinde de cep telefonu kullanıcılarının dünya nüfusunu geçmesi beklenmektedir. Cep telefonları artık hayatımızın ayrılmaz bir parçasını oluşturmakta ve evde unutulduğunda dahi geri dönüp alacak kadar günlük rutinlerimizin içerisinde yer almaktadır. Cep telefonları e-posta kontrolünde, fotoğraf, video, konum paylaşımında, yol tarifleri bulma için

kullanılabilmekte, oyun oynama, diğer bireylerle iletişim, banka hesabına erişim, fiziksel aktiviteler gibi çok geniş bir kullanım alanı sunmaktadır. Özellikle cep telefonlarının dahi her alanda bu kadar veri topladığı düşünülürse, siber uzayda bireyler açısından güvenlik açıklıkları ve siber tehdit yaratma olasılığının arttığı da söylenebilmektedir. Sosyal medya siteleri ve cep telefonları kullanımı bir araya geldiğinde dahi özel şirketlerin elinde nasıl muazzam bir veri barındırdıkları ve bireylerin özel hayatına nasıl müdahil olarak ihlal ettikleri daha kolay anlaşılmaktadır.

İnsan haklarının ilk kez Evrensel İnsan Hakları Beyannamesi ile oluşturulması iki dünya savaşının bir sonucu olarak karşımıza çıkmaktadır. Bu da tarihsel süreç içerisinde insan haklarının ihlal kaynaklı olarak ortaya çıktığını bizlere göstermektedir. Siber uzayın ortaya çıkışıyla özel hayatın gizliliği hakkının hükümetler ve özel şirketler tarafından açıkça ihlal edilmesi yeni insan hakları tanımlarını da beraberinde getirmiştir. İnternetin iletişimleri birbirine bağlaması ile daha çok iletişim hakları altında ele alınan bu haklar internete erişim hakkı, anonimlik hakkı ve unutulma hakkı çerçevesinde tartışılmaya başlanmıştır. İnterneti erişim hakkı bireylerin siber uzayda bilgiye erişimi ile ilgiliyken, anonimlik hakkı bireylerin kendi düşüncelerini herhangi bir baskı altında olmadan ifade etmesini sağlamaktadır. Unutulma hakkı ise bireyin rızası dışında siber uzayda paylaşılan bilgileri, verileri hakkında daha çok söz sahibi olması durumu olarak karşımıza çıkmaktadır. Görüldüğü üzere yeni tartışılan bu hakların hepsi siber uzayda bireyin özgürce hem kendini gerçekleştirmesine olanak tanımakta hem de olası ihlal durumunda bireyin toplum içindeki itibar, onur ve şöhretini korumayı amaçlamaktadır.

İnternete erişim hakkı, unutulma hakkı ve anonimlik hakkı gibi bilgi iletişim teknolojilerinin gelişmesiyle birlikte yeni hakların ortaya çıkması var olan hakların bireyi tam anlamıyla koruyamadığının göstergesi olarak da karşımıza çıkmaktadır. Söz konusu haklar dijital teknolojilerle birlikte ortaya çıkan ihlallere yanıt olarak gelişmiştir. Aynı zamanda bu hakların ortaya çıkışı eski hakların ortadan kalkmadığı ancak bu hakların da dahil edildiği uluslararası toplum tarafından tanınan ve korunan kapsamlı bir çerçeveye duyulan ihtiyacın bir göstergesidir. Böylesi yeni bir uluslararası sözleşmeye duyulan ihtiyaç elzem olsa da uluslararası toplumun bu konuda birtakım çekinceleri karşımıza çıkmaktadır.

Siber uzayda uluslararası bir sözleşmenin oluşturul(a)mamasının nedenleri olarak bazı çekinceler (argümanlar) olduğunu belirlemek gereklidir. Bu argümanları uluslararası toplumda var olan genel kanı ve devletlerin bakış açısı olarak ikiye ayırabilmek mümkündür. Uluslararası toplumda var olan genel kanı, temel insan haklarının değişmez olduğu veya olması gerektiği görüşüdür. Bu görüşe göre bilgi iletişim teknolojileri özellikle internet, dönüştürücü bir etkiye sahip olmaktan ziyade, insan haklarının kullanılabilmesi veya ihlal edilebileceği yöntemleri değiştirmektedir (Souter,2012 s.38). Bu yüzden mevcut insan hakları rejiminde yapılacak revizyonlar ile ilgili tüm haklar zaten uluslararası ve bölgesel metinlerde yer almaktadır. Dolayısıyla yeni bir uluslararası anlaşma gereksiz olarak kabul edilmekte hem de geleneksel insan haklarına zarar verecek daha geniş değişiklikleri de beraberinde getireceği için tehlikeli sayılmaktadır (Souter, 2012, s. 24). Hızla gelişen teknoloji karşısında yapılabilecek yeni bir bağlayıcı uluslararası anlaşmanın esneklikten yoksun olabileceğini savunmaktadırlar.

Uluslararası hukuk kapsamında devletlerin egemenliği ve bütünlüğü esastır. Devletler açısından ise, anarşik bir yapısı olan ve sınırları olmayan bir siber uzayda yönetişimin ne şekilde ele alınacağı sorusu gündeme gelmektedir. Siber uzayda toprak egemenliği olmaması, siber uzayın anarşik durumu ve kontrol edilemez doğası devletleri birtakım zorluklarla karşı karşıya bırakmaktadır.

Siber uzayın sınırlarının kesin bir çerçevede çizilememesinin, bazı devletleri eskisinden daha çok müdahaleci duruma getirebileceği öngörülmektedir (Pirker, 2013, s. 2014). Bu durum günümüzde devletlerin siber ordularını güçlendirme girişimlerinden de görülmektedir. Bir diğer yandan da yeni bir uluslararası sözleşmenin söz konusu olması devletlerin anayasal geleneklerine dayanan tutumlarını terk etmeleri anlamına gelecektir (Pirker, 2013, s. 2016). Devletlerin lehlerine olan bir durumu tersine çevirmek istemediği de görülmektedir. Devletler, uluslararası ve bölgesel anlaşmalardaki özel hayatın gizliliği hakkının genel bir tanımı olmaması ve hakkın unsurlarının çok geniş çerçevede yorumlanabilmesi nedeniyle anlaşma maddelerini esneterek kendi lehlerine kullanabilmektedirler. Günümüzde çoğu durumda hükümetler devletin güvenliği tezini öne sürerek bu hakkı ihlal etmekte ve yasal olmayan bir şekilde verileri elde etmektedir. Yapılacak yeni bir uluslararası

anlaşmanın, hükümetlerin siber uzayda hareket alanını kısıtlayacağı öngörülmektedir. Bu ve bunun gibi siber uzayın karmaşık doğası uluslararası hukukun oluşturulamamasının nedenlerinden biri olarak karşımıza çıkmaktadır.

Ancak tüm bu argümanlar siber uzayda özel hayatın gizliliğini hakkının var olan uluslararası ve bölgesel anlaşmalar tarafından tam anlamıyla korunabildiği anlamına gelmemektedir. 1890'lardan 1960'lara kadar kamusal ve yasal tartışmalarda yer aldığı şekliyle özel hayatın gizliliği ile 1970'lerde devletler ve büyük şirketler tarafından artan bilgisayar kullanımı ile yeniden şekillenen özel hayatın gizliliği teknolojik ve sosyal bağlamlar olarak birbirinden farklı kavramlar olarak karşımıza çıkmaktadır (Mulligan, D. K., Koopman, C., & Doty, 2016, s.8). EİHB ile uluslararası hukukta ilk defa tanınan özel hayatın gizliliği hakkı o dönemin uluslararası konjonktürüne, sosyal bağlamlarına uygun olarak hazırlanmıştır. EİHB'nin 1948 yılında nihai sonucuna ulaştığından yola çıkacak olursak henüz bilgi iletişim teknolojilerinin günümüzdeki gibi gelişmediği açıkça karşımıza çıkmaktadır. Öznenin henüz sadece fiziki ortam üzerinden değerlendirildiği bir çağda yapılan uluslararası anlaşmada tanımlanan bu hak doğal olarak bireyin fiziki çevresi dikkate alınarak hazırlanmıştır. İstihbaratın dahi sadece bireyler tarafından yapılan bir eylem olduğu, cep telefonlarının olmadığı, iletişimin yüz yüze olduğu ve bürokrasinin kağıt üzerinden yürütüldüğü bir dönemde temeli atılan bu hak günümüzde bireyi siber uzayda tam anlamıyla koruyamamaktadır. Özellikle 1970li yıllardan sonra yaşanan teknolojik gelişme ve 1990'lı yıllarda bu teknolojilerin devlet ve büyük şirketlerin tekelinden çıkıp topluma yayılması özel hayatın gizliliği hakkının kapsamını da genişletmiştir. Uluslararası hukuk var olan bu hak kavramını terk etmek yerine, üzerinde tartışarak ve bu hakkı dönüştürmeye çalışarak kavramsal olarak açıklama stratejisini benimsemiştir.

Uluslararası hukuk ve bölgesel sözleşmelerle korunan özel hayatın gizliliği hakkı bütüncül bir şekilde ele alınmadığından dolayı ülke ve bölgesel düzeydeki uygulamalarda farklılık göstermektedir. Bu da kavram karmaşıklığına neden olmaktadır. Örneğin Avrupa'da tanınan unutulma hakkının Amerika kıtasında hak olarak ele alınamamasına neden olmaktadır. Ayrıca günümüzde hükümetlerin vatandaşlarına ve ülkede yaşayan yabancılara farklı prosedürler uyguladığı görülmektedir. Bu konu en çok siber gözetim uygulamalarında iç ve dış gözetim olarak

karşımıza çıkmaktadır. Devletlerin ülkede ikamet eden yabancıları daha fazla siber gözetime tabii tuttukları görülmektedir. Oysaki bireyin nerede ikamet ettiğine bakılmaksızın tüm bireylere aynı standartların uygulanması gerekmektedir. Siber uzayda güvenlik teknik gelişmelerle de ilgili olarak görülse de aynı zamanda sosyal normları, küresel iş birliğini ve çok taraflı paydaşları da içeren bütüncül bir yaklaşım ile ele alınmalıdır.

Mevcut uluslararası sistemde özel hayatın gizliliği hakkı genellikle “özel yaşam, aile, konut ve haberleşme” unsurları olarak ele alınmıştır. Geleneksel özel hayatın gizliliği hakkının unsurları, diğer hakların kullanılması için gerekli olan temel bir insan hakkı olarak tanımlanmıştır. Ancak günümüzde bu unsurların bireyi korumada yetersiz kaldığı görülmektedir. Dijital ortam özel hayatın gizliliği hakkının unsurlarının da genişlemesine neden olduğu görülmektedir. Büyük veri, nesnelerin interneti, yapay zeka, otomatik karar verme ve veri profillemeye, bireylerin dijital çağda temel insan haklarına saygı gösterilmesini sağlayan unsurlardan daha fazla korumaya ihtiyacı olduğunu göstermektedir.

Var olan uluslararası ve bölgesel anlaşmalarda özel hayatın gizliliği hakkının tanımı yer almamaktadır. Bu da uygulamalarda birtakım zorlukları beraberinde getirmektedir. Bu konuda da farklı görüşler mevcut olduğu görülmektedir. İlk görüşe göre tanımın açık bir şekilde yapılmaması uygulamada birtakım esneklikleri beraberinde getirmekte, özel hayatın gizliliği hakkı teknolojik gelişmeler karşısında daha kapsamlı ve geniş çerçevede tanımlanabilmektedir. AIHM kararları bu bağlamda içtihat hukukunu kullanmaktadır bir başka deyişle sözleşmelerde ilgili konuyla ilgili açık tanım bulunmadığından dolayı yetkili üst kurullar tarafından kararlar alınmaktadır. İkinci görüşe göre ise, tanımın açık olmaması uygulamanın zorluğunu da beraberinde getirmektedir. Örneğin, ihlal edilen hakkın ne olduğunu açıklamak ve Mahkeme’yi söz konusu hususun özel hayatın gizliliği hakkının kapsamına girdiğine ikna etmek başvuran kişilere düşmektedir (Roagna, 2012, s.10). Bireyin mahkemeyi ikna edemediği durumlarda söz konusu ihlal ortadan kalkmayacak, birey bu hakkından yararlanamayacaktır. Oysa ki bir hakkın kullanılması için karşı tarafın ikna edilme çabası dahi varolan unsurların eksikliğini ortaya koymaktadır.

20. yüzyılın başlarından ortalarına kadar gelişen uluslararası hukuk daha sonra ortaya çıkan bilgi iletişim teknolojilerindeki gelişmeleri kapsamadığından dolayı günümüzde karmaşık sorunları da beraberinde getirmektedir. Teknolojik gelişmelerin bir sonucu olarak meydana gelen özel hayatın gizliliği hakkının ihlaline yönelik endişeler, özel sektörün ve hükümetlerin bu alana yönelik artan tehditleri, mevcut sözleşmelerin yetersiz kalmasına neden olmaktadır. Yukarıda bahsi geçen tüm bu nedenlerden dolayı özel hayatın gizliliği hakkını siber uzay bağlamında, yeni, kapsamlı ve bütüncül bir yaklaşımla ele alacak uluslararası sözleşmeye ihtiyaç duyulmaktadır. Yeni sözleşmede Ziolkowski'nin dile getirdiği üzere, devletlerarası ilişkiler için siber uzay ortak bir alan olarak tanımlanabilir (2013, s. 183). Böylece devletlerin egemenlik ve bütünlük ilkesini sekteye uğratmadan özel hayatın gizliliği hakkı yeni bir uluslararası anlaşma kapsamında ele alınabilecektir. Deibert de Ziolkowski gibi siber uzayın kimseye ait olmayan, ancak herkesin siber uzayın temelini şekillendirmede etkili bir role ve evriminde paya sahip olduğunu kabul eden bir model önermektedir. Bu modelin özünde üç temel ilke bulunmaktadır. Bunlar birleştirme, paylaşırma ve sınırlandırmadır.

Birleştirme, paylaşılan bir alanda yönetim rolleri ve sorumlulukları olan birden fazla aktörün kasıtlı olarak bir araya getirilmesini; paylaşırma ise tek bir aktörün diğerlerinin iş birliği ve rızası olmadan söz konusu alanı kontrol edemediği bir tasarım ilkesini ifade eder...sınırlandırma ilkesi belki de en önemlisidir ve muhtemelen aşırı tepki nedeniyle en fazla tehdit altında olanıdır. Siber uzayın güvenliğinin sağlanması, hükümetler, kolluk kuvvetleri ve istihbarat üzerindeki kontrol ve dengeler de dahil olmak üzere, güç üzerindeki kısıtlamaların gevşetilmesinden ziyade, kurumlar ve özel sektör üzerinde güçlendirilmesini gerektirmektedir (Deibert, 2013, s. 400-403).

Farklı yetki alanlarına dağıtılmış ve teknolojik gelişmelerdeki hızlı büyümenin olduğu bir zeminin tam ortasında yer alan özel hayatın gizliliği hakkının uluslararası toplumda yeni bir sözleşme ile daha kapsamlı bir şekilde tanınması bu hakkın korunması açısından elzem olarak görünmektedir. Deibert ve Ziolkowski'nin önerdiği gibi siber uzayın ortak bir alan olarak belirlenip, özel hayatının gizliliği hakkının siber uzayı da içerecek şekilde yeniden tanımlanması, tüm paydaşların aktif olarak siber

uzayın yönetiminde yer alacağı, etkili denetim mekanizmalarını da içeren yeni bir sözleşme hazırlanmalıdır.

Yeni sözleşme hazırlanırken birtakım hususlar göz önüne alınmalıdır; bunlardan ilki, özel hayatın gizliliği hakkının tanımının açık bir şekilde yapılması gerekliliğidir. Böylece siber uzayın tüm paydaşları kavram kargaşasından kurtularak, hem bireylerin haklarının kapsamını bilmesine olanak sağlayacak hem de özel hayatın gizliliği hakkının korunmasına yönelik yükümlülükler net bir şekilde ele alınmış olacaktır. İkincisi, özel hayatın gizliliği hakkının unsurları teknolojideki gelişmeleri de içerecek şekilde tekrar tanımlanmalıdır. Siber gözetim, büyük veri, nesnelerin interneti, yapay zeka, algoritmalar siber istihbarat ve kişisel verilerin korunması çerçevesinde bu hakkın unsurlarının genişletilmesi gerekmektedir. Üçüncü olarak sözleşmenin tüm paydaşları içermesi gerekir. Siber uzayın paydaşları özel şirketler, devletler ve bireylerden oluşmaktadır. Günümüzde siber uzaya yön veren devletlerden ziyade özel şirketlerdir. Dolayısıyla özel şirketlerin olası bir sözleşme hazırlanması aşamasında yer alması büyük önem arz etmektedir. Özel şirketlerin yanı sıra yararlanıcı olarak birey haklarını da koruyan sivil toplum örgütlerinin de bu süreç içerisinde yer alması gerekir. Paydaşlardan birinin sözleşme hazırlanırken dahil olmaması sözleşmenin kapsayıcılığı bakımından engel teşkil edecektir. Dördüncü ve son olarak ise olası sözleşmenin etkin bir yaptırım mekanizmasının olması gereklidir. Etkin bir yaptırım mekanizması olarak belirtilmesinin nedeni, sözleşmenin kağıt üzerinde yaptırım mekanizması olsa dahi hükümetlerin fiili olarak zayıf görecekları bir yaptırım mekanizmasının sözleşme hükümlerine uymaması sonucunu doğurabilmektedir. Dolayısıyla etkin bir yaptırım mekanizmasının olması ve hükümetlerin bunu tehdit olarak görmeleri sözleşme hükümlerinin uygulanması ve korunması konusunda daha etkili olacaktır.

Günümüzde bu şekilde bir uluslararası sözleşmenin ortak bir platformda hazırlanması zor görünmektedir. Özellikle siber uzayın anarşik doğası ve devletlerin bu alanda üstün olmak adına verdikleri savaş ve yatırımlar da göz önüne alındığında yakın gelecekte böyle bir sözleşmenin yapılabilmesi ihtimalini azaltmaktadır. Ancak yeni bir sözleşmenin zorluğu, gereklilik olmadığı anlamına da gelmemektedir. Teknolojik gelişmelerin hızla devam edeceği öngörülmektedir. Önemli olan teknolojik

gelişmeler ile birlikte genelde insan haklarının özel de ise özel hayatın gizliliği hakkının siber uzayda korunabilmesidir. Bu bağlamda öncelikle teknolojinin hesap verilebilir, şeffaf ve hakları koruyacak biçimde ne şekilde kurgulanabileceği daha sonraki araştırmalara konu olabilir. Böylece teknolojik gelişmeler devam ederken diğer yandan da insan haklarına zarar vermeden ne şekilde geliştirilebileceği olası yeni bir sözleşmenin oluşturulmasına da yardımcı olacaktır.

Kısaca özetlenecek olursa bazı somut sonuçlar ve çözümleri aşağıdaki gibi olabilir.

- Özel hayatın gizliliği hakkı geleneksel unsurlarını korumuş ancak siber uzay bağlamında kapsamı genişlemiş ve çeşitlenmiştir. Siber uzayda, internet, sosyal medya, akıllı cihazlar gibi teknolojiler aracılığıyla kişiler, gerçek hayatta olduğu gibi özel ve mahrem bilgilerini paylaşabilmektedir. Bu nedenle, siber uzayda da kişilerin özel hayatına saygı gösterilmesi ve mahremiyetlerinin korunması gerekmektedir.

- Siber uzayda özel hayatın gizliliği hakkı, geleneksel anlamdaki özel hayatın gizliliği hakkı ile karşılaştırıldığında bazı farklılıklar göstermektedir. Siber uzayda, kişilerin özel hayatına ilişkin bilgiler çok daha kolay ve hızlı bir şekilde toplanabilir ve yayılabilir. Bu nedenle, siber uzayda özel hayatın gizliliği hakkının korunması daha zordur.

- Siber uzayda özel hayatın gizliliği hakkının korunması için bazı önlemler alınması gerekmektedir. Bu önlemler arasında, siber güvenlik önlemleri, hukuki önlemler, idari önlemler, kişisel verilerin korunması düzenlemeleri ve eğitim faaliyetleri yer almaktadır.

- Siber uzayda özel hayatın gizliliği hakkının kapsamı, geleneksel anlamdaki özel hayatın gizliliği hakkının kapsamından daha geniştir. Siber uzayda, kişilerin özel hayatına ilişkin bilgiler, sadece gerçek hayatta paylaştıkları bilgilerle sınırlı değildir. Kişilerin, internette yaptıkları paylaşımlar, sosyal medya hesaplarında paylaştıkları bilgiler, akıllı cihazları aracılığıyla toplanan veriler gibi bilgiler de özel hayatın gizliliği hakkı kapsamındadır.

- Siber uzayda özel hayatın gizliliği hakkının ihlali, geleneksel anlamdaki özel hayatın gizliliği hakkının ihlalinden daha ciddi sonuçlar doğurabilir. Siber uzayda,

özel hayatın gizliliği hakkının ihlali, kişilerin kişilik haklarına, itibarına ve hatta güvenliğine zarar verebilir.

- Siber uzayda özel hayatın gizliliği hakkının korunması, uluslararası işbirliğini gerektirmektedir. Siber uzayda özel hayatın gizliliği hakkının korunması için, uluslararası hukuk normlarının geliştirilmesi ve uygulanması gerekmektedir.

Bu sonuçların ışığında, siber uzayda özel hayatın gizliliği hakkının korunması için aşağıdaki önlemlerin alınması önerilmektedir:

- Siber güvenlik önlemleri güçlendirilmelidir. Bu önlemler, kişilerin özel verilerinin kötü amaçlı kişiler tarafından ele geçirilmesini ve kullanılmasını engellemeye yöneliktir.

- Kişisel verilerin korunması düzenlemeleri geliştirilmelidir. Bu düzenlemeler, kişilerin özel verilerinin toplanması, işlenmesi ve paylaşılması konusundaki kuralları belirlemektedir.

- Eğitim faaliyetleri artırılmalıdır. Bu faaliyetler, kişilerin siber uzayda özel hayatın gizliliği hakkının önemi konusunda bilinçlendirilmesini amaçlamaktadır.

- Hukuki ve idari önlemlerin ve düzenlemelerin yapılması gerekmektedir.

- Paydaşlar arası işbirliğinin artırılması bu hakkın korunmasına çok katkı sağlayacaktır.

- Siber uzayda özel hayatın gizliliği hakkı, kişilerin temel hak ve özgürlükleri arasında yer almaktadır. Bu hakkın korunması, kişilerin siber uzayda özgürce ve güvende yaşamasını sağlayacaktır.

Yeni Araştırmalar için öneriler;

Siber uzayda özel hayatın gizliliği hakkı, geleneksel hukuk anlayışından farklı bir şekilde ele alınması gereken karmaşık bir konudur. Siber uzayda, gerçek dünyadaki gibi fiziksel bir sınırlama yoktur ve bu durum özel hayatın gizliliğini ihlal etme riskini artırmaktadır.

Siber uzayda özel hayatın gizliliği hakkı ile ilgili yeni çalışma alanları şunlardır:

- Uluslararası hukukta siber uzayda özel hayatın gizliliği hakkının düzenlenmesi: Siber uzayda özel hayatın gizliliği hakkı, henüz uluslararası hukukta tam olarak düzenlenmiş değildir. Bu alanda yapılacak çalışmalar, uluslararası hukukta bu hakkın daha etkin bir şekilde korunmasını sağlayacaktır.

- Siber uzayda özel hayatın gizliliğini ihlal eden yeni teknolojiler: Siber uzayda özel hayatın gizliliğini ihlal eden yeni teknolojilerin ortaya çıkması, bu alandaki çalışma ihtiyacını artırmaktadır. Bu teknolojilerin tespiti ve önlenmesi için yeni çözümler geliştirilmelidir.

- Siber uzayda özel hayatın gizliliğini korumak için bireysel önlemler: Siber uzayda özel hayatın gizliliğini korumak için bireyler de bazı önlemler alabilir. Bu önlemlerin farkındalığı artırılmalıdır.

Bu konular üzerinde yapılacak çalışmalar, siber uzayda özel hayatın gizliliği hakkının daha iyi anlaşılmasına ve korunmasına yardımcı olacaktır.



KAYNAKÇA

- Arab Convention on Combating Information Technology Offences. (2010). Arab Convention on Combating Information Technology Offences. League of Arab States General Secretariat. <https://www.asianlaws.org/gclid/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf>, [Eriřim:14 Mayıs 2022]
- African Union Convention on Cyber Security and Personal Data Protection. (2014). African Union Convention on Cyber Security and Personal Data Protection. African Union. https://www.opennetafrica.org/?wpfb_dl=4, [Eriřim:22 Temmuz 2022]
- Aka, B. (2017). Sosyal Medyada Kiřilik Hakkı İhlalleri Ve Hukukî Korunma Yollari. *İzmir Barosu Dergisi*, 82(2), 231-287.
- Akyeřilmen, N. (2016). Cybersecurity and Human Rights: Need for a Paradigm Shift?, “. Cyberpolitik Journal, 1(1), 32-55. https://d1wqtxts1xzle7.cloudfront.net/52001985/cyber_security_and_human_rights-libre.pdf, [Eriřim:1 Ekim 2020]
- Akyeřilmen, N. (2018). *Disiplinlerarası Bir Yaklařımla: Siber Politika & Siber Güvenlik*. Orion Kitabevi
- Akyeřilmen, N. (2021). *İnsan Hakları Hukuku, Siyaseti ve Felsefesi*. Orion Kitabevi
- Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.
- American Convention on Human Rights. (1969). American Convention on Human Rights. Inter-American Commison on Human Rights. <http://www.cidh.org/Basicos/English/Basic3.American%20Convention.htm>, [Eriřim:22 Temmuz 2022]
- Anderson, David. 2015. A Question of Trust: Report of the Investigatory Powers Review Presented to the Prime Minister Pursuant to Section 7 of the Data Retention and Investigatory Powers Act 2014. <https://terrorismlegislationreviewer.independent>.

- gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf., [Eriřim:22 Temmuz 2022]
- Andorno, R. (2005). The Oviedo Convention: A European Legal Framework at the Intersection of Human Rights and Health Law. *Bioethics*, (1), 133-143.
- Annual Data Breach Report. (2022). Annual Data Breach Report. Identity Theft Resource Center. <https://www.idtheftcenter.org/publication/2022-data-breach-report/>, [Eriřim:15 Eylöl 2023].
- Antović and Mirković v. Montenegro Davası (Bařvuru No: 70838/13). (2018). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-178904%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-178904%22]}), [Eriřim:20 Ağustos 2022].
- Asquith, P. M., & Morgan, P. L. (2020, July). Representing a human-centric cyberspace. In *International Conference on Applied Human Factors and Ergonomics* (pp. 122-128). Springer, Cham.
- Avrupa İnsan Hakları Sözleşmesi (1950). Avrupa İnsan Hakları Sözleşmesi. Council of Europe. https://www.echr.coe.int/documents/d/echr/convention_tur, [Eriřim:15 Ağustos 2022].
- Aycaguer v. France Davası (Bařvuru No: 8806/12). (2017). Avrupa İnsan Hakları Mahkemesi Raporları. <https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001175007&filename=CASE%20OF%20AYCAGUER%20v.%20FRANCE.pdf&logEvent=False>, [Eriřim:10 Nisan 2022].
- Badenhoop, E. (2021). The Fallacy of Perfect Regulatory Controls: Lessons from Database Surveillance of Migration in West Germany from the 1950s to the 1970s. *Regulation & Governance*, 15(3), 952-968.
- Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *The John Marshall journal of computer & information law*, 18(1), 1-111. https://www.researchgate.net/publication/242448871_Privacy_human_rights-an_international_survey_of_privacy_laws_and_developments/link/5a58d99e45851545026fc712/download, [Eriřim:5 Mart 2021].

- Barbaro, M. (2017). Government interference with the right to privacy: is the right to privacy an endangered animal. *Can. J. Hum. Rts.*, 6, 127.
- Bărbulescu v. Romania (Başvuru No: 61496/08). (2017). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-177082%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-177082%22]}), [Erişim:10 Nisan 2022].
- Barrett-Maitland, N., & Lynch, J. (2020). *Social Media, Ethics and the Privacy Paradox*. In *Ethics, Laws, and Policies for Privacy, Security, and Liability*. IntechOpen: Intech Open: London, UK.
- Bates, E. (2010). *The evolution of the European Convention on Human Rights: from its inception to the creation of a permanent Court of Human Rights*. Oxford University Press.
- Bauman, Z., & Lyon, D. (2016). Akışkan Gözetim. Çev. Elçin Yılmaz), (2. Basım), İstanbul: Ayrıntı Yayınları.
- Baybutt, P. (2004).Cyber Security Risk Analysis for Process Control Systems Using Ringsof Protection Analysis (ROPA).*Process Safety Progress*, 23(4): 284-291.
- Bellaby, R. W. (2016) Justifying Cyber-Intelligence?, *Journal of Military Ethics*, 15:4, 299-319.
- Ben Faiza v. France Davası (Başvuru No: 31446/12). (2018). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-180657%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-180657%22]}), [Erişim:20 Ağustos 2022].
- Benkler, Y. (2006). *The Wealth of Networks*. New Heaven, CT: Yale University Press.
- Bennett, C. J., & Raab, C. D. (2017). *The Governance of Privacy: Policy Instruments in Global Perspective*. Routledge.
- Bernal, P. (2014), *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge (UK): Cambridge University Press: 82-117.
- Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 1(2), 243-264. <https://www.tandfonline.com/doi/epdf/10.1080/23738871.2016.1228990?needAccess=true&role=button>, [Erişim:12 Şubat 2022].

- Big Brother Watch And Others v. The United Kingdom Davası (Başvuru No: 58170/13, 62322/14 and 24960/15). (2021). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/#{%22fulltext%22:...}](https://hudoc.echr.coe.int/#{%22fulltext%22:...) , [Erişim:20 Ağustos 2022].
- Boyd, D. (Nisan 2010). Privacy and publicity in the context of big data.<http://www.danah.org/papers/talks/2010/WWW2010.html>, [Erişim:4 Şubat 2021].
- Boyd, D. (2012.) Networked Privacy. *Surveillance & Society* 10(3/4): 348-350.
- Bozlak, A. (2013). *Avrupa İnsan Hakları Mahkemesi Kararları Çerçevesinde, Türk Ceza Hukukunda Özel Hayatın Korunması*. Adalet Yayınevi.
- Brown, E. L. (2003). Echelon: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security. *CommLaw Conspectus*, <https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1260&context=commlaw> , [Erişim:22 Ocak 2021].
- Buckley Davası (Başvuru No: 20348/92). (1996). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%2200158076%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%2200158076%22]}) , [Erişim:9 Eylül 2022].
- Buturugă v. Romania Davası (Başvuru No: 56867/15). (2020). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22languageisocode%22:...}](https://hudoc.echr.coe.int/eng#{%22languageisocode%22:...) , [Erişim:10 Nisan 2022].
- Cabra, M. (1980). Rights and Duties Established by The American Convention on Human Rights. *American University Law Review*, 30(1), 21-64.
- Callard, F. (2010). Between Legislation and Bioethics: The European Convention on Human Rights and Biomedicine. In *Ethics in Psychiatry* (pp. 73-96). Springer, Dordrecht.
- Campbell Christie Davası (Başvuru No: 21482/93). (1994). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-1870"\]}](https://hudoc.echr.coe.int/eng#{) , [Erişim:9 Eylül 2022].
- Campbell, D. (2000). Global surveillance: the evidence for Echelon. In *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the*

- assumptions,149-154. <https://dl.acm.org/doi/pdf/10.1145/332186.332274>, [Eriřim:3 Ekim 2022].
- Cannataci, J. (2016). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. A/HRC/31/64. <https://dig.watch/wp-content/uploads/2021/12/A-HRC-31-64.pdf>, [Eriřim:1 Aęustos 2022].
- Carter, E. L. (2016). The right to be forgotten. In Oxford Research Encyclopedia of Communication. <https://doi.org/10.1093/acrefore/9780190228613.013.189>, [Eriřim:1 Aęustos 2022].
- Castagna, M. J. (1997). Virtual intelligence: Reengineering doctrine for the information age. *International Journal of Intelligence and Counter Intelligence*, 10(2), 180-195.
- Cavelty, M. D. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and engineering ethics*, 20(3), 701-715.
- Centrum för Rättvisa v. Sweden Davası (Bařvuru No: 35252/08). (2021). Avrupa İnsan Hakları Mahkemesi Raporları.<https://hudoc.echr.coe.int/fre#{%22documentcollectionid%22>, [Eriřim:20 Aęustos 2022].
- Cerf, V. G. (2012, 4 Ocak). Internet access is not a human right. New York Times. Eriřim adresi:<https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html>, [Eriřim:8 Mart 2022].
- Chapman Davası (Bařvuru No:27238/95). (2001). Avrupa İnsan Hakları Mahkemesi Raporları.[https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22059154%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22059154%22]}), [Eriřim: 9 Eylöl 2022].
- Charter of Fundamental Rights of the European Union (2000). Charter of Fundamental Rights of the European Union. Official Journal of the European Communities. https://www.europarl.europa.eu/charter/pdf/text_en.pdf. [Eriřim: 22 Eylöl 2022].
- Choucri, N. (2012). *Cyberpolitics in International Relations*. MIT Press.
- Clark, R. M. (2020). *Geospatial Intelligence: Origins and Evolution*. Georgetown University Press.

- Commission on Human Rights. (t.y.). Brief historic overview of the Commission on Human Rights. <https://view.officeapps.live.com/op/view.aspx?src>, [Eriřim:1 Ağustos 2022].
- Commission on Human Rights Drafting Committee on an International Bill of Human Rights First Session. (1947a). Report of the Drafting Committee to the Commission On Human Rights E/CN.4/21.<https://documents-dds-ny.un.org/doc/UNDOC/GEN/GL9/000/26/PDF/GL900026.pdf?OpenElement>, [Eriřim:1 Ağustos 2022].
- Commission on Human Rights Drafting Committee (1947b). Draft Outline of International Bill of Rights (prepared by the Division of Human Rights) E/CN.4/AC.1/3. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/NG9/000/25/PDF/NG900025.pdf?OpenElement>, [Eriřim:1 Ağustos 2022].
- Convention on Cybercrime. (2001). Convention on Cybercrime.Council of Europe. <https://rm.coe.int/1680081561>., [Eriřim:8 Ekim 2022].
- Copland v. The United Kingdom Davası (Bařvuru No: 62617/00). (2007). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-79996"\]}](https://hudoc.echr.coe.int/eng#{), [Eriřim:9 Eylül 2022].
- Cornescu, A. V. (2009). The generations of human's rights. In *Days of Law: The Conference Proceedings* (Vol. 1).
- Council of Europe (1996). Convention for the Protection of Human Rights and Dignity of Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine. Directory of Legal Affairs, Strasbourg.
- Council of Europe (2018). Convention 108 + Convention for the protection of individuals with regard to the processing of personal data. <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>, [Eriřim:15 Kasım 2022].
- Council of Europe. Committee of Ministers. (2001). Explanatory Report for the Convention on CyberCrime. <https://rm.coe.int/16800cce5b>., [Eriřim:9 Eylül 2022].

- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS quarterly*, 673-687.
- Dahlberg, L. (2001). Extending the public sphere through cyberspace: The case of Minnesota E-Democracy. *First Monday*, 6(3).
- Damen, J., Köhler, L., & Woodard, S. (2017). The Human Right of Privacy in the Digital Age. <https://publishup.uni-potsdam.de/frontdoor/index/index/docId/39926>, [Eriřim:9 Eylül 2022].
- Daniels, N. (22 Mart 2023). Big Data and Privacy: What is It and What are the Risks? <https://vpnoverview.com/privacy/anonymous-browsing/big-data-and-privacy/>, [Eriřim:12 Nisan 2022]
- Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In *Privacy online* (pp. 47-60). https://link.springer.com/chapter/10.1007/978-3-642-21521-6_5, [Eriřim:1 Ekim 2020]
- Declaration on Freedom of Communication on the Internet, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805dfbd5, [Eriřim:9 Eylül 2022].
- De Hert, P., ve Kloza, D. (2012). Internet (access) as a new fundamental right. Inflating the current rights framework?. *European Journal of Law and Technology*, 3(3), 1-23.
- Deleuze, G. (1992). *Postscript on the Societies of Control*. The MIT Press.
- Deleuze, G. (2013). *Foucault*, çev. Burcu Yalım ve Emre Koyuncu, İstanbul: Norgunk.
- Demades Davası (Bařvuru No: 16219/90). (2003). Avrupa İnsan Hakları Mahkemesi Raporları, <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-61272%22%5D%7D>, [Eriřim:22 Eylül 2022].
- Demir, A. (2017). Panopticon ve synopticon geriliminde özgürlük paradoksu. Kaygı. *Bursa Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi*, (28), 55-65. <https://dergipark.org.tr/tr/download/article-file/307183>, [Eriřim:9 Eylül 2022].
- Denning, D. E., & Lin, H. S. (1994). *Rights and Responsibilities of Participants in Networked Communities*. National Academy Press, 2101 Constitution Avenue, NW, Washington, DC 20418.

- Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, 32(4), 411-424.
- Doneda, D., & Almeida, V. A. (2015). Privacy governance in cyberspace. *IEEE Internet Computing*, 19(3), 50-53.
- Doyle, A. (2011). Revisiting the synopticon: Reconsidering Mathiesen's 'The Viewer Society' in the age of Web 2.0. *Theoretical criminology*, 15(3), 283-299.
- Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review*, 14(3), 441-458. <https://academic.oup.com/hrlr/article/14/3/441/644279>, [Erişim:9 Eylül 2022].
- Du Pont, G. F. (2000-2001). The Criminalization of True Anonymity in Cyberspace. *Michigan Telecommunications and Technology Law Review*, 7, 191-216.
- ECtHR (European Court of Human Rights). (September 2022). New Technologies. https://www.echr.coe.int/documents/d/echr/fs_new_technologies_eng, [Erişim: 9 Eylül 2022].
- Edwards, J. (21 Kasım 2013). Google's Top Futurist Says Your 'Privacy May Be An Anomaly'. <https://www.businessinsider.com/google-vinton-cerf-declares-an-end-to-privacy-2013-11>. , [Erişim:20 Ocak 2020].
- Eijkman, Q., & Weggemans, D. (2012). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Security and Human Rights*, 23(4), 285-296.
- Ettinger, J. (2019). *Cyber Intelligence Tradecraft Report the State of Cyber Intelligence Practices in the United States*.
- Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2021). Systematic Literature Review to Investigate the Application of Open Source Intelligence (Osint) with Artificial Intelligence. *Journal of Applied Security Research*, 16(3), 345-369.
- European Commission. (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace. Brussels. https://edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf, [Erişim:9 Eylül 2022].
- European Court of Human Rights. (2022). Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home

- and correspondence. https://www.echr.coe.int/documents/guide_art_8_eng.pdf, [Eriřim:9 Eylül 2023].
- European Data Protection Supervisor. (t.y). Data Protection. https://edps.europa.eu/data-protection/data-protection_en, [Eriřim:22 Mayıs 2023].
- European Union Agency for Law Enforcement Cooperation. (t.y.). Cyber Intelligence. <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/intelligence-analysis/cyber-intelligence>, [Eriřim:9 Ağustos 2023].
- Federal Bureau of Investigation. (t.y). About, Leadership & Structure. <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch>, [Eriřim:18 Ağustos 2022].
- Fırat, M. S. (2015). Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu. *Hacettepe Hukuk Fakültesi Dergisi*, 5(2), 101-116.
- Fried, C. (1968). Privacy. *The Yale Law Journal* Vol. 77, No. 3. s. 475-493.
- Fischer-Hübner, S. (1997). Privacy at Risk in the Global Information Society. In *An Ethical Global Information Society* (pp. 261-274). Springer, Boston, MA.
- Foucault, M. (1992). *Hapishanenin Doğuşu* (Çev. Mehmet Ali Kılıçbay). Ankara: İmge Kitabevi.
- Foucault, M. (2019). *Ethics: Subjectivity and Truth: Essential Works of Michel Foucault 1954-1984*. Penguin UK.
- Fourkas, V. (2004). What is cyberspace. <http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace>, [Eriřim:8 Ekim 2021].
- Fuchs, C. (2021). Social media: A critical introduction. *Social Media*, 1-440.
- Gandía, J. L., Marrahí, L., & Huguet, D. (2016). Digital transparency and Web 2.0 in Spanish city councils. *Government Information Quarterly*, 33(1), 28-39.
- Garnaga Davası (Bařvuru No: 20390/07). (2013). Avrupa İnsan Hakları Mahkemesi Raporları. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-119681%22%5D%7D>, [Eriřim:9 Eylül 2022].
- Gaughran v. The United Kingdom Davası (Bařvuru No: 45245/15). (2020). Avrupa İnsan Hakları Mahkemesi Raporları.

- [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-200817%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-200817%22]}),
[Eriřim:10 Nisan 2022].
- Gavison, R. E. (1980). Privacy and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471.
- Galič, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30, 9-37.
- Gemalmaz, S.M. (2012). *Ulusalüstü İnsan Hakları Hukukunun Genel Teorisine Giriř*, Cilt 2, 8. Bası, Legal Yayınevi, Aralık.
- Gibson, W. (1984). *Neuromancer*. New York: ACE.
- Giddens, A. (1984). *The constitution of society. Outline of the theory of structuration*. Cambridge: Polity Press.
- Giddens, A. (1987). *Social theory and modern sociology*. Cambridge: Polity Press.
- Goldman, R. K. (2009). History and Action: The Inter-American Human Rights System and the Role of the Inter-American Commission on Human Rights. *Human Rights Quarterly*, 31, 856-887.
- Gorlov and Others v. Russia Davası (Bařvuru No: 27057/06). (2019). Avrupa İnsan Hakları Mahkemesi Raporları. <https://shorturl.at/txANR>, [Eriřim:20 Ağustos 2022].
- Greenwald, G. (31 Temmuz 2013). XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. <https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>, [Eriřim:9 Ocak 2022].
- Gözübüyük, ř., & Gölcüklü, F. (2011). *Avrupa İnsan Hakları Sözleşmesi ve Uygulaması*. Turhan Kitabevi, Ankara.
- Greathouse, C. B. (2014). Cyber war and strategic thought: Do the classic theorists still matter?. In *Cyberspace and International Relations* (pp. 21-40). Springer, Berlin, Heidelberg.
- Goldsmith, D. (2021). Security Concepts: The Three Pillar. https://github.coventry.ac.uk/pages/CUEH/245CT/1_Introduction/SecurityConcepts_Pillars/, [Eriřim: 8 Mart 2022].

- Goldstein, K., & Tov, O. S, ve Prazeres, D. (2018). Report Privacy in Digital Age, <https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf>, [Eriřim:9 Mayıs 2022].
- Guillot Davası (Bařvuru No: 22500/93). (1993). Avrupa İnsan Hakları Mahkemesi Raporları. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58069%22%5D%7D>, [Eriřim:9 Eylül 2022].
- Gür, B. A. (2018). Uluslararası Hukuk ve AB Hukuku Boyutuyla Kiřisel Verilerin Yurt Dıřına Aktarılması. *Marmara Üniversitesi Hukuk Fakóltesi Hukuk Arařtırmaları Dergisi*, 25(2), 850-872
- Hadas, E. (22 Mayıs 2019). Breakingviews - Hadas: “Zero privacy” is both blessing and curse. <https://www.reuters.com/article/us-technology-privacy-breackingviews-idUSKCN1SS1OS>, [Eriřim:22 Ocak 2020].
- Haggerty, K. D., and Ericson, R. V. (2000). The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622
- Hassib, B., & Shires, J. (2022). Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy*, 29(1), 90-103. <https://onlinelibrary.wiley.com/doi/full/10.1111/mepo.12616>. [Eriřim:22 Nisan 2023].
- Hekimođlu, M. M. (2003). İnsan Haklarının Tarihsel Perspektif İerisindeki Geliřimi. *Yönetim ve Ekonomi Arařtırmaları Dergisi*, 1(1), 73-92.
- Henschke, A., Reed, A., Robbins, S., & Miller, S. (2021). *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Springer Nature.
- Hijmans, H. (2014). Right to Have Links Removed: Evidence of Effective Data Protection: Case C-131/12 Google v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja Gonzalez, Judgment of 13 May 2014. *Maastricht Journal of European and Comparative Law*, 21(3), 555-563.
- Hildebrandt, M. (2014). Location Data, Purpose Binding and Contextual Integrity: What’s the Message?. *Protection of Information and the Right to Privacy-A New Equilibrium?*, 31-62.

- Hiranandani, V. (2011). Privacy and security in the digital age: contemporary challenges and future directions. *The International Journal of Human Rights*, 15(7), 1091-1106.
- Hollis, D., & Ohlin, J. (2018). What if Cyberspace Were for Fighting? *Ethics & International Affairs*, 32(4), 441-456.
- HU, C., Kumar, S., Huang, J., & Ratnavelu, K. (2017). Disinhibition of negative true self for identity reconstructions in cyberspace: Advancing self-discrepancy theory for virtual setting. *PloSOne*, <https://doi.org/10.1371/journal.pone.0175623>, [Eriřim:9 Eylül 2022].
- Iliya Stefanov Davası (Bařvuru No: 65755/01). (2008). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-86449"\]}](https://hudoc.echr.coe.int/eng#{), [Eriřim:9 Eylül 2022].
- Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, 3, 1-25.
- Johnson, B. (11 Ocak 2010). Privacy no longer a social norm. <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>, [Eriřim:22 Ocak 2020].
- Jones, S. G. (1997). The Internet and its social landscape. *Virtual culture: Identity and communication in cybersociety*, 1, 7-36.
- Jørgensen , R. F. (2020). The right to privacy under pressure . *Nordicom review*, 37(s1), 165-170.
- Joyce, D. (2015). Internet Freedom and Human Rights. *European Journal of International Law*, 26(2), 493-514.
- Kafka, F. (2017). *Dava*. Ebrar Karadeniz (Çev.), Timař Yayınları.
- Karppinen, K., & Puukko, O. (2020). Four discourses of digital rights: Promises and problems of rights-based politics. *Journal of Information Policy*, 10(1), 304-328
- Kahn, J. D. (2003). Privacy as a Legal Principle of Identity Maintenance. *Seton Hall Law Review*, 33(2), 371-410. https://heinonline.org/HOL/Page?handle=hein.journals/shlr33&div=18&g_sent=1&casa_token=&collection=journals, [Eriřim:4 Mayıs 2021].

- Kaya, E.N.(2022). *Dijitalleşme ve Mahremiyet: Özel Hayatın Değişen Dinamikleri*. Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Kazi, N. (2011). Public sphere and dynamics of the Internet. *Bodhi: An Interdisciplinary Journal*, 5(1), 173-180.
- Khan, M. Z., Gilani, I. S., & Nawaz, A. (2012). From Habermas Model to New Public Sphere: A Paradigm Shift. *Global Journal of Human Social Science*, 12(5), 42-52.
- Kişisel Verileri Koruma Kurumu, (2021). “Unutulma Hakkı (Unutulma Hakkının Arama Motorları Özelinde Değerlendirilmesi)”, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/11b6fd99-d42a-45b1-a009-21f2d36ded21.pdf> , [Erişim:9 Eylül 2022].
- Kleinman, Z. (10 Haziran 2013). What does Prism tell us about privacy protection?. <https://www.bbc.com/news/technology-22839609>, [Erişim:12 Mart 2022].
- Kloppenburger, S., & Van der Ploeg, I. (2020). Securing identities: Biometric technologies and the enactment of human bodily differences. *Science as Culture*, 29(1), 57-76.
- Koops, B. J., Hoepman, J. H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, 29(6), 676-688.
- Kovacs, A., & Hawtin, D. (2013). Cyber security, cyber surveillance and online human rights. GlobalPartnersDigital, <https://www.gp-digital.org/wpcontent/uploads/2013/05/Cyber-SecurityCyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf>, [Erişim:12 Kasım 2020].
- Klass and Others v. Germany Davası (Başvuru No: 5029/71). (1978). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57510%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}), [Erişim:4 Mayıs 2020].
- Kling, R., Lee, Y. C., Teich, A., & Frankel, M. S. (1999). Assessing anonymous communication on the internet: Policy deliberations. *The Information Society*, 15(2), 79-90.
- Kuçuradi, İ. (2011). *İnsan hakları: kavramları ve sorunları:-insan hakları ve hukuk-devlet-siyaset felsefesi yazıları*. Türkiye Felsefe Kurumu.

- La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement>, [Eriřim:11 Kasım 2022].
- Leslie, D., Burr, C., Aitken, M., Cows, J., Katell, M., & Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. https://www.turing.ac.uk/sites/default/files/202103/cahai_feasibility_study_primer_final.pdf, [Eriřim:9 Eylül 2022].
- Leto, C., & Dean, S. (2011). The Right to Reputation under the European Convention on Human Rights/ResearchGate. https://www.researchgate.net/publication/311310149_The_Right_to_Reputation_under_the_European_Convention_on_Human_Rights, [Eriřim:9 Eylül 2022].
- Levine, N. (1996). Establishing Legal Accountability for Anonymous Communication in Cyberspace. *Columbia Law Review*, 96(6), 1526-1572.
- Liaropoulos, A. N. (2016). Reconceptualising cyber security: Safeguarding human rights in the era of cyber surveillance. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 6(2), 32-40.
- Lichinitzer, A., & Snir, I. (2022). Self-Surveillance in a Settler-Colonial Context: CCTV and Tribal Authority in the Bedouin Town of Hura. <https://onlinelibrary.wiley.com/doi/epdf/10.1111/anti.12834>, [Eriřim:20 Ocak 2023].
- Lin, H. (2013). *Cyber Conflict and National Security*, in *International Politics: Enduring Concepts and Contemporary Issues*, Robert Art and Robert Jervis (eds.) Pearson.
- Løkke, E. (2018). *Mahremiyet: Dijital Toplumda Özel Hayat*, İstanbul: Koç Üniversitesi Yayınları.
- Ludi Davası (Bařvuru No: 12433/86). (1992). Avrupa İnsan Hakları Mahkemesi Raporları. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-57784%22%5D%7D>, [Eriřim:9 Eylül 2022].

- Lyon, D. (1997). The world wide web of surveillance: The internet and off-world power-flows. <https://journals.library.ualberta.ca/ojs.cais-acsi.ca/index.php/cais-asci/article/view/40/36>, [Eriřim:4 Nisan 2021].
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education (UK).
- Lyon, D. (2010). Liquid surveillance: The contribution of Zygmunt Bauman to surveillance studies. *International political sociology*, 4(4), 325-338.
- Lyon, D. (2013). *Gözetim Çalışmaları* (Çev. Ali Toprak). İstanbul: Kalkedon Yayınları.
- Mahlouly, D. (2013). Rethinking the public sphere in a digital environment: similarities between the eighteenth and the twenty-first centuries. *ESharp*, 20(6).
- Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance and Society*, 16(2).
- Margareta ve Roger Andersson Davası (Bařvuru No: 12963/87). (1992). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["00157748"\]}](https://hudoc.echr.coe.int/eng#{), [Eriřim:9 Eylül 2022].
- Mario Costeja González Davası (Dava C-131/12). (2014). Mahkeme Kararı. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>, [Eriřim:10 Eylül 2022].
- Mangır, D. ř., & Küçükırlı, S. N. (2019). Gelenekselden Dijitale Siber İstihbarat ve Rus Dıř Politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (42.1), 296-308.
- Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues*, 59(2), 411-429.
- Mathiesen, K. (2012). The human right to Internet access: A philosophical defense. *The International Review of Information Ethics*, 18, 9-22.
- Matney, L. (4 Ağustos 2015). Uncovering ECHELON: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life. <https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/?guccounter=1>, [Eriřim:2 řubat 2021].

- Mbanaso, U. M. (2018). Personal Data Privacy and Security-Who, What, When, Why, Where and How? Theme/Focus Area: Data Privacy and Security, <https://www.researchgate.net/profile/Uche-Mbanaso/publication/...>, [Eriřim:2 Şubat 2021].
- Mbanaso, U., & Dandaura, E. S. (2015). The Cyberspace and Intensification of Privacy Invasion. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 24-31.
- McCarroll, E. (2019). Weapons of Mass Deportation: Big Data and Automated Decision-making Systems in Immigration Law. *Geo. Immigr. LJ*, 34, 705.
- McLaughlin, G. M. (2 Ocak 2023). Data, Privacy, And the Future of Artificial Intelligence. https://www-cyberdefensemagazine-com.translate.goog/data-privacy/?_x_tr_sl=en&_x_tr_tl=tr&_x_tr_hl=tr&_x_tr_pto=sc. [Eriřim:20 Haziran 2023].
- McMullan, T. (23 Temmuz 2015). What does the panopticon mean in the age of digital surveillance?.<https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham>, [Eriřim:9 Ocak 2022].
- M.D. ve Others v. Spain Davası (Bařvuru No: 36584/17). (2022). Avrupa İnsan Hakları Mahkemesi Raporları. <https://hudoc.echr.coe.int/fre#{%22tabview%22:...>, [Eriřim:20 Ağustos 2023].
- Menteř vd. Davası (Bařvuru No: 23186/94). (1997). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-58120%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58120%22]}), [Eriřim: 9 Eylül 2022].
- Metin, Y. (2002). Avrupa Birlięi Temel Haklar řartı. *Ankara Üniversitesi SBF Dergisi*, 57(04).
- Metin, Y., & Kaygısız, Ü. (2011). Avrupa Birlięi'nde Temel Hakların Korunması ve Lizbon Antlaşması'nın Getirdięi Yenilikler. *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 1(1), 125-158.
- Meyers, C. A., Powers, S. S., & Faissol, D. M. (2009). Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. <https://doi.org/10.2172/967712>, [Eriřim: 19 Şubat 2021].
- Miller, B. H. (2018). Open source intelligence (OSINT): an oxymoron?. *International Journal of Intelligence and CounterIntelligence*, 31(4), 702-719.

- Milli İstihbarat Teşkilatı. (t.y.). İstihbarat Oluşumu. <https://www.mit.gov.tr/isth-olusum.html>, [Erişim: 19 Şubat 2021].
- Moise, A. C. (2018). Cybersecurity and Human Rights. *Universul Juridic*, (Suplim), 160-164.
- Mombelli, I., & Piodi, F. (2014). *The ECHELON Affair: The EP and the global interception system 1998–2002*. Luxembourg: Publications Office of the European Union.
- Moreham, N. A. (2008). Why is privacy important? Privacy, dignity and development of the New Zealand breach of privacy tort. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383510, [Erişim: 19 Şubat 2021].
- Moorehead, A. (2017). *Out of the Shadows: Recommendations to Advance Transparency in the Use of Lethal Force*. New York, Columbia Law School Human Rights Clinic.
- Morsink, J. (2010). *The Universal Declaration of Human Rights*. In *The Universal Declaration of Human Rights*. University of Pennsylvania Press.
- Naankiel, P. W., & Iortyer, P. T. (2014). An appraisal of the Council of Europe. *Journal of the National Association for Science, Humanities and Education Research*, 12(1), 46-53.
- Niemietz Davası (Başvuru No: 13710/88). (1992). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57887%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57887%22]}), [Erişim: 9 Eylül 2022].
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79(1), 119-157.
- Nissenbaum, H. (2005) Where Computer Security Meets National Security. *Ethics and Information Technology* 7 (2): 61–73.
- Nissenbaum, H (2011). A Contextual Approach to Privacy Online. *Dædalus, the Journal of the American Academy of Arts & Sciences*, 140(4): 32-48.
- Noveck, B. S. (1999). Transparent space: Law, technology and deliberative democracy in the information society. *Journal for Cultural Research*, 3(4), 472-491.
- Nunn, S. (2001). Cities, Space, and the New World of Urban Law Enforcement Technologies. *Journal of Urban Affairs*, 23(3-4), 259-278.

- Nye, J. S. (2014). *The regime complex for managing global cyber activities* (Vol. 1), 5-15. Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University.
- Nye, J. S. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, 5(4), 18-38.
- Ogundoyin, S. O. (2020). A Lightweight Privacy-Preserving Data Aggregation Scheme with Provable Security for Internet-of-Things. *International Journal of Computers and Applications*, 42(3), 315-327.
- Olcaý, S. (2019). Konut Dokunulmazlığı Hakkı ve Konut Dokunulmazlığının İhlali Suçu. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 6(1), 225-264.
- Orlemans, J.J. (25 Şubat 2022). Privacy risks of (automated) Open Source Intelligence (OSINT). <https://aboutintel.eu/privacy-and-automated-osint/>, [Erişim:2 Şubat 2021].
- Organization for Economic Co-operation and Development. (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Paris, France. <https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>, [Erişim:4 Ocak 2022].
- Orwell, G. (2008). *Bin Dokuz Yüz Seksen Dört*. İstanbul: Penguin Kitapları.
- Othman, Z., Buys, L., & Aird, R. (2013, February). Home and the Embodiment of Privacy. In *TS+ B1 (Time, Space and Body) Global Conference*. <https://eprints.qut.edu.au/67484/>, [Erişim:28 Ocak 2021].
- Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. <https://search.proquest.com/openview/11c3f4f3a7ca044eeb3a18a4929dc5ff/1?pq-origsite=gscholar&cbl=396500>, [Erişim:28 Haziran 2020].
- Özbek, M. (2004). Giriş: Kamusal-Özel Alan, Kültür ve Tecrübe, (Ed. Meral Özbek). İstanbul: Hil Yayınları, 443-499.
- Papacharissi, Z. (2002). The virtual sphere: The internet as a public sphere. *New media & society*, 4(1), 9-27
- Pereira, C. S., Durão, N., Moreira, F., & Veloso, B. (2022). The importance of digital transformation in international business. *Sustainability*, 14(2), 834.

- Petri Sallinen ve Diğerleri Davası (Başvuru No: 50882/99). (2005). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-70283"\]}](https://hudoc.echr.coe.int/eng#{), [Erişim:9 Eylül 2022].
- Ploug, T. (2009). *Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction*. Springer Science & Business Media.
- Pokempner, D. (2013). Cyberspace and State Obligations in the Area of Human Rights. *Peacetime regime for state activities in cyberspace, International law, international relations and diplomacy, Tallinn*, 239-260.
- Post, R. C. (1986). The Social Foundations of Defamation Law: Reputation and the Constitution. *California Law Review*, 74(3), 691-742.
- Poster, M. (1990). *The Mode of Information. Post-Structuralism and Social Contexts*. Chicago: University of Chicago Press.
- Poster, M. (2018). Foucault, Deleuze ve Yeni Medya. (Özel sayı) *Cogito* (70-71), s. 536-551.
- Popa, I. F. (2015). Extensive transparency as principle of cyberspace governance and cyber security dilemma prevention. *Annals of the Constantin Brancusi University of Targu Jiu, Letters and Social Sciences Series*, 2015(1), 59-62.
- Posner, R.A. (1983), *The Economics of Justice* (5. print ed.), Harvard University Press. Cambridge.
- Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, 323-333.
- Rajpari, A. (12 Ekim 2020). Is Internet Access a Human Right?. <https://sites.uab.edu/humanrights/2020/10/12/is-internet-access-a-human-right/>, [Erişim:20 Ocak 2021].
- Rane, P. B., & Meshram, B. B. (2012). Transaction security for e-commerce application. *International Journal of Electronics and Computer Science Engineering*, 1(3), 1720-1726.
- Rao, K. K. (2016). Human Rights and Cyberspace: Use and Misuse. *Bharati Law Review*, 12(2), 5-31.
- Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). *Artificial Intelligence & Human Rights: Opportunities & Risks*. Berkman Klein Center Research Publication.

- Reber, P. (1 Mayıs 2010). What Is the Memory Capacity of the Human Brain? <https://www.scientificamerican.com/article/what-is-the-memory-capacity/>, [Eriřim:1 Eylül 2021].
- Reglitz, M. (2020). The human right to free internet access. *Journal of Applied Philosophy*, 37(2), 314-331.
- Rengel, A. (2014). Privacy as an International Human Right and the Right to Obscurity in Cyberspace. *Groningen Journal of International Law*, 2(2),37-42.
- Richards, N. M. (2013). The Dangers Of Surveillance. *Harvard Law Review*, 126(7), 1934-1965. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239412, [Eriřim:20 Mayıs 2029].
- Roagna, I. (2012). Avrupa İnsan Hakları Sözleşmesi Kapsamında Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkının Korunması. *Ayşegül Alkış Schäling, Avrupa Konseyi, Strazburg*. <https://rm.coe.int/16806f15ae>, [Eriřim:10 Nisan 2022].
- Robathin v. Austria Davası (Bařvuru No: 30457/06). (2012). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-111890%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-111890%22]}), [Eriřim:10 Nisan 2022].
- Robertson, A. H. (1965). The Political Background and Historical Development of the European Convention on Human Rights. *Int'l & Comp. LQ Supp. Pub.*, 11, 24. https://heinonline.org/HOL/Page?handle=hein.journals/icqlsup11&div=7&g_s ent=1&casa_token=&collection=journals, [Eriřim:18 Eylül 2022].
- Roman Zakharov v. Russia Davası (Bařvuru No: 47143/06). (2015). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-159324%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}), [Eriřim:10 Nisan 2022].
- Rona, G., & Aarons, L. (2016). State responsibility to respect, protect and fulfill human rights obligations in cyberspace. *Journal of National Security Law and Policy*,8(3), 503-530.

- Rosen, J. (2012). "The Right to Be Forgotten." *Stanford Law Review* 64. (88-92)
<https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>, [Eriřim:20 Ocak 2021].
- Royston, S. W. (2016). The Right to Be Forgotten: Comparing US and European Approaches. *St. Mary's Law Journal*, 48(2), 253-275.
<https://commons.stmarytx.edu/thestmaryslawjournal/vol48/iss2/4/>, [Eriřim:3 Ocak 2021].
- Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning?. *International Data Privacy Law*, 3(2), 74-87.
- S. and Marper v. the United Kingdom Davası (Bařvuru No: 30562/04 ve 30566/04). (2008). Avrupa İnsan Hakları Mahkemesi Raporları.
[https://hudoc.echr.coe.int/#{%22fulltext%22:...}](https://hudoc.echr.coe.int/#{%22fulltext%22:...), [Eriřim:10 Nisan 2022].
- Salihpařaoęlu, Y. (2013). Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İtihatları Iřığında Bir Deęerlendirme. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakóltesi Dergisi*, 17(3), 227-266.
- Schäfer, M. S. (2015). Digital Public Sphere. G. M. (Ed.), K. G. Barnhurst, K. Ikeda, R. C. Maia, & H. Wessler içinde, *The International Encyclopedia of Political Communication* (s. 322-328). London: Wiley Blackwell.
- Sennett, R. (2013). *Kamusal İnsanın Çöküşü* (Çev: Abdullah Yılmaz, Serpil Durak). İstanbul: Ayrıntı Yayınları.
- Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
- Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *New York Law Review*, 86(6).
https://scholarship.law.gwu.edu/faculty_publications/940/, [Eriřim:10 Nisan 2022].
- Sebeny, H. (2013). Indian wars. In K. Piehler (Ed.), *Encyclopedia of military science* (Vol. 1, pp. 660-664). SAGE Publications.
- Security&Infrastructure Security Agency (2019). What is Cyber Intelligence?
https://fedvte.usalearning.gov/publiccourses/ICI/course/videos/pdf/ICI_D01_S01_T01_STEP.pdf, [Eriřim:10 Eylül 2021].
- Shimonski, R. (2014). *Cyber reconnaissance, surveillance and defense*. Syngress.

- Shue, H. (2009). Temel hakların evrenselliği. *İnsan Haklarının Felsefi Temelleri*, Ankara: Türkiye Felsefe Kurumu, 3, 39-65.
- Simpson, A. W. Brain, (2004). 'From the Brussels Treaty to the Council of Europe', Human Rights and the End of Empire: Britain and the Genesis of the European Convention, Oxford.
- Singleton, S. (1999). Panel on privacy issues in cyberspace. *Texas Journal of Women and the Law*, 8(2), 295-304.
- Sivil ve Siyasal Haklar Konvansiyonu (1976). International Covenant on Civil and Political Rights. https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf, [Erişim:20 Ağustos 2022].
- Skepys, B. (2012). Is There a Human Right to the Internet?. *Journal of Politics and Law*, 5(4), <http://dx.doi.org/10.5539/jpl.v5n4p15>, [Erişim:2 Nisan 2020].
- Snijder, M. (2016). Biometrics, surveillance and privacy. *JRC Science Hub European Union*. https://erncipproject.jrc.ec.europa.eu/sites/default/files/JRC104392_biometrics_surveillance_and_privacy_final.pdf. [Erişim:15 Ocak 2023].
- Snowden-Interview: Transcript. (26 Ocak 2014). https://web.archive.org/web/20140128224439/http://www.ndr.de/ratgeber/netzwelt/snowden277_page-3.html. [Erişim:21 Şubat 2022].
- Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-564. <https://www.jstor.org/stable/40041279>, [Erişim:26 Nisan 2022].
- Solove, D. (2007). Anonymity and Accountability. *The Future of Reputation. New Haven, Yale*.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press, Cambridge.
- STM Teknolojik Düşünce Merkezi. (2021). Yüz Tanıma Sistemlerinin Bugünü ve Geleceği. TrendAnaliziEkim 2021. https://thinktech.stm.com.tr/uploads/docs/1635615850_stm-yuz-tanima-sistemleri.pdf, [Erişim:22 Şubat 2022].
- Stottlemire, S. A. (2015) HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence, *International Journal of Intelligence and Counter Intelligence*, 28:3, 578-589.

- Szabó ve Vissy v. Hungary Davası (Başvuru No: 37138/14). (2016). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-160020%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-160020%22]}), [Erişim:20 Ağustos 2022].
- Şen, E. (1989). Özel Hayatın Gizliliği ve Korunması Hakkı (Yayımlanmamış Yüksek Lisans Tezi). Marmara Üniversitesi, Türkiye.
- Şenol, M. (2018). *Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık*. (Ed: Şeref Sağıroğlu ve Mustafa Alkan). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık. Ankara: Grafiker Yayınları, 181-221.
- Jørgensen, R. F. & Desai, T. (2017) Right to Privacy Meets Online Platforms: Exploring Privacy Complaints against Facebook and Google, *Nordic Journal of Human Rights*, 35:2, 106-126.
- Taylor-Sabori Davası (Başvuru No: 47114/99). (2003). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-60696"\]}](https://hudoc.echr.coe.int/eng#{), [Erişim:9 Eylül 2022].
- T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. Erişim adresi: <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-planlari-2020-2023.pdf>. [Erişim:20 Ağustos 2022].
- TechTarget. (2015). SIGINT (Signals Intelligence). Erişim adresi: <https://www.techtarget.com/whatis/definition/SIGINT-signals-intelligence#...> [Erişim:7 Eylül 2021].
- Teknolojik Düşünme Merkezi-STMthinktech. (t.y.). Veri Odaklı Çağda İstihbarat”. https://thinktech.stm.com.tr/uploads/docs/1608845963_stm-blog-veri-odakli-cagda-istihbarat.pdf, [Erişim:20 Ağustos 2022].
- Tene, O., & Polonetsky, J. (2013). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239. <https://redi.anii.org.uy/jspui/handle/20.500.12381/442>, [Erişim:7 Eylül 2021].
- Tezcan, D. (1991). “Bilgisayar Karşısında Özel Hayatın Korunması”, *Anayasa Yargısı Dergisi*, C. 8, s. 385-392, <https://ayam.anayasa.gov.tr/media/4797/dtezcan.pdf>, [Erişim:19 Mart 2021].

- Tezcan, D. (2006). AİHS ve Ek Protokoller İle Güvence Altına Alınan Haklar ve AİHS’de Yer Almayan Temel Haklar. *İnsan Hakları, Konferans, Panel ve Sempozyumlar*, 31.
- The General Data Protection Regulation (2018). General data protection regulation (GDPR). European Public Service Union, 24(1). https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf, [Erişim:22 Mart 2022].
- Townsend, T., Ludwick, M., McAllister, J., Mellinger, A. O., & Sereno, K. A. (2013). *SEI Innovation Center report: Cyber intelligence tradecraft Project: Summary of key findings*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.
- Tully, S. (2014). A human right to access the Internet? problems and prospects. *Human Rights Law Review*, 14(2), 175-195.
- Tüfekçi, Z. (19 Mart 2018). Facebook’s Surveillance Machine. <https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html>, [Erişim:11 Ocak 2020].
- Ulbashiev, A. K. (2020). The right to a name: Back to the future. *Digital Law Journal*, 1(3), 40-50. <https://doi.org/10.38044/2686-9136-2020-1-3-40-50>, [Erişim:12 Nisan 2021].
- United Nations Drafting Committee Report-1st Session (1947). Universal Declaration of Human Rights (1948), Drafting History. <https://research.un.org/en/undhr/draftingcommittee/1>, [Erişim: 11 Aralık 2022].
- United Nations Drafting Committee-2nd Session (1948). Report of the Drafting Committee [on an International Bill of Rights] to the Commission on Human Rights: E/CN.4/95. <https://research.un.org/en/undhr/draftingcommittee/2>, [Erişim: 11 Aralık 2022].
- UN General Assembly. (1948). Draft International Declaration of Human Rights, Report of the Third Committee to the 3rd Session A/777. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/NL4/812/19/PDF/NL481219.pdf?OpenElement>, [Erişim: 11 Aralık 2022].
- UN Human Rights Committee (8 Nisan 1988). CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home

- and Correspondence, and Protection of Honour and Reputation. <https://www.refworld.org/docid/453883f922.html> [Eriřim: 11 Aralık 2022].
- United Nations Human Rights Office of the High Commissioner. (2021). The Right to Privacy in the Digital Age. <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>, [Eriřim: 10 Nisan 2022].
- Universal Declaration of Human Rights. (1948). Universal Declaration of Human Rights. United Nations. URL: <https://www.un.org/en/universal-declaration-human-rights/>, [Eriřim: 1 Mart 2022].
- Üzeltürk, S. (2004). *1982 Anayasası ve İnsan Hakları Avrupa Sözleşmesi'ne Göre Özel Hayatın Gizlilięi Hakkı*, Beta Basım A.Ş. , İstanbul.
- Vilić, V., Radenković, I. (2017). The Right to Privacy, Informational Privacy and the Right to Information in the Cyberspace. *In Sinteza 2017-International Scientific Conference on Information Technology and Data Related Research*. doi:10.15308/Sinteza-2017-74-78, [Eriřim: 7 Eylül 2022].
- Volodina v. Russia Davası (Bařvuru No: 40419/19). (2021). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-211794%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-211794%22]}), [Eriřim:20 Ağustos 2023].
- X Davası (Bařvuru No: 7308/75). (1978). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-73955%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-73955%22]}), [Eriřim:9 Eylül 2022].
- X ve Y Davası (Bařvuru No: 8962/80). (1982). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-74290%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-74290%22]}), [Eriřim:10 Eylül 2022].
- Yao, M. Z. (2011). *Self-protection of online privacy: A behavioral approach. In Privacy online: Perspectives on privacy and self-disclosure in the social web* (111-125). Berlin, Heidelberg: Springer Berlin Heidelberg.
- Yılmaz, O. (2020). Franz Kafka'nın Dava adlı eseri bağlamında siber gözetim ve birey. *RumeliDE Dil ve Edebiyat Arařtırmaları Dergisi*, RumeliDE.Ö8 (Kasım) II. Uluslararası Akademik Filoloji Çalışmaları Kongresi, 423-431.

- Wacks, R. (1987) . Secrets: On the Ethics of Concealment and Revelation. *The Modern Law Review*, 50 (1). 125-128
- Wachter, S. (2018). The GDPR and the Internet of Things: a three-step transparency model. *Law, Innovation and Technology*, 10(2), 266-294.
- Waltz, S. (2002). Reclaiming and rebuilding the history of the Universal Declaration of Human Rights. *Third World Quarterly*, 23(3), 437-448. <https://www.tandfonline.com/doi/abs/10.1080/01436590220138378>, [Eriřim:9 Eylül 2022].
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. https://www.jstor.org/stable/1321160#metadata_info_tab_contents, [Eriřim:9 Eylül 2022].
- Warso, Z. (2019). *Analysis of the legal and human rights requirements for Human Enhancement Technologies in and outside the EU*. SIENNA Project
- Watt, E. (2021). *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. In *State Sponsored Cyber Surveillance*. Edward Elgar Publishing.
- Weber, R. H. (2011). The right to be forgotten: more than a pandora's box?. *Journal of Intellectual Property, Information Technology and E-Commerce (JIPITEC)*, 2(2), 120-130.
- Weber, R. H., & Heinrich, U. I. (2012). *Anonymization*. Springer Science & Business Media.
- Weintraub, J., & Kumar, K. (Eds.). (1997). *Public and private in thought and practice: Perspectives on a grand dichotomy*. University of Chicago Press.
- Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 25(1), 166. <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>, [Eriřim:3 Temmuz 2022].
- Westlund, M. (2018). The development of the right to privacy under the ECHR: A study on the effect of Article 8 on third parties. Yayınlanmamıř Yüksek Lisans Tezi, Uppsala Universitet, İsveç.

- Weil, G. L. (1963). The Evolution of the European Convention on Human Rights. *American Journal of International Law*, 57(4), 804-827.
- Whittaker, J. (2004). *The Cyberspace Handbook*. Psychology Press.
- Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine* (Second Edition). The M.I.T. Press.
- Wiener, N. (1948). Cybernetics. *Scientific American*, 179(5), 14-18.
- Williams, M. (2004) Understanding King Punisher and his order: Vandalism in an online community – Motives, meanings and possible solutions. *Internet Journal of Criminology* 1–40. <https://orca.cardiff.ac.uk/id/eprint/60676/>, [Eriřim:5 Temmuz 2021].
- Wieser ve Bicos Beteiligungen GmbH Davası (Bařvuru No: 74336/01). (2007). Avrupa İnsan Hakları Mahkemesi Raporları. [https://hudoc.echr.coe.int/eng#{"itemid":\["001-82711"\]](https://hudoc.echr.coe.int/eng#{), [Eriřim:9 Eylöl 2022].
- Winter, J. (2013). *René Cassin and human rights: from the Great War to the Universal Declaration*. Cambridge University Press.
- Wise, J. (26 Mayıs 2023). How Many CCTV Cameras in London Are There in 2023? <https://earthweb.com/how-many-cctv-cameras-in-london-are-there/>, [Eriřim:3 Temmuz 2023].
- Wise, J. (7 Ağustos 2023). How Many People Have Smartphones In 2023? (Key Statistics) <https://earthweb.com/smartphone-statistics/>. [Eriřim:18 Ekim 2023].
- Wood, D. (2003). Foucault and panopticism revisited. *Surveillance & Society*, 1(3), 234-239. <https://doi.org/10.24908/ss.v1i3.3338>, [Eriřim:18 Ekim 2023].
- Working Group Report. (10 Aralık 1947). Working Group on the Declaration on Human Rights, Report to the Commission on Human Rights. <https://digitallibrary.un.org/record/561278>. [Eriřim:18 Ekim 2020].
- Ziccardi, G. (2013). Digital Resistance, Digital Liberties and Human Rights. In *Resistance, Liberation Technology and Human Rights in the Digital Age* (pp. 125-160). Springer, Dordrecht.
- Ziolkowski, K. (2013). Peacetime regime for state activities in cyberspace. *Tallinn: NATO CCD COE Publications*.