T.C.

İSTANBUL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİYASET BİLİMİ ve ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

BİLİŞİM SUÇLARININ ULUSAL VE ULUSLARARASI DÜZEYDE DEĞİŞEN GÜVENLİK ALGISI ÜZERİNDE ETKİSİ

HAKAN EHLİZ

2501100589

TEZ DANIŞMANI

Prof. Dr. LEVENT ÜRER

İSTANBUL-2019

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı	:	HAKAN EHLİZ	**Numarası**	: 2501100589
Anabilim Dalı / Anasanat Dalı / Programı	:	SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER	**Danışmanı**	: PROF. DR. LEVENT ÜRER
Tez Savunma Tarihi	:	21.10.2019	**Saati**	: 11.00
Tez Başlığı	:	BİLİŞİM SUÇLARININ ULUSAL VE ULUSLARARASI DÜZEYDE DEĞİŞEN GÜVENLİK ALGISI ÜZERİNE ETKİSİ.		

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin **36. Maddesi** uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. LEVENT ÜRER		KABUL
2- PROF. DR. NAMIK SİNAN TURAN		KABUL
3- DR. ÖĞR. ÜYESİ LEVENT DEMİRELLİ		RED

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. BURAK SAMİH GÜLBOY		
2- DR. ÖĞR. ÜYESİ ATAHAN BİROL KARTAL		

ÖZ

BİLİŞİM SUÇLARININ ULUSAL VE ULUSLARARASI DÜZEYDE DEĞİŞEN GÜVENLİK ALGISI ÜZERİNDE ETKİSİ

Hakan EHLİZ

Güvenlik kavramı üzerine yapılan çalışmalara bakıldığında, ilk dönem çalışmalarında güvenliğin, askeri güç ve coğrafi sınırlar ile dar bir alan çerçevesinde incelendiği görünmektedir. Özellikle Soğuk Savaş'ın sona ermesi ile birlikte değişen uluslararası sistem, güvenlik algısı üzerinde de etkili olmuştur. Güvenlik kavramının içeriği, askeri boyutun ötesine taşınmış, çevresel, siyasi, ekonomik ve sosyal boyutlar da eklenerek kapsamı genişlemiştir.

20. yüzyılın sonlarında başlayan ve günümüzde devam eden teknolojik gelişmeler, güvenliğin başka bir boyut kazanmasına neden olmuş ve siber güvenlik kavramı ortaya çıkmıştır. İnternetin tüm dünya geneline yayılabilme özelliği, ucuz ve kolay erişilebilir olması nedeniyle kullanımının her geçen gün artması bu alanda güvenliğin tesis edilmesini hem zorlaştırmış hem de bir zorunluluk haline getirmiştir. Bilişim suçları diye adlandırılan bu ortamdaki suç potansiyeli oldukça fazladır. Birey ya da devlet olarak her ölçekte tehdit ile karşı karşıya olunan bu sanal dünyada güvenliğin sağlanması için çeşitli tedbirler alınması gerekmektedir.

Bu çalışmada, günümüzün çok boyutlu güvenlik algısı içerisinde siber güvenliğin öneminden söz edilmiş, daha sonra bu güvenliği tehdit eden bilişim suçları ayrıntıları ile değerlendirilmiş ve devletlerin bu suçlara karşı tedbirlerinden bahsedilmiştir. Son olarak da bu tedbirlerin kişi hak ve özgürlüklerine karşı etkisi değerlendirilmeye çalışılmıştır.

Anahtar Sözcükler: Güvenlik, Bilişim Suçları, Siber, Siber Güvenlik, Erişim Engelleme.

ABSTRACT

THE EFFECT OF INFORMATICS CRIMES ON NATIONAL AND INTERNATIONAL LEVEL OF DEVELOPİNG SECURITY PERCEPTION

Hakan EHLIZ

When the studies on the concept of security are examined, it is seen that security was examined within the framework of a narrow area only with military power and geographical boundaries. Particularly with the end of the Cold War, the changing international system has had an impact on the perception of security. The content of the concept of security has been extended beyond the military dimension and its scope has been expanded by adding environmental, political, economic and social dimensions.

The technological developments that started at the end of the 20th century and continued today have led to another dimension of security and the concept of cyber security has emerged. Due to the fact that the internet can be connected easyly from all over the World, and it can be reached cheaply, its use increases day by day, making the establishment of security in this field both difficult and obligatory. The crime potential in this environment, which is called informatics crimes, is quite high. Various measures need to be taken in order to ensure security in this virtual world which is faced with threats at every scale as an individual or a state.

In this study, the importance of informatics security in today's multi-dimensional security perception is mentioned, then the informatics crimes that threaten this security are examined in detail and the measures of the states against these crimes are mentioned. Finally, the effects of these measures against individual rights and freedoms have been tried to be explained.

Key Words: Security, İnformatics Security, Cyber, İnformatics Crimes, Access Blocking.

ÖNSÖZ

20. yüzyıl iki büyük dünya savaşının yaşandığı bir dönem olarak karşımıza çıkmaktadır. Dolayısıyla uluslararası sistemin güvenlik anlayışı da daha çok askeri güvenlik üzerinde odaklanmıştır. Yine bu dönemde coğrafi sınırlar da askeri güç ile birlikte ele alınan güvenlik konularından olmuştur.

İki büyük savaşı takip eden Soğuk Savaş süreci, Sovyetler Birliği'nin yıkılması ile son bulmuştur. 20. yüzyılın son yıllarına rastlayan bu dönem uluslararası sistemin yeniden şekillenme sürecine girmesinde etkili olmuştur. Çok kutuplu olarak nitelenen yeni uluslararası yapıdan, güvenlik algısı da etkilenmiş ve çok boyutlu bir güvenlik anlayışı ortaya çıkmıştır.

Çok kutuplu güvenlik anlayışına küreselleşmenin etkisiyle coğrafi sınırların ötesinde düşünme zorunluluğunu da eklediğimizde güvenlik anlayışı karmaşık bir hal almıştır diyebiliriz. Özellikle son yıllarda bilim ve teknoloji alanındaki gelişmeler ile birlikte internetin günlük hayatın içerisine hızlı bir şekilde girmesi, sanal dünyanın birçok alanda fiziki dünyada yapılan işlemlere alternatif hale gelmesi siber güvenlik kavramını ön plana çıkarmıştır.

Sanal dünyanın bu özellikleri kötü niyetli kişi/gruplar için de çekici olmaktadır. Bu kişi/gruplar sanal alanda suç işlemek suretiyle çeşitli amaçlarla çıkar sağlayabilmektedir. Bilişim suçları olarak ifade edilen bu suçlar, son yıllarda kişi ve devlet güvenliğini ciddi boyutlarda tehdit eder hale gelmiştir.

'Bilişim Suçlarının Ulusal ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerinde Etkisi' başlıklı bu çalışmada, değişen güvenlik algısı ile siber güvenlik arasındaki ilişki incelendikten sonra sanal dünyada işlenen bilişim suçları içerik, kapsam ve hukuki boyut açılarından ayrıntılı şekilde ele alınacaktır. Daha sonra bilişim suçlarına karşı Türkiye ve dünyada ne tür önlemlerin alındığından bahsedilecektir. Ardından devletlerin internet ortamında işlenebilecek suçlara ve internette bulunan zararlı içeriğe yönelik olarak erişimin engellenmesi veya otomatik filtreleme şeklinde

aldıkları tedbirlerden söz edilecek ve bu yaklaşımın kişi hak ve özgürlüklerine etkileri de ayrıca tartışılacaktır.

Bu çalışmamda değerli fikirleri ile beni yönlendiren ve benden yardımlarını hiçbir zaman eksik etmeyen çok değerli hocam ve tez danışmanım Prof. Dr. Levent Ürer'e, çalışmayı hazırlama sürecimde beni cesaretlendiren aileme ve arkadaşlarıma teşekkür ediyorum…

Hakan EHLİZ

İstanbul – 2019

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

SİBER GÜVENLİĞİN SAĞLANMASI BAĞLAMINDA İNTERNETE ERİŞİMİN ENGELLENMESİNİN ULUSAL VE ULUSLARARASI SEVİYEDE İRDELENMESİ

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

A.e. : Aynı Eser

a.g.e. : Adı Geçen Eser

AİHS : Avrupa İnsan Hakları Sözleşmesi

AİHM : Avrupa İnsan Hakları Mahkemesi

APEC : Asya-Pasifik Ekonomik İşbirliği Forumu

AR-GE : Araştırma-Geliştirme

ARI : Advanced Resources International

ARPANET : Gelişmiş Araştırmalar Projeleri Dairesi Ağı

BTK : Bilgi Teknolojileri ve İletişim Kurumu

Bknz./bknz. : Bakınız

BM : Birleşmiş Milletler

Bs./bs. : Baskı/Basım

BTK : Bilgi Teknolojileri ve İletişim Kurumu

DARPA : Savunma İleri Düzey Araştırma Projeleri Birimi

Ed./ed. : Editör (Yayına Hazırlayan)

IMF : Uluslararası Para Fonu

ITU : Uluslararası Telekomünikasyon Birliği

Md./md. : Madde

NAFTA : Kuzey Amerika Serbest Ticaret Bölgesi

NATO : Kuzey Atlantik Antlaşması Örgütü

ODTÜ	: Orta Doğu Teknik Üniversitesi
OECD	: Ekonomik İşbirliği ve Kalkınma Örgütü
PTT	: Posta ve Telgraf Teşkilatı Genel Müdürlüğü
R.G.	**:** Resmi Gazete
S.	**:** Sayı (dergi/gazetelerde)/Sayfa/Slayt (sunumlarda)
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TCK	: Türk Ceza Kanunu
TÜVEKA	: Türkiye Üniversiteler ve Araştırma Kurumları Ağı
Vol.	**:** Volume (Cilt)
yy.	**:** Yüzyıl

GİRİŞ

20. yüzyılın sonlarına doğru başlayan ve günümüzde hızlı bir şekilde devam eden bilim ve teknoloji alanındaki ilerlemeler, küreselleşme olgusunun beraberinde getirdiği gelişmelerle bir araya geldiğinde karşımıza çok daha farklı ve karmaşık bir güvenlik algısı çıkmaktadır.

Klasik güvenlik anlayışı, genel anlamda coğrafi sınırlar üzerinden askeri güç merkezli çıkarımlar yapmakta ve bu yönde bir güvenlik perspektifi oluşturmaktaydı. Ancak Soğuk Savaş'ın sona ermesi, iki kutuplu dünya düzeni üzerine kurgulanmış uluslararası sistemde değişime neden olmuştur. Çok kutuplu ve hegemon ABD'nin oluşturduğu yeni uluslararası sistemde devletlerin yanına çok uluslu şirketler, uluslararası kurum ve kuruluşlar gibi yeni aktörler eklenmiştir.

21. yüzyılda yaşanan bu gelişmeler ışığında güvenlik algısının çok boyutlu bir hal alması da kaçınılmaz olmuştur. Bu boyutlar arasında ekonomik, çevresel, siyasal ve sosyal boyutlar sayılabilir. Güvenlik konusunun farklı boyutlarda değerlendirilmesinin en önemli nedenlerinden biri de internetin günlük hayatın içerisine hızlı ve yoğun bir şekilde girmesidir.

Türkiye İstatistik Kurumu'nun bu konuda yaptığı çalışmalara bakıldığında; 2019 yılı için işyeri, kurum ve kuruluşlarda internet erişimi % 94,9, hanelerde internet erişimi ise % 88,3 olarak hesaplanmıştır[1]. 2019 yılı Ocak ayı itibariyle de dünya genelinde nüfusun % 57'sinin (4,39 milyar kişi) internet kullanıcısı, % 45'inin (3,48 milyar kişi) sosyal medya kullanıcısı, % 67'sinin de mobil telefon kullanıcısı olduğu ve geçen yılın aynı ayına oranla internet kullanımının % 9,1 (367 milyon kişi) arttığını göz önüne aldığımızda internetin her ortama girebildiğini daha iyi görebiliriz[2].

[1] TÜİK, **Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması, Hanelerde Bilişim Teknolojileri Kullanımı Araştırması, (**çevrimiçi) http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=1615, Erişim: 12 Eylül 2019.

[2] "We Are Social 2019 Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri", çevrimiçi https://wearesocial.com/global-digital-report-2019, Erişim: 14 Eylül 2019.

İnternet kullanımının yaygınlaşmasının doğal bir sonucu olarak bu alanda da bazı sorunlar ortaya çıkmıştır. Özellikle internet kullanımının ucuz oluşu, erişim kolaylığı gibi nedenlerin de etkisiyle internet üzerinden işlenen bireysel ve organize suçlarda da artışlar yaşanmıştır. Bu bağlamda internette güvenliğin sağlanması hususu öne çıkmış ve her ülke bu yönde çalışmalar yapmaya başlamıştır.

"Bilişim Suçlarının Ulusal ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerindeki Etkisi" isimli çalışmadaki temel amaç; 21. yüzyılda teknolojinin hızlı bir biçimde geliştiği küreselleşen dünyada bilişim alanında giderek artan ve farklılaşan suçların ülkelerin güvenlik algılarına etkisini belirlemeye çalışmak, bu suçların önlenmesi amacıyla gerçekleştirilen faaliyetlerin neler olduğunu ve bu faaliyetlerin olası sonuçlarını ortaya koymaya çalışmaktır. Bu çalışma kapsamında;

- Soğuk Savaş sonrası dönemde güvenlik algısında ne tür değişimlerin olduğu,
- Bilişim suçlarının değişen güvenlik algısı üzerinde nasıl bir rolü/içeriği olduğu,
- Bilişim suçlarının önlenmesi için devletler tarafından yapılan çalışmaların neler olduğu ve bu çalışmaların kişi hak ve özgürlükleri üzerinde bir baskı oluşturup oluşturmadığı, sorularına yanıt aranacaktır. Bu araştırma soruları bağlamında çalışmanın hipotezi şu şekildedir:

Bilişim suçlarının önlenmesi amacıyla devletlerin internet erişimini kısıtlamalarının kimi zamanlarda kötüye kullanılabileceği ve bu durumun da kişilerin hak ve özgürlükleri üzerinde sorunlara neden olabileceğidir. Bu kapsamda;

Çalışmanın ilk bölümünde güvenlik kavramı ve klasik güvenlik anlayışının günümüze kadar geçirdiği süreç incelenecektir. Takiben güvenlik algısının 21. yüzyılda yaşanan bilimsel ve teknolojik gelişmeler ışığında nasıl şekillendiği ve bunun elektronik ortamdaki izdüşümleri ile ilgili incelemeler yapılacaktır. Siber alan diye tanımlanan bu ortamda tehdit ve saldırıların karakteristik yapılarının da farklılaştığını

ve ona göre tedbirlerin alınacağını ifade etmek suretiyle siber güvenlik kavramı incelenmeye devam edilecektir.

Çalışmanın ikinci bölümünde, internet kavramını tarihsel arka planı üzerinden incelenecek ve internetin teknik özelliklerinden kısaca bahsedilecektir. Daha sonra bu çalışmanın temel unsurlarından olan bilişim suçları konusuna daha derin bir giriş yaparak, bilişim suçlarının özellikleri ve sınıflandırılması, bilişim suçu işleme yöntemleri üzerinde durulacaktır. Akabinde Türkiye ve dünya ölçeklerinde bilişim suçlarını önlemeye yönelik hazırlanmış hukuki düzenlemelere yer verilecektir. Yine Türkiye ve dünyada işlenmiş bilişim suçları ile ilgili örnekler verilmek suretiyle konuya somut bir boyut kazandırılacaktır. Son olarak Türkiye'de bilişim sistemlerinin güvenliği analiz edilmeye çalışılacaktır.

Çalışmanın üçüncü ve son bölümünde, bilişim suçlarının önlenmesi amacıyla internete erişimin engellenmesi süreci, güvenlik algısı ile birlikte ele alınarak incelenecektir. Erişimin engellenmesi ile ilgili uygulanan genel yöntemler açıklandıktan sonra Türkiye ve dünyada erişimin engellenmesi ile ilgili uygulamalara yer verilecektir. Yine bu noktada internetin kısıtlanmasına karşı çıkan organizasyonlardan kısaca söz edilecektir. Bölümün son kısmında, internete erişimin engellenmesi sürecini ifade özgürlüğü üzerinden değerlendirmeye çalışılacak ve bu konudaki uygulamalara değinilecektir.

Tezin Önemi

Bilişim suçları ile yapılan çalışmalara bakıldığında genel olarak suç, suçun hukuki boyutları, internet uygulamaları gibi alanlara fazla bir yönelim olduğu görülmektedir. Ancak bu çalışmada olduğu üzere, bilişim suçları ile güvenlik ilişkisinin kurulmaya çalışıldığı ve internet dünyasındaki özgürlükler ile güvenlik arasındaki ilişkinin irdelendiği çalışma sayısının nispeten az olması nedeniyle literatüre bu alanda katkı sağlanacağı düşünülmektedir.

Tezin Varsayımları

Bu tez çalışmasında; aşağıdaki hususlar ispatına gerek duyulmadan doğru olarak kabul edilmiştir:

- 21. yüzyılda meydana gelen gelişmeler internetin önemini arttırmıştır.
- İnternetin uluslararası alanda kullanımının artması internetin güvenliği sorunsalını ortaya çıkarmıştır.
- İnternet kullanımının ucuz, erişimin kolay olması bu alanda işlenen suç miktarını arttırmaktadır.

Tezin Sınırlılıkları

Bu araştırmanın sınırlılıklarına bakıldığında;

- Uluslararası ilişkiler teorilerinin güvenlik ile ilintili kısımlarına değinilmektedir.
- Bilişim suçları ile ilgili dünya incelemeleri yapılırken belli başlı Batı ülkeleri ile Çin, Rusya ve Kuzey Kore dikkate alınmaktadır.
- Yukarıda bahsi geçen ülkelerle ilgili açık kaynaklarda elde edilebilen ikincil verilere yer verilmektedir.

Yöntem

"Bilişim Suçlarının Ulusal ve Uluslararası Düzeyde Değişen Güvenlik Algısı Üzerindeki Etkisi" isimli çalışma, nitel bir çalışma olup çalışmada genel tarama modeli kullanılacaktır. Çalışma bağlamında genel tarama modeli ile güvenlik algısının değişim süreci, internet kullanımının yaygınlaşmasının olumsuz sonuçlarından biri olarak bilişim suçlarının her yönüyle analizi ve bilişim suçlarının önlenmesi amacıyla uygulanan internete erişim engellemesinin doğurabileceği sonuçlar değerlendirilmeye çalışılacaktır. Çalışmada, akademik veri tabanları, yayın tarama siteleri, medya ve internet üzerinden elde edilecek ikincil kaynaklardan belgesel tarama yöntemi ile

yararlanılacaktır. Ayrıca hukuki metinler gibi birincil nitelikte olan ve erişime açık resmi belgelerden de araştırma ve analizin gerektirdiği ölçekte faydalanılacaktır.

BİRİNCİ BÖLÜM

KLASIK ANLAMDA GÜVENLİK ALGISININ ÇAĞDAŞ GÜVENLİK ALGISINA DÖNÜŞÜMÜ BAĞLAMINDA SİBER GÜVENLİK

1.1 Güvenlik Kavramı, Tanımı ve Kapsamı

Güvenlik kavramı ile ilgili yapılan birçok çalışmaya rağmen kavram üzerinde herkesin mutabık kaldığı bir tanıma ulaşmak mümkün olmamıştır. Bu durumun en önemli sebeplerinden biri güvenliğin çok boyutlu bir kavram olarak gösterilmesidir. Güvenlik konusunda çalışmaları bulunan Booth, güvenlik kavramının türetilmiş bir yapıda olduğunu söylerken herkesin kabulleneceği bir tanım yapılabilmesinin de zorluğunu ifade etmiştir[3]. Yine tüm zaman ve mekânlar üzerinden değerlendirme yapılmak istenildiğinde de aynı şekilde güvenlik kavramını tam anlamıyla karşılayabilecek yegâne bir cevabın bulunmadığı görülmektedir. Hem kişi hem de toplum bazında güvenlik algılayışı farklılık göstermektedir. Bu farklılığın temelinde siyasi, felsefi, inanç, tecrübe gibi etkenler rol oynamaktadır[4]. Bu karmaşık durumun bir sonucu olarak güvenlik, az gelişmiş bir kavram olarak nitelenmekte ve Barry Buzan'ın da sıkça ifade ettiği literatür eksikliği doğmaktadır[5].

Literatür açısından yaşanan bu sorunlara rağmen güvenliğin tanımlanması ile ilgili yapılan çalışmalara bakıldığında; Luciani'ye göre güvenlik, bir yeteneği ifade etmektedir. Dış tehdit ve saldırılara karşı kendini savunabilme yeteneğidir[6]. Devleti odak noktasına alan perspektiften değerlendirme yapıldığında güvenlik; barış zamanında sahip olunan değerlerin tehditlere karşı korunabilmesi ayrıca savaş

[3] Ken Booth, "Security and Self: Reflections of a Fallen Realist", **Critical Security Studies: Conceptsand Cases**, 1997, s. 84.
[4] Münevver Cebeci, "Tehdit Algılamasında Yapısal ve Konjonktürel Nitelikler / İthal Tehditler", **Türkiye'ye Yönelik Dış Kaynaklı Risk ve Tehditler Sempozyum Bildirileri**, Harp Akademileri Komutanlığı, İstanbul, 2007, s. 33.
[5] Barry Buzan, **People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era**, Great Britain, Harvester Wheatsheaf, 1991, s. 7.
[6] Giacomo Luciani, "The Economic Content Of Security", **Journal of Public Policy**, No: 8, 1989, s. 151.

durumuyla karşılaşıldığında zafer elde edebilme kudretidir[7]. Yine benzer şekilde Terriff de güvenliği, tehlike ve tehditlere karşı emniyette olmak şeklinde tanımlamıştır[8]. Bu tanımlamalara ek olarak güvenlik; düşmanını çeşitli yol ve yöntemler kullanarak kendi yanına çekme, dost yapabilme yeteneğidir[9]. Başka bir görüşe göre güvenlik kavramı, çeşitli formasyon ve içerikler yüklense de toplum içerisinde yaşamaya başlayan insan için korunma, barınma, sığınma ve yaşamını sürdürebilme ihtiyacının bir ürünü olagelmiştir[10]. Güvenliğin tanımı girişimleri farklı noktalardan hareketle yapılmış olsa da son kertede, kazanılmış değerlerin, dışardan gelecek saldırılar karşısında savunulması adına çeşitli davranış biçimleri ve faaliyetler eliyle tehdit ve risk barındıran unsurların etkisiz hale getirilmesi sürecidir[11]. Güvenlik kavramı, insanın varoluşundan itibaren hayatın içindeki yerini almış ve günümüze gelene kadar farklı evrelerden geçmiştir. Geçmişten günümüze bakıldığında kavramsal olarak güvenlik, genellikle bir süreç şeklinde ele alınmıştır. İçinde bulunulan dönem ve şartlar zemininde meydana gelen olaylar dizisi güvenlik kavramına içerik olarak zenginlik katmıştır[12].

Güvenlik çalışmalarına bakıldığında temel amacın, güç kullanılması için gerekli ortamı yaratan şartları belirlemek ve analiz etmek olduğu görünmektedir. Bunun yanında yine bu çalışmalarda elde edilmesi düşünülen alt amaçlar ise; güç kullanılmasının birey, toplum ve devlet üzerindeki etkilerini, devleti yönetenlerin güç kullanırken uygulayacakları politikaları etkileyip etkilemediğini ve etkiliyorsa ne şekilde olduğunu ortaya koymaya çalışmaktır.

Güvenlik alanında yapılan çalışmalara öncelikle Amerika Birleşik Devletleri (ABD)'nde rastlamaktayız. İkinci Dünya Savaşı'nın bitişini müteakip başlayan bu çalışmalar, dönemin de etkisiyle dar bir bakış açısıyla ve sadece askeri boyut üzerinden

---

[7] Ian Bellany, "Towards a Theory of International Security", **Political Studies**, Vol: XXIX, I: 1, 1981, s. 102.
[8] Terry Terriff, **Security Studiest Today**, Cambridge, Polity Press, 1999, s. 1.
[9] Edward A. Kolodziej, **Security and International Relations**, Cambridge, Cambridge Press, 2005, s. 25.
[10] Sertif Demir, "Avrupa Güvenlik Mimarisinin Tarihsel Gelişimi ve Türkiye'nin Bu Güvenlik Mimarisindeki Yeri", **Güvenlik Stratejileri Dergisi**, No: 9, 2009, s. 10.
[11] Şeref Çetinkaya, "Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", **21. Yüzyılda Sosyal Bilimler Dergisi**, Sayı: 2, 2012, s. 242.
[12] Beril Dedeoğlu, **Uluslararası Güvenlik ve Strateji**, İstanbul, Yeniyüzyıl Yayınları, 2008, s. 26.

değerlendirilmiştir. Güvenlik çalışmalarındaki büyük değişim 1970'li yıllarda yaşanmaya başlamıştır. Bu dönemde özellikle Ford Vakfı tarafından güvenlik sorunları ile ilgili çalışma yapan akademik kuruluşları fonları ile destekleyeceğinin ilan edilmesi ve güvenlik alanında başat rolü oynayacak bilimsel dergi olan *International Security*'nin 1959 yılının Ocak ayında yayın hayatına başlaması bu gelişim sürecinin temelini oluşturduğu söylenebilir.[13]

Güvenlik kavramını genişletme ve güncelleme amaçlı çalışmalar ise, iki kaynaktan beslenmektedir: İlk olarak, klasik bakış açısı ile askeri güce ağırlık veren güvenlik anlayışı ile ilgili problemler giderek artmaya başlamış ve silahlanma yarışının önlenemeyen artışına paralel biçimde güvenlik artışının sağlanamadığı şeklindeki görüşlere bir de artan silahlanma anlayışının ortaya çıkardığı ekonomik külfetin kaldırılamayacak noktalara erişmesi bu tür sorunların daha da görünür olmasına sebep olmuştur. İkinci kaynaktan beslenen çalışmalar ise güvenlik alanının genişletilmesi, farklı alanların da güvenlik içerisinde değerlendirilerek harmanlanması şeklindeki taleplere dayanmaktadır. Birey ya da devlet seviyesinde değerlendirme yapıldığında; günümüz risk ve tehditlerinin karmaşık yapısı karşısında klasik askeri güvenlik yaklaşımının yetersiz kaldığını görmek mümkündür.[14]

Güvenlik kavramı bir hedefe yönelik olmadığı takdirde yeterince anlamlı olmamaktadır. Bir başka deyişle hedef belirlenmemiş ya da doğru hedef seçilememişse güvenlik anlayışından söz etmek bu noktada çok tutarlı görünmemektedir. Ayrıca hedefin basit bir şekilde bir devlet ya da bir kişi olarak belirlenmesi çoğunlukla yetersiz kalmaktadır. Bir kişi ya da bir devletin entegre şekilde diğer benzer unsurlarla hareket edebileceği ihtimali bulunmaktadır[15]. Daha da öteye gidilirse karşımıza kişilerden ya da devletlerden ve bağlı unsurlardan oluşan bir sistem çıkabilir. Dolayısıyla sistemin oluşturduğu yapıya göre bir güvenlik anlayışı ihtiyacı ortaya çıkabilir. Bu sebeple güvenliğin kim için olacağı net bir şekilde ortaya konulmalıdır.

[13] Sait Yılmaz, "Güçsüz Güç", **Güvenlik Stratejileri Dergisi**, No: 5, 2007, s. 70.
[14] Ken Booth, "Güvenlik ve Özgürleştirme", **Avrasya Dosyası Güvenlik Bilimleri Özel**, Çev. Çiğdem ŞAHİN, C: IX, No: 2, 2003, s. 59.
[15] Buzan, **a.g.e**., s. 26.

Güvenlik stabil bir konu değildir, aksine, dinamik bir süreçtir. Hedeflerin farklılaşması, tehdit algılarında yaşanan değişimler doğal olarak güvenlik anlayışını da daha karmaşık bir hale getirmektedir. Güvenlik olgusu ile bu değişim ve gelişmeler arasında bir illiyet bağı olduğunu söyleyebiliriz[16]. Güvenliği hangi boyutta ele alırsak alalım (devlet, toplum ya da birey bazında) kazanımlar arttıkça bunların kaybedilme riski karşısında güvenliğe olan ihtiyaç da artmaktadır. Eğer hiçbir şeye sahip değilseniz kaybetme riskiniz yoktur, buna karşın birçok edinime sahipseniz bunları bir gün kaybetme riskine ve korkusuna da sahipsinizdir.

Güvenliğin sağlanmasında derecenin (seviyenin) ne olacağının belirlenmesi bu alandaki önemli konulardan biri olarak karşımıza çıkmaktadır[17]. Her seviyede geliştirilmesi düşünülen tedbirler birbirinden farklılaşmaktadır. Örneğin bir binanın güvenliği ile bir kişinin güvenliği ya da bir coğrafyanın güvenliği ile bir ülkenin güvenliği farklı perspektiflerde değerlendirilerek ona göre tedbirler alınmasını içermektedir. Bu aşamada hangi seviyede ve ne için güvenlik sorusu güvenliğin tanımlanmasında ön plana çıkmaktadır.

İnsan güvenliği kavramı toplumsal adaletin ve barışın sağlanabilmesi için birey bazında hak, özgürlük ve ihtiyaçların devlet güvencesi ile koruma altına alınmasıyla mümkün olacağı anlayışını ortaya koyan ve insanı merkeze oturtan bir yaklaşım olarak karşımıza çıkmaktadır. İnsani güvenliğin karşısında risk unsuru olarak duran etkenlerden bazıları; terör ve şiddet, doğal afetler, kuraklık, yoksulluk, temel hak ve özgürlüklere karşı yapılan ihlaller, ulaşım, sağlık ve eğitim gibi hizmetlerden yoksun bırakılmaktır[18].

İnsan güvenliği[19] denilince akla gelen risk unsurları her seviyede birbiriyle bağlantılı olmaktadır. Yerel, ulusal ya da küresel temelde karşımıza çıkan tehdit ve riskler genel anlamda birbirleriyle bağlantılıdır. Bu haliyle riskleri en aza indirgemek

[16] Dedeoğlu, **a.g.e**., s. 28.
[17] David A. Baldwin, "The Concept of Security", **Review of International Studies**, No: 23, 1997, s. 14.
[18] Çetinkaya, **a.g.e**., s. 244.
[19] İnsan güvenliği konusu ile ilgili ayrıntılı bilgi için bknz; Gizem Bilgin Aytaç, "Human Security Concepts For NGO's in Post Intervention Societies- A Case Study In Iraq", **Journal of International Social Research,** Vol. X, I: 50, 2017, ss. 167-173.

ve mümkünse ortadan kaldırmak için geliştirilecek çözüm önerilerinin de bu bağlantının dikkate alınarak hazırlanması doğru bir yaklaşım olacaktır. Kişisel seviyede yaşanan işsizlik sorunu bir süre sonra topluma yayıldığında ulusal bir soruna dönüşebilmektedir ya da uluslararası seviyede yaşanan küresel ısınma sorununun ulusal ya da bireysel seviyelerde farklılaşmış olsa da yansımaları da olacaktır. Dolayısıyla insan güvenliği olgusu, oldukça karmaşık görünen birçok sorunun farklı seviyelerle ilişkilerini kurmak suretiyle yeni oluşturulacak perspektifler ışığında değerlendirilebilmesine yardımcı olmaktadır[20].

Toplumsal güvenlik kavramı ise sosyo-kültürel kimlikle birlikte ele alınarak değerlendirilmektedir. Bu noktada devletin güvenliğinin tesis edilmesi ile toplumsal güvenliği sağlamak arasında önemli farklılıklar bulunmaktadır. Devletler siyasi yanları ile ön plana çıkar ve birbirlerinden ayrılabilirken toplumların ayırt edici özellikler arasında gelenekler, kültürler, dilleri ve dinleri sayılabilir[21]. Kopenhag ekolüne göre, geçmişte toplumsal kimlikler din eksenli bir tanımlamaya tabi tutulurken günümüzde bu tanımlama etnik kimlikler üzerinden yapılmaktadır. Dolayısıyla bu olgular ve bu olgulara karşı risk ve tehdit oluşturan unsurlar da güvenlik alanında bir aktör haline gelmektedirler. Kopenhag Okulu tarafından öne sürülen bu görüşe Theiler karşı çıkmıştır. Theiler'e göre toplumsal güvenliği açıklarken Kopenhag Okulu'nun toplumu sanki maddi bir cisim gibi tanımlamakta olduğunu belirtmiş ve bu noktada eksik bir tanımlama yapıldığını iddia etmiştir[22].

Küresel güvenlik denilen kavram ise daha geniş anlamları içinde barındırmaktadır. Küreselleşme doğrultusunda çalışmalarını aralıksız devam ettiren uluslararası yapının güvenliğinin tesis edilmesi ve bunu gerçekleştirmek adına bu yapıya yönelik risk ve tehditlerin bertaraf edilmesi bu kavramın temel odak noktasını oluşturmaktadır. Güvenlik olgusu insanlığın tümüyle direkt ilişkilidir. Karacasulu da

[20] Alpaslan Özerdem, "İnsani Güvenlik", http://wwwm.coventry.ac.uk/researchnet/CPRS/Turkey/conference/Documents/CPRSInsaniGuvenlik.pdf, 06 Aralık 2016.
[21] Karacasulu, **a.g.e**., s. 13.
[22] Tobias Theiler, "Societal Security and Social Psychology", **Review of International Studies**, C: XXIX, No: 2, 2003, s. 251.

güvenlik çalışmalarının kapsamının genişlemesine küreselleşmenin neden olduğunu belirtmeye çalışmıştır[23].

Klasik güvenlik anlayışının daha kapsamlı bir hale gelmesi ve bu anlamda yeni bir bakış açısının kazanılması bu kavramın içeriğinin genişletilmesi sonucunda olmuştur. Klasik güvenlik anlayışında odak noktası devlet ve devletin güvenliği olarak karşımıza çıkmaktadır. Bu konseptteki anlayışa bakıldığında tehdit ve risk alanlarını askeri konular oluşturmakta ve yine tedbir olarak da askeri yöntemler kendini göstermektedir. Bu haliyle geleneksel güvenlik anlayışının askeri güvenliğin sağlanması ile eşdeğer olduğunu söylemek doğru olacaktır[24].

İkinci Dünya Savaşı sona erdikten sonraki süreçte güvenlik askeri terim ve bakış açıları ile ele alınmıştır. Bu dönem askeri perspektifte ele alınan bu konulara "yüksek politika (high politics)" ismi verilmiştir. Büyük savaşın henüz sona ermiş olması askeri konuların birincil seviyede değerli olmasına neden olurken sağlık, göç, iktisat gibi konuların ikinci plana atılmasına da zemin hazırlamıştır. Dolayısıyla ikinci plandaki konular güvenlik sorunu olarak görülmemiş ve "alçak politikanın (low politics)" ilgi alanında kalmaktan kurtulamamışlardır[25].

Güvenliğin bu şekliyle değerlendirildiği dönemde devletlerin güvenliğinin tesis edilmesinde caydırıcı olma esasına dayalı bir perspektif belirlenmiştir. Bu anlayışa göre sistemi yeniden şekillendirme amacını güderek hareket eden bir devlet ve bu devletin uyguladığı politikalar kendini gösterdiğinde karşısında bulunan diğer devletler bir araya gelmek suretiyle "güçler dengesi"ni kurmakta ve karşı bloğu inşa etmek suretiyle dengeleyici bir yapı oluşturulmaktaydı. Caydırıcılık politikasının temelinde diğer devletlerin güvenliğini riske atacak şekilde politika yapan ve uygulayanlar açısından karşılaşacakları maliyetlerin ne kadar büyük olduğunu göstermek bulunmaktadır[26].

---

[23] Z. Nilüfer Karacasulu, "Security and Globalization in the Context of International Terrorism", **Review of International Law and Politics**, C: II, No: 5, 2006, s. 2.
[24] Z. Nilüfer Karacasulu, **Bölgesel Güvenlik Analizi Afganistan**, İstanbul, Beta Yayınları, 2011, s. 10.
[25] Baldwin, **a.g.e**., s. 9.
[26] Tarık Oğuzlu, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", **Güvenlik Stratejileri Dergisi**, No: 6, 2007, s. 13-14.

1990'lı yıllarda yaşanan gelişmeler geleneksel güvenlik anlayışının sorgulanır hale gelmesine neden olmuştur. O döneme kadar güvenlik konusunun yegâne aktörü olarak görülen devlet ve onun güvenliği yine önemi korumakta ancak ilave olarak toplum güvenliği, insan güvenliği, çevresel güvenlik, küresel güvenlik gibi alt düzeyde bile olsa güvenliğin farklı boyutlarda da ele alınmasının önü açılmaya başlamıştır[27]. Uluslararararası ilişkiler teorileri ile güvenlik arasındaki ilişki üzerinden bu süreç daha iyi anlaşılabilecektir.

1.2. Uluslararası İlişkiler Teorilerinin Güvenliğe Bakışı

Uluslararası ilişkiler ile ilgili yapılan çalışmalara bakıldığında; bu çalışmaların çok gerilere gidebildiğini görebiliriz. Birçok siyaset bilimci bu çalışmaların başlangıç noktası olarak Aristo ve Eflatun'u işaret etmektedir. Yine Yunan bilim insanı Thucydides' in ''Pelopenezya Savaşları Tarihi'' isimli çalışması ve Machiavelli'nin ''Prens''i klasik çalışmaların öncüleri olarak ifade edilmektedir. Uluslararası ilişkiler alanında yapılan çalışmalar 1914 yılına kadar genel anlamda diplomasi ve uluslararası hukuk temelinde yapılmıştır.[28] 1919 yılında Galler Aberystwyth Üniversitesi'nde açılan uluslararası ilişkiler bölümü, bu alanın akademik bir disiplin haline gelmesinde bir ilk olmuştur[29].

Uluslararası ilişkiler akademik bir disiplin haline geldikten sonra bu alandaki ilk kuramsal yaklaşım da "idealizm" olarak ortaya çıkmıştır. İdealizm, liberalizmin bir yansıması şeklinde I. Dünya Savaşını takip eden on yıllık süreçte egemen bir yaklaşım olmuştur. Ancak idealizm tam anlamıyla bir uluslararası ilişkiler teorisi olarak ifade edilmemekte bunun yerine uluslararası ilişkilerin nasıl yapılanması gerektiği üzerinde duran bir idealler demeti olarak nitelendirilmiştir[30]. Ancak II. Dünya Savaşı'nın başlaması, idealizm görüşü üzerinde soruların artmasına ve bu görüşün geçerliliğini

[27] Karacasulu, **a.g.e**., s. 13.
[28] Tayyar Arı, **Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İşbirliği**, (7. Baskı), Bursa, MKM Yayıncılık, 2011, s. 16.
[29] John Baylis ve Steve Smith, **The Globalization of World Politics: An Introduction to International Studies**, New York, Oxford University Press, 2005, s. 4.
[30] Sait Yılmaz, **21. Yüzyılda Güvenlik ve İstihbarat**, (2. Baskı), İstanbul, Milenyum Yayınları, 2007, s. 7.

yitirmesine neden olmuştur. Bu noktadan sonra realizm görüşü ön plana çıkmaya başlamıştır[31].

1.2.1. Realizm Teorisi ve Güvenliğe Bakışı

1648 yılında yapılan Vestfalya Anlaşması'ndan itibaren 'devletler', uluslararası sistem içerisindeki en önemli aktör olarak kabul edilmişlerdir. Uluslararası ilişkileri düzenleyen devletler üstü bir otorite olmayışı, devletlere kendi güvenliklerini sağlama konusunda meşruiyet kazandırmıştır[32].

Devleti ana aktör olarak ele alan realizm teorisi [33], Thucydides'den Machiavelli'ye kadar uzanan, devamında ise Thomas Hobbes'un bayrağı devraldığı bir fikir akımı olarak karşımıza çıkmaktadır. Teorinin uluslararası ilişkiler alanında özgün olarak ilk kullanımı ise Hans J. Morgenthau[34] ile başlamıştır. Bundan sonra güç, ulusal çıkarlar, uluslararası politika gibi kavramlar uluslararası yapının açıklanmasında kullanılmaya başlanmıştır[35].

Realist teorinin savunucuları askeri konulara öncelik vermektedir. Bu nedenle uluslararası ilişkileri ve sistemi anlamak için güç kavramını kullanmaktadırlar. Realistler, uluslararası sistemde ortaya çıkacak anlaşmazlıkları güç kullanımıyla çözümlemenin en doğru yol olduğunu söylemektedirler[36]. Realistler, siyasal alan ile ilgili çalışmalarında diğer alanları göz ardı etmişlerdir. Bu nedenle askeri ve siyasi konular ağırlık kazanırken, ekonomi, kültür ve sosyal konular yüzeysel kalmıştır[37].

---

[31] Bülent Uğrasız, "Uluslararası İlişkilerde İki Farklı Yaklaşım: İdealizm ve Realizm", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,** C. V, S. 2, s. 140.
[32] John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, C. V, S: 18, 2008, s. 71.
[33] Yılmaz, **a.g.e**., s. 9.
[34] Hans J. Morgenthau, **Politics Among Nations: The Struggle for Power and Peace**, New York, Alfred A. Knopf-McGraw Hill, 1948. Ayrıca Hans J. Morgenthau, **Uluslararası Politika- Güç ve Barış Mücadelesi**, (Çev. Baskın Oran ve Ünsal Oskay), Türk Siyasi İlimler Derneği Yayınları, 1970.
[35] Faruk Sönmezoğlu, **Uluslararası İlişkiler Sözlüğü**. İstanbul, Der Yayınları, 2000, s. 585.
[36] Torbjorn L. Knutsen, **A History of International Relations Theory: An Introduction.** Manchester, Manchester University Press, 1992, s. 235.
[37] Faruk Sönmezoğlu, **Uluslararası Politika ve Dış Politika Analizi**, İstanbul, Filiz Kitabevi, 1995, s. 97.

Realist görüş, uluslararası ortamı 'anarşik' olarak nitelendirmektedir. Bunun sebebi olarak uluslararası sistem içerisinde devletlerden daha güçlü bir otoritenin bulunmaması gösterilmektedir[38]. Bu nedenle devletlerin bu anarşik yapı içerisinde kendi güvenliklerini sağlamak için ulusal çıkarları doğrultusunda hareket edeceği fikri öne sürülmektedir[39].

Realizmin insan unsurunu ele alış biçimine bakıldığında kötümser bir bakış açısına rastlamak mümkündür. İnsan, çıkarcı, kötü, saldırgan ve günahkâr bir yapıya sahiptir ve ilişkilerinde gücü kullanmayı sevmektedir[40]. Aynı şekilde Shimko da insanın hırslı ve açgözlü olduğu fikrindedir[41]. Thucydides de insana bakış açısı olarak kötümser olması, güç vurgusunda bulunması ve ahlaki değerleri daha az önemsemesi nedeniyle ilk realist düşünür olarak ifade edilmektedir[42]. Hobbes'in ünlü eseri Leviathan'da[43] belirttiği üzere insanlar doğa durumunda kendilerini barış içerisinde yaşatacak bir otoriteden yoksundurlar ve bu nedenle kendi aralarında anlaşmazlıkların ve hatta savaşların çıkması kaçınılmazdır[44].

Realistlerin bu karamsar bakış açıları, devletlerin işbirliği yapabilme yetisinin de olmadığı fikrinin temelini oluşturmaktadır. Realistlere göre, uluslararası güvenlik ancak güçlerin dengelenmesiyle sağlanabilir. Güçlü devletlerin denge kurması gerekli görülmekte ve bu dengeyi sağlayabileyecek hegemon bir devlete ihtiyaç duyulmaktadır. Realistler bu noktada işbirliğini olumsuz etkileyen bir diğer kavramdan, 'relative gains'den söz etmektedir. Yani bir ülkenin kazancının diğerinden fazla olması ile ilgili bir endişeden bahsetmektedirler[45].

---

[38] Alan Collins, **Contemporary Security Studies.** New York, Oxford University Press, 2007, s. 23.
[39] Alec Stone, "What Is a Supranational Constitution? An Essay in International Relations Theory", **The Review of Politics,** C. LVI, S: 3, 1994, s. 449.
[40] Arı, **a.g.e**., s. 160.
[41] Keith L. Shimko, "Realism, Neorealism and American Liberalism", **The Review of Politics,** C.XLIII, S: 127, ss. 5-19.
[42] W. Julian Korab-Karpowicz, "How International Relations Theorists Can Benefit By Reading Thucydides", **The Monist**, C. LXXXIX, S: 2, 2006, s. 233.
[43] Thomas Hobbes, **Leviathan**, (Çev. Semih Lim), 18. bs., İstanbul, Yapı Kredi Yayınları, 2018.
[44] Ahmet Nuri Yurdusev, "Thomas Hobbes and International Relations: From Realism to Rationalism", **Australian Journal Of International Affairs,** C. LX, S: 2, 2006, s. 307.
[45] Nilüfer Z. Karacasulu, **Bölgesel Güvenlik Analizi Afganistan**, İstanbul, Beta Yayınları, 2011, s. 19.

Realizm teorisyenlerinin çalışmalarında temel meselenin ulusal güvenlik üzerinde yoğunlaştığı görülebilir. Yine ulusal güvenliğin sağlanmasında ve daha genel anlamda uluslararası yapıyı düzenlenmesinde başat unsur olarak 'güç' konusuna işaret edilmektedir[46].

1.2.2. Neorealizm Teorisi ve Güvenliğe Bakışı

1970'li yıllarda realizme yönelik eleştirilerin giderek artması neorealizmin doğuşunda önemli rol oynamıştır. Neorealist düşünürlerin en önde gelen temsilcilerinden biri Kenneth N. Waltz'dur. Waltz da uluslararası sistemin devletin davranışlarına sınırlama getirdiğini iddia etmektedir[47]. Güvenlik durumu, uluslararası sistemin bir sonucu olmaktadır. Uluslararası ortamın anarşik oluşu süreklilik arz etmektedir ve bu durum gelecekte de şiddete olan eğilimi beslemeye devam edecektir[48].

Neorealistler ile realistlerin uzlaştıkları noktalar da bulunmaktadır. Ana aktörü devlet olarak gören her iki teori de devletleri üniter yapılar olarak kabullenmişler ve yine devletlerin kendi çıkarları doğrultusunda hareket ettiklerini belirtmişlerdir[49]. Bu çıkar çatışmasından dolayı anarşi ortamı hayat bulmaktadır[50]. Bu ortamda devletler açısından güvenliklerinin sağlanması en önemli konu olarak karşımıza çıkmaktadır. Anarşinin hâkim olduğu uluslararası yapıda devletler arasındaki ilişkileri düzenleyen konu sahip oldukları güçtür. Ancak neorealistlerin güç kavramına bakışı realistlerden farklılaşmaktadır. Realizmde güç amaç olarak değerlendirilirken, neorealistler gücü devletin yaşamını sürdürmesinde ve güvenliğin sağlanmasında bir araç olarak ifade etmektedirler[51].

---

[46] Paul R. Viotti ve Mark V. Kauppi, **International Relations Theory: Realism, Pluralism, Globalism,** New York, Macmillan Publishing, 1993, s. 36.
[47] Kenneth N. Waltz, **Theory of International Politics**, New York, MacGraw-Hill, 1979.
[48] Baylis, **a.g.e**., s. 72.
[49] Arı, **a.g.e**., s. 193.
[50] Cenap Çakmak, "Realist Teori, Uluslararası İlişkilere Etkisi ve Kritiği", **Kamu Hukuku Arşivi Dergisi,** S: 9, 2006, s. 44.
[51] Gülden Ayman, **Neo-realist Bir Perspektiften Soğuk Savaş Sonrası Yunan Dış Politikası Güç Tehdit ve İttifaklar,** Ankara, SAEMK Yayınevi, 2001, s. 2.

Devletler her ne kadar farklı ideolojilere sahip olsa da bazı durumlarda benzer tepkiler verebilmektedirler. Bunun sebebi uluslararası yapı kaynaklıdır. Ulusal yapı ile uluslararası yapı birbirinden farklıdır. Bu nedenle benzer davranışlara kaynak olan kavram 'yapı'dır şeklinde ifade edilebilir[52].

Neorealizm, daha önce de ifade edildiği üzere uluslararası ilişkileri yorumlarken özellikle sistem ve yapı üzerinden değerlendirmeler yapmaktadır. Güvensizlik durumunun en önemli nedeni olarak uluslararası ortamın anarşik olması gösterilmektedir. Yine neorealistler savaş ve çatışma kavramlarını açıklamak için bir başka kavram olan 'güvenlik ikilemi'ni kullanmaktadırlar[53]. Güvenlik ikilemi, iki devletten önce bir tanesinin diğerini tehdit olarak algılayarak silahlanması durumuna karşılık diğer devletin de bu durumu tehdit sayarak aynı şekilde silahlanmasına verilen isimdir. Her iki devletin de bu şekilde silahlanması ekonomik ve askeri açılardan ciddi maliyetler anlamına gelmektedir. Ayrıca silahlanma, tehdidi sona erdirmesi bir yana diğer devletin de silahlanmasıyla tehdidin daha da artar hale gelmesine sebep olmaktadır. Bu ikilem uluslararası ilişkiler literatüründe güvenlik ikilemi (*security dilemma*) olarak ifade edilmektedir[54]. Bu noktada realizm ile neorealizm arasındaki belirgin farklılıklardan bir tanesine daha değinmek uygun olmaktadır. Neorealizmde uluslararası yapı çok fazla öne çıkmakta insan doğası ise es geçilmektedir. Realistler ise bu iki kavramı bir arada değerlendirmişlerdir[55].

1.2.3. Eleştirel Teori ve Güvenliğe Bakışı

Eleştirel teorinin ortaya çıkışı Frankfurt Okulu düşünürleri tarafından gerçekleşmiştir. 1920'li yıllarda kurulan Frankfurt Okulu, sosyal ve entelektüel yaşamın bazı kısımlarını eleştirmiş, toplumda ekonomi ile düşünme yapısı arasındaki bağı incelemeye çalışmıştır. Eleştirel teori bu anlamda Neo-Marksizm ya da Batı

[52] Kenneth N. Waltz ve George H. Quester, **Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi, (**Çev. Ersin Onulduran), Ankara, SBF Yayınları, s. 9-10.
[53] Michael Nicholson, **Formal Theories in International Relations,** Cambridge, Cambridge University Press, 1989, s. 26.
[54] Robert Jervis, "Cooperation under the Security Dilemma", **World Politics**, C. XXX, S: 2, 1978, s. 168.
[55] Steven Forde, "International Realism and The Science of Politics: Thucydides, Machiavelli and Neorealism", **International Studies Quarterly,** C. XXXIX, S: 2, 1995, s. 141-159.

Marksizm'i olarak da isimlendirilmiştir[56]. Okulun önde gelen temsilcileri arasında okulun kurucusu Max Horkheimer'ın dışında, Friedrich Pollock, Theodor Adorno, Herbert Marcuse sayılabilir[57].

Eleştirel teori ile ilgili yapılan tanımlamalarda Frankfurt Okulu'nun kurucularından Max Horkheimer başı çeken kişi olmuştur. 1937 yılında yaptığı tanıma göre eleştirel teori, topluma anlama ve açıklamasının yanında toplumu bütüncül bir yaklaşımla ele alan, eleştiren ve değişmesini sağlayarak özgürleştiren bir teoridir[58]. Frankfurt Okulu tarafından ortaya atılan ideolojik eleştiri, Karl Marx'ın ekonomi-politik alanındaki eleştirisinden türetilmiştir. Doğa üzerinde tesis edilen bilimsel-teknik rasyonalitenin topluma uygulanması sonucunda bilim, Adorno ve Horkheimer'a göre, ideoloji haline gelir[59].

Eleştirel teori düşünürlerinin, realizmin güç ve çıkar kavramlarını odak noktası haline getiren uluslararası sistem değerlendirmesi ve güvenlik konusunun merkeze alınmak suretiyle sistemin yapılandırılması konularında tepkileri olmuştur[60]. Eleştirel teori düşünürlerinin realizm ve neorealizm gibi teorilere yaptıkları eleştirilerin bir diğer odak noktası da bu teorilerin Batılı güçlü devletlerin çıkarlarına hizmet ettiğini düşündükleri mevcut durumu korumaya çalıştıkları şeklinde ortaya çıkmaktadır[61].

Eleştirel teoriye bakıldığında güç kavramının üç boyuta sahip olduğunu görmek mümkündür. Bu boyutlar şu şekildedir[62]:

- 'Üzerinde Güç': Herhangi bir devleti istenilen yöne sevketmek için aleni bir biçimde uygulanan güç,

[56] Ahmet Cevizci, **Paradigma Felsefe Sözlüğü**, İstanbul, Paradigma Yayıncılık, s. 682.
[57] Phil Slater, **Frankfurt Okulu Kökeni ve Önemi**, (Çev. Ahmet Özden), İstanbul, Kabalcı Yayınevi, 1998, s. 9.
[58] Hasret Çomak, **Uluslararası İlişkilere Giriş: Teorik Bakış**, Kocaeli, Umuttepe Yayınları, s. 190.
[59] Tim Dant, **Knowledge, Ideology and Discourse: A Sociological Perspective**, London, Routledge Press, 1991, s. 86.
[60] Vefa Toklu, **Uluslararası İlişkiler**, Ankara, İmaj Yayıncılık, 2004, s. 42.
[61] Yılmaz, **a.g.e.**, s. 14.
[62] **A.e.**, s. 14-15.

- ‘Gizli Güç’: Güçlü devletin gündemi belirlediği, aleniyetten uzak, daha çok el atından uygulanan; daha edilgen, fakat örgütleyici bir yönü olan güç,

- ‘Yapısal Güç’: Devletler arasındaki ilişkileri daha çok belirli özendirme ve sınırlandırma yöntemleri ile koşullandıran güçtür.

1.2.4. Liberalizm ve Güvenliğe Bakışı

Liberalizm teorisi, Batı dünyasını özellikle 18. ve 19. yüzyıllarda etkisi altına almıştır. İngiltere ve ABD’nin öncülüğünde gelişen teori, politik ve iktisadi düşünce tarihinde önemli bir yere sahip olmuştur. Liberal teorisyenlerin odak noktaları eşitlik, gerçekçilik, hürriyet ve mülkiyet kavramları olmuştur. Bu teorisyenlerin öncüsü John Locke’tur. Locke’un fikirlerini devam ettiren ve geliştiren diğer teorisyenler olarak da David Hume, Adam Smith, Montesquieu, Voltaire ve Kant sayılabilir. Liberal teori, 1688 ile 1789 yılları arasındaki aydınlanma dönemi felsefecilerinin düşünce biçimlerinin temelini oluşturmuştur. Aydınlanma yoluyla insanın hürriyetini kazanacağını savunan liberal teorisyenler, siyasi alandaki hürriyet anlayışının ekonomi alanına da yansayacağını ifade etmişlerdir[63].

Realizmde savaş kavramının uluslararası ilişkilerin doğasından kaynaklandığı belirtilmiştir. Ancak liberaller bu noktada itiraz etmektedirler. Uluslararası ilişkilerin dengelenmesi savaş tercihi yerine işbirliği yolu ile sağlanmalıdır. Liberal düşünürlere göre demokrasinin gelişmesi ve özgürlüklerin genişlemesi kişilerin zenginleşmesinde önemli faktörlerdir. Bu şekilde zenginleşen bireyler, ticaret yoluyla birbirlerine bağımlılıklarını arttırmak suretiyle çatışma ve savaş hallerine düşmekten kaçınacaklardır. Bu sayede savaş ve çatışma kaynaklı maliyetlerden uzaklaşan ve refah-barış eksenine oturan devletler arasında işbirliği için zemin de hazırlanmış olacaktır[64].

Realizmde devlet tek aktör olarak ele alınırken, liberalizm, devleti tek aktör olarak kabul etmez, uluslararası organizasyonlar, çok uluslu şirketler, ulus aşan sivil

[63] Arı, **a.g.e**., s. 342.
[64] Çetinkaya, **a.g.e**., s. 253-254.

toplum kuruluşları da devletin yanına aktör olarak entegre edilir. Bu kapsamda devlet, sadece çıkarları peşinde koşan kendi içinde bir bütün veya birleşmiş aktör değil, ona yön veren kendi çıkarları peşindeki bürokratik organizasyonların toplamıdır [65].

Liberalizmin devlete bakışında, devlet ile bireyin birbirine benzer yönleri olduğu fikri öne çıkmaktadır. Buna göre bireylerin doğuştan gelen hakları vardır (özgürlük, yaşam, eşitlik gibi). İşte bireyin bu haklarının korunması için devlet vardır ve devlet de tıpkı bireylerde olduğu gibi yaşama ve bağımsızlık gibi haklara sahiptir[66].

Liberal teorisyenler için güvenlik kavramı, devletin bekasının korunması ve ülke coğrafyasının savunulması için askeri faaliyetlerin organizasyonundan daha fazlasına karşılık gelmektedir. Soğuk Savaş'ın sona ermesini takiben iki kutuplu uluslararası sistem çökmüş ve yerine çok kutuplu bir yapı ortaya çıkmıştır. Bu durumun bir sonucu olarak güvenlik algısında da değişimler yaşanmaya başlamıştır. Güvenlik anlayışı askeri boyutun ötesine geçmiş ve güvenliğin farklı boyutları ortaya çıkmıştır. Bu konu daha sonraki kısımlarda ayrıntılı olarak ele alınacaktır.

1.2.5. Kopenhag Ekolü ve Güvenliğe Bakışı

Barry Buzan ve Ole Waever'in öncülüğünde gelişen Kopenhag Ekolü'nün ortaya çıkışı, 1985 yılında kurulan Kopenhag'ın Çatışma ve Barış Araştırma Enstitüsü'nde (*Conflict and Peace Research Institute*) gerçekleşmiştir. Bu iki teorisyene Jaap de Wilde, Morten Kelstrup, Pierre gibi düşünürler de çalışmalarıyla destek vermişlerdir. Bu bilim insanları özellikle güvenlikleştirme ve normalleştirme fikirlerine üzerine çalışmışlardır[67].

Kopenhag Ekolü, güvenlik ile ilgili çalışmalarda özellikle üç kavram üzerinde durmuştur. Bu kavramlar: Güvenliğin boyutları (*sectors*), bölgesel güvenlik alanları (*regional security complexes*) ve güvenlikleştirme (*securitization*)'dir. Kopenhag düşünürleri, güvenliğin yalnızca askeri boyutunun olmadığını ve toplamda beş

[65] Yılmaz, **a.g.e**., s. 10.
[66] Arı, **a.g.e**., 350-351.
[67] Başar Baysal ve Çağla Lüleci, "Kopenhag Okulu ve Güvenlikleştirme Teorisi", Güvenlik Stratejileri, C. XI, S: 22, 2015, s. 70.

boyutunun bulunduğunu savunmuşlardır. Bu düşünürler, güvenliğin boyutları olarak askeri güvenliğin yanına ekonomik güvenlik, çevresel güvenlik, sosyal güvenlik ve siyasi güvenlik boyutlarını da eklemişlerdir[68].

Kopenhag Ekolü'nün en önde gelen temsilcilerinden Buzan ve Weaver topyekûn bir güvenlik algılamasının doğru olmadığını söylemişlerdir. Bu iki teorisyene göre bölgesel analizler yapılmalıdır. Dünyayı bir bütün olarak ele almaktan kaçınmışlar ve coğrafi bölgeler temelinde çalışılması gerektiğini ifade etmişlerdir. Çünkü her bölge için farklı risk ve tehdit analizleri yapılmalıdır ve alınacak önlemler de buna göre şekillenmelidir[69].

Ekol'ün bakış açısına göre güvenlik bir söz-edimdir. Olaylar söz-edim vasıtası ile bir güvenlik sorunu olarak ifade edilebilmekte ve bu sürece de 'güvenlikleştirme' ismi verilmektedir[70]. Kopenhag düşünürlerinin odaklandığı ve üzerinde çalıştığı en önemli kavram olarak güvenlikleştirme, sıradan bir konunun beka sorunu olarak ifade edilmesi suretiyle bir güvenlik problemine dönüştürülmesidir. Herhangi bir meselenin güvenlik sorunu haline gelebilmesi için bazı şartların oluşması gerekmektedir. Öncelikle politik bir aktör olmalıdır. Bu politik aktörün söylemlerinin o konuyu devletin bekasına bir tehdit olarak yansıtması ve bu şekilde konuyu güvenlikleştirmesi gerekmektedir. Ancak güvenlikleştirme sürecinin tamamlanması için politik aktör tarafından güvenlik sorunu haline gelen konunun hedef kişi ya da kitle tarafından da aynı düzeyde bir tehdit olarak algılanması da gereklidir. Bu anlamda güvenlikleştirme için özneler arası bir süreç denilebilir[71]. Bu noktada tehdit kavramı, sosyal ve politik süreçler içerisinde kurgulanan ve subjektif değerlendirmelerin öne çıktığı bir yapım sürecinin çıktısı olarak karşımıza çıkmaktadır[72].

---

[68] Barry Buzan, Ole Waever ve Jaap de Wilde, **Security: A New Framework for Analysis,** Colorado, Lynne Rienner Publishers Inc, 1998, s. 21-40.
[69] Barry Buzan ve Ole Waever, **Regions and Powers: The Structure of International Security,** Cambridge, Cambridge University Press, 2003.
[70] Ole Waever, "Securitization and Desecuritization", Ronnie D. Lipschutz (ed.), **On Security**, New York, Columbia University Press, 1995, s. 7.
[71] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context", **European Journal of International Relations**, C. XI, S: 2, 2005, s. 178.
[72] Gencer Özcan, "Türkiye'de Siyasal Rejim ve Güvenlikleştirme Sorunsalı", **İktisat, Siyaset, Devlet Üzerine Yazılar**, İstanbul, Bağlam Yayınları, 2006, s. 356.

Uluslararası ilişkiler teorileri üzerinden güvenlik kavramının tarihsel sürecine değindikten sonra bu noktada değişen güvenlik algısı üzerinde durmak uygun olacaktır.

1.2.6. Bölgesel Güvenlik Kavramı ve Ekonomik Anlamda Bölgesel Güvenlik

Soğuk Savaş diye tabir edilen karışıklık sonrası iki kutuplu uluslararası sistemin sona ermesiyle başlayan ve halen devam eden süreçte küreselleşme kavramının yanı sıra, ulus devlet kavramının sınırlarını ve gücünü aşan sorunların da baş göstermesiyle birlikte bölgeselleşme kavramı önemli bir hale gelmiştir. Bu kavram ülkelerin stratejileri ve politikalarının belirlenmesi noktasında etkin bir noktaya ulaşmıştır. Birleşmiş Milletler Şartı'nın öngördüğü esaslardan biri olan kolektif güvenlik anlayışının yanında yeni bir anlayış olarak bölgesel güvenlik anlayışı son yıllarda adından sıkça söz ettirmektedir. Bu bağlamda, Soğuk Savaş sonrası dönemde, bölgesel dinamiklerin sistemsel dinamiklerden daha baskın hale geldiği, bölgesel düzeyde yerel aktörlerin istikrarın sürmesi ya da istikrarsızlıklar üzerinde sistemsel aktörlerden daha etkili olduğu, coğrafi ve jeopolitik unsurun öneminin ön plana çıktığı değerlendirilmektedir. Güvenlik kavramının mekânsal boyuna baktığımız vakit, güvenlik konusundaki politikaların klasik amaçlarının (ulusal bağımsızlığın toprak ve yönetim sistemi olarak korunması) da bölgesel iş birliği ve küresel ölçekli değerlendirmeler ışığında farklılaştığı söylenebilir[73].

Bölgesel güvenlik anlayışı bir kısım uzman tarafından şu şekilde tanımlanmaktadır[74]: Birden fazla ülkenin güvenliğine ilişkin risk ve tehditlerin, birbirleriyle iç içe geçmiş ve birbirinden bağımsız düşünülemeyecek olması nedeniyle aynı kulvar içerisinde değerlendirilmesidir. Söz konusu güvenlik kaygıları ise aynı

[73] Verlag C.H. Beck, **United Nations: Law, Policies and Practice**, Edt. Rüdiger Wolfrum, C: I, Munich, Martinus Nijhoff Publishers, 1995, s.405-406-; Jobst Delbrück, "Collective Security", **Encyclopedia of Public International Law**, Edt. Rudolf Bernhardt, Oxford, Elsevier, 1982, s. 104-107.

[74] Björn Hetne, "Teori ve Pratikte Güvenliğin Bölgeselleşmesi", **Uluslararası İlişkiler Akademik Dergisi**, (Çev. Evren Çelik-Wiltse), C: V, No: 18, Yaz 2008, s. 90-91, (çevrimiçi) http://www.uidergisi.com.tr/wp-content/uploads/2011/06/Teori-ve-Pratikte-Guvenligin-Bolgesellesmesi.pdf, 16 Aralık 2016.

bölge içinde ekonomik, çevresel ve toplumsal gibi farklı sektörlere ilişkin olabilmektedir. Bu çerçevede, birden fazla devlet arasındaki güvenlik önceliklerinin ve dinamiklerinin örtüşmesi, bu durumun da karşılıklı bir bağlayıcılık ve bağımlılık oluşturması gerekmektedir.

Bölgesel güvenlik kavramı, bir devletin güvenliğinin sağlanması bulunduğu bölgedeki diğer devletlerin güvenliğinden bağımsız düşünülemez, doğrudan birbirleriyle ilişkilidir. Tarihe dayalı dostluk ilişkileri ve ortak ihtiyaçlar gibi faktörler bölgesel güvenlik anlayışının ortaya çıkışında ve belirli bir yapıya dönüşmesinde etkili olmaktadır. Bu noktada bir devlet için birden çok bölgesel güvenlik kompleksi içerisinde bulunabileceğini söylemek mümkündür[75].

Ekonomik anlamda bölgesel güvenlik kavramına bakıldığında ise herhangi bir bölgede bulunan birden fazla ülke ile bu ülkelerin politik birimlerinin iktisadi alanda birbirleriyle uyumlu bir şekilde çalışarak bölgedeki iktisadi gelişmelerin tam anlamıyla birbirini tamamlayan bir noktaya ulaşması şeklinde bir tanımlama karşımıza çıkmaktadır. Güvenliğin bölgeselleşmesi ise belli bir coğrafi alanda devletler ve diğer aktörlerin bölgede bir çatışma ortamı ortaya çıkarma potansiyeli taşıyan ulusal veya devletler arası çıkarlarını, dayanışmacı bölgesel dış ilişkilere ve bölge içi barışı sağlamaya dönük bir güvenlik kompleksine dönüştürmesi şeklindeki bir 'önleyici diplomasi' olarak belirtilmektedir[76].

Uluslararası ekonomik sistem günümüzde ulusal güvenlik kavramının temel elementlerini de içine alan bütün bir konu olarak görülmektedir. Günümüzün büyük uyuşmazlıkları uluslararası ekonominin temel yapı ve işleyişine yönelik olarak ortaya çıkmakta, bu durum da uluslararası ekonomik sistemin uluslararası politika ile yakın ilintisini ortaya koymaktadır[77].

[75] Buzan, **a.g.e.**, s. 105-106.
[76] Hettne, **a.g.e.**, s. 91-92.
[77] Buzan, **a.g.e.**, s. 128-129.

1.3. 21. Yüzyılda Güvenlik Algısı ve Ulusal Güvenlik Kavramı

21. yüzyıla dâhil olurken dünya konjonktüründeki değişiklikler yerleşik dengeleri altüst etmiştir. Sınırlar değişmeye başlamış, çift kutuplu dünya düzeni sona ermiş ve hegemonik güce sahip bir ABD ortaya çıkmıştır. Buna ek olarak dünyada yeni güç merkezleri de oluşmuştur.

Güç merkezi olabilmek için yedi genel kriterin sağlanmış olması gerekmektedir:

- **Ekonomi:** Kendi kendine yetebilecek ekonomik refah seviyesine ulaşmak ve bir sonraki seviyeye geçebilecek duruma gelmek.

- **Teknoloji:** Uluslararası alanda yaşanan bilimsel ve teknolojik gelişmeleri yakından takip etmek suretiyle özellikle haberleşme ve iletişim konularında teknik yeterliliklere sahip olmak.

- **Değerli Para:** Küresel çapta tasarruf tercihi olabilen ve dolayısıyla itibarı olan bir paranın sahibi olmak.

- **Askeri:** Askeri alanda özellikle nükleer güce sahip olabilmenin yanında dünya üzerinde deniz aşırı olarak kullanılabilecek nitelikte 10 adet piyade tümenine sahip olmak.

- **Coğrafi:** Enerji kaynaklarına, içilebilir su kaynaklarına yakınlık derecesi göz önüne alınması suretiyle bu noktalara hâkim olabilecek ayrıca ulaşım kanallarını ülke dışında da güvenli hale getirebilecek bir pozisyona sahip olmak.

- **Kültürel:** Küresel çapta sanatsal ve kültürel eserler vasıtasıyla dünyanın dikkatini çekebilen, dinsel boyutta uluslararası alanda çekim merkezi olabilen bir durumda olmak.

- **Diplomasi:** Dış politikada emperyal emelleri tasarlayıp bunları uygulayabilecek bir devlet yapısına sahip olmak[78].

Güç merkezlerinin sınıflandırılmasında değişik ölçütler kullanılabilir. Bunlardan en yaygın kabul gören ölçüt, jeopolitik ölçüttür. Jeopolitik güç merkezleri; içinde bulundukları coğrafya içerisindeki güç kaynaklarını diğer ülkelere oranla daha etkin bir şekilde kendi lehine kullanabilen devletler ya da devletler topluluğu olarak ifade edilebilir [79] . Bu kapsamda jeopolitik güç merkezleri şu şekilde tasnif edilmektedir[80]:

- Küresel güç merkezi: ABD
- Kıtasal güç merkezleri: Çin ve Rusya Federasyonu
- Bölgesel güç merkezleri: Hindistan, Brezilya, İran ve Japonya
- Birleşik güç merkezleri: NATO, Şangay İş Birliği Örgütü
- Sınırlı güç merkezleri: Kanada, Meksika, Türkiye, İsrail, Güney Kore
- Ekonomik güç merkezleri ise: AB, NAFTA ve APEC tir.

Son dönemde oluşan dünya ekonomik güç merkezleri ise üç kutuptan oluşan bir görünüm arz etmektedir. Birinci kutup, bütünleşme süreci içinde olan Avrupa Birliği'dir[81]. İkinci kutup ise Kuzey Amerika Serbest Ticaret Bölgesi'dir (NAFTA). NAFTA, ABD, Kanada ve Meksika'dan oluşmaktadır. Üçüncü kutup da, Asya Pasifik İş Birliği Konseyi'dir (APEC) ve ABD ve Japonya dâhil 17 ülkeyi bir araya getiren bu forum, ileride Pasifik Havzası'nın bir nevi serbest ticaret bölgesini veya ekonomi topluluğunu oluşturma amacı taşımaktadır[82].

---

[78] Nevzat Denk, **21. Yüzyıla Girerken Türkiye'nin Jeopolitik Durumu**, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1998, s. 16.
[79] Ufuk Levent, **21. Yüzyılın Eşiğinde Türkiye**, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1997, s. 2.
[80] Denk, **a.g.e**., s. 24.
[81] Beril Dedeoğlu, **Dünden Bugüne Avrupa Birliği**, İstanbul, Boyut Kitapları, 2003, s. 418.
[82] Sait Yılmaz, **Güç ve Politika**, İstanbul, Alfa Basım Yayım, 2008, s. 65.

21. yüzyılda yaşanan gelişmelerin yanı sıra bilim ve teknoloji alanındaki ilerlemeler, güvenlik olgusunun yeni boyutlar kazanmasına yol açmıştır. Bunlara ek olarak küreselleşme sürecinden kaynaklı bazı zorunluluklar da göz önüne alındığında ortaya askeri güvenlikten çok daha karmaşık bir güvenlik olgusu karşımıza çıkmaktadır. Ortaya çıkan bu yeni ortamda, küresel sisteme ve bu sistemin işleyişine engel olacak her türlü suç, göç dalgaları, siber saldırılar yoluyla işlenen terör faaliyetleri gibi yeni tehdit türleri güvenlik alanında kendini göstermeye başlamıştır[83]. Manisalı'dan hareketle küreselleşmenin gün yüzüne çıkardığı en önemli sorunlar arasında etnik ve mezhepsel tabanlı çatışmaların yaşanmasına zemin hazırlaması ve ulus devlet yapısında çatlaklar meydana getirmesi sayılabilir[84]. Küreselleşme olgusunun başka bir özelliği de kavramın kendi değerlerini, bakış açılarını ve kurumsal yapılarını inşa etmesi savından kaynaklıdır. Diğer bir ifadeyle küreselleşme süreci sürdüğü esnada diğer yandan bu sürecin meydana getirdiği yeni bir devlet anlayışı da oluşmaya başlamaktadır. Artık devletlerin kendilerini dünyadan izole etmek suretiyle strateji ve politika üretmeleri neredeyse imkânsız hale gelmiştir. Bu noktada karşımıza ulus devletin bütünlüğünü riske sokan ve devletlerin karar verme süreçlerine doğrudan ya da dolaylı olarak etki edebilen üç aktörün varlığından bahsedilmektedir. Bu aktörler; uluslararası örgütler, sivil toplum kuruluşları ve çok uluslu şirketler olarak gösterilmektedir. Bu üç yeni aktörün küreselleşme sürecinin bir sonucu olarak ortaya çıktıkları fikrinin yanında yine küreselleşmenin inşa ettiği yeni düzenin şekillenmesinde de etkili oldukları tezi de ön plana çıkmaktadır[85].

Soğuk Savaş'ın sona ermesi ile artık dünyanın daha güvende bir yer olduğu üzerinde durulmuş ve bu nedenle güvenlik üzerine çalışmalar gerçekten ihmal edilmiş, ancak kısa sürede bu uygulamanın doğru olmadığı anlaşılmıştır. Bu dönemdeki gelişmeler dizisi, güvenliğin sadece askeri konularla alakalı olmadığını farklı alanlarda da güvenliğin söz konusu olduğunu ispatlamıştır. Güvenlik kavramı, sosyal,

[83] Ahmet Küçükşahin ve Tamer Akkan, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", **Güvenlik Stratejileri Dergisi**, No: 5, 2007, s. 43.
[84] Erol Manisalı, **Türkiye ve Küreselleşme**, İstanbul, Derin Yayınları, 2003, s. 41.
[85] Kemal Cebeci, "Küreselleşme Bağlamında Ulus-Devletin Egemenlik Gücünün Dönüşümü", **Sayıştay Dergisi**, No: 71, 2008, s. 23.

ekonomik, siyasi ve çevresel boyutlarının da eklenmesiyle yeni bir anlama kavuşmuştur[86]:

- Askeri güvenlik kavramı; bir ülkenin iç ve dış tehditlere karşı savunma ve karşılık verebilme gücü ve yeteneği, diğer ülkeleri askeri olarak değerlendirebilme ve analiz edebilme gücü,

- Siyasî güvenlik kavramı; ülke içerisinde var olan hükümet sistemi, bu sistemin alt sistemleri ile bunun temelini oluşturan fikri zeminin güvenliği,

- Ekonomik güvenlik kavramı; gerek ülke seviyesinde gerekse de birey bazında refah seviyesinin arttırılması, ülkenin kalkınması ve bunlara zemin hazırlayacak kaynak ve finansın elde edilmesi ve korunması,

- Sosyal güvenlik kavramı; kültürel, dini, lisani yaşamların ve süreçlerin, ulusal kimliğin, gelenek ve göreneklerin devam ettirilebilir noktada korunabilmesi,

- Çevresel güvenlik kavramı; ulusal ve uluslararası seviyelerde çevrenin ve yerkürenin korunması ile ilgilidir[87].

Sovyetlerin yıkılması, güvenlik çalışmalarını yakından etkilemiş ve bu etkinin bir sonucu olarak yeni (kapsayıcı) bir güvenlik anlayışı ortaya çıkmıştır. Yeni (kapsayıcı) güvenlik kavramı, Soğuk Savaş döneminin güvenlik algılamalarını sorgulamaya başlamış ve caydırıcılık esası odaklı güvenlik politikalarının yetersizliğini ortaya koymuştur. Aşağıdaki yer alan tabloda klasik güvenlik ile yeni (kapsayıcı) güvenlik algılamaları karşılaştırılmalı bir analize tabii tutulmaktadır[88]:

[86] Küçükşahin ve Akkan, **a.g.e**., s. 45.
[87] Buzan, **a.g.e**., s. 19-20.
[88] Karacasulu, **a.g.e**., s. 17.

Tablo 1: Klasik Güvenlik-Yeni (Kapsayıcı) Güvenlik Karşılaştırılması

	KLASİK GÜVENLİK	YENİ (KAPSAYICI) GÜVENLİK
Tehdit Kaynağı	Düşman Devletler	Devlet ve Devlet Dışı Tehditler (Yerel veya Sınır Ötesi)
Tehdidin Niteliği	Askeri	Askeri ve Askeri Olmayan (Ekonomik, Siyasi, Çevresel, Uyuşturucu Ticareti, Göç, Kitle İmha Silahları, Terör gibi…)
Kime Yönelik	Devlete	Devlete/Bireye/Topluma/Tüm İnsanlara
Çözüm	Askeri	Askeri ve Askeri Olmayan (Demokratikleşme, Küresel Serbest Pazar gibi…)

Kaynak: Nilüfer Karacasulu, **Bölgesel Güvenlik Analizi Afganistan**, İstanbul, Beta Yayınları, 2011, s.17.

Uluslararası politikanın temelini oluşturan aktörler arasında, uluslararası ortamı etkileyen, bağımsız ve otonom olarak davranabilen, bunun yanı sıra egemenlik gücüne sahip olmayan ve devletin yapmış olduğu hukuksal tanım içinde de yer almayan birimler mevcuttur[89]. Bu noktadan hareketle BM, AB gibi uluslararası örgütlerin dışında Dünya Bankası, IMF, Katolik Kilisesi gibi egemenliği ve ülkesi olmayan aktörler de uluslararası politikanın önemli bir parçası olarak yer kaplamaktadır[90].

1.3.1. Ulusal Güvenlik

Ulusal güvenlik kavramı kısaca bir ülkenin ulusal düzeydeki çıkarlarının içeriden ya da dışarıdan gelebilecek saldırılar karşısında korunması olarak tanımlanabilir. Bu noktada ulusal güvenlik anlayışı içerisinde ulusal çıkarlar, risk ve tehditler ile bunlara karşı geliştirilecek önlemler yer almaktadır[91]. Bir başka tanımda ise bir ülkenin anayasal düzenine, ulusal bağımsızlığına yönelik siyasi, ekonomik,

[89] Arı, **a.g.e**., s. 41.
[90] Yılmaz, **a.g.e.**,2007, s. 357.
[91] **A.e**., s. 214.

kültürel ve diğer alanlarda gerçekleşebilecek saldırılara karşı savunulması ve önlem alınmasıdır[92].

Gerek devlet seviyesinde gerek birey boyutunda değer kavramı yaşam süreleri boyunca oldukça etkili olmaktadır. Devlet bazında değerler ile birey seviyesindeki değerler farklılaşıyor olsa da (örn; güvenlik, ekonomik refah gibi) temelde ortak noktaları her iki seviye için geçerli olan değerlerin korunup kollanması faaliyetidir. Klasik anlamda ulusal güvenlik kavramı, korunup kollanması gereken değerler olarak toprak bütünlüğünü ve bağımsızlık anlayışını içerse de bazı durumlarda farklı değerleri de içermektedir.

Ulusal güvenlik anlayışında bir bütünlük söz konusu olmaktadır. Öyle ki ülke sınırları içerisinde yaşayan vatandaşlara yönelik olarak iç güvenlik anlayışını, ülkeye sınırları dışından yapılabilecek aktif ve pasif saldırılara karşı dış güvenlik anlayışını kapsadığı ifade edilmektedir. İç ve dış güvenlik bir bütün olarak değerlendirilmekte, birbirinden bağımsız düşünülememektedir. İç ve dış güvenliğin ayrımı, güvenliği tehdit eden unsurların kaynağını gösterme noktasında olmaktadır.

Ulusal güvenlik sistemi, güvenlik ortamı ile ilgili her noktanın değerlendirilmesinden güçlü-zayıf yönlerin, fırsat ve tehditlerin saptanmasına, ihtiyaç duyulan istihbari bilgilerin elde edilerek analizinin yapılmasından durumun değerlendirilmesine, amaca ilişkin strateji ve politikaların optimum seviyede belirlenmesinden kaos ve kriz şartlarında uygun politikaların uygulanmasına kadar çok çeşitli fonksiyonları sağlayacak süreç ve unsurları bünyesine entegre etmiş olmalıdır[93]. Ulusal güvenliğin sağlanması için belirlenen politikalar üç temel noktaya işaret etmektedir. Bunlar; ulusal düzeyde güvenliğin tesis edilmesi, ulusal hedeflerin gerçekleştirilmesi ve bu iki noktaya ulaşılması için gerekli hareket ve davranış biçimlerinin belirlenmesidir[94].

---

[92] Harp Akademileri Komutanlığı, **Geçmişte ve 21. Yüzyılda Savaşlar: Stratejiler ve Stratejiler**, İstanbul, Harp Akademileri Basımevi, 2002, s. 25.
[93] Yılmaz, **a.g.e.**, 2008, s. 98-99.
[94] Harp Akademileri Komutanlığı, **a.g.e.**, s. 46.

Ulusal güvenlik kavramı, ülkelerin siyasi yapılanmaları içerisinde öncelikli öneme sahiptir. Ülkelerin takip ettiği güvenlik politikalarının nihai hedefi de, algıladığı tehdit ve baskılar karşısında bağımsızlığını ve çıkarlarını korumak ve kollamaktır. Bu ise öncelikle stratejik seviyede bilme ve değerlendirme ihtiyacını karşılayacak ve örtülü yöntemlerden politik vasıta olarak istifade edecek ve nihayet koruyucu güvenlik sağlayacak istihbarat yapılanmalarını gerekli kılmaktadır[95].

1.3.2. Ulusal Çıkar ve Ulusal Strateji Kavramları

Ulusal çıkar (*national interest*) kavramı üretilen tüm dış politika kararlarının temelini oluşturan itici güçtür. Dolayısıyla alınan kararların hiçbiri ulusal çıkarlara aykırı olamayacaktır. Bununla birlikte ulusal çıkar kavramının nesnel bir tanımının yapılmasının çok zor olduğu görüşü kabul görmektedir. Uluslararası ilişkiler alanında çalışma yapan araştırmacıların önemli bir bölümü kavramın yeterince belirgin olmadığını belirterek bu kavramı kullanmamayı tercih etmişlerdir. Ulusal çıkarın tanımı yapabilmek, bu anlamda hangi unsurun ya da faaliyetin ne seviyede ulusal çıkara uygun olup olmayacağını belirleyebilecek kıstasları ortaya koymak oldukça zordur[96].

Ulusal çıkar, güç ve güvenlik kavramları ile birlikte realist teorinin uluslararası ilişkileri açıklamada kullandığı en temel kavramdır. Realist teorisyenlerin uluslararası ilişkilerde ana aktör olarak ele aldıkları devletin, önceliklerini ve hareket tarzlarını anlama noktasında ulusal çıkar kavramı önemlidir. Bunun en önemli sebebi, ulusal çıkarların, devletin dış poltikasını belirleyen en temel itici güç olmasıdır[97]. Bu anlamda devletler arasındaki ilişkilerde, sürekli dostluklar olmayacağı, sürekli çıkarlar olacağı ifade edilmektedir[98]. Devletler uluslararası arenada hareket tarzlarını belirlerken ulusal çıkarlarını gözetmek durumundadırlar. Ancak çıkarların zamana göre değişim

[95] Yılmaz, **a.g.e.**, 2007, s. 214.
[96] Erol Mütercimler, **Geleceği Yönetmek: Yüksek Stratejiden Etki Odaklı Harekâta**, İstanbul, Alfa Yayınları, 2006, s. 380.
[97] Mitat Çelikpala,"Geçmişten Günümüze Vazgeçilemeyen Kavram: Ulusal Çıkar", **H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi,** C. XXIII, S: 1, 2005, s. 441.
[98] İlhan Uzgel, **Ulusal Çıkar ve Dış Politika: Türk Dış Politikasının Belirlenmesinde Ulusal Çıkarın Rolü,** Ankara, İmge Yayınları, 2004, s. 64-65.

gösterebilen dinamik bir yapıya sahip olması devletler açısından bu durumu zorlaştırmaktadır.

Devletler ulusal çıkarlarını korumak, ulusal hedeflerine ulaşmak ve uluslararası ilişkilerde avantaj sağlamak amacıyla çeşitli yol ve yöntemler kullanmaktadırlar. Bu noktada öne çıkan bazı yöntemler şunlardır[99]:

- **Zorlayıcı Diplomasi ve İstihbarat:** Zorlayıcı diplomasi uygulamasında hedef alınan ülkenin hükümranlık haklarına yönelik demokrasi, insan hakları vb. kavramlar üzerinden temellendirilmiş müdahaleler söz konusu olmaktadır. Zorlayıcı diplomaside ikna kabiliyeti yüksek seviyededir ve bu amaçla karşı tarafın algıları üzerinde soru işaretleri yaratılır. Buna ilave olarak da propaganda, manipülasyon gibi çeşitli istihbarat teknikleri de kullanılır. Bu anlamda propagandanın düşmanın moral ve motivasyonunu çökertmekte en önemli vasıtalardan biri olduğunu belirtmek gerekir[100].

- **Güvenlik Ortamının Düzenlenmesi:** Uluslararası güvenliğin sağlanması açısından yapılacak faaliyetleri sıralamak istediğimizde; demokrasinin, evrensel insan haklarının korunduğu ve saygı gösterildiği, zararlı ve yıkıcı faaliyetlerin önlenmeye çalışıldığı ve özellikle kitle imha silahlarının yaygınlaşmasının önlenmesi için çalışmaların yapıldığı bir sistem karşımıza çıkmaktadır.

- **Kontrol Etme:** Kontrol etme sürecinde elde edilmesi planlanan ana nokta, hedef ülkenin hâlihazırda var olan düşünme biçimini ve sistemini çeşitli yöntemler (beyin yıkama, ortak görüş, örgütleme vb.) vasıtasıyla değiştirmek ve istenilen bakış açılarının oluşmasını sağlamaktır.

- **Açık Toplum Yöntemi:** Bu yöntemde hedef olarak belirlenen ülke içerisindeki vakıflar, meslek birlikleri, sendikalar, dernekler gibi sivil toplum örgütleri üzerine çalışmalar yapılmaktadır. Bu kuruluşlar vasıtası ile o ülkenin

[99] Yılmaz, **a.g.e.**, 2007, s. 301-321.
[100] Nevzat Tarhan, **Psikolojik Savaş: Gri Propaganda**, 8.bs, İstanbul, Timaş Yayınları, 2006.

ulus devlet yapısını geçirgen hale getirmek suretiyle olumsuz anlamda etkilemek ve toplum içerisinde kargaşa yaratmak temel amaçlardır.

- **Bilgi Çarpıtma (Dezenformasyon):** Dezenformasyon sürecinin iki önemli ayağı bulunmaktadır. İlki, doğru ya da yanlış olduğu net olarak bilinmeyen ya da bilinse dahi çarpıtılan bir bilginin varlığı ikincisi ise bu bilginin kasıtlı bir şekilde ortalığa sürülmesidir. Bu yöntemde amaç, insanların doğru bildikleri ve inandıkları konular hakkında şüpheler oluşturarak inançlarını değiştirmek ve arzu edilen yönde inançlar aşılamaktır. İstihbarat kurumları tarafından sıklıkla bu yöntem kullanılmaktadır.

- **İktisadi Yöntemler:** Hedef ülke içerisindeki ekonomik merkezleri etkilemek suretiyle karar alma noktasındaki yöneticileri istenilen yöne çekmek temel amaçtır. Bu amaca ulaşmak için finans ve sermaye piyasaları kullanılmakta bu sayede ülke içinde ekonomik istikrarın bozulması için çalışmalar yapılmaktadır. Dünya Bankası, Uluslararası Para Fonu, uluslararası kredi derecelendirme kuruluşları bu yöntemde aktif olarak rol alan araçlar arasında sayılabilmektedir[101].

- **Askeri Yöntemler:** Hedef ülkenin silahlı kuvvetlerini yıpratmak ve bu haliyle etki altına almak ana amaçtır. Bu yöntemde yıpratma harekâtı doğrudan yapılabileceği gibi düşük yoğunluklu stratejiler uygulanarak da faaliyetler yürütülmektedir.

- **Terör Faaliyetleri:** Terörist faaliyetlerin temel amacı; toplum içerisinde korku duygusunu yayarak insanların kendini güvende hissetmelerini engellemek ve bu sayede oluşan karmaşa ortamında ülkedeki karar alıcıların istenen yönde hareket etmesini sağlamaktır. Bu faaliyetlerin planlanması, hazırlanması, finans desteği ve uygulamaya konulması genellikle dış destek ile iç unsurlar tarafından yapılmaktadır[102].

---

[101] Mustafa Çınkı, **Rant Lordları**, Ankara, Karlar Yayınevi, 2004, s. 231-248.
[102] Gürol Korkmaz, **Terör ve Medya İlişkileri**, Ankara, Emniyet Genel Müdürlüğü Yayınları, No: 1999-1, 1999, s. 13.

Ulusal strateji; kısa bir ifadeyle, ulusal çıkarları referans noktası olarak kabul ederek belirlenmiş hedeflere ulaşmak için yapılan planları, planları hayata geçirirken atılacak adımları kapsayan bir kavram olarak karşımıza çıkmaktadır.

Güvenlik stratejilerinin belirlenmesi süreci dinamik bir yapıya sahiptir. Güncel risk ve tehdit analizleri yapılarak güvenlik stratejileri güncellenmektedir. Güvenlik stratejilerinde ortak unsurlar ön plana çıkmaktadır. Bunları şu şekilde sıralayabiliriz[103]:

- Caydırıcı yöntemlerin ortaya konması,
- Güvenlik ortamının yapılandırılması,
- Kriz dönemlerinin iyi yönetilmesi ve savaş harici harekâtların planlanması,
- Güç kullanımına ilişkin sınırların belirlenmesi,
- Son noktada yaşanabilecek (konvansiyonel/nükleer) savaşların planlanmasıdır.

Ulusal (milli) strateji, ulusal çıkarlar temelinde belirlenen hedeflere ulaşmak amacı ile gerek savaş gerek barış dönemlerinde toplumsal bütünleşmeyi gerçekleştirmektir. Ulusal ve uluslararası düzeyde var olan sorunları ortadan kaldırmak adına iktisadi, politik, askeri, bilimsel ve teknolojik, kültürel ve sosyo-psikolojik alanlarda geliştirilen stratejiler ulusal strateji kapsamında değerlendirilmektedir. Bu alanlarda yaşanan gelişmeler bazen zaman içerisinde bazen de aniden ulusal güvenliği etkileyebilmektedir. Ulusal güvenliği oluşturan bu stratejiler, ulusal güvenlikle özdeştir de diyebilmekteyiz.

Güvenlik kavramının zaman içerisinde geçirdiği değişim ve bu konuya ilişkin kavramların açıklanmasını takiben, araştırmaya temel teşkil eden bilişim suçları ile mücadele edilmesi noktasında karşımıza çıkan ve güvenliğin bir başka boyutu olan siber alanda güvenlik konusuna giriş yapmak uygun olacaktır.

[103] Reşat Turgut, **Küreselleşmenin Askeri Boyutları ve Güvenlik Stratejilerine Etkileri**, Ankara, Genel Kurmay Askeri Tarih ve Stratejik Etüt Başkanlığı Yayınları, 2003, s. 41.

1.3.3. Siber Alanda Güvenlik

Siber güvenliğin ne olduğuna geçmeden önce siber kelimesinin neyi ifade ettiğini belirtmekte fayda görünmektedir. Siber, her ne kadar 'elektronik ortam'ı ifade etse de içerisinde çok sayıda öğe barındırmaktadır. Bu öğelerin yer aldığı, işleme konulduğu ve geliştirildiği ortamdaki veriler de; bilgisayar, algoritma, sistem, yazılım gibi unsurlardan oluşmaktadır[104].

Siber alanın en önemli unsurlarından bir tanesi de internettir. Yine elektronik ortamda birbirlerine bağlı telsizler, cep telefonları, bilgisayarlar, enerji nakil hatları, drone, elektromanyetik sistemler, uydu ve robot sistemleri de siber alanı oluşturan unsurlardandır[105].

Siber alanda güvenliğin sağlanabilmesi konusunundan önce siber suç ve siber terör kavramlarından bahsetmek gereklidir. Siber suçlar, dar anlamıyla, bilgisayar ve veri işleme sistemlerine yönelik eylemler olarak tanımlanırken, geniş anlamıyla siber suçlar ise bilgisayar sistemleri ve ağlar yardımıyla bu sistem ve ağlar içerisinde ya da farklı ağlar ve sistemlere yönelik gerçekleştirilen kanunsuz eylemlerdir[106]. Bir başka tanıma göre ise siber suç, bilgisayar ve/veya bilgisayar ağlarının siber alanda kanun dışı bir eylem amacıyla kullanılmasıdır[107]. Siber terör kavramı ise, bilgiye, bilgisayar yazılımlarına ve direkt şekilde savaş içerisinde olmayan hedeflerin ellerinde bulunan verilerine karşı siyasi nedenlerden ötürü planlı olarak yapılan saldırı biçimidir[108]. Diğer bir ifadeyle siber terör, suç örgütlerince terör ya da politik bir takım amaçlar nedeniyle devletin üst seviyedeki kişi ve kurumlarına yönelik yapılan saldırılardır[109].

---

[104] Şeref Sağıroğlu, **Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık**, (ed. Şeref Sağıroğlu ve Mustafa Alkan), Ankara, BGD Siber Güvenlik ve Savunma Kitap Serisi, 2018, s. 24.
[105] Hasan Çifçi, **Her Yönüyle Siber Savaş**, İstanbul, TÜBİTAK Popüler Bilim Kitapları, 2013, s. 5.
[106] Yılmaz Yazıcıoğlu, "Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", **Dokuz Eylül Üniversitesi Uluslararası İnternet Sempozyumu**, İzmir, 2002, s. 460.
[107] Oğuz Turhan, "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)", **Planlama Uzmanlığı Tezi**, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, Nisan 2006, s. 31.
[108] İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye'deki Durum,** Ankara, Adalet Yayınevi, 2008, s. 40.
[109] H. Çolak, "Siber Terör, Yargılama Usulü ve Önleyici Tedbirler", **Kazancı Hakemli Hukuk Dergisi,** 2011, S: 79-80, s. 81.

Siber dünya teröristleri için internet ortamı oldukça elverişlidir. İnternette denetim mekanizmasının zayıf oluşu, internet kullanımının ucuzluğu, kısıtlamanın olmayışı gibi faktörler siber teröristler için çekici unsur olmaktadır [110]. Siber teröristlerin temel amacı, sanal ağlar ve iletişim hatları üzerinden yaptıkları yasa dışı eylemler vasıtası ile siyasi, sosyal veya ideolojik konularda karşı tarafı kabule zorlamak, korku ve panik ortamı yaratmaktır[111].

Siber dünya ile ilgili bir diğer önemli kavram da siber savaştır. Siber alanda, saldırı ya da savunma amacıyla bilgi ve iletişim teknolojilerine zarar verilmesini ya da ortadan kaldırımasını kapsayan faaliyetlerin tamamı siber savaş olarak nitelenebilir[112].

Tablo-2: Konvansiyonel Savaş ile Siber Savaş Arasındaki Farklar

DEĞİŞKEN	KONVANSİYONEL SAVAŞ	SİBER SAVAŞ

[110] Haydar Çakmak ve Cenker Korhan Demir, "Siber Dünyadaki Tehdit ve Kavramlar", (ed. Haydar Çakmak ve Taner Altunok, **Suç, Terör ve Savaş Üçgeninde Siber Dünya,** 1. Baskı, Ankara, Barış Platin Kitabevi, 2009, s. 38.
[111] Murat Güneştaş ve Diğerleri,"Siber Terörizm: Motivasyon ve Yöntem", (ed. Fatih Tombul ve diğerleri), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele,** Ankara, Global Politika ve Strateji, s. 88-89.
[112] Çakmak ve Demir, **a.g.e**., s. 48.

SALDIRI KAYNAĞININ TESPİT EDİLMESİ	Kolaydır	Zordur ve Hatta Bazen İmkânsızdır
SALDIRININ HIZI	En Hızlı Muharebe Silahı Hızındadır	İnternet Hızındadır
SALDIRININ ETKİSİ	Coğrafi Sınırlar İçerisinde	Siber Uzay İçerisinde
SAVAŞÇILARI	İki veya Daha Fazla Ülke Orduları Savaşmaktadır	Tek Bir Kişi, Bir Grup, Bir Örgüt veya Devletler Savaşmaktadır
MALİYETİ	Genellikle Çok Pahalıdır	Ucuzdur
KULLANILAN SİLAHLAR	Tank, Tüfek, Bomba, Füze vs. Kullanılır	Bilgisayarlar, Bilgi Sistemleri vb. Kullanılır.
İLERİ TEKNOLOJİ İHTİYACI	Vardır	Yoktur. Mevcut Teknoloji Genellikle Yeterlidir
SALDIRININ BELİRTİLERİ	Tespit Edilebilir	Tespit Edilemeyebilir
HASAR TESPİTİ	Kolaydır	Zordur

Kaynak: Atalay Keleştemur, **Siber İstihbarat**, 1. Baskı, İstanbul, Yazın Basın Yayınevi, 2015, s. 164-165.

Tablo'dan da anlaşılacağı üzere siber savaş ile konvansiyonel savaş arasında çok ciddi farklar bulunmaktadır. Siber savaşta saldırının kaynağını belirlemek oldukça zordur ve bu nedenle saldıraya yönelik cevap verme süresi de uzamakta dolayısıyla

alınacak hasar da artabilmektedir. Yine siber saldırıların maliyetinin çok düşük olmasına rağmen oluşturabileceği hasarın büyük olabilme ihtimali nedeniyle daha fazla tercih edilebilir[113].

Siber terörizm ve siber savaş ile gerçekleşen saldırılara karşı koyma faaliyetlerini önleme çalışmalarına –basit anlamıyla- siber güvenlik denilmektedir. Birleşmiş Milletler'e bağlı Uluslararası Telekomünikasyon Birliği (ITU) ise siber güvenliği şu şekilde tanımlamaktadır[114]: "Siber dünyada organizasyon ve kullanıcıların bekalarını devam ettirmek için kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünüdür". Bir başka tanıma göre siber güvenlik, iletim sistemleri ve hatlarına yönelik tasarlanan ve onları çalışamaz hale getirmeyi amaçlayan her türlü tehdit ve saldırıya karşı bu sistemleri korumaktır[115].

2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'nde de siber güvenlik konusuna ayrıntılı şekilde yer verilmiş ve siber güvenliğin tanımı şu şekilde yapılmıştır: Siber güvenlik kavramı, siber uzayda bulunan bilgi ve iletişim sistemlerinin siber tehdit ve siber saldırılardan korunması, yine bu ortamda bulunan bilginin gizlilik, bütünlük ve erişilebilirliğinin sağlıklı bir şekilde sağlanması sürecidir. Ayrıca saldırıya maruz kalındığı takdirde gerekli cevapların verilmesi ve sistemlerin önceki hallerine geri döndürülmesi süreci de siber güvenlik kapsamındadır[116].

Siber alanda güvenliğin sağlanabilmesi bilginin gizliliğinin (*confidentiality*), bütünlüğünün (*intergrity*) ve erişilebilirliğinin (*availability*) sağlanması ile mümkün olmaktadır. Bilginin gizliliği, bilgiye erişim yetkisi olmayan kişilerin o bilgiye ulaşamamalarını ifade etmeketedir. Bu erişim, yazılı bir bilginin okunması ya da bilişim sistemlerinde saklanan bilginin sadece yetkili kişilerce görüntülenebilmesi gibi

---

[113] Atalay Keleştemur, **Siber İstihbarat**, 1. Baskı, İstanbul, Yazın Basın Yayınevi, 2015, s. 163.
[114] ITU, "Cybersecurity for All: ITU's Work for a Safer World", 2008, (çevrimiçi) https://www.itu.int/pub/S-GEN-CYBER-2008, Erişim: 15 Ekim 2018.
[115] Sedat Akleylek ve Zeliha Yüce Tok, "Siber Güvenlikte Kriptoloji", **Siber Güvenlik Çalıştayı Raporu**, Ankara, 2011.
[116] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **2016-2019 Ulusal Siber Güvenlik Stratejisi**, s. 8. (çevrimiçi) https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Erişim: 19 Ekim 2018.

erişimlerdir. Bu noktada hassas olarak nitelenen bilgilerin varlığından bile yalnızca ilgili kişilerin haberdar olması gerekmektedi. Bilginin bütünlüğü kavramından ise anlaşılan; bilgi üzerinde oynama yapılmamış, değiştirilmemiş, kısmen ya da tamamen silinmemiş olmasıdır. Erişilebilirlik ise, saklanan bilginin ihtiyaç halinde yetkili kişiler tarafından erişilebilir olmasıdır[117].

Siber güvenlik; siber alandaki güvensizlik ortamına ve bu alandaki güvenlik risklerine karşı önlem almak ve güven ortamını devam ettirebilmek amacıyla kendine özgü bir takım araçlara sahiptir. Bu araçlar siber saldırlarıların türlerine göre zaman içerisinde gelişmekte ve güncellenmektedir[118]. Siber saldırı yöntemleri ve bunlara karşı kullanılan araçlara ileriki bölümlerde ayrıntılı olarak yer verilecektir.

Siber güvenlik konusu, bir diğer ifade ile siber alandaki varlıkların, bilgilerin ve diğer sistemlerin savunulması oldukça geniş kapsamlı ve önemlidir. Siber güvenliğin önemini aşağıdaki maddelerde özetlemek mümkündür[119]:

- Bir ülkenin siber alandaki bilgi ve varlıkları, o ülke için dijital topraklar anlamına gelmektedir ki ülkeler bu dijital topraklarını her türlü saldırıya karşı korumak zorundadır.

- Bilişim sistemlerinin dünyada kullanımının artışına paralel olarak Türkiye'de de bilişim teknolojilerini kullanan kişilerin sayıları giderek artmaktadır. Bilişim teknolojilerini kullananlar, bilişim güvenliği ile ilgili içeriği bilmek ve uygulamak durumundadırlar. Kişisel ya da kurumsal seviyedeki kullanıcılar, bilişim güvenliği konusunda dikkatli olmadıkları takdirde, kişisel ya da kurumsal imajların zedelenmesi, kişilere ya da kurumlara olan güvenin sarsılması, iş gücü ve zaman kaybı oluşması,

[117] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies,** C. 1, No: 1, 2017, s. 25.
[118] Vahit Güntay, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi**, S: 27, s. 81.
[119] Sağıroğlu, **a.g.e**., s. 35-37.

maliyeti yüksek sorunlarla karşı karşıya kalınması gibi ciddi problemler karşı karşıya kalabileceklerdir.

- Siber alan, her tür veri, bilgi, belge ve sistemin depolandığı ortamlardır. Bu ortamlardaki verilerin boyutu, kapsamı, çeşitliliği artmakta ve bu verilerden değer elde etme durumu ise yaygınlaşmaktadır. Bu nedenle, bu verilerin ihlali ve kötüye kullanımının önüne geçilebilmesi için verilerin korunması önem arz etmektedir.

- Siber alanda depolanan verilerin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması, hem rekabet gücünü artırma hem de ticari imajı korumak ve sürdürmek için bir zorunluluk haline gelmiştir.

- Kişisel ya da kurumsal seviyede, sahip olunan varlıkların korunması açısından; casusluk, sabotaj, sahtekârlık gibi çeşitli tehlikelere karşı koymanın yanı sıra, virüslere, casus yazılımlara, siber saldırılara, bilgisayar korsanlarına karşı koyabilmek de oldukça önemli hale gelmiştir. Bu tehlikeleri ortadan kaldırmak için siber güvenliğin sağlanması gerekmektedir.

- Siber alanda; internet üzerinden yapılan alışveriş sistemleri, bankacılık ve finans sistemleri, elektrik-üretim ve dağıtım tesisleri, cep telefonu opretatörleri ve haberleşme sistemleri, doğal gaz kontrol ve aktarma sistemleri, hava trafik kontrol merkezleri, bilgisayar ve iletişim sistemleri gibi kritik altyapılar ve ağlar, kritik yazılımlar ve sistemler bulunmaktadır. Bu sistemlere yapılacak saldırıların başarılı olması durumunda, kurumsal ve ulusal seviyelerde karışıklıklar, aksaklıklar ve hatta kaosa neden olabilecektir. Bu nedenle siber güvenliğin sağlanması hayati derecede önemli olmaktadır.

- Yapay Zekâ, Nesnelerin İnterneti, Kuantum Hesaplama gibi yeni yaklaşımların, teknolojilerin ve uygulamalarının giderek arttığı günümüzde farklı tehdit ve tehlikelerin oluşacağı dikkate alındığında, siber güvenliğe olan gereksinim giderek arttığını söylemek mümkündür.

Son yıllarda yaşanan teknolojik gelişmelerin de katkısıyla bilişim toplumu olma yolunda ilerleyen Türkiye'de, bu alandaki teknolojileri kullanan her seviyedeki personel, kurum ve kuruluşa, siber güvenlik kavramının kapsamını ayrıntılarıyla öğretilmeli, siber alan konusunda farkındalığı arttırıcı eğitimler verilmeli ve siber alandaki mevcut varlıkları korumanın ne kadar önemli olduğunun anlatılması elzem görünmektedir. Bu anlamda siber güvenlik, ulusal bir konu haline gelmektedir[120].

Siber güvenlik ile genellikle aynı anlamda kullanılmasına rağmen aralarında fark olan bir diğer kavram da bilgi güvenliği kavramıdır. Bilgi güvenliği, siber güvenlikten farklı olarak sadece siber alanı değil fiziki alanı da kapsamaktadır. Bilgi güvenliği kavramı, bir varlık olarak bilginin zararlardan ve yanlış kişilerin eline geçmesinden korunması sürecini ifade etmektedir[121].

21. yüzyıl bilginin çağı olarak adlandırılmakta ve dolayısıyla bilgi toplumu ortaya çıkmaktadır. Bilgi toplumunun temeli de bilgidir. Bilginin günümüz toplumunda yayılma vasıtaları ve hızını düşünüldüğünde bilgi güvenliği konusunun gündeme gelmesi de kaçınılmaz olmaktadır[122]. Bilgi, niteliği itibarı ile çeşitli iletişim vasıtaları ile başkalarına iletilebilen, depolanabilen, fiziksel bir ortamda kaydedilmiştir. Bu süreçte bilginin güvenliği öne çıkmaktadır[123]. Bu noktada bilginin yayılması kadar yayılacak bilginin güvenliği de önem arz etmektedir.

Siber güvenlik ve bilgi güvenliği kavramlarına kısaca değindikten sonra siber alanda karşılaşılabilecek tehdit ve saldırılardan söz etmek uygun olacaktır. Özellikle internet kullanımının gün geçtikçe arttığı günümüzde siber alanda çok çeşitli yol ve yöntemlerle işlenen suçlar giderek toplum güvenliğini de etkiler hale gelmiştir. Bu noktadan hareketle siber alanda gerçekleşen suç girişimlerini daha kapsayıcı bir

[120] **A.e**., s. 38.
[121] Gürol Canbek ve Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi,** C. IX, S: 3, 2006, s. 169.
[122] Hüseyin Koçak ve Kamile Memiş, "Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu", **Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi,** C. XX, S: 3, Aralık 2018, s. 5.
[123] Cihan Dura ve Hayriye Atik, **Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye**, İstanbul, Literatür Yayınları, 2002, s. 114.

kavram olan ‘bilişim suçları‘ başlığı altında incelemek ve bilişim suçlarına karşısında alınabilecek önlemlere bakmak uygun olacaktır.

İKİNCİ BÖLÜM

SİBER ALANDA GÜVENLİĞE YÖNELİK TEHDİTLER: BİLİŞİM SUÇLARI

2.1. İnternet Olgusunun Tarihsel Gelişimi

İnterneti, "tüm dünyada ağlar arası ağ" olarak genel anlamda tanımlamak mümkündür.[124] İnternet, *Interconnected Networks*'den türetilen yani 'birbirine bağlı ağlar' anlamında büyük bir ağdır. İnternet, dünya çapında milyonlarca bilgisayarın ağ üzerinden birbirine bağlı olduğu ve sürekli gelişerek büyüyen bir ağdır. İnsanların bilgiye ulaşma ve saklama istekleri sonrasında ortaya çıkmış bir kavram üzerine gelişmiş bir teknolojik sistem olan internet, bu sistem vasıtasıyla insanlara bilgiye hızlı erişim imkanı sunmaktadır. Küreselleşen dünyamızda bilgiye erişim anlamında internetin önemli bir rolü bulunmaktadır. İnternet, kullanıcıların çeşitli konularda büyük bir arşive erişmesini, kullanıcılarla iletişime geçmesini ve veri değişimi için diğer kullanıcılara bağlanmasını sağlar. Bu ağ birçok küçük merkezi ağdan oluşur. İnterneti bilgiye erişim, iletişim kurma, eğlence, sosyal medya ve ticaret gibi birçok alanda kullanmaktayız. Akıllı telefonların da ortaya çıkışı ile birlikte interneti artık mobil telefonumuz üzerinden her yerde kullanmaktayız.

İnternet, TCP/IP protokolü adı verilen bir paket veri aktarım protokolü ile birçok bilgisayarın ağ üzerinden birbirine bağlandığı sistemdir. TCP/IP protokolü ağ üzerindeki sistemlerin birbirlerine hangi kurallarla paket veri aktaracağı, aktarılan verideki hataların kontrolü ve ayıklanması amacıyla geliştirilmiş bir protokoldür. TCP/IP protokolünde, iletilen veriler katmanlara göre paketlenirler ve alıcı da bu paketleri tek tek çmak suretiyle veriye ulaşır. Her katmanda yollanan verinin türüne göre (e-posta, dosya aktarımı) belirli protokoller görev yapar[125].

---

[124] Boğaç Erkan ve Murat Songür, **Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü**, Ankara, Hacettepe – Taş Yayınevi, 1999, s. 282.

[125] İTÜ Bilgi İşlem Daire Başkanlığı, "TCP/IP Protokolü", Eylül 2013, (çevrimiçi) https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/tcp-ip-protokolu, Erişim: 10 Ağustos 2019.

Günümüz internetinin fikir babası olarak değerlendirilen J.C.R. Licklider, ABD'nin teknoloji alanında dünya çapında ünlü üniversitelerinden Massachusetts Institute of Technology'de (MIT) 1962 yılında yayınladığı makalelerinde değindiği "Intergalactic Computer Network (Galaktik Bilgisayar Ağı)" kavramı günümüz internetinin çıkış noktasını oluşturmaktadır.[126] Licklider'in öne sürdüğü bu Galaktik Bilgisayar Ağı kavramı, evrensel olarak birbirine bağlı bir ağ üzerinden herkesin dilediği yerden bilgiye erişebilmesini ve iletişime geçebilmesini öne sürüyordu.

Licklider, 1962 senesinde DARPA'nın (Savunma İleri Düzey Araştırma Projeleri Biriminin) başına geçmiş ve bu birimde faaliyetlerini devam ettirmiştir. 1965 yılında Thomas Merrill ve beraber çalıştığı Roberts, Massachusetts'teki bir TX-2 bilgisayarını California'daki bir Q-32 bilgisayarına yavaş hızda bir telefon hattı üzerinden birbirine bağlamayı sağlamıştır ve bu WAN (Wide Area Network) adını alan ilk geniş alan bilgisayar ağıdır.[127]

İnternet ilk olarak ABD Savunma Bakanlığı Pentagon'un 1969 senesinde DARPA (*Defense Advanced Research Project Agency*) ismiyle kısaltılan Savunma İleri Düzey Araştırma Projeleri Birimi'nin bilgisayarları birbirine bağlayan ve herhangi bir ana bilgisayara bağlı olmayan bir ağ sistemi düşüncesi sonucu yapılan çalışma ile gerçekleştirilen ağ iletişimini temel alır. Daha sonra bu ağ çeşitli fikirlerle ARPANET (Advanced Research Projects Agency Network) olarak kısaltılan Gelişmiş Araştırma Projeleri Dairesi Ağı ismini alarak gelişim sürecini sürdürmüştür.[128]

Daha sonra ilk olarak ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı) projesi ile başlayan süreç bugün kullandığımız küresel internet ağının öncüsü olmuştur. Hızlı bir şekilde daha sonradan diğer merkezlerde bulunan bilgisayarlar da bu geliştirilen ARPANET ağına bağlanmış olup, bilgisayarların birbirine bağlanması için gerekli ağ protokolü olarak da günümüzde de halen kullanmakta olduğumuz İletişim Kontrol ve Aktarım Protokolü olan TCP/IP (Transmission Control Protocol/ Internet

[126] Çevrimiçi, https://internethalloffame.org/inductees/jcr-licklider, Erişim: 3 Haziran 2019
[127] Çevrimiçi, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarihçesi, Erişim: 4 Haziran 2019
[128] İTÜ Bilgi İşlem Daire Başkanlığı, "İnternetin Tarihçesi", Eylül 2013, (çevrimiçi), https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-tarihçesi, Erişim: 1 Haziran 2019.

Protocol) protokolü geliştirilerek internet ağının ana halkası olarak yerini almıştır.

İlerleyen süreçte Amerikan askeri bilgisayar ağı, ARPANET'ten ayrılmış olup, ABD Ulusal Bilim Kuruluşu (*National Science Foundation*) 1986 senesinde ARPANET kapsamında ABD genelinde beş farklı büyük bilgisayar projesini ileri sürdü. ARPANET projesi ABD yönetiminin maddi desteği ile NSFNET adını aldı ve işletmesi özelleştirildi.[129] Bu tarihten itibaren gerek ABD'de bulunan merkezler gerekse de diğer ülkelerden bağlantı sağlanarak gelişen süreçte tüm dünyaya yayılarak internet büyük bir küresel ağ haline gelmiştir.

İnternet ağında merkezi ana bilgisayar kavramı yoktur. İnternetin ortaya çıkış sürecinde de asıl amaç tek merkeze bağlı olmayan bir ağ sistemi kurma fikriydi. Böylece ağa bağlı herhangi bir bilgisayar ağdan koptuğunda diğer bilgisayarlar arasındaki bağlantı devam edecekti. İnternet ağında tüm dünya üzerinden farklı noktalardaki bilgisayarlar ağ üzerinden birbirine bağlanmıştır ve bu bağlantılar çok yönlüdür. İnternet ağındaki tüm bilgisayarlar merkezi ana bilgisayara bağlı olmayıp hepsi çok yönlü birbirine bağlıdır ve dolayısıyla herhangi bir bilgisayarın ağdan kopması genel iletişimi kesmemektedir. İnternet ağından bir bilgisayar koptuğu zaman genel iletişim kesilmez sadece internet ağından kopan bilgisayarın sunduğu içeriğe erişilemez.

İnternet insanlığın iletişim ve bilgiye erişim düşüncesinin sonucu olarak ortaya çıkmıştır ve dünya çapında destek görerek geniş çaplı kullanım alanına erişmiştir. İnternet, ağa bağlanan tüm bilgisayarlara iletişim ve bilgi alışverişi imkanı sunmaktadır. Ağa bağlanan bilgisayar kullanıcıları, ağ üzerindeki diğer kullanıcıların erişimi için çeşitli bilgiler sunmaktadır.

İnternete ülkemizden ilk bağlantı erişim sürecini incelediğimizde, bağlantı yapılan geniş alan ilk ağının, 1986 senesinde sağlanan TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) olduğu anlaşılmaktadır. Devam eden süreçte TÜVEKA ağının artık artan talebe cevap veremez hale gelmesiyle ve

[129] "İnternetin Tarihçesi", (çevrimiçi), https://www.armadigital.net/bilgi-bankasi/internetin-tarihcesi, Erişim: 1 Haziran 2019.

teknolojik altyapısının da yetersiz kalması sonucu 1991 senesinde ODTÜ ve TÜBİTAK, talebe cevap verebilecek daha gelişmiş bir hat üzerinde proje çalışmalarına başlamışlardır. Yeni kurulan ağın oluşumu kapsamında ilk test bağlantısı 1992 senesinde Hollanda'ya denenmiş; 1992 senesinde PTT'ye iletilen çalışma ile ilgili konuların bildirilmesine müteakip, 12 Nisan 1993 tarihinde düşük (64 Kbps) ağ bandı çaplı kiralık bir ağ hattı vasıtasıyla, Bilgi İşlem Daire Başkanlığı (ODTÜ) Ağ Sistemleri bölümündeki routeurlar (bağlantı göndericiler) aracılığıyla, merkezi ABD'de bulunan internet ağına TCP/IP protokol kuralları çerçevesinde NSFNet (*National Science Foundation Network*)'e ülkemizden internete bağlantıda bir ilk yaşanmıştır.[130] Akabinde ülkemizin farklı yerlerindeki üniversitelerden de internet bağlantısı sağlanmış olup, ilerleyen dönemde birçok akademik kuruluş ve ilgili kurumlar, internet bağlantısına kavuşmuşlardır.

İnternet günümüzde Türkiye'de ve tüm dünyada çok yaygın kullanım oranına ulaşmıştır. İnternetin ortaya çıkış sürecinde ağlar arası sürekli iletişim ve bağlantı mantığı temel oluşturmuştur. İnterneti bugün iletişim, bilgiye erişim, eğlence, sosyal medya, bankacılık işlemleri, alışveriş gibi gündelik hayatımızın her alanında kullanabiliyoruz. İnternete dilediğimiz yerden hızlı bir şekilde bağlanabildiğimiz akıllı telefonlara sahip olduğumuz günümüzde internet iş hayatımızın ve günlük hayatımızın vazgeçilmez bir parçası haline gelmiş ve bugünkü şeklini almıştır[131].

2.2. İnternet İle İlgili Temel Kavramlar

İnternetin ortaya çıkışı ile birlikte bir takım yeni kavramlar da literatürümüze girmiştir. Bu kavramlar genel olarak internetin çalışma mantığı ve sistemi üzerinden başlayarak kullanım alanı, iletişim kurma ve bilgiye erişme gibi konularda geliştirilen sistemleri anlatmaktadır. İnternet ile ilgili bu temel kavramlardan en sık duyulan ve kullanılanları şöyle sıralayabiliriz;

2.2.1. Elektronik Posta (E-Mail)

Elektronik posta klasik olarak somut anlamda bir adrese gönderdiğimiz

[130] ODTÜ Bilgi İşlem Daire Başkanlığı, "İnternet Tarihi", (çevrimiçi), http://www.internetarsivi.metu.edu.tr/tarihce.php, Erişim: 2 Haziran 2019.
[131] Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, Beta Yayınları, 2001, s. 23.

postanın dijital, elektronik versiyonudur. Bilgisayar ve internetin ortaya çıkışı ile birlikte ağ üzerinden haberleşmede kullanılmaya başlanan ilk sistemdir. İnternetin bilgiye erişim ve iletişim amaçlı olarak icad edildiği düşünüldüğünde, bu iletişimin sağlanması noktasında günümüzde hala yaygın şekilde elektronik posta sistemi kullanılmaktadır. E-posta servisini bugün internet üzerinden çok sayıda e-posta sistemlerinden birini tercih ederek hızlı bir şekilde kullanabiliriz. Gmail, hotmail ve diğer birçok e-posta servisini ücretsiz ve hızlı şekilde kullanabilmekteyiz. E-posta servisleri üzerinde e-posta gönderirken yazdığımız metinlere ek olarak fotoğraf, ses, çeşitli multimedya dosyalarını da ek olarak gönderip alabilmekteyiz[132].

2.2.2. World Wide Web (WWW)

Veri akışını kontrol protokolü TCP/IP Protokolü ve internette veri aktarımını ve veri aranmasını sağlayan dünyayı saran ağ olarak tanımlanan " World Wide Web" internetin teknik unsurlarından birisidir.[133]

2.2.3. Web Sitesi (Internet Sitesi)

İnternette Web tarayıcıları vasıtasıyla erişim sağlanan, belirli bir kodlama ve grafik tasarım ile genel hatları şekillenen ve bu tasarımın üzerine içeriği yüklenen yerlerdir.[134] İnternet sitelerinde bugün ihtiyacımız olan bilgi, iletişim araçları ve çeşitli görsel-işitsel dosyalara erişim sağlayabilmekteyiz. Günlük hayatımızda sıklıkla haber okumada, bilgi araştırmada, video izlemede, oyun oynamada vs. çeşitli alanlarda internet sitelerini kullanmaktayız. Her alanda çok fazla sayıda site dünya genelinde internet kullanıcılarının hizmetine sunulmaktadır. İnternet sitelerinin genel uzantısı ".com" dur, bu uzantı aynı zamanda sitenin ABD menşeli olduğunu ve serverının orada bulunduğuna işaret eder, diğer ülkeler için her ülke ".com" uzantısına ek olarak ülke kısaltmasını ekler. Örneğin; Türkiye için sitenin uzantısı ".com.tr" olur. "com" uzantısı aynı zamanda sitenin genel olarak ticari amaçlı olduğuna işaret eder. İngilizce ticaret anlamına gelen "commercial" kelimesinin kısaltmasıdır. Ayrıca diğer faaliyet

---

[132] Turhan, **a.g.e**., s. 13.
[133] "WWW Nedir?", (çevrimiçi) https://www.baskent.edu.tr/~tkaracay/etudio/ders/internet/html/htmlbasics/web.htm, Erişim: 15 Ağustos 2019
[134] "Web Sitesi", (çevrimiçi) https://whatis.techtarget.com/definition/Web-site, Erişim: 15 Ağustos 2019

alanlarıyla ilgili de çeşitli site uzantıları mevcuttur. Bunlar da yine çeşitli kelimelerin kısaltmasıdır. Örnek olarak "education" kısaltması "edu", "government" kısaltması ".gov" dur.

2.2.4. Web Tarayıcısı (Web Browser)

İnternette yer alan belgelerin yazıldığı bilgisayar dilini deşifre etmek suretiyle; bu belgelerin monitörledre yazılar, resimler ve benzeri belgeler olarak görmemizi sağlayan aracı programlardır [135] . İnternet üzerinde bulunan internet sitelerine bağlanabilmek için Web Tarayıcısı (Web Browser) isimli bir program kullanmak gerekir. Microsoft Windows işletim sistemlerinin standart (default) tarayıcısı İnternet Explorer, Google Chrome web tarayıcısı, Mozilla Firefox, Apple'ın Mac OS işletim sistemiyle gelen Safari web tarayıcısı en yaygın kullanılan web tarayıcılardır. İnternet sitelerine erişim sağlamak, bu siteler arası dolaşmak yani internet tabiriyle sörf yapmak için bir tarayıcı programa ihtiyacımız vardır, İnterneti uygun ve işlevsel bir biçimde kullanmak için iyi ve güvenli bir web tarayıcısına ihtiyacımız vardır.

Günümüzde Web tarayıcı güvenliği de en önemli unsurlardan biridir. Web tarayıcının güvenliğini artırmak için çeşitli güvenlik eklentileri mevcuttur. İnternet sitelerinde çok sayıda zararlı yazılım barındıran reklamlar bulunmaktadır. Bu reklamlar biz internet siteleri arasında dolaşırken sürekli karşımıza çıkmakta ve bizi etkileyip reklama tıklamamızı beklemektedir. Bu reklamların çoğu zararlı yazılım içeren "pop-up" tabir edilen yeni bir sayfa açarak bizi başka bir siteye yönlendirmeye çalışmaktadır veya bilgisayarımıza yeni bir zararlı içerikli program indirmeye çalışmaktadır.

Bu reklamlardan korunmak amacıyla web tarayıcılarının çoğuna reklam engelleyici günümüzde oldukça popüler olan eklentiler eklenebilmektedir. "Ad-Block Plus" ve "U-block Origin" isimli uzantılar, bu reklam engelleyici uzantıların en çok tercih edilenleridir. Aynı zamanda tarayıcımıza ünlü antivirüs yazılımlarının eklentilerini de ekleyerek tarayıcımızı daha da güvenli hale getirebiliriz. Avast, McAfee gibi çeşitli antivirüs yazılımlarının eklentilerini kullanarak internete daha

[135] Fazıl Saray, "İnternet Ders Notları, s. 2. (çevrimiçi), http://www.selcuk.edu.tr/dosyalar/files /074/%C4%B0nternet_ders_notu.pdf, Erişim: 10 Ağustos 2019.

güvenli erişim sağlayabiliriz. Bu eklentiler her girdiğimiz internet sitesini tarayarak güvenli olup olmadığıyla ilgili bize bilgi vermektedir. Zararlı siteleri otomatik kapatarak bizi korumaktadır.

2.2.5. Arama Motoru (Search Engine)

Arama motoru internet üzerinde ulaşabileceğimiz tüm içerikleri aramak için kullanılan, ihtiyacımız olan belgelere, aradığımız bilgilere en hızlı şekilde ulaşmamızı sağlayan aracı yazılımlardır.[136] Bu motorlar, arama kutucuğuna yazdığımız belirli kelimeler ve seçtiğimiz belirli şartlar çerçevesinde bize aradığımız içeriğin bulunduğu web sitelerini listeleyerek sonuçlandıran uygulamalardır. İnternetteki çok sayıda kaynak ve internet sitesi arasından aradığımız sözcüklere göre bize en doğru kaynağı ve siteyi gösteren yazılımlardır. Arama motorları arasında en bilinen ve en sık kullanılanlar arasında Google ve Yandex arama motorları gelmektedir. Günümüzde milyonlarca internet sitesi arasından hangi bilginin hangi sitede olduğunu bilmenin zorluğunu düşününce arama motorunun önemi daha iyi anlaşılmaktadır.

Bugün milyarlarca dolarlık değere sahip Google firması, ilk olarak arama motoru ile kendisini duyurmuş ve daha sonra çeşitli alanlara da yayılarak bugün kendi markasıyla üretilen Google Pixel isimli akıllı telefon, android işletim sistemi ve çeşitli uygulamaları başta olmak üzere çeşitli teknoloji ve yazılım alanlarında faaliyet yürüten devasa bir teknoloji şirketi haline gelmiştir. Google gibi yine çok kullanılan bir başka arama motoru da Yandex arama motorudur[137]. Yandex firmasının yazılımları da başta navigasyon ve çeviri uygulaması olmak üzere günümüzde yaygın şekilde kulalnılmaktadır. Arama motorları ile ilgili kayıt tuttuğu iddiasıyla bazı kullanıcılar arama kaydı tutmayan arama motorlarına yönelmişlerdir. Bu kayıt tutmayan arama motorlarının en çok kullanılanı DuckDuckGo'dur. DuckDuckGo'nun sloganı da "sizi takip etmeyen arama motoru"'dur

---

136 "Arama Motoru Nedir?", (Çevrimiçi) https://www.aramamotoru.com/arama-motoru-nedir/, Erişim: 13 Ağustos 2019

137 "En Çok Kullanılan 21 Arama Motoru", (çevrimiçi) https://www.aramamotoru.com/en-cok-kullanilan-21-arama-motoru/, Erişim: 12 Ağustos 2019.

2.2.6. Transmission Control Protocol/ Tcp/Ip Protokolü

TCP/IP protokolü, bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır.[138] İnternet üzerinde bilgisayarlar arası ağ üzerinden iletişimin, veri akışının ve bunların hata kontrolünün hangi şartlarda yapılacağını belirleyen kurallar bütünüdür.

Veri akışını düzenleyen TCP/IP Protokolü bugün internetin temel unsurlarından birisidir. TCP/IP'nin V4 ve V6 olarak iki versiyonu bulunmaktadır. V4 günümüzde halen aktif olarak kullanılmakta ve şu an için yeterli olmaktadır.

2.2.7. Alan Adı (Domain Name)

Alan adı sistemi, internet tarayıcısına bağlanmak istediğimiz internet sitesini yazarak bahse konu siteye bağlanmamıza yarayan sistemdir.[139] İnternette her sitenin bir ip adresi vardır. Bu ip adresleri örneğin 192.168.1.1 şeklinde dört bölümden oluşur. Örneğin 172.217.168.206 gibi uzun ve kompleks bir rakam gurubunu hafızamızda tutmak yerine www.google.com şeklinde tarayıcımıza girerek en sık kullandığımız arama motoru olan google'a erişim sağlayabilmekteyiz. Domain name sistemi internet kullanıcılarına büyük kolaylık sağlamaktadır. Web tarayıcısına dört bölümlü karmaşık rakamlardan oluşan bir ip adresi yazmak yerine bağlanmak istediğimiz sitenin ismini yazarak kolaylıkla ve hızlı bir şekilde erişim sağlayabilmekteyiz. Bu sistem internetin kullanım pratikliği açısından önemli bir buluştur. Alan adı uzantıları da Web sitesi kısmında bahsedildiği üzere; ".com", ".edu", ".gov" ve ".net" şeklindedir ve ülke kısaltmalarıyla beraber örneğin; İstanbul Üniversitesi'nin web sitesinin alan adı "https://www.istanbul.edu.tr" şeklindedir. Alan adının başındaki "https" kısmı ise sitenin bulunduğu sunucuya güvenlik sertifikası ile bağlantı yapıldığını ve bağlantının güvenli olduğunun onaylandığını gösterir. Https teriminin açılımı ise Güvenli Hiper Metin Aktarım Protokolüdür.

Alan adlarına ilişkin yasal düzenleme çerçevesinde 5651 sayılı kanuna bağlı

---

138 "TCP/IP protokolleri", (Çevrimiçi) https://www.ip-adres.com/bilgi/tcp-ip-protokolleri, Erişim: 16 Ağustos 2019

139 "Hosting(Alan adı) Nedir?", (Çevrimiçi) https://www.hosting.com.tr/bilgi-bankasi/hosting-ve-domain-nedir/, Erişim: 15 Ağustos 2019

İnternet Alan Adları Yönetmeliği bulunmaktadır. Bu yönetmelikte detaylı şekilde alan adlarının tanımı, alım satım, feragat işlemleri, alan adı sahibinin hakları ve yükümlülükleri, uyuşmazlık çözümleri ve Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) bu alandaki rolü ve yetkileri detaylı şekilde düzenlenmiştir.

2.2.8. Ip Adresi (Internet Protocol Adress)

Ağ ortamında olup olmadığına bakılmaksızın her bilgisayarın kendine ait bir IP numarası vardır. Bu IP numaraları manuel olarak ayarlanacağı gibi otomatik olarak bilgisayar tarafından da (örneğin DHCP sunucu ile) atanabilmektedir[140]. Ip adresi, çevrimiçi olduğumuz zaman bilgisayarımızın internetteki kimliğidir. Her insanın kendisine ait bir kimlik veya pasaport numarası olduğu gibi, bilgisayarların da internetteki kimliğini belirleyen ip adresidir. Sabit IP(Statik IP) ve Değişken IP(Dinamik IP) şeklinde çeşitleri vardır. Sabit IP'de kullanılan IP adresi değişmezken dinamik IP adresinde kullanıcının IP adresi her bağlantı kopup yeniden bağlandığında yenilenir. İnternet servis sağlayıcılar tarafından atanan bu ip adresleri bilgisayarların internet üzerindeki kimliği işlevi görerek kullanıcılara kolaylık sağlamaktadır. Suçun önlenmesi ve araştırılmasında günümüzde ip adresleri üzerinden takipler yapılmakta ve kullanıcılar tespit edilip gerekli işlemler yapılmaktadır.

2.2.9. Sunucu (Server)

İnternet üzerinden eriştiğimiz internet sitelerinin ve çeşitli görsel işitsel materyalin saklandığı bilgisayarlar ve yazılım sistemleridir.[141] Bağlandığımız tüm internet sitelerinin içeriğinin tutulduğu başka bir bilgisayar sistemi vardır. Biz web tarayıcımız üzerinden kendi bilgisayarımızdan örneğin "youtube.com" sitesine bağlandığımızda youtube sitesinin sunucularından birisine bağlanırız, site üzerinden bir videoyu açtığımızda aynı şekilde videonun saklandığı sunucuya bağlanarak videoyu izleriz. Sunucuların da internet üzerinde tüm bilgisayarların sahip olduğu gibi bir ip adresi vardır. Youtube sitesinin içeriğindeki çok sayıda videoyu kullanıcılarına ulaştırabilmesi için çok geniş çaplı sunucu sistemleri vardır.

---

[140] "TCP/IP ve İnternet", (çevrimiçi) http://web.firat.edu.tr/mbaykara/tcpipveinternet.pdf, Erişim: 13 Ağustos 2019.

[141] "Server nedir?", (çevrimiçi) https://immibbilisim.com/blog/40/server-nedir, Erişim: 14 Ağustos 2019

İnternet olgusu ile ilgili temel kavramlardan söz ettikten sonra, çalışmanın ana unsurlarından biri olan ve siber alanda gerçekleşen bilişim suçlarına bu noktada giriş yapmak yerinde olacaktır.

2.3. Bilişim Suçlarına Genel Bakış

Bilişim, insanların teknik, ekonomik, sosyal vb. konularda sahip oldukları verinin saklanması, bu verinin elektronik olarak işlenmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılması şeklinde tanımlanmaktadır[142].

Kişilerin bilişim alanında sahip olduğu değerler, onların özel mülkleri gibidir. Nasıl ki özel mülke girmek için hâkim ya da savcı izni gerekiyorsa, bilişim sistemlerine izinsiz girmek de kişinin özel mülküne ya da şahsiyetine taciz olarak kabul edilmektedir[143].

Bilgi ve iletişim teknolojisiyle birlikte 'bilgi toplumu' olarak gelişen dünyayı tehdit eden siber saldırıların sayısı gün geçtikçe artmaktadır. Son yıllarda bilgisayar ve internet, hayatımıza hızlıca girerek pek çok akıllı teknolojiyle enerji, sağlık, eğitim, mühendislik, ekonomi gibi birçok alanda fayda sağlamaktadır. Ancak hızlı bir şekilde sürekli değişen ve gelişen bilgi teknolojisinin yaşam kalitesini artırmasının yanında güvenlik zaafiyeti nedeniyle ortaya çıkan bilişim suçu bağlantılı siber saldırılar önemli bir tehdit oluşturmaktadır.

Bilgisayar ve internetin gelişmesiyle erişim kolaylığı, kişisel verilerin ele geçirilmesi, bilişim suçlarının işlenmesi, ülkelerin temel ve hassas altyapılarına zarar vermek isteyerek, çeşitli güvenlik zaafiyeti tarayan bilgisayar korsanlarının, bilişim casuslarının, internet korsanlarının saldırılarına hedef haline gelmiştir. İnternet üzerinden yapılan saldırıların başında spamlar, oltacılık, hırsızlık, dolandırıcılık, ulusal veyahut uluslararası kaos yaratmak amacıyla yapılan saldırılar, yazılım ve sistemlerin açıklarını yakalayarak zarar vermek, kişisel tatmin gibi bir çok amaçla internetin kötüye kullanıldığı gerçeği yadsınamaz boyuttadır.

---

[142] Mehmet Emin Artuk, Ahmet Gökcen, Ahmet Caner Yenidünya, **Türk Ceza Kanunu Şerhi**, C. V, Ankara, Turhan Kitapevi, 2009, s. 4643.
[143] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008, s. 79.

İnternet yapısı itibariyle dünya çapında çok büyük bir ağ olması ve internetin iletişimi sağlamada sınırsız bir alana hitap etmesi nedeniyle bilişim suçlarının işlendiği bir ortam olması da kaçınılmazdır.

Bilgi ve iletişim yani bilişim teknolojilerinde meydana gelen büyük ilerlemeler, önemli buluşlar bizi bilgisayar ve internet gibi çok önemli icatlarla buluşturmuştur. Ancak gerçek hayattaki suç işleyebilecek şahıslar ve organize gruplar internet ortamına yani sanal aleme de taşınmış ve bu alemde de çeşitli suç tipleri ortaya çıkmıştır. Bu gelişmeler ile birlikte yeni kavramlar da ortaya çıkmıştır. Çeşitli tanımlamalarla bu kavramlar internet suçları, bilgisayar suçları, bilgi ve iletişim alanında suçlar, bilişim suçları, sanal suçlar, siber suçlar gibi farklı isimlerle anılmışlardır.

Bilişim suçları öncelikli olarak internet bağlantısının ilk sağlandığı, daha çok internet kullanıcısının bulunduğu büyük ülkelerde öncelikli olarak ön plana çıkmış ve ilk olarak bu ülkelerce çeşitli tedbirle, önlemler alınarak gerekli yasal düzenlemeler yapılmıştır. Özellikle Amerika Birleşik Devletleri ve Avrupa'nın önde gelen büyük ülkeleri bu alandaki hukuki altyapılarını hızla tamamlama yoluna girmişlerdir.

2.3.1. Bilişim Suçlarının Tanımı

Bilişim suçu; verileri otomatik olarak işleyebilme yeteneğine haiz bir sisteme (bilgisayar, cep telefonu gibi) yasa ve ahlak dışı yani izin almaksızın girilmesi, müdahale edilmesidir[144]. Bilişim suçları ile alakalı yapılan, literatürde geçen çok sayıda isimlendirme ve tanımlama bulunmaktadır. Uluslararası alanda bu suçlar genellikle Cyber Crimes (Siber Suçlar), Network Crimes (Ağ Suçları), Digital Crimes (Dijital Suçlar) ve Computer Crimes (Bilgisayar Suçları) şeklinde isimlendirilmektedir. Türkiye'de ise bu suçlara ilişkin bilişim suçları, bilgisayarla ilgili suçlar, bilgi teknolojileri suçları, internet üzerinden işlenen suçlar, siber suçlar gibi tanımlamalar yapılmaktadır. Kullanım oranına bağlı olarak en sık kullanılan iki tanımlama Bilişim suçları ve Siber Suçlar tanımlamalarıdır. Bu alandaki suçlar, 5237

[144] Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle**, İstanbul, Alfa Yayınevi, 1997.

sayılı Türk Ceza Kanunu'nda Bilişim Suçları Başlığı altında tanımlanmışken[145], bu alandaki suçlara karşı mücadele eden Emniyet Müdürlüklerine bağlı Şube Müdürlüklerinin ismi ise Siber Suçlarla Mücadele Şube Müdürlüğüdür. Buradan da görüldüğü üzere aynı suçlarla ilgili farklı isimler kullanılabilmektedir.

İlk başlarda bilişim suçları tanımlamaları mevcut suç tiplerinin bilgisayar ve internet aracılığıyla işlenmesi olarak düşünülse ve bu şekilde tanımlama yapılsa da sürekli değişen ve gelişen teknolojinin getirdikleriyle bu alanda çok farklı suç tipleri ortaya çıkmıştır. Bilişim suçları işlemek için bu alanda kodlama ve program yazma tarzı özel bilgiler gerekmektedir, bu bağlamda bu alanda sürekli olarak değişen tarzda yeni yöntemler ve suç tipleri ortaya çıkmaktadır.

Bilişim Suçları, Avrupa Ekonomik Topluluğu (*European Economic Community*) Komisyonu'nun Paris'te 1983 senesindeki oturumunda "Bilgisayar gibi bilgileri otomatik olarak işleyen herhangi bir sistemde ahlak dışı, kanunsuz ve izinsiz gerçekleştirilen hareketler" olarak genel anlamda tanımlanmıştır.[146]

Avrupa Komisyonu (*European Commission*)'nun bu konuyla ilişkili olarak yaptığı tanımlamada bu suç tiplerinin klasik ülke sınırlarını aştığı, herhangi bir yerden çok uzak başka bir yerdeki kullanıcıya karşı işlenebildiği ve bilişim sistemlerinin ya hedef olduğu ya da araç olduğu suç tipleri olarak genel anlamda bahsedilmiştir.

Bilgi ve enformasyon teknlojilerinde gün geçtikçe ortaya çıkan yenilikler ve gelişmelere bağlı olarak hızlı şekilde değişen internet ortamı dijital anlamda da birçok hukuki yararın ihlal edildiği bir ortam halini almıştır. Bu alanda sanal olarak gerçekleştirilen fiil genel olarak bir hak ihlali yaratıyor ve hukuka aykırı bir sonuç doğuruyorsa bunun bilişim suçu olarak tanımlanabileceği aşikardır.

Bilgisayar ve internet üzerinden genel evrensel hukuka aykırı fiiller ihlal edilmeye başladıktan sonra mağdur olan kişi ve kuruluşlar da haklarını arama yoluna gitmişlerdir. Bu mağduriyetler bilişim suçlarına dikkat çekmiş ve bu konuda kişileri

---

[145] Serkan Gönen, Halil İbrahim Ulus ve Ercan Nurcan Yılmaz, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", **Bilişim Teknolojileri Dergisi**, C. IX, S: 3, 2016, s. 229.

[146] Cevat Özel, "Bilişim ve İnternet Suçları Üzerine Bir İnceleme İnternet Hukuku", www.law.ankara.edu.tr/yazi, Erişim: 4 Mayıs 2019.

kendi imkanları çerçevesinde güvenlik almaya, devletleri ve uluslararası kuruluşları da bu alanda gerekli yasal düzenlemeler yaparak bu alandaki suçlarla mücadele etme yoluna itmiştir.

2.3.2. Bilişim Suçlarının Belirlenmesinde Avrupa Konseyi Siber Suçlar Sözleşmesinin Temelinde Yeralan İlkelerin Dikkate Alınması

Avrupa Konseyi Siber Suçlar Sözleşmesi (tam metin için bkz: EK-2) 2001 yılında kabul edilen ve 2010 yılında Türkiye'nin de taraf olduğu[147], siber suçlarla uluslararası seviyede mücadele etmek için hazırlanmıştır. Bu sözleşmenin çalışmamız ile ilgili kısmından kısaca söz edilecektir.

2.3.2.1.Bilişim Suçlarının Belirlenmesinde Ortak Asgari Standartlara Uyulması İlkesi

Sözleşmenin en önemli amacı bilişim suçlarının belirlenmesinde ortak asgari standartlara uyulmasının sağlanabilmesidir. Özellikle internet ortamında işlenen bilişim suçlarıyla mücadelede uluslararası işbirliğinin tesis edilebilmesinde ön koşuldur. Bu işbirliğinin gerçekleşebilmesi için de, fiilin işbirliği yapacak ülkelerde suç sayılması gerekmektedir. Bazen bir ülkede suç sayılan bir fiil, diğer bir ülkede suç sayılmayabilir. Bilişim sistemi ile işlenen bir fiil Türk Hukukunda suç sayıldığı halde, ABD'de suç sayılmıyorsa, ABD'de bulunan bir kişi için verilecek cezanın uygulanabilmesi mümkün olamayacağı gibi, ABD'den internet üzerinden işlenen bir suçta, Türkiye ile ABD'nin işbirliği yapabilmesi de olanaklı görünmemektedir. Bu sebeple, ortak asgari standartlara uyulması son derece önemlidir.

2.3.2.2. Fiilin Haksız ve Kasten İşlenmiş Olması İlkesi

Sözleşmede yer alan suçların haksız biçimde ve kasten işlenmiş olması gerekmektedir. Fiilin haksız olması suç unsurunun zorunlu bir sonucu olup, rıza, zorda kalma veya bazı hak ve yetkilerin kullanılması hallerinde bilişim suçlarında ceza sorumluluğu ortadan kalkmaktadır. Örneğin bilişim sistemi sahibinin izin vererek sistem güvenliğini test ettirmek üzere bilişim saldırıları yaptırması haksız

[147] Türkiye'nin taraf olma süreci ile ilgili ayrıntılı bilgi için; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C. IV, No: 2, 2018, ss. 35-42.

olmayacağından suç teşkil etmeyecektir. Sözleşmenin gerekçesinde "kasıtlı olarak" ibaresinin kesin anlamının her devletin kendi iç hukukunun yorumuna bırakıldığı belirtilmiştir. Bilişim suçu sayılan fiillerin taksirle işlenmesinde ceza sorumluluğundan bahsedilemeyecek olup, suçun kasıtlı işlenmesi kusurlu sorumluluğu ifade etmektedir.

2.4. Bilişim Suçlarının Tarihsel Gelişimi

Sanayi devriminden sonra günümüzde yaşanan en büyük gelişme olarak nitelendirilen "bilişim devrimi" hızlı bir şekilde ilerleyen teknolojinin sonucu olarak karşımıza çıkmaktadır. Bilgi ve iletişim çağı olan günümüzde tekonolojinin yaşantımızda getirdiği yenilikleri hızla karşılayıp adapte olmaya çalışırken, beraberinde getirmiş olduğu sorunlara karşı ne kadar duyarlı olduğumuz tartışmalıdır.

Bilişim teknolojisinin yarattığı sanal dünyada gelişmeleri takip etmek kadar zor olan bir diğer husus da bu alanda işlenen suçlar ve bu suçlarla mücadeledir. Tüm hayatımıza girmiş olan bilişim sistemleriyle işlenen suçlar ise bilgi ve teknolojilerinin hukuksal boyutu olup, dünyada ve ülkemizde yapılan düzenlemelerle mücadele edilmeye çalışılmaktadır. Dünyada ilk olarak bilişim suçlarına dikkat çeken uluslararası kanun tasarısı ABD Kongresinde Senetör Ribikoff tarafından 1977 yılında verilmiş olup, kabul edilmemesine rağmen konuya dikkat çekmek açısından bilişim tarihindeki ilk önemli duyuru olarak kabul edilmektedir.[148]

Bilişim suçlarıyla ilgili olarak uluslararası gelişmelerin başlangıcı açısından ise OECD (Ekonomik İşbirliği ve Kalkınma Örgütü) bünyesinde kurulan uzman komitenin bilişim suçlarıyla ilgili belirli suç kategorileri konusunda tavsiyeleri, Avrupa Konseyi tarafından kurulan komitenin tavsiye kararları, Birleşmiş Milletler'in Havana'daki Ceza Kongresi, BM Bilgisayarlarla Gerçekleştirilen Suçlara İlişkin Strateji Metni ve Almanya'daki Wurzburg Konferansındaki bilişim

[148] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara, Seçkin Yayıncılık, 2014, s. 99.

suçlarıyla mücadeleye ilişkin tartışmalar, Avrupa Konseyi'nin 1995 yılında bilgi teknolojisiyle ilgili usul hukuku problemleriyle ilgili tavsiye kararları öne çıkmaktadır.

Avrupa Konseyi'nin bilişim teknolojileri ve suçları alanına ilgisi, suç sayılan fiil ve kategorilerinin belirlenmesi, konseyin birbirini takip eden tavsiye kararlarıyla devam etmiştir. Avrupa Konseyi'nde alınan tavsiye kararlarından sonra 1997 yılında bilişim suçları ile internet üzerindeki iletişime bağlı olarak suç sorumluluklarını, yargısal hakları ve yeni suç türlerini belirlemek üzere uzmanlar komitesi oluşturulmuştur. Uzmanlar komitesi toplantılarına Amerika Birleşik Devletleri (ABD), Japonya, Güney Afrika ve Kanada çağrılmıştır. Komitenin çalışmaları sonucunda "Convention on Cybercrime" Siber Suç Sözleşmesi, ülkelerin dış işleri bakanlarınca kabul edilmiş ve 23 Kasım 2001 tarihli olarak Budapeşte (Macaristan) şehrinde imzaya sunulmuştur. Avrupa Konseyi'ne üye 26 ülkenin temsilcisi bakanları ile birlikte yukarıda adı geçen davetli ülkelerin de dahliyle bahse konu Sözleşme imzalanmıştır. Bu sözleşmenin, en az üçü Konsey üyesi olan toplam beş devletin de onaylandığı tarihte yürürlüğe girmesi öngörülmüştür. Bu hüküm gereğince 1 Temmuz 2004 tarihinde Sözleşme yürürlüğe girmiş bulunmaktadır.

Türkiye, Avrupa Konseyi Siber Suçlar Sözleşmesini 10 Kasım 2010 tarihinde imzalamış olup, 22.04.2014 tarihli ve 6533 sayılı yasayla Budapeşte'de imzalanan Avrupa Konseyi Siber Suçlar Sözleşmesi onaylanmış, bu kanun Resmi Gazete'de 02.05.2014 tarihinde yayımlanarak yürürlüğe girmiştir.[149]

2.5. Bilişim Suçlarının Kategorize Edilmesi

Bilgi ve iletişim teknolojilerinde gerçekleşen baş döndürücü gelişmeler, günümüzde akıllı telefonlar üzerinden internetin daha sık ve yaygın şekilde kullanımına da bağlı olarak bilişim alanda yaşanan suç artışında etkili olmuştur. Bu alanda ağırlıklı olarak illegal maddi kazanç elde etme ile ilgili suçların daha çok planlanarak icra edildiğine tanık olmak mümkündür. Günümüzde artık internet üzerinden bankacılık işlemleri, para transferleri ve çeşitli elektronik ticaret faaliyetleri

[149] **A.e.**, s. 100.

yapılmaktadır. Bütün bu maddi içerikli faaliyetler, amacı yasadışı maddi imkân elde etmek olan kişileri cezbetmektedir. İllegal olarak maddi kazanç elde etmek isteyen bu kişiler internet üzerinden dönen bu para trafiğine müdahale edip hukuka aykırı yarar sağlamaya çalışmaktadırlar.

Bilişim suçları, klasik anlamda asayiş konulu ve diğer suç tiplerinin internet üzerinden bilişim sistemleriyle işlenmesi ile birlikte farklı bir boyut kazanmıştır. Bilişim sistemlerinin doğrudan hedef olduğu yeni suç tipleri de ortaya çıkmıştır. Günümüzde artık herkesin aşina olduğu Hacking (Sistem güvenliğini aşarak yetkisiz erişim sağlama) ve bunu gerçekleştiren Hacker diye tabir edilen kişiler hedef olarak belirledikleri sisteme güvenlik korumalarını aşarak erişim sağladıktan sonra verileri çalma, değiştirme veya yok etme yollarına gitmektedirler. İnternet üzerinde en sık karşılaşılan husus kredi kartı bilgilerinin çalınması olayıdır. İnternet üzerinden kredi kartı vasıtası ile uluslararası alanda çoğu ticari işlemi gerçekleştirilebilmektedir. Örnek verecek olursak; bir seyahat planı yaptığımızda internet üzerinden uçak biletlerimizi kredi kartı vasıtası ile alabilmekteyiz, ülkemiz dışında faaliyet yürüten yabancı bir havayolu şirketi de olsa rahatlıkla kredi kartımız ile bilet alabilmekteyiz. Yine aynı şekilde booking.com gibi birçok seyahat sitesi ve mobil uygulamaları üzerinden dünyanın herhangi bir yerinden kredi kartımız ile kalacak yer rezerve edebilmekteyiz. Uluslararası alanda çok fazla sayıda kredi kartıyla işlem gerçekleştirilmektedir. Özellikle Hacker diye tabir edilen kişilerin en sık başvurduğu yöntem de bu kredi kartı bilgilerinin çalınması (*Account Takeover*) işlemidir[150].

Birleşmiş Milletler (United Nations) tarafından 14 Aralık 2000 tarihinde İtalya'da tertiplenen "The Challenge of Borderless Cyber Crime (Uluslararası alanda sınır tanımayan Siber suçlar) ile mücadele etmenin önemi için yapılan toplantıda siber suçlar konuşulmuş ve alınabilecek önlemler tartışılmıştır. Bu panelde siber suçlar alanında 11 suç türü belirlenmiştir. Bunlar; hizmetlerin çalınması; suç eylemlerini kolaylaştırıcı iletişim; bilgi korsanlığı ve sahteciliği; saldırgan materyallerin yayılması; siber takip; sanal gasp (fidye); elektronik kara para aklama; elektronik

[150] Türkiye Bankalar Birliği, **Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önleme Yöntemleri**, Ekim 2015, s. 62.

vandalizm ve terörizm; telefonla pazarlama sahtekârlığı; yasadışı müdahale ve elektronik fon transfer dolandırıcılığı şeklinde çeşitlendirilmiştir.[151]

2.6. Avrupa Siber Suçlar Sözleşmesinde Bilişim Suçları Kategorileri

8 Kasım 2001 tarihinde Avrupa Konseyi (Council of Europe) Bakanlar Komitesi tarafından onaylanan ve amacınının uluslararası alanda sınır tanımayan siber suçlara karşı iç hukuklarda toplumu koruyucu tedbirlerin alınması ve bu alanda sıkı bir iş birliğine gidilmesi amacı ile ortaya çıkan Avrupa Konseyi Siber Suç Sözleşmesi'nde bilişim suçları dört farklı ana başlıkta "bilişim sistemlerinin veri bütünlüğüne, yetkisiz bağlantı sağlanmasına ve sistemin mahremiyeti ile bağlantılı suçlar, genel oalrak bilgisayar ve sistemiyle ilgili suçlar, sunulan içerik hususunda suçlar ve telif hakkı ihlallerini kapsayan suçlar" olarak ele alınmıştır.[152]

2.6.1. Bilişim Sistemlerinin Veri Bütünlüğüne, Yetkisiz Bağlantı Sağlanmasına ve Sistem Mahremiyeti İle Bağlantılı Suçlar

Avrupa Siber Suçlar Sözleşmesi'nin (ASSS) başlangıç kısmında belirtilen bu başlıktaki suçlar veri bütünlüğü, sistem mahremiyeti ve yetkisiz erişimin engellenmesine yönelik olup, yasadışı erişim, veri casusluğu, yasadışı müdahale ve sistemlere müdahale olarak belirtilmiştir. Bu başlıktaki suçlar, en genel bilişim suçları olarak nitelendirilebilir. Bu suçlarla bir taraftan bilişim sistemleri korunurken, diğer taraftan da bu sistemi kullananların çeşitli hakları korumaktadır. Bu kategorideki suçlar, sözleşmenin 2 ila 6ncı maddelerinde düzenlenmiştir.

2.6.1.1. Yasadışı Erişim

Yasadışı erişim kavramı, bilişim sistemlerine yönelik tehdit ve saldırı şeklindeki temel suçlara işaret etmektedir[153]. Yasadışı erişim kavramı ASSS'de düzenlenen "Yasadışı Bağlantı" başlığıyla benzerlik taşımaktadır[154]. ASSS'nin "Yasadışı Bağlantı" başlıklı 2. maddesinde sözleşmeyi imzalayan ülkelerin herhangi bir bilişim veya bilgisayar sistemine yetkisiz erişim sağlanması eylemini iç

[151] (çevrimiçi), http://www.unis.unvienna.org/unis/en/pressrels/2000/cp390.html, Erişim: 5 Temmuz 2019.
[152] (çevrimiçi, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, Erişim: 8 Temmuz 2019.
[153] Gönen, Ulus ve Yılmaz, **a.g.e**., s. 235.
[154] Yılmaz Yazıcıoğlu, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", **Hukuk ve Adalet: Eleştirel Hukuk Dergisi**, İstanbul, 2004, s. 177.

hukuklarında suç olarak tanımlama ve gerekli tedbirleri alma yükümlülüğü getirmektedir.

Yasadışı erişim, bilgisayar sistemine veya herhangi bir bölümüne, yasal olmayan şekilde erişim olup, bilgisayar sistem ve verilerinin güvenliğine yönelik tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Sözleşmede neyin yasal olmayacağı konusunun içeriğini, seviyesini, koşullarını belirleyebilmede, taraf devletlere takdir hakkı tanımaktadır.

Bilgisayar sistemlerine yasadışı erişim virüs, trojan, zararlı yazılımlar, hacking gibi sistem kırıcılık saldırıları olarak bir çok yolla gerçekleştirilen suçlar gün geçtikçe artmaktadır. Buna ilişkin olarak 5237 sayılı Türk Ceza Kanunu'nun "Bilişim Sistemine Erişim" alt başlıklı 243. md'sinde bilişim sisteminin herhangi bir kısmına veya tamamına yasaya aykırı olarak erişen ve sisteme bağlı kalmayı sürdüren kişiye ceza verilmesi belirlenmiş ve illegal erişim suç olarak düzenlenmiştir. Böylece Avrupa Siber Suçlar Sözleşmesinin iç hukukta uygulaması yer bulmuş ve sözleşmeyle uyum sağlanarak ülkeler arası suç ve cezada işbirliği sağlanmıştır.

2.6.1.2. Yasadışı Araya Girme

Avrupa Siber Suçlar Sözleşmesinin "Yasadışı Araya Girme" başlıklı 3. maddesinde bir bilgisayar sistemine veri akışı esnasında yasadışı şekilde araya girme eylemini ulusal hukuklarında suç olarak tanımlama ve gerekli tedbirleri alma yükümlülüğü getirmektedir.

Bu suç tanımıyla veri iletişimin gizliliği korunmak istenmektedir. Telefon görüşmelerinin araya girerek yasadışı dinlenmesi ve kaydedilmesi, bilgisayar sistemine girilerek veri akışına müdahale edilmesi gibi saldırılar veri iletişimin gizliliğine müdahaledir. Maddeyle kastedilen telefon, faks, bilgisayar, elektronik posta ve veri transferi yapan bütün elektronik cihazları kapsamaktadır. Maddenin temelindeki iletişimin gizliliği ilkesi AİHS' nin 8. maddesinde de belirtilmiş olup, önemli haklardandır.

2.6.1.3. Verilere Müdahale

Avrupa Siber Suçlar Sözleşmesinin "Verilere Müdahale" başlıklı 4. maddesinde bir bilgisayar sistemine ait verilerin illegal şekilde silinmesi, zarar verilmesi ve engellenmesi eylemini ulusal hukuklarında suç olarak tanımlama ve gerekli tedbirleri alma yükümlülüğü getirmektedir.

Bu hükmü belirlemenin temel gayesi, bilişim sistemlerinin güvenliğini sağlayarak koruma altına almaktır. Maddenin birinci paragrafında müdahalenin birden fazla şekilde yapılacağı belirtildiğinden seçimlik hareketleri belirtilerek suçun genel çerçevesi gösterilmiştir. Veriye seçimlik hareketlerden birisiyle zarar verilmesi suçun unsurlarındandır, ancak bu zararın ciddi zarara yol açması koşulu taraf devletlere bırakılmıştır.

2.6.1.4. Sisteme Müdahale

Avrupa Siber Suçlar Sözleşmesinin "Sisteme Müdahale" başlıklı 5. maddesinde bir bilgisayar sistemine müdahale ederek sistemin işleyişinin haksız yere engellenmesi eylemini suç olarak tanımlama ve gerekli tedbirleri alma yükümlülüğü getirmektedir. Failin amacı verileri silerek, değiştirerek, gizleyerek, erişimi engelleyerek bilgisayar sisteminin çalışmasını engellemektir.

2.6.2. Bilgisayarlarla İlgili Suçlar

Sözleşmede "Bilgisayarlarla Bağlantılı Sahtecilik" ve "Bilgisayarlarla Bağlantılı Dolandırıcılık" başlıkları altında düzenlenmiş olan bu suçlar araç olarak bilgisayar sistemleri kullanılarak gerçekleştirilen klasik suçlarla ilgilidir.

2.6.2.1. Bilgisayar Bağlantılı Sahtecilik

Sözleşmenin 7. maddesinde bir bilgisayar sisteminde verileri değiştirerek sahtecilik yapma eylemini tanımlamaktadır. Bu suçta verilerin alınması, değiştirilmesi ve tamamı ile silinmesi yöntemlerini kullanarak illegal maddi kazanç temin etmedir. Bu madde ile amaçlanan elektronik ortamdaki verilerin doğruluğu ve bütünlüğü korunmak istenmektedir. Belgelerdeki sahtecilik suçunun elektronik ortama yansıması söz konusudur.

2.6.2.2. Bilgisayar Bağlantılı Dolandırıcılık

Sözleşmenin 8. maddesinde bir bilgisayar sisteminde hile ve sahtecilik yoluyla içerik değiştirerek maddi menfaat sağlama eylemini tanımlamaktadır. Bu maddede, sözleşmenin 4. maddesindeki verilere müdahale, 5. maddesindeki sistemlere müdahaleden farklı olarak failde dolandırıcılık niyeti söz konusudur. Bu suçun en temel özelliği dikkate alındığında bilişim dolandırıcılığı, bilgisayar bağlantısıyla yapılan her türlü dolandırıcılık fiilleri olarak tanımlanabilir. Bilişim alanında gizli verilerin ele geçirilmesi suretiyle dolandırıcılık en sorunlu konudur. Bu alanda en göze çarpan örnek, kredi kartlarına yönelik dolandırıcılık filleridir.

2.6.3. İçerikle İlgili Suçlar

Sözleşmenin 'İçerikle İlgili Suçlar' şeklindeki 3. başlığında 'çocuk pornografisi' ve 'telif haklarının ihlali' ile ilgili suçlar ele alınmıştır.

2.6.3.1. Çocuk Pornografisi ile Bağlantılı Suçlar

Sözleşmenin 9. maddesinde çocuk pornografisiyle ilgili olarak; "18 yaş altı olmak veya küçük gibi görünmek" şeklinde çerçeve koyarak, taraf devletlere bilgisayar sistemleri üzerinden çocuk pornografisi ile ilişkili materyal üretme, erişime sunma, dağıtma, temin etme ve depolama fiilerini suç olarak tanımlayarak gerekli mevzuat düzenlemesini yapma yükümlülüğü getirmektedir.

Sözleşmenin bu maddesinde, siber ortamdaki çocuk pornografisinin üretilmesi, bulundurulması ve dağıtılmasıyla ilgili suçlar belirlenmiştir. Birçok ülkede, sözleşmeye paralel hükümlere yer verilmiştir. İngiltere'de internet yoluyla elde edilen çocuk pornografisine ilişkin fotograf ve materyallere sahip olmak suç sayılmaktadır.

2.6.4. Telif Hakları Ve Bağlantılı Hak İhlallerine Yönelik Suçlar

Sözleşmenin 10. maddesinde taraf devletlere fikri mülkiyet hakları ve telif haklarına ilişkin uluslararası alandaki mevcut anlaşmalarda geçen hususlar çerçevesinde, bilgisayar sistemlerinde ve internet sunucularında telif haklarını ihlal eden içerik bulundurmanın suç sayılması ile ilgili düzenleme yapma yükümlülüğü getirmektedir.

İnternetin işlevlerinden olan bilginin yayılması, telif haklarını ve telif haklarına ilişkin suçları doğurmaktadır. Bilginin, markanın, tasarımların, ürünlerin, projelerin yayınlandığı elektronik ortamdan alınarak kopyalanması, taklit olarak kullanılması ve pazarlanması mümkündür. Dolayısıyla bu durum, telif hakkına ilişkin ihlalin internet ortmaında yaygınlaşması ve yapılmasına neden olmaktadır.

Telif hakkı eser sahibinin emek ve fikir ürününü koruyan bir hak olup, eserin fiziksel yapıda olmasının şart olmadığı elektronik ortama aktarılmış olması eserin korunmayacağı anlamına gelmeyeceğinden tartışmalar sonrasında sözleşme kapsamına alınmıştır. Telif haklarının fiziksel ve elektronik yapıda olmasının parelel olması düşüncesiyle fiziksel yapıdaki telif haklarına ilişkin uluslararası kaynakların madde içeriğinde belirtilmiş olmasından anlaşılmaktadır.

2.7. Bilişim Suçlarını İşleme Yöntemleri

Bilişim suçları, klasik suçlarla işleniş amaçları açısından benzerlik göstermekle birlikte, yöntem ve araç açısından farklılıkları bulunmaktadır. Bu tip suçları işlemede araç olarak internet, bilgisayar, pos makinesi, cep telefonu ve diğer çeşitli teknolojik cihazın kullanılması bakımından klasik suçlardan büyük ölçüde farklılıklar göstermektedir. Bilişim suçları klasik suçlar gibi herhangi bir fiziksel mekâna gereksinim duyulmadan herhangi bir bilgisayar veya bir internet ağı üzerinden dünyanın herhangi bir yerinde bu suçu işleyebilmekte; kişilere, kurum ve kuruluşlara istedikleri yerde büyük zararlar verebilmektedir. Bilişim suçu günümüz dünyasında sürekli değişen ve hızla artan herhangi bir fiziki mekana ihtiyaç duymayan bir suç türü olmaktadır. Her an her yerde gerçekleşme durumu vardır. [155]

Bilişim suçlarına konu olan olayların neredeyse tamamına yakını aşağıda belirtilen yöntemlerden biri veya birkaçının birleşimi şeklinde meydana gelmektedir. Yani suçu işleyen kimseler, suçun işlenişi esnasında birden fazla yöntem ve tekniği bir

[155] Hüseyin Akarslan, **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2012, s.12.

arada kullanabilmektedir. Bu yöntemler bağlamında genel olarak bilişim suçları fiilleri içerisinde şu unsurları barındırmaktadır[156];

- İnternet kullanıcılarının bağlantısına açık olan web sitelerinin homepage (ana) sayfalarını silmek, istedikleri yere yönlendirmek veya sayfa yapısı ile oynamak,
- Erişime açık sitelerdeki içeriğe sızarak veri kopyalamak suretiyle veri çalmak, bilgi hırsızlığı yaparken ifşa ve deşifre olmamak adına var olan dosyaları değiştirmemek gibi birtakım önlemler almak,
- Erişime açık olan sitelerde tahribat yaratarak bu siteleri saldırılarla kullanılamaz hale getirmek,
- Virüs ve zarar verici benzer yazılımları şahıs ve kurumların bilgisayarlarına yükleyerek zararlar vermek, bu zararlı yazılımlar ile uzak sistemlere erişim sağlayarak fiziksel zararlar vermek, sisteme veya kullanıcıya kalıcı tahribatlar vermek,
- Bilgi hırsızlığı yaparak bir sonraki siber suçunda kullanmak üzere bilgiler elde etmek,
- Sanal ortamda yasal veya yasal olmayan faaliyetlerin propaganda alanı gibi kullanmak veya yasal olmayan faaliyetleri organize ve koordine eden bir merkez haline dönüştürerek kullanmak,
- Farklı yöntemlerle ele geçirerek kendilerine bağladıkları bilgisayarları (zombi veya köle bilgisayar olarak) kullanarak büyük çaplı hizmete erişim engelleme saldırılarında bulunmak,

[156] Bahaddin Alaca, "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle)", Yüksek Lisans Tezi, Ankara Üniversitesi Antropoloji Anabilim Dalı, Ankara, 2008, s. 56-71.

- Telif hakkı içeren materyallerle ve bilgisayar oyunlarıyla ilgili cracking yaparak yani mevcut yazılım koruma şifrelerini kırarak illegal kullanıma sunmak,

- Sanal alemi diğer kişilerin haklarını ihlal etmek suretiyle genel asayiş suçlarını (hakaret, tehdit vs.) işleme yeri gibi davranmak, sanal alemi spam amaçlı ve dolandırıcılık amaçlı kullanmak,

- Sanal ortamda çocuk pornografisi üretmek, depolamak, paylaşmak, erişime sunmaktır.

Günümüz dünyasında internetin her an yanımızda ve hayatımızıın tam merkezinde olduğundan dolayı, bu alanda insanlara ve kurumlara zarar verici nitelikte yazılımların arttığı da aşikârdır.

2.7.1. Bilgisayar Korsanlığı: Sistem Güvenliğini Aşarak Erişim Sağlama (Hacking)

Bilgisayar korsanları günümüzde yaygın olarak internet üzerinden diğer bilgisayarlara illegal erişim sağlamaktadırlar[157]. Bu illegal erişimi sağlarken de gerek farklı sistem açığı arama teknikleri kullanma, gerekse de farklı zararlı yazılımları programlayarak veya kullanarak sağlamaktadır. İllegal erişimi sistem güvenlik uzmanı veya admini (yöneticisi) fark edip müdahale edene kadar hacker, sistemden veri çalma, verileri silme ve sisteme zarar verme türlerinde illegal fiillerde bulunabilmektedir.

Bilişim sisteminin güvenlik duvarının kırılarak sisteme ulaşılması fiilinin yani yaygın tabirle hacking eyleminin en öne çıkan özelliği, bu fiili gerçekleştiren hacker diye anılan şahıslar tarafından kendi kontrollerinde gerçekleştirilmektedir. Yani fiilin her aşamasında bizzat kendisi bulunarak kendi kontrolünde bu eylemi gerçekleştirir. Bazı durumlarda güvenlik şifrelerinin çözülmesinde teknolojik imkanlar yardımıyla olasılık ve kombinasyon hesaplarını hızlı yapan teknikler kullansalar bile, sistemin içerisine girdikten sonra içeride kontrol hackerdadır. Bu fiil ile yapılan işlemler haberleşme hürriyetine müdahale kapsamında kişilik haklarına karşı yapılan fiillerdir.

[157] Türkiye Bankalar Birliği, **a.g.e**., s. 15.

2.7.2. Oltalama Saldırıları (Phishing Attacks)

Oltalama Saldırıları (Phishing Attacks); bilişim suçu işleyen kişilerin internet kullanıcılarının bilgilerini, verilerini ve kredi kartı bilgileri gibi hassas birtakım verilerini hazırladıkları sahte bir sayfa veya çeşitli farklı teknikle kullanıcının sahte siteye yönlendirilip hassas bilgilerini kendiliğinden girmesini sağlamayı amaçlayan saldırılardır.

Oltalama saldırıları, bilgisayar korsanlarınca günümüzde oldukça yaygın olarak kullanılan ve son dönemde giderek artan şekilde kullanılan bir yöntemdir[158]. İnternet kullanımının yaygınlaşması ile beraber online bankacılık işlemlerini artık bilgisayar hatta mobil uygulamalar aracılığı ile akıllı telefonlarımız üzerinden kolay ve hızlı şekilde yapabilmekteyiz. Ancak özellikle banka internet sitelerinin birebir aynısı yapılarak ve kullanıcıyı bu sahte siteye yönlendirmeye çalışarak işlenen phishing ismiyle uluslararası alanda yaygın olarak kullanılan bu yöntemde ciddi artışlar olmuştur. Bilgisayar korsanları tarafından da phishing yöntemi sıklıkla kullanılmakta ve bunun sonucu hesaba erişen bilgisayar korsanları haksız kazançlar sağlamaktadırlar.

Ayrıca hackerlar belirledikleri mağdurların e-mail hesaplarını veya kredi kartı bilgilerini ele geçirebilmek için mağdurlara bahse konu hizmeti sağlayan yerden geliyormuş gibi gösterdiği sahte bir form içeren dosyayı mail veya başka yöntemlerle mağdura ulaştırarak, mağdurun formu doldurup göndermesiyle birlikte hassas bilgilere ulaşarak haksız çıkar elde etmektedir. Oltalama saldırılarının büyük çoğunluğu banka hesap bilgilerini ele geçirme amacı gütmektedir. Bu bağlamda hedef kullanıcıların mail hesaplarına bankadan gelen bir e-posta gibi masum gözüken bir mail veya link göndererek akabinde de kullanıcıyı sahte hazırlanmış, ancak gerçekten dışardan bakıldığında bankaya ait internet sitesiymiş gibi gözüken bir siteye yönlendirerek bilgilerini çalmaktadırlar[159].

---

[158] Afyon Kocatepe Üniversitesi Bilgi İşlem Dairesi Başkanlığı, "Phishing (Oltalama) nedir?", (çevrimiçi) https://bim.aku.edu.tr/phishing-oltalama-nedir/, Erişim: 17 Ağustos 2019.

[159] Hakan Hekim, "Oltalama (Phishing) Saldırıları", **Siber Tehditler ve Sorunlar**, 2015, s. 66-69.

Oltalama saldırılarından kurtulmak için yapılması gerekenleri şu şekilde sıralamak uygun olacaktır: Gelen mail ve linkler iyi incelenmeli, şüpheli bağlantılara tıklanmamalıdır. Yanlışlıkla da girilse sitenin URL'si kontrol edilmeli ve kimliği doğrulanmamış yani "Https" bağlantılı güvenli olarak sertifikalandırılmamış sitelere girilmemeli ve kesinlikle kişisel bilgiler paylaşılmamalıdır. Ayrıca bilgisayar programları ve işletim sistemleri güncel olmalı ve güncel bir antivirüs yazılımı kullanılmalıdır.

2.7.3. Bilgisayar Virüsleri ve Solucanları (Computer Viruses and Worms)

Bilgisayar virüsleri, bilgisayar kodlama dillerinin imkânlarını kullanarak yazılan ve çeşitli yöntemlerle ağ veya USB bellek tarzı harici depolama birimleri üzerinden diğer bilgisayarlara bulaşan bir tip bilgisayar kodlaması ve programıdır. Virüslere kodlamayla bulaştığı hedef bilgisayarda nereye yerleşeceği ve ne zaman ne yapacağı, hangi verileri sileceği, kopyalayacağı, sisteme ne şekilde zarar vereceği belirlenmektedir. Genel olarak virüsler sisteme zarar verme üzerine kodlanırlar ve yayılabileceği kadar yayılıp verebileceği kadar çok sayıda sisteme zarar vermeye çalışırlar. En sık karşılaşılan virüs türü ".exe" uzantılı yani çalıştırılan kurulan dosyalarla bulaşan türüdür. Bu tür virüsler ".exe" uzantılı dosyalar her çalıştığında sisteme bulaşırlar ve yayılırlar. Bilgisayarlara virüs bulaşma yöntemleri arasında; e-posta üzerinden bulaşma, indirilen bir program üzerinden bulaşma, tıklanan bir link üzerinden bulaşma, oynanan bir oyun veya izlenen bir videodan bile sisteme virüs bulaşma şeklinde sayılabilir.

Bilgisayar solucanları da bir çeşit bilgisayar virüsü türüdür. Kendisini bir sistemden diğerine kopyalayarak yayılma konusunda çok iyidir ve bunu çok hızlı bir şekilde otomatik olarak yapar. Bilgisayarın sistemini ele geçirerek kendisini çoğaltmaya çalışır ve e-posta vb. uygulamaları kullanarak kendisini başka sistemlere de yayarak çoğaltmaya çalışır[160]. Bu bir domino tarzı hızlı bir şekilde ağ üzerinden yayılabilir. Sistemlerin ve sunucuların yavaşlamasına hatta kilitlenmesine yol açarak

[160] Joseph F. Gustin, **Cyber Terrorism: A Guide for Facility Managers**, The Fairmont Press, Georgia, 2003, s. 24.

ciddi zararlar oluştururlar. Kendisinin ve biraz daha değiştirilmiş kopyasını ağ üzerinden hızlıca dağıtarak kısa sürede çok sayıda sisteme bulaşıp zarar verme amacı taşırlar. Yayılmak için herhangi bir dosya veya taşıyıcı programa ihtiyaç duymadan bilgisayarın denetimini ele geçirerek, kendilerine bir yol bularak hızlı şekilde yayılırlar. Sasser solucanı ve Blaster solucanı geçmiş dönemde adı duyulan önemli solucanlardır.[161]

2.7.4. Truva Atı (Trojan Horse) Programları

Truva atı (Trojan Horse) yönteminde faydalıymış gibi görünen bir dosya veya program içerisine zararlı yazılım yüklenerek karşı bilgisayara bağlantı kurulur ve çeşitli bilgiler ele geçirilir.[162] Truva atı, ismini Truva savaşında şehri ele geçirmek için içerisine gizlice asker yerleştirilen bir at heykelinin şehre sokulması olayından almaktadır.

Truva atı programı virüs veya solucan gibi davranamaz ve kendisini çoğaltamaz, karşı bilgisayara bir sunucu açarak erişim kurulmasına yarar. Hedef bilgisayara bulaşan Truva atı yazılımı kendisini sistem dosyası veya faydalı bir işlem gibi göstererek gizler. Günümüzde bu yöntem sıkça kullanılmaktadır. Özellikle internetten çok sayıda download (indirme) işlemi yapıldığı için indirilen programlarda Truva atı programının olma ihitimali bulunmaktadır. Bu yüzden indirilen dosyaları antivirüs taramasından geçirmek önem arz etmektedir.

2.7.5. Fidye Amaçlı Yazılımlar (Ransomware)

Günümüzde popüler olan ve özellikle son dönemlerde oldukça sık kullanılan bu yöntem başta büyük kurumlar, şirketler olmak üzere tüm kullanıcıları tehdit etmektedir. Bu yöntemle sisteme sızan zararlı yazılımı kullanan suçlu, sistemdeki dosyaları ve belgeleri kitleyerek, belgelerin kurtarılması için mağdurdan ücret talep etmektedir.[163] Bu suçlular genellikle ifşa olmamak için fidyeyi, günümüzde oldukça

---

161 "Worm:Win32/Sasser.E" (çevrimiçi), https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Worm:Win32/Sasser.E&threatId=-2147461386, Erişim: 6 Eylül 2019.

162 "Truva Atı Virüsü Nedir?" (çevrimiçi), https://www.kaspersky.com.tr/resource-center/threats/trojans, Erişim: 6 Eylül 2019

163 "Fidye Yazılımı (Ransomware)", (çevrimiçi) https://www.eset.com/tr/ransomware/ Erişim: 7 Eylül 2019

yaygın olarak kullanılan kripto para birimlerinden Bitcoin ve türevi kripto paraları olarak anonim bir hesaba aktarılmasını talep etmektedir. Ancak fidye ödense dahi belgelerin kurtarılması kesin değildir. "Wannacry" ve "Notpetya" son dönem ünlü fidye yazılımlarındandır.

2.7.6. Klavye İşlemlerini Kaydeden Program (Keylogger)

Kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır[164]. Tanım olarak klavye işlemlerini kaydeden programlara yaygın kullanım ismiyle keylogger denir. Bu programlar çok küçük programlar olup ancak çok tehlikelidirler. Klavye işlemlerini kaydedip önceden kodunda belirlenen adrese yollarlar. Bu durum çok ciddi bir tehlikedir çünkü program yazdığımız herşeyi kaydedip suçlu kişiye göndermektedir. Hem özel hayatımızın gizliliği bağlamında hem de ticari ve bankacılık işlemlerinin güvenliği anlamında çok ciddi tehdit oluşturmaktadırlar. Sadece yazılım olarak değil, klavye altına yerleştirilen bir cihazla da gerçekleştirilebilen bu eylem çok ciddi bir güvenlik zaafiyeti yaratmaktadır. İnternet üzerinden kredi kartı bilgilerimizi girdiğimizde bu program tüm bilgileri rahatlıkla kopyalayabilmektedir. Günümüzde bazı şirketler güvenli ödeme yöntemi olarak telefonlara kısa mesaj göndermek suretiyle de daha güvenli bir sistem sunmaktadırlar. Aynı şekilde donanımsal olarak keyloggerlar banka ATM'lerinin klavyelerine de yerleştirilmek suretiyle kredi kartı bilgilerini çalma fiilinde kullanılabilmektedir.

2.7.7. Dağıtık Hizmeti Engelleme Saldırısı (Distributed Denial of Service Attack (DDOS)

Dağıtık Hizmeti Engelleme Saldırısı, Botnet isimli bir bilgisayar ordusu tarafından belirli bir sunucuya aşırı yüklenme yaparak hizmetin yavaşlamasını veya engellenmesini amaçlayan saldırılardır.[165] Botnet tanımlaması, bot bilgisayarlar, zombi bilgisayarlar veya köle bilgisayarlar olarak isimlendirilen bilgisayarların kurudğu ağdır. Çok sayıda zombi bilgisayar ile bir veya birden çok sunucuya

[164] Gürol Canbek ve Şeref Sağıroğlu, "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Üniv. Müh. Mim. Fak. Dergisi, C. XXII, No: 1, 2007, s. 126.
[165] "DDoS Nedir?", (çevrimiçi) https://www.chip.com.tr/haber/ddos-nedir-ddos-saldirisi-nasil-yapilir_66331.html Erişim: 7 Eylül 2019

yüklenerek yapılan saldırılardır. Sunucu bilgisayara Botnet tarafından çok sayıda istek gönderilerek, sunucu işlemez hale getirilmeye çalışılır.

Botnet yazılımları çeşitli yöntemlerle hedef bilgisayarlara yüklendikten sonra kullanılana kadar pasif bekler ancak kullanıldığı zaman hedef sunucu ip'sine çok sayıda istek göndererek sistemi kilitler, sunucu eğer geniş kapasiteli değilse çöker. Biz farkında olmadan bilgisayarımız bir botnete dâhil olabilir ve bir botnet saldırısında kullanılabilir. Özellikle bilgisayar başında değilsek ve bilgisayar başında olsak bile bilgisayarımızdan çok sayıda ping diye tabir edilen bağlantı çıkış talebinin farkına varamazsak ne olduğunu anlama imkânımız yoktur.

2.7.8. Sosyal Mühendislik Saldırıları

Bilişim suçlarında kullanılmakta olan en etkili yöntemlerden birisi de sosyal mühendislik yöntemidir. Sosyal mühendislik, normal şartlarda insanların tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatıdır. Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir[166]. Sosyal mühendislik yönteminde insanları aldatarak çeşitli bilgiler elde etmek suretiyle sisteme zarar verme, verileri çalma ve sistemi ele geçirme amacı vardır. Oltalama yapma, Spam postalar, telefonla arama ve mesaj gönderme gibi yöntemler en sık kullanılan sosyal mühendislik yöntemleridir.

2.7.9. İstek Dışı Alınan E-Postalar (SPAM)

Spam, intenet üzerinden çok sayıda kullanıcıya çeşitli içeriklerde kullanıcının istemi dışında genelde tanıtım amaçlı gibi gönderilen mesajlardır.[167] Bu spam mailleri gönderen kişilere de spammer denilmektedir.

Spammer olarak adlandırılan bu kişiler elde ettikleri mail adresleri ile bir veritabanı oluşturmak suretiyle çeşitli alanlarla ilgili reklam başta olmak üzere çeşitli içeriklerde postalar göndermekte veya bu elde ettiği veritabanını para karşılığı satmaktadır. Posta kutumuzu kontrol ettiğimizde hergün yüzlerce spam mail aldığımızı görebiliriz. Bu spam maillerin birçoğu da masum olmayıp genelde zararlı

[166] Ünal Tatar, "Sosyal Mühendsilik Saldırıları", **TÜBİTAK Bilgem 4. Ağ ve Bilgi Güvenliği Sempozyumu**, Kasım 2011, s. 9.
[167] "Spam Nedir?", (çevrimiçi), http://web.deu.edu.tr/sss/spam.html Erişim: 8 Eylül 2019

içerikli yazılım barındırmakta veya bizi aldatmak suretiyle sosyal mühendislik amaçlı gönderilmiş olmaktadır.

2.7.10. Hukuka Aykırı İçerik Sunma

Hukuka aykırı içerik sunma eylemi genel olarak yayınlanması yasak olan müstehcen, kişilik haklarına saldıran, telif haklarını ihlal eden ve çocuk pornografisi içeren içeriğin internet kullanıcılarının erişimine sunulmasıdır. Söz konusu içeriklerin sunulması değişik platformlarda icra edilerek gerçekleştirilmektedir. Hukuka aykırı içerik konusunda dünya genelinde sadece çocuk pornografisi ile ilgili ortak bir görüş vardır. Diğerleri ülkelerin mevcut yönetim şekilleri, siyasi yapıları, gelenek ve göreneklerine göre farklılık göstermektedir.

2.7.11. Sık Kullanılan Diğer Yöntemler

Bilişim suçlarını işleme yöntemlerinden en çok bilinenleri detaylı olarak inceledikten sonra diğer sık kullanılan tekniklerden şu şekilde bahsedebiliriz;

- **Gizlice Dinleme (Sniffing, Evaesdropping):** Bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak verilerin elde edilmesi yöntemidir[168]. Bu yöntemde, bir ağdaki veri trafiğini gizlice izleyerek veri toplanır. Bunun için kullanılan çeşitli yazılımlar mevcuttur. Evaesdropping yöntemi de bir çeşit gizli dinleme metodudur. Bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak ve kullandığı ağlara girilerek verilerin elde edilmesi yöntemidir.

- **Bilgi (Veri) Aldatmacası (Data Diddling):** Sisteme verinin yanlış girilmesi veya girilen verinin değiştirilmesine veri aldatmacısı denilmektedir[169]. Bilişim suçlarında kullanılan yaygın, basit ve güvenli bir suç yöntemidir. Bilgi Aldatmacası ile veri-işlem belgelerini bozarak, saklanan verileri özel olarak tasarlanmış cihazlar ile değiştirilmesi, bazı kayıtların iptali veya kontrol mekanızmasından gözardı edilmesi

[168] Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları", **Denetişim**, 2011, s. 78.
[169] **A.e**., s. 78.

yöntemlerden birkaçı sayılabilir. Mevcut bir ağ üzerinden bilişim sistemlerine giren şahısların güvenlik tedbirlerini ekarte ederek bu suçu işleyenler dışında verileri kaydeden, nakleden, şifreleyen, kontrol eden kişilerin de söz konusu şahıslardan olabileceği unutulmamalıdır.

- **Süper Darbe (Super Zapping) Sistemi:** Bu sisteme ait yazılımlar tüm güvenlik protokollerini atlatarak sisteme giriş yapabilen yazılımlardır. Bazı kullanıcıların, faydalı olabilecek bazı programların tüm güvenlik kontrollerinden geçtiğini bildiğinden dolayı bu açığı kullandığında büyük zarar verme noktasında imkan tanımaktadır[170]. Amerikan Bankasında çalışan bilgi işlem görevlisi müşterilerinden birinin hesabındaki paranın azaldığını fark etmesi üzerine Süper Darbe tekniğini kullandığı anda güvenlik aşamalarının devrede olmadığını farketmesi üzerine yakınlarının hesaplarına değişik tutarlarda para transferi gerçekleşmiştir.

- **Salam Yöntemi (Salami Technique):** Salam yönteminde, çok fazla sayıda kaynaktan, çok az sayıda değerlerin transferini esas almaktadır[171]. Genellikle Truva atı yazılımları kullanılarak birden çok banka hesabından fark edilmeyecek derecedeki küçük tutardaki paraların hukuka aykırı olarak belli bir hesaba aktarılmasıdır. Aktarılan para o kadar küçüktür ki hesap sahipleri ile banka yöneticileri fark edememektedir.

- **Artık Toplama (Scavenging) Taktiği:** Bilişim sisteminde bir işlemden geriye kalan bilgilerin analiz edilerek veya sistemin belleğinde bulunan, silinmiş bilgileri, gelişmiş metodlarla tekrar geri getirmeye "Scavenging" veya "Artık toplama" denilmektedir.

- **Tuzak Kapı-Arka Kapı (Trap Door-Back Door) Bırakma Yöntemi:** Sistemin yazılımını kuran şahıs tarafından, içine gizli bir biçimde koyulan virüs yazılımına Tuzak kapısı ya da arka kapı denilmektedir. Uzaktan iletişim metoduyla da sistem koruyucularını saf dışı bırakarak içeri girmesi

[170] Turhan, **a.g.e**., s. 52.
[171] Altunok ve Vural, **a.g.e**., s. 79.

mümkündür. Backdoor, bir yazılım veya sistemde veri giriş/çıkışı noktalarının dışında olan açık noktalara verilen genel bir isimdir[172].

- **Mantık Bombaları (Logic Bombs- Time Bomb):** Mantık bombaları, bilişim sistemlerinde kodlandığı ve devreye girmesi gereken uygun an oluşuncaya kadar zararlı bir fiilde bulunmayan ancak uygun an oluştuğunda zarar verici sonuçlar oluşturan programlardır[173]. Mantık bombalarının amacı sızdıkları sisteme zarar vermektir. Örneğin ilk kez Haziran 1998 tarihinde yayılan Güney Doğu Asya kökenli olan CIH (Çernobil) virüsü bir mantık bombası olarak adlandırılabilir. Belirli bir tarih veya zamanı bekleyip Çernobil Faciasının yıl dönümü olan her 26 Nisan ile her ayın 26. günü aktif duruma geçen bilinen bir sürümlerdendir. Bu yöntemler haricinde kullanıcıları aldatma sistemine dayanan Bukalemun (Chameleon) tekniği, yerine geçme (masqeradıng) yöntemi, korsan amaçlı yazılım kullanma, sql veritabanına kod enjekte etme gibi bilinen yöntemler de bulunmaktadır. Bilişim suçlarının günümüz hızla gelişen ve değişen bilgi ve internet çağında, bilişim suçu işleme yöntemlerinin ve tekniklerinin de sürekli değişim halinde olduğu aşikârdır bu bağlamda her geçen gün yeni bir teknik ortaya çıkabilmektedir.

2.7.12. Uluslararası Alanda Bilişim Suçları

Uluslarası alanda bilişim suçlarıyla ilgili tanımlamalar ve suç kategorilerinin belirlenmesinin yanısıra bilişim sistemleri güvenliği ülkelerin en önem verilen konularından biri haline gelmiştir. Bilişim sistemleri güvenliğinin sağlanması ve korunmasında kamu kurumlarına, özel sektöre, kamu ve özel sektör arasında işbirliğine, üniversitelere önemli görevler düşmekle birlikte, amaç bilginin erişebilirliğinin bütünlüğünün ve gizliliği korunarak siber güvenliği sağlamaktır.

Bilişim sistemleri güvenliğinin etkin şekilde sağlanabilmesi için bilişim suçlarıyla uluslararası alanda kapsamlı şekilde mücadele edilmesi gerekmektedir. Gün geçtikçe değişerek artan oltama, phishing, spam ve zararlı yazılımlar gibi birçok

[172] Keleştemur, **a.g.e**., s. 225.
[173] Altunok ve Vural, **a.g.e**., s. 79.

bilişim suçlarına karşı önlemlerin alınmasında ülke politikalarıyla birlikte uluslararası örgütlerin çalışmaları önemli ve gereklidir.

İnternetin global çapta çok büyük bir ağ sarmalı olması, suçla mücadele ve suçluları tespit etme hususunda çeşitli güçlükleri de yaratmıştır. Bu sebeplerden ötürü dünyada birçok devlet mevzuatlarını değiştirerek, yetmediği dönemlerde de yasalar çıkararak bilişim ile alakalı suçların tarifini yapmış ve bu suç ve suçlularla mücadele edecek birimler kurmuştur.

Yukarıda belirtilen bilişim suçu işlemede en sık kullanılan yöntemleri kullanma vasıtasıyla dünyanın herhangi bir yerinden çok uzak başka bir noktasına karşı bile siber saldırı gerçekleşbilmekte ve suç oluşabilmektedir. Yani bu husus kuramsal olarka incelendiğinde internette herhangi bir noktadan bir konumdan, ulaşılmaması gereken askeri ve politik iletişimler üzerinde yasadışı bilgi toplama operasyonlarının gerçekleştirilebileceğini göstermektedir. Günümüzde bu tür saldırıların ne zaman yapılabileceğini bilmemiz olanaksızdır. Bilişim suçu herhangi bir zamanda anlık olarak gerçekleşebilmektedir. Bu nedenden dolayı bu tür karşılaşılabilecek saldırılara zaman kaybetmeden karşılık vermek gerekmektedir.

2.8. Türkiye'de Bilişim Suçlarıyla İlgili Kanuni Düzenlemeler

Bilgisayar dünyasında yaşanan süratli gelişmelere eş güdümlü olarak ülkemizde bilgisayar, yaşamın her kısmında pozitif ve negatif yönüyle etkin bir şekilde kullanılmaya başlanmıştır. Bilgisayar ve internet kullanımı 2017 yılında 16-74 yaş grubundaki bireylerde sırasıyla % 56,6 ve % 66,8 iken, bu oranlar 2018 yılında sırasıyla % 59,6 ve % 72,9 olmuştur[174]. Bilgisayar ve internet kullanımınn tüm dünya ile paralel olarak ülkemizde de artmasıyla birlikte dünya çapında bu alanda ortaya çıkan suçlara ilişkin önlemler ve yasal düzenlemeler yapma ihtiyacı hasıl olmuştur. Bu bağlamda başta bilgisayar ve internetin bulunduğu yer olan ABD ve diğer geşilmiş ülkeler bilişim suçlarına karşı önlemler alma ve gerekli yasal düzenlemeleri yapma

[174] Halil Bayrak, "TUİK Türkiye'nin İnternet Kullanım Alışkanlıkları Raporu", 17 Ağustos 2018, (çevrimiçi) http://www.tuik.gov.tr/PreIstatistikTablo.do?istab_id=1615, Erişim: 12 Eylül 2019.

yoluna gitmişlerdir. Aynı zamanda Avrupa Konseyi ve diğer çok uluslu topluluklar da bu alanda taraf devletlere bazı yasal düzenlemeler yapma zorunluluğu getirmiştir.

Türkiye de bilişim suçlarıyla mücadele alanında dünyada önemli bir konuma sahiptir. Gerek 82 milyonluk nüfusuyla [175] gerekse de nüfusun internet kullanım oranıyla bu alanda öne çıkan ülkelerden birisidir. Türkiye'de birçok üniversitede bilişim ve teknoloji alanında önemli gelişmeler takip edilmekte ve özellikle son dönemde global çapta popüler olan yapay zeka konularında önemli çalışmalar yapılmaktadır. Bu bağlamda teknolojiyi ve interneti iyi kullanan bir ülke olarak, ülkemizde de bu alanda işlenen suçlarda artış gözlemlenmektedir. Gerek yurtiçine gerekse de yurtdışına yönelik siber saldırılar ülkemiz üzerinden veya ülkemize yönelik olarak yapılabilmektedir.

Türkiye ise gerek Avrupa Konseyi'nin Siber Suçlar Sözleşmesi'ndeki yükümlülüklerini yerine getirmek gerekse de bu alanda işlenen suçlarla etkin mücadele edebilme bağlamında çeşitli yasal düzenlemeler yapma yoluna gitmiştir. Bu yasal düzenlemeler kapsamında hem 5237 sayılı TCK'da bu alandaki suçları ayrı bir başlık altında toplayarak detaylandırmış hem de gerekli diğer hususlar için 23 Mayıs 2007 tarihinde, 26530 sayılı Resmi Gazete'de yayınlanan 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" gibi yeni kanunlar kabul etmiştir. Bu hukuki düzenlemeleri detaylı şekilde ilerleyen kısımlarda ele alacağız.

2.8.1. Bilişim Suçlarının Hukuki Boyutu

Ülkemizde bilişim suçlarına dair düzenlemelerin 90'lı yılların ilk zamanlarından itibaren mevzuatımıza yer bulmaya başladığı görülmektedir. Bilişim suçuna dair ilk düzenlemeler 765 sayılı TCK'nın, 06.06.1991 tarihli ve 3756 sayılı Yasa ile 'Bilişim Kapsamında Suçlar' ismiyle 525. maddeye a,b,c,d bendinde bulunan maddelerinde meydana gelen eklenmeleriyle meşru düzeyde bir boyut kazanmıştır.

[175] TÜİK verilerine göre; Türkiye'nin 31 Aralık 2018 tarihindeki nüfusu 82.003.882 kişiden oluşmaktadır.

Türk Ceza Kanunu'nda yapılmaya başlanan değişikliğin arkasından 5846 sayılı Fikir ve Sanat Eserleri yasasının 2. maddesi, 07.06.1995 tarihli ve 4110 s. yasa ile uygulanan tadille bilgisayar programları ve uygulama neticesi doğurması şartıyla bunlarda hazırlanma aşamaları da yapıt olarak kabul görerek, bilgisayar uygulamalarına yönelik fiiler de yasa yönünden suç sayılmıştır.

Sonrasında ise 15.01.2004 tarihli ve 5070 sayılı Elektronik İmza yasası ile e-imzanın yükümlülüğü onaylanmış ve yasanın 16. maddesinde düzmece elektronik imza oluşturmak ve kullanmak, 17. maddesi gereğince düzmece elektronik sertifikaların oluşturulması ve kullanılmasının cezalandırılacağı belirtilmiştir.

2.8.1.1. 5237 sayılı Türk Ceza Kanunu

01.06.2005 tarihli yürülüğe konulan 5237 sayılı Türk Ceza Kanunu'nda bilişim suçlarında "Bilişim Alanında Suçlar" bölümüne yer verilmiştir. 5237 sayılı TCK'daki "Bilişim Alanındaki Suçlar" Onuncu Bölüm'de yer almaktadır.

Kanunda "Bilişim sistemine giriş" (m.243), "Sistemin engellemesi, bozulması, bilgilerin yok edilmesi ya da değiştirilmesi" (m.244), "Banka veya kredi kartlarının kötüye kullanılması" (m.245) ve "Tüzel kişiler hakkında güvenlik tedbiri uygulanması" ise 246. maddede işlenmiştir.

"Nitelikli Hırsızlık" fiili ise 142/2-(e) maddesindeki çalma suçunun "bilgisayar sistemlerini kullanarak işlemek" ve "Nitelikli Dolandırıcılık" yan başlığıyla 158/1- (f) maddesinde bulunan dolandırıcılığa giren suçun "bilişim mekanizmalarının banka ya da kredi kurumlarının vasıta olarak kullanmak amacıyla işlenmesi" ağırlaştırıcı bir sebep olarak belirtilmiştir.

Yine, 5237 sayısındaki TCK'da "haberleşmenin gizliliğinin ihlali" (m. 132), "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması" (m.133), "özel hayatın gizliliğini ihlal" (m. 134), "kişisel bilgileri kaydetmek" (m. 135) ve "kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m. 136), "hakaret fiili" (m.125), "müstehcenlik suçu" (m.226) bilişim suçlarını kapsayan suç tipleridir.

Bilişim suçları ile mücadelede ceza hukukunun ve yargılamasının beraber ele almayla netice elde edilmesi olası olacaktır. Bilişim suçlarının milletler arası kalitede

olması nedeniyle kabahatin işlenmesi ve failin yargılanması açısından taraf olunan Avrupa Siber Suçlar Sözleşmesi önem kazanmaktadır. Sözleşmenin Milletlerarası İşbirliğiyle alakalı genel esaslar isimli 23. maddede "Taraf ülkeler birbirinden, bu sebeple belirti edilen şartlar genelinde, gerekli koordinasyonun sağlanarak uygun bir şekilde işbirliğine gidilmesi gerektiği belirtilmiştir." hükmü yer almaktadır. Düzenleme gereği, uluslararası işbirliğinin sağlanabilmesi için işbirliğine gidecek devletlerin mevzuatların birbirleriyle uyumlu olması ve teknik altyapılarının yeterli olması gerekmektedir.

2.8.1.2. Elektronik İmza Kanunu

23.01.2004 tarihli 5070 sayılı Elektronik İmza Kanununda elektronik imzanın hukuki ve teknik yönleriyle kullanmak amacıyla bağlantılı esası düzenlenmek ve e-imzanın hukuksal altyapısı, e-sertifikaların erişim sağlayıcılarının hareketi ile e-imzanın kullanım amacıyla bağlantılı kararlara yer verilmektedir.

Elektronik İmza Kanunu'nun 3. maddesi elektronik imzayı, "diğer bir elektronik bilgiye eklenmesi ya da elektronik bilgiye mantık yönünden ilişkisi tespit edilen ve kimlik doğruluğunu sağlama hedefiyle kullanılan elektronik veri" olarak tanımlanmış olup, imza sahibi kişi "elektronik imza meydana getirmek hedefiyle imza oluşturma amacıyla aracını kullanan reel kişi" olduğu ifade edilmiştir.

Elektronik İmza Kanunu'nun 5. maddesinde belirtildiği üzere "Güvenlikli olan elektronik imza, elimizle attığımız imza ile aynı hukuksal neticeyi doğurmaktadır." Fakat maddenin devamında "Kanun maddelerin resmiyetteki şekline veya zati bir kurala bağlı tuttuğu hukuksal iş ve işlemlerle banka güvencesi mektupları dışındaki teminat sözleşmeleri, güvenli olan elektronik imza ile gerçekleştirilmez." denilmiştir. Buradaki düzenleme gereği, tapu devir sözleşmeleri, araç alım ve satımları, mal düzeni sözleşmeleri, vasiyetname, evlenme gibi durumlar elektronik imzayla gerçekleştirilemez.[176]

[176] Uğur Özüdoğru, "BTK Siber Suç ile Mücadele Yöntemleri, Evrensel Uygulmaları ve Ülkemiz İçin Çözüm Önerileri", **Bilişim Uzmanlığı Tezi**, Ankara, Aralık 2011, s. 115.

EİK' nın 16. ve 17. maddelerinde adli suçlar, 18. maddesinde ise idari suçlar düzenlenmiştir. EİK' nın 16. maddesinde imza bilgilerin izin olmadan kullanılması düzenlenmiştir. Maddelerdeki metinde "Elektronik imzaları oluşturma hedefi ile alakalı bireyin rızası olmadan; imza bilgisi ya da imza oluşturma aracını elde edenler, verenler, kopyalayanlar ve bu araçlar üzerinden tekrardan oluşturan kişiler ile uygunsuz ele geçirilen imza üretme yollarını uygulayarak e-imza yaratılması gerekli adli ceza ile cezalandırlacağı ve adli para cezası uygulanabileceği şeklinde düzenleme yer almaktadır.

Kanunun 17. maddesinde düzenlenen diğer suç ve yaptırım ise elektronik sertifikalarda sahtekârlıktır. Madde metninde "Tam olmak üzere ya da kısmi olarak sahte elektronik sertifika oluşturan kişilerin ya da geçerli olarak yapılan sertifikaları taklit ve tahrif eden kişiler ile taklit edilen bu e-sertifikaları konudan haberi olarak kullanan kişilerin, gerekli hapis ve adli para cezası ile cezandırılacağı düzenlenmiştir. Bu alanda yetkili kişilerce işlenmesi ise ağırlaştırıcı sebep olmaktadır.

Kanunun 18. maddesinde düzenlenen idari para cezası ise kanundaki ilgili maddelerdeki yükümlülüklerini yerine getirmeyen elektronik sertifika hizmet sağlayıcısına getirilen tedbirler olup, Bilgi Teknolojileri Kurumu tarafından verileceği belirtilmiştir. Ayrıca kanunun 19. Maddesinde, bu kanun ile tariflenen suçlarla alakalı tüzel şahıslar ile alakalı TCK'nın 60. maddesindeki hükmüne bağlı olarak tüzel şahıslara özgü güvenlik önlemleri hükmolunacağı, ayrıca idari yönden para cezası gerektiren filler işlendikleri tarih itibariyle geriye doğru üç sene içerisinde üç defa işlenmesi hâlinde hizmet sağlayıcının tüzel bireyin etkinlik izninin iptal edileceği bildirilmiştir.

2.8.1.3. Elektronik Haberleşme Kanunu

10.10.2008 tarih ve 5809 sayılı Elektronik Haberleşme Kanunun 4. maddesinde İlkeler başlığı altında "alakalı merciler doğrultusunda e-haberleşme hizmetinin sunulmasında, bu konuda yapılacak düzenlemeler ile bilgi güvenliğini ve haberleşme gizliliğini gözetme" ilkesine yer verilmektedir. Elektronik Haberleşme yasasıyla BTK'ya bilgi güvenliğiyle iletişim gizliliğini gözetmek, izin alınmadan erişime karşı şebeke güvenliği sağlanması, kişisel bilgilerin korunması, haberleşmeye

yönelik olarak, milli güvenliğin ve kamusal düzenin veya kamusal hizmetin gerektiği ölçüde yapılması amacıyla mevzuatın öngördüğü tedbirlerin alınması görevi verilmiştir.

2.8.1.4. 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"

Türkiye'nin internet ile tanıştığı tarihten itibaren erişim engellemeleri ile ilgili gelişmeler dikkate alındığında, internet erişim engellemeleri ve içeriğe müdahalenin üç döneme ayrılabilir: Bunlar; 1993-2000 yılları arasındaki internet ile tanışma ve kullanımın yaygınlaşması dönemi, 2001-2006 yılları arasındaki hukuki düzenlemeler ile müdahale dönemi ve 2007 ve sonrası 5651 Sayılı Kanun çerçevesinde başlayan erişim engelleme dönemidir[177].

İnternet kullanım oranının ve etkinliğinin artmasıyla birlikte internette yer alan zararlı ve hukuka aykırı içeriklerin engellenmesi söz konusu olmuştur. Söz konusu müdahalelerin, erişimin engellenmesinin, internet konusuna müdahil olma yetkisini verdiği bir kanun maddesine dayanmaması, genel hükümler çerçevesinde bu engellemelerin yapılması tartışmalara yol açmıştır. Bu tartışmalar ve artan bilişim suçlarının önlenmesi amacıyla 5651 sayılı Kanun düzenlenerek 04.05.2007 tarihinde yürülüğe girmiştir.[178]

5651 sayılı yasayla içerik, yer, erişim ve toplu kullanma sağlayıcılarının sorumluluk ve yükümlülükleriyle internet dünyasında yapılan intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı maddeleri kullanmayı kolaylaştırmak, sıhhat için tehlike arz eden maddeleri temin etmek, fuhuş yaptırmak ve kumar oynatmak amacıyla yer temin etme, 5816 sayısında Atatürk aleyhine işlenen suç ile ilgili kanun üzerinde bulunan ve 7258 sayısında futbol ve başka spor dallarında bahis, şans oyunları düzenlemeleri ilgili yasada bulunan suçların yayınlara erişimin engelleneceği bildirilmiştir.

---

[177] Türkay Henkoğlu ve Bülent Yılmaz, "İnternet Erişim Özgürlüğünün Kısıtlanması: Türkiye Üzerine Bir Değerlendirme", **Bilgi Dünyası**, C. XIV, S: 2, 2013, s. 219.
[178] Özüdoğru, **a.g.e.**, s. 114.

2.9. Dünyada Bilişim Suçlari İle Ilgili Düzenlemeler

Dünya çapında çoğu ülke halen kendini yenilemekte olan ve her geçen gün yeni bir saldırı tarzı üzerinden bir bilişim suçunun işlenme olasığını gördüğü için bu alanda uzman yetiştirme ve bu suçlarla mücadele eden özel birimler kurma yoluna girmiştir. Bu kapsamda yeni kanunlar çıkarmış ya da mevcut kanunlarında düzenlemeye gitmişlerdir. Bu kısımda diğer ülkelerde bilişim suçlarıyla mücadele yöntemleri ve konuyla ilgili yapılan kanuni düzenlemeler, oluşturulan özel birimler gibi husulara değineceğim;

2.9.1. Amerika Birleşik Devletleri (ABD)

ABD, bilgisayarın bulunduğu, bununla ilgili teknolojik araştırma-incelemelerin yapılıp sonuçlarının ortaya çıktığı ve bilgisayarların ağ olarak birbirleri ile bağlanarak internetin geliştirildiği ülkedir.

ABD California eyaletinde bulunan "Silikon Vadisi" olarak adlandırılan bilgisayar, internet, yazılım, kodlama ve bilişim sistemleri alanında dünyanın en büyük şirketleri yer almaktadır. Bu şirketlerin değerleri 100 milyarlarca dolar olup bugün tüm dünyaya teknoloji desteği sunan öncü şirketlerdir. Bu şirketler arasında Google, Apple, Microsoft ve Oracle sayılabilir.

Bilgisayarın anavatanı olarak sayılan ABD doğal olarak ilk olarak suistimallerle karşılaşan ve bu suistimallere karşı mücadeleyi başlatmış olan ilk ülke olmuştur. ABD bilindiği üzere eyaletlerden oluşmaktadır. Bu eyaletlerin kendine özgü yasaları bulunmakla birlikte tüm ABD'yi kapsayan kanuni düzenlemeler de bulunmaktadır.[179]

Bilişim suçlarıyla ilgili bu suçları işleyebilecek kapasitede olan, bu konuda gerekli bilgi ve yeteneğe sahip Hacker olarak tabir edilen şahısların da yoğun olarak bulunduğu ülkelerin başında gelen ABD, konuyla ilgili gerekli ve kapsamlı yasal düzenlemeleri yapmış ve bu suç türleriyle mücadele eden özel birimler kurmuştur.

[179] Levent Kurt, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yayınları, 2005, s. 29.

ABD'de bilişim suçlarına karşı mücadele etmek için özel birimler bulunmaktadır. FBI (Federal Bureau of İnvestigation) içerisinde kurulan özel bir birim olan National Infrastructure Protection Center (Ulusal Sızma Engelleme Merkezi), Amerika Bilgi Teknolojileri Kurumu (Information Technology Association of America)[180], Amerikan Güvenlik ve İstihbarat Kurumu Homeland Securty'e bağlı The National Infrastructure Coordinating Center (NICC) [181] gibi özel oluşturulmuş birirmler bu alanda danışmanlık ve suç tespit faaliyeti yürütmektedir.

ABD tarafından 1996 yılında yayınlanan icra emrinde "Commision of Critical Infrastructure Protection" (Kıritik Altyapı Koruma Komisyonu) ismiyle başkana bağlı özel bir komisyon oluşturmuştur. Komisyon özellikle acil durumlarda başta telekomünikasyon ve iletişim ağları olmak üzere kritik altyapıların korunmasıyla ilgili gerekli çalışmaları yapmak üzere görevlendirilmiştir.[182]

FBI, Ulusal Sızma Engelleme merkezini yanısıra, siber suçlara karşı da Cyber crime Squad isimli bir yapı oluşturarak bu alandaki suçları yakın takibe almıştır. "Computer Crime Squad" bilgisayar sistemlerine girme ve buna benzer suçları izlemek amacıyla oluşturulmuştur. Ayrıca ABD Adalet bakanlığı tarafından "Computer Crime and Intellectual Property Section" ismiyle oluşturulan bu kısım konu ile alakalı çeşitli çalışmalar yapıp destek olmaktadır.[183]

ABD'de bilişim suçlarıyla ilgili gerekli yasal düzenleme kapsamında çok sayıda kanun çıkarılmıştır, bu kanunlar ise şunlardır;

- 18. U.S.C. 1029 sayılı "Erişim cihazlarıyla ilgili dolandırıcılık ve ilgili faaliyetler" başlıklı yasa,
- 18. U.S.C. 1030 sayılı "Bilgisayarlarla bağlantılı olarak dolandırıcılık ve ilgili faaliyetler" başlıklı yasa,

[180] (çevrimiçi) https://www.bloomberg.com/profile/company/0363934Z:US, Erişim: 10 Temmuz 2019.
[181] (çevrimiçi) https://www.dhs.gov/cisa/national-infrastructure-coordinating-center, Erişim: 11 Temmuz 2019.
[182] (çevrimiçi) http://naturalenvironmentsociety-arizonasouthwest.com/references/PDFs/presidential-actions/outline1/Clinton_EO_13010.pdf, Erişim: 8 Temmuz 2019.
[183] Hüseyin Çeken, "ABD'de Siber Suçlar", http://www.jura.uni-sb.de/turkish/HCeken.html, Erişim: 10 Temmuz 2019.

- 18. U.S.C. 2511 sayılı "Telgraf, sözlü veya elektronik haberleşmelerin durdurulması ve açıklanmasını yasaklayan" yasa,
- 18. U.S.C. 2701 sayılı "Kaydedilmiş haberleşmeye illegal Erişim" başlıklı yasa,
- 18. U.S.C. 2702 sayılı "Müşteri iletişimlerinin veya kayıtlarının kasten açıklanması" başlıklı yasa,
- 18. U.S.C. 2703 "Müşteri iletişiminin veya kayıtlarının hangi şartlarda açıklanması gerekliliğini düzenleyen yasalardır."[184]

2.9.2. Rusya Federasyonu

Bilgisayar üzerinden gerçekleştirilen suçlarla ilgili olarak Rusya'da 1999'a kadar herhangi bir düzenleme bulunmamaktaydı, fakat 1997 yılında G-8 ülkerinin İçişleri ve Adalet Bakanları toplantısında onaylanan duyuru ile "Ülkesel Koordinasyon Yerleri" ayarlanması kararlaştırılmıştır. Bu bağlamda Rusya'da koordinasyon yeri oluşturulmuştur. Yargı organları, güvenlik ve diğer ülkeler ile temas halinde bulunan bu bölüm "R Dairesi" olarak adlandırılmıştır.[185]

Günümüzde Rusya dünya siyasetinde politika belirlemede etkin ülkelerden birisidir. Bilişim sistemleri kapsitesi ve teknolojisi olarak da dünyanın önde gelen ülkelerindendir. Rusya'da bilişim suçları işleme kapasitesi bulunan hacker olarak tabir edilen internet korsanları aktif bir şekilde faaliyetlerini sürdürmektedirler.

Rusya'da son yıllarda işlenen bilişim suçları oranlarında ciddi artış gözlemlenmektedir. Bu konuyla ilgili olarak İçişleri Bakanlığı yetkilisi Alexei Moşkov, Şanghay İşbirliği Örgütü ve BRICS ülkelerinin katılımıyla Moskova'da düzenlenen iş forumunda, Rusya'da son yıllarda artan siber suçlar hakkında açıklamalarda bulunmuştur. Moşkov, telekomünikasyon ve bilgi alanlarında

[184] (çevrimiçi) https://www.law.cornell.edu/uscode/text/18/1030, Erişim: 6 Temmuz 2019.
[185] (çevrimiçi) http://www.turkhukuksitesi.com/makale_154.htm, Erişim: 8 Temmuz 2019.

dolandırıcılık yapma amaçlı işlenen siber suçların Rusya'da son 4 yıl içerisinde 6 katına çıktığını bildirmiştir.[186]

Rusya İçişleri Bakanlığı, bu tür Internet kullanılarak işlenen suç ve bu suçu işleyenlerin takibinin kolaylaşması ve delillerin muhafazası için internet servis ve erişim sağlayıcılarla koordine olarak bu kayıtları saklama ve gerektiğinde yetkili makamlarla paylaşma şartı koymuştur.

RF Ceza Kanununda 242, 272, 273 ve 274. maddelerde bilişim suçları tanımlanarak yasallaştırılmıştır. Bu bağlamda bilişim suçu anlamında müstehcen içerik üretme ve sunma, sistemlere illegal erişim ve müdahale, zararlı yazılım üretme gibi suçlar düzenlenmiştir.

Rusya'da bilişim suçlarıyla mücadelede son dönemde dikkat çeken bir konu olarak şunu örnek vermek mümkündür; 2011 yılında ünlü anti-virüs firması Kaspersky Lab, kapsamlı ve bir o kadar da kötü amaçlı yazılım olarak bilinen Lurk trojenini kullanarak sistemlere giren hacker grubunu tespit ederek bunu yetkili makamlarla koordineli bir şekilde takibini yaparak bu hacker çetesinin yakalanmasını sağlamıştır. Bahse konu hacker çetesi kullandıkları bu ileri seviye trojen ile mağdurların hesaplarından yüklü miktarda para transferi yapmıştır.[187]

2.9.3. İngiltere

İngiltere, ABD'den sonra bilgisayar ve internet kavramlarının ilk olarak kendisine yer bulduğu ülkelerden biridir. Günümüzde BM'nin 5 daimi ülkesinden biri ve küresel politikada önemli bir aktördür. Bu bağlamda bilişim suçlarının da geliştiği ve ciddi sorunlar yarattığı ülkelerden biri haline gelmiştir.

29.08.1990 tarihinde düzenlenen "Bilgisayarın Suistimal Edilerek Kullanılması Yasası (Computer Misuse Act)", İngiltere'de bilişim suçlarını düzenleme alanında başı çekmektedir. Bununla beraber bu suçları düzenleyen ek yasalar çıkarılarak başta çocuk pornografi alanında bilişim suçlarını düzenleyen bu yasa

[186] (çevrimiçi) https://www.haberler.com/rusya-da-4-yilda-siber-suclarin-sayisi-6-kat-artti-9700882-haberi/, Erişim: 7 Temmuz 2019.
[187] (çevrimiçi) http://www.hurriyet.com.tr/teknoloji/rusyanin-en-buyuk-siber-suc-grubu-cokertiliyor-40114672, Erişim: 07 Temmuz 2019.

haricinde özellikle pornografi alanında ve ekstrem pornografi ile ilgili düzenlemeler yapılmıştır. Bunun harici mevcut yasalarda da çeşitli düzenlemeler ve eklemeler yapılarak mevzuata yerleştirilmiştir.[188]

Bilgisayarın Suistimal Edilerek Kullanılması Yasası'nın ilk maddesinde, özetle program veya bilgisayar sistemine hiçbir yetkisi olmadığı halde erişmek suç sayılmıştır. Bahse konu suç için hapis veya para cezası veya hem hapis hem para cezası 6 ayı geçmemek şartıyla birlikte verilebilecektir.

Bir sisteme izinsiz olarak giriş yapmaya çalışırken başarısız olunsa dahi ve izinsiz olarak yapılan erişimde sisteme zarar verilmese de suç oluşmakta ve bu fiil suç sayılmaktadır. Farklı birisine ait özel verilerle sisteme illegal bağlantı kurmak, bilgileri kopyalamak gibi fiiller bu kapsamdadır.

Aynı şekilde Bir sisteme izinsiz olarak giriş yapmak, verileri kopyalamk, değiştirmek, silmek, sisteme zarar vermek fiileri de suç olarak düzenlenmiştir. Bu bağlamda zararlı yazılım (solucan, virüs, trojan vb.) kullanmak da ayrıca belirtilmiştir.

Veri Koruma Kanunu, İngiltere'de bilişim sistemleri aracılığı ile kişilere ait verilerin haksız elde edilmesini suç kapsamına almıştır. Bu yasa ile veri sahibinden izinsiz dosyalarla alakalı herhangi bir fiilde bulunulması kanunda suç sayılmıştır. Bu hususta erişim sağlayıcı kuruluşalara da kişisel verilerin korunması hususunda ek yükümlülükler getirilmiştir.

Sanal ortamda bilişim sistemleri vasıtasıyla yapılan sahtecilik ve dolandırıcılık suçları da ayrıca Bilgisayarın Kötüye Kullanılması Hakkında kanun kapsamında cezalandırılır. Bilişim suçları kapsamında bir internet kullanıcısının kredi kartı bilgilerini ve banka hesap bilgilerine illegal erişip fiiller de bulunmak da bu kapsamda dolandırıcılık başlığı altında suç olarak tanımlanmıştır.

2.9.4. Almanya

Almanya'da bilişim suçları Türkiye'ye benzer şekilde mevcut Ceza Kanunu kapsamında yasallaştırılmıştır. Fakat farklı maddelerde ayrı ayrı düzenlenmiş ve bizim

[188] (çevrimiçi) http://www.yttlaw.com/bilisim-suclari-ve-cezalari/, Erişim: 01 Temmuz 2019.

Ceza Kanunumuz gibi belli bölümde düzenlenmemiştir.[189] Ancak konuyla ilgili özel çıkarılan kanunlar da mevcuttur.

Alman Ceza Kanununun Onbeşinci Bölüm, "Özel hayat ve özel hayatın gizli alanının ihlâli" başlığı altında madde 202a'da - veri casusluğu, madde 202b'de- verilerin iletilirken ele geçirilmesi, madde 202c'de - veri casusluğunun ve verilerin iletilirken ele geçirilmesinin hazırlığı suç olarak düzenlenmiştir. Ayrıca On Üçüncü Bölüm, bireyin cinsel davranışını tayin hakkına (cinsel dokunulmazlığa) karşı suçlar başlığı altında, madde 184b - çocuk pornografisi içeren yazılar yayma, edinme veya bulundurma fiilleri suç olarak tanımlanmış ve cezalandırılmıştır.[190]

İnternet yayınları ile ilgili ceza sorumluluğunun şartları 13 Temmuz 1997 senesinde onaylanan Teleservisler Kanunu ile belirlenmiştir. [191] İnternet içerik sağlayıcıların sitede bulunan içerikten sorumlu oldukları belirtilmiştir. İnternet erişim ve servis sağlayıcıların çeşitli yükümlülükleri düzenlenmiş ve konusu suç teşkil eden içeriğin servis sağlayıcı tarfından kaldırılması gerekliliği düzenlenmiştir.

2.9.5. Fransa

Bilişim suçları, Fransa'da ayrı bir kanunla belirlenmeden önce mevcut Ceza Kanunu'ndaki diğer suçlarla ilişkilendirilmek suretiyle bu alanda mücadele edilmeye çalışılmaktaydı. Bilişim suçları, mevcut Fransa Ceza Kanunu'ndaki asayiş suçları (hırsızlık, dolandırıcılık vb.) ve diğer suçlar başlığı altında değerlendirilmekteydi.[192]

Ancak bu durumun yetersiz olduğu anlaşılınca mevcut ceza kanununda 5 Ocak 1988 tarihli ve 88-19 sayılı yasayla ilk kez bilişim suçlarıyla alakalı yasa çıkarılmıştır. Bu yasada bilişim sistemlerine yetkisiz erişim, sistemde kalma, sisteme zarar verme, verilerin işleyişini bozma, veri kopyalama-silme, dijital verilerde sahtekârlık yapma ve dağıtma gibi suç türleri düzenlenmiştir. Daha sonra aynı içerik 1 Mart 1993

[189] (çevrimiçi) http://www.yttlaw.com/bilisim-suclari-ve-cezalari/, Erişim: 2 Temmuz 2019.
[190] "Alman Ceza Kanunu", çevrimiçi, http://www.hukukmarket.com/images/contentspdf/143772.pdf, Erişim: 12 Temmuz 2019.
[191] (çevrimiçi) http://www.yasad.org.tr/tr/Sayfa/bilisim-hizmetleri-kanun-tasarisi, Erişim: 11 Temmuz 2019.
[192] Yener Ünver, **"**Türk Ceza Kanununun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. LIX, S: 1-2, 2001, s. 71.

senesinde kabul edilen Yeni Fransız Ceza Kanunu'nda mala karşı işlenen suçlar başlığı ile ayrı bir bölümde yürürlüğe girmiştir.[193]

Bilişim alanındaki hızlı ilerleme ve internetin dünyada hızla yayılmasına paralel olarak bilişim suçlarının sayısının artması, popüler olması, ciddi maddi zararlara yol açtığı görüldükçe, bu suç türleriyle mücadele önem kazanmıştır. Bu bağlamda ülkeler yeni yasalar çıkarmak zorunda kalmıştır. Fransa'da bu hususta, 1978 senesinde 78-17 sayılı bilgi, belge ve telif haklarının karunmasına ilişkin yasa ve akabinde 1985 senesinde 85-660 sayılı görsel-işitsel materyallerin telif haklarına yönelik yasa çıkarılmıştır.[194]

Fakat bu düzenlemeler bilişim ile ilgili bütün fiilleri içermediği için, 1988 senesinde 88-19 sayılı "Bilgisayar Dolandırıcılığı" başlıklı yasa çıkarılmıştır.[195] Bu yasada, sistemlere yetkisiz erişim, sistemde kalma, sisteme zarar verme, verilerin işleyişini bozma, veri kopyalama-silme, dijital verilerde sahtekârlık yapma ve dağıtma gibi suç türleri düzenlenmiştir. [196]

Son olarak üzerinde 29.05.2019 tarihinde değişiklik yapılan güncel Fransız Ceza Kanunu'nda (**CODE PÉNAL**) bilişim suçlarıyla ilgili 7. Kitap Küçüklere ve Aileye Karşı Suçlar (Chapitre VII: Des atteintes aux mineurs et à la famille) başlığı altında 227-23. maddesinde çocuk pornografisi içerikli materyalin üretimi, depolanması, dağıtımı suç olarak tanımlanmıştır. Yaş sınırı ise 15 olarak belirlenmiştir. Yasanın 323-1, 323-2 ve 323-3. maddelerinde, "bilgiyi otomatik işleyen sistemlere yönelik saldırılar" başlığı altında bilgisayar sistemlerine yetkisiz erişim, sistemde kalma, sisteme zarar verme, verilerin işleyişini bozma, veri kopyalama, verileri tahrip etme, değiştirme ve silme, bu sistemler üzerinden dolandırıcılık yapma fiilleri suç olarak tanımlanmıştır. [197]

---

[193] (çevrimiçi) http://www.yasad.org.tr/tr/Sayfa/bilisim-hizmetleri-kanun-tasarisi, Erişim: 12 Temmuz 2019.
[194] (çevrimiçi) http://www.yttlaw.com/bilisim-suclari-ve-cezalari/, Erişim: 3 Temmuz 2019.
[195] Dijital Platform İletişim Hizmetleri A.Ş., **İletişim Şurası Notları,** Ankara, 20-21 Şubat 2003, s. 255.
[196]Kurt, a.g.e., s.102.

[197] "Fransız Ceza Kanunu"**,** çevrimiçi, http://codes.droit.org/CodV3/penal.pdf, Erişim: 12 Temmuz 2019.

2.9.6. İsviçre

İsviçre'de teknolojik suçlarla ve siber terörizmle mücadeleye ilişkin, "Haksız Rekabet Yasası" ve "Federal Ceza Yasası" olmak üzere 2 federal yasa mevcuttur. "Haksız Rekabet Yasası"nın içeriği ticari saikle bu alanda işlenen fiiller ile ilgilidir. "Federal Ceza Yasası" ise illegal yöntemlerle veri çalma, veri edinme veya verileri değiştirme, tahrip etme ve yok etme fiillerini suç olarak düzenlemektedir.[198]

Federal ceza yasasında, bilişim suçlarına ilişkin az da olsa düzenleme mevcuttur. Bahse konu yasa içeriği internet sürelerine ilişkin düzenlemelerle ilgilidir. "Haksız Rekabet Kanunu", bahse konu bilişim suçları konusundaki diğer düzenlemelerin yer aldığı içeriklerden oluşmaktadır. Bu kanunun içeriğinde daha çok ticari amaçlı bilgisayar suçları vardır.[199]

2.9.7. İtalya

547 Sayılı yasa ile 1993 senesinde İtalya, bilişim suçları konusunda ilk yasal düzenlemesini yapmıştır. Bilişim ile ilgili gerçekleştirilen birçok eylem, İtalya'nın Ceza Kanunu'ndaki bazı maddelere yapılan eklemelerle suç olarak tanımlanmıştır.

Bilişim suçlarına ilişkin önlem alma amaçlı 1998 senesinde İtalyan polisi bünyesinde iletişim güvenliği birimi kurulmuştur. Bu birim ülke çapında başta interent üzerinden çocuk pornografisi, terörizm gibi konular olmak üzere bu alandaki suçlarla mucadele etmektedirler.[200]

2.10. Çok Uluslu Topluluklarda Bilişim Suçları İle İlgili Düzenlemeler

2.10.1. Avrupa Birliği

Avrupa Birliği Bilişim Politikası'nın ana özellikleri başta 1987 yılında Yeşil Kitap'ta bulunmaktadır. Bu dökümanda "bilişim sistemleri için birlikte ortak bir alanın yaratılması ve işbirliği çerçevesinde bu alandan faydalanılması amaçlanmıştır.[201] İnternet ile beraber ortaya çıkan problemler ve bu alanda yasal düzenleme ihtiyacı

---

[198] Ünver, **a.g.e**., s. 77.
[199] Kurt, **a.g.e.,** s. 112.
[200] Dijital Platform İletişim, **a.g.e**., s. 255.
[201] "Avrupa Birliği Bilişim Politikasi ve Türkiye'nin Uyumu", http://www.ab.org.tr/ab05/tammetin/89.doc, Erişim: 15 Nisan 2012.

1996 senesinde Bologna (İtalya) şehrinde gerçekleşen bakanlar toplantısında konuşulmuştur.[202]

Daha sonra bu amaçla Avrupa Komisyonu, çalışma ekibi kurulmak suretiyle bu alandaki suçlara karşı çalışma yapılmıştır. Bu ekipte internet servis ve içerik sağlayıcılar da yer almıştır. Bu ekip daha sonra çocuk istismarı ve internet konulu toplantıda olası önlemler üzerinde çalışmıştır.[203]

1997 senesinde internetteki zararlı içerik ile alakalı Avrupa Konseyi'nin toplantısı gerçekleşmiş ve toplantı sonunda "Bonn Açıklaması" ilan edilmiştir. Yayınlanan bu deklarasyonda internet servis, erişim ve içerik sağlayıcıların yasal tanımlarının netleştirilmesinin öneminden bahsedilmiştir.[204]

Dijital imzalar ile kişilerin kendi eliyle attığı imzaların aynı konumda kullanılması için 1999 senesinde Avrupa parlementosu tavsiye karar almıştır. Bu kararda ıslak imzanın özelliklerinin dijital imza için de kullanılabilmesi ve bu konuda üye ülkelere farkındalık oluşturma amacı vardır.

Fransa'nın Strasbourg şehrinde 29 Haziran 2001 tarihinde Avrupa Birliği Bilişim Politikası çerçevesinde kabul edilen Avrupa Siber Suçlar Konvansiyonunda, taraf ülkelerin bilişim suçları alanında gerekli çalışmaları yapması ve yasal mevzuatlarını düzenlemeleri kararı alınmış aynı zamanda bu alanda sıkı işbirliği öngörülmüştür.

Bunların yanında Siber Suçlar Konvansiyonu'nda bilişim suçları bölümlere ayrılarak işlenmiştir. Bilgisayar sistem ve verilerinin bütünlüğüne, güvenliğine karşı işlenen yetkisiz erişim ve veri tahribatı suç olarak belirtilmiştir.

---

[202] Kayıhan İçel, Füsun Sokullu Akıncı, Yener Ünver, R.Barış Erman ve Hasan Sınar, **Avrupa Birliği'ne Uyum Sürecinde Türk Ceza Hukuku**, İstanbul, Beta Yayınevi, 2000, s. 117.
[203] A.e., s. 118.
[204] Clive Walker ve Yaman Akdeniz, **The Internet, Law and Society**, Ocak 2001, s. 48

İçerikle alakalı suçlar bölümünde; telif hakları, çocuk pornografisi işlenmiş Bilgisayarlar ile bağlantılı suçlar başlığında; sahtekarlık ve dolandırıcılık suçları işlenmiştir. [205]

2.10.2. Avrupa Konseyi

1980'li yılların sonlarına doğru Avrupa Konseyi bu konudaki ilk çalışmasını yapmıştır. Ceza kanunları ile nasıl bir yasal düzenlemenin gerekli olduğunu belirleyerek; güvenlik kavramları ile kişisel hak ve özgürlüklerin nasıl dengelenmesi gerektiği ve uyuşmazlıkların nasıl giderileceği Konsey'in bu çalışmayı başlatmasındaki en büyük amaç olmuştur.

Avrupa Konseyi'nin çalışmaları sonucunda bilişim suçlarının nasıl engellenebileceği, bu suçların soruşturulması, bilgisayarların muhafaza altına alınıp incelenmesi ve bu suçların araştırılması konuları belirlenmiştir ve bu hususlar taraf devletlere 1989 senesinde bildirilmiştir.[206]

Avrupa Konseyi bu konu hakkında diğer taslağını 1995 yılında yayınlamıştır. Bu taslakta bilişim suçlarının ceza muhakemleri kapsamında soruşturlma usulleri tartışılmış ve bu bağlamda yeni düzenlemeler yapılması gerektiği bildirilmiştir.

2.10.3. Birleşmiş Milletler

1985 tarihinde ilk defa Birleşmiş Milletler bünyesinde bilişim suçlarına ilişkin harekete geçilmiştir. "7. Suçtan Korunma ve Suçluların Rehabilitasyonu" toplantısının akabinde açıklanan "Milan Eylem Planı"nda bilişim suçları da ele alınmıştır.

14 Aralık 2000 yılında İtalya'da BM desteğiyle yapılan "The Challenge of Borderless Cyber Crime" (Sınıraşan Siber Suçlar Çıkmazı) panelinde bilişim suçları tartışılarak bu konuyla alakalı farklı tarzda çözüm önerileri geliştirilmeye çalışılmıştır. Daha sonra "Asya-Pasifik Bölgesel İştirakçileri" panelinde bilgisayar suçlarına dikkat çekilerek teknolojik gelişimin etkileri belirtilmiştir. Bu panellerin 12. toplantısında Kanada adına katılan temsilci bilgisayar ile bağlantılı suçlarla alakalı önlemlerin yer

[205] (çevrimiçi) https://ab.org.tr/ab05/tammetin/89.doc, Erişim: 15 Temmuz 2019.
[206] "United Nations Manual on the Prevention and Control of the Computer-Related Crime", (çevrimiçi) http://216.55.97.163/wp-content /themes /bcb /bdf /int_regulations /un/ Comp Crims_UN_Guide.pdf, Erişim: 12 Temmuz 2019.

aldığı bir çalışmayı toplantıda bulunanlara sunmuş ve üye ülkeler bahse konu taslağı kabul ederek bilişim suçlarına karşı mücadele edilmesini kararlaştırmıştır.

2000 yılında yapılan toplantıda da taraf devletlerin bilişim sistemlerine yetkisiz erişim, sistemi işlemez hale getirmek, içeriği silmek gibi fiillerin suç sayılarak yasa ile düzenlenmeleri tavsiye edilmiştir.[207]

2.11. Türkiye ve Dünyada Bilişim Suçları İle İlgili Yaşanmış Örnekler

Bilgisayar ve internetin ortaya çıkışıyla birlikte internet üzerinden yetkisiz erişim, kimlik hırsızlığı, sistemlere izinsiz erişim gibi hem bilişim sistemlerine özgü yeni suç türleri ortaya çıkmış hem de günlük hayatımızda karşılaştığımız asayiş ve diğer suç türlerinin internet üzerinden yani online olarak işlenmeye başlandığı görülmüştür. Bilişim suçlarında dünya çapında milyarlarca dolar zarara neden olan veya milyonlarca sisteme zarar veren çok ciddi zararlı eylemler gerçekleşmiştir. Bu kısımda küresel çapta büyük zararlara yol açmış saldırılara değinilecektir.

2.11.1. Siber Dünyada Bilinen Beş Büyük Saldırı

2.11.1.1. WannaCry Saldırısı

WannaCry, Mayıs 2017 tarihinde küresel çapta gerçekleşen Ransomware olarak adlandırılan fidye yazılım türüdür. Çok kısa sürede dünyaya yayılmış ve birçok kamu kuruluş, özel şirket ve hastane cihazlarını bile etkilemiştir. Saldırıda Windows işletim sisteminde bulunan bir güvenlik açığı kullanılmıştır. Bu açık sayesinde sisteme sızan bu solucan çok kısa sürede bilgisayarların ve diğer yazılımla çalışan cihazların sistemini şifreleyerek kilitlemiştir. Fidye olarak da 300 dolar değerinde kripto para olan Bitcoin talep edilmiştir.[208]

2.11.1.2. NotPetya / ExPetr Saldırısı

NotPetya/ExPetr, Ransomware yani fidye amaçlı yazılım saldırılarının tavan yaptığı 2017 Haziran ayında, küresel çapta birçok sisteme bulaşarak bu sistemlerin kilitlenmesine yol açmıştır. Aynı zamanda fidye talep etmesine rağmen şifreyi çözme

[207] (çevrimiçi) http://legal.un.org/ola/website/legal_counsel15.aspx, Erişim: 9 Temmuz 2019.
[208] (çevrimiçi) https://www.bitdefender.com.tr/dunyayi-aglatan-saldiri-wannacry, Erişim: 13 Temmuz 2019.

kimliği bulunmuyordu yani fidye ödense bile belgeler kurtarılamıyordu. Bu saldırı çok yüksek maliyetli olmuş ve ciddi zararlar vermiştir. Sistemdeki Eternal isimli bir açığı kullanarak sistemlere bulaşmış ve çok hızlı yayılarak çok sayıda sistemi kilitlemiştir.

NotPetya saldırısında yaklaşık 10 milyar dolar zarara uğrandığı düşünülürken bu miktar WannaCry da 4-8 milyar dolar arasında olduğu tahmin edilmektedir.[209]

2.11.1.3. Stuxnet Saldırısı

Muhtemelen ünü en fazla olan saldırı, 2010 senesinde İran'ın uranyum zenginleştirme santrifüjlerine engel olan ve bu ülkenin nükleer programını birkaç sene yavaşlatan çok yönlü ve karmaşık olan bu kötü hedefli yazılımın saldırısıdır. Bu tarz sistemlere yönelik siber saldırıların kullanılması yönüyle bu saldırı çok konuşulmuş ve bu alanda farklı bir yere sahip olmuştur.

Karmaşık olma konusunda Stuxnet gerçekten farklıydı. Diğer hiçbir virüs, solucan veya zaralı yazılım türüne benzemiyordu. Özel bir amaçla üretildiği, kodlandığı aşikârdı. Burada ana hedefin tüm dünyada tepkiye neden olan İran tarafından nükleer silah amaçlı yapıldığı öne sürülen uranyum zenginleştirme çalışmalarını hedef almıştır. Bu solucan, internete veya ulusal herhangi bir ağa bağlı bulunmayan sistemlere bile bulaşabilecek tarzda programlandığı için tespiti zor olmuştur. Sistemler üzerinde bulunan çok sayıda açığı aynı anda kullanabilmesi de Stuxnet'in hiç de sıradan bir saldırı olmadığını gösteriyordu.

Stuxnet'in çıkış yeri kim tarafından yazıldığı ile alakalı olarak çeşitli senaryolar üretilmiş olup kodların arasında geçen birkeç kelimeden İsrail'i işaret eden noktalar bulunsa da bunların birer komplo teorisi olduğu iddiaları da yayılmıştır. Konuyla ilgili İsrail'den resmi bir açıklama yapılmamıştır. Bu solucan özellikle İran'ın kullandığı Siemens marka cihazlar üzerinden de çok başarılı şekilde yayılmıştır ve uranyum zenginleştirme programına zarar vermiştir. Siemens firması yazılım

[209] (çevrimiçi) https://www.kaspersky.com.tr/blog/five-most-notorious-cyberattacks/5394/, Erişim: 13 Temmuz 2019.

güncellese de İran güncellenen yazılımlarla Siemens'in Stuxneti koruduğunu iddia ederek kendisi açığı kapatma yoluna gitmiştir ve artık tehdit ortadan kalkmıştır.[210]

2.11.1.4. Dark Hotel Saldırıları

Kafe ya da havalimanlarındaki herkese açık olan Wi-Fi'lerin çok güvenilir olmadığı bilinen bir gerçektir. Bir otelin ağı herkese açık olsa bile, en azından bir tür yetkilendirmeye ihtiyaç duymalıdır.

Dark Hotel olarak isimlendirilen bu saldırı 2014 yılında keşfedilmiş ancak 4 yıldır aktif olduğu düşünülmüştür. Bu saldırı yönteminde, özellikle Asya bölgesinde en lüks oteller de dâhil olmak üzere, otel müşterilerinin bilgilerini ele geçirme amacıyla saldırılar yapılmıştır. Genelde otellerin kablosuz ağ bağlantısı hedef alındığı için ismi Dark Hotel yani karanlık otel olarak adlandırılmıştır.

Bu saldırı sistemi şöyle işlemektedir; genellikle otel müşterileri check-in yaptıktan sonra otelin kablosuz internet ağı Wi-fi ağına bağlanır, onlardan isim ve oda numarası talep edilir. Bu bilgileri girerek ağa bağlanan kişiye daha sonra bu ağa sızmış olan hackerlar tarafından Google, Microsoft veya Adobe gibi ünlü ve herkesin bildiği firmalardan bir güncelleme varmış gibi mağdurlara gönderilir, mağdurlar bu güncellemeyi yükleyince cihazlarına bir backdor yani hackerın sisteme sızmak için kullancağı arka kapı yüklenir. Daha sonra mağdurun cihazına backdoor üzerinden keylogger yüklenir ve mağdurun kredi kartı bilgileri veya önemli bir yönetici ise hassas bilgileri, mesajları çalınması şeklinde gerçekleştirilen saldırıdır.[211]

2.11.1.5. Mirai Botnet Saldırısı

İnternetin meydana çıkmasıyla beraber ortaya çıkan güvenlik açıkları zombi bilgisayarlardan oluşan Botnetlerin de ortaya çıkmasına yol açmış ve botnetler için uygun bir ortam hazırlamıştır. Botnet oluşturmak için, daha önceleri güvenliği hiç düşünülmemiş olan ve ortamında hiçbir antivirüs uygulaması bulunmayan aygıtlara virüs bulaştırarak veya sistemde var olan açıkları kullanarak bu botnetler oluşturulmuştur. Sonrasında bu aygıtlar da kendi türündeki cihazlara yayılmıştır. Bu

[210] (çevrimiçi) http://www.e-data.com.tr/dogrusuyla-yanlisiyla-stuxnet.aspx, Erişim: 13 Temmuz 2019.
[211] (çevrimiçi) https://www.kaspersky.com/blog/the-dark-story-of-darkhotel/15022/, Erişim: 13 Temmuz 2019.

şekilde kullanıma hazır hale gelene kadar çok fazla sayıda sisteme bulaşarak büyümüştür.

21 Ekim 2016 tarihinde, bu büyük botnet ağının sahipleri yeteneklerini büyük DNS servis sağlayıcısı DYN'e yönelik DDoS saldırısında bulumuşlardır ve aralarında Twitter'ın da bulunduğu birçok hizmet bu saldırıdan etkilenerek geçici de olsa erişilememiştir.

2.12. Türkiye'ye Yönelik Siber Saldırılar ve Örnekler

Siber dünya olarak tabir edilen küresel ölçekteki internet ağında ülkeler bazında düşünmek oldukça dar kapsamlı olmaktadır çünkü siber dünyada her ne kadar devletler tarafından bağlantılar kontrol edilse de klasik anlamdaki gibi sınırlar mevcut değildir. Özelllikle siber ortamda yapılan küresel çaplı saldırılardan tüm devletler etkilenmektedir. Bu bağlamda yukarıda örneğini verdiğimiz çok geniş çaplı saldırılardan Türkiye de etkilenmektedir. Siber saldırıların çoğunun amacı tüm dünyada yayabildiği kadar kötü amaçlı yazılımı yaymak ve saldırıyı genişletmektir. Bu kapsammda ağ üzerinden internete bağlı olsun olmasın bir bilgisayara bulaşsa bile internete bağlı olmayan diğer bilgisayarlara da bu zaralı yazılımlar hızla bulaşarak ve sınır tanımayarak ilerlemektedir.

Türkiye, güvenlik firması FireEye'ın açıkladığı rapora göre 25 milyon siber saldırıya maruz kalma sayısı ile bu alanda birinci olarak en fazla saldırıya maruz kalan ABD ve ikinci sıradaki Brezilya'dan sonra en çok saldırılan 3. ülke konumunda yer alıyor.[212] Bunun dışında bir diğer çok önemli husus ise Microsoft'un yayınladığı raporda; dünyada en çok botnet bilgisayarı bulunma oranına sahip ülke Türkiye'dir. Bu rapora göre, ülkemizden çok fazla sayıda bilgisayar küresel botnet ağlarına dâhil edilmiştir. Bu husus ülkemizde bilinçsiz internet kullanımını ve fazla sayıda lisanssız ürün indirildiğine de işarettir.[213] Ayrıca ülkemize yönelik olarak 14 Aralık 2015

[212] "Türkiye'ye yapılan siber saldırı sayısı: 25 milyon", Eylül 2018, (çevrimiçi) https://siberbulten.com/sektorel/trky/turkiyeye-yapilan-siber-saldiri-sayisi-25-milyon/>, Erişim: 12 Temmuz 2019.
[213] (çevrimiçi) https://shiftdelete.net/turkiye-ye-yapilan-siber-saldiri-sayisi-sasirtti, 13 Temmuz 2019.

tarihinde 10 gün süreyle ".tr" uzantılı sitelere yapılan DDoS atağı da bir süre erişim engellemelerine sebep olmuştur.[214]

Türkiye'deki hacker örneklerine bakıldığında ise Türkiye Cumhuriyeti'nin, resmi olarak yargılanan ilk hackerı olan, 1981 doğumlu Tamer Şahin, 1999-2001 senelerinde dönemin internet servis sağlayıcılarından Superonline internet servis sağlayıcısı, Osmanlı Bankası ve Microsoft'un bilgisayar sistemlerine girdiği suçlamalarıyla karşı karşıya kalmış ve yargılanmıştır.[215]

2.13. Türkiye'de Bilişim Sistemleri Güvenliği Analizi ve Bilişim Güvenliğinin Sağlanması

Türkiye'de siber suçlara karşı etkin bir savunma yapabilmek ve gerekli önlemleri alabilmek için ulusal çapta bir siber güvenlik çalışması yapılması kararlaştırılmış ve bu bağlamda 2012 yılında 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" 28447 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu karar ile kamu kurum ve kuruluşlarının bilişim sistemleri üzerinden sağladıkları hizmetlerde veri ve işlem güvenliğini sağlama ve kritik altyapıların güvenliğinin sağlanması hususunda kurallar belirlenmiştir. Bu stratejik eylem planları yenilenerek ve güncellenerek günümüze kadar devam etmiştir. Güncel olarak 2016-2019 eylem planı uygulamadadır.

Türkiye'nin Ulusal Siber Güvenlik Stratejisi ile "siber dünyayı meydana getiren sistemlerin saldırılardan korunmasını, bu durumda işlenen veriyi her yönden emniyet altına almak, saldırılara karşı siber emniyet tedbirlerini belirlemek, bu belirlemelere karşı reaksiyonel mekanizmaları devreye almak ve saldırı sonrasında bu sistemleri önceki hallerine geri döndürerek işler hale getirmek" şeklinde tanımlanmıştır.[216]

Türkiye'nin, yerel siber güvenlik stratejisi ile alakalı eylem maddesinde, bütün kamu kurumları ve kritik sektörlerdeki planlama ve denetleme ile yetkili kuruluşlara

[214] (çevrimiçi) https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan, Erişim: 13 Temmuz 2019.
[215] (çevrimiçi) https://tamersahin.com/tr/, Erişim: 12 Temmuz 2019.
[216] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**, Ankara, 2012, s. 9.

SOME (Siber Olaylara Müdahale Ekipleri) oluşturulmasıyla alakalı görev yüklenmiştir. Bu timlerin kurulmasıyla birlikte sektörler arası veri akışının hızlanması, ilerleyen tehditlere karşı aktif olarak mücadele edilme olanağı sağlayabilecektir[217]. Çeşitli programlar, planlar, TSK bünyesinde yapılan faaliyetler ve oluşumlar ile ülkemizde siber güvenlik bilincini yükseltmek amaçlanmış ve son olarak bu konuda değişik çalışmalar yapılmıştır. Bilişim güvenliği yönünden ülkemizin, dünyadaki başka ülkelere kıyasla stratejik konumu son derece önemlidir. Bu açıdan bakıldığında yukarıda da bahsedildiği gibi Türkiye, Avrasya bölgesinde en çok siber saldırıya maruz kalan ülkedir. Örnek verecek olursak; siber güvenlik üzerinde çalışmalar yapan FireEye firması tarafından hazırlanmış raporda[218]; 2016 senesinde Türkiye'de bütün Avrupa ülkelerinde meydana gelen olaylardan daha çok "güdümlü zararlı yazılım" bulunduğu vurgulanmıştır.

Türkiye'de siber güvenlik problemi ile ilgili katkıda bulunmak hedefiyle "Siber Güvenliği Sağlamak, Ülkemizdeki Mevcut Durumlar ve Alınması Gereken Tedbirler" başlıklı bir çalışma hazırlanmıştır[219]. Bu çalışma üzerinden sanal tehditlerin amacına, önemli altyapıların korunmasına ve siber güvenliğin sağlanmasına yönelik tespitlere yer verilmiş, yerel siber güvenliğin sağlanması hedefiyle yapılması gerekenler ve oluşabilecek sorunların sebepleri belirtilmiştir. Bilişim suçlarında klasik reaktif anlayış etkili olmamaktadır çünkü saldırı gerçekleştikten sonra dünya çapında milyarlarca dolarlık zararlara neden olmaktadır. Bu bağlamda bu suçlarla mücadelede küresel çapta proaktif bir anlayış benimsenerek sıkı işbirliği yapılması faydalı olacaktır.

İnternet olgusunun ortaya çıkması ve kullanımının giderek yaygınlaşması sonucunda bilişim suçları adı verilen yeni bir suç türü karşımıza çıkmıştır. Bilişim suçları, siber alanda çok çeşitli şekillerde işlenebilmektedir. Bu nedenle bilişim suçlarının önlenmesi ve siber güvenliğin sağlanması oldukça zorlaşmaktadır. Siber

---

[217] **A.e**., s. 19.
[218] "Kritik rapor: Türkiye'nin jeopolitik durumu siber casusları cezbediyor", Şubat 2017, (çevrimiçi) https://siberbulten.com/sektorel/trky/kritik-rapor-turkiyenin-jeopolitik-durumu-siber-casuslari-cezbediyor/, Erişim: 14 Temmuz 2019.
[219] Mustafa Ünver, Cafer Canbay ve Ayşe Gül Mirzaoğlu, "Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", **BTK Raporu**, Mayıs 2009.

güvenliğin sağlanması için alınacak kişisel önlemlere ilave olarak, ulusal ve uluslararası düzeylerde birtakım hukuki düzenlemeler yapılmaktadır. Bu düzenlemeler arasında en çok tartışılan konulardan biri internete erişimin engellenmesidir. Güvenlik-özgürlük ikileminden hareketle, siber güvenliğin sağlanması için gerekli görülen bu engellemelerle ilgili mevzuatı, uygulamaları ve gerek kişisel gerek toplumsal sonuçları bu noktada incelemek uygun olacaktır.

ÜÇÜNCÜ BÖLÜM

SİBER GÜVENLİĞİN SAĞLANMASI BAĞLAMINDA İNTERNETE ERİŞİMİN ENGELLENMESİNİN ULUSAL VE ULUSLARARASI SEVİYEDE İRDELENMESİ

Bilişim ve iletişim alanında yaşanan hızlı değişimin doğal bir sonucu olarak devletlerin de siber alana doğru kayması kaçınılmaz olmuştur. Özel şirketlerin ticari ilişkilerinde internet kullanımını arttırmaları, devletin siber alana girmesini hızlandırmıştır. Bu noktada devletlerin de bir takım hizmetlerini siber ortama taşıdığını söylemek mümkündür. Özellikle "E-devlet" projesi ile tüm vatandaşların kişisel bilgilerini siber ortama taşıyan devletler için bu verilerin korunması oldukça önemlidir.[220] Devletlerin ve vatandaşların siber ortamdaki bilgileri, bilişim suçluları ya da diğer devletler tarafından her an ele geçirilme tehdidiyle karşı karşıyadır. Bu bilgiler ifşa edilebilir ya da bilgilerin bütünlüğü bozulabilir ve kullanılabilirliğine zarar verilebilir[221].

Siber ortamda karşı karşıya olunan bu tehditler nedeniyle bazı devletler 2010 yılından itibaren siber komutanlıklar kurmaya başlamışlardır. Çin, ABD, Rusya, Almanya, İngiltere siber komutanlıklar kuran devletlerdendir[222]. Devletler her ne kadar siber komutanlıklar kurmak suretiyle siber alan üzerinde hâkimiyet kurmaya çalışsa da bu o kadar kolay olmamaktadır. İnternette ticari faaliyetlerin, artması ve sınırların ortadan kalkarak uluslararası bir kimliğe bürünmesi devletlerin bu alandaki güvenlik kaygısını daha da arttırmaktadır. Bu noktada devletlerin klasik ceza hukukları da tam anlamıyla çözüm olamamakta ve yeni hukuki düzenlemelere ihtiyaç duyulmaktadır[223]. Bu anlamda devletler, özel hukuki düzenlemeler hazırlamak suretiyle siber güvenliğin sağlanmasını amaçlamaktadırlar. Ancak bu düzenlemeler zaman zaman güvenlik-özgürlük ikileminde tartışmalara neden olmaktadır. Bu tartışmaların en yoğun biçimde

---

[220] Bülent Akkuş, "Özgürlük ve Güven(siz)lik İkileminde Siber Uzay", Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı, İstanbul, 2013, s. 90.

[221] Michael G. Solomon ve Mike Chapple, **Information Security Illuminated**, ABD, Jones and Barlett Publishers, 2005, s. 4.

[222] Akkuş, **a.g.e**., s. 91.

[223] Michael Froomkin, "The Internet as a Source of Regulatory Arbitrage", **Borders in Cyberspace: Information Policy and the Global Information Infrastructure**, Brian Kahin ve Charles Nesson (edt.), USA, MIT Press, 1997, s. 129.

yaşandığı noktalardan biri internete erişimin engellenmesidir. Devletlerin bu yöntemi kullanması gerek ulusal gerek uluslararası seviyede sorunlara yol açabilmekte ve demokrasi, ifade özgürlüğü gibi kavramlar üzerinden tartışmalar boyut kazanmaktadır.

3.1. Genel Olarak Erişim Engelleme Yöntemleri

Erişimin engellenmesi, hukuka aykırılık teşkil eden içerik barındıran bir internet sayfasına belli bir ülkeden giriş yapılmasının engellenmesi veya zorlaştırılmasıdır[224]. Bu haliyle erişimin engellenmesi kavramı, içeriğinde suç bulunan öğe, sitenin tümünde yer almadıkça sitenin tamamı ile erişime kapatılması anlamına gelmemektedir. Hukuki nitelik açısından değerlendirildiğinde; erişimin engellenmesi kararı bir yaptırımdan ziyade zararın oluşmasını engellemek amacıyla alınan bir "ihtiyatî tedbir" niteliğindedir[225].

Erişim engellemenin birçok yolu ve yöntemi vardır ve bu yöntemler zaman içerisinde daha çok geliştirilmiştir. 5651 sayılı kanuna göre erişim engelleme yöntemleri; internet protokol (IP) uzantısından erişim engelleme, alan adından erişim engelleme, site URL'si üzerinden erişim engelleme ve muhtelif benzer yöntemler kullanılarak erişimin engellenmesi başlıkları altında ele alınmıştır. Bu yöntemleri kısaca inceleyelim.

3.1.1. Alan Adından Erişim Engelleme

Herhangi bir internet sitesine ulaşmak için kullanılan adreslere "Alan Adı" (domain name) ismi verilmektedir[226]. DNS (Domain Name System) Türkçe'ye alan adı sistemi olarak çevrilmekte ve alan adlarının IP'ye çevrilmesinde kullanılan bir sistemdir.

Alan adları her biri eşsiz olacak şekilde tayin edilmektedir. Hiçbir alan adı başka bir web sitesi için kullanılamamaktadır. Alan adına göre erişim engelleme

[224] Tekin Memiş, "Erişimin Engellenmesi, Hukukî Sorunlar ve Çözüm Önerileri", **EÜHFD**, C. XIII, S: 3-4, 2009, s. 161.
[225] Murat Tumay, "Denetim ve Özgürlük ikileminde İnternet Erişimi", **SETA Analiz**, S: 133, Temmuz 2015, s. 9.
[226] Doğan Kılınç, "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S: 2, 2010, s. 408.

yapılması durumunda bu işlem neticesinde engellenen web sitesine giriş yapılamayacaktır.

3.1.2. IP Adresinden Erişim Engelleme

İnternette dolaşan her bilgisayara bir IP adresi verilmektedir. IP adresi TCP/IP protokolünü kullanan ve belirli bir ağa bağlı cihazlara, ağ üzerinden birbirleri ile iletişimde ve veri paylaşımında bulunmaları için atanan rakamlardan oluşan etiketlere verilen isimdir[227]. Günümüzde yaygın olarak kullanılan IPv4 teknolojisine göre IP adresi 4 adet 8 bitlik olmak üzere toplamda 32 bitlik noktalara ayrılmış olup, alan adı yerine tarayıcıya doğrudan yazılarak da bu adrese ulaşılabilmektedir. Günümüzde internete bağlanan cihaz sayısının ciddi oranda arttığı ve bu ivmeli artışın devam etmesinden ötürü hali hazırda IPv4 teknolojisi yetersiz kalmaya başlamış ve şirketler bu konuya ortak IP adresi atama yoluyla geçici çözümler aramaktadır. Bunun yanında IP teknolojisi için yeni protokol çalışmaları devam etmekte ve gelecekte daha çok kombinasyon ihtimali sunan yeni IP protokoller geliştirilmesi için çalışmalara devam edilmektedir.

Her kullanıcının kullanmak durumunda olduğu IP adresleri statik ve dinamik olmak üzere ikiye ayrılmaktadır. Belli bir ağa bağlı cihazların birbirini tanıması ve veri alışverişi yapması için kullandıkları zaman ve oturuma bağlı olarak değişkenlik göstermeden, sistem yöneticisi tarafından tanımlanan ve değiştirilebilen IP adresleri sabit IP adresi diye geçmekte bunun yanı sıra zamana ve bağlantı oturumuna göre değişen, her internete bağlanıldığında yeni IP adresi oluşturan IP adresi türüne ise değişken IP adresleri denmektedir.

IP adresleri birden fazla alan adına sahip olabilir. Dolayısıyla IP adresi üzerinden erişim engelleme politikası izlenirse bu adres üzerindeki tüm alan adlarına olan erişim engellenecektir[228]. Buna istinaden birden fazla alan adı bulunan IP adreslerinin kullanımı beraberinde sorunlar getirebilir, bunun sebebi ise suçlu suçsuz gözetmeksizin aynı IP adresi üzerindeki tüm alan adları tek bir suçlu alan adı sebebiyle cezai yaptırımlara maruz kalabilmesidir.

---

[227] Tumay, **a.g.e**., s. 9.
[228] Kılınç, **a.g.e**., s. 409.

3.1.3. Nesne Tabanlı (URL) Erişim Engelleme

IP adreslerinin aksine her URL yalnızca bir internet sitesinin kullanımındadır. Site içinde dolaşmanın adres üzerindeki yoludur. Yine IP adresinin aksine bu yöntem üzerinden erişim engeli uygulanması durumunda siteyle ilgili diğer adresler etkilenmemekte fakat bu yöntem daha zor ve maliyetli olmaktadır. Bir diğer yan etkisi ise internet trafiğinde hız düşüşlerine yol açmasıdır[229].

3.2. Türkiye'de Erişim Engelleme ve Filtreleme

Türkiye 1993 yılında internet ile tanışmasına karşın, internet kullanımının yaygınlaşması 1990'lı yıllarınsonuna kadar sürmüştür. Türkiye'de 2000 yılına kadar internet filtreleme veya erişim engellemesine yönelik herhangi bir müdahale olmamıştır.

Erişim engelleme ve içeriğe müdahale ile ilgili gelişmeler Türkiye'de 3 ayrı dönemde incelenmektedir. İlk dönem internetin ilk yaygınlaştığı yıl olan 1993 yılı ile 2000 yılına kadar olan dönemdir. Bu dönem internet kullanımının başladığı ve yeni yeni yaygınlaştığı dönemdir. İkinci dönem 2001-2006 yılları arasındaki dönemdir. Bu dönem erişim engellemesi ve içeriğe yönelik müdahaleye ilişiklin ilk yasal düzenlemelerin yapıldığı dönemdir. Son dönem ise 2007 yılından sonra başlayarak 5651 sayılı "İnternet ortamında Yapılan Yayınların Düzenlemesi ve Bu Yayınlar Yoluyla İşlenen suçlarla Mücadele Edilmesi Hakkında Kanun" çerçevesinde yapılan erişim engelleme dönemidir[230].

Türkiye'de erişim engelleme olarak ilk uygulama 2001 yılında 4676 sayılı "Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanun, Basın Kanunu, Gelir Vergisi Kanunu ile Kurumlar Vergisi Kanununda Değişiklik Yapılmasına Dair Kanun Tasarısı" olmuştur. Kanun tasarısı ile Basın Kanunu'nun da yaptığı değişikler neticesinde yeni sorunların meydana gelebileceği değerlendirilerek 2001 yılı Haziran ayında Cumhurbaşkanı tarafından veto edilerek yürürlüğe girmemiştir. Cumhurbaşkanı'nın tasarıyı veto etmesindeki diğer nedenlerin başında ifade özgürlüğü ve kişilik haklarının korunması gibi gerekçeler bulunmaktadır. İfade

[229] Tumay, **a.g.e**., s. 10.
[230] Henkoğlu ve Yılmaz, **a.g.e**., s. 219.

özgürlüğüne ilk müdahale girişimi olan bu yasa tasarısı veto edildikten yaklaşık bir yıl sonra konu tekrar 2002 yılında gündeme alınmış TBMM tarafından aynı şekilde hiçbir değişiklik olmadan "4756" sayılı kanun olarak kabul edilmiş ve yürürlüğe girmiştir. [231]

Türkiye'de erişim engellemesine yönelik yasal uygulamalar 3 başlık altında incelenebilir[232].

- "5651" sayılı kanun gereği uygulanılan erişim engellemesi kararları,
- "5846" sayılı Fikir ve Sanat Eserleri Kanunu'nun Ek 4. madde bağlamında uygulanan engelleme kararları,
- Mahkemelerce verilen "ihtiyati tedbir" kararları kapsamında erişim engellemesidir.

5846 sayılı Fikir ve Sanat Eserleri yasası bağlamında belirtilen kurallara uymayan siteler bu kanun gereğince erişim engelleme kararı kapsamında kapatılabilmektedir. "İhtiyati tedbir" kararları kişilik hakları ve ifade özgürlüğü gibi haklar bağlamında verilen kararlardır. 5651 sayılı kanun ise madde 9 kapsamında hakkı ihlal edilen ve mağduriyet yaşayan kişilerin bu mağduriyeti giderme imkânı sunmaktadır.

Türkiye de gelişmiş ülkelerde olduğu üzere her alanda yasa çıkarırken, uluslararası sözleşmelere, insan haklarına ve hukukun üstünlüğüne uygun şekilde davranmaya çalışmaktadır. Bunun yanında birçok uluslararası anlaşmaya da taraf ülke olarak imza atmıştır. Bu anlaşmalar İnsan Hakları Evrensel Bildirgesi gibi kişi hak ve özgürlüklerini ele alan evrensel metinler iken, bazı anlaşmalar ve kanunlar, internette filtrelemeye ve erişim engellemeye ilişkindir. Bu durum güvenlik-özgürlük bağlamında bir ikilemin ortaya çıkmasına neden olmaktadır. Türkiye, internet ortamında suç olarak tanımlanan içeriklere karşı kanuni düzenlemeler yapmış ancak

[231] Yaman Akdeniz ve Kerem Altıparmak, **İnternet: Girilmesi Tehlikeli ve Yasaktır-Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme**, Kasım 2008, s. 6-7. (çevrimiçi) https://docplayer.biz.tr/749780-Dr-yaman-akdeniz-dr-kerem-altiparmak-kasim-2008.html, Erişim: 17 Ağustos 2019.
[232] Henkoğlu ve Yılmaz, **a.g.e**., s. 219.

güvenlik-özgürlük ikileminin neden olduğu tartışmaların yaşanmasına engel olamamıştır.

3.3. 5651 Sayılı Kanun Kapsamında Erişimin Engellenmesi

3.3.1. Erişim Engellemeye Yetkin Makamlar

3.3.1.1. Erişimin Engellenmesi

Erişimin engellenmesi, yetkili kamusal merciler tarafından hukuka aykırı bulunan internet içeriğini çeşitli teknik yöntemler uygulamak suretiyle kişilerin o içeriğe ulaşımının engellenmesi olarak tanımlanabilir[233]. Burada içerik, erişim ve yer sağlayıcılara yönelik bir engellemeden bahsedilmektedir. Bu sebeple erişimin engellenmesi kavramı yerine "iletişimin engellenmesi" kavramının daha doğru bir kavram olduğu da ifade edilmektedir[234].

Erişim engeli gibi cezai uygulamalar ceza niteliğinde değil öngörü ve tedbir niteliğindedir. Bununla birlikte yalnızca mahkeme sonucu ile değil herhangi bir şüphe durumunda dahi erişim engeli yasağı getirilebilmektedir. Adli mercilerin bu kararı alması durumuna koruma tedbiri, idari mercilerin bu kararı alması durumuna da idari tedbir adı verilmektedir. Her ne kadar BTK tarafından erişim engelleme amaçlı olarak idari tedbir kararları yasada geçse de Anayasa Mahkemesi BTK'nın re'sen erişim engelleme kararı verme yetkisini iptal etmiştir[235].

Erişim engeli söz konusu olan sitelere, erişim sağlamak istediğinde ulaşamayan kullanıcıların, buna müteakip süreci araştırmak, bu durum hakkında bilgi edinmek veya itirazda bulunmak isteyebileceği de göz önünde bulundurularak, kanunca erişim engeli gelmiş siteye girerken bir uyarı sayfasına yönlendirilmeye ve engeli getiren merciiye kadar birçok bilgiyi elde etmeye olanak sağlanmıştır.

---

[233] Yasin Söyler, "Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi", Doktora Tezi, Gazi Üniversitesi Kamu Hukuku Anabilim Dalı, Ankara, 2013, s. 215.

[234] Murat Volkan Dülger, "İnternet İletişiminin Engellenmesinin Hukuki Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", **İstanbul Barosu Dergisi**, C. LXXXI, S: 2007/4, 2007, s. 1479.

[235] "Anayasa Mahkemesi BTK'nın erişim engelleme yetkisini iptal etti", 7 Şubat 2018, (çevrimiçi) https://www.cnnturk.com/turkiye/anayasa-mahkemesi-btknin-erisim-engelleme-yetkisini-iptal-etti, Erişim: 14 Ağustos 2019.

3.3.1.2. Erişimin Engellenmesi Kararının Türleri

Erişimi engelleme kararının, önceki bölümlerde ayrıntılı şekilde anlatıldığı üzere; alan adından, IP adresinden, URL adresinden ve diğer yollar olmak üzere türleri bulunmaktadır.

3.3.1.3. Koruma Tedbiri Olarak Erişim Engellenmesi Kararı

4 Mayıs 2007 tarihinde yürürlüğe giren 5651 sayılı yasanın 8. madde 2. fıkrasında; "soruşturma evresinde hâkim kararı ile kovuşturma evresinde ise ilgili kurumların talebine istinaden mahkeme kararı ile erişimin engellenmesi kararı verilir" hükmü yer almaktadır. Gecikmesinde sakınca bulunan hallerde savcı tarafından doğrudan erişim engellenmesine karar verilebilir.

Cumhuriyet savcısı tarafından alınacak erişim engellenmesi kararı ise iki farklı koşulun gerçekleşmesine bağlanmıştır. Bunlardan ilki, erişim engellenmediği takdirde başka türlü engellenmenin mümkün olmadığı bir halin oluşması, diğeri ise alınan kararın 24 saat içinde hâkim onayına sunulması şartıdır. Hâkimin onaylamadığı karar savcı tarafından 24 saat içinde onaylanmadığını takdirde derhal kaldırılmalıdır. Erişim engelleme kararına istinaden BTK ya erişim engelleme kararı iletilir. Bu kanunun yönetmeliğinin 16/1'de BTK, tarafına bildirilen erişim engelleme kararını servis sağlayıcılara elektronik ortamda bildirir servis sağlayıcılar kararın gereğini yerine getirir.

3.3.1.4. İdari Tedbir Olarak Erişimin Engellenmesi Kararı

Yasalarda katalog suç olarak belirtilen suçların işlendiği yayınlarda, yer veya içerik sağlayıcılar Türkiye hatta yurt dışında bulunmuş olsa dahi, 237 sayılı TCK'nın 103. maddesinin 1 numaralı fıkrasında yer alan çocukların cinsel istismarı veya 5237 sayılı TCK'nın 226. maddesinde yer alan müstehcenlik suçlarını ya da TCK'nın 227. maddesindeki fuhuş suçlarını meydana getiren yayınlara ilişkin olarak erişimin engellenmesine Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından resen karar verilir hükmü yer almakla birlikte bu kısım Anayasa Mahkemesinin 15/11/2017 tarihli ve E.: 2015/76, K.: 2017/153 sayılı Kararı ile iptal edilmiş ve 7/2/2018 tarihli ve 30325 sayılı Resmî Gazete'de yayımlanmıştır. Günümüz itibariyle BTK (Bilgi Teknolojileri ve İletişim Kurumu) tarafından re'sen erişim engeli uygulanamamaktadır.

3.4. Kullanıcı İradesine Bağlı Sunulan Güvenli İnternet Hizmeti

Kamuoyu tarafından filtreleme olarak de bilinen güvenli internet hizmeti[236]; internet üzerindeki tehlikeli ve uygunsuz içeriği filtrelemek suretiyle kullanıcılara güvenlik sağlamak amacını gütmektedir. Bu hizmet, hem kullanıcılardan gelen filtreleme talepleri hem de devletin re'sen harekete geçmesiyle devreye girmektedir. 22 Kasım 2011'de başlatılan bu proje sayesinde internet kullanıcıları güvenli internet hizmetini kullanmaya başlamıştır. Güvenli intenet hizmeti yalnızca ailelerin tercih ettiği bir hizmet olmakla kalmayıp, güvenli bankacılık hizmeti sunması sebebiyle iş çevrelerince de ilgi görmektedir. Ayrıca çocukların ve gençlerin psikolojik açıdan sağlıklarını olumsuz yönde etkileyebilecek zararlı içerikler de güvenli internet hizmeti yardımıyla engellenebilmektedir.

Güvenli İnternet Hizmeti, internet kullanıcılarından Bilgi Teknolojileri ve İletişim Kurumuna gelen talepler ve şikâyetler göz önünde bulundurularak geliştirilmiştir. Bu hizmete ilişkin usul ve esaslar, ilgili kurumlar ve işletmecilerle yapılan çalışmalar neticesinde 24 Ağustos 2011 tarihinde "İnternet'in Güvenli Kullanımına İlişkin Usul ve Esaslar" şeklinde BTK tarafından yayımlanmıştır.[237]

Günümüzde internet kullanımının yaygınlaşması ve internet hizmetinin mobil telefonlar ile de sağlanması sebebiyle güvenli internet hizmetine olan ihtiyaç artmıştır. Bu hizmete ilişkin dünya uygulamalarına da bakılarak kullanıcının tercihine bağlı ve ücretsiz olarak lanse edilmiştir. Aile ve çocuk profili üzerinde iki seçenek üzerinden çalışan hizmet herhangi bir talepde bulunulmasa dâhi otomatik olarak devreye girmektedir. Ancak kullanıcının talebi doğrultusunda internet servis sağlayıcılarıyla iletişime geçilmesi halinde filtreler ve erişim engeli kaldırılabilir.

Güvenli internet hizmeti, BTK tarafından iki başlık altında ele alınmıştır. Bunlar; çocuk ve aile profilleridir. Aboneler istedikleri zaman internet servis sağlayıcılarının kendilerine verdikleri kullanıcı adı ve parolası ile profiller arası geçiş yapabilmektedir veya filtreleri kullanım dışı bırakabilmektedir. Bu hizmet Türkiye'de

---

[236] Nurhan Kavaklı, "Güvenli İnternet Hizmeti Uygulaması'nın Yazılı Basında Sunumu: Haberlerdeki Aktörler ve Çerçevelemeler", **Galatasaray Üniversitesi İletişim Dergisi**, S: 17, 2012, s. 65.

[237] "Güvenli İnternet Hizmeti Nedir", (çevrimiçi) http://guvenlinet.org.tr/tr/menu/12-Guvenli_Internet_Hizmeti_Nedir_.html, Erişim: 5 Temmuz 2019.

ailelelere çocuklarını hatta kendilerini, uyuşturucu satışı yapan sitelerden, çocuk pornografisi ile ilgili sitelerden, suç işlemeyi teşvik eden veya anlatan sitelerden, terör propagandası yapan ve patlayıcı malzeme yapma yöntem ve yollarını gösteren sitelerden, ırkçılık yapan sitelerden, nefret propagandası ve ayrılıkçı söylemlere bulunan sitelerden ve basit anlamda şiddet içerikli sitelerden bu sitelerin filtrelenmesini sağlamak yoluyla korunma hizmeti sunmaktadır. Güvenli internet hizmeti muhtelif sebeplerle bilgisayar kullanımında yetersiz olan kişiler için daha kolay bir yöntemle filtreleme yapma imkanı sağlar[238]. Bu sayede güvenli internet hizmeti, çocuklarını internetteki zararlı içeriklerden korumak isteyen ailelere uygun bir hizmet olarak sunulmaktadır.

3.5. Uluslararası Alanda Erişim Engelleme ve Filtreleme Uygulamaları

İnternet kullanıcılarının içerik üretim sürecine dâhil olması ile web 2.0 çağı başlamış ve web 2.0 teknolojisi internet üzerinde herkesin ulaşımına açık bir bilgi patlamasına neden olmuştur[239]. Herkesin kolaylıkla istediği bilgiyi, hem hızlı hem de kolay bir şekilde bulabilmesinin yanı sıra, web 2.0 teknolojisi daha önce olmadığı kadar zararlı içerikle karşı karşıya kalınmasına da olanak sağlamaktadır. Bugün internet, her türlü zararlı içeriğe hem yetişkin hem de çocukların kolayca maruz kalabileceği, ayrıca dünya genelinde suç kabul edilen uyuşturucu ticareti, çocuk pornografisi, terörizme eleman temini, patlayıcı yapımını ve hatta kişiyi intihara yölendirme (mavi balina) suçlarının yoğun şekilde işlendiği veya öğretildiği kontrolsüz bir ortam haline gelmiştir[240].

Bu kontrolsüz ve kaotik yapısı sebebiyle internet marifeti ile işlenebilen suçlarla mücadele edilmesi amacıyla, devletler ve topluluklar filtreleme ve erişim engeli gibi önlemler almak zorunda kalmıştır. Bu önlemler, bazı ülkelerde hükümetlerce zararlı görülen içeriğin kaldırılması veya siyasi gerekçelerle sosyal içerik üretilebilen, küresel olarak tanınırlığı olan sitelerin yasaklanması gibi sert

---

238 "Güvenli İnternet Hizmeti", (çevrimiçi) https://www.turktelekomguvenlik.com/urunler/bireysel/guvenli-internet-hizmeti/kisaca, Erişim: 11 Ağustos 2019.

239 Pelin Baycan, "Sosyal Medyanın Y Kuşağı Satın Alma Davranışı Üzerindeki Rolü", Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü, İstanbul, 2017, s. 62.

240 Ayrıntılı bilgi için bknz. Mustafa Demirel, Muhsin Yörük ve Okan Özkan, "Çocuklar İçin Güvenli İnternet: Güvenli İnternet Hizmeti ve Ebeveyn Görüşleri Üzerine Bir Araştırma", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. IV, S: 7, 2012, s. 57-59.

uygulamalara dönüşebilirken bazı ülkelerde ise daha yumuşak uygulamalar olarak karşımıza çıkmaktadır.

Dünya genelinde yaklaşık 4,4 milyar internet kullancısı bulunmaktadır ve bu sayı her geçen gün hızla artmaktadır[241]. Kullanıcı sayısına artış ile orantılı olarak her geçen gün daha sofistike hale gelen teknikler kullanılarak yeni online sansür, erişim engeli ve filtreleme yöntemleri geliştirilmektedir. Bu yöntemler ve bu yöntemleri kullanmaya iten sebepler ve yöntemlerin ne kadar etkili kullanıldığı, ülkeden ülkeye değişkenlik göstermektedir.

Farklı ülkelerde spesifik konulara yönelik filtereler olduğu gibi genel anlamda bütün dünya ülkelerinin çoğunda geçerli olan filtre ve sansür uygulamaları da vardır. Örneğin; Nazizim ve soykırım gibi konular Fransa ve Almanya gibi ülkelerde yasaklıyken, çocuk pornografisi dünya üzerindeki birçok ülkede engellidir. Bunun yanı sıra dünya üzerinde ifade özgürlüğü ve basın özgürlüğüne uzun yıllar önem vermiş, demokrasinin hâkim olduğu ülkelerin de içinde bulunduğu birçok ülke belli oranlarda çevrimiçi sansür uygulamakta ve bu sansür uygulamaları politik gerekçelerle ciddi halk desteği almaktadır[242].

İnternete erişim ve bilişim suçları ile ilgili olarak küresel bazda ortak bir uygulama bütünlüğü bulunmamaktadır. Devletlerin bazıları internete giriş için özel izin isterken bazıları da neredeyse hiç müdahale etmemektedir[243]. Devletlerin yönetim sistemlerine ve hükümetlerinin kararlarına bağlı olarak internet sitelerine erişim engellenmesi ve filtreleme tedbirleri uygulanmaktadır (Tablo-3).

Tablo 3: İnternete Erişim Engellemede Ülkeler Kıyaslaması

[241] "Verilerle dünyada internet ve sosyal medya kullanımı: Türkiye İnstagram kullanımında birinci sırada", (çevrimiçi) https://dokuz8haber.net/toplum-yasam/verilerle-dunyada-internet-ve-sosyal-medya-kullanimi-turkiye-instagram-kullaniminda-birinci-sirada/, Erişim: 15 Ağustos 2019.
[242] Ayrıca internet yasaklarıyla ilgili ülkelerin durumu için bknz. Kerem Congar, "İnternetin en çok yasaklandığı ülkeler hangileri?", 30 Ağustos 2018, (çevrimiçi) https://tr.euronews.com/2018/08/30/internet-en-cok-hangi-ulkelerde-yasaklaniyor-, Erişim: 17 Ağustos 2019.
[243] Özüdoğru, **a.g.e**., s. 51.

	TÜRKİYE	ABD	RUSYA	ÇİN
ERİŞİM KISITLAMASININ TEKNİK GELİŞMİŞLİĞİ	ORTA GELİŞMİŞ (DNS HIJACKING, DEEP PACKET INSPECTION)	AZ GELİŞMİŞ (İÇERİK KALDIRTMA, DEEP PACKET INSPECTION)	ORTA GELİŞMİŞ (DEEP PACKET INSPECTION)	ÇOK GELİŞMİŞ (DEEP PACKET INSPECTION, DNS HIJACKING, IP BLOĞU YASAKLAMA, ORTADAKİ ADAM SALDIRISI)
ERİŞİM KISITLAMASININ AŞILABİLİRLİĞİ	HERKES AŞABİLİR (VPN)	HERKES AŞABİLİR (VPN)	HERKES AŞABİLİR (VPN)	TEKNİK YETKİNLİĞİ OLAN KİŞİLER AŞABİLİR (VPN, TOR)
ERİŞİM KISITLAMASI BAŞLATMAYA YETKİLİ MAKAMLAR	Bilgi Teknolojileri ve İletişim Kurumu	Amerika Birleşik Devletleri Senatosu Yargı Komitesi	İletişim Bilgi Teknolojisi Denetim Kurumu	Merkez Siber İşler Komisyonu
ERİŞİM KISITLAMASI GEREKTİRECEK SUÇLAR VE YASAL DAYANAKLAR	***Kanun No. 5651*** 1) İntihara yönlendirme 2) Çocukların cinsel istismarı 3) Uyuşturucu veya uyarı madde kullanılmasını kolaylaştırma 4) Sağlık için tehlikeli madde temini 5) Müstehcenlik 6) Fuhuş 7) Kumar oynanması için yer ve imkân sağlama	***Public Law 105-304 (DMCA)*** 1) Fikri mülkiyet hakları ihlali ***47 U.S.C. § 231 (COPA)*** 1) Çocuğa karşı işlenecek suçlar 2) Çocuk pornografisi ***47 U.S.C. § 230*** 1) Saldırgan içeriğin kaldırılması ***H.R.4225 (SAVE)*** ***SESTA-FOSTA***	***398-FZ*** ***139-FZ***	***CL97*** 1) Devlete karşı işlenen suçlar 2) Pornografi
NOTLAR	BTK'nın resen erişim kısıtlaması koyma yetkisi Anayasa Mahkemesinin 2017/153 sayılı kararı ile iptal edilmiş olup 2019 yılı itibariyle kanuni altyapı belli değildir.			

Kaynak: İlgili referanslar kullanılarak derlenmiştir[244].

[244] (çevrimiçi) https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/, (çevrimiçi) http://kararlaryeni.anayasa.gov.tr/Karar/Content/9160bf09-3c94-43ae-b1d3-c84815c1b2ba, (çevrimiçi) https://www.govinfo.gov/app/details/PLAW-105publ304, (çevrimiçi) https://www.law.cornell.edu./uscode/text/47/231, (çevrimiçi) https://www.law.cornell.edu./uscode/text/47/230, (çevrimiçi) https://www.congress.gov/bill/113th-congress/house-bill/4225, (çevrimiçi) https://www.congress.gov/bill/115th-congress/senate-bill/1693/text, (çevrimiçi) http://cis-legislation.com/document.fwx?rgn=26853, (çevrimiçi) https://398-fz.rkn.gov.ru/docs/398-FZ_eng.pdf, (çevrimiçi) https://wilmap.law.stanford.edu/entries/federal-law-no-139-fz-blacklist-law, (çevrimiçi) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410, (çevrimiçi) www.cac.gov.cn/, 5651 sayılı kanun madde no: 1-2-4-8, Resmi Gazete: Sayı 26530.

3.6. İnternetin Kısıtlanmasına Karşı Çıkan Uluslararası Organizasyonlar

3.6.1. OpenNet

Tam adı "OpenNet initiative report" olan bu ortak projenin amacı, devlet tarafından yönetilen internet filtreleme araçlarının amacını ve kapsamını belirlemek, izlemek ve geniş kitleleri bu uygulamalardan habedar etmektir[245].

3.6.2. Freedom on the Net

Yıllık olarak "internet özgürlüğü" çalışması yaparak bunu yayınlayan Freedom on the Net organizasyonun amacı, internet kullanıcıların ifade özgürlükleri, bilgi edinme hakları, özel yaşamlarının dokunulmazlığı gibi değerleri savunarak liberal demokratik değerlere uygun bir internet ortamı oluşturulması için yıllık raporlar hazırlamaktır[246].

3.6.3. Reporters Without Borders (RWB)

Reporters Without Borders (*Sınır tanımayan gazeteciler*)[247], amacının basın özgürlüğünü temin etmek olduğunu ifade eden bir sivil toplum kuruluşudur. 1985 yılında Fransa'da kurulmuş ve her yıl "internet düşmanları" olarak adlandırılan dünyadaki internet sansürünün en yoğun olduğu ülkelerin listesini yayınlamaktadır. 2009 yılında yayınlanan listeye göre; internet düşmanı olan 12 ülke bulunmaktadır: Burma, Çin, Küba, Mısır, İran, Kuzey Kore, Suudi Arabistan, Suriye, Tunus, Türkmenistan, Özbekistan, Vietnam. RWB Internet sansür seviyelerine göre bir dünya haritası hazırlamıştır. Bu haritada internet sansürü uygulanma yoğunluğuna göre ülkeler "sansür uygulanmayan ülkeler", "kısmen sansür uygulanan ülkeler", "gözetim altındaki ülkeler" ve "internet kara delikleri" olmak üzere dört gruba ayrılmıştır. Türkiye ve Avrupa ülkelerinin büyük bir çoğunluğu "kısmen sansür uygulayan ülkeler" sınıfında yer almaktadır[248].

---

[245] (çevrimiçi) https://opennet.net/, Erişim: 12 Ağustos 2019.
[246] "About Freedom on the Net", (çevrimiçi) https://freedomhouse.org/report-types/freedom-net, Erişim: 12 Ağustos 2019.
[247] (çevrimiçi) https://rsf.org/en, Erişim: 17 Ağustos 2019.
[248] Güven Köse ve Kerem Özen, "İnternet'te Sansür Üzerine Bir Değerlendirme", 2010, s. 115, (çevrimiçi) https://docplayer.biz.tr/1283326-Internet-te-sansur-uzerine-bir-degerlendirme.html, Erişim: 19 Ağustos 2019.

3.6.4. Turkey Blocks

Turkey Blocks, Türkiye'de internet toplu sansür raporlarını tanımlamayı ve doğrulamayı amaçlayan, bağımsız ve partizan olmayan bir dijital şeffaflık projesi olarak kendisini tanımlamaktadır.[249] Dijital adli tekniklerin bir birleşimini kullanarak geniş çaplı internet yavaşlama ve kapatma olaylarını ölçmektedir. Sosyal medya hizmetlerine ve çevrimiçi kitle iletişim ağlarına erişimi, Türkiye'nin ana nüfus alanlarının çevresinde bulunan *problar* olarak bilinen izleme düğümlerini kullanarak izlemektedir ve konuyla ilgili raporlar sunmaktadır.

3.7. Dünyada Erişim Engelleme ve Filtreleme Uygulamaları

3.7.1. Amerika Birleşik Devletleri

İnternet, ABD'de dünyanın geri kalanına oranla göreceli olarak özgürdür denilebilir. Bunun yanında, kullanıcılar internete erişim ve internette istediklerini yayınlama konusunda bazı engellemeler ile karşı karşıyadırlar. ABD'de internetin kısıtlanması ile ilgili sebepleri genel olarak altı başlık altında toplamak mümkündür. Bunlar; çocukların istismardan korunması, ulusal güvenlik, telif hakları, yasadışı kumar, hakaret ve bilgisayar güvenliğidir[250].

ABD'de ilk internet erişim engelleme yasaları; 1996'da yürürlüğe giren, internette pornografik içeriklerin ve materyallerin kontrol edilmesini amaçlayan "İletişimde Uygunluk Yasası" ve 2000 yılında yürürlüğe giren federal para yardımı sağlayarak Amerika'da okullarda, kütüphanelerde sansür, filtreleme ve engelleme yazılımı ve uygulamaları kurulmasını, bu sayede pornografik içeriklerin engellenmesini öngören "Çocukları İnternet'ten Koruma Kanunu"dur (*CIPA*)[251]. Ayrıca 1999 yılında ABD senatosundan geçen internette kumarın yasaklanmasına ilişkin bir kanun da bulunmaktadır. Bu sayede internetten kumar ve şans oyunları oynanması ve oynatılmasının önüne geçilmesi, suç ve istismardan korunması

[249] (çevrimiçi) https://turkeyblocks.org/about/, Erişim: 5 Temmuz 2019.
[250] OpenNet, "Country profiles: United States and Canada overview", 2010, s. 379, (çevrimiçi) https://opennet.net/sites/opennet.net/files/ONI_UnitedStatesandCanada_2010.pdf, Erişim: 1 Eylül 2019.
[251] Özüdoğru, **a.g.e.**, s. 75.

amaçlanmıştır[252]. ABD'de pornografi, kumar ve suç işlenmesini engellemeye yönelik filtreleme ve engellemenin yanında siyasi kapsamda engellemelerin de uygulandığı, hatta bu engellemelerin bazen Terörizm yasası gibi ulusal güvenlik ve hassasiyet gerektiren yasalardaki maddeleri gerekçe ederek gerçekleştirildiği iddia edilmektedir.

3.7.2. Çin Halk Cumhuriyeti

Çin Halk Cumhuriyeti, sahip olduğu değerleri korumak, ulusal çıkarlarını gözetmek, ulusal güvenliğini sağlamak, halkı denetlemek, yönetimini ve varlığını güçlü kılmak, aykırı sesleri kesmek bunun yanında da dünyaya daha fazla açılmak istemektedir. Bu hedeflere yönelik olarak da internet ile ilgili radikal uygulamalarda bulunmuştur[253]. Çin Halk Cumhuriyeti, öncelikle oluşturduğu siber güvenlik kanunu, internet hakkındaki diğer kanunlar ve anayasada bulunan kanunlar doğrultusunda, internete ve bir takım yeni medya platformlarına yasaklar ve kısıtlamalar getirmiştir. Yasaklara uymayan platformlar/siteler ise kapatılmış ya da diğer cezai yaptırımlar uygulanmıştır.

Yalnızca nüfusunun yaklaşık dörtte birinin sağlıklı bir internet erişimi olan Çin dünyanın en ağır internet kısıtlamalarından birine maruz kalmıştır. "The Great Firewall of China" olarak veya resmi adıyla "Golden Shield Project" olarak bilinen sırasıyla Çin Büyük Güvenlik Duvarı ve Altın Kalkan Projesi olarak tercüme edilen dünyanın en karmaşık, aynı zamanda en büyük filtreleme sistemi ile Çin Halk Cumhuriyeti kısıtlama uygulamalarını tam anlamıyla bir ulusal güvenlik meselesi haline getirmiştir[254]. Çin'de iki milyondan fazla internet polisi, sanal suçları minimum seviyeye çekmek için çalışmakta ve sayısız web sitesini yasaklamaktadır[255].

Çin, engelleme ve filtrelemeye yönelik ağır uygulamalarının yanında, internet

---

[252] Fatih Canata, "5651 Sayılı Kanun Kapsamında İnternet Düzenlemeleri ve Düşünce-İfade Özgürlüğü Üzerine Bir Değerlendirme", **Türk Kütüphaneciliği**, C. XXX, S: 2, 2016, s. 192.
[253] Sefer Kalaman, Elif Kaya ve Ünal Kaya, "Çin Halk Cumhuriyeti'nde Yeni Medya Uygulamaları: Nitel Bir Araştırma", **AJIT-e: Online Academic Journal of Information Technology**, C. IX, S: 32, 2018, s. 108.
[254] Ali Burak Darıcılı ve Barış Özdal, "Analysis of the Cyber Security Strategies of People's Republic of China", **Güvenlik Stratejileri Dergisi**, Yıl: 14, S: 28, 2018, s. 27.
[255] "Çin'de İnternet Sansürü Giderek Büyüyor", (çevrimiçi) https://gizlilikveguvenlik.com/cin-icin-en-iyi-vpn/, Erişim: 4 Eylül 2019.

kullanıcıların internet kafeye kimlik bilgilerini vererek girmesi, gazetecilerin hatta sıradan kullanıcıların bile haber sitelerine yorum yazabilmek için gerçek kimlikleri ile üye olma şartını getirmesi, toplum üzerinde ağır siyasi baskı oluşturmaktadır. Birçok gazeteci ve internet yorumcusunun açık veya gizli olarak tutuklandığı Çin Halk Cumhuriyeti'nin en bilinen kısıtlama uygulamaları[256]:

- Dalai Lama'dan bahseden web sitelerinin engellenmesi (dini içerikli engellemeler),
- 1989 Tiananmen Meydanı olaylarından bahseden sitelerin engellenmesi,
- Falun Gong tarikatına yönelik engelleme,
- Whatsapp, Facebook ve Youtube gibi birçok sosyal medya sitesine yönelik Çin hükümeti tarafından uygulanan kısıtlamalardır.

Çin Halk Cumhuriyeti bu engellemeleri dış ülke hükümetlerini susturmak ve halkını galeyana getircek hatta organize kontrol dışı bir topluluk oluşturacak tüm eylemleri engellemek amacıyla yapmaktadır. Ancak bunların yanında dünyada internetin kısıtlanmasına karşı çıkan uluslararası organizasyonlar da oluşmuştur. Bunun yanında kalabalık kullanıcı ve müşteri kitlesi bulunan Google, Yahoo, Microsoft gibi global şirketler, bu engellemelere göz yumdukları için insan hakları savunucusu birçok kişi ve kurumca eleştirilmiştir. "google.cn", Google şirketi tarafından Çin'de bulunan kullanıcıları için hazırlanmış ve Çin Hükümeti'nin belirlediği kriterlere göre sansür uygulanmıştır[257]. "google.cn" Çin üzerinden büyük çaplı siber saldırıya uğramış ve Çin Hükümeti tedbir almadığı takdirde ülkeden tamamen çekileceğini açıklamış bu kapsamda 2010 yılında merkezini Çin'den Hong Kong'a taşımıştır.

[256] Leyla Budak ve İlker Erdoğan, "1990 Sonrası Çin Halk Cumhuriyeti'nde Kitle İletişim Sistemi ve Temel Sorunlar", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,** Yıl: 5, S: 9, Bahar 2006/1, s. 115.

[257] Ayrıntılı bilgi için bknz. James S. O'Rourke, "Google's Entry into the Chinese Market: A Lesson in Government Censorship and Corporate Reputation", **Journal of Business Strategy**, C. XXVIII, S: 3, 2007, ss. 12-22.

3.7.3. Rusya

Rusya'da internet engelleme ve filtreleme birçok kanun temelinde ve birçok farklı mekanizma ile sağlanmaktadır. 2012'den bu yana Rusya'da internet kısıtlamaları artmış[258], ve bu tarihten itibaren internet kısıtlamalarından sorumlu olarak görev yapan Rusya Federasyonu Dijital Kalkınma, İletişim ve Kitle İletişim Bakanlığı[259] (*Ministry of Digital Development, Communications and Mass Media of the Russian Federation*) tarafından oluşturulan "Single Register"[260] olarak bilinen bir kara listeye sahip olan Rusya, bu listeyi farklı URL, domain adresi ve IP adresini sansürlemek için kullanmaktadır. Bu kara liste ile temelde uyuşturucu kullanımı ve özendirmesini, saldırı metodlarının tanımlamasını ve çocuk pornografisi içeren sitelerin engellenmesini amaçlamıştır. Liste daha sonra "federal aşırıcı materyallerin listesi" adındaki yeni bir liste ile genişletilerek aşırıcılıkla da mücadele etmeyi amaçlamıştır.

ABD merkezli ve Amerikan hükümetince desteklenmekte olan ve "demokrasi", "politik özgürlük" ve "insan hakları" alanında çalışmalar yapan "Freedom House" isimli organizasyonun yayınlamış olduğu raporlara göre[261], bu yasal düzenlemeler sıklıkla hükümete veya yerel yönetimlere yönelik siyasi eleştirilerin engellenmesi amacıyla da suistimal edilmiştir. Yine bu organizasyon tarafından "kısmen özgür statüsünde" yer almakta ve bunun yanında Sınır Tanımayan Gazeteciler kuruluşunun 2010 ve 2013 yılları arasında yayınlanan listelerinde "gözlem altındaki ülkeler listesinde" yer almıştır. Ayrıca Rusya, Çin Halk Cumhuriyetinin kullanmış olduğu The Great Firewall of China isimli kısıtlama uygulama sistemlerine veri sağlayarak ve sistemini geliştirerek işbirliği yapmaktadır.

3.7.4. İngiltere

İngiltere'de filtreleme ve erişim engellemenin yasal dayanağı, 1978 tarihli

---

[258] Abdulkadir Baharçiçek ve Osman Ağır, "Rusya'nın Başarısız Demokratikleşme Tarihi", **Birey ve Toplum**, C. IV, S: 8, Güz 2014, s. 19.
[259] (çevrimiçi) https://digital.gov.ru/en/, Erişim: 21 Ağustos 2019.
[260] Jean-Loup Richet, "Russia Uses 'Single Register' Law To Selectively Block Internet Content", 22 Mayıs 2013, (çevrimiçi) https://www.infosecurity-magazine.com/blogs/russia-uses-single-register-law-to-selectively-blo/, Erişim: 21 Ağustos 2019.
[261] "Russia, Freedom in the World 2014", (çevrimiçi) http://freedomhouse.org, http://freedomhouse.org/country/russia#.U9udQ2VrOUl, Erişim: 21 Ağustos 2019.

Çocukları Koruma Kanunu (*Protectıon Of Children Act*), 2008 yılında kabul edilen Göçmen Yasası (*Immigration Act*), 1959 & 1964 tarihli Müstehcen Yayınlar Kanunu (*Obscene Publications Act*), 2003 tarihli Cinsel Suçlar Kanunu (*Sex Offences Act*), 1986 tarihli Kamu Düzeni Kanunu (*Public Order Act*) sayılı kanunlardır[262]. 2000 yılında Avrupa Birliği tarafından, internet üzerinden e-ticareti düzenleyen bir Direktif hazırlanmış, bu Direktif'in İngiltere'de yürürlüğe girmesi 2002 yılında gerçekleşmiştir. Direktif'in uygulanması ise internet servis sağlayıcıların sorumluluğuna bırakılmıştır[263].

2004 senesinde British Telecom (*İngiliz İnternet Servis Sağlayıcı*) temiz internet çerçevesinde erişim engelleme filtresini kullanıma sunmuştur. Bu sayede çocuk pornografisi ve çocukların cinsel istismarına yönelik içeriklerin engellenmesi amaçlanmıştır. Sistem engellenen sitelerin bloke edilmesinden sonra, aratılan içeriğe yönelik herhangi bir bilgi vermemekte ve aratıldığı takdirde sayfaya ulaşılamadığı (hata kodu 404) uyarasını verecek şekilde çalışmaktadır[264].

Ayrıca kullanıcıların internette gördükleri zararlı içeriği ihbar edebileceği bir merkez kurulmuş, 1996 yılında kurulan bu merkez adliye, polis ve internet servis sağlayıcıların ortaklaşa çalışmasıyla faaliyet yürütmekedir[265]. Polis, hükümet ve internet endüstrisindeki şirketlerin ortak anlaşmasıyla kurulan İngiltere İnternet İhbar Merkezi (*Internet Watch Foundation-IWF*), çocuk pornosu ile mücadelede bu mutabakat zaptına göre işlem yapmaktadır. Bu zapt Birleşik Krallık'ta çocuk pornografisi ile mücadele hususunda ayrıcalıklı bir yere sahiptir[266].

British Telecom, tarafından uygulanan filtreleme sistemine benzer bir filtreleme uygulaması hükümet tarafından diğer internet servis sağlayıcılardan da talep edilmiştir.

İngiltere internet sitelerine hususi düzenleme yapmasa da gerçek hayatta suç

---

[262] Kılınç, **a.g.e**., s. 420.
[263] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML, Erişim: 25 Ağustos 2019.
[264] Kılınç, **a.g.e**., s. 420.
[265] (çevrimiçi) http://www.iwf.org.uk/, Erişim: 25 Ağustos 2019.
[266] (çevrimiçi) http://www.opsi.gov.uk/Acts/acts2003/plain/ukpga_20030042_en, Erişim: 25 Ağustos 2019.

olan her şeyi internet ortamında da suç olarak kabul etmiştir. İngiliz Ceza Kanunu'nda suç olarak kabul edilen herhangi bir suçun işlenmesi durumunda erişim engellemesi yetkili kurumlar vasıtasıyla yapılır. Dolayısıyla yalnızca aşırıcı unsurlar içeren pornografi, çocuk pornografisi ve ırkçılık gibi konularda değil, mahkemelerde suç unsuru olarak kabul edilebilecek bütün konularda erişim engellemesi yönünde karar verilebilmektedir[267].

3.7.5. Fransa

Fransa, Nazi hatıraları koleksiyonunun satışını açık arttırma ile yapan Yahoo açık arttırma sitesi hakkında başvuru yapılmasından sonra, Fransız mahkemesi, Fransa'daki Yahoo kullanıcılarının yaklaşık yüzde 75'inin IP'lerinin analiz edilerek tespit edilmesini ve kullanıcıların yasaklı içeriğe erişiminin engellenmesi adına tedbirlerin alınmasını talep etmiştir. Bu taleplerin yerine getirilmediği takdirde Yahoo Fransa ofisine yönelik cezai müeyyide uygulanacağını hatta ofisin gelirlerine el konulabileceğine karar vermiştir. Yahoo bu olaydan sonra 2001 yılının Ocak ayında Nazi hatıraları koleksiyonunun satışını açık arttırma sitelerinden kaldırmıştır[268]. Ancak bu konuya ilişkin ABD California Bölge Mahkemesi, Amerika'daki "ifade özgürlüğü" hakkının anayasal düzeyde korunmasından ötürü, Fransız mahkemesinin Yahoo şirketinden talep etmiş olduğu ırkçılık hakkındaki yaptırımların temel insan haklarından olan kişinin ifade özgürlüğü hakkına aykırılık teşkil edeceğine karar vermiştir[269].

Telif haklarını ihlal eden kullanıcıların, öncesinde uyarılarak internet servis sağlayıcılar aracılığı ile internet bağlantılarının kesilmesi amacıyla, Fransız hükümeti 2008 yılında kabul edilen yasa tasarısı ile "HADOPI" isimli bağımsız bir kurumun kurulmasını sağlamıştır. Fransız yasalarına göre internet telif haklarının ihlal edilmesini önlemeyi amaçlayan "HADOPI" kanunu, Fransa'da internette fikir sanat eserlerinin korunması amacıyla hazırlanan taslağın takma ismidir. İnternet ortamında

---

[267] Kılınç, **a.g.e**., s. 421.

[268] "France bans internet Nazi auctions", (çevrimiçi) http://news.bbc.co.uk/2/hi/europe/760782.stm, Erişim 2 Eylül 2019.

[269] "Judge dismisses French case against Yahoo", (çevrimiçi) https://www.computerweekly.com/news/2240043064/Judge-dismisses-French-case-against-Yahoo, Erişim: 2 Eylül 2019.

fikir sanat eserlerinin korunmasına yönelik hakları düzenleyen taslak 2009 da Fransız Ulusal meclisinin kararı ile reddedilmiş aynı yıl mayıs ayında tekrar Ulusal Meclis'te görüşülmüş ve bir hafta içinde Fransız Senatosu'nda kabul edilerek yürürlüğe girmiştir[270].

Ağ üzerinde insan haklarını savunmayı hedefleyen bu kanun beraberinde, bir ceza sistemini de getirmiştir. Sisteme göre ihtar edildikten sonra hala korsan film indiren kişiler bir yıla kadar internet bağlantı kesme cezası veya internet hesabını tamamen kaybetme cezası ile karşı karşıya kalabilmektedir. "Three Strikes-Out"[271] sistemi adı verilen bir sistem ile abonmanlar ilk önce mail yolu ile uyarılarak daha sonra bahse konu cezalar tatbik edilmektedir.

HADOPI kanunu, internet telif haklarını koruması ve ihlal edenlere yönelik getirmiş olduğu cezai yaptırımları sayesinde, müzik, sinema alanında içerik üretimi yapan kişilerden önemli derecede destek toplamıştır. Bahse konu kanun, uluslararası "ifade özgürlüğü" gerekçe gösterilerek Fransız Anayasa Konseyi tarafından internetin ifade özgürlüğünün bir parçası olması gerektiği ve masumiyet ilkesine aykırı olması sebebiyle, 2009 yılının Haziran ayında iptal edilmiştir[272]. Bu çerçevede, Fransa'da internete erişimin HADOPI tarafından değil, ancak mahkemeler tarafından engellenebileceği ortaya çıkmıştır[273].

Fransız Ulusal Güvenlik Performansını Planlama Kanunu, 2010 yılında Fransız Ulusal Meclisi'nce kabul edilen ve internet sitelerine erişimin engellenmesine ve filtrelenmesene yönelik bir diğer kanundur. Kanun çocukların korunması amacıyla yargı denetimine gerek kalmadan idari makamların kendi yetkisi ile internet sitelerinin

---

[270] Kılınç, **a.g.e**., s. 424.

[271] Savaş Çömlek, "Özgür Uçkan: İnterneti sansür girişimi olan SOPA yasası geçerse, tüm dünya Çin'e benzeyecek", 2012, (çevrimiçi) https://yesilgazete.org/blog/2012/01/20/ozgur-uckan-interneti-sansur-girisimi-olan-sopa-yasasi-gecerse-tum-dunya-cine-benzeyecek/, Erişim: 3Eylül 2019.

[272] "French anti-filesharing law overturned", (çevrimiçi) https://www.theguardian.com/technology/2009/jun/10/france-hadopi-law-filesharing, Erişim: 2 Eylül 2019.

[273] Önder Erol Ünsal, "HADOPI Yasası Çatırdıyor – Fransa'da İnternet Üzerinden Yasadışı Dosya Paylaşımı ve Dosya İndirme Hakkında Yasal Düzenleme", Temmuz 2013, (çevrimiçi) https://iprgezgini.org/2013/12/17/hadopi-yasasi-catirdiyor-fransada-internet-uzerinden-yasadisi-dosya-paylasimi-ve-dosya-indirme-hakkinda-yasal-duzenleme/, Erişim: 2 Eylül 2019.

erişiminin engellenmesini öngörmüştür.

Kanun polislere içerik paylaşım sitelerine zararlı yazılımlar yükleme yetkisi vermiş ve çocuk pornografisi başta olmak üzere birçok suç teşkil eden konuda Fransız İçişleri Bakanlığı'na belirlenen kara listelerin internet servis sağlayıcılara bildirilmesi yolu ile gerekli prosedür işlemler yapılarak "uygunsuz" içeriğin engellenmesi sağlamayı amaçlamıştır. İnternet servis sağlayıcıları, Fransız İçişleri Bakanlığı'nın ilgili kurumlarınca kendisine bildirilen "uygunsuz" içeriklere yönelik derhal engelleme yapması gerekmektedir. Engelleme yapılmaması veya gecikmesi durumunda yasa, 75.000 Euro para cezasını hatta 1 yıla kadar hapis cezasını öngörmektedir. Bununla beraber bahse konu yasa, Fransız emniyet birimlerini şüpheli şahısların ikametlerine girme ve şahsi elektronik cihazlarına casus yazılım yükleme yetkisi ile donatmaktadır. Bu yetkiler ve internet filtreleme ve erişim engelleme yöntemleri, ifade özgürlüğü, kişi özel hayatının gizliliği gibi en temel kişi hak ve hürriyetlerini tehdit ettiği gerekçesiyle uluslararası ve yerel organizasyonlar tarafından ciddi eleştirilere maruz kalmıştır[274].

3.7.6. Almanya

Alman hükümetinin interneti kontrol etme hususunda birçok Batı ülkesinden daha sert politikalar izlediği görülmüştür. Münih Yerel Mahkemesi'nce, 1997 senesinde internet içerik sağlayıcı şirket Compuserve yetkilisi Somm'un uygunsuz içerik (pornografik) yayınlamaktan suçlu bulunmuş ancak Soom, 1999 senesinde Bavyera Mahkemesi tarafından ise suçsuz bulunmuştur. Compuserve firması kendini, uygunsuz içerikli yayınları yasaklamak için çalıştıklarını söyleyerek savunmasına rağmen, Münih Yerel Mahkemesi, ''Daha fazlasını yapabilirsiniz'' alt metniyle Felix Somm' un cezasının 2 yıl ertelenmesine ve 100.000 Mark tutarında para cezasına hükmetmiştir[275].

İnternette filtrelemeyi gereklilik olarak gören olan hükümet, filtreleme

[274] Kılınç, **a.g.e**., s. 425.
[275] Edmund L. Andrews, "German Court Overturns Pornography Ruling Against Compuserve", 1999, (çevrimiçi)https://archive.nytimes.com/www.nytimes.com/library/tech/99/11/biztech/articles/18compuserve-germany.html, Erişim: 3 Eylül 2019.

mantığını daha çok benimsemiş ve daha kapsamlı yürütmek için Kuzey Westfalya otoriteleri 2001 yılı Ekim ayında 80'den fazla yerel internet sağlayıcısından kendi kara listelerindeki web sitelerine erişimleri engellemeleri talebinde bulunmuş ve gençleri koruma komisyonu kurulup, bu komisyon yer sağlayıcılar üzerinde filtreleme konusunda yetkilendirilmiştir[276].

Almanya, Avrupa Birliği'ne üye birçok ülke gibi internet servis sağlayıcılarına, çocuk pornografisi, kumar, uyuşturucu kullanımı, terörizm ve ırkçılık gibi konularda içerik yayınlayan web sitelerinin kaydını tutarak sürekli güncellenen bir kara liste vermekte ve bu listede bulunan sitelerin engellenmesi ve filtrelenmesi konusunu takip etmektedir. Yapmış olduğu kontrollerle yasaklı içeriği kaldırmayan veya kaldırılmasında geciken internet servis sağlayıcıları 50.000 Euro para cezası ile cezalandırılmaktadır. İnternet servis sağlayıcılarının aynı zamanda kara listede bulunan ve engellenmesi öngörülen sitelerin erişiminin zorlaştırılması için her türlü tedbiri alması beklenmektedir. Kendilerine bildirilmesinden en geç 6 saat içinde gereken tedbir ve filtrelemelerin yapılması gerekmektedir[277].

Her ne kadar Almanya internet sansürleme, filtreleme ve erişim engellemesi konularında genel anlamda uluslararası kuruluşlardan düşük puan almış olsa da Google şeffaflık raporunu göre, Alman hükümeti Amerika'dan sonra aktif olarak en çok data talebinde bulunan ülke olmuştur[278]. Freedom House isimli uluslararası kuruluşun raporuna göre[279], internet statüsü özgür olarak belirtilen Almanya, araştırmada incelenen 100 ülke arasında internet özgürlüğü sıralamasında da 19. sırada yer almaktadır.

3.8. İnternete Erişim Engeleme ve Filtreleme Uygulamalarının "İfade Özgürlüğü" Bağlamında Değerlendirilmesi

İfade özgürlüğü, anayasa ve insan hakları ile ilgili düzenlemelerde yer alan

[276] Kılınç, **a.g.e**., s. 426.
[277] (çevrimiçi) https://www.t-online.de/nachrichten/deutschland/id_19158670/kinderpornografie-bundestag-beschliesst-gesetz-zur-internet-sperre.html, Erişim: 6 Eylül 2019.
[278] Semih Sönmez, "Google şeffaflık raporunu yayınladı", 20/07/2016, (çevrimiçi) https://www.dunyahalleri.com/google-seffaflik-raporunu-yayinladi/, Erişim: 6 Eylül 2019.
[279] "Freedom on the Net Countries", 2018, (çevrimiçi) https://freedomhouse.org/report/countries-net-freedom-2018, Erişim: 6 Eylül 2019.

temel haklardan bir tanesidir. İfade özgürlüğü kavramı, kişinin kendi zihin dünyasında bulunan, istemediği sürece kimse tarafından bilinemeyecek olan düşüncesini, diğer kişilerin de öğrenmesi amacıyla kelimelere dökebilme serbestisi olarak ifade edilebilmektedir[280].

İfade özgürlüğünün ortaya çıkışı ilk kez Protestan hareketin kiliseye muhalefeti ile gerçekleşmiştir. 16. yüzyıldaki bu karşı duruş, ifade özgürlüğünün ilk nüvesi olarak değerlendirilmektedir. İfade özgürlüğü kavramı, inanç özgürlüğü ve düşünce özgürlüğü kavramları ile birlikte ele alınmaktadır. İnanç özgürlüğü ile oldukça ilişkili bir kavram olan ifade özgürlüğünün, hukuki olarak ortaya çıkışı ise İngiltere'de 1689 Haklar Bildirisi (*Bill of Rights*) ile olmuştur[281].

İfade özgürlüğü, Avrupa İnsan Hakları Sözleşmesi (AİHS)'nde 10. maddede düzenlenmiştir. İki paragraf olarak düzenlenen maddenin ilk paragrafında ifade özgürlüğü kavramının tanımı, ikinci paragrafında ise ifade özgürlüğü ile ilgili sınırlamalar belirtilmiştir[282]. II. Dünya Savaşı'ndan önce, Almanya'da Nasyonal Sosyalistlerin, Alman Anayasası'nda var olan özgürlüklerden faydalanarak iktidara gelmeleri, demokrasilerin her zaman baskıcı rejimlere karşı üstünlük sağlayabileceği inancının mutlaklığını kaybetmesine neden olmuştur. Özgürlüklere, kendisini ortadan kaldırabilecek durumları engelleyecek sınırlar çizilmesi II. Dünya Savaşı sonunda Avrupa'nın kabul ettiği bir ilke hâline gelmiş ve AİHS'de bu durum somut bir hale gelmiştir[283].

AİHS, daha önce de belirtildiği üzere, ifade özgürlüğünün sınırlarını 10. maddenin ikinci paragrafında belirlemiştir. Bu sınırlamalar ile ilgili olarak da Avrupa İnsan Hakları Mahkemesi (AİHM) tarafından ölçütler belirlenmiştir. Bu ölçütler; gereklilik ve orantılılıktır. Bu ölçütlerin bulunmadığı durumlarda ifade özgürlüğünün kısıtlanması mümkün olmamaktadır. İnternet ile ilgili erişim engellemesi ve filtreleme

---

[280] Mehmet Emin Akgül, "İfade Özgürlüğünün Tarihsel Süreci ve Milli Güvenlik Gerekçesiyle İfade Özgürlüğünün Kısıtlanması", **AUHFD**, C. LXI, S: 1, 2012, s. 3.
[281] Elisabeth Zoller, "Freedom of Expression: Precious Right in Europe, Sacred Right in The United States", **Indiana Law Journal**, Vol: 84, I. 3, 2009, s. 803.
[282] "Avrupa İnsan Hakları Sözleşmesi", s. 11-12, (çevrimiçi) https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf, Erişim: 12 Eylül 2019.
[283] Münci Kapani, **Kamu Hürriyetleri**, Ankara, Yetkin Yayınları, 1993, s. 221-222.

konularında da bu ölçütler dikkate alınmalıdır; bu gerek milletler arası sözleşmelerden gerek anayasal düzenlemelerden kaynaklanan bir zorunluluktur[284].

İnternet, iletişim alanında yaşanan gelişmeler bağlamında günümüzde en çok kullanılan kitle iletişim araçlarından biri haline gelmiştir. Bilgi alış-verişinin hızlı, ucuz ve kolay şekilde yapılabildiği internet ortamında aynı zamanda eğitim, ticaret ve sosyal alanlarda da faaliyetlerde bulunulabilmektedir[285]. Bu derece yoğun şekilde kullanılan internet ortamında ifade özgürlüğü-güvenlik ikilemi de zor bir alan olarak karşımıza çıkmaktadır.

İnternet üzerinden bilgiye ulaşmanın ve yaymanın kolaylığı, kötü niyetli kişi ve grupların da ilgisinin bu alana kaymasında etkili olmuştur. Topluma zarar verebilecek bilgilerin elde edilerek internette yayılması olumsuz birtakım olayların yaşanmasına neden olabilecektir. Bunun yanında gerek çıkar amaçlı suç örgütlerinin gerekse de terör örgütlerinin, propaganda yapmak, gizli iletişim kurmak ve finansal kaynaklarını arttırmak amacıyla internet ortamını kullandıkları da bilinmektedir. Yine mafya ve terör organizasyonları, sanal bankalar yardımıyla finansman sağlayarak ayakta kalmakta, kazandıkları yasa dışı paraları yine internet üzerinden aklamak suretiyle yasal hale getirmektedirler[286].

AİHS'nin ifade özgürlüğü ile ilgili maddesinin ikinci paragrafında[287] bahsi geçen konularda ifade özgürlüğü noktasında kısıtlamaya gidilebilecektir. Ancak özellikle ulusal güvenlik ile ilgili konuların belirlenmesi sürecinde birtakım sorunlar yaşanmaktadır. Ulusal güvenlik, subjektif bir konudur. Başka bir ifade ile her ülkenin kendi ulusal güvenliğini sağlaması için farklı tehdit türleri ve tanımlamaları bulunmaktadır. Bu nedenle uluslararası seviyede, ulusal güvenlik algılamaları ile ilgili

---

[284] Dülger, **a.g.e**., s. 1488.
[285] Manuel Castells, **Enformasyon Çağı: Ekonomi, Toplum ve Kültür-Binyılın Sonu,** C. III, (çev. Ebru Kılıç), İstanbul, Bilgi Üniversitesi Yayınları, 2007, s. 62-63.
[286] Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu**, Ankara, Turhan Kitabevi, 2007, s. 125-126.
[287] AİHS 10. madde ikinci paragraf; "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" şeklindedir.

üzerinde tam olarak anlaşmaya varılmış tanımlamalara rastlamak zor olmaktadır. AİHM'in önüne gelen, ifade özgürlüğünün ulusal güvenlik kısıtı ile engellenmesi ile ilgili dosyalarda, ülkelerin kendilerine göre belirledikleri güvenlik kıstaslarına göre mi yoksa AİHS'ne göre mi karar vereceği noktasında da zaman zaman anlaşmazlıklar ortaya çıkmaktadır[288].

Ulusal güvenlik gerekçeleri ile birçok ülke, global olarak hizmet vermekte olan Facebook, Whatsapp, Twitter vb. uygulamaları ve diğer sosyal medya platformlarıyla, kendi kurumları aracılığı ile işbirliği yapma yoluna gitmektedir. Uluslararası olarak önemle takip edilen terörizm suçları, çocuk istismarı ve uyuşturucu ticareti gibi birçok alanda anlaşmalar yapılmıştır. Bunun yanı sıra her ne kadar "merkezi olmadığı" iddia edilse de ABD'nin internetin merkezi olduğu düşünüldüğü için, başta Avrupa ülkeleri olmak üzere birçok ülkenin, kişisel bilgilerin güvenliği ve sanal istihbarat zafiyeti endişesi ile interneti tarafsızlaştırma çabaları devam etmektedir. Bu çalışmalara ilave olarak belirtmek gerekir ki, dünyada birçok filtreleme ve kısıtlama uygulamaları bulunmaktadır. Devletlerin bu uygulamaları kullanma sebebi her ne kadar, pornografi, uyuşturucu ile mücadele, ulusal güvenlik gibi endişeler olsa da, uygulamada bu filtreleme yöntemleri suistimale açık olup, yönetimler tarafından çeşitli gerekçelerle farklı alanlarda da uygulanabilmektedir. Bu durum Çin ve Kuzey Kore başta olmak üzere diğer demokrasi ile yönetilen bazı ülkelerinde içinde bulunduğu birçok ülkede suistimal edilebilmektedir[289].

Suç unsuru bulunduran içeriklerin internet üzerinden yayınlanması ve bunların engellenmesi ile ilgili uygulamalar ve tartışmalar neticesinde basın özgürlüğü konusunda da birtakım endişelere yol açmıştır. Özellikle internet iletişimine yönelik uygulanacak kısıtlamalar ile ilgili endişeler de, terör eylemlerini yansıtma şekillerine getirilmesi önerilen sınırlamalardan kaynaklanmaktadır[290]. Bu noktada, internet üzerinden ne şekilde kısıtlamaların yapılacağı konusunda tartışmalar devam etmektedir[291]. İnternet iletişiminin engellenmesinin yasalarla, uluslararası

[288] Akgül, **a.g.e**., s. 25-26.
[289] Erdem Güven, "Juche İdeolojisinin Hizmetinde Gelenekselden Dijitale Kuzey Kore Medyası", **Selçuk İletişim**, C. XI, S: 1, 2018, s. 206.
[290] Çetin Özek, **Basın Özgürlüğünden Bilgilenme Hakkına**, İstanbul, Alfa Yayıncılık, 1999, s. 15-16.
[291] Murat Volkan Dülger, **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2004, s. 328-329.

sözleşmelerle, ulus üstü kurumlarca veya kendi kendine olması gerektiği şeklinde farklı görüşler bulunmaktadır. Ayrıca bu sınırlamalar yapılırken kişilerin bilgi edinme hakları asgari seviyede etkilenmelidir. Yine yapılacak sınırlamaların, siyasal iktidarların basını ya da muhalif sesleri engellemek amacıyla araç haline dönüşmesi önlenmelidir[292].

Bütün bu gelişmeler ışığında değerlendirildiğinde; internette oluşabilecek güvensiz ortam nedeniyle, devletlerin ve hükümetlerin ulusal güvenlik algısında birtakım değişiklikler meydana gelmiştir. Devletlerin ulusal güvenlik kaygıları, internette erişim engelleme ve filtreleme yöntemlerinin fazlaca kullanılmasına neden olmaktadır. Buna karşın internet kullanıcıları her geçen gün yeni teknik ve yöntemlerle filtreleme ve erişim engellemelerini aşmaya çalışmakta ve aradığı içeriğe ulaşmaktadır. Birçok özel ve devlete bağlı kurum ve kuruluş, yeni trendleri takip ederek erişim ve filtreleme yöntemi geliştirilmekteyken, aynı şekilde oluşan market talebini karşılamak için özellikle "Silikon Vadisi"[293] başta olmak üzere onlarca yeni şirket kurulmakta ve erişim engellemesine yönelik VPN (sanal özel ağ) hizmeti sunmaktadır. İnternette filtreli ve yasaklı sitelerin arasında anonim bir şekilde gezinme imkanı sağlayan VPN uygulamalarının, artan talep neticesinde 2024 yılına kadar yaklaşık olarak 50 milyar dolara ulaşan market değerlerine sahip olması beklenmektedir. 'İnternet by-pass'ı olarak da tabir edilebilecek bu yöntem, internet kullanıcılarına anonim olarak internette dolaşma imkanı sağlamakta bu da suç işleme amacı olan veya anonim olarak düşüncesini ifade etmek isteyen kişilere gizlilik sağlamakta ve takip edilebilirliğini zorlaştırmaktadır[294].

[292] Dülger, **a.g.e**., 2007, s. 1496.
[293] Ayrıntılı bilgi için bknz. Ankara Kalkınma Ajansı, **Ankara KalkınmaAjansı Silikon Vadisi Ziyareti ve Bilişim Ekosistemi Dünya Örnekleri**, Kasım 2012, (çevrimiçi) http://www.ankaraka.org.tr/archive/files/yayinlar/raporlar/silikon-vadisi-ziyaret.pdf, Erişim: 12 Eylül 2019.
[294] N. Özlem Ünverdi ve Zeynep Yüksel, "Ağ Güvenliği ve Güvenlik Duvarında VPN Uygulaması", (çevrimiçi) http://www.emo.org.tr/ekler/c246594da24758e_ek.pdf, Erişim: 12 Eylül 2019.

SONUÇ

Sovyetlerin yıkılması ile son bulan Soğuk Savaş'ı takip eden süreçte uluslararası sistem yeniden şekillenmeye başlamıştır. Bir tarafında ABD diğer tarafında SSCB'nin bulunduğu iki kutuplu sistem, çok kutuplu, bölgesel güç merkezlerinin ortaya çıktığı yeni bir ortama evrilmiştir. Bu yeni uluslararası sistemde ABD ise hegemonya olarak uluslararası yapıdaki yerini almıştır.

Uluslararası yapıdaki bu değişimlere teknoloji ve bilim alanlarındaki ilerlemeler ile küreselleşme olgusunu da eklediğimizde birçok kavramın kapsamının değiştiğini görebilmekteyiz. Bunlardan biri de güvenlik kavramıdır. Klasik güvenlik anlayışı askeri güç üzerine odaklanmaktadır. Ancak 20. yüzyılın sonlarında başlayan ve halen süren bu değişim süreci güvenliğin farklı boyutlarının ortaya çıkmasına sebep olmuştur. Güvenliğin, ekonomik, çevresel, sosyal ve siyasi boyutlarının ortaya çıkmasına ek olarak son yıllarda üzerinde çalışmaların giderek arttığı siber güvenlik boyutu da literatürdeki yerini almıştır.

Siber alan diye isimlendirilen tüm elektronik ortamları kapsayan sanal dünyanın güvenliğinin sağlanması da fiziki güvenlik kadar önemli bir hale gelmiştir. Dünya nüfusunun yarısından fazlasının internet kullanıcısı olduğu düşünüldüğünde siber güvenlik konusunun önemi daha iyi anlaşılabilecektir. Kişisel kullanımdan devlet boyutuna kadar her ölçeği yakından ilgilendiren siber güvenlik, kişisel kredi kartları ile ilgili yaşanabilecek dolandırıcılık olaylarından devletin gizli belgelerinin sızdırılmasına kadar çok geniş bir yelpazeyi içinde barındıran bir konudur.

İnternet ve bilgisayar sistemleri ile iletişim hatlarının tamamında güvenlik sağlamak çok kolay bir durum değildir. Bu alanda işlenen suçlar için en kapsayıcı kavram olan bilişim suçları, her geçen gün farklılaşabilmekte ve güvenliği tehdit eder duruma gelmektedir. Bilişim suçları ile yalnızca kişi güvenliği tehdit altında değildir.

Özellikle devletler ölçeğinde karşı kaşıya kalınan bilişim suçları kimi zaman devletin ulusal güvenliğini doğrudan hedef alır nitelikte olabilmektedir.

İnternet ortamında işlenen bilişim suçlarının artışının arkasında yatan birçok sebep bulunmaktadır. İnternete erişimin kolay ve ucuz olması, kişilerin özel ve gizli bilgilerine ulaşabilme ve ele geçirmenin nispeten kolaylığı, çok fazla enerji gerektirmeyen suç işleyebilme imkânları, bu sebeplerden yalnızca birkaçı olarak sayılabilir. Bir başka deyişle, teknolojik ilerlemeleri kendi çıkarları için kullanmayı planlayan, bu durumdan haksız kazanç elde etmeye çalışan kişiler ve örgütler için siber alan fazlasıyla çekici bir ortam olarak ifade edilebilir.

Bilişim suçlarında artış yaşanmasının önemli sebeplerinden bir tanesi de henüz yeterli altyapıya sahip olunamadığı halde bilişim sistemlerinin çok hızlı bir şekilde her alana girmesiyle ilgilidir. Yine sanal dünyadaki karmaşık düzen bilişim suçlarının kolaylıkla işlenmesine zemin hazırlamaktadır. Bilişim alanındaki suçların gündelik hayatın içine bu denli girmesine rağmen farkındalık seviyesinin halen yeterli bir noktada olmadığını söylemek yanlış olmayacaktır. Bu sebeple ulusal ve uluslararası seviyelerde bilişim suçları ile ilgili farkındalık yaratacak strateji ve politikalar üretmek devletlerin üzerinde durması gereken konulardan birisi haline gelmiştir.

Bilişim suçları, her bireyin ya da organizasyonun işleyebileceği bir suç türü değildir. Bilişim suçu işleyecekler belirli bir yetenek ve bilgi birikimine sahip olmak durumundadır. Bilgi seviyesi ve yeteneği işlenecek bilişim suçunun niteliğini de etkilemektedir. Bu sebeple her geçen gün farklı seviyelerde işlenen bilişim suçlarının niteliği de değişmektedir. Bu haliyle bilişim suçlarına yönelik geliştirilecek önleme faaliyetlerinin de niteliğinin artması gerekmektedir. Bu da bilişim suçlarının dinamik bir yapıya sahip olduğunu ve bununla mücadele etmek için de alınacak önlemlerin bu yapıya uyum sağlaması gerektiğini göstermektedir.

Bilişim suçları ile mücadele konusunda kamu kurumları kadar özel şirketler de çalışmalar yapmaktadır. Son yıllarda online alışveriş miktarındaki artışlar nedeniyle ve kendi sistemlerinin güvenliği için bir çok özel şirket, içerisinde yeni bir departman olarak siber güvenlik birimleri kurmaya ve bu alanda çalışabilecek kişileri/grupları

istihdam etmeye başlamışlardır. Aksi halde bilişim yoluyla karşı karşıya gelebileceği risk ve tehditler sonucunda şirketin sadece maddi kaybı olmayacak ve belki de piyasadaki imajı da ciddi şekilde zedelenecektir.

Bilişim suçlarını önlemede siber güvenlik birimlerinin oluşturulması da aslında tek başına yeterli olmayabilir. Bu konudaki eğitim ve farkındalığın arttırılması gibi hususlar da önem arz etmektedir. Güvenliğin sağlanması adına teknolojinin geliştirilmesi bilişim suçu işleyen kişi/grupları insan unsurunun zafiyetlerinden faydalanmaya itmektedir. Bir başka deyişle güvenliği sağlama noktasında en zayıf halka insan unsuru olmaktadır. Dolayısıyla insan unsuruna bağlı olarak meydana gelebilecek siber güvenlik risklerini sıfıra indirgemese de minimum düzeye çekebilecek farkındalığın oluşturulması gerekmektedir. Farkındalık düzeyini arttırmak için bu konuda eğitimler verilebilir.

Bilişim suçları ile mücadele edebilmek adına özel sektörde olduğu gibi ve belki de daha fazla kamuda da bu konuda çalışmalar yapılmaktadır. Gerek Türkiye'de gerekse dünyanın diğer ülkelerinde bilişim suçlarını önlemeye yönelik birçok adım atılmaktadır. Bunlardan bir tanesi de bilişim suçlarıyla ilgili hazırlanan hukuki düzenlemelerdir.

Türkiye'de bilişim suçları ile ilgili ilk hukuki düzenleme 1991 yılında onaylanan 3756 sayılı eski Türk Ceza Kanunudur. Bu kanunda çok dar kapsamlı da olsa bilişim suçlarına 4 maddelik bir yer verilmiştir. Daha sonraki yıllarda farklı kanun ve maddelerde yer verilen bilişim suçları ile ilgili en kapsamlı düzenleme, 2007 senesinde onaylanan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile yapılmıştır. Yine 5271 sayılı Türk Ceza Kanunu'nda da bilişim suçları ile ilgili maddeler bulunmaktadır. Buna ilave olarak uluslararası kurumlar tarafından hazırlanan düzenlemeler de Türkiye'nin bilişim suçları kapsamındaki çalışmalarını etkilmektedir. 2001 yılında onaylanan, 2004 yılında yürürlüğe giren Avrupa Konseyi Siber Suçlar Sözleşmesi'ne Türkiye'nin imza atması 2010 yılında gerçekleşmiştir. 2014 yılında Türkiye'de de yürürlüğe girmesi ile birlikte uluslararası işbirlikleri ve

ortak çalışmaların yapılması daha kolay hale gelmiştir. Bu haliyle bilişim suçları uluslararası bir nitelik kazanmıştır.

Bilişim suçlarını önleme noktasında devletler tarafından kullanılan bir diğer yöntem de bir çok tartışmaya da konu olan internete erişimin engellenmesidir. İnternete erişimin engellenmesi hem Türkiye hem de dünyanın hemen her ülkesinde uygulanan bir yaptırım şeklidir.

Türkiye'de erişim engellenmesi sürecine bakıldığında, 5651 sayılı Kanun, 5846 sayılı Fikir ve Sanat Eserleri Kanunu ve hukuk mahkemeleri tarafından verilen ihtiyati tedbir kararları karşımıza çıkmaktadır. Bu üç hukuki düzenleme nedeniyle erişimin engellenmesi kararı verilebilmektedir. Özellikle 5651 sayılı Kanun erişimin engellenmesi konusu ile ilgili doğrudan ilişkilidir.

5651 sayılı Kanun'un, müstehcenlik ile ilgili maddesi nedeniyle kimi zaman veriler erişimin engellenmesi kararları toplumun farklı kesimlerinden tepkilere neden olabilmektedir. Bu tepkilerin temelinde müstehcenlik konusunda hangi kriterlerin gözetildiği konusunda net bir ayrımın olmadığı iddiasıdır. Yine yetkili mahkemelerce verilen erişimin engellenmesi kararları da kimi zaman daha yoğun tepkiler çekmektedir. Youtube, milyarlarca videonun bulunduğu ve dünyanın her yerinden erişimin sağlandığı bir internet sitesi olmasına rağmen birkaç sakıncalı içeriğe sahip video bulunduğu iddiası ile tamamen siteye ulaşımın engellenmesi örneğinde olduğu gibi benzeri olaylarda da toplumun tepkisi olmuştur. Bu durumu hak ve özgürlüklere müdahale olarak görenlerin sayısı da az değildir.

İlgili mevzuat hükümlerince çok sayıda internet sitesinin yasaklandığını görmekteyiz. Daha önce de belirtildiği üzere, bu sitelerin bir kısmına erişimin engelenmesi toplum tarafından kabul görürken diğer kısmı da toplumun tepkisini çekmiştir. Diğer bir açıdan bakıldığında ise kapatılan sitelere yönelik ilginin azalmadığı ve yasaklı sitelere erişim için farklı yöntemler kullandığı görünmektedir.

İnternete erişim engellemesi konusunda dünya uygulamalarına bakıldığında, ortak noktaların oldukça az olduğu yalnızca çocuk istismarı ve pornografisi ile ilgili sitelerin engellenmesi konusunda uzlaşı olduğunu görmekteyiz. Dünya üzerindeki

erişim engellemelerinin genel olarak kumar, intihara yönlendirme, uyuşturucu maddeye yönlendirme, patlayıcı madde yapımı gibi konularda uygulanmaktadır. Bunun yanında politik, dini ve kültürel sebeplerle internete erişimi engelleyen Çin ve İran gibi ülkelere sansür niteliği taşıyan bu engellemeler nedeniyle uluslararası ölçekte tepkiler olmaktadır. Daha önce de belirtildiği üzere Türkiye'deki internete erişim engellemelerinin kapsamlı bir sansür uygulaması olduğunu söylemek doğru olmayacaktır.

Demokrasinin egemen olduğu ülkelerde devlet yönetimi elbette toplumu, aileyi, çocukları korumak ve kollamak konusunda gereken herşeyi yapmakla yükümlüdür. Bunu yapmak için en kısa ve kolay yol olan yasaklamayı seçmek her zaman doğru ve istenen sonuçlar doğurmayabilir. Öncelikle yasaklamak yerine bu konuda kişilerin eğitilmesi ve öz denetim yeteneklerinin kazandırılması daha uygun olabilir.

Bu çalışmanın sonunda şunu belirtmek uygun olacaktır; bilişim suçlarının önlenmesi amacıyla devletlerin, internete erişimi engellemesinin, çok haklı olabileceği durumların yanında, net sınırları ve kriterleri belirlenmemiş konularda da gerçekleşmesi durumunda toplum tarafından kişisel hak ve özgürlüklerine müdahale edildiği algısının oluşabileceği değerlendirilmektedir.

KAYNAKÇA

KİTAPLAR, SÜRELİ YAYINLAR, TEZLER ve MEVZUAT

Akarslan, Hüseyin :**Bilişim Suçları,** Seçkin Yayıncılık, Ankara, 2012.

Akdeniz, Yaman ve

Altıparmak, Kerem :**İnternet: Girilmesi Tehlikeli ve Yasaktır-Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme**, Kasım 2008, s. 6-7. (çevrimiçi) https://docplayer.biz.tr/749780-Dr-yaman-akdeniz-dr-kerem-altiparmak-kasim-2008.html, Erişim: 17 Ağustos 2019.

Akgül, Mehmet Emin :"İfade Özgürlüğünün Tarihsel Süreci ve Milli Güvenlik Gerekçesiyle İfade Özgürlüğünün Kısıtlanması", **AUHFD**, C. LXI, S: 1, 2012, ss. 1-42.

Akkuş, Bülent :"Özgürlük ve Güven(siz)lik İkileminde Siber Uzay", Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı, İstanbul, 2013.

Akleylek, Sedat ve

Tok, Zeliha Yüce :"Siber Güvenlikte Kriptoloji", **Siber Güvenlik Çalıştayı Raporu**, Ankara, 2011.

Alaca, Bahaddin :"Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle)",

Yüksek Lisan Tezi, Ankara Üniversitesi Antropoloji Anabilim Dalı, Ankara, 2008.

Aliusta, Cahit ve

Benzer, Recep :"Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dâhil Olma Süreci", **Uluslararası Bilgi Güvenliği Mühendisliği Dergisi**, C. IV, No: 2, 2018, ss. 35-42.

Altunok, Ebru ve

Vural, Ali Fatih :"Bilişim Suçları", **Denetişim**, 2011, ss. 74-84.

Arı, Tayyar :**Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İşbirliği,** (7. Baskı), Bursa, MKM Yayıncılık, 2011.

Andrews, Edmund L. :"German Court Overturns Pornography Ruling Against Compuserve", 1999, (çevrimiçi) https://archive.nytimes.com/www.nytimes.com/library/tech/99/11/biztech/articles/18compuserve-germany.html, Erişim: 3 Eylül 2019.

Ankara Kalkınma Ajansı :**Ankara KalkınmaAjansı Silikon Vadisi Ziyareti ve Bilişim Ekosistemi Dünya Örnekleri**, Kasım 2012, (çevrimiçi) http://www.ankaraka.org.tr/archive/files/yayinlar/raporlar/silikon-vadisi-ziyaret.pdf, Erişim: 12 Eylül 2019.

Artuk, Mehmet Emin,

Gökcen, Ahmet ve

Yenidünya, Ahmet Caner :**Türk Ceza Kanunu Şerhi**, C. V, Ankara, Turhan Kitapevi, 2009.

Aslay, Fulya : "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", **International Journal of Multidisciplinary Studies and Innovative Technologies,** C. 1, No: 1, 2017, ss. 24-28.

Ayman, Gülden :**Neo-realist Bir Perspektiften Soğuk Savaş Sonrası Yunan Dış Politikası Güç Tehdit ve İttifaklar**, Ankara, SAEMK Yayınevi, 2001.

Aytaç, Gizem Bilgin :"Human Security Concepts For NGO's in Post Intervention Societies- A Case Study In Iraq", **Journal of International Social Research**, Vol. X, I: 50, 2017, ss. 167-173.

Baldwin, David A. :"The Concept of Security", **Review of International Studies**, No: 23, 1997, ss. 14.

Baharçiçek, Abdulkadir ve

Ağır, Osman :"Rusya'nın Başarısız Demokratikleşme Tarihi", **Birey ve Toplum**, C. IV, S: 8, Güz 2014, ss. 5-27.

Balzacq, Thierry :"The Three Faces of Securitization: Political Agency, Audience and Context", **European Journal of International Relations**, C. XI, S: 2, 2005, ss. 171-201.

Baycan, Pelin :"Sosyal Medyanın Y Kuşağı Satın Alma Davranışı Üzerindeki Rolü", Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi Dış Ticaret Enstitüsü, İstanbul, 2017.

Baylis, John ve

Baylis, John :"Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, C. V, S: 18, 2008, ss. 69-85.

Bayrak, Halil :"TUİK Türkiye'nin İnternet Kullanım Alışkanlıkları Raporu", 17 Ağustos 2018, (çevrimiçi) https://dijilopedi.com/tuik-turkiyenin-internet-kullanim-aliskanliklari-raporu/, Erişim: 20 Ağustos 2019.

Baysal, Başar ve

Lüleci, Çağla :"Kopenhag Okulu ve Güvenlikleştirme Teorisi", **Güvenlik Stratejileri**, C. XI, S: 22, 2015, ss. 61-96.

Beck, Verlag C.H. :United Nations: Law, Policies and Practice, Edt. Rüdiger Wolfrum, C: I, Munich, Martinus Nijhoff Publishers, 1995, s.405-406-; Jobst Delbrück, "Collective Security", **Encyclopedia of Public International Law**, Edt. Rudolf Bernhardt, Oxford, Elsevier, 1982, ss. 104-107.

Bellany, Ian :"Towards a Theory of International Security", **Political Studies**, Vol: XXIX, I: 1, 1981, ss. 102.

Booth, Ken :Ken Booth, "Security and Self: Reflections of a Fallen Realist", **Critical Security Studies: Conceptsand Cases**, 1997, ss. 84.

Booth, Ken :"Güvenlik ve Özgürleştirme", **Avrasya Dosyası Güvenlik Bilimleri Özel**, Çev. Çiğdem ŞAHİN, C: IX, No: 2, 2003, ss. 51-70.

Budak, Leyla ve

Erdoğan, İlker :"1990 Sonrası Çin Halk Cumhuriyeti'nde Kitle İletişim Sistemi ve Temel Sorunlar", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,** Yıl: 5, S: 9, Bahar 2006/1, ss. 109-123.

Buzan, Barry :People, **States and Fear: An Agenda for International Security Studies in the Post-Cold War Era**, Great Britain, Harvester Wheatsheaf, 1991.

Buzan, Barry,

Waever, Ole ve

de Wilde, Jaap :**Security: A New Framework for Analysis**, Colorado, Lynne Rienner Publishers Inc, 1998.

Buzan, Barry ve

Waever, Ole :**Regions and Powers: The Structure of International Security**, Cambridge, Cambridge University Press, 2003.

Canata, Fatih :"5651 Sayılı Kanun Kapsamında İnternet Düzenlemeleri ve Düşünce-İfade Özgürlüğü Üzerine Bir Değerlendirme", **Türk Kütüphaneciliği**, C. XXX, S: 2, 2016, ss. 185-205.

Canbek, Gürol ve

Sağıroğlu, Şeref :"Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi**, C. IX, S: 3, 2006, ss. 165-174.

Canbek, Gürol ve

Sağıroğlu, Şeref :"Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", **Gazi Üniv. Müh. Mim. Fak. Dergisi,** C. XXII, No: 1, 2007, ss. 121-136.

Castells, Manuel :**Enformasyon Çağı: Ekonomi, Toplum ve Kültür-Binyılın Sonu,** C. III, (çev. Ebru Kılıç), İstanbul, Bilgi Üniversitesi Yayınları, 2007.

Cebeci, Münevver :Münevver Cebeci, "Tehdit Algılamasında Yapısal ve Konjonktürel Nitelikler / İthal Tehditler", **Türkiye'ye Yönelik Dış Kaynaklı Risk ve Tehditler Sempozyum Bildirileri**, Harp Akademileri Komutanlığı, İstanbul, 2007, ss. 33

Cebeci, Kemal :"Küreselleşme Bağlamında Ulus-Devletin Egemenlik Gücünün Dönüşümü", **Sayıştay Dergisi**, No: 71, 2008, ss. 23.

Cevizci, Ahmet :**Paradigma Felsefe Sözlüğü**, İstanbul, Paradigma Yayıncılık

Collins, Alan :**Contemporary Security Studies**. New York, Oxford University Press, 2007.

Congar, Kerem :"İnternetin en çok yasaklandığı ülkeler hangileri?", 30 Ağustos 2018, (çevrimiçi) https://tr.euronews.com/2018/08/30/internet-en-cok-hangi-ulkelerde-yasaklaniyor-, Erişim: 17 Ağustos 2019.

Çakmak, Cenap :"Realist Teori, Uluslararası İlişkilere Etkisi ve Kritiği", **Kamu Hukuku Arşivi Dergisi**, S: 9, 2006, ss. 44-55.

Çakmak, Haydar ve

Demir, Cenker Korhan :"Siber Dünyadaki Tehdit ve Kavramlar", (ed. Haydar Çakmak ve Taner Altunok, **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, 1. Baskı, Ankara, Barış Platin Kitabevi, 2009, ss. 23-54.

Çeken, Hüseyin :"ABD'de İnternet Yoluyla İşlenen Suçlara İlişkin Düzenlemeler", **Adalet Dergisi**, Sy.114, 2002.

Çeken, Hüseyin : "ABD'de Siber Suçlar", http://www.jura.uni-sb.de/turkish/HCeken.html, Erişim: 10 Temmuz 2019.

Çelikpala, Mitat :"Geçmişten Günümüze Vazgeçilemeyen Kavram: Ulusal Çıkar", **H.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi,** C. XXIII, S: 1, 2005, ss. 439-461.

Çetinkaya, Şeref :"Güvenlik Algılaması ve Uluslararası İlişkiler Teorilerinin Güvenliğe Bakış Açıları", **21. Yüzyılda Sosyal Bilimler Dergisi**, Sayı: 2, 2012, ss. 242.

Çınkı, Mustafa :**Rant Lordları**, Ankara, Karlar Yayınevi, 2004.

Çifçi, Hasan :**Her Yönüyle Siber Savaş**, İstanbul, TÜBİTAK Popüler Bilim Kitapları, 2013.

Çolak, H. :"Siber Terör, Yargılama Usulü ve Önleyici Tedbirler", **Kazancı Hakemli Hukuk Dergisi**, 2011, S: 79-80, ss. 62-142.

Çomak, Hasret :**Uluslararası İlişkilere Giriş: Teorik Bakış**, Kocaeli, Umuttepe Yayınları.

Çömlek, Savaş :"Özgür Uçkan: İnterneti sansür girişimi olan SOPA yasası geçerse, tüm dünya Çin'e benzeyecek", 2012, (çevrimiçi) https://yesilgazete.org/blog/2012/01/20/ozgur-uckan-interneti-sansur-girisimi-olan-sopa-yasasi-gecerse-tum-dunya-cine-benzeyecek/, Erişim: 3Eylül 2019.

Dant, Tim :Knowledge, **Ideology and Discourse: A Sociological Perspective, London**, Routledge Press, 1991.

Darıcılı, Ali Burak ve Özdal, Barış :"Analysis of the Cyber Security Strategies of People's Republic of China", **Güvenlik Stratejileri Dergisi**, Yıl: 14, S: 28, 2018, ss. 1-36.

Dedeoğlu, Beril :**Uluslararası Güvenlik ve Strateji**, İstanbul, Yeniyüzyıl Yayınları, 2008.

Dedeoğlu, Beril :**Dünden Bugüne Avrupa Birliği**, İstanbul, Boyut Kitapları, 2003.

Değirmenci, Olgun :**Mukayeseli Hukukta ve Türk Hukukunda Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama Suçu**, Ankara, Turhan Kitabevi, 2007.

Demir, Sertif :"Avrupa Güvenlik Mimarisinin Tarihsel Gelişimi ve Türkiye'nin Bu Güvenlik Mimarisindeki Yeri", **Güvenlik Stratejileri Dergisi**, No: 9, 2009, ss. 9-51.

Demirel, Mustafa

Yörük, Muhsin ve

Özkan, Okan :"Çocuklar İçin Güvenli İnternet: Güvenli İnternet Hizmeti ve Ebeveyn Görüşleri Üzerine Bir Araştırma", **Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. IV, S: 7, 2012, ss. 54-68.

Denk, Nevzat :**21. Yüzyıla Girerken Türkiye'nin Jeopolitik Durumu**, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1998.

Dijital Platform İletişim : **İletişim Şurası Notları**, Ankara, 20-21 Şubat 2003.

Dura, Cihan ve

Atik, Hayriye :**Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye**, İstanbul, Literatür Yayınları, 2002.

Dülger, Murat Volkan :**Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2009.

Dülger, Murat Volkan :"İnternet İletişiminin Engellenmesinin Hukuki Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", **İstanbul Barosu Dergisi**, C. LXXXI, S: 2007/4, 2007, ss. 1477-1545.

Erkan, Boğaç ve

Songür, Murat :**Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü**, Ankara, Hacettepe – Taş Yayınevi, 1999.

Forde, Steven :"International Realism and The Science of Politics: Thucydides, Machiavelli and

Neorealism", **International Studies Quarterly**, C. XXXIX, S: 2, 1995, ss. 141-159.

Froomkin, Michael :"The Internet as a Source of Regulatory Arbitrage", **Borders in Cyberspace: Information Policy and the Global Information Infrastructure**, Brian Kahin ve Charles Nesson (edt.), USA, MIT Press, 1997, ss. 129-164.

Gönen, Serkan,

Ulus, Halil İbrahim ve

Yılmaz, Ercan Nurcan :"Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme", **Bilişim Teknolojileri Dergisi**, C. IX, S: 3, 2016, s. 229-236.

Gözler, Kemal :**Türk Anayasa Hukuku Dersleri**, Ekin Kitabevi, Bursa, 2007.

Gustin, Joseph F. :**Cyber Terrorism: A Guide for Facility Managers**, The Fairmont Press, Georgia, 2003.

Güneştaş, Murat

ve Diğerleri :"Siber Terörizm: Motivasyon ve Yöntem", (ed. Fatih Tombul ve diğerleri), **Siber Suçlar, Tehditler, Farkındalık ve Mücadele**, Ankara, Global Politika ve Strateji, ss. 85-113.

Güntay, Vahit :"Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi**, S: 27, ss. 79-111.

Güven, Erdem :"Juche İdeolojisinin Hizmetinde Gelenekselden Dijitale Kuzey Kore Medyası", **Selçuk İletişim**, C. XI, S: 1, 2018, ss. 190-211.

Harp Akademileri Komutanlığı :**Geçmişte ve 21. Yüzyılda Savaşlar: Stratejiler ve Stratejiler**, İstanbul, Harp Akademileri Basımevi, 2002.

Hekim, Hakan :"Oltalama (Phishing) Saldırıları", **Siber Tehditler ve Sorunlar**, 2015, ss. 57-83.

Henkoğlu, Türkay ve

Yılmaz, Bülent :"İnternet Erişim Özgürlüğünün Kısıtlanması: Türkiye Üzerine Bir Değerlendirme", **Bilgi Dünyası**, C. XIV, S: 2, 2013, ss. 215-239.

Hetne, Björn :"Teori ve Pratikte Güvenliğin Bölgeselleşmesi", **Uluslararası İlişkiler Akademik Dergisi**, C: V, No: 18, Yaz 2008, s. 90-91, (çevrimiçi) http://www.uidergisi.com.tr/wp-content/uploads/2011/06/Teori-ve-Pratikte-Guvenligin-Bolgesellesmesi.pdf, 16 Aralık 2016.

İçel, Kayıhan vd. :**Avrupa Birliği'ne Uyum Sürecinde Türk Ceza Hukuku**, Beta Yayınevi, İstanbul, 2000.

İsmail, Ergün :**Siber Suçların Cezalandırılması ve Türkiye'deki Durum**, Ankara, Adalet Yayınevi, 2008.

Jervis, Robert :"Cooperation under the Security Dilemma", **World Politics**, C. XXX, S: 2, 1978, ss. 167–174.

Kalaman, Sefer

Kaya, Elif ve

Kaya, Ünal :"Çin Halk Cumhuriyeti'nde Yeni Medya Uygulamaları: Nitel Bir Araştırma", **AJIT-e: Online Academic Journal of Information Technology**, C. IX, S: 32, 2018, ss. 101-122.

Kangal, Zeynel T. :"Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu", **İÜHFM**, C:LIX, S:1-2, İstanbul, 2001, ss. 227-240.

Kapani, Münci :**Kamu Hürriyetleri**, Ankara, Yetkin Yayınları, 1993.

Karacasulu, Z. Nilüfer :"Security and Globalization in the Context of International Terrorism", **Review of International Law and Politics**, C: II, No: 5, 2006, ss. 1-17.

Karacasulu, Z. Nilüfer :**Bölgesel Güvenlik Analizi Afganistan**, İstanbul, Beta Yayınları, 2011.

Karagülmez, Ali :**Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Seçkin Yayıncılık, Ankara 2014**.**

Karpowicz, W. Julian Korab :"How International Relations Theorists Can Benefit By Reading Thucydides", **The Monist**, C. LXXXIX, S: 2, 2006, ss. 232-244.

Kavaklı, Nurhan :"Güvenli İnternet Hizmeti Uygulaması'nın Yazılı Basında Sunumu: Haberlerdeki Aktörler ve Çerçevelemeler", **Galatasaray Üniversitesi İletişim Dergisi**, S: 17, 2012, ss. 63-83.

Keleştemur, Atalay :**Siber İstihbarat**, 1. Baskı, İstanbul, Yazın Basın Yayınevi, 2015.

Ketizmen, Muammer :**Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008.

Kılınç, Doğan :"Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S: 2, 2010, ss. 407-454.

Koçak, Hüseyin ve

Memiş, Kamile :"Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu", **Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi**, C. XX, S: 3, Aralık 2018, ss. 1-10.

Kolodziej, Edward A. :**Security and International Relations**, Cambridge, Cambridge Press, 2005.

Korkmaz, Gürol :**Terör ve Medya İlişkileri**, Ankara, Emniyet Genel Müdürlüğü Yayınları, No: 1999-1, 1999.

Köse, Güven ve

Özen, Kerem :"İnternet'te Sansür Üzerine Bir Değerlendirme", 2010, s. 115, (çevrimiçi) https://docplayer.biz.tr/1283326-Internet-te-sansur-uzerine-bir-degerlendirme.html, Erişim: 19 Ağustos 2019.

Kurt, Levent :Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, Ankara, 2005.

Küçükşahin, Ahmet ve

Akkan, Tamer :"Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", **Güvenlik Stratejileri Dergisi**, No: 5, 2007, ss. 43.

Levent, Ufuk :**21. Yüzyılın Eşiğinde Türkiye**, İstanbul, Harp Akademileri Komutanlığı Yayınları, 1997.

Hobbes, Thomas :**Leviathan** (Çev. Semih Lim), 18. bs., İstanbul, Yapı Kredi Yayınları, 2018.

L. Knutsen, Torbjorn :**A History of International Relations Theory: An Introduction**. Manchester, Manchester University Press, 1992.

Luciani, Giacomo :"The Economic Content Of Security", **Journal of Public Policy**, No: 8, 1989, ss. 149-158.

Manisalı, Erol :**Türkiye ve Küreselleşme**, İstanbul, Derin Yayınları, 2003.

Memiş, Tekin :"Erişimin Engellenmesi, Hukukî Sorunlar ve Çözüm Önerileri", **EÜHFD**, C. XIII, S: 3-4, 2009, ss. 161-176.

Morgenthau, Hans :**Politics Among Nations: The Struggle for Power and Peace**, New York, Alfred A. Knopf-McGraw Hill, 1948.

Mütercimler, Erol :**Geleceği Yönetmek: Yüksek Stratejiden Etki Odaklı Harekâta**, İstanbul, Alfa Yayınları, 2006.

M. Walt, Stephen :"The Renaissance of Security Studies", **International Studies Quarterly**, C: XXXV, No: 2, 1991, ss. 211-239.

Nicholson, Michael :**Formal Theories in International Relations**, Cambridge, Cambridge University Press, 1989.

Oğuzlu, Tarık :"Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", **Güvenlik Stratejileri Dergisi**, No: 6, 2007, ss. 7-42.

O'Rourke, James S. :"Google's Entry into the Chinese Market: A Lesson in Government Censorship and Corporate Reputation", **Journal of Business Strategy**, C. XXVIII, S: 3, 2007, ss. 12-22.

Özcan, Gencer :"Türkiye'de Siyasal Rejim ve Güvenlikleştirme Sorunsalı", **İktisat, Siyaset, Devlet Üzerine Yazılar**, İstanbul, Bağlam Yayınları, 2006, ss. 355-378.

Özek, Çetin :**Basın Özgürlüğünden Bilgilenme Hakkına**, İstanbul, Alfa Yayıncılık, 1999.

Özel, Cevat **:**"Bilişim ve İnternet Suçları Üzerine Bir İnceleme İnternet Hukuku", www.law.ankara.edu.tr/yazi, Erişim: 4 Mayıs 2019.

Özüdoğru, Uğur :BTK Siber Suç ile Mücadele Yöntemleri, Evrensel Uygulmaları ve Ülkemiz İçin Çözüm Önerileri, **Bilişim Uzmanlığı Tezi**, Ankara, Aralık 2011.

Richet, Jean-Loup :"Russia Uses 'Single Register' Law To Selectively Block Internet Content", 22 Mayıs 2013, (çevrimiçi) https://www.infosecurity-magazine.com/blogs/russia-uses-single-register-law-to-selectively-blo/, Erişim: 21 Ağustos 2019.

Sağıroğlu, Şeref :**Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık**, (ed. Şeref Sağıroğlu ve Mustafa Alkan), Ankara, BGD Siber Güvenlik ve Savunma Kitap Serisi, 2018.

Shimko, Keith L. :"Realism, Neorealism and American Liberalism", **The Review of Politics**, C.XLIII, S: 127, ss. 5-19.

Sınar, Hasan :**İnternet ve Ceza Hukuku**, İstanbul, Beta Yayınları, 2001.

Slater, Phil :**Frankfurt Okulu Kökeni ve Önemi**, (Çev. Ahmet Özden), İstanbul, Kabalcı Yayınevi, 1998.

Smith, Steve :**The Globalization of World Politics: An Introduction to International Studies**, New York, Oxford University Press, 2005.

Solomon, Michael G. ve

Chapple, Mike :**Information Security Illuminated**, ABD, Jones and Barlett Publishers, 2005.

Sönmez, Semih :"Google şeffaflık raporunu yayınladı", 20/07/2016, (çevrimiçi) https://www.dunyahalleri.com/google-seffaflik-raporunu-yayinladi/, Erişim: 6 Eylül 2019.

Sönmezoğlu, Faruk :**Uluslararası İlişkiler Sözlüğü**. İstanbul, Der Yayınları, 2000.

Sönmezoğlu, Faruk :**Uluslararası Politika ve Dış Politika Analizi**, İstanbul, Filiz Kitabevi, 1995.

Söyler, Yasin :"Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi", Doktora Tezi, Gazi Üniversitesi Kamu Hukuku Anabilim Dalı, Ankara, 2013.

Stone, Alec :"What Is a Supranational Constitution? An Essay in International Relations Theory", **The Review of Politics**, C. LVI, S: 3, 1994, ss. 441-473.

Tarhan, Nevzat :**Psikolojik Savaş: Gri Propaganda**, 8.bs, İstanbul, Timaş Yayınları, 2006.

Tatar, Ünal :"Sosyal Mühendsilik Saldırıları", **TÜBİTAK Bilgem 4. Ağ ve Bilgi Güvenliği Sempozyumu**, Kasım 2011.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı :**Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**, Ankara, 2012.

Theiler, Tobias :"Societal Security and Social Psychology", **Review of International Studies**, C: XXIX, No: 2, 2003, ss. 249-268.

Toklu, Vefa :**Uluslararası İlişkiler**, Ankara, İmaj Yayıncılık, 2004.

Tumay, Murat :"Denetim ve Özgürlük ikileminde İnternet Erişimi", **SETA Analiz**, S: 133, Temmuz 2015.

Turgut, Reşat :**Küreselleşmenin Askeri Boyutları ve Güvenlik Stratejilerine Etkileri**, Ankara, Genel Kurmay

Askeri Tarih ve Stratejik Etüt Başkanlığı Yayınları, 2003.

Turhan, Oğuz :"Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)", **Planlama Uzmanlığı Tezi**, Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, Nisan 2006.

Türkiye Bankalar Birliği :**Bankacılıkta Dolandırıcılık Eylemleri Tespit ve Önleme Yöntemleri**, Ekim 2015.

Uğrasız, Bülent :"Uluslararası İlişkilerde İki Farklı Yaklaşım: İdealizm ve Realizm", **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, C. V, S. 2, ss. 139-145.

Uzgel, İlhan :**Ulusal Çıkar ve Dış Politika: Türk Dış Politikasının Belirlenmesinde Ulusal Çıkarın Rolü,** Ankara, İmge Yayınları, 2004.

Ünsal, Önder Erol :"HADOPI Yasası Çatırdıyor – Fransa'da İnternet Üzerinden Yasadışı Dosya Paylaşımı ve Dosya İndirme Hakkında Yasal Düzenleme", Temmuz 2013, (çevrimiçi) https://iprgezgini.org/2013/12/17/hadopi-yasasi-catirdiyor-fransada-internet-uzerinden-yasadisi-dosya-paylasimi-ve-dosya-indirme-hakkinda-yasal-duzenleme/, Erişim: 2 Eylül 2019.

Ünver, Mustafa

Canbay, Cafer ve

Mirzaoğlu, Ayşe Gül :"Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler", **BTK Raporu**, Mayıs 2009

Ünver, Yener **:"**Türk Ceza Kanununun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, C. LIX, S: 1-2, 2001, ss. 51-153.

Ünverdi, N. Özlem ve

Yüksel, Zeynep :"Ağ Güvenliği ve Güvenlik Duvarında VPN Uygulaması", (çevrimiçi) http://www.emo.org.tr/ekler/c246594da24758e_ek.pdf, Erişim: 12 Eylül 2019.

Viotti, Paul R. ve

Kauppi, Mark V. :**International Relations Theory: Realism, Pluralism, Globalism**, New York, Macmillan Publishing, 1993.

Waever, Ole :"Securitization and Desecuritization", Ronnie D. Lipschutz (ed.), **On Security**, New York, Columbia University Press, 1995.

Walker, Clive ve

Akdeniz, Yaman : **The Internet, Law and Society**, Ocak 2001.

Waltz, Kenneth N. :**Theory of International Politics**, New York, MacGraw-Hill, 1979.

Waltz, Kenneth N. ve

Quester, George H. :**Uluslararası İlişkiler Kuramı ve Dünya Siyasal Sistemi**, (Çev. Ersin Onulduran), Ankara, SBF Yayınları

Yazıcıoğlu, Yılmaz :**Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle**, İstanbul, Alfa Yayınevi, 1997.

Yazıcıoğlu, Yılmaz :"Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", **Dokuz Eylül Üniversitesi Uluslararası İnternet Sempozyumu**, İzmir, 2002, ss. 451-470.

Yazıcıoğlu, Yılmaz :"Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", **Hukuk ve Adalet: Eleştirel Hukuk Dergisi**, İstanbul, 2004, ss. 172-185.

Yılmaz, Sait :**21. Yüzyılda Güvenlik ve İstihbarat**, (2. Baskı), İstanbul, Milenyum Yayınları, 2007.

Yılmaz, Sait :"Güçsüz Güç", **Güvenlik Stratejileri Dergisi**, No: 5, 2007, ss. 67-104.

Yılmaz, Sait :**Güç ve Politika**, İstanbul, Alfa Basım Yayım, 2008.

Yurdusev, Ahmet Nuri :"Thomas Hobbes and International Relations: From Realism to Rationalism", **Australian Journal Of International Affairs**, C. LX, S: 2, 2006, ss. 305-321.

Zoller, Elisabeth :"Freedom of Expression: Precious Right in Europe, Sacred Right in The United States",

Indiana Law Journal, Vol: 84, I. 3, 2009, ss. 803-808.

İNTERNET KAYNAKLARI

Alpaslan Özerdem, "İnsani Güvenlik", http://wwwm.coventry.ac.uk/researchnet /CPRS/Turkey/conference/Documents/CPRSInsaniGuvenlik.pdf, Erişim 6 Aralık 2019.

Avrupa Birliği Bilişim Politikasi Ve Türkiye'nin Uyumu, https://www.ab.org.tr/ab05/tammetin/89.doc, Erişim: 15 Nisan 2019.

"Avrupa İnsan Hakları Sözleşmesi", s. 11-12, (çevrimiçi) https://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf, Erişim: 12 Eylül 2019.

International Review of Criminal Policy-United Nations Manual on the Prevention and Control of the Computer-Related Crime,< http://www.uncjin.org/Documents/irpc4344.pdf> (12.04.2019)

ITU, "Cybersecurity for All: ITU's Work for a Safer World", 2008, (çevrimiçi) https://www.itu.int/pub/S-GEN-CYBER-2008, Erişim: 15 Ekim 2018.

OpenNet, "Country profiles: United States and Canada overview", 2010, s. 379, (çevrimiçi)https://opennet.net/sites/opennet.net/files/ONI_UnitedStatesandCanada_2010.pdf, Erişim: 1 Eylül 2019.

"Russia, Freedom in the World 2014", (çevrimiçi) http://freedomhouse.org, http://freedomhouse.org/country/russia#.U9udQ2VrOUl, Erişim: 21 Ağustos 2019.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, "2016-2019 Ulusal Siber Güvenlik Stratejisi", s. 8. (çevrimiçi) https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf, Erişim: 19 Ekim 2018.

TÜİK, Girişimlerde Bilişim Teknolojileri Kullanımı Araştırması, Hanelerde Bilişim Teknolojileri Kullanımı Araştırması, (çevrimiçi) http://www.tuik.gov.tr/UstMenu.do?metod=temelist, Erişim: 12 Nisan 2019.

"We Are Social 2019 Dünya İnternet, Sosyal Medya ve Mobil Kullanıcı İstatistikleri", çevrimiçi https://dijilopedi.com/2019-internet-kullanimi-ve-sosyal-medya-istatistikleri/, Erişim: 12 Nisan 2019.

https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/,

http://kararlaryeni.anayasa.gov.tr/Karar/Content/9160bf09-3c94-43ae-b1d3-c84815c1b2ba,

https://www.govinfo.gov/app/details/PLAW-105publ304,

https://www.law.cornell.edu./uscode/text/47/231,

https://www.law.cornell.edu./uscode/text/47/230,

https://www.congress.gov/bill/113th-congress/house-bill/4225,

https://www.congress.gov/bill/115th-congress/senate-bill/1693/text,

http://cis-legislation.com/document.fwx?rgn=26853,

https://398-fz.rkn.gov.ru/docs/398-FZ_eng.pdf,

https://wilmap.law.stanford.edu/entries/federal-law-no-139-fz-blacklist-law,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410,

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'in-arihçesi>,01.06.2019

https://internethalloffame.org/inductees/jcr-licklider >,03.06.2019

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/internet'intarihçesi>,04.06.2019

https://www.armadigital.net/bilgi-bankasi/internetin-tarihcesi >,01.06.2019

http://www.internetarsivi.metu.edu.tr/tarihce.php>,02.06.2019

http://www.unis.unvienna.org/unis/en/pressrels/2000/cp390.html>, 05.07.2019

http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm,08.07.2019

https://fazlamesai.net/posts/yeni-bir-solucan-w32-sasser-b-worm, 06.07.2019.

http://naturalenvironmentsociety-arizonasouthwest.com/references/PDFs/presidential-actions/outline1/Clinton_EO_13010.pdf>,08.07.2019.

https://www.law.cornell.edu/uscode/text/18/1030>,06.07.2019

http://www.turkhukuksitesi.com/makale_154.htm>, 08.07.2019

https://www.haberler.com/rusya-da-4-yilda-siber-suclarin-sayisi-6-kat-artti-9700882-haberi/>,07.07.2019

http://www.hurriyet.com.tr/teknoloji/rusyanin-en-buyuk-siber-suc-grubu-cokertiliyor-40114672>, 07.07.2019

http://www.yttlaw.com/bilisim-suclari-ve-cezalari/>, 01.07.2019

http://www.yttlaw.com/bilisim-suclari-ve-cezalari/,03.07.2019

http://legal.un.org/ola/website/legal_counsel15.aspx>, 09.07.2019

http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.14416&MevzuatIliski=0>,11.07.2019

http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.14416&MevzuatIliski=0>,10.07.2019

https://turkeyblocks.org/about/,05.07.2019

EKLER

EK 1

5156 SAYILI İNTERNET ORTAMINDA YAPILAN YAYINLARIN DÜZENLENMESİ VE BU YAYINLAR YOLUYLA İŞLENEN SUÇLARLA MÜCADELE EDİLMESİ HAKKINDA KANUN

Kanun Numarası	**: 5651**
Kabul Tarihi	**: 4/5/2007**
Yayımlandığı R.Gazete	**: Tarih : 23/5/2007 Sayı : 26530**
Yayımlandığı Düstur	**: Tertip : 5 Cilt : 46**

Amaç ve kapsam

MADDE 1- (1) Bu Kanunun amaç ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usûlleri düzenlemektir.

Tanımlar

MADDE 2- (1) Bu Kanunun uygulamasında;

a) Bakanlık: Ulaştırma Bakanlığını,

b) Başkanlık: Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığını,

c) Başkan: Telekomünikasyon İletişim Başkanını,

ç) Bilgi: Verilerin anlam kazanmış biçimini,

d) Erişim: Bir internet ortamına bağlanarak kullanım olanağı kazanılmasını,

e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,

f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

g) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

ğ) İnternet ortamında yapılan yayın: İnternet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri,

h) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

ı) Kurum: Telekomünikasyon Kurumunu,

i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı,

j) **(Değişik: 26/2/2014-6527/15 md.)** Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,

k) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

l) Yayın: İnternet ortamında yapılan yayını,

m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

n) **(Ek: 6/2/2014-6518/85 md.)** Birlik: Erişim Sağlayıcıları Birliğini,

o) **(Ek: 6/2/2014-6518/85 md.)** Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

ö) **(Ek: 6/2/2014-6518/85 md.)** İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,

p) **(Ek: 6/2/2014-6518/85 md.)** URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,

r) **(Ek: 6/2/2014-6518/85 md.)** Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini,

ifade eder.

Bilgilendirme yükümlülüğü

MADDE 3- (1) İçerik, yer ve erişim sağlayıcıları, yönetmelikle belirlenen esas ve usûller çerçevesinde tanıtıcı bilgilerini kendilerine ait internet ortamında kullanıcıların ulaşabileceği şekilde ve güncel olarak bulundurmakla yükümlüdür.

(2) Yukarıdaki fıkrada belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından iki bin Türk lirasından elli bin Türk lirasına kadar idarî para cezası verilir. [(1)]

(3) **(Ek: 6/2/2014-6518/86 md.)** Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir.

(4) **(Ek: 26/2/2014-6527/16 md.; Değişik: 10/9/2014-6552/126 md.; İptal: Anayasa Mahkemesi'nin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)** [(2)]

İçerik sağlayıcının sorumluluğu

MADDE 4- (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.

(2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.

(3) **(Ek: 6/2/2014-6518/87 md.)** İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır.

Yer sağlayıcının yükümlülükleri

MADDE 5- (1) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

(2) **(Değişik: 6/2/2014-6518/88 md.)** Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.

(3) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

(4) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

---

(1) 10/9/2014 tarihli ve 6552 sayılı Kanunun 126 ncı maddesiyle, bu fıkrada yer alan "ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına" ibaresi "iki bin Türk lirasından elli bin Türk lirasına" şeklinde değiştirilmiştir.

(2) Söz konusu İptal Kararı 1/1/2015 tarihli ve 29223 sayılı Resmi Gazete'de yayımlanmıştır.

(5) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.

(6) **(Ek: 6/2/2014-6518/88 md.)** Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir.

Erişim sağlayıcının yükümlülükleri

MADDE 6- (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu Kanun hükümlerine uygun olarak haberdar edilmesi halinde (…)[1] erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla,

c) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usûllere uygun olarak Kuruma teslim etmekle,

ç) **(Ek: 6/2/2014-6518/89 md.)** Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) **(Ek: 6/2/2014-6518/89 md.)** Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla,

yükümlüdür.

(2) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

(3) Birinci fıkranın (b), (c), (ç) ve (d) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir. [2]

Erişim Sağlayıcıları Birliği

MADDE 6/A- (Ek: 6/2/2014-6518/90 md.)

(1) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuştur.

(2) Birlik özel hukuk tüzel kişiliğini haizdir. Birliğin merkezi Ankara'dır.

(3) Birliğin çalışma usul ve esasları Kurum tarafından onaylanacak Tüzükle belirlenir. Tüzük değişiklikleri de Kurumun onayına tabidir.

(4) Birlik, Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar.

(5) Birlik, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşan ve koordinasyonu sağlayan bir kuruluştur.

---

(1) 6518 sayılı Kanunun 89 uncu maddesiyle bu bentte yer alan "ve teknik olarak engelleme imkânı bulunduğu ölçüde" ibaresi çıkartılmıştır.

(2) 6518 sayılı Kanunun 89 uncu maddesiyle bu bentte yer alan "(b) ve (c)" ibaresi "(b), (c), (ç) ve (d)" şeklinde değiştirilmiştir.

(6) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları erişim sağlayıcılar tarafından yerine getirilir. Kararların uygulanması amacıyla gerekli her türlü donanım ve yazılım erişim sağlayıcıların kendileri tarafından sağlanır.

(7) Bu Kanunun 8 inci maddesi kapsamı dışındaki erişimin engellenmesi kararları gereği için Birliğe gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim sağlayıcılara yapılmış sayılır.

(8) Birlik, kendisine gönderilen mevzuata uygun olmadığını düşündüğü kararlara itiraz edebilir.

(9) Birliğin gelirleri, üyeleri tarafından ödenecek ücretlerden oluşur. Alınacak ücretler, Birliğin giderlerini karşılayacak miktarda belirlenir. Bir üyenin ödeyeceği ücret, üyelerin tamamının net satış tutarı toplamı içindeki o üyenin net satışı oranında belirlenir. Üyelerin ödeme dönemleri, yeni katılan üyelerin ne zamandan itibaren ödemeye başlayacağı ve ödemelere ilişkin diğer hususlar Birlik Tüzüğünde belirlenir. Süresinde ödenmeyen ücretler Birlikçe kanuni faizi ile birlikte tahsil edilir.

(10) Birliğe üye olmayan internet servis sağlayıcıları faaliyette bulunamaz.

Toplu kullanım sağlayıcıların yükümlülükleri

MADDE 7- (1) Ticarî amaçla toplu kullanım sağlayıcılar, mahallî mülkî amirden izin belgesi almakla yükümlüdür. İzne ilişkin bilgiler otuz gün içinde mahallî mülkî amir tarafından Kuruma bildirilir. Bunların denetimi mahallî mülkî amirler tarafından yapılır. İzin belgesinin verilmesine ve denetime ilişkin esas ve usûller, yönetmelikle düzenlenir.

(2) **(Değişik: 6/2/2014-6518/91 md.)** Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

(3) **(Değişik: 6/2/2014-6518/91 md.)** Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.

(4) **(Ek: 6/2/2014-6518/91 md.)** Bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir.

Erişimin engellenmesi kararı ve yerine getirilmesi

MADDE 8- (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228),

suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

(2) Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir. Bu durumda Cumhuriyet savcısı kararını yirmidört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. **(Ek cümle: 6/2/2014-6518/92 md.)** Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

(3) Hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının birer örneği, gereği yapılmak üzere Başkanlığa gönderilir.

(4) İçeriği birinci fıkrada belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği birinci fıkranın (a) bendinin (2) ve (5) ve (6) numaralı alt bentlerinde yazılı suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkanlık tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir.(1)

(5) Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir. (2)

(6) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkanlık tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur.

(7) Soruşturma sonucunda kovuşturmaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmaya yer olmadığı kararının bir örneğini Başkanlığa gönderir.

(8) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir.

(9) Konusu birinci fıkrada sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır.

(10) Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.(3)

(11) İdarî tedbir olarak verilen erişimin engellenmesi kararının yerine getirilmemesi halinde, Başkanlık tarafından erişim sağlayıcısına, onbin Yeni Türk Lirasından yüzbin Yeni Türk Lirasına kadar idarî para cezası verilir. İdarî para cezasının verildiği andan itibaren yirmidört saat içinde kararın yerine getirilmemesi halinde ise Başkanlığın talebi üzerine Kurum tarafından yetkilendirmenin iptaline karar verilebilir.

---

(1) 6518 sayılı Kanunun 92 nci maddesiyle bu fıkrada yer alan "(2) ve (5)" ibaresi "(2), (5) ve (6)" şeklinde değiştirilmiştir.

(2) 10/9/2014 tarihli ve 6552 sayılı Kanunun 127 nci maddesiyle, bu fıkrada yer alan "yirmi dört saat" ibaresi "dört saat" şeklinde değiştirilmiştir.

(3) 6518 sayılı Kanunun 92 nci maddesiyle bu fıkrada yer alan "altı aydan iki yıla kadar hapis cezası" ibaresi "beş yüz günden üç bin güne kadar adli para cezası" şeklinde değiştirilmiştir.

(12) Bu Kanunda tanımlanan kabahatler dolayısıyla Başkanlık veya Kurum tarafından verilen idarî para cezalarına ilişkin kararlara karşı, 6/1/1982 tarihli ve 2577 sayılı İdarî Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulabilir.

(13) **(Ek: 5/11/2008-5809/67 md.)** İşlemlerin yürütülmesi için Başkanlığa gönderilen hakim ve mahkeme kararlarına 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre Başkanlıkça itiraz edilebilir.

(14) **(Ek: 12/7/2013-6495/47 md.)** 14/3/2007 tarihli ve 5602 sayılı Şans Oyunları Hasılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3 üncü maddesinin birinci fıkrasının (ç) bendinde tanımlanan kurum ve kuruluşlar, kendi görev alanına giren suçların internet ortamında işlendiğini tespit etmeleri hâlinde, bu yayınlarla ilgili olarak erişimin engellenmesi kararı alabilirler. Erişimin engellenmesi kararları uygulanmak üzere Telekomünikasyon İletişim Başkanlığına gönderilir.

(15) **(Ek: 26/2/2014-6527/17 md.)** Bu maddeye göre soruşturma aşamasında verilen hâkim kararı ile 9 uncu ve 9/A maddesine göre verilen hâkim kararı birden fazla sulh ceza mahkemesi bulunan yerlerde Hâkimler ve Savcılar Yüksek Kurulu tarafından belirlenen sulh ceza mahkemeleri tarafından verilir.

(16) **(Ek: 10/9/2014-6552/127 md.; İptal: Anayasa Mahkemesi'nin 2/10/2014 tarihli ve E.: 2014/149, K.: 2014/151 sayılı Kararı ile.)** [(1)]

İçeriğin yayından çıkarılması ve erişimin engellenmesi[(2)]

MADDE 9- (Değişik: 6/2/2014-6518/93 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

---

(1) Söz konusu İptal Kararı 1/1/2015 tarihli ve 29223 sayılı Resmi Gazete'de yayımlanmıştır.

(2) Bu maddenin başlığı "İçeriğin yayından çıkarılması ve cevap hakkı" iken 6518 sayılı Kanunun 93 üncü maddesiyle metne işlendiği şekilde değiştirilmiştir.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi

MADDE 9/A- (Ek: 6/2/2014-6518/94 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Başkanlığa doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir.

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkanlık, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir.

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Başkanlığa gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

(6) Hâkim tarafından verilen bu karara karşı Başkanlık tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Başkanlık tarafından yapılır. **(Mülga cümle: 26/2/2014-6527/18 md.)**

(9) **(Ek: 26/2/2014-6527/18 md.)** Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.

İdarî yapı ve görevler

MADDE 10- (1) Kanunla verilen görevler, Kurum bünyesinde bulunan Başkanlıkça yerine getirilir.

(2) Bu Kanunla ekli listedeki kadrolar ihdas edilerek Başkanlığın hizmetlerinde kullanılmak üzere 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununa ekli (II) sayılı listeye eklenmiştir. Başkanlık bünyesindeki iletişim uzmanlarına, Kurumda çalışan Telekomünikasyon Uzmanlarına uygulanan malî, sosyal hak ve yardımlara ilişkin hükümler uygulanır. İletişim Uzmanı olarak Başkanlığa atanan personelin hakları saklı kalmak kaydıyla, kariyer sistemi, Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde çıkarılacak yönetmelikle düzenlenir.

(3) Başkanlığa Kanunla verilen görevlere ilişkin olarak yapılacak her türlü mal veya hizmet alımları, ceza ve ihalelerden yasaklama işleri hariç, 4/1/2002 tarihli ve 4734 sayılı Kamu İhale Kanunu ile 5/1/2002 tarihli ve 4735 sayılı Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(4) Kanunlarla verilen diğer yetki ve görevleri saklı kalmak kaydıyla, Başkanlığın bu Kanun kapsamındaki görev ve yetkileri şunlardır:

a) Bakanlık, kolluk kuvvetleri, ilgili kamu kurum ve kuruluşları ile içerik, yer ve erişim sağlayıcılar ve ilgili sivil toplum kuruluşları arasında koordinasyon oluşturarak internet ortamında yapılan ve bu Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye, internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye yönelik çalışmalar yapmak, bu amaçla, gerektiğinde, her türlü giderleri yönetmelikle belirlenecek esas ve usûller dahilinde Kurumca karşılanacak çalışma kurulları oluşturmak.(1)

b) İnternet ortamında yapılan yayınların içeriklerini izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen gerekli tedbirleri almak.

c) İnternet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirlemek.

ç) Kurum tarafından işletmecilerin yetkilendirilmeleri ile mülkî idare amirlerince ticarî amaçlı toplu kullanım sağlayıcılara verilecek izin belgelerinde filtreleme ve bloke etmede kullanılacak sistemlere ve yapılacak düzenlemelere yönelik esas ve usûlleri belirlemek.

d) İnternet ortamındaki yayınların izlenmesi suretiyle bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dahil, gerekli her türlü teknik altyapıyı kurmak veya kurdurmak, bu altyapıyı işletmek veya işletilmesini sağlamak.

e) İnternet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirlemek.

f) Bilişim ve internet alanındaki uluslararası kurum ve kuruluşlarla işbirliği ve koordinasyonu sağlamak.

---

(1) 6518 sayılı Kanunun 95 inci maddesiyle bu bentte yer alan "yayınları önlemeye" ibaresinden sonra ", internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye" ibaresi eklenmiştir.

g) Bu Kanunun 8 inci maddesinin birinci fıkrasında sayılan suçların, internet ortamında işlenmesini konu alan her türlü temsili görüntü, yazı veya sesleri içeren ürünlerin tanıtımı, ülkeye sokulması, bulundurulması, kiraya verilmesi veya satışının önlenmesini teminen yetkili ve görevli kolluk kuvvetleri ile soruşturma mercilerine, teknik imkânları dahilinde gereken her türlü yardımda bulunmak ve koordinasyonu sağlamak.

(5) **(Değişik: 6/2/2014-6518/95 md.)** Başkanlık; Bakanlık bünyesinde 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.

(6) **(Ek: 6/2/2014-6518/95 md.)** Başkanlık, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar.

(7) **(Ek: 6/2/2014-6518/95 md.)** Başkanlık kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurabilir.

Yönetmelikler

MADDE 11- (1) Bu Kanunun uygulanmasına ilişkin esas ve usûller, Adalet, İçişleri ve Ulaştırma bakanlıklarının görüşleri alınarak Başbakanlık tarafından çıkarılacak yönetmeliklerle düzenlenir. Bu yönetmelikler, Kanunun yürürlüğe girdiği tarihten itibaren dört ay içinde çıkarılır.

(2) Yer veya erişim sağlayıcı olarak faaliyet icra etmek isteyen kişilere, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine ilişkin esas ve usûller, Kurum tarafından çıkarılacak yönetmelikle düzenlenir. Bu yönetmelik, Kanunun yürürlüğe girdiği tarihten itibaren beş ay içinde çıkarılır.[(1)]

İlgili kanunlarda yapılan değişiklikler

MADDE 12- (1) **(4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanunu ile ilgili olup yerine işlenmiştir.)**

(2) **(4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salahiyet Kanunu ile ilgili olup yerine işlenmiştir.)**

(3) **(5/4/1983 tarihli ve 2813 sayılı Telsiz Kanunu ile ilgili olup yerine işlenmiştir.)**

(4) **(1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu ile ilgili olup yerine işlenmiştir.)**

EK MADDE 1 – (Ek: 5/11/2008-5809/67 md.)

(1) Telekomünikasyon İletişim Başkanlığına verilen görevlerin gerektirdiği asli ve sürekli görev ve hizmetler, iletişim başuzmanı, iletişim uzmanı, teknik uzman ve idarî uzman ile iletişim, teknik ve idarî uzman yardımcılarından oluşan meslek personeli ve diğer personel eliyle yürütülür. Başkanlıkta; başkan, daire başkanı, müşavir ve meslek personeli kadrolarında çalışanların; mühendislik alanında elektronik, elektrik-elektronik, elektronik ve haberleşme, endüstri, fizik, matematik, bilgisayar, telekomünikasyon ve işletme mühendisliği fakültelerinden veya bölümlerinden, sosyal bilimler alanında siyasal bilgiler (bilimler), iktisadi ve idarî bilimler,

---

(1) 6/2/2014 tarihli ve 6815 sayılı Kanunun 96 ncı maddesiyle bu fıkrada yer alan "yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine" ibaresi "yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine" şeklinde değiştirilmiştir.

iktisat, hukuk, işletme, iletişim fakülteleri veya bölümlerinden veya bu fakülte ve bölümlere denkliği yetkili makamlarca kabul edilmiş yurt dışındaki yüksek öğretim kurumlarından mezun olmaları ya da belirtilen bölümlerden mezun olmamakla birlikte sayılan fakülte ve bölümlerde yüksek lisans veya doktora yapmış olmaları, uzman unvanlı kadrolarda çalışanların en az dört yıllık fakültelerden mezun, diğer personelin ise en az lise ve dengi okul mezunu olmaları gerekir. Daire başkanı kadrolarına Güvenlik Bilimleri Fakültesinden mezun olanlar da atanabilir. **(Ek cümle: 24/10/2011-KHK-661/80 md.)** Telekomünikasyon İletişim Başkanı müşterek kararname ile atanır. Başkanlık personelinden; daire başkanları Telekomünikasyon İletişim Başkanının teklifi ve Kurul Başkanının uygun görüşü üzerine Kurul, diğer personel Telekomünikasyon İletişim Başkanının önerisi üzerine Kurul Başkanı tarafından atanır.

(2) Uzman yardımcılığına atanabilmek için; yukarıdaki fıkrada sayılan fakülte veya bölümlerden mezun olmak, merkezî yarışma sınavına katılmak, belirlenecek yabancı dillerden en az birini istenen seviyede bilmek, Kurum alan sınavının yapıldığı yılın Ocak ayının ilk gününde otuz yaşını doldurmamış olmak ve bu sınavda başarılı olmak gerekir.

(3) Uzman yardımcılığına atananlar; en az üç yıl çalışmak ve olumlu sicil almak kaydıyla hazırlayacakları tezin kabul edilmesi ve yeterlik sınavında başarılı olması halinde ilgisine göre iletişim uzmanı, teknik uzman veya idari uzman olarak atanırlar. Bunlara bir defaya mahsus olmak üzere bir derece yükseltilmesi uygulanır. Tez savunmasında ve yeterlik sınavında iki defa başarılı olamayanlar uzman yardımcılığı unvanını kaybederler ve mükteseplerine uygun kadrolara atanırlar.

(4) Uzman ve uzman yardımcılarının giriş ve yeterlik sınavları, çalışma usul ve esasları ile ilgili diğer hususlar Kurum tarafından çıkarılacak yönetmelikle düzenlenir.

(5) **(Ek: 6/2/2014-6518/97 md.)** 8/6/1984 tarihli ve 217 sayılı Devlet Personel Başkanlığı Kuruluş ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 2 nci maddesinde sayılan kamu kurum ve kuruluşlarında çalışanlar kurumlarının, hâkim ve savcılar ise kendilerinin muvafakati ile aylık, ödenek, her türlü zam ve tazminatlar ile diğer mali ve sosyal hak ve yardımları kurumlarınca ödenmek kaydıyla geçici olarak Telekomünikasyon İletişim Başkanlığı emrinde görevlendirilebilir. Bu kapsamda görevlendirilen personel sayısı Kurumun kadro sayısının yüzde yirmisini geçemez. Bu personel kurumlarından izinli sayılır. İzinli oldukları sürece memuriyetleri ile ilgili özlük hakları devam eder ve bu süreler terfi ve emekliliklerinde hesaba katılır. Terfileri başkaca bir işleme gerek kalmaksızın süresinde yapılır.

(6) **(Ek: 6/2/2014-6518/97 md.)** Başkanlık personelinin, kanunlar kapsamındaki görevlerini yerine getirirken, görevin niteliğinden doğan veya görevin ifası sırasında işledikleri iddia olunan suçlardan dolayı haklarında cezai soruşturma yapılması, Telekomünikasyon İletişim Başkanı için ilişkili Bakanın, diğer personel için ise Kurum Başkanının iznine bağlıdır.

(7) Bu Kanunla ekli (V) sayılı cetveldeki kadrolar ihdas edilerek Telekomünikasyon İletişim Başkanlığı hizmetlerinde kullanılmak üzere 5651 sayılı Kanuna ekli (I) sayılı listeye eklenmiştir.[1]

---

(1) 6518 sayılı Kanunun 97 nci maddesiyle bu maddenin dördüncü fıkrasından sonra gelmek üzere (5) ve (6) nolu bentler eklenmiş ve bu bentte buna göre teselsül ettirilmiştir.

EK MADDE 2 – (Ek: 6/2/2014-6518/99 md.)

Başkanlığa verilen görevlerin yürütülmesi için, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanunu ile diğer kanunların sözleşmeli personel çalıştırılmasına dair hükümlerine bağlı kalınmaksızın özel bilgi ve ihtisas gerektiren konularda Başkanlıkta sözleşmeli personel çalıştırılabilir. Bu suretle çalıştırılacakların unvanı, sayısı, süresi, ücretleri ve diğer hususlar Bakanlar Kurulunca yürürlüğe konulacak hizmet sözleşmesi esaslarına göre tespit edilir. Bunlara ödenecek ücret, 657 sayılı Kanunun 4 üncü maddesinin (B) bendine göre çalıştırılanlar için uygulanmakta olan sözleşme ücreti tavanının beş katını, çalıştırılabilecek toplam sözleşmeli personel sayısı ise yetmiş beşi geçemez ve bu fıkrada belirtilen ücret dışında herhangi bir ödeme yapılamaz."

GEÇİCİ MADDE 1- (1) Başkanlığın kuruluştaki hizmet binasının yapımı, ceza ve ihalelerden yasaklama işleri hariç, Kamu İhale Kanunu ve Kamu İhale Sözleşmeleri Kanunu hükümlerine tâbi olmaksızın Kurum bütçesinden karşılanır.

(2) Halen faaliyet icra eden ticarî amaçla toplu kullanım sağlayıcılar, bu Kanunun yürürlüğe girdiği tarihten itibaren altı ay içinde 7 nci maddeye göre alınması gereken izin belgesini temin etmekle yükümlüdürler.

(3) Halen yer veya erişim sağlayıcı olarak faaliyet icra eden kişilere, Kurum tarafından, telekomünikasyon yoluyla iletişim konusunda yetkilendirme belgesi olup olmadığına bakılmaksızın, yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla bir yetkilendirme belgesi düzenlenir.

GEÇİCİ MADDE 2 - (Ek: 5/11/2008-5809/67 md.)

(1) Telekomünikasyon İletişim Başkanlığı kadrolarında bulunan personelden ek 1 inci maddede belirtilen öğrenim şartlarını haiz olanlar; kamuda üç yıllık hizmet süresini tamamlamaları, KPDS'den en az 60 veya uluslararası geçerliliği olan sınavlardan muadili puan almaları ve hazırlayacakları tezin kabul edilmesi halinde bu Kanunun yayımı tarihinden itibaren beş yıl içerisinde iletişim uzmanı kadrosuna atanabilirler. Bu personelden; diğer kamu kurum ve kuruluşlarında özel mevzuatları uyarınca yarışma sınavına tabi tutularak mesleğe alınan ve yeterlik sınavını vererek veya tezi başarılı bulunarak kariyer meslek kadrolarına atanmış olanlar yabancı dil şartını karşıladıklarında; yüksek lisans veya doktora öğrenimini tamamlamış
olanlardan, hazırladıkları yüksek lisans veya doktora tezlerinin konularının Kurumun veya Başkanlığın görev alanı ile ilgili olduğunun yapılacak inceleme sonucu belirlenenlerden doktora öğrenimini tamamlamış olanlar doğrudan, yüksek lisans öğrenimini tamamlamış olanlar yabancı dil şartını karşıladıklarında, iletişim uzmanı olarak atanabilirler.

(2) Telekomünikasyon İletişim Başkanlığı personelinden dört yıllık fakülte mezunu olanlar, kamuda üç yıllık hizmet süresini tamamlamaları, çıkarılacak yönetmelikte öngörülen şartları taşımaları ve buna ilave olarak hazırlayacakları tezin kabul edilmesi veya tezli yüksek lisans veya doktora yapmaları halinde, bu Kanunun yayımı tarihinden beş yıl içinde öğrenim alanına göre teknik uzman veya idarî uzman kadrosuna atanabilirler.

GEÇİCİ MADDE 3 - (Ek: 6/2/2014-6518/100 md.)

(1) Birliğin kuruluşu bu Kanunun yayımı tarihinden itibaren üç ay içinde tamamlanır.

(2) Birlik, mevcut internet servis sağlayıcıları ile erişim hizmeti veren işletmecilerin en az dörtte birinin katılımıyla imzalanan Birlik Tüzüğünün Kurum tarafından incelenerek uygun bulunmasını müteakip faaliyete başlar. Birliğin kurulmasını müteakip en geç bir ay içinde hâlen üye olmayan internet servis sağlayıcıları ve erişim hizmeti veren işletmeciler üyeliklerini tamamlamak zorundadır.

(3) Belirtilen sürede Birliğin kuruluşunu tamamlayamaması hâlinde, Kurum tarafından internet servis sağlayıcılarına ve internet erişim hizmeti veren diğer işletmecilere bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

(4) Birliğin kurulmasını müteakip bir ay içinde üye olmayan internet servis sağlayıcılarına veya internet erişim hizmeti veren diğer işletmecilere, Kurum tarafından bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanır.

Yürürlük

MADDE 13- (1) Bu Kanunun;

a) 3 üncü ve 8 inci maddeleri, yayımı tarihinden altı ay sonra,

b) Diğer maddeleri yayımı tarihinde,

yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu Kanun hükümlerini Bakanlar Kurulu yürütür.

EK-2

AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ

Giriş

İmzaları bulunan Avrupa Konseyi Üye Devletleri Diğer Devletler bu konuyla ilgili;

Avrupa Konseyinin amacının üyeleri arasındaki birliğin daha büyük boyutlarda gerçekleştirilmesi amacını gözönüne alarak;

Bu konvensiyondaki diğer devlet taraflarla kooperasyonu teşvik etmenin değerinin farkında olarak;

Uygun yönetmeliğin uyarlanması ve uluslararası kooperasyonun teşvik edilmesi ile, siber suç karşı toplumun korunması amaçlı genel bir suç planının, gözetilmesi ihtiyacının gerektiğinden emin olarak;

Bilgisayar ağlarının sürmekte olan globalizasyonu, birbirlerine yakınlaşması ve dijitalizasyonu ile gelen derin değişikliklerin bilincinde;

Bilgisayar ağlarının ve elektronik bilginin, suç işlemek için kullanılabilme ihtimali ve bu tip suçlara dair kanıtların, saklanılabilirliği ve bu ağlar tarafından iletibilirliği ile ilgili endişeler doğrultusunda,

Siber suçla mücadele ve kullanımdaki meşru menfaalerin ve bilgi teknolojileri gelişiminin korunması gerekliliği ile ilgili özel Devletler ve özel endüstri arasındaki kooperasyonun gerekliliğini tanıyarak,

Siber suçlara karşı, etkili bir mücalenin, arttırılmış, hızlı ve suçsal meselelerde, iyi çalışan uluslararası bir işbirliğini gerektirdiği inancıyla,

Gizliliğe, entegrasyona ve bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin, suç haline getirilmesi vasıtasıyla yanlış kullanımlarına da yöneltilen eylemleri engellemek için, mevcut konvensiyonun gerekliliğinin inancında , bu konvensiyonda tanımlandığı üzere, ve bu tip suçlarla etkin bir şekilde mücadele edilmesi, hem yerel hem uluslararası seviyelerde, için gerekli gücün elde edilmesi,

Hukuki yaptırımların (Yürütme) konuları ile, İnsan Haklarını ve Temel Özgürlüklerini Korunması için 1950 Avrupa Toplantısı Konseyi, Medeni ve Siyasi Haklarla ilgili 1966 Birleşmiş Milletler Uluslararası Akit ve her bireyin, müdahale olmaksızın, bir fikre, ve bunun yanısıra, özel hayatla ilgili haklarının, sınırsız bir şekilde, her çeşit fikir ve bilgiyi araştırma, edinme ve bildirmeye ilişkin özgürlükleri dahil olmak üzere, ifade özgürlüğü hakkına sahip olmasını teyit eden diğer ilgili uluslararası insan hakları sözleşmelerinde korunduğu üzere temel insan haklarına saygı arasında uygun bir dengeyi sağlamanın gerekliliği önemsenerek,

Görüşüldüğü üzere, örneğin, Kişisel Verinin Otomatik İşlenmesi ile ilgili Bireylerin Korunması İçin 1981 Avrupa Konseyi Konvensiyonu gibi, Kişisel Verinin Korunması Hakkını da Aynı Şekilde Önemseyerek,

1989 Çocuk Hakları İle İlgili Birleşmiş Milletler Konvensiyonu ve 1999 Uluslararası İşçi Organizasyonu Çocuk İşçi Konvensiyonunun En Kötü Formlarını Değerlendirerek,

Avrupa Konseyi Üye Devletleri ve diğer devletler arasında bulunan benzer anlaşmaların yanısıra, ceza alanında işbirliği için, mevcut Avrupa Konseyi Konvensiyonlarını da hesaba katarak ve mevcut konvensiyonun, bilgisayar sistemleri ve verilerine ilişkin suçlarla ilgili suçların soruşturulması ve kovuşturmalarının yapılması ve suçların elektronik formdaki kanıtlarının toplanmasına imkan verilebilmesi için, bu konvensiyonlara ilave etme amacını güttüğünü vurgulayarak.

Birleşmiş Milletler, OECD, Avrupa Birliği ve'G8 ler tarafından yapılan eylemler dahil olmak üzere, siber suçların mücadelesinde uluslararası anlayış ve işbirliğini daha ileri taşıyan son gelişmeleri de kucaklayarak.

Telekomünikasyonu önleme için, sorgu mektupları açısından, Kriminal Konularda Karşılıklı Yardım İçin Avrupa Konvensiyonunun pratik uygulamasını ilgilendiren, Bakanlar Komitesi Önerileri No. R (85) 10, Telif Hakları ve Komşu Haklar alanındaki korsanlık üstüne No. R (88) 2, polis sektöründe kişisel verinin kullanımın düzenleyen No. R (87) 15, belli bilgisayar suçlarının tanımlamalarıyla ilgili ulusal yasamalar için, bilgisayarla ilişkili suçun rehberliğinin sağlanması konusunda No. R (89) 9 ve bilgi teknolojilerine bağlı kriminal prosedürle ilgili kanun problemleri ile ilgili No R (95) 13'ün yanısıra, özellikle telefon servisleri ile ilgili, telekomünikasyon servisleri alanında, kişisel verinin korunması ile ilgili No. R (95) 4, hatırda tutarak,

Suç Problemleri İle İlgili Avrupa Komitesi (CDPC) tarafından, yerel kanun yaptırımlarının birbirlerine daha çok yaklaştırılmaya çalışılması ve bu tip soruşturmaların yapılmasıyla etkili şekilde kullanımı ile ilgili gerçekleştirilen siber suça ilişkin işlerin Bakanlar Komitesi tarafından desteklenmesini öneren (10, 11 Haziran 1997) Prag Avrupa Adalet Bakanları 21. Konferansı tarafından benimsenen, Resolution No 1 ve görüşme yapan tarafların en uygun çözümleri bulabilmesi için, konvensiyona en yüksek sayıda devletin, taraf olabilmesine imkan verebilmesi adına çabalarının desteklendiği, 8 – 9 Haziran 2000 Londra Avrupa Adalet Bakanları 23. Konferansında benimsenen, Resolution No 3 ve siber suça karşı mücadelede özel olarak gerekenleri hesaba katan, uluslararası işbirliğinin gerekliliğinin kabul edilmesini de içererek.

Benzer şekilde, devlet başları ve Avrupa Konseyi Hükümetinin 10 - 11 Ekim 1997 Strasbourg tarihli İkinci Zirvesi tarafından benimsendiği üzere eylem planına ilişkin, Avrupa Konseyi değerleri ve standartlarını baz alan yeni bilgi teknolojilerinin gelişmelerine ortak cevap aranması açısından,

Taraflar aşağıdaki şekilde anlaşmışlardır.

Bölüm I – Terimlerin Kullanımı

Madde 1 – Tanımlamalar

Bu konvensiyonun amaçlarına yönelik:

a. "Bilgisayar Sistemi", bir program çerçevesinde , otomatik veri işlemi yapan bir veya birden fazla birbirine bağlı veya ilgili cihaz ve cihaz grupları anlamına gelir;

b. "Bilgisayar verisi", bir bilgisayar sisteminin belli bir fonksiyonu yerine getirmesini sağlayan uygun programları içeren, bir bilgisayar sistemi içinde işlem yapmaya uygun bir formda bilgi veya konsept ve bilgilerin sunumu anlamına gelir.

c. "Servis Sağlayıcı":

   i. Servis kullanıcılarının bir bilgisayar sistemi aracılığıyla, iletişim kurabilmelerini sağlayan herhangi kamu veya özel bir oluşum, ve

   ii. Bu tip bir iletişim servisi veya böyle bir servisin kullanıcıları adına, bilgisayar verisi işleyen veya saklayan herhangi bir oluşum anlamına gelir.

d. "Veri Trafiği", iletişimin, orijinini, gideceği noktayı, tarih, zaman, boyut, süre veya temel servis tipini belirterek, o iletişimin bir zincirini oluşturan bir bilgisayar sistemi aracılığıyla yapılan bir iletişimle ilgili herhangi bir bilgisayar verisi anlamına gelir.

Bölüm II – Ulusal Boyutta Alınacak Önlemler

Kısım 1 – Esas Ceza Hukuku

Başlık 1 – Bilgisayar Veri Ve Sistemlerinin Mevcudiyeti, Bütünlüğü Ve Gizliliğine Karşı Suçlar.

Madde 2 – İllegal Giriş

Taraflardan herbiri, hakkı olmaksızın bir bilgisayar sisteminin bir bütününe veya bir parçasına girilmesi, kasten yapılması durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır. Taraftardan her biri, suçun, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemi ile ilgili veya diğer kötü niyetli veya bilgisayar verisini elde etme amacıyla, güvenlik önlemlerinin ihlal edilmesi yoluyla işlenmiş olduğunu talep edebilir.

Madde 3 - Gayrimeşru Ele Geçirme

Taraflardan herbiri, bu tip bilgisayar verisi taşıyan bilgisayar sistemlerinden, elektromanyetik yayınlar dahil, sistem içindeki, genele açık olmayan bilgisayar verisinin, teknik yollarla, haksız yere ele geçirilmesi, durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır. Taraftardan herbiri, suçun, başka bir bilgisayar sistemine bağlı bir bilgisayar sistemi ile ilgili veya kötü niyetle işlenmiş olduğunu talep edebilir.

Madde 4 – Veri Etkileşimi (Engellenmesi)

1. Taraflardan herbiri, kasten yapıldığında, haksız yere, bilgisayar verisinin yokedilmesi, değiştirilmesi, bozulması, silinmesi, veriye zarar verilmesi, , durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.
2. Taraflar, Paragraf 1 de tanımı yapılan tutumun, çok ciddi zararlarla sonuçlanacağını talep etme hakkını saklı tutabilir.

Madde 5 – Sistem Etkileşimi (Engellenmesi)

Taraflardan her biri, kasten yapıldığında, bilgisayar verisinin yokedilmesi, değiştirilmesi, bozulması, silinmesi, veriye zarar verilmesi, iletilmesi ve giriş yapılması aracılığıyla, bir bilgisayar sisteminin fonksiyonunun, ciddi şekilde engellenmesi durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

Madde 6 – Donanımların Suistimali

1. Taraflardan her biri, kasten ve haksız yere,

i Madde 2'den Madde 5'e kadar kabul edilmiş suçlardan herhangi birinin işlenmesi amaçlı uyarlanmış veya dizayn edilmiş bir bilgisayar programı dahil olmak üzere, bir donanımın,

ii Madde 2'den Madde 5'e kadar kabul edilmiş suçlardan herhangi birinin işlenmesi amaçlı, tümü veya bir bilgisayar sisteminin herhangi bir bölümüne giriş yapabilen, bir bilgisayar şifresi, giriş kodu veya benzer verinin,

a. Üretilmesi, satışı, kullanım için tedariği, ithali, dağıtılması veya elde edilebilir hale getirilmesi ve

b. Madde 2'den Madde 5'e kadar kabul edilmiş suçlardan herhangi birinin işlenmesi amaçlı, yukardaki a.i veya ii paragraflarında belirtilen bir öğenin mülkiyeti. Taraflardan biri, kanunen, önceden edinilmiş bu tip öğelerin mülkiyetinin, cezai sorumluluk gerektirdiğini talep edebilir.

Durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

2. Bu madde, bir bilgisayar sisteminin korunması veya yetkili şekilde test edilmesi gibi, bu maddenin 1. Paragrafında bahsedilenlerin mülkiyeti, edinilmesi, dağıtılması, ithal edilmesi, satışı, kullanım için tedariği ve üretimi, konvensiyonun 2. İla 5. Maddeleri boyunca belirtilen suçların işlenmesi amaçlı olmadığı durumlarda, cezai yükümlülüğü beraberinde getirmesi şeklinde algılanmayacaktır.

3. Tarafların her biri, bu maddenin 2. Paragrafını uygulamama hakkını, saklı tutma, bu maddenin 1. Paragrafı a.ii de belirtilen öğelerin tedarik edilmesi, dağıtılması, ve satışını ilgilendirmemesi kaydıyla, saklı tutabilir.

Başlık 2 – Bilgisayarla İlişkili Suçlar

Madde 7 – Bilgisayarla İlişkili Sahtekarlık

Taraflardan her biri, kasten ve haksız yere yapıldığında, verinin direkt olarak okunabilir, anlaşılabilir olup olmadığına bakmaksızın, yasal amaçlara uygun şekilde hazırlanmış veya kabul edilebilmesi amacıyla yapılan gerçek dışı sonuçlar oluşturarak, bilgisayar verisinin yokedilmesi, değiştirilmesi, bozulması, silinmesi, veriye zarar verilmesi, iletilmesi ve giriş yapılması aracılığıyla, bir bilgisayar sisteminin fonksiyonunun, ciddi şekilde engellenmesi durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır. Taraflardan biri, dolandırıcılık veya benzer bir kastın, cezai sorumluluk gerektirdiğini talep edebilir.

Madde 8 – Bilgisayarla İlgili Dolandırıcılık

Taraflardan herbiri, kasten ve haksız yere,

a. bilgisayar verisinin yok edilmesi, silinmesi, değiştirilmesi, veriye giriş yapılması
b. kendi veya başka bir kişinin maddi çıkarı için, haksız yere, dürüst olmayan bir niyet taşıyarak, bir bilgisayar sisteminin fonksiyonunun engellenmesi durdurulması

vasıtasıyla başka bir kişinin mülkiyet kaybına sebebiyet verilmesi durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

Başlık 3 – İçerikle İlgili Suçlar

Madde 9 – Çocuk Pornografisi ile İlgili Suçlar

1. Taraflardan herbiri, aşağıdaki tutumların, kasten ve haksız yere yapılması durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır:

a. Başka bir bilgisayar sistemi ile dağıtılılması amaçlı, çocuk pornografisi üretimi.
b. Bir bilgisar sistemi vasıtasıyla çocuk pornografisinin elde edilmesinin sağlanması.
c. Bir bilgisayar sistemi ile çocuk pornosunun dağıtımı, iletilmesi veya aktarılması.
d. Kendi veya başka bir kişi için, bir bilgisayar sistemi ile çocuk pornosunun temin edilmesi
e. Bir bilgisayar veri depolama ortamında veya bir bilgisayar sisteminde çocuk pornografisinin mülkiyeti.

2. Yukardaki 1. Paragrafın amacına yönelik olarak, "çocuk pornografisi" terimi,

a. Cinsel Davranışta Bulunan Reşit Olmayan Bir Kişi

b. Cinsel Davranışta Bulunan Reşit Olmayan Bir Kişi Gibi Gözüken Kişi

c. Cinsel Davranışta Bulunan reşit Olmayan Bir Kişiyi Tasvir eden gerçekçi resimler.

3. Yukarıdaki 2. Paragrafın amacına yönelik olarak, "küçük" terimi, 18 yaşın altındaki tüm kişileri içerir. Taraflardan biri, 16'dan daha az olmayacak şekilde, daha düşük bir yaş limitini talep edebilir.

4. Herbir taraf, bir bütün veya parçalı olarak, 1. Paragrafı, alt paragrafları d ve e'yi ve alt paragraflardan b ve c.'yi uygulamama hakkını saklı tutabilir.

Başlık 4 – Telif Hakları ve Benzer Hakların İhlali İle İlgili Suçlar

Madde 10 – Telif Hakları ve Benzer Hakların İhlali İle İlgili Suçlar

1. Taraflardan herbiri, ticari bir ölçekte ve bir bilgisayar sistemi vasıtasıyla, bu tip eylemlerin kasten işlendiği, herhangi ahlaki hakların konvensiyonlar tarafından hariç tutulduğu üzere, WIPO Telif Hakları Antlaşması, Fikri Hakların Ticari Yönleri Anlaşması, Fikir ve Sanat Eserlerinin Korunması için Bern Konvensiyonunu revize eden 24 Temmuz 1971 Paris Kanunuyla garanti altına alınmış yükümlülüklere uygun olarak, taraflardan birinin kanunlarında belirtildiği üzere, telif hakları ihlalleri durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

2. Taraflardan herbiri, ticari bir ölçekte ve bir bilgisayar sistemi vasıtasıyla, bu tip eylemlerin kasten işlendiği, herhangi ahlaki hakların konvensiyonlar tarafından hariç tutulduğu üzere, İcracılar, Fonogram Üreticileri ve Yayın Kuruluşlarını Koruma Uluslararası Konvensiyonu (Roma Konvensiyonu) , Fikri Hakların Ticari Yönleri Anlaşması ve WIPO Performans ve Fonogram Antlaşmasıyla garanti altına alınmış yükümlülüklere uygun olarak, taraflardan birinin kanunlarında belirtildiği üzere, ilgili hakların ihlalleri durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

3. Taraflar, sınırlı durumlarda, diğer kanuni yolların mevcudiyetinin bulunması ve saklı tutma durumunun, bu maddenin 1. ve 2. Paragrafında belirtilen uluslararası belgelerde ortaya konmuş yükümlülüklerini ihlal etmemesi şartıyla, bu maddenin 1. ve 2. Paragrafındaki cezai sorumluluğu empoze etmeme hakkını saklı tutabilir.

Başlık 5 – Yardımcı Sorumluluklar ve Yaptırımlar

Madde 11 – Teşebbüs ve Yardım Etme veya Yataklık (İştirak Etme)

1. Taraflardan herbiri, kasten yapıldığında, bu tip bir suçun işlenmesi niyetiyle mevcut konvensiyonun 2. İla 10. Maddeleri boyunca belirtilmiş herhangi bir suçlara yardım, yataklık veya iştirak edilmesi durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

2. Taraflardan herbiri, kasten yapıldığında, bu konvensiyonun 3. ila 5, 7, 8 ve 9.1.a ve c. maddeleri boyunca belirtilmiş suçlardan herhangi birini işlemeye teşebbüs etmesi durumunda, iç hukuku uyarınca, bunun suç olarak kabul edilmesi için gerekli yasal ve diğer önlemleri alacaktır.

3. Taraflar, bir bütün veya parçalı olarak, bu maddenin 2. Paragrafını uygulamama hakkını saklı tutabilirler.

<u>Madde 12 – Tüzel Yükümlülük</u>

1. Taraflardan herbiri,

a. Tüzel Kişiliğin temsilci gücü
b. Tüzel Kişilik adına kararlar alan bir yetkili
c. Bir Tüzel Kişilikte kontrol uygulayan bir yetkiliye

dayalı olarak, ileri gelen bir pozisyonu olan, tüzel kişinin bir organının bölümü veya bireysel olarak hareket etmesiyle herhangi bir gerçek kişinin menfaatine göre yapılmış, bu konvensiyonda belirtilen suçlarla ilgili, tüzel kişilerin sorumlu tutulmasının teminat altına alınması için, gerekli yasal ve diğer önlemleri alacaktır.

2. Bu maddenin 1. Paragrafında sunulmuş durumlara ek olarak, taraflardan herbiri, Paragraf 1'de bahsi geçen gerçek kişinin denetim ve kontrol eksikliği yüzünden, yetkisi dahilinde gerçek kişi tarafından, tüzel kişilik yararına, bu konvensiyonda belirtilmiş suçların oluşması durumlarında, tüzel kişilerin sorumlu tutulmasının teminat altına alınması için, gerekli önlemleri alacaktır.

3. Tarafların hukuki prensiplerine bağlı olarak, tüzel kişiliğin yükümlülüğü, cezai, hukuki veya idare olabilir.

4. Bu tip bir yükümlülük, suçu işleyen gerçek kişilerin cezai yükümlüklerine bağlı olmayacaktır.

Madde 13 – Yaptırımlar ve Önlemler

1. Taraflardan herbiri, Madde 2 ila Madde 11 arasında belirtilmiş suçların, etkili, orantılı ve caydırıcı yaptırımlarla (özgürlüğün kısıtlanması dahil) cezalandırılmasının teminat altına alınması için gerekli yasal ve diğer önlemleri alacaktır.

2. Taraflardan herbiri, Madde 12 ile ilgili olarak sorumlu tutulan tüm tüzel kişilerin, etkili, orantılı ve caydırıcı cezai veya cezai-olmayan yaptırımlara tabi tutulmalarının teminat altına alınması için gerekli yasak ve diğer önlemleri alacaktır.

Kısım 2 – Usul Hukuku

Başlık 1 – Ortak Hükümler

Madde 14 – Usul Hükümleri Kapsamı

1. Taraflardan herbiri, gerekli soruşturma ve kanuni takibatlar için bu bölümde sağlanmış yetki belgesi ve prosedürleri saptamak için gerekli yasak ve diğer önlemleri alacaktır.

2. Madde 21'de özellikle belirtilmiş olması dışında, taraflardan her biri,

a. Bu konvensiyonun 2. Maddesinden 11. Maddesi boyunca belirtilen suçlarla
b. Bir bilgisayar sistemi aracılığı ile gerçekleştirilen diğer suçlarla
c. Bir suçun elektronik şekilde bir kanıtının toplanmasıyla

İlgili olarak bu maddenin 1. Paragrafında yer alan tüm yetki ve prosedürleri uygulayacaktır.

3.

a. Taraflardan herbiri, Madde 20'de belirtilen önlemleri uygulama hakkını, sadece saklı tuttuğunda belirttiği suçlara veya suç kategorilerine göre, bu tip suç veya kategorilerin alanı, Madde 21'de belirtilen önlemlere uygulanan suçların alanından daha kısıtlı olmaması şartıyla, saklı tutabilir. Tarafların her biri, Madde 20'de belirtilen önlemin en geniş uygulamasına imkan veren bir saklı tutma kısıtlamasını gözönünde tutacaktır.

b. Taraflardan biri, mevcut Konvensiyonun edinilmesi süresinde, yürürlükteki yaptırımlarındaki kısıtlamalardan ötürü, Madde 20 ve 21 de belirtilen önlemleri,

i. Sistemin kapalı bir kullanıcılar grubu adına çalıştığı
ii. Kamu iletişim ağlarını kullanmadığı ve ister kamu olsun ister özel başka bir bilgisayar ağına bağlı olmadığı

Bir servis sağlayıcının bilgisayar sistemi içinde iletilmekte olan iletişimlerle ilgili uygulayamıyor ise, sözkonusu taraf, bu tip iletişimlere karşı önlemleri uygulamama hakkını saklı tutar. Tarafların her biri, Madde 20 ve 21'de belirtilen önlemin en geniş uygulamasına imkan veren bir saklı tutma kısıtlamasını gözönünde tutacaktır.

Madde 15 - Koşullar ve Tedbirler

1. Taraflardan her biri bu bölümde sağlanan tüm yetki ve prosedürlerin uygulanması, işletilmesi, yürütülmesini, 1950 Avrupa Konseyi İnsan Hakları ve Temel Özgürlükleri Konvensiyonu, 1966 Birleşmiş Milletler Sivil ve Siyasi Haklar Uluslararası Anlaşması ve diğer uygulanabilen Uluslararası İnsan Hakları Kanunları ve ölçülülük ilkesini de içine almış yükümlülüklere uygun olmasından kaynaklanan haklar dahil olmak üzere, insan hakları ve özgürlüklerinin yeterli bir şekilde korunmasına imkan veren, kendi iç hukukuna göre, sağlanmış koşullar ve tedbirlere bağlı olmasını teminat altına alacaktır.
2. Bu tip koşullar ve tedbirler, ilgili prosedür veya yetki mahiyeti görüşüne uygun olarak, diğerlerine ilaveten, yargısal veya diğer bağımsız denetim, uygulama gerekçelerini, kapsamın sınırlandırılması ve bu yetki veya prosedürün süresini içine alacaktır.
3. Kamu yararına uygun olduğu ölçüde, özellikle adaletin doğru yönetimi durumunda, taraflardan her biri, üçüncü partilerin hakları, sorumlulukları ve yasal çıkarları ile ilgili bu bölümdeki yetki ve prosedürlerin etkisini consider gözönünde tutacaktır.

Başlık 2 – Depolanmış Bilgisayar Verisinin Hızlı Şekilde Korunması

Madde 16 – Depolanmış Bilgisayar Verisinin Hızlı Şekilde Korunması

1. Taraflardan her biri, yetkililerinden isteyebileceğine, özellikle, bilgisayar verisinin kaybına veya değiştirilmesine açık olduğuna dair gerekçeler bulunduğunda, bir bilgisayar sistemi aracılığıyla depolanan, trafik verisi dahil, özel bilgisayar verilerinin hızlı şekilde korunmasının sağlanmasını, yetkililerinden talep edebilmesine imkan veren kanun ve diğer önlemleri benimseyecektir.

2. Taraflardan biri, yukarıda 1. paragraftakileri, bir kişiden, özellikle o kişinin kontrolündeki depolanmış bilgisayar verisinin korunmasını talep ederek yürürlüğe koyduğunda, yetkililerin açıklarını bulmasına imkan verebileceği, en fazla 90 gün olmak üzere, bilgisayar veri bütünlüğünün gerektiği sürece korunmasıyla ilgili o kişiyi yükümlü kılmasını gerektiren kanun ve diğer önlemleri benimseyecektir. Taraflar, böyle bir talebin daha sonra yenilenmesini şart koşabilirler.

3. Taraflardan her biri, iç hukukuna göre şartları belirlenmiş, bu tip prosetürlerin taahhüdünün gizli tutulması ile ilgili bilgisayar verisini koruması gereken, sorumlu kişi ve herhangi kişiyi yükümlü kılabilmesi için gerekli kanun ve diğer önlemleri benimseyecektir.

4. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

Madde 17 – Hızlı Koruma ve Trafik Verisinin Kısmi Açıklanması

1. Taraflardan herbiri, Madde 16'daki korunması gereken trafik verisi açısından,

a. İletişimde bir veya birden fazla servis sağlayıcının olup olmadığına bakmaksızın, bu tip trafik verilerinin acilen korunmasının olup olmadığının temin edilmesi,
b. İletişimin aktığı yol ve servis sağlayıcıların, ilgili taraf tarafından belirlenebilmesi için, yeterli bir trafik verisinin, ilgili tarafın yetkili kişisine, ya da o yetkili kişi tarafından atanmış olan kişiye hızlı bir şekilde bildirilmesinin temin edilmesi,

için gerekli kanun ve diğer önlemleri benimseyecektir.

2. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

Başlık 3 – Üretim Siparişi

Madde 18 – Üretim Siparişi

1. Taraflardan her biri, yetkili otoritelerinin,

a. Bir bilgisayar sistemi veya bir bilgisayar veri depolama ortamında tutulan, kişinin bilgisi ve kontrolündeki belirlenmiş bilgisayar verisinin sunulması için o kişiye,

b. Servis sağlayıcının bilgisinde ve kontrolünde bulunan servislerle ilgili, ilgili tarafa abone bilgisini sunabilmek için, ilgili tarafın alanı içinde, servis veren bir servis sağlayıcıya,

Talepte bulunabilmesine yetki verilmesi için gerekli kanunları ve diğer önlemleri benimseyecektir.

2. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

3. Bu maddenin amacına yönelik olarak, "Abone Bilgisi" terimi,

a. Kullanılan iletişim servis tipi, teknik hükümler ve servisin süresinin

b. Servis anlaşması çerçevesinde, abonenin kimliği, posta veya coğrafi adresi, telefonu veya diğer ulaşılabilecek numarası, fatura ve ödeme bilgisinin

c. Servis anlaşması çerçevesinde, iletişim ekipmanının kurulduğu yerle ilgili diğer bilgilerin

Tahsis edildiği, trafik veya içerik verisinden ziyade, servislerle ilgili abonelere ilişkin, bilgisayar verisi veya başka bir şekilde bulunan bilgi anlamına gelmektedir.

Başlık 4 – Depolanan Bilgisayar Verisinin Araştırılması ve Yakalanması

1.Taraflardan her biri, yetkili otoritelerine, o alan içinde,

a. Bir bilgisayar sistemi veya bir bölümü ve içinde saklanan bilgisayar verisine/verisinin; ve

b. Bilgisayar verisinin saklanabildiği bir bilgisayar veri depolama ortamına/ortamının

aranmasına ve erişilmesine yetki verebilmesi için gerekli yetki ve diğer önlemleri benimseyecektir.

2. Taraflardan herbiri, yetkilileri, paragraf 1.a'ya göre, bir bilgisayar sistemi veya bir bölümünü araştırdığı veya o sisteme veya bölümü erişim sağladığı, aradığı verinin bir başka bir bilgisayar sisteminde veya o alanın başka bir bölümünde ve bu tip bir verinin yasal olarak, ana sistemden erişilebilir olduğu ile ilgili bir düşüncesi olduğu durumlarda, yetkililerin, diğer bir sisteme, hızlı bir şekilde benzer erişimi veya o sistemi araştırmasına imkan verecek yetki ve diğer önlemleri benimseyecektir.

3. Taraflardan her biri, yetkililerinin, paragraf 1 veya 2'ye göre erişilen bilgisayar verilerini elde etmek veya güvenlik altına alabilmesi için, o kişileri yetkilendirmeleri ile ilgili gerekli yetki ve diğer önlemleri benimseyecektir. Bu önlemlerin içinde;

a. Bir bilgisayar sisteminin veya bir bölümünün veya bir bilgisayar veri depolama ortamının elde edilmesi veya benzer şekilde güvenlik altına alınması

b. Bu bilgisayar verisinin bir kopyasının alınması tutulması.

c. İlgili depolanmış bilgisayar verisinin bütünlüğünün sağlanması.

d. Erişilen bilgisayar sistemindeki bu bilgisayar verisinin silinmesi veya erişilmez hale getirilmesi

yeralır.

4. Taraflardan herbiri, yetkili otoritelerinin, bilgisayar sisteminin çalışmasıyla, paragraf 1 ve 2'de bahsi geçen önlemlerin alınmasına imkan vermek için şart koşulmuş bilgisayar verilerini korumak için uygulanan önlemlerle ilgili bilgisi olan herhangi birine, talepte bulunması ile ilgili yetkilendirmeyi gerektiren, yetki ve diğer önlemleri benimseyecektir.

5. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

Başlık 5 – Bilgisayar Verisinin Gerçek Zamanlı Toplanması

Madde 20 – Trafik Verisinin Gerçek Zamanlı Toplanması

1. Taraflardan herbiri, yetkili otoritelerinin;

a. Sözkonusu tarafın alanında, teknik araçların uygulanmasıyla toplaması ve kayıt yapabilmesi, ve

b. Mevcut teknik kapasitesi içinde, bir servis sağlayıcıyı

i. Sözkonusu tarafın alanında, teknik araçların uygulanmasıyla toplama ve kayıt yapabilme; veya

ii. Bir bilgisayar sistemi vasıtasıyla kendi alanından geçirilen belirlenmiş bir iletişimle ilgili, gerçek zamanlı trafik verisinin kaydı, ve toplanması işleminde, yetkili otoriteleriyle işbirliği yapması, yardım etmesini

mecbur kılabilmesini gerektiren, yetki ve diğer önlemleri benimseyecektir.

2. Taraflardan biri, kendi iç yasal sisteminin prensipleri yüzünden, paragraf 1.a da belirtilen önlemleri benimseyemezse, onun yerine, o alan içinde teknik araçların uygulanmasıyla, o alan içinden geçen belirli iletişimle ilgili trafik verisinin tam zamanlı toplanması ve kayıt edilmesini temin etmek için gerekli yetki ve diğer önlemleri benimseyebilir.

3. Taraflardan her biri, bu maddede şart koşulmuş herhangi bir yetkinin işletilmesi veya bunla ilgili bir bilginin gizli tutulması için bir servis sağlayıcıyı yükümlü kılması için gereken yetki ve diğer önlemleri benimseyecektir.

4. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

Madde 21 – İçerik Verisinin Ele Geçirilmesi

1. Taraflardan herbiri, kendi iç kanunları tarafından belirlenecek bir dizi ciddi suçla ilgili, yetkili otoritelerinin;

a. Sözkonusu tarafın alanında, teknik araçların uygulanmasıyla toplaması ve kayıt yapabilmesi, ve

b. Mevcut teknik kapasitesi içinde, bir servis sağlayıcıyı

i. Sözkonusu tarafın alanında, teknik araçların uygulanmasıyla toplama ve kayıt yapabilme; veya

ii. Bir bilgisayar sistemi vasıtasıyla kendi alanından geçirilen belirlenmiş bir iletişimle ilgili, gerçek zamanlı içerik verisinin kaydı, ve toplanması işleminde, yetkili otoriteleriyle işbirliği yapması, yardım etmesini

mecbur kılabilmesini gerektiren, yetki ve diğer önlemleri benimseyecektir

2. Taraflardan biri, kendi iç yasal sisteminin prensipleri yüzünden, paragraf 1.a da belirtilen önlemleri benimseyemezse, onun yerine, o alan içinde teknik araçların uygulanmasıyla, o alan içinden geçen belirli iletişimle içerik verisinin tam zamanlı toplanması ve kayıt edilmesini temin etmek için gerekli yetki ve diğer önlemleri benimseyebilir.

3. Taraflardan her biri, bu maddede şart koşulmuş herhangi bir yetkinin işletilmesi veya bunla ilgili bir bilginin gizli tutulması için bir servis sağlayıcıyı yükümlü kılması için gereken yetki ve diğer önlemleri benimseyecektir.

4. Bu maddede bahsi geçen yetki ve prosedürler, Madde 14 ve Madde 15'e tabidir.

Bölüm 3 – Yargı Yetkisi

Madde 22 – Yargı Yetkisi

1. Taraflardan herbiri, bu konvensiyonda Madde 2'den Madde 11'e kadar uygun olmak üzere saptanmış her suç üstünde; suç;

a. Kendi alanında; veya

b. İlgili tarafın bayrağını taşıyan bir gemide; veya

c. İlgili tarafın kanunları çerçevesinde kayıtlı bir uçakta;

d. O ülkenin vatandaşlarından biri tarafından, İşlendiği yerdeki Yasal kanuna göre, suçun cezalandırılabilir olması durumunda veya suçun herhangi bir tevletin yargı yetkisi alanı dışında işlenmesi durumunda

işlendiği zaman, yargı yetkisini gerektiren yetki ve diğer önlemleri benimseyecektir.

2. Taraflardan her biri, bu maddenin 1.b'sinden 1.d'ye kadar veya bir bölümünde konulmuş yargı yetkisi kuralları şartları veya sadece belirli vakaları uygulama veya uygulamama hakkını elinde tutabilir.

3. Taraflardan her biri, iddia edilen suçlunun, kendi alanı içerisinde olduğu, geri iadesi talebinden sonra, sadece milliyeti açısından, başka bir tarafa geri iadesi olmadığı durumlarda, bu konvensiyonun Madde 24, paragraf 1 de belirtilen suçlarla ilgili yargı yetkisini kullanabilmesi için gerekli yetki ve diğer önlemleri benimseyecektir.

4. Bu konvensiyon, bir tarafın, kendi iç kanunları ile icra edilen herhangi bir suç yargılama yetkisini hariç tutmaz.

5. Birden fazla tarafın, bu konvensiyona göre iddia edilen bir suç üstünde, yargı yetkisi talebi olduğu durumlarda, konuyla ilgili taraflar, adli takibat ile ilgili en uygun yargı yetkisinin belirlenmesini istişare edeceklerdir.

Bölüm III – Uluslararası İşbirliği

Kısım 1 – Genel Prensipler

Başlık 1 – Uluslararası İşbirliğine ilişkin Genel Prensipler

Madde 23 – Uluslararası İşbirliğine ilişkin Genel Prensipler

Taraflar, bu bölümün hükümlerine uygun olarak, bilgisayar sistemleri ve verileri, veya suçun elektronik ortamda kanıtının toplanması ile ilgili suçları ilgilendiren prosedürler, mümkün olabilen en geniş soruşturmalarla, karşılıklı yapılan düzenlemeler ve suç vakalarında başvurulacak gerekli uluslararası belgelerin uygulanması için birbirleriyle işbirliği yapacaklardır.

Başlık 2 – Suçluların İadesine İlişkin Prensipler

Madde 24 – Suçluların İadesi

1.
   a. Bu madde, taraflar arasında, bu konvensiyonun Madde 2'den 11'e kadar olan bölümünde gerçekleşen suçlarla ilgili, her iki ilgili tarafın kanunları dahilinde, özgürlüklerinin en az bir yıllık olmak üzere, en uzun süre boyunca veya daha şiddetli cezaların uygulanması kaydıyla, suçluların iadesini uygular.

   b. İki veya daha fazla taraf arasında uygulanabilen, Avrupa Konvensiyonu Suçluların İadesi (ETS No.24) dahil olmak üzere, karşılıklı yapılan düzenleme veya suç iadesi anlaşması üstünde, farklı minimum ceza uygulanması gerektiğinde, anlaşmanın veya düzenlemenin gerektirdiği minimum ceza uygulanacaktır.

2. Bir anlaşmaya göre şartlı olarak suçluların iadesini yapan taraflardan biri, suçluların iadesi ile ilgili bir anlaşması olmayan başka bir taraftan, suçluların iadesi ile ilgili bir talep alırsa, sözkonusu taraf, bu maddenin 1. Paragrafında belirtilen herhangi bir suçla ilgili, bu konvensiyonu, suçluların iadesi ile ilgili yasal bir temel olarak kabul edebilir.

3. Bir anlaşmanın varlığına istinaden şartlı suçlu iadesi yapmayan taraflar, bu maddenin 1. Paragrafında bahsedilen suçları, kendi aralarında suçluları iade edilebilir olarak kabul edeceklerdir.
4. Suçluların iadesi, ilgili talep edilen tarafın kanunlarına konmuş şartlara veya talep edilen tarafın suçlu iadesini reddetmesi durumuyla ilgili gerekçeleri dahil, uygulanabilir suçluların iadesi anlaşmalarına tabidir.

5. Bu maddenin 1. Paragrafında belirtilen bir suç için, suçluların iadesi, aranan kişinin milliyeti temel alınarak münhasıran reddedilir ise veya talep edilen taraf, suç üstünde yargı yetkisi olduğunu varsayarsa, talep edilen taraf, talep eden tarafın isteği üzerine, yetkili kişilere, kovuşturma amaçlı, davayı ibraz edecek ve talep eden tarafa en son neticeyi zamanı gelince raporlayacaktır. Bu yetkililer, kararlarını alacaklar ve kendi araştırmalarını ve prosedürlerini sözkonusu tarafın kanunlarına göre, karşılaştırılabilir yapıda herhangi bir diğer suç olarak aynı tutum içinde yapacaklardır.

6.
   a. Taraflardan herbiri, imzaların atıldığı noktada veya mütalaa, kabul, onay veya katılma belgesini sunduğunda, Avrupa Konseyi Genel Sekreteri ile iletişime geçecek, suçluların iadesi taleplerini yapma, alma veya anlaşmanın yokluğunda geçici tutuklamadan sorumlu her yetkili kişilerin isimlerini ve adreslerini tanımlayacaklardır.

   b. Avrupa Konseyi Genel Sektereteri, taraflar tarafından belirlenen bu yetkililerin bir kaydını tutacak ve güncelleyecektir. Tarafların herbiri, her zaman için, kayıtlardaki detayların doğru olduğundan emin olacaklardır.

Başlık 3 – Müşterek Yardıma İlişkin Genel Prensipler

Madde 25 – Müşterek Yardıma İlişkin Genel Prensipler

1. Bilgisayar sistemleri ve verileri veya suçların elektronik şekliyle kanıtlarının toplanması ile ilgili araştırmalar ve prosedürler için mümkün olan en geniş karşılıklı yardımlaşmayı yapacaklardır.

2. Taraflardan her biri, Madde 27'den 35'e kadar olan bölümde düzenlenmiş yükümlülükleri yerine getirmek için gerekli tüm yetki ve önlemleri benimseyeceklerdir.

3. Taraflardan her biri, acil durumlarda, talep eden taraf tarafından istendiğinde, takip eden resmi konfirmasyonlarla birlikte, gerektiğinde şifrelemele, güvenlik ve yetkilendirmenin uygun seviyelerini kullanarak, faks ve e mail dahil, hızlandırılmış iletişimler vasıtasıyla, karşılıklı yardımlaşma iletişim ricalarında bulunabilirler.

4. Bu bölümdeki maddelerde özel olarak tersi söylenmediği müddetçe, karşılıklı yardım, talep eden tarafın kanunlarına göre sağlanmış şartlara veya talep edilen tarafın işbirliğini reddedebileceği gerekçeler dahil olmak üzere, uygulanabilir karşılıklı yardım anlaşmalarına tabi olacaktır. Talep edilen taraf, Madde 2'den Madde 11'e kadar belirtilmiş suçlarla ilgili olarak karşılıklı yardımı, suçla ilgili talep, suçun bir finansal suçu ilgilendirdiği gerekçesi ile reddetmeyi işleme almayacaktır.

5. Bu bölümün hükümlerine göre, talep edilen tarafın, çift suçluluk durumuna bağlı olarak, karşılıklı yardım vermesine izin verilir. Kanunun, suçu, suçun aynı kategoriye koymasına veya talep eden taraf olarak aynı terminoloji tarafından suçun adlandırılmasına bakmaksızın, yardımın istendiği suçun altını çizen tutum, kanunlar çerçeverinde suç olarak kabul edilir.

Madde 26 – Spontan Bilgi (Kendi Kendine Gelişen Bilgi)

1. Taraflardan biri, kendi kanunlarının sınırları ve istek olmaksızın, diğer tarafa, bu konvensiyonda belirtilen suçları ilgilendiren soruşturma ve prosedürleri yapması ile ilgili, veya bu bölüm altında, o taraftan gelebilecek bir işbirliği talebi meydana gelme ihtimali olduğunda, ilgili tarafa yardımcı olabilecek, bilgilerin açığa konması ile ilgili, kendi soruşturma çatısı altında elde ettiği bilgileri paylaşabilir.

2. Böyle bir bilginin paylaşımı öncesinde, sağlıyıcı taraf, bilginin gizli tutulmasını ve sadece belli şartlara bağlı kullanılmasını rica edebilir. Eğer bilgiyi alan taraf, bu ricayı yerine getiremeyecekse, bu bilginin yine de paylaşıp paylaşılmayacağını tesbit edecek olan tarafa bunu haber vermelidir. Eğer bilgiyi alan taraf, şartları tabi bilgiyi kabul ederse, bu, iki taraf tarafından bağlı olacaktır.

Başlık 4 – Uygulanabilir Uluslararası Anlaşmaların Yokluğunda Karşılıklı Yardım Talepleri ile İlgili Prosedürler

Madde 27 Uygulanabilir Uluslararası Anlaşmaların Yokluğunda Karşılıklı Yardım Talepleri ile İlgili Prosedürler

1. Talep eden ve talep edilen taraflar arasında, karşılıklı bir mevzuat veya bir bütünlükle ilgili, yardım anlaşması veya düzenleme olmadığı durumlarda, Bu maddenin 2. Paragrafından, 9. Paragrafına kadar olan bölümdeki hükümler geçerli olacaktır. Bu maddenin hükümleri, tarafların, bu maddenin tamamı veya kalanının uygulanması konusunda hemfikir olduğu durumlar hariç, herhangi bir anlaşma ve düzenleme mevcut ise, geçerli olmayacaktır.

2.
   a. Taraflardan her biri, karşılıklı yardıma ilişkin, yardımları alma ve yollama işleminden ve bu tip taleplerin yerine getirilmesinden veya bu talepleri yerine getirilmesi için yetkililerine iletmesinden, sorumlu yetkilileri veya bir merkez yetkilisini atayacaktır.

   b. Merkezi Yetkililer birbirleriyle direkt olarak iletişimde bulunacaklardır.

c. Taraflardan herbiri, imzaların atıldığı noktada veya mütalaa, kabul, onay veya katılma belgesini sunduğunda, Avrupa Konseyi Genel Sekreteri ile iletişime geçecek, bu paragraf uyarınca atanmış sorumlu yetkili kişilerin isimlerini ve adreslerini tanımlayacaklardır.

d. Avrupa Konseyi Genel Sektereri, taraflar tarafından belirlenen bu yetkililerin bir kaydını tutacak ve güncelleyecektir. Tarafların herbiri, her zaman için, kayıtlardaki detayların doğru olduğundan emin olacaklardır.

3. Bu maddedeki karşılıklı yardım talepleri, talep eden tarafın kanunlarının uyumsuz olmadığı müddetçe, o taraf tarafından belirlenen prosedürlere göre yerine getirilecektir.

4. Yardımın talep edildiği taraf, Madde 25, 4. Paragrafta belirtilen yardımın reddiyle ilgili gerekçelere ek olarak, ilgili yardımı:

a. Eğer yapılan rica, yardımı talep eden taraf, suçu bir politik suç olarak kabul ediyorsa veya politik bir suçla ilişkili bir suç ise, veya

b. Yardımı talep eden tarafta, ricanın yerine getirilmesinin, egemenliğini, güvenliğini, kamu düzenine zarar verecekse,

reddedebilir.

5. Talep edilen taraf, eğer böyle bir eylem, kendi yetkilileri tarafından yürütülen ceza soruşturmalarını ve prosedürlerine zarar verecek ise, hareketini geciktirebilir.

6. Yardımı reddetme veya ertelemeden önce, yardımın talep edildiği taraf, yardımı talep eden tarafla uygun şekilde değerlendirme yaparak, talep edilen isteğin kısmi olarak yerine getirilip getirilemeyeceğini veya şartlara bağlı olup olmayacağını gözden geçirecektir.

7. Yardımı talep edilen taraf, yardımı talep eden tarafa, yardım ricasının yerine getirilmesinin sonuçlarını bildirecektir. Talebin reddi veya ertelenmesi ile ilgili sebepler verilecektir. Yardımı talep edilen taraf, yardımı isteyen tarafa, talebin geciktirilmesinin veya yerine getirilememesinin sebeplerini belirgin şekilde bildirecektir.

8. Yardım talep eden taraf, yardımı talep ettiği taraftan, konusu dahil bu bölümde yapılmış herhangi bir isteği gizli tutmasını talep edebilir. Eğer yardım talep edilen taraf, gizlilikle ilgili talebi yerine getiremiyorsa, yardımı talep eden, o tarafı bilgilendirecek, buna göre, yardımın yine de yapılıp yapılmayacağını tesbit edecektir.

9.

a. Acil durumlar sözkonusu olduğunda, karşılıklı yardım veya iletişimle ilgili talepler, yardımı talep eden adli yetkililer tarafından, ilgili yetkililere gönderilebilir. Böyle durumların her birinde, yardım talep eden tarafın merkezi yetkilisine aynı anda, yardımı talep eden merkezi yetkili aracılığı ile bir kopya yollanacaktır.

b. Bu paragraf altındaki herhangi bir istek veya iletişim, Uluslararası Suç Polis Organizasyonu (Interpol) aracılığıyla yapılmış olabilir.

c. Bu maddenin alt paragraf a'sına uygun bir talep yapıldığında ve yetkili bu taleple ilgili yetkisi yeterli değil ise, sözkonusu yetkili, isteği, ulusal yetkili otoriteye iletecek ve bu durumu, yardımı talep eden tarafa direkt olarak bildirecektir.

d. Zorlayıcı eylemi gerektirmeyen bu paragraf altındaki talepler veya iletişimler, yardım talep eden tarafın yetkilileri tarafından,, ilgili yetkililere direkt olarak iletilebilir.

e. Taraflardan herbiri, imzaların atıldığı noktada veya mütalaa, kabul, onay veya katılma belgesini sunduğunda, Avrupa Konseyi Genel Sekreterini, yeterlilikle ilgili, bu paragraf altında yapılan tüm taleplerin merkezi otoriteye yöneltilmesi ile ilgili bilgilendirilecektir.

Madde 28 – Gizlilik ve Kullanımdaki Sınırlama

1. Talep eden ve talep edilen taraflar arasında, karşılıklı bir mevzuat veya bir bütünlükle ilgili, yardım anlaşması veya düzenleme olmadığı durumlarda, bu maddenin, hükümleri geçerli olacaktır. Bu maddenin hükümleri, tarafların, bu maddenin tamamı veya kalanının uygulanması konusunda hemfikir olduğu durumlar hariç, herhangi bir anlaşma ve düzenleme mevcut ise, geçerli olmayacaktır.
2. Yardım talep edilen taraf, aşağıdaki şartların sağlanması koşuluna bağlı olarak, bilgi veya materyal temin edebilir:

a. Karşılıklı adli yardım, böyle bir şartın yok olması durumunu uymaması talebi sözkonusu olduğunda bilginin gizli tutulması.

b. Bilginin, talepte belirtilen dışında, soruşturma ve yürütmelerde kullanılmaması.

3. Eğer bilgiyi talep eden taraf, paragraf 2'de belirtilen şarta uygun hareket edemezse , bu bilginin yine de paylaşıp paylaşılmayacağını tesbit edecek olan karşı tarafa bunu haber vermelidir. Eğer bilgiyi alan taraf, şartları kabul ederse, bu, iki taraf tarafından bağlı olacaktır.

4. Paragraf 2'de belirtilen şarta tabi olan bilgi ve materyali tedarik eden taraflardan herhangi biri, diğer partiden, bu şartla ilgili olarak, sözkonusu bilgi ve materyalin kullanımının açıklanmasını rica edebilir.

Bölüm 2 – Özel Hükümler

Başlık 1 – Geçici Önlemlere İlişkin Karşılıklı Yardım

Madde 29 – Depolanmış Bilgisayar Verisinin Hızlandırılmış Korunması

1. Taraflardan biri, diğer taraftan, bir bilgisayar sistemi aracılığı ile, talep eden tarafın, araştırma veya benzer erişim, el koyma veya benzer güvenlik altına alma veya verinin açğa çıkması için isteyebileceği bir taleple ilgili olarak, diğer tarafın alanı içinde yer alan ve depolanmış verinin hızlı bir şekilde korunmasının sağlanmasını isteyebilir.

2. Paragraf 1 de belirtilen koruma ile ilgili talep;

a. Korunmayı arayan yetkiliyi,

b. Suçla ilgili soruşturmaya veya davalara konu suçun veya ilgili bilgilerinin kısa bir özetini;

c. Korunması gereken depolanmış bilgisayar verisi ve suçla bağlantısını;

d. Depolanmış bilgisayar verisinin veya bilgisayar sisteminin yerinin sorumlusunu gösteren mevcut herhangi bir bilgisini.

e. Korunmanın gerekliliğini; ve

f. Taraflardan birinin, araştırma veya benzer erişim, el koyma veya benzer güvenlik altına alma veya verinin açığa çıkması için isteyebileceği bir talepte bulunmasını

belirtmelidir.

3. Diğer taraftan alınan talep üstüne, Talep edilen taraf, kendi kanunlarına uygun olarak, bahsi geçen verinin hızlı bir şekilde korunması için yeterli tüm önlemleri alacaktır. Talebe cevap vermek açısından, çift suçluluk, bu tip korunmanın sağlanması için gerekli şart olarak istenmeyecektir.

4. Araştırma, benzer erişim, elde etme veya benzer güvenlik altına alma veya depolanmış verinin açığa çıkartılması için karşılıklı yardım talebine cevap verme konusunda, çift suçluluğu şart koşan taraflardan biri, bu konvensiyonun 2. Maddesinden 11. Maddesine kadar olan bölümde belirtilen suçların dışındaki suçlarla ilgili olarak, çift suçluluğun şartlarının, açığa çıkarılma anında yerine getirilmediği inancının taşındığı durumlarda, bu maddedeki korunma talebini reddetme hakkını saklı tutabilir.

5. Buna ek olarak, korunmaya ilişkin talep ancak;

a. Sözkonusu talep, talep edilen tarafın, politik bir suç olarak kabul ettiği bir suç veya bir politik suçla bağlantılı ise, veya

b. Yardımı talep eden tarafta, ricanın yerine getirilmesinin, egemenliğini, güvenliğini, kamu düzenine zarar verme durumu oluşacaksa,

reddedilebilir.

6. Talep edilen taraf, korumanın, verinin geleceğe dönük mevcudiyetini teminat altına almayacağına, gizliliği tehdit edeceğine veya talep eden tarafın araştırmasına zarar vereceğine dair inancı oluşursa, sözkonusu taraf, , talebin yine de işlem görüp görmeyeceğini belirleyecek tarafa bildirecektir.

7. 1. Paragrafta bahsi geçen talebe istinaden yapılan herhangi bir koruma, yardımı talep eden tarafın, araştırma, benzer erişim, elde etme veya benzer güvenlik altına alma veya verinin açığa çıkarılması için, sözkonusu tarafın talepte bulunmasına imkan vermesi yönünden, 60 günden az olmayacaktır. Böyle bir talebin alınmasını takiben, bu taleple ilgili bir karar verilene kadar veri korunmaya devam edecektir.

Madde 30 – Korunmuş Trafik Verisinin, Hızlandırılmış Bir Şekilde Açığa Çıkması

1. Özel bir iletişimi ilgilendiren trafik verisinin korunması için, Madde 29'a uygun yapılmış bir talebin yerine getirilme esnasında, yardım talep edilen tarafın, başka bir ülkedeki bir servis sağlayıcısının, iletişimin aktarımı ile ilgisi olduğunu görmesi durumunda, yardım istenen taraf, hızlı bir şekilde, servis sağlayıcısının ve iletişimin aktarıldığı yolun belirlenmesi için gerekli trafik veri miktarını, öbür tarafla paylaşacaktır.

2. Paragraf 1 altında bahsi geçen trafik verisinin paylaşımı ancak;

a. Sözkonusu talep, talep edilen tarafın, politik bir suç olarak kabul ettiği bir suç veya bir politik suçla bağlantılı ise, veya

b. Yardımı talep edilen taraf, talebin yerine getirilmesini, egemenliğine, güvenliğine, ve kamu düzenine zarar vereceğini düşünürse

duraklatılabilir.

Başlık 2 – Araştırmacı Güçlere İlişkin Karşılıklı Yardım

Madde 31 – Depolanmış Bilgisayar Verisine Erişime İstinaden Karşılıklı Yardım

1. Taraflardan biri, diğer taraftan, Madde 29'a göre korunmuş veriler dahil, talep istenen tarafın alanı içinde yeralan bir bilgisayar sistemi aracılığı ile, depolanan verinin, araştırılmasını, veya benzer şekilde erişilebilmesini, el konmasını veya benzer bir şekilde güvenlik altına alınmasını isteyebilir.

2. Talep istenen taraf, talebe, Madde 23'te belirtilen uluslararası hukuki belgeler, düzenlemeler ve kanunların uygulanması vasıtasıyla ve bu bölümün diğer gerekli şartlara uygun olarak cevap verecektir.

3. Talep en hızlı şekilde;

a. İlgili verinin özellikle kaybolmaya ve değiştirilebilmeye açık olmasına inanmak için gerekçeler mevcut olduğu

b. Paragraf 2 de bahsi geçen hukuki belgeler, düzenlemeler ve kanunlar, hızlandırılmış bir işbirliğinin şart koşulduğu

durumlarda, hızlandırılmış bir temelde cevaplanacaktır.

Madde 32 – İzin Verilmiş Veya Kamuya Açık Olma Durumu Sözkonusu Olduğunda, Depolanmış Bilgisayar Verisine Trans-border Erişim

Taraflardan biri, diğer bir tarafın izni olmaksızın;

a. Coğrafik olarak verinin nerede olduğuna bakmaksızın, kamuya açık (açık kaynak) depolanmış bilgisayar verisine erişim sağlayabilir.

b. Alanındaki bir bilgisayar sistemi aracılığıyla, eğer, diğer taraf, sözkonusu bilgisayar sistemi vasıtasıyla,,tarafına, veriyi paylaşabilecek kanunu yetkiye sahip kişiyi sağlaması durumunda, diğer tarafta yeralan depolanmış bilgisayar verisine erişebilir veya veriyi alabilir.

Madde 33 – Trafik Verisinin Gerçek Zamanlı Toplanmasına İlişkin Karşılıklı Yardım

1. Taraflar, bir bilgisayar sistemi aracılığıyla, kendi alanlarında aktarılan, belirlenmiş iletişimlerle ilgili, trafik verisinin gerçek zamanlı toplanması konusunda birbirlerine karşılıklı yardım edeceklerdir. Paragraf 2'nin şartlarına bağlı olarak, bu tip yardım, yerel kanunlarla belirlenen şartlar ve prosedürler tarafından düzenlenecektir.

2. Taraflardan her biri, en azından, trafik verisinin gerçek zamanlı toplanabilmesinin benzer yerel durumlarda mümkün olabildiği suçlara ilişkin bu yardımları sağlayacaklardır..

Madde 34 - İçerik Verisinin Interception ına İlişkin Karşılıklı Yardım

Taraflar, yerel kanunları ve uygulanabilir anlaşmalarının izin verdiği en geniş ölçüde, bir bilgisayar sistemi aracılığıyla, aktarılan belirlenmiş iletişimin içerik verilerinin kayıt altına alınması veya gerçek zamanlı toplanabilmesi için birbirlerine karşılıklı yardım sağlayacaklardır.

Başlık 3 – 24 / 7 Ağ

Madde 35 – 24 / 7 Ağ

1. Taraflardan herbiri, bilgisayar sistemleri ve verileri ile ilgili suçlara ilişkin araştırmalar ve prosedürlerle ilgili acil yardım koşulunu temin etmek veya bir suçun elektronik formundaki kanıtların toplanması için, haftanın 7 günü, 24 saat bazında, bir kontakt noktası oluşturacaklardır. Bu tip bir destek, işi hızlandıracak olup, uygulama ve yerel kanunlar izin veriyorsa , aşağıdaki önlemleri direkt olarak uygulayacaklardır.

a. Teknik tavsiyenin koşulu.

b. 29. ve 30. Maddelere göre verinin korunması.

c. Kanıtların toplanması, hukuki bilginin koşullarının, şüphelilerin yerinin belirlenmis.

2.

a. Taraflardan birine ait contact noktasının, hızlandırılmış temelde, diğer tarafın contact noktası ile iletişimleri gerçekleştirmeye kapasitesi olacaktır.

b. Eğer bir taraf tarafından belirlenen contact noktası, o tarafın, Uluslararası karşılıklı yardım veya iadeden sorumlu yetkilierinin bir parçası değil ise, kontact noktası, hızlandırılmış durumlarda, bu tip yetki veya yetkililerle koordine olabileceğinden emin olmalıdır.

3. Taraflardan her biri, ağın çalışmasını hızlandırabilmek için eğitimli ve ekipmanlı personelinin olduğundan emin olacaktır

Bölüm 4 – Final Provizyonları

Madde 36 - İmza ve Devreye Girme

1. Bu konvensiyon, Avrupa Birliği Üye Devletleri ve bu olgunlaşma içinde yeralan Üye Olmayan Devletler tarafından imzaya açılacaktır.

2. Bu konvensiyon, , kabul veya onaya tabidir. Onay belgeleri, kabul veya onaylar, Avrupa Birliği Genel Sekreteri ile işleme sokulacaktır.

3. Bu konvensiyon, en az üç üye devleti, Avrupa Birliği Üye Devleti olmak üzere, 5 devletin, 1. Ve 2. Paragraftaki şartlara göre Konvensiyon tarafından bağlılıklarının taahüt etmesinden sonraki 3 aylık bir periyodun sona ermesini takip eden ayın ilk günü yürürlüğe girecektir.

4. İmzasıyla taahütlerine bağlı olduğu ifade eden herhangi bir devlet imzası ile ilgili olarak, konvensiyon, 1. Ve 2. Paragraftaki şartlarına göre, Konvensiyon tarafından bağlılıklarının taahhüt edilmesinden sonraki 3 aylık bir periyodun sona ermesini takip eden ayın ilk günü yürürlüğe girecektir.

Madde 37 – Konvensiyonun Katılımı

1. Bu konvensiyonun yürürlüğe girmesinden sonra, Avrupa Birliği Bakanlar Komitesi, Konvensiyona Kontrat Yapan Devletlerin oybirliğiyle muvafakatlarının sağlanması ve incelenmesinden sonra, konseyin üyesi olmayan ve bu konvensiyona accede yapmak için elaboration da yeralmayan herhangi bir devleti davet edebilirler. Kararlar, Bakanlar Komitesinde oturmaya yetkili, kontratlı devletlerin temsilcilerinin oybirliği ile ve Avrupa Konseyi Statüsünün, 20. Maddesinde şart koşulan çoğunluk tarafından alınacaktır.

2. Üstteki 1. Paragraftaki, konvensiyona katılan herhangi bir devletle ilgili olarak, konvensiyon, Avrupa Konseyi Genel Sekreteri ile katılım belgesinin ibraz tarihinden sonraki 3 aylık periyodun bitimini takip eden ayın ilk günü yürürlüğe girecektir.

Madde 38 – Bölgesel Uygulama

1. İmzanın atılması veya kabul, onay veya katılım belgesinin ibraz edilmesinden sonra, herhangi bir devlet, bu konvensiyonun hangi bölge veya bölgelerde geçerli olacağını belirleyebilir.

2. Daha sonra herhangi bir zamanda olmak üzere, Avrupa Koneyi Genel Sekreterliğine ithafen yapılan bir deklarasyon sayesinde, herhangi bir devlet, deklarasyonda belirlediği alanları bu konvensiyonun uygulaması ile arttırabilir. Böyle bir alanla ilgili olarak, Konvensiyon, Genel Sekreter tarafından deklarasyonun alınma tarihinden sonraki 3 aylık bir periyodun bitimini takip eden ayın birinci günü yürürlüğe girer.

3. Üstteki iki paragrafta yapılan herhangi bir deklarasyon, bu deklarasyonda belirtilen alanla ilgili olarak, Avrupa Konseyi Genel Sekreterliğine yapılan bir bildirimle, durdurulabilir. Durdurma işlemi, Genel Sekreterin, bu tip bir bildirimi alma tarihinden sonraki 3 aylık bir periyodun bitimini takip eden ayın birinci günü yürürlüğe girer.

Madde 39 – Konvensiyonun Efektleri

Mevcut Konvensiyonun amacı,

- 14 Aralık 1957'de (ETS No. 24) Paris'te imzaya açılan, Extradition İle İlgili Avrupa Konvensiyonu

- 20 Nisan1959'da (ETS No. 30) Strasbourg'da imzaya açılan, Suça Dair Konularda Karşılıklı Yardım İçin Avrupa Konvensiyonu

- 17 Mart 1978'de (ETS No. 99) Strasbourg'da imzaya açılan, Suça Dair Konularda Karşılıklı Yardım İçin Avrupa Konvensiyonuna Ek Protokol

şartlarını içine alarak, taraflar arasındaki uygulanabilir, çok yanlı veya çift taraflı anlaşmalar veya sözleşmeler eklemektir.

2 . Eğer iki veya daha fazla taraf, bu konvensiyonda geçen konularla ilgili sözleşme veya anlaşmalar üstünde bir sonuca çoktan varmışlar ise veya bu konular üstünde ilişkiler kurmuşlar veya gelecekte kuruyor olurlarsa, aynı şekilde ,bu ilişkileri buna göre düzenlemek için veya anlaşma ve sözleşmelerini uygulamak için yetkili olacaklardır.

Buna rağmen, tarafların ilişkilerini, oradaki düzenlenmiş hallerinden ziyade, mevcut konvensiyonda bulunan konularla ilgili kurması durumunda, bunları konvensiyonun amaçları ve prensiplerine uyumsuz olmayan bir tutum içinde yapmış bulunacaklardır.

3. Bu konvensiyondaki hiçbir şey, taraflardan birinin haklarını, kısıtlamalarını, yükümlülüklerini ve sorumluluklarını etkilemeyecektir.

Madde 40 – Deklarasyonlar

Avrupa Konseyi Genel Sekreterliğinin dikkatine yapılan yazılı bir bildirim aracılığıyla, Herhangi bir ülke, imzasını attığı anda veya onay belgesi, kabul, onay veya katılım ibrazını ettiğinde, Madde 2,3,6 paragraf 1.b, 7,9 paragraf3,ve 27, paragraf 9.e de şart koşulmuş olarak ek öğelerin gerekliliğinin ihtimaliile ilgili kendinin uygun olduğunu deklare etmiş olur.

Madde 41 – Federal Madde

1. Federal bir devlet, bu konvensiyonun 2. Bölümündeki ,merkezi yönetim ve kurucu devletler arasındaki ilişkileri düzenleyen temel prensiplerden oluşan yükümlülükleri veya Bölüm 3'teki işbirliğini şart koşan diğer benzer bölgesel varlıkları farz etme hakkını saklı tutabilir.

2. Paragraf 1'le ilgili bir rezervasyon yapılırken, federal bir devlet, bu tip, devre dışı bırakılabilecek bir rezervasyonun kurallarını uygulamayabilir, Bölüm 2'de belirlenmiş önlemlerin şartlarının yükümlülüklerini azaltabilir. Bir bütün olarak bakıldığında, bu önlemlere nazaran, çok geniş ve etkili bir kanun yaptırımı sağlayacaktır.

3. Bu konvensiyonun şartları ile ilgili, constituent Devletlerin yasamalır altında gelenin veya kanuni önlemler alması için federasyonun kurucu sistemi tarafından mecbur bırakılmayan, diğer benzer bölgesel varlıkların uygulanması durumunda, Federal Hükümet, bu ülkelerin yetkili otoritelerini bahsi geçen provisionla önerdikleri fikirleri paylaşacak, onların uygun eylemleri yapması ile ilgili cesaretlendirecektir.

Madde 42 – Rezervasyonlar

Avrupa Konseyi Genel Sekreterliğine yapılan yazılı bir bildirim aracılığıyla, herhangi bir devlet, imzasını attığı anda veya onay belgesi, kabul, onay veya katılım ibrasızını ettiiğinde, Madde 4, paragraf 2, Madde 6, paragraf 3, Madde 9, Paragraf 4, Madde 10, Paragraf 3, Madde 11, Paragraf 3, Madde 14, Paragraf 3, Madde 22, Paragraf 2, Madde 29, Paragraf4 ve Madde 41, Paragraf 1'de şart koşulan rezervasyonlarla ilgili kendinin uygun olduğunu beyan eder. Bunun dışında hiçbir başka rezervasyon yapılamaz.

Madde 43 – Durum ve Rezervasyonların Çekilmesi

1. Madde 42'ye göre bir rezervasyon yapmış olan bir taraf, bir bütün veya kısmi olarak bu rezervasyonu, Avrupa Konseyi Genel Sekreterliğine ithafen bir bildiri vasıtasıyla çekedebilir. Bu tip bir geriçekme, Genel Sekreterin, bu bildirimi aldığı tarihte geçerli sayılacaktır. Eğer sözkonusu bildiri, bir rezervasyonun çekilmesinin, sözkonusu olarak belirtilen bir tarihte yürürlüğe girmesi gerektiğiini belirtiyorsa ve bu tarih, Genel Sekreterin, bildirimi aldığı tarihten sonraki bir tarih ise geri çekilme, belirtilen sonraki tarihte geçerli olacaktır.

2. Madde 42'de bahsi geçen bir rezervasyonu yapan bir taraf, bu rezervasyonu, bir bütün veya kısmi olarak, koşullar izin verir vermez, geri çekecektir..

3. Avrupa Konseyi Genel Sekreteri, periyodik olarak, Madde 42'de bahsi geçen bir veya daha fazla rezervasyon yapan tarafları, bu tip rezervasyonların geri çekilmeleri açısından araştıracaktır.

Madde 44 – Değişiklikler

1. Bu konvensiyona yapılan değişiklikler, herhangi bir taraf tarafından önerilebilir ve Avrupa Konseyi Genel Sekreteri tarafından, Avrupa Birliği Üye Devletlerine, bu konvensiyonun 37. Maddesine göre, katılıma davet edilmiş herhangi bir devletin yanısıra, bu konvensiyonun oluşumunda yeralan üye olmayan Devletlere iletilir.

2. Bir taraf tarafından önerilen herhangi bir ek, önerilen ekle ilgili fikrini, Komite Başkanlarına yollayacak olan, Suç Problemleri İle İlgili Avrupa Komitesine (CDCP) ye iletilecektir.

3. Bakanlar Komitesi, önerilen ekleri değişiklikleri ve CDCP tarafından verilen fikirleri değerlendirecek, bu konvensiyona üye olmayan devletlerle bir değerlendirmeyi takiben, değişikliği kabul edebilir.

4. Bu maddenin 3. Paragrafına göre, Bakanlar Komitesi tarafından kabul edilen herhangi bir değişiklik yazısı, kabulü için taraflara yollayanacaktır.

5. Bu maddenin 3. Paragrafına göre kabul edilmiş herhangi bir değişiklik, tüm tarafların, sözkonusu değişikliği kabul ettiğine dair, Genel Sekreterliğe bilgi vermesinin 30. Günü geçerli sayılacaktır.

Madde 45 – İtilafların Çözümlenmesi

1. Suç Problemleri İle İlgili Avrupa Komitesi (CDPC), bu konvensiyonun yorumu ve uygulaması ile ilgili bilgilendirilecektir.

2. Taraflar arasında, bu konvensiyonun yorumu veya uygulaması ile ilgili bir ihtilaf sözkonusu olduğunda, taraflar, itilafın çözümü için görüşmeler aracılığıyla veya kendi tercihleri doğrultusunda herhangi barışçıl bir yol vasıtasıyla, CDPC ye ihtilafın bildirilmesi dahil olmak üzere, kararları Taraflar üstünde bağlayıcı olan bir hakem veya Uluslararası Adalet Mahkemesine sunacaklardır.

Madde 46 – Tarafların Konsültasyonu

1. Taraflar, uygun şekilde,

a. Problemlerin tanımlanması, konvensiyon altında yapılan herhangi bir deklarasyon veya rezervasyonun etkileri de dahil olmak üzere, bu konvensiyonun etkili faydası ve hayata geçirilmesi

b. Elektronik formdaki kanıt toplama ve siber suç ile ilgili teknolojik gelişmeleri, politikaları, belirgin legal bilgilerin değiş tokuşu

c. Konvensiyona muhtemel ekler veya değişiklikler

Konusunda kolaylaştırıcı bir görüşle birbiriyle konsültasyon yapacaklardır.

2. Suç Problemleri İle İlgili Avrupa Komitesi (CDPC), periyodik olarak, Paragraf 1'de bahsedilen konsültasyonların sonuclarına ilişkin bilgilendirilecektir.

3. CDPC, uygun olduğu şekilde paragraf 1 de bahsedilen konsültasyonları, kolaylaştıraca, tarafları, konvensiyona yapacakları ek ve değişiklikler ile ilgili çabalarında yardımcı olmak için önlemler alacaktır. Mevcut konvensiyonun yürürlüğe girmesinden sonraki en sonki 3 yılında, Suç Problemleri İle İlgili Avrupa Komitesi (CDPC), taraflarla işbirliği içinde, konvensiyonun şartlarının tümünün bir gözden geçirmesini yönetecek, gerekirse uygun ekler yapılmasını önerecektir.

4. Avrupa Konseyi tarafından varsayılanlar haricindeki, 1. Paragraftaki şartların gerçekleştirilmesinden çıkan tüm masraflar, taraflar tarafından, kendilerinin tesbit ettiği bir tutum içinde üstlenilmiş olacaktır.

5. Tarafların bu maddeye göre fonksiyonlarını yerine getirebilmeleri için, Konsey Sekreterliği, taraflara yardım edecektir.

Madde 47 – Kınama

1. Taraflardan biri herhangi bir zamanda, bu konvensiyonu, Avrupa Konseyi Genel Sekreterliğine ithafen yazılı bir bildirim ile kınayabilir.

2. Bu tip kınama, Genel Sekreterin Bildirimi alma tarihinden, sonraki 3 aylık bir periyodu takip eden, ayın ilk gününde geçerlilik kazanacaktır.

Madde 48 - Bildirim

Avrupa Konseyi Genel Sekreterliği, Avrupa Birliği Üye Devletlerini, bu konvensiyona katılmaya davet edilmiş veya katılmış devletlerin yanısıra, bu konvensiyonun oluşumunda yer alan üye olmayan devletleri;, bu konvensiyonun;

Herhangi bir imzası

Herhangi bir onay belgesi, kabul, onay ve katılım ibrazı
Madde 36 ve Madde 37 ye göre,, bu konvensiyonun yürürlüğe girmesinin herhangi bir tarihi
Madde 40'a göre yapılmış herhangi bir deklarasyon, Medde 42'ye göre yapılmış herhangi bir rezervasyon
Bu konvensiyona dair herhangi diğer eylem, bildiri ve iletişim.

Konusunda bilgilendirecektir.

Aşağıda imzası bulunanların şahitliğinde, bu konvensiyonu imzaladım.

Budapeşte'de, 23 Kasım 2001de, İngilizce ve Fransızca, her iki tekst de eşit olarak Avrupa Konseyi arşivine konmak üzere tek bir kopya halinde
Avrupa Konseyi Genel Sekreteri, yetkili kopyaları, tüm Avrupa Birliği Üye Devletlerine, bu konvensiyonun elaborationında yer alan üye olmayan devletlere, ve bu konvensiyonu accede etmeye davet edilmiş herhangi bir devlete iletecektir.