

**T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

TÜRKİYE’DE GÜVENLİ İNTERNET POLİTİKALARI

**SERHAT ÖZEREN
YÜKSEK LİSANS TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI**

**GEBZE
2017**

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

TÜRKİYE’DE GÜVENLİ İNTERNET
POLİTİKALARI

SERHAT ÖZEREN
YÜKSEK LİSANS TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMAN
DOÇ. DR. MEHMET GÖKTÜRK

GEBZE

2017

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

POLITICS OF SAFER INTERNET IN TURKEY

SERHAT ÖZEREN
A THESIS SUBMITTED FOR THE DEGREE OF
MASTER OF SCIENCE
DEPARTMENT OF ELECTRONIC ENGINEERING

THESIS SUPERVISOR
ASSOC. PROF. DR. MEHMET GÖKTÜRK

GEBZE
2017



GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 02/05/2017 tarih ve 2017/24 sayılı kararıyla oluşturulan jüri tarafından 09/05/2017 tarihinde tez savunma sınavı yapılan Serhat Özeren'in tez çalışması Elektronik Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Doç. Dr. Mehmet Göktürk

ÜYE

: Prof. Dr. M. Hakan Hocaoglu

ÜYE

: Prof. Dr. Ertugrul Karaçuha

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve/..... sayılı kararı.

İMZA/MÜHÜR

Doç. Dr. Arif Çağdaş AYDINOĞLU
Gebze Teknik Üniversitesi
Fen Bilimleri Enstitüsü Müdürü

ÖZET

Bu çalışmada Türkiye’de uygulanmakta olan Güvenli İnternet Hizmeti’nin kapsam ve etkinliği incelenmiştir. İnternet ortamındaki risk ve tehdit unsurlarını belirleyen literatür araştırmasının ardından Türkiye’de uygulanan Güvenli İnternet Hizmeti diğer ülkelerdeki uygulamalarla kıyaslanmış ve uluslararası mevzuat ve sözleşmeler çerçevesinde Türkiye’nin bulunduğu konum tespit edilmiştir. Çalışmanın ikinci bölümünde kullanıcıların güvenli İnternet kavramına yönelik algılarının ve genel bilinç düzeyinin tespit edilmesi için anket çalışması yapılmıştır. Literatür taraması ve anket sonuçlarının istatistiksel analizi sonucunda elde edilen bulgular ışığında güvenli İnternet kavramının ve Güvenli İnternet Hizmeti’nin etkinliğine yönelik sonuçlar elde edilmiştir.

Anahtar Kelimeler: Güvenli İnternet, İnternet Güvenliği, Bilgi Güvenliği, Bilişim Hukuku.

SUMMARY

In this study, the content and the efficiency of ‘Safe Internet Service’ applied in Turkey, was examined. After literature search that determines the risks and threat factors in internet, Safe Internet Service applied in Turkey was compared to the applications in other countries and Turkey’s position was detected in the international regulations and agreements. In the second part of the study, a survey was carried on in order to evaluate the perception and consciousness level of the users for Safe Internet concept. In the light of the findings of literature search and the statistical analyses of the survey, the results were reached with regard to the efficiency of the concept of safe internet and Safe Internet Service.

Key Words: Safe Internet, Internet Security, Security of Information, Information Technology (IT) Law.

TEŞEKKÜR

Tez çalışmamın araştırma aşaması ve anket uygulaması konularında destek veren Telekomünikasyon ve Enerji Hizmetleri Tüketici Hakları ve Sektörel Araştırmalar Derneği (TEDER), Teknoloji Bilgilendirme Platformu (TBP) ve Tüm Telekomünikasyon İş Adamları Derneği (TÜTED) yönetim kurulu üyeleri ve çalışanlarına; literatür taraması ve bilimsel analiz konularında yardımcı olan tez danışmanım Doç.Dr. Mehmet GÖKTÜRK'e, bu süreç içerisinde bana desteğini eksik etmeyen eşim Ülkü ÖZEREN'e, kızlarım Zeynep ve İrem'e teşekkürlerimi sunarım.

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	v
SUMMARY	vi
TEŞEKKÜR	vii
İÇİNDEKİLER	viii
SİMGELER ve KISALTMALAR DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
TABLolar DİZİNİ	xii
1. GİRİŞ	1
1.1. Tezin Amacı, Katkısı ve İçeriği	1
2. İNTERNET TEKNOLOJİSİ	2
2.1. İnternet ve İletişim Teknolojileri Yaygınlığı	3
3. GÜVENLİ İNTERNET	11
3.1. Güvenli İnternet Hizmeti	11
3.2. Google Güvenli İnternet Hizmeti	12
4. GÜVENLİK TEHDİTLERİ	14
4.1. İstemcilere Yönelik Tehditler	14
4.2. Sosyal Mühendislik	16
4.3. Sunuculara Yönelik Tehditler	19
4.3.1. Bilgi Tarama (Probe ya da scan)	19
4.3.2. Hizmet Engelleme (Denial of Service - DoS)	20
4.3.3. Yönetici Hesabı ile Yerel Oturum Açma	20
4.3.4. Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi	20
5. SİBER GÜVENLİK	21
5.1. Siber güvenlik konusunda bakanlıklar düzeyindeki çalışmalar	21
5.1.1. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı	21
5.1.2. Milli Savunma Bakanlığı	22
6. KİŞİSEL VERİLERİN KORUNMASI	24
6.1. Kimlik Bilgileri	25
6.2. Adres Bilgileri	25
6.3. Kredi Kartı Bilgileri	26

7. TÜRKİYE CUMHURİYETİ MEVZUATINDA GÜVENLİ İNTERNET	28
7.1. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	28
7.1.1. 5651 Sayılı Yasa Hakkında Değişiklik Önerileri	29
8. TÜRKİYE’DE GÜVENLİ İNTERNET HİZMETİ	31
8.1. Uluslararası Normlar ve Güvenli İnternet Uygulamaları	32
9. ANKET ÇALIŞMASI	38
9.1. Anketin Pilot Çalışması	38
9.2. Frekans Dağılımları	39
9.3 Analizler	51
10. SONUÇLAR VE YORUMLAR	67
 KAYNAKLAR	 69
ÖZGEÇMİŞ	71
EKLER	73

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Açıklamalar

Kısaltmalar

UDHB	: Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
TİB	: Telekomünikasyon İletişim Başkanlığı
TÜİK	: Türkiye İstatistik Kurumu
GİH	: Güvenli İnternet Hizmeti

ŞEKİLLER DİZİNİ

<u>Sekil No:</u>	<u>Sayfa</u>
2.1: Kıtalara göre İnternet kullanımı dağılım grafiği.	4
2.2: Kıtalara göre Facebook kullanımı dağılımı.	8
2.3: Ülkelere göre Facebook kullanımı dağılımı.	9
2.4: Şehirlere göre Facebook kullanımı dağılımı.	10

TABLÖLAR DİZİNİ

<u>Sekil No:</u>	<u>Sayfa</u>
2.1: Kıtalara göre İnternet kullanımı dağılımı.	3
2.2: Hanelerde bilişim teknolojileri bulunma oranı.	5
2.3: Hanelerde İnternet erişim imkanı.	6
2.4: Hanelerde kullanılan İnternet bağlantı türü.	7
9.1 Katılımcıların Cinsiyet Dağılımı	39
9.2 Katılımcıların Doğum Yerleri.	40
9.3 Katılımcıların Doğum Yılları	43
9.4 Katılımcıların Eğitim Durumları.	44
9.5 Katılımcıların Meslekleri.	45
9.6 Katılımcıların Medeni Durumları.	45
9.7 Çocuk Sahibi Katılımcılar.	46
9.8 Katılımcıların Gelir Seviyeleri.	46
9.9 Katılımcıların İnternet Kullanıcısı Oldukları Süreler.	46
9.10 Katılımcıların İnternet Kullanım Amaçları.	47
9.11 Katılımcıların İnternet'e Eriştikleri Ortamlar.	49
9.12 Katılımcıların İnternet'i Kullanım Amaçları	51
9.13 Katılımcıların Güncel Gelişmeleri Takip Etme Durumu.	53
9.14 Akıllı Cep Telefonu Kullanımı.	57
9.15 Antivirüs Yazılım Kullanımı	58
9.16 İnternet Dolandırıcılığı.	58
9.17 İnternet ve Özgürlük.	58
9.18 Güvenli İnternet Hizmeti.	59
9.19 Çapraz Tablo Analizleri Cinsiyet.	60
9.20 Çapraz Tablo Analizleri Çocuk Bilgisi	61
9.21 Anket Soruları Karşılaştırmalı Analizler.	62

1. GİRİŞ

Bilişim ve mobil iletişim teknolojileri geliştikçe günlük yaşantımızdaki süreçler İnternet ortamına entegre olmaktadır. Günümüzde vatandaşlar, firmalar ve devletler arasındaki pek çok ilişki İnternet teknolojileri üzerinden yürütülmektedir. Akıllı telefonların yaygın kullanımıyla birlikte nüfusun büyük bir çoğunluğu 24 saat İnternet bağlantısına sahip olmuştur.

İnternet teknolojilerinin yaygın kullanımının doğal bir sonucu olarak devletler özellikle çocuk istismarlarını engellemek ve çocukları zararlı içeriklerden korumak amacıyla uluslararası sözleşmelere taraf olmaya ve ulusal İnternet politikaları geliştirmeye başlamıştır.

1.1 Tezin Amacı, Katkısı ve İçeriği

Bu çalışmanın amacı, ülkemizde uygulanmakta olan Güvenli İnternet Hizmeti'nin kapsamı ve etkinliğinin incelenmesidir. Yürürlükteki uygulamanın diğer ülkelerdeki uygulamalarla kıyaslanması ve İnternet tabanlı tehditlere karşı etkinliğinin ölçülmesi için literatür çalışması yapılmıştır. Ülkemizdeki kullanıcıların güvenli İnternet kavramı ve Güvenli İnternet Hizmeti'ne yönelik algılarını tespit etmek için anket çalışması yapılmıştır. Elde edilen bulgular çerçevesinde güvenli internet hizmetinin etkinliği tartışılmıştır.

2. İNTERNET TEKNOLOJİSİ

İnternet, dünya genelindeki bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirine bağlayan elektronik iletişim ağıdır [1]. Türk Dil Kurumu, İnternet sözcüğüne karşılık olarak “genel ağ” ifadesini önermiştir. İnternet, çok protokollü bir ağ olup birbirine bağlı bilgisayar ağlarının tümü olarak da tanımlanabilir. Binlerce akademik ve ticari ağla devlet ve serbest bilgisayar ağının birbirine bağlanmasıyla oluşmuştur. Bilgisayarlar arasında bilgi TCP/IP protokolleri aracılığıyla transfer edilmektedir.

İnternet'in kökeni, kesintisiz, sağlam ve özel bir bilgisayar ağı kurmak isteyen Amerika Birleşik Devletleri hükümeti tarafından 1960 yılında başlatılan araştırmalara dayanmaktadır. 1980'lerde Ulusal Bilim Vakfı tarafından yeni bir ABD omurgasının finansmanı için toplanan özel fonlar, dünya çapında katılım ve birçok özel ağın birleşmesini sağlamıştır. 1990'larda uluslararası bir ağın yaygınlaşması ile internet, modern insan hayatının temelinde yer almıştır. Günümüzde günlük yaşantıdaki pek çok süreç (Bankacılık işlemleri, alışveriş, rezervasyon, hukuki işlemler vb.) İnternet üzerinden yürütülmektedir.

İnternet üzerinden ağ sayesinde iletişim kuran bilgisayar sistemleri olan askeri iletişim sistemi Semi-Automatic Ground Environment (SAGE) ve ticari havayolu rezervasyon sistemi olan Semi-Automatic Business Research Environment (SABRE) 1950'lerin başında çalışmaya başlamıştır. 1960 larda ise the Advanced Research Projects Agency (ARPA), ABD nin savunda sistemi için the Advanced Research Projects Agency Network (ARPANET) ün tasarım finansmanı olmaya başladı. 1960'larda oluşturulan projeler sayesinde 1969'da İnternet o dönemin zirvesine ulaşmıştır. Bu tarihten sonra da ARPANET bildiğimiz modern İNTERNET olarak hayatımıza girmiş oldu. 70'li yılların başında Amerikan üniversitelerinde bu projeden yararlanma imkânı verilmesinin ardından e-posta (SMTP) ve NNTP uygulamaları yaygınlık kazanmaya başlamıştır. Bunları FTP ve HTTP izlemiştir [2].İnternet iletişimi TCP/IP (Transmission Control Protocol / Internet Protocol) adı verilen bir protokol kümesi kullanılarak sağlanmaktadır. Bu protokollere örnek olarak, dosya alma/gönderme protokolü (FTP, File Transfer Protocol), Elektronik posta iletişim protokolü (SMTP Simple Mail Transfer Protocol), TELNET protokolü verilebilir. Web sayfalarına bağlanmak için kullanılan protokol ise Hyper Text Transfer Protocol

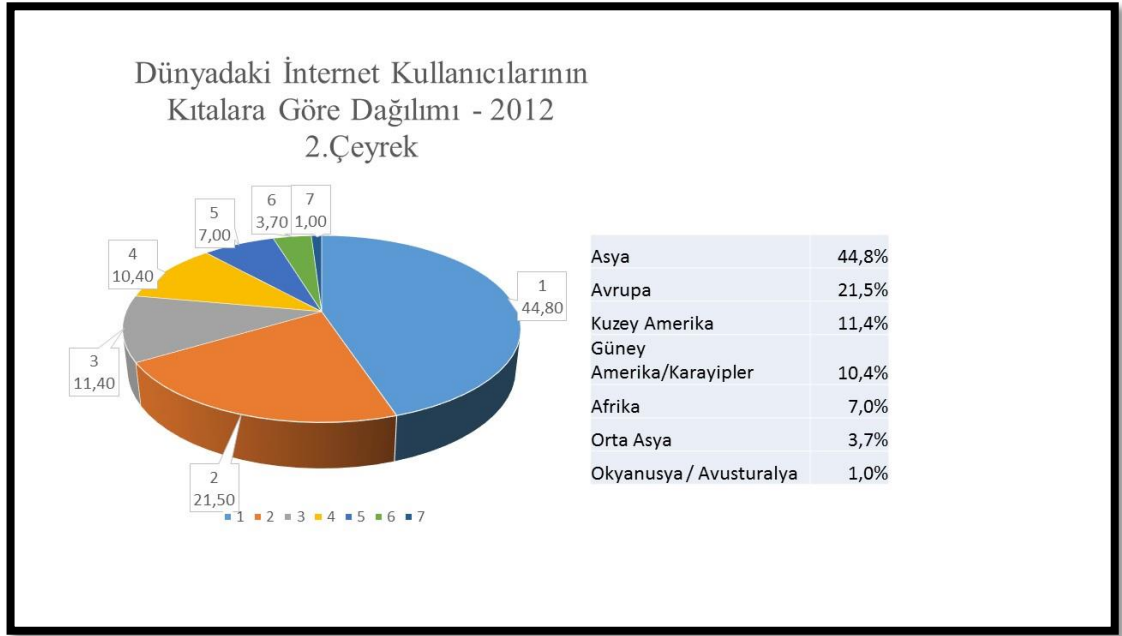
(HTTP) olarak adlandırılmaktadır. TCP/IP protokolü aynı zamanda, diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok farklı tipte bilgisayar veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır [3].

2.1. İnternet ve İletişim Teknolojileri Yaygınlığı

Kentlerde iletişim teknolojilerinin kullanımına ilişkin yapılan araştırmalarda 2000 yılından 2012 yılına kadar dünya genelinde %566,4 lük bir artış görülmektedir. 2000-2012 yılları arasında en büyük artış %3.606,7 ile Asya kıtasında en düşük artış ise %153.3 ile Kuzey Amerika'da hesaplanmıştır. Kuzey Amerika, dünya üzerinde iletişim teknolojilerini nüfusa oranla en yoğun olarak kullanan bölge olduğu için artış hızı diğer bölgelere göre daha yavaş ilerlemektedir.

Tablo 2.1: Kıtalaraya göre İnternet kullanımı dağılımı [7].

DÜNYA İNTERNET KULLANIMI VE NÜFUS İSTATİSTİKLERİ 30.06.2012						
Dünya Bölgeleri	Nüfus (2012 Tahmini)	İnternet Kullanıcıları 31.12.2000	İnternet Kullanıcıları En Son Data	Penetrasyon	2000-2012 Arası Büyüme	Kullanıcı Oranları
Afrika	1,073,380,925	4,514,400	167,335,676	15,6%	3,606.7 %	7.0 %
Asya	3,922,066,987	114,304,000	1,076,681,059	27,5%	841.9 %	44.8 %
Avrupa	820,918,446	105,096,093	518,512,109	63,2%	393.4 %	21.5 %
Orta Asya	223,608,203	3,284,800	90,000,455	40,2%	2,639.9 %	3.7 %
Kuzey Amerika	348,280,154	108,096,800	273,785,413	78,6%	153.3 %	11.4 %
Güney Amerika / Karayipler	593,688,638	18,068,919	254,915,745	42,9%	1,310.8 %	10.6 %
Okyanusya/Avustralya	35,903,559	7,620,480	24,287,919	67,6%	218.7 %	1.0 %
DÜNYA TOPLAM	7,017,846,922	360,985,492	2,405,518,376	34,3%	566.4 %	100.0 %
NOTLAR: (1) İnternet Kullanımı ve Dünya Nüfus İstatistikleri 30.06.2012 tarihi içindir. (2) Demografik(Nüfus) sayılarda ABD Nüfus Müdürlüğü ve yerel Nüfus Müdürlüklerinin dataları baz alınmıştır. (3) İnternet Kullanım Bilgisi Nielsen Online, GFK, Uluslararası Telekomünikasyon Birliği ve Yerel ICT Düzenleyicileri tarafından yayınlanan datadan gelmiştir.						



Şekil 2.1: Kıtalara göre İnternet kullanımı dağılım grafiği.

Ülkemizde TUIK tarafından yapılan Şekil 2.1’de gösterilen “Hane Halkı Bilişim Teknolojileri 2012” araştırmasında elde edilen bulgulara göre;

Türkiye genelinde hanelerin %47,2’si evden İnternete erişim imkânına sahiptir. Bu oran 2011 yılının aynı ayında %42,9 idi. Evden İnternete erişim imkânı olmayan hanelerin %27,6’sı evden İnternete bağlanmama nedeni olarak İnternet kullanımına ihtiyaç duymadıklarını belirtmişlerdir.

İnternet erişim imkânı olan hane oranı kentsel yerlerde %55,5 iken, kırsal yerlerde %27,3’tür. İstatistiki Bölge Birimleri Sınıflaması (İBBS) Düzey-1’e göre %60,5 ile TR1-İstanbul, %49,7 ile TR2-Batı Marmara, %60,6 ile TR4-Doğu Marmara, %57,5 ile TR5-Batı Anadolu bölgesinde İnternet erişim imkanı olan hane oranı Türkiye ortalamasının üzerindedir.

2012 yılı Nisan ayında hanelerin %43,2’sinde genişbant İnternet erişim imkânı bulunmaktadır. ADSL, %31,3 ile tüm haneler, %66,4 ile İnternet kullanılan haneler arasında en çok kullanılan bağlantı türüdür. 3G bağlantı ise tüm hanelerin %13,9’unda, İnternet kullanılan hanelerin %29,5’inde İnternet erişim imkânı sağlamaktadır.

Tablo 2.2: Hanelerde bilişim teknolojileri bulunma oranı.

Hanelerde bilişim teknolojileri bulunma oranı (%)			
			2012
	Türkiye	Kent	Kır
Masaüstü bilgisayar (PC)	31,8	38,2	16,3
Taşınabilir bilgisayar (Dizüstü, tablet)	27,1	33,5	11,8
Cep telefonu	93,2	95,1	88,5
Oyun konsolu	4,6	5,8	1,7
Avuçiçi (PDA)	1,4	1,7	0,5
Sabit hatlı telefon	45,5	47,4	40,9
Dijital fotoğraf makinesi / kamera	27,1	33,2	12,4
DVD / VCD / DivX oynatıcı	35,0	42,0	18,0
Yazıcı, tarayıcı, faks veya en az ikisinin bir arada bulunduğu çok fonksiyonlu cihazlar	16,0	20,0	6,4
Diğer	0,0	0,1	0,0
Hiçbiri	2,9	1,9	5,2

Tablo 2.3: Hanelerde İnternet erişim imkanı.

Hanelerde İnternet erişim imkanı (%)				
				2012
		İnternete erişim imkanı var	İnternete erişim imkanı yok	Bilmiyo r
TR	Türkiye	47,2	51,6	1,2
TR	Kent	55,5	43,8	0,8
TR	Kır	27,3	70,6	2,1
TR1	İstanbul	60,5	39,1	0,4
TR2	Batı Marmara	49,7	49,4	0,9
TR3	Ege	45,5	53,7	0,8
TR4	Doğu Marmara	60,6	39,0	0,4
TR5	Batı Anadolu	57,5	41,4	1,1
TR6	Akdeniz	39,6	58,9	1,5
TR7	Orta Anadolu	41,0	57,3	1,6
TR8	Batı Karadeniz	39,5	60,3	0,2
TR9	Doğu Karadeniz	32,6	62,0	5,5
TR A	Kuzeydoğu Anadolu	41,5	54,2	4,3
TRB	Ortadoğu Anadolu	35,6	60,8	3,7
TR C	Güneydoğu Anadolu	21,5	77,8	0,7

Tablo 2.4: Hanelerde kullanılan İnternet bağlantı türü.

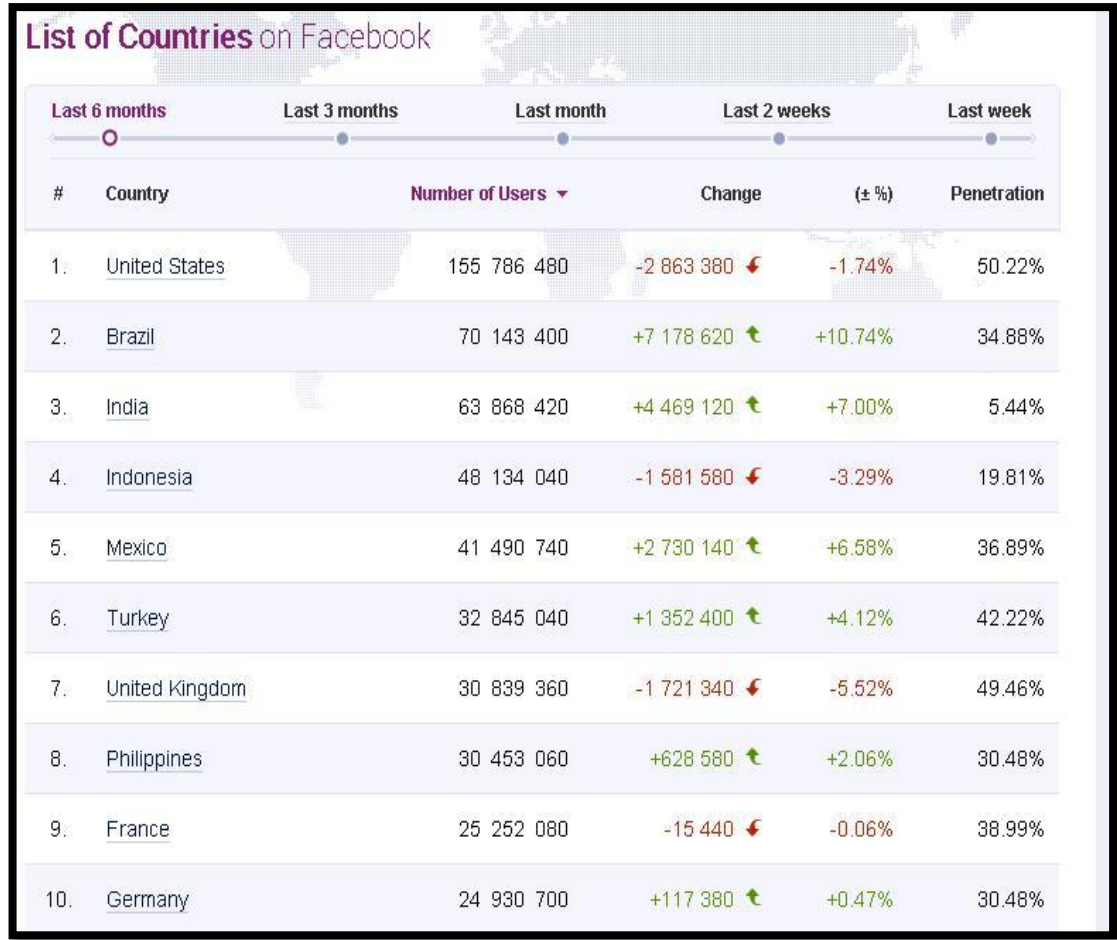
Hanelerde kullanılan İnternet bağlantı türü (%)						
						2012
İnternet bağlantı türü	Türkiye	Kent	Kır	Evden İnternete erişim imkanı olan haneler içinde		
				Türkiye	Kent	Kır
Darband bağlantı	7,6	7,6	7,8	16,2	13,7	28,5
Telefon hattı ile çevirmeli bağlantı veya ISDN bağlantısı	0,2	0,3	0,0	0,4	0,5	0,0
Cep telefonu üzerinden darband bağlantı (WAP, GPRS)	7,5	7,3	7,8	15,8	13,2	28,5
Genişband bağlantı	43,2	52,1	21,6	91,5	94,0	79,1
ADSL bağlantı	31,3	37,8	15,6	66,4	68,2	57,2
Kablolu sabit bağlantı (Kablo TV)	3,9	5,4	0,3	8,3	9,7	1,2
Kablosuz sabit İnternet bağlantısı (uydu, WiFi)	1,9	2,3	0,7	3,9	4,2	2,5
Kablosuz mobil bağlantı (3G)	13,9	16,6	7,5	29,5	29,9	27,4
Cep telefonu üzerinden 3G bağlantı	9,8	11,5	5,6	20,7	20,8	20,4
3G modemi üzerinden mobil bağlantı (VINN, JET, VODEM gibi mobil modem)	5,6	6,8	2,5	11,8	12,3	9,2

Günümüzde iletişim teknolojilerinin yaygınlığını ölçmek için sosyal medya kullanımı yaygınlığı ölçümleri oldukça önemli bir göstergedir. Sosyal Medya istatistikleri üzerine çalışmalar yapan socialbakers.com sitesi tarafından elde edilen

bulgular ışığında Facebook kullanan nüfusun kıtalara göre oranı hesaplandığında en büyük oranın %42,43 ile Kuzey Amerika; en düşük oranın %5,03 ile Afrika olduğu görülmektedir.

List of continents on Facebook			
#	Continent	Users	Penetration
1	Asia	273 408 920	6.75%
2	Europe	249 532 800	30.15%
3	North America	230 724 820	42.73%
4	South America	150 023 640	37.83%
5	Africa	51 279 160	5.03%
6	Oceania	14 334 740	38.68%

Şekil 2.2: Kıtalarla göre Facebook kullanımı dağılımı.



Şekil 2.3: Ükelere göre Facebook kullanımı dağılımı.

Aynı çalışmanın ülke başkentleri üzerinde yapılması sonucunda aşağıdaki bulgular elde edilmiştir.

List of cities on Facebook

#	City	Users ▼	Pen. ▲
1.	Bangkok	12 797 500	250.71%
2.	Jakarta	11 658 760	136.52%
3.	London	6 811 680	90.14%
4.	Mumbai	5 926 980	46.70%
5.	Seoul	5 510 100	53.24%
6.	Buenos Aires	5 473 060	41.85%
7.	Rio de Janeiro	5 062 320	84.04%
8.	Santiago	4 937 820	102.08%
9.	Kuala Lumpur	4 784 040	329.03%
10.	Taipei	4 552 920	57.84%
11.	Paris	4 171 320	195.05%
12.	Bangalore	3 811 960	74.69%
13.	Madrid	3 773 400	115.89%
14.	Delhi	3 570 320	32.67%
15.	Ankara	3 091 780	87.91%

Şekil 2.4: Şehirlere göre Facebook kullanımı dağılımı.

3. GÜVENLİ İNTERNET

Güvenli İnternet, teknik güvenlik ve içerik güvenliği olarak iki açıdan değerlendirilmektedir. İngilizce’de teknik güvenlik “security” kavramıyla, içerik güvenliği ise “safety” kavramıyla tanımlanmaktadır. Güvenli İnternet terimi Türkiye’deki mevzuat çerçevesinde Internet Safety teriminin Türkçe karşılığı olarak kullanılmaktadır.

3.1. Güvenli İnternet Hizmeti

İnternetin toplumumuzda daha yaygın ve bilinçli kullanılmasına katkı sağlamak amacıyla başlatılan Güvenli İnternet Hizmeti ilk zamanlarda yapılan olumsuz propagandaların etkisini kolayca üzerinden atarak hızla yaygınlaşmaya başlamıştır.

22 Kasım 2011 de hayata geçirilen proje ile dileyen İnternet kullanıcıları bu hizmetten yararlanmaya başlamıştır. Özellikle ailelerin tercih ettiği bu alternatif hizmete iş çevrelerinin de bankacılık gibi işlemlerde güvenli internet ortamı sunması nedeniyle tercih ettiği görülmektedir. Güvenli İnternet Hizmeti, çocukların ve gençlerin İnternet üzerindeki bilgi kirliliğinden ve zararlı içeriklerden korunmaları amacıyla ortaya çıkan bir projedir. Güvenli İnternet Hizmetine ilişkin düzenleme yapılırken, İnternet kullanıcılarının Bilgi Teknolojileri ve İletişim Kurumuna ilettikleri talepler ve şikayetler dikkate alınmıştır. İlgili İşletmecilerle yapılan teknik çalışmalar sonucunda 24 Ağustos 2011 tarihinde “İnternet’in Güvenli Kullanımına İlişkin Usul ve Esaslar” Bilgi Teknolojileri ve İletişim Kurulu tarafından belirlenerek yayımlanmıştır.

İnternet kullanımının ülkemizde yaygınlaşması ve çocukların evden İnternet’e bağlanmalarının yanı sıra mobil internet ile de bağlantı kurdukları gözetildiğinde bu şekildeki bir alternatif hizmetin gerekli olduğu düşünülmektedir. Güvenli İnternet Hizmeti’nin en önemli özelliği ise demokratik teamüller gözetilerek dünya uygulamaları paralelinde tamamen tercihe bağlı ve ücretsiz olmasıdır. Hizmetin önemi kullanıldıkça daha da çok anlaşılmaktadır.

Güvenli İnternet Hizmetinin alt yapısı Erişim Sağlayıcılar tarafından oluşturulmaktadır. Güvenli İnternet Hizmeti tamamen isteğe bağlıdır ve Hizmeti talep edecek aboneler isteklerini internet servis sağlayıcılarına bildirmektedirler. Hiç bir

talepte bulunmayan aboneler mevcut İnternet hizmetlerini kullanmaya devam etmektedirler ve hizmetten memnun kalmamaları durumunda Güvenli İnternet Hizmeti almayı kesebilmektedirler.

Güvenli internet Hizmetinde çocuk ve aile profili olmak üzere iki profil mevcuttur. Aboneler diledikleri an internet servis sağlayıcılarından temin ettikleri kullanıcı adı ve şifre ile profiller arasında geçiş yapabilmektedirler.

3.2. Google Güvenli İnternet Hizmeti

Dünyanın en çok kullanılan arama motoru Google, İnternet ortamında en geniş etkiye sahip güvenli internet hizmetini sunmaktadır. Google tarafından yayınlanan güvenli internet tavsiye dökümanı tarafından kullanıcıların ailesiyle çevrimiçi güvenlik konusunda konuşmaları önerilmektedir.

Ailelerin teknolojiye ilişkin aile kuralları, beklentileri ve uygunsuz kullanımın sonuçlarıyla ilgili net bir tavır seri belirten dökümandaki tavsiyeler aşağıda sıralanmıştır.

Çocuklarınızın zor kararlarla karşılaştıklarında sizden yardım isteyebilecek kadar rahat hissetmelerini sağlayın. Bu yaklaşım, aile üyelerinizin kendi başlarına İnternet'i keşfederken güvende hissetmelerine ve soruları olduğunda size sorabileceklerini bilmelerine yardımcı olabilir.

Teknolojiyi çocuklarınızla birlikte kullanın. Bu, çevrimiçi güvenliği öğretmenin iyi bir yoludur ve çevrimiçi güvenlik konularını ortaya çıktıkça ailenizle birlikte ele almanız için fırsatlar sağlar.

Ailenizle çevrimiçi hizmetleri ve İnternet sitelerini konuşun. Ailenizle ne tür siteleri ziyaret etmeyi sevdiklerini ve her bir aile üyesi için neyin uygun olduğunu konuşun.

Şifreleri koruyun. Ailenize, çevrimiçi ortamda güvenli şifrelerin nasıl ayarlanacağını öğrenmeleri için yardım edin. Ailenize şifrelerini, bir ebeveyn gibi güvenecekleri yetişkinler dışında kimseye vermemelerini hatırlatın. Bir okul, kafe veya kütüphane gibi herkese açık bilgisayarlardayken, çevrimiçi hesaplarından çıkış yapma alışkanlığı edindiklerinden emin olun.

Gizlilik ayarlarını ve paylaşım denetimlerini kullanın. Düşünceleri, fotoğrafları, videoları, durum güncellemelerini ve daha pek çok içeriği paylaşmak için birçok site

vardır. Bu hizmetlerin birçoğu gizlilik ayarları sunar ve yayınlamadan önce içeriğinizi kimlerin görebileceğine karar vermenize yardımcı olacak denetimler sağlar. Ailenizle neleri herkesle paylaşıp paylaşmamaları gerektiğini konuşun. Aileniz ve arkadaşlarınızla ilgili kişisel bilgileri gizli tutarak ve herkese açık paylaşılan içeriklerde kişilerin adlarını belirtmeyerek diğer kişilerin gizliliğine saygı duymalarına yardımcı olun.

Yaş kısıtlamalarını kontrol edin: Google dahil birçok çevrimiçi hizmetin, hizmetlerini kullanabilecek kişileri kısıtlayan yaş sınırlamaları vardır. Örneğin, bir Google hesabınızın olması için yaş gereksinimlerini karşılamanız gerekir ve bazı Google ürünleri, 18 yaşında veya daha büyük kullanıcılarla sınırlandırılmıştır. Çocuğunuzun bir hesap kaydı oluşturmaya izin vermeden önce web sitelerinin kullanım şartlarını her zaman kontrol edin ve çocukların kullanabileceği siteler ve hizmetlerle ilgili aile kurallarınız varsa çocuklarınıza bunlar konusunda açıkça bilgi verin.

Ailenize sorumlu bir şekilde iletişim kurmayı öğretin. Şu pratik kuralı uygulayabilirsiniz: Bir şeyi bir kişinin yüzüne söylemiyorsanız, bunu kısa mesaj, e-posta, anlık mesajla göndermeyin veya bir kişinin sayfasında yorum olarak yayınlamayın. Çevrimiçi ortamda söylediğiniz şeylerin diğer kişilerin kendilerini nasıl hissetmelerine yol açacağını konuşun ve uygun ilişki türleri konusunda aile kuralları belirleyin.

Diğer yetişkinlerle konuşun. Arkadaşlarınız, akrabalarınız, öğretmenler, antrenörler ve danışmanlarla görüşün. Çocuklarla çalışan diğer ebeveynler ve profesyoneller, özellikle aşına olmadığınız teknoloji alanıyla uğraşırken, aileniz için doğru olana karar vermenize yardımcı olacak harika birer kaynaktır.

Bilgisayarınızı ve kimliğinizi koruyun. Virüsten korunma yazılımı kullanın ve bunu düzenli olarak güncelleyin. Virüsten korunma yazılımına ihtiyacı olmayan bir Chromebook'unuz varsa bu gerekmez. Vatandaşlık numarası, telefon numarası veya ev adresi gibi, çevrimiçi ortamda yayınlanmaması gereken kişisel bilgi türleri konusunda ailenizle konuşun. Ailenize tanımadıkları kişilerden gelen dosyaları kabul etmemelerini veya e-posta eklerini açmamalarını öğretin.

Güvenlik konusunu sürekli hale getirin. Güvende olmak bir defalık bir şey değildir; teknoloji geliştikçe ailenizin gereksinimleri de değişecektir. Sürekli diyalog içinde olmaya çalışın. Ailenizin temel kurallarını, herkesin durumunu göz önünde bulundurarak yeniden belirleyin ve düzenli aralıklarla konuşmak için zaman ayırın [4].

4. GÜVENLİK TEHDİTLERİ

4.1. İstemcilere Yönelik Tehditler

İnternet güvenliği konusunda en sık karşılaşılan tehditler, istemcilere yönelik olarak düzenlenen saldırı ve aldatma yöntemleridir. Bu yöntemlerden bazıları bilişim sistemlerine herhangi bir saldırgan yazılım veya sistemdeki güvenlik açıkları gibi teknik unsurlar kullanmadan doğrudan kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerini dikkate alarak uygulanan yetkisiz erişim teknikleridir.

Yetkisiz erişim amacıyla en yaygın olarak kullanılan yöntem, şifre veya şifreye erişim için kullanılan gizli soru yanıtının tahmin edilmesidir. Bir çok bilişim sistemi, kullanıcıların şifrelerini unutmaları durumunda kullanılmak üzere bir gizli soru ve yanıt ikilisinin tanımlanmasını istemektedir. Günümüzde telefon bankacılığı işlemlerinde banka yetkilileri tarafından sorulan anne kızlık soyadı, gizli soru ve yanıt ilişkisinin en yaygın örneğidir.

Kullanıcıların bilişim sistemlerine erişim şifrelerini yazarken gözlenmesi, gizlice izlenmesi, ajanda post-it, not kağıtları gibi şifre yazılabilecek materyallerin incelenmesi şeklinde uygulanan yöntem ise “Omuz Sörfü” adı verilmiştir [5]. Yazılım kullanımı ile yetkisiz erişim yöntemlerinde ise bir bilişim sistemine erişim için kullanılan temel araçlar, sözlük atağı (dictionary attack) ya da kaba kuvvet algoritmaları (brute force attack) yöntemleri biçiminde uygulanmaktadır. İnternet teknolojisinin gelişmesiyle birlikte söz konusu temel yetkisiz erişim araçlarına trojan, keylogger ve screen logger algoritmaları da eklenmiştir.

Sözlük Atağı, bir bilişim sistemini koruyan şifrenin, sözlükte bulunan bir sözcükle eşdeğer olduğu varsayımına dayanan bir saldırı yöntemidir. Şifre denemelerini otomatik olarak tekrarlayan bir algoritmanın bir metin dosyasındaki sözcükleri denemesiyle çalışan sözlük atağı yöntemi, uzak sistemlere yetkisiz erişim amacıyla kullanılmaktadır.

Kaba kuvvet algoritmaları ise, bir bilişim sistemini veya bir belgeyi koruyan şifrenin, bütün harf, rakam ve özel karakter kombinasyonlarını kullanan algoritmalar aracılığıyla çözülmesini sağlayan bir saldırı yöntemidir. Sözlük atağından farklı olarak

anlamalı anlamsız bütün harf, rakam ve karakter kombinasyonları kullanılmakta ve şifre ne kadar karmaşık ve uzun olursa olsun mutlak suretle çözülmektedir.

Kaba kuvvet algoritmaları, çok uzun süren işlemler olduğu ve gelişen teknolojiyle birlikte önleyici teknikler geliştiği için uzak sistemleri tehdit etmemektedir. Ancak şifreli belgelerin (word, excel, pdf) şifrelerini çözmek için halen kullanılmakta olan bir yöntemdir.

Kullanıcının klavye’de basmış olduğu tuşları, basım sırasına göre bir metin dosyası içerisine yazıp daha sonra e-posta ya da uzaktan erişim yöntemiyle uzak sisteme transfer eden yazılım türüne keylogger adı verilmektedir.

Screen Logger ise, kullanıcının fare ile her tıklama hareketi sonucunda, farenin ekranda durduğu noktanın köşegen merkezi olan ve 100x100 (bu değer değişebilmektedir) piksel büyüklüğündeki bir grafiği düşük çözünürlükte kaydederek kullanıcı bilgisayarının sabit diskinde daha sonra alınmak üzere saklayabilen veya e-posta yolu ile uzak sisteme transfer eden yazılım türüne verilen addır.

Kullanıcı bilgisayarında, açılışta çalışma özeliği bulunan gizli bir sunucu (server) oluşturarak bütün sistem kaynaklarını uzak sistemdeki kişinin kullanmasını sağlayan, bilgisayarda yapılan bütün işlemleri izleme, dinleme ve müdahale etme yetkisini uzak sisteme devreden yazılım türüne trojan adı verilmektedir.

Yukarıda tanımlanan güvenlik tehditleri için birtakım önlemler mevcuttur. Bu önlemlerin yaygın olarak kullanılanları şifre sağlamlık denetimi ve CAPTCHA algoritması olarak öne çıkmaktadır.

Şifre sağlamlık denetiminde, kullanıcının tercih ettiği şifre, bilişim sistemlerinde bulunan sözlük dosyaları ile karşılaştırılarak kullanıcının sözlükte bulunan sözcükleri şifre olarak tanımlaması engellenmektedir. Ayrıca kullanıcı adıyla tanımlanan şifre arasındaki uyumlar da farklı algoritmalar tarafından kontrol edilmektedir.

Sunucuya gönderilen şifre denemelerine sınırlama getiren algoritmalar, güvenlik resmi ya da güvenlik kodu olarak bilinen CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) algoritmaları, tek kullanımlık şifre üreten token cihazları, mobil imza, e-imza gibi yöntemler şifrelerin saldırganlar tarafından yazılımlar aracılığı ile elde edilmesini engellemektedir.

4.2. Sosyal Mühendislik

Bilgisayar ve ağ güvenliği açısından sosyal mühendislik, insan davranışındaki unsurları güvenlik açıkları olarak değerlendirip, bu açıklardan faydalanma yöntemiyle güvenlik süreçlerini aşarak sistem yöneticisi ya da kullanıcıların yetkilerine erişim tekniklerini kapsayan bir terimdir.

Sosyal mühendislik kavramını tanımlayan ve bilişim dünyasında konuyla ilgili en temel kaynaklardan biri olarak kabul edilen ‘Art Of Deception’ adlı kitabın yazarı Kevin Mitnick, kitabında insan unsurunu ağ güvenliğinin en zayıf halkası olarak tanımlamaktadır .

Bilişim teknolojilerinin gelişimine paralel olarak bilişim sistemlerine yönelik saldırılarda ve bilişim suçlarında önemli artışlar gözlenmektedir. Bilişim sistemlerindeki gelişmeler, kullanımı yaygınlaşan yeni platformlar (mobil teknolojiler, cep bilgisayarları) yeni güvenlik açıklarını da beraberinde getirmektedir. Ayrıca, bilişim teknolojisindeki yeni araçlar (bilgisayar dilleri, veri tabanı yapıları) yeni saldırı yöntemlerinin gelişmesine olanak sağlamaktadır. Bilişim teknolojisindeki hızlı gelişim, bilişim suçlarının çeşitliliği ve yaygınlığının daha büyük oranlarda artmasına neden olmaktadır.

Sosyal mühendislik kavramının farklı bir boyutu olan ‘tersine sosyal mühendislik (reverse social engineering)’ kavramı ise; sosyal mühendislik yöntemi ile saldırıya uğrayan mağdurun, yardım almak amacıyla farkında olmadan sistemine saldırı düzenleyen kişiyle temas kurması olarak tanımlanmıştır [6].

Sosyal mühendislik yöntemiyle yapılan yetkisiz erişim denemeleri yalnızca bir kullanıcının hedef alınması veya kullanıcıların toplu halde hedef alınması şeklinde iki farklı biçimde gerçekleşmektedir.

Yalnızca bir kullanıcının hedef alındığı yetkisiz erişim denemelerinde; yüz yüze, telefon, faks veya e-posta iletişim kanalları kullanılmaktadır. Söz konusu iletişim yöntemleri doğrudan hedef alınan kişiye karşı olduğu gibi, kimlik taklidi yöntemiyle sistem yöneticilerine yönelik olarak da uygulanabilmektedir.

İletişim kanallarının kitlesel hedeflere yönelik olduğu durumlarda genellikle aldatıcı web sitesi ve yığın e-posta iletişim kanalının birleşimi tercih edilmektedir. Fake mail, phishing, e-posta aldatmacaları ve hoax e-postaları kitlesel hedefleri aldatmaya yönelik olarak uygulanan yöntemlerin başlıcalarıdır.

Sosyal mühendislik yöntemi, bireylerin davranış karakteristikleri ve niteliklerindeki unsurları güvenlik açıkları olarak değerlendirerek sistemlere yetkisiz erişim olanağı elde etmektedirler. Aşağıda söz konusu genel geçer davranış modellerinden bazıları ve modellerdeki rol aktör davranışları örnek olarak verilmiştir;

- Otoriter tavırlar insan davranışlarını yönlendirir ve etkiler

Sosyal mühendislik yönteminin en yaygın kullanım biçimlerinden birisi saldırının hedefi olan kişiye karşı otoriter bir kimlikle yaklaşmaktır. Genellikle kamu görevlisi ya da kolluk kuvveti rolüyle iletişim kuran saldırgan, şifre ya da kişisel bilgileri elde etmek amacıyla mağdurun farkında olmadan adli bir kovuşturmayaya maruz kaldığını veya hesap bilgilerini elde eden bir kişi tarafından zor durumda bırakıldığını öne sürerek kişisel bilgilerini almaya çalışır.

- Aynı karakteristik özelliklere, zevk ve tercihlere sahip kişiler birbirlerini daha kolay etkiler

Sosyal mühendislik yönteminin diğer yaygın kullanım biçimi şifre veya kişisel bilgileri elde edilmek istenen kişiye ortak ilgi alanlarının var olduğu hissi yaratılarak güven verilmesi ve diyalog sonrası elde edilen bilgiler yardımıyla özel bilgilere ulaşılması şeklinde gerçekleşmektedir.

- Yardımsever tavırlar güven telkin eder

Sosyal mühendislik yöntemlerinde kullanılan bir diğer rol, güven vermeye yönelik olarak uygulanan yardımsever tavırlardır. Özellikle ATM cihazlarında işlem yapan kişileri hedef alan senaryolarda mağdurun ATM cihazında kalması sağlanan banka kartının iptali için şifre bilgisinin istenmesi söz konusu rolün en yaygın örneğidir.

- İnsanlar az bilgiye sahip oldukları konularda kendilerine söylenen sözlere inanma eğilimindedir

Otoriter tavırların insan davranışları üzerindeki etkisi ve yardımsever tavırların güven telkin etmesi varsayımlarının birleşimi olan senaryolarda genellikle teknik konularda bilgisi yetersiz olan kişiler seçilmekte ve söz konusu davranış niteliği otoriter veya yardımsever bir tavırla suistimal edilebilmektedir.

- İnsanlar zor durumdaki kişilere yardımcı olmaktan hoşlanırlar

Bireylerin yardımseverliğini hedef alan aldatıcı senaryolarda kullanılan varsayımlardan birisi de zor durumdaki kişilere yardımcı olma davranışıdır. Özellikle ATM cihazlarında işlem yapan kişileri hedef alan senaryolarda, para çekme limiti dolduğu için parasız kalan mağdur rolünü oynayan kişilerin, başkalarının hesabını havale veya EFT için kullanmaları söz konusu davranış niteliğinin kötü niyetle kullanımının örneğidir.

Sosyal mühendislik yöntemlerinin günümüzde hızla yaygınlaşan kullanım biçimleri, iletişim teknolojilerini ve karmaşık olmayan algoritmaları destek unsur olarak içermesi veya teknoloji odaklı zarar verici uygulamalara (virüs, yığın e-posta vb.) yardımcı unsur olarak tercih edilmesi şeklinde gözlenmektedir. Bu yöntemlerin en yaygını PHISHING yöntemi olarak adlandırılmıştır.

Açılımı password harvesting fishing sözcüklerinden oluşan phishing yöntemi oltacılık olarak da adlandırılmaktadır. Genellikle banka ve finans sitelerinden gönderilmiş gibi hazırlanan ve kullanıcıları tedirgin edecek ifadeler ile birlikte ilgili kurum ya da kuruluşun sahte web site bağlantısını içeren e-posta iletileridir. İletiler açıldığında kullanıcıların girdiği bilgiler, ortadaki adam olarak tanımlanan saldırgana iletilmekte, kullanıcıya ise sistemin geçici olarak servis dışı olduğuna ilişkin bir mesaj görüntülenmektedir.

Günümüzde sosyal mühendislik uygulamaları sistemlere yetkisiz erişim ve kişisel bilgi temini amacıyla olduğu kadar, haksız kazanç elde etmek için de kullanılmaktadır. Çeşitli ve sürekli olarak yenilenen senaryolar aracılığıyla yapılan saldırıların en yaygın örnekleri arasında yeşil kart, loto, kara para transfer, sahte ürün tuzakları bulunmaktadır.

Bazı bilgisayar virüsleri yayılma hızlarını artırmak için sosyal mühendislik tekniklerini kullanmaktadırlar. İlk örneği Win32/Sober adlı virüs olan söz konusu virüsler yerleştikleri bilgisayar sistemlerindeki belge adlarını inceleyerek bilgisayar kullanıcısının iş veya hobi niteliklerine uygun bir isimle kopyalarını adres defterindeki kişilere göndermektedir.

Sober virüsü için Microsoft'un web sitesinde 'Bu solucan, kullanıcıları sosyal mühendislik yoluyla e-postadaki ekli bir dosyayı veya yürütülebilir dosyayı açmaya ikna etmeye çalışır. Alıcı dosyayı ve yürütülebilir dosyayı açarsa, solucan kendisini sistemin adres defterindeki tüm kişilere gönderir.' açıklaması yapılmıştır [7].

Yığın e-postaların küresel bir sorun haline gelmesi sonucu kullanıcıların e-postaları açmadan silme davranışlarını geliştirmeleri nedeniyle, posta göndericileri sosyal mühendislik yöntemlerini uygulamaya başlamıştır. E-postaların konu başlığında re: ibaresinin bulunması, bir başvurunun tamamlanması ya da bir hizmet veya servisin süresinin dolmasına ilişkin sahte mesajların yer alması gibi örnekler yığın e-postaların yayılmasında sosyal mühendislik yöntemlerinin uygulama örnekleridir.

E-posta adreslerini yığın e-posta gönderen kişi ve kuruluşlara temin etmek için hazırlanan sahte içerikli e-postalarda sosyal mühendislik teknikleri yaygın olarak kullanılmaktadır. Bu tür e-postalar, toplumsal açıdan tepki yaratması amaçlanan aldatıcı, yanlış bilgiler içermekte ve genellikle son bölümlerinde çok sayıda kişiye iletilmesi için telkinler yer almaktadır. Bir ülke ya da kuruma yönelik gerçek dışı bilgiler, sağlıkla ilgili tehditler, kan aranması, zor durumdaki kişilere yardım talebi gibi çeşitleri bulunan e-posta aldatmacaları uzun yıllardır kullanılmakta olan etkin bir yöntemdir [8].

4.3. Sunuculara Yönelik Tehditler

Bilgisayar sistemlerinde en genel anlamda sızma ya da saldırı makine başından yapılacak izinsiz erişimlerden başlar ve çok geniş bir yelpazeye yayılır. Bilgisayar ağları söz konusu olduğunda ise saldırılar sadece bu tip kullanıcı ve erişim temelli saldırılar ile sınırlı kalmaz. Ağ üzerinden yapılan saldırılar günümüzde çok sık karşılaşılan problemler arasındadır. Ağ saldırılar 4 temel kategoride incelenebilirler.

4.3.1. Bilgi Tarama (Probe ya da scan)

Bu saldırılar bir sunucunun ya da herhangi makinanın, geçerli ip adreslerini, aktif portlarını veya işletim sistemini öğrenmek için yapılan saldırılardır. Bilinen saldırılardan bunlara örnek olarak, belirli bir protu sürekli tarama saldırısı (ipsweep) bir sunucu üzerindeki hizmetleri bulmak için tüm portların taranması (portsweep) verilebilir.

4.3.2. Hizmet Engelleme (Denial of Service - DoS)

Bu saldırılar genelde TCP/IP protokol yapısındaki açıklardan faydalanarak veya bir sunucuya çok sayıda istek yöneltmek hizmet engellenmesine neden olan saldırılardır. DoS saldırıları kendi içinde gruplara ayrılır [9].

- i) Smurf: ICMP mesajlarının broadcast ile tüm ağı dağıtılmasıyla oluşur.
- ii) Selfping: Kullanıcının sunucuya sürekli ping isteği göndermesiyle gerçekleşir.
- iii) tcprset: saldırgan bilgisayarın kurmaya çalıştığı bağlantılar için bilgisayar adına reset isteği göndererek bağlantısını engeller.
- iv) mailbomb: saldırgan sunucuya sürekli olarak e-posta gönderir.

4.3.3. Yönetici Hesabı ile Yerel Oturum Açma

Kullanıcı haklarına sahip olunmadığı durumda misafir ya da başka bir kullanıcı olarak izinsiz erişim yapılmasıdır. Yaygın örnekleri:

- i) Ssh Trojan: unix üzerinde çalışan bir trojan saldırısıdır.
- ii) guest: tahmini kolay şifreleri kullanarak sisteme girilmesidir.

4.3.4. Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi

Bu tip saldırılarda sisteme girme izni olan fakat yönetici olmayan bir kullanıcının yönetici izni gerektirecek işler yapmaya çalışmasıdır. Örnekleri:

- i) Eject: Solaris üzerinde eject programı ile tampon taşmasına yol açıp, yönetici haklarına sahip olunmasıdır.
- ii) Sqlattack: sql veritabanı kurulu Linux makinalarda sunucuya bağlanan kullanıcının belirli komutlarla yönetici hakları ile komut satırı elde etmesidir.

5. SİBER GÜVENLİK

Siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır. Siber güvenliğin temel hedefleri erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizliliklerdir. (ITU – T X.1205 sayılı Tavsiye Kararında yer alan ve uluslar arası alanda kabul gören tanımdır) [10].

5.1.Siber güvenlik konusunda bakanlıklar düzeyindeki çalışmalar

5.1.1. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile TÜBİTAK arasında Siber Güvenlik konusunda 3 Mayıs 2012 tarihli bir protokol imzalanmıştır.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Bilim Sanayi ve Teknoloji Bakanlığı arasında Siber Güvenlik konusunda 14 Ağustos 2012 tarihli bir protokol imzalanmıştır

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile TÜBİTAK arasında Ulusal Siber Güvenlik Teknoloji Geliştirme Programı Konusunda 14 Ağustos 2012 tarihli bir “Danışmanlık Hizmetleri Alımı Sözleşmesi” imzalanmıştır.

Bakanlar Kurulu’nun, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı, 20 Ekim 2012 tarihli Resmi Gazete’de yayınlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Siber Güvenlik Kurulu'nun 1'inci toplantısında 20 Aralık 2012 tarihinde onaylanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Bakanlar Kurulu tarafından 20 Haziran 2013 tarihinde kabul edilmiştir.

Siber Olaylara Müdahale Ekiplerinin (SOME) Kurulu, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ, 11 Kasım 2013 tarihli Resmi Gazete'de yayınlanmıştır.

655 sayılı KHK, 5809 sayılı Elektronik Haberleşme Kanunu ve 5651 sayılı Kanun'la ilgili değişiklikler 02.12.2013 tarihli Bakanlar Kurulu toplantısında görüşülmüştür. Değişiklik talepleri Siber güvenlik çalışmaları ve Siber Güvenlik Kurulunun varlığı ve işleyişi, Yer sağlayıcılara yönelik hapis cezası uygulamasının kaldırılması, Yer sağlayıcıların sınıflandırılması ve teşviki, Yer sağlayıcılar için, faaliyet belgesi yerine bildirim usulü getirilmesi başlıklarında değerlendirilmiştir.

Adalet Bakanlığı Siber Güvenlik Kanun Taslağı ilgili kurumların görüşlerine gönderilmiştir [11].

5.1.2. Milli Savunma Bakanlığı

Genelkurmay Muhabere Elektronik ve Bilgi Sistemleri Başkanlığı tarafından konuya ilişkin olarak, Ekim 2012 tarihinde başlatılan süreç içerisinde ilgili makamlar ile koordine edilerek söz konusu mutabakat muhtırası hazırlanmıştır. 20 Haziran 2013 tarihinde Ulaştırma Denizcilik ve Haberleşme Bakanlığında icra edilen 2'nci Siber Güvenlik Kurulunda alınan karar doğrultusunda, Türkiye Cumhuriyeti Hükümeti ile NATO Siber Savunma Yönetim Kurulu arasında, siber savunma alanında işbirliğine yönelik olarak hazırlanan "NATO Siber Savunma Mutabakat Muhtırası" nı imzalamaya, Türkiye Cumhuriyeti adına Millî Savunma Bakanlığı yetkilendirilmiştir. Bu kapsamda; 12 Temmuz 2013 tarihinde Dışişleri Bakanlığında, 22 Kasım 2013 ve 27 Kasım 2013 tarihlerinde Millî Savunma Bakanlığında; Genelkurmay Başkanlığı, Dışişleri Bakanlığı, Ulaştırma Denizcilik ve Haberleşme Bakanlığı ve TÜBİTAK katılımı ile icra edilen toplantılar neticesinde söz konusu mutabakat muhtırası güncellenerek uzlaşma ile nihai hale getirilmiştir. "NATO Siber Savunma Mutabakat Muhtırası"nın, Türkiye Cumhuriyeti Hükümeti ile NATO Siber Savunma Yönetim

Kurulu arasında imzalanması için gerekli işlemlerin ve sürecin başlatılması aşamasına gelinmiştir [12].

6. KİŞİSEL VERİLERİN KORUNMASI

İnternet ve iletişim teknolojisindeki hızlı gelişmeler, kişisel veri ve bilgilerin korunması sorununu da gündeme getirmiştir. Bu doğrultuda ulusal ve uluslararası kuruluşlar konunun üzerinde durmaya başlamışlardır. Bilişim sistemlerinde toplanan kişisel bilgiler, ilgili kişilere zarar vermeyecek doğrultuda kullanılmalıdır. Kişisel bilgilerin korunması sorunu, kişisel bilgilerin açıklanmasının kişiye verebileceği zarardan kaynaklanmaktadır

Kişilerin kendilerinin konu oldukları bilgilere, “isme bağlı veriler” veya “bireysel veriler” denilmektedir. İsme bağlı veriler, örgütler tarafından depo edilmekte, işlenerek bilgi haline getirilmekte, talep halinde üçüncü kişilere devredilmektedir. Bu dolaşım bazen sınır ötesine de uzanmaktadır. Toplumsal örgütler ve bazı serbest meslekler grupları kişisel veri toplayıcısıdır. Toplumsal örgütler kapsamına ise en başta devlet olmak üzere çeşitli kamu kuruluşları, özel hukuk kesiminde kar amaçlı kuruluşlar, sivil toplum kuruluşları girmektedir.

Meslekler kapsamında ise doktorluk, avukatlık, noterlik, bankacılık gibi meslekler bu kapsamda sayılabilir. Kısacası, toplumda hemen herkes bilgi toplamakta değerlendirmekte ve bunları değişime tabi tutmaktadır [13].

Bu kavram kapsamında, toplumları ilgilendiren en önemli konu, hangi bilginin bireye özgü, dolayısıyla gizli tutulması ve korunması gerektiği konusudur. Bu alanda, tüm ülkelerin üzerinde anlaştığı tek bir doğru bulunmamaktadır. Bir ülke vatandaşlarının değerlendirmelerine göre açık olması gereken bir bilgi, diğer ülke vatandaşları tarafından gizlenmesi gereken bir bilgi olarak değerlendirilebilmektedir.

Türkiye’de kişisel verilerin korunmasına ilişkin kanun tasarısı 22 Nisan 2008 tarihinde TBMM onayına sunulmuş ve halen meclis onayı beklenmektedir. Kanun kapsamında kişisel veriler, belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgileri; kişisel verilerin işlenmesi kavramı ise kişisel verilerin, kullanılan araç ve yöntemlere bakılmaksızın toplanması, elde edilmesi, kaydedilmesi, düzenlenmesi, depolanması, uyarlanması veya değiştirilmesi, değerlendirilmesi, kullanılması, açıklanması, aktarılması veya elde edilebilir olması, ayrılması veya birleştirilmesi, dondurulması, silinmesi veya yok edilmesi gibi işlemlerden herhangi birini ifade etmektedir.

Kanun kapsamında kişisel verilerin taşınması gereken nitelikler;

- i) Hukuka ve dürüstlük kurallarına uygun olarak elde edilmesi ve işleme tâbi tutulması,
- ii) Belirli, açık, hukuka ve dürüstlük kurallarına uygun amaçlar için kaydedilmesi, kullanılması ve bu amacın aşılması,
- iii) Doğru ve güncel olması, gerektiğinde yenilenmesi veya silinmesi,
- iv) Kişilerin kimliklerini belirtecek bir biçim altında, ancak toplandıkları amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur.

Şeklinde ifade edilmiştir.

Kişilerin ırk, siyasî düşünce, din veya diğer inançları ile sağlık, gizli ve özellikle cinsel yaşamlarına ilişkin kişisel veriler ve ceza mahkûmiyetleri, ancak kişi için yeterli koruyucu güvenceler sağlayan özel kanunî düzenlemeler varsa işleme tabi tutulabilir. Kanun söz konusu verileri “özel niteliği olan kişisel veriler” olarak tanımlamıştır [14].

6.1. Kimlik Bilgileri

Ülkemizde vatandaşların kimlik bilgilerini tutan bir çok kurum vardır. Nüfus ve tapu Müdürlükleri, vergi daireleri, sosyal güvenlik kurumları (SSK, Emekli Sandığı, Bağkur), Adli Sicil Kurumu, emniyet birimleri, muhtarlıklar, okullar, hastaneler gibi bir çok merkezde birbirinden ayrı ve bağımsız kayıtlar mevcuttur.

Nüfus ve vatandaşlık İşleri Genel Müdürlüğü tarafından 1974 yılında başlatılan MERNİS Projesi (Merkezi Nüfus İdaresi Sistemi) çerçevesinde, Türk vatandaşlarına ilişkin tüm bilgilerin elektronik ortama işlenmesi ve farklı kurumların tuttuğu kayıtların ortak bir havuzda toplanarak aralarındaki tutarsızlıkların giderilmesi hedeflenmiştir.

6.2. Adres Bilgileri

İkametgah, bir kimsenin yerleşmek niyetiyle oturduğu yer anlamına gelmektedir. Medeni kanunun ifadesiyle, “Yerleşim yeri bir kimsenin sürekli kalma niyetiyle oturduğu yerdir” (Bkz.Türk Medeni Kanunu Madde 19.) Yine başka bir tanımla, ikametgah bir kişinin bir yere bağlılığını ifade eden bir kavramdır. Bir kişinin

kendisinin veya ailesinin sürekli ve geçici olarak konakladığı, ikamet ettiği yerlere ait bilgiler de kişisel veri niteliğindedir. Adres bilgilerinin yetkisiz şahısların eline geçmesi halinde istenmeyen rahatsızlıklara sebebiyet verebilecekleri açıktır.

Kimlik Bildirim ve İkamet Yasası 1973 yılında kabul edilmiştir. Ancak bu kanun daha çok asayiş sağlamaya ve güvenlik birimlerinin işini kolaylaştırmaya amacıyla hazırlanmıştır.

Kanun, kişilerin ikamet bilgilerini kolluk güçlerine ve muhtarlıklara verilmesi gerektiğini belirtmiştir.

6.3. Kredi Kartı Bilgileri

Kredi kartı kullanan kişilerin adresleri, telefon numaraları ve gelir düzeyi kredi kartı işletmecisi tarafından, kartın hazırlanması aşamasında istenmekte ve kayda geçirilmektedir. Bundan daha önemlisi, kredi kartı ile yapılan tüm harcamaların kaydı tutulmaktadır.

Kredi kartı ile yaptığı alışverişlerden, bireyin ne zaman nerede bulunduğu kolayca öğrenilmektedir. Yaptığı alışverişlerin içeriğinden, alışveriş alışkanlıkları anlaşılabilir. Bireyin zaman içinde nerede bulunduğuna ilişkin bilgi, hakkında yasal soruşturma yapılıyorsa anlamlıdır. Ancak, hakkında yasal soruşturma kararı olmayan bireyin bu yolla izlenmesi, bireysel haklara tecavüz olarak değerlendirilmelidir.

İnsanların alışveriş alışkanlıkları, ticari kuruluşlar için önemli ipuçları verir. Bu nedenle, özellikle hizmet ve pazarlama kuruluşları, bireylere ilişkin bilgilere sahip olmaya çalışmaktadırlar. Ticari kuruluşlar, bireylere ilişkin, bilgilerden (cinsiyet, eğitim, adres, alışveriş listesi ve benzeri) oluşturdukları veri ambarı üzerinde, veri madenciliği yöntemleri ile, müşteriye mutlu kılacak şekilde satışlarını artırıcı uygulamalar geliştirebilir ya da ileriye dönük öngörülerde bulunabilirler.

Ticari beklentilerle toplanan bu bilgilerin amaç dışında kullanılması sakınca yaratacaktır.

Sözgelimi, toplanmış olan bilgilerin bir başka kuruma satılması sonucunda, yeni kurumun bu bilgileri değerlendirip, bireyi istenen alışverişe yönlendirmesi olanağı bulunmaktadır. Bireye gönderilecek duyurular, kişiyi istenen bir yerden alışveriş

yapmaya yöneltebilir. Birey bu yönlendirmeden habersiz olduğu için, haksız bir ticarete zorlanmış olacaktır. Bu da bireysel haklara tecavüz sayılabilir.

Kişisel Verilerin Korunması Yasa Tasarısı'na göre, isim, telefon numarası, pasaport numarası, resim, görüntü ve ses kayıtları, parmak izleri gibi bilgiler devlet veri bankasında olacaktır. Bu veriler yasal zorunluluk dışında sır kabul edilip kimseyle paylaşılmayacaktır. Kişisel verileri yasalara aykırı olarak ele geçiren, kaydeden, bir başkasına verenlere ilişkin Türk Ceza Kanunu'nda yer alan cezalara ek olarak yeni ceza maddeleri de tasarıda yer almaktadır. Buna göre bu yönetmeliğin hükümlerine aykırı olarak kişisel verileri depolayan, muhafaza eden, değiştiren, yeniden düzenleyen, açıklayan, kullanılmasını engelleyen veya üçüncü kişilere aktaranlar 6 aydan 3 yıla kadar hapis cezası ile cezalandırılacak. Verileri silmeyen, yok etmeyen veya anonim (belirlenemez) hale getirmeyen sorumlulara da 6 aydan 1 yıla kadar para cezası verilecektir.

Kişisel verilerle ilgili bir diğer yasal düzenleme ise 24 Temmuz 2012 tarihinde resmi gazetede yayınlanan 28363 sayılı “Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik”dir.

Yönetmeliğin amacı “elektronik haberleşme sektöründe kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması için elektronik haberleşme sektöründe faaliyet gösteren işletmecilerin uyacakları usul ve esasları düzenlemektir. Haberleşmenin içeriğine ilişkin verilerin saklanması söz konusu yönetmeliğin kapsamına dahil değildir.

Amerika Birleşik Devletleri ve Almanya, kişisel verilerin korunmasına ilişkin hukuksal altyapının geliştirilmesi konusunda lider ülkeler konumunda bulunmaktadır. Günümüzde ABD, tüketici verilerini işleyerek para kazanan işletmelere karşı yeni yaptırımlar getirmeye hazırlanmaktadır. Amerikan Kongresi, tüketicilerden toplanan verilerin pazarlanması konusunu incelemektedir. İncelemeye alınan veri kolektörleri arasında özel yazılımlarla çevrimiçi ve mobil aktiviteleri takip edenler kadar çevrimdışı bilgi toplayanlar da yer almaktadır. Almanya ise 1990 yılında yürürlüğe giren “Federal Veri Koruması Yasası” ile 23 yıldır kişisel verilerin işlenmesi ve kullanılması konularını denetim altında tutmaktadır.

7. TÜRKİYE CUMHURİYETİ MEVZUATINDA GÜVENLİ İNTERNET

Türkiye Cumhuriyeti'nde İnternet ile ilgili konuları düzenleyen yasalar genel çerçevede, 5237 sayılı Türk Ceza Kanunu, 5846 sayılı Fikir ve Sanat Eserleri Kanunu ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dan oluşmaktadır.

7.1. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Ülkemizde İnternet içerik güvenliği konusunda yürürlüğe giren ilk ve tek kanun 04.05.2007 tarihinde yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında kanundur.

Kanunun 2. maddesine göre, içerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri ifade etmektedir. Aynı maddede erişim sağlayıcı ise kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler olarak tanımlanmıştır. İnternet sükjelerinin bu şekilde tanımlanmasının ardından Kanun 4. maddesinde, içerik sağlayıcının internet ortamında kullanıma sunduğu her türlü içerikten sorumlu olduğunu ifade etmiştir. Ancak Kanuna göre, içerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Kanunun 6. maddesinde ise erişim sağlayıcıların sorumluluk rejimi düzenlenmiştir. Buna göre erişim sağlayıcı, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, 5651 Sayılı Kanun hükümlerine uygun olarak haberdar edilmesi halinde ve teknik olarak engelleme imkanı bulunduğu ölçüde erişimi engellemekle yükümlüdür. Ancak Kanun burada doğru bir uygulamayla, erişim sağlayıcının, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü olmadığını da açıkça ortaya koymuştur.

Türkiye'de yetkili makamlar tarafından erişime engellenmesi kararı verilebileceği açıklıkla belirtilen yegane mevzuat (5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nun EK-4. maddesinde tanınan istisna haricinde) 5651 Sayılı Kanun'dur.

Yasanın 8. maddesi ve bu maddeye atıf yapan diğer mevzuat erişim engellemeyi kanuni kılmaktadır. Ancak internet siteleri hakkında erişim yasağı uygulaması, bu kanundan önce de vardı ve mahkemeler, tedbir amaçlı olarak bazı sitelere erişim yasağı getirmişlerdi. Erişim engelleme kararına konu olabilecek suçlar 5651 sayılı kanunun Kanun'un 8/1 ve bağlı yönetmeliğinin 15 de 12. maddelerinde sınırlı olarak katalog suçlar olarak sayılmıştır. Bu katalog suçlar esasen TCK'da yer alan intihara yönlendirme (madde 84), çocukların cinsel istismarı (madde 103/1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190), sağlık için tehlikeli madde temini (madde 194), müstehcenlik (madde 226), fuhuş (madde 227), kumar oynanması için yer ve imkan sağlama (madde 228) suçları ile 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlar olarak sayılmışlardır. Bu katalog suçlardan birine giren bir içeriğin bulunması halinde, içeriğin bulunduğu internet sitesine erişim Kanunda yazdığı şekliyle 'tedbiren' engellenmektedir.

7.1.1. 5651 Sayılı Yasa Hakkında Değişiklik Önerileri

5651 Sayılı Kanun'a ilişkin değişiklik önerisi metinleri ve bizzat İnternet Kurulu'nun değişiklik önerisine ilişkin bildirilen görüşler ile bu hususta detaylı şekilde hazırlanmış raporlar bulunmaktadır. İnternet Kurulu kamuoyundan bu anlamda değişiklik fikirlerini talep etmiş ve gönderilen bu öneri, eleştiri, fikir ve raporları da sitesinden kamuoyu ile paylaşmıştır.

22.12.2012 tarihi itibarıyla görüş göndermiş bulunan kurumlar arasında Türk Telekom, TTnet, Vodafone, Avea, Turkcell şirketleri ile birlikte İnternet Teknolojileri Derneği (İNETD), Türkiye Bilişim Sanayicileri Derneği (TÜBİSAD), Türkiye Bilişim Vakfı (TBV), Türk Sanayicileri ve İşadamları Derneği (TÜSİAD), Türkiye Bilişim Derneği Antalya Şubesi (TBD Antalya) Alternatif Bilişim Derneği, Medya Derneği, Elektrik Mühendisleri Odası (EMO) gibi sivil toplum kuruluşları ve Avrupa Birliği Bakanlığı da bulunmaktadır. Kurumlar dışında görüş bildiren kişiler olarak Av. Levent Berber & Av. Bedii Kaya, ELİG Hukuk Bürosu avukatları, Av. Ali Osman Özdilek & Av. Gökhan Ahi, Av. Başak Purut, Av. İlker Atamer gibi avukatların yanı sıra Yrd. Doç. Dr. Leyla Keser Berber (Bilgi Üniversitesi), Prof. Dr. Yaman Akdeniz (Bilgi Üniversitesi), Çığır İlbaş (Başkent Üniversitesi) ve Şeref Sağıroğlu'nun (Bilgi

Güvenliđi Derneđi) görüř ve öneri metinlerine İnternet Geliřtirme Kurulu'nun İnternet sitesinden ulaşılabilir [15].

8. TÜRKİYE’DE GÜVENLİ İNTERNET HİZMETİ

Güvenli İnternet Hizmeti, altyapısı erişim sağlayıcılar tarafından oluşturulan ücretsiz, talebe bağlı ve alternatif bir İnternet erişim hizmetidir.

Güvenli İnternet Hizmetine ilişkin çalışmalar, Anayasanın “Ailenin korunması ve çocuk hakları” başlıklı 41. Maddesi ve “Gençliğin korunması” kenar başlıklı 58. Maddesi hükümlerine dayanmaktadır. Ayrıca bu Anayasal hükümlerin yanında Elektronik Haberleşme Kanununun Tüketici ve Son Kullanıcı haklarını düzenleyen hükümleri ile bu kanun uyarınca çıkarılan Tüketici Hakları Yönetmeliği’nin “İnternetin Güvenli Kullanımı” başlıklı 10.maddesi de uygulamanın kapsamını belirlemiştir. Yönetmelik, İşletmecilere İnternetin Güvenli Kullanımına yönelik ücretsiz alternatif hizmeti sunma yükümlülüğü getirmiştir.

Bu hizmet kullanıcıların bireysel tercihlerine dayalı olarak talep etmeleri halinde alabilecekleri ve kullandıkları profiller arasında her an geçiş yapabilecekleri ve Güvenli İnternet Hizmeti dışına çıkabilecekleri bir işleyişi öngörmektedir.

Güvenli İnternet hizmetiyle aileler İnternet’in olumsuz içeriklerinden olan pornografik sitelerden, uyuşturucu ticareti yapan sitelerden, şiddet içeren sitelerden, ırkçılık ve nefret suçları üzerine yayın yapan sitelerden, suç işlemeyi anlatan sitelerden, terör propagandası yapan sitelerden talebe bağlı ve ücretsiz olarak korunma imkanına kavuşmaktadır.

Mevcut filtreleme hizmetlerinden faydalanamayan (kendi bilgisayar kullanma beceri düzeyleri vb. sebeplerle bu tür filtre programlarını kuramamış olan kullanıcılar) kullanıcıların kolayca kullanabileceği bir hizmettir. Çocuk veya Aile profilden birini tercih eden kullanıcı karşılaştığı sorunu yine kullanmakta olduğu profil ile ilgili olarak geri bildirimde bulunma ve bu çerçevede tedbir alınmasını talep etme hakkına sahip olmaktadır.

Güvenli İnternet Hizmeti süreci ile 5651 sayılı Kanun birbirinden bağımsız konulardır. 5651 sayılı Kanun gereği yapılan erişim engellemelerde herhangi bir değişiklik söz konusu değildir.

2012 yılı Mayıs ayı verilerine göre güvenli İnternet Hizmetini kullanan abone sayısı yaklaşık 1 milyon, bu aboneler arasında çocuk profilini kullananların oranı ise %14 olarak hesaplanmıştır [17].

8.1. Uluslararası Normlar Ve Güvenli İnternet Uygulamaları

Avrupa Konseyi Siber Suç Sözleşmesinin reşit olmayanlara ilişkin düzenlemesi, Avrupa Konseyinin Çocukların Cinsel Sömürü ve İstismara Karşı Korunmasına Yönelik 201 sayılı Sözleşmesinin ilgili hükümleri, Birleşmiş Milletler Çocuk Haklarına Dair Sözleşme'ye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokolün çocuk pornografisine ilişkin düzenlemeler güvenli internet hizmetinin temelindeki etik anlayışın temel çerçevesini oluşturmaktadır [18].

Dünyadaki İnternet içerik düzenlemelerine kıyasla Avrupa'da yapılan İnternet filtreleme, Avrupa'nın demokratik geleneği ve özgür ifade için verdiği mücadele göz önünde bulundurulduğunda dikkat çekici olmaktadır.

Filtreleme; devlet tarafından emredilen, ülke içerisinde barındırılan yasadışı içeriğin kaldırılması (uyar-kaldır), yurtdışında barındırılan içeriğe erişimin kısıtlanması, yasadışı içeriğe yönelik arama motorlarında sonuçların filtrelenmesi gibi çeşitli şekiller alabilmektedir. Birçok durumda, İnternet servis sağlayıcıları, arama motoru veya içerik sağlayıcı tarafından yapılan filtreleme “gönüllü” olarak adlandırılmakta ancak kamu otoritelerinin bu alanda yasama yapmaksızın oluşturdukları baskılar ile “zorunlu gönüllü” olarak sistem işletilmektedir.

Filtre edilen yasadışı içeriğin kapsamı genel olarak çocuk pornografisi, ırkçılık, nefreti ve terörü besleyen materyaller, telif hakları ve kumar sitelerinden oluşmaktadır. Bununla birlikte gerçek hayatta suç olan online ortamda da suç sayıldığından, başvurular üzerine mahkemelerce farklı konularda da filtreleme kararları alınabilmektedir.

AB düzeyinde, internet kullanımının izlenmesi konusunda İSS'lerin genel bir yükümlülükleri olmadığı gibi, yasadışı içeriğin sorumluluğundan da korunmaktadırlar. Ancak, kendilerine bu tür içerik bildirildiğinde filtreleme yapmak zorundadırlar. Bu nedenle, üye ülkelerdeki filtrelemenin derecesi, hükümetlerin, kolluk kuvvetlerinin, sivil toplum kuruluşlarının, yasadışı içeriği tanıma ve rapor etme yönündeki kamuoyu bilincine göre değişmektedir.

Geçen on beş yılda, AB düzeyinde internet düzenleme konusunda ortak politikalar ve uygulamalar ortaya koyma çalışmaları devam etmektedir. Bunlar bölgesel ticaretin ve rekabetin gelişmesi, internet suçlarının ve terörizm ile mücadelenin bir gereği olarak görülmüştür. Diğer taraftan, yasadışı içerik hususunda

İSS'lerin sorumluluğu ve verilerin korunması hususunda yükümlülükleri öne çıkmıştır.

Avrupa'da bölgesel düzenlemeye ilişkin yaklaşım ilk olarak, Avrupa Konseyinin, Komisyondan, 1 Nisan 1996 da "İnternetin hızlı gelişiminin neden olduğu problemlere ilişkin bir özet" istemesi ile başlamıştır.

Bu talebe Komisyon, "İnternette Yasadışı ve Zararlı İçerikler" başlıklı bir rapor ve "Görsel-işitsel hizmetlerde küçüklerin ve insan onurunun korunması" başlıklı Yeşil Kitap (Green Paper = Bilimsel Çalışma) ile cevap vermiştir. Bu belgelere dayanılarak, Ocak 1999 – Aralık 2002 arasında uygulamaya konulan "İnternetin Güvenli Kullanımının Desteklenmesi Harekat Planı" (Action Plan on Promoting Safe Use of the Internet)nda ifadesini bulan "AB düzeyinde İnternetin kendi kendine düzenlenmesi için ortak çatı" taslağı hazırlanmıştır. Safer Internet Action Plan, düzenleme gerektirmeyen inisiyatifleri destekleyerek gerçekleştirmeyi amaçlamaktadır.

Bu kapsamda hem endüstriyi hem de internet kullanıcılarını, uygun, öz denetim sistemlerini uygulamak noktasında cesaretlendirmek, teknik çözümleri hareketlendirmek, aileleri ve öğretmenleri internet üzerinden zararlı ve yasadışı içeriklerle ilgili bilgilendirmek ve deneyimleri paylaşmak hedeflenmektedir.

Bu hedefler için dört hareket noktası belirlenmiştir.

i) Daha emniyetli bir ortam oluşturmak

- Avrupa İhbar Merkezleri ağı oluşturmak (INHOPE).
- Gönüllü düzenleme ve Prensipl Kararlarını (Code of Conduct) teşvik etmek.

ii) Filtreleme ve izleme programlarını geliştirmek

- Filtreleme ve izlemenin faydalarını göstermek.
- İzleme programlarına dair uluslararası anlaşmaları kolaylaştırmak.

iii) Bilinçlendirme Aktivitelerini cesaretlendirmek

- Bilinçlendirme Aktiviteleri için yer sağlama
- Geniş çaplı Bilinçlendirme Aktivitelerini cesaretlendirme

iv) Destek faaliyetleri

- Yasal suçlara değer vermek.
- Benzer uluslararası inisiyatiflerle işbirliği yapmak.

Internet Action Plan ilk defa tasarlandığı 1999 yılından bu güne kadar yasadışı ve zararlı içerikten korunmayı yasal ve düzenleyici bir çerçeveye oturtmaya yönelik bir dizi girişimler ve gelişmeler yaşanmıştır. Avrupa Konseyinin daha sonraki kararları ile Güvenli İnternet Programları uzatılmış ve halihazırda 2009-2013 yıllarını kapsayan (A multi-annual Community programme on protecting children using the Internet and other communication Technologies: İnternet ve diğer İletişim Teknolojilerini Kullanan Çocukları Korumaya İlişkin Yıllara Sari Topluluk Programı) devam etmektedir.

Müstehcen içeriği düzenleme hareketi AB düzeyinden önce ülkeler düzeyinde ve İnternet Servis Sağlayıcılarca gönüllü uygulanacak filtre uygulamaları ile başlamıştır. Bunda en belirgin model, İngiltere'deki uygulama olmuştur. İngiltere'deki en büyük İSS olan BT, Haziran 2004 de İçişleri Bakanlığı ile işbirliği içerisinde "Cleanfeed" projesini uygulamaya koymuştur.

Projeye göre, BT, dünyanın her hangi bir yerinde barındırılan çocuk istismarı (1978 tarihli Çocukların Korunması Kanununda belirtildiği şekliyle) görüntüsü taşıyan internet içeriğini filtrelemektedir. Bu içerikler, bir sivil toplum örgütü olan İnternet Watch Foundation (IWF) tarafından bir liste halinde derlenmektedir. Üst düzey yöneticileri emekli polis teşkilatı mensuplarından oluşan ve bünyesinde hukukçu barındırmayan IWF, Sexual Offences Act 2003'de yer alan düzenlemeler ve İngiltere'deki 52 polis teşkilatı ile imzalamış oldukları iyi niyet anlaşmaları sayesinde, çocukların cinsel istismarına yönelik yayınları inceleyip işlem sürecini tetikleyebilmektedir. IWF tarafından oluşturulan kara liste, İSS'lere, Mobil operatörlere, içerik sağlayıcılara ve arama motorlarına verilmektedir. Bu içeriklere ulaşmak istenildiğinde bir hata mesajı ile karşılaşılmaktadır.

İngiltere dahilinde barındırılan içerik için ise, Uyar – Kaldır yöntemi ile erişim sağlayıcılardan ve içerik sağlayıcılardan kaldırılması istenmektedir.

Her ne kadar bu sistemin esası "gönüllü" ise de, İngiltere hükümeti tarafından 2007 yılının sonuna kadar bütün İSS'lerin benzer bir sistem uygulaması istenmiştir.

İsveç, Norveç, Danimarka, Finlandiya ve İtalya gibi diğer ülkelerde de benzer programlar uygulanmaktadır.

Eylül 2004'de, engelleme sistemi farklı bir türde gönüllü olarak Telenor İSS tarafından Norveç'te hayata geçirilmiştir. Kullanılan engelleme yöntemi de DNS zehirlenme olarak bilinen DNS kara listesidir. DNS kara listeyi kullanarak, belirli bir

web sayfasını veya site içerisindeki alt alan sayfalarını engellemek mümkün değildir. Sadece tüm site (domain) engellenebilir.

29 Ocak 2008 tarihinde Danimarkalı bir mahkeme tarafından Danimarkalı İSS'lere popüler bir İsveç tabanlı bir dosya paylaşım arama motoru sitesi olan Pirate Bay'a erişimi engelleme kararı gönderilmiştir.

Danimarka, İsveç, Finlandiya, Hollanda ve İsviçre gibi ülkelerde özellikle çocuk cinsel istismarı objelerine yönelik benzer tedbirler alınmış, bazı kara listeler hazırlanmış ve bazı ülkelerde DNS engelleme yoluna gidilmiştir.

İlk filtreleme çalışmaları çocuk pornosu gibi sınırlı alanlarda kalırken bu günlerde yetişkin pornografisi, online kumar, bahis, ırkçılık, kamu otoritelerine hakaret, saldırgan içerikler gibi alanlar için de filtreleme uygulamaları olduğu gözlenmektedir.

AB genelinde politik karşıtlık sebebiyle yapılmış olan bir filtreleme söz konusu olmamakla birlikte ulusal kimliği ve resmi kurumların saygınlığını korumaya yönelik filtrelemelere de rastlanılmaktadır. 2002 yılında İsveç'te, İsveç Mahkemelerini şiddetle eleştiren ABD'de barındırılan 3 adet web sitesine erişimin engellenmesi istenmiş, tepki gösteren İSS yetkilileri hakkında yasal soruşturma başlatılmıştır.

Avrupa ülkeleri, offline politikalarını internete de uyarlayarak nefret ifadelerine karşı harekete geçmişlerdir. Örneğin 2000 yılında Fransa'da, iki Anti Semitist STK tarafından Mahkemeye taşınan bir davada, Mahkeme Yahoo'yu, Nazi hatıraları da ihtiva eden bir açık artırma sitesine erişim sağladığı için sorumlu tutmuş, ya bu siteye Fransa'dan imkansız kılması veya ceza ile karşı karşıya kalacağını bildirmiştir. Yahoo, davayı, Fransız yargı kararlarının ABD'de geçersiz olduğu iddiasıyla ABD bölge mahkemesine taşımış, mahkeme 2001 Kasımında Yahoo lehinde karar vermiş, devam eden süreçte Ocak 2006 da dava düşmüştür.

Benzer şekilde, yine Aralık 2000'de, Alman Federal Mahkemesi, Nazileri öven ve Holokostu inkâr eden bir materyalin nerede barındırıldığına bakılmaksızın Alman kanunlarına göre sansür edilmesi gerektiğine karar vermiş, 2002 yılında 78 İSS'ye Neo-Nazi içerik taşıyan iki yabancı sitenin yayınlarının durdurulması talimatı verilmiştir.

Diğer Avrupa ülkelerinde de Holokostu reddeden veya ırksal nefreti besleyen materyalleri yasaklayan mevzuat bulunmakta olup bu mevzuat, Avrupa Konseyi'nin Siber Suç Sözleşmesi ile senkronize edilmiştir. Bu duruma göre, Yasadışı içerik söz konusu olduğunda, uyarı verilmesi durumunda, sitenin yurt içi veya dışında

barındırıldığına göre, İSS’ler ya ilgili web sitesinden içeriği kaldıracak ya da siteyi bloke edeceklerdir.

AB üyesi ülkeler, internet ve diğer elektronik ağlar üzerinden medya veya diğer yayınlar tarafından yapılacak hakaret veya iftira durumunda uygulanacak basitleştirilmiş bir çatinın gerekliliğini ifade etmektedirler. Bu gereklilik Şubat 2007 de Avrupa Parlamentosunda tekrar ifade edilmiştir.

Ülkeler düzeyinde ise, özellikle İngiltere’de, Hakaret yasaların bir web sitesi kaldırma kültürü oluşturduğu yönünde eleştirilere sebep olmaktadır.

Pek çok Avrupa ülkesi, Telif hakları ihlallerin karşı, ABD’de uygulanan “Uyar – Kaldır” yöntemine benzer internet filtreleme yöntemleri kullanmaktadır. Avrupa’da telif hakları ihlallerine karşı İSS, arama motorları temsilcilerinin sorumlu tutularak gözaltına alındığı, para cezasına çarptırıldığı veya sitelerinin kapatıldığı birçok örnek bulunmaktadır.

Bölgesel olarak ise, internet içerikleri ve Fikri haklar konusunda iki direktif göze çarpmaktadır. Bu direktifler 9 Nisan 2001’de kabul edilmiş olan “Bilgi Toplumunda Telif Hakları ve İlgili Haklar” ve 8 Haziran 2000’de kabul edilmiş olan “2000/31/EC sayılı Elektronik Ticaret Direktifi”dir. Yasama konusunda ortak bir platform oluşturma çabaları, üye ülkelerin kültürel yapılarına ve mevcut mevzuatına verilen önemden ötürü yavaş ve karışık bir yol izlemektedir.

Yasama dışında, İngiltere örneğinde olduğu gibi Hükümetler tarafından İnternet Servis Sağlayıcılarına, çocukların yasadışı ve zararlı içeriklerden korunmaları için çalışmalar yapmaları ve bu konuda filtreleme seçenekleri geliştirmeleri yönünde teklif ve talimatlar verilmektedir.

Avrupa dışındaki ülkelere Avusturalya’da 31 Mart 2010 tarihi itibariyle, İSS’ler web sayfalarına erişimin engellenmesinde filtreleme sunucu düzeyini uygulamak için kanun veya başka bir yonteme bağı kalmadan gerçekleştirmeye başlamışlardır. Bu İSS’lerden bazıları bu filtreleme işlemini birkaç yıldır gönüllü olarak uygulamaktadır.

Bütün bu uygulamalara rağmen 2007 Kasım ayında seçilen Avustralya Federal İşçi Hükümeti yapılanları yetersiz bulmuştur. Bu konuda hükümet, sunucu tabanlı filtreleme sistemi ile bir devlet kurumu tarafından hazırlanacak bir kara liste ile erişim engellenmesi yolunu tüm İSS’lere uygulatma konusunda bir plan oluşturmaktadır.

Kanada’da ise 23 Kasım 2006’da sekiz İSS online çocuk cinsel istismarına karşı yeni bir gönüllü girişim başlattı. Bu tarihlerde engellenen site sayısının 500-800

arasında olduđu bildirildi. Eriřim engellemeleri herhangi bir yasal zorunluluk olmamakla beraber tamamen İSS lerin gönüllük esasına dayanmaktadır.

9. ANKET ÇALIŞMASI

Güvenli İnternet konusu için çalışma alanı olarak Üniversite öğrencileri, Telekomünikasyon ve İnternet konusunda faaliyet gösteren sivil toplum kuruluşları olan TEDER, TBP ve TÜTED çalışanları ile telekomünikasyon sektörü mühendis ve çalışanlarından oluşan bir örneklem seçilmiştir. Anket ayrıca sosyal ağlar üzerinde de paylaşılmıştır.

Anket beş bölümden oluşmaktadır;

- i) Demografik bilgiler.
- ii) Teknoloji, bilgisayar ve İnternet konularına yönelik ilginin ölçülmesi ve beraberinde katılımcının İnternet kullanım profilinin belirlenmesi
- iii) İnternet'in özgürlüğü konusundaki görüş ve düşünceler, güvenli İnternet hizmeti kullanımına ilişkin sorular.
- iv) İnternet güvenliğiyle ilgili kavram ve kurallardan oluşan beşli likert ölçeğindeki sorular.
- v) Güvenli İnternet kavramının katılımcılar için ne anlama geldiğini yazabilecekleri metin kutusu.

9.1. Anketin Pilot Çalışması

Anket soruları taslak olarak hazırlandıktan sonra, Bilgisayar Bilimleri Bölümü öğretim üyeleri, Bilişim Hukuku alanında çalışan avukatlar, Türkiye Barolar Birliği Bilişim Hukuku Sertifika eğitimi veren öğretim elemanları ve avukatlar tarafından incelenmiş ve önerileri doğrultusunda yeni eklemeler ya da açıklamalar yapılarak ankete son hali verilmiştir.

Araştırmada örneklem birimi sivil toplum kuruluşu çalışanları olarak alınmış ve tabakalı örnekleme yöntemi kullanılarak örneklem büyüklüğü belirlenmeye çalışılmıştır.

Anket 415 katılımcı tarafından doldurulmuş ancak anketlerin geçersiz sayılacak düzeyde doldurması sonucunda, anketi tamamlayan 264 katılımcı olmuştur. Dolayısıyla bu araştırmada anketin cevaplanma oranı %63,61'dir.

Anket sorularına verilen yanıtların frekans dağılımları oluşturulmuş, değişkenler arasındaki ilişkileri görebilmek için çapraz tablo ve ki-kare testi analiz yöntemleri uygulanmıştır.

9.2.Frekans Dağılımları

Tablo 9.1: Katılımcıların Cinsiyet Dağılımı.

Cinsiyet	Frekans	Yüzde	Kümülatif Yüzde
Erkek	165	62,5	62,5
Kadın	99	37,5	100,0
TOPLAM	264	100,0	

Katılımcıların %62.5’lik oranı erkek; %37.5’lik oranı kadınlardan oluşmaktadır.

Tablo 9.2: Katılımcıların Doğum Yerleri.

Doğum Yeri	Frekans	Yüzde	Kümülatif Yüzde
ADANA	4	1,5	1,5
ADİYAMAN	1	,4	1,9
AFYONKARAHİSAR	3	1,1	3,0
AĞRI	1	,4	3,4
AKSARAY	1	,4	3,8
AMASYA	2	,8	4,5
ANKARA	72	27,3	31,8
ANTALYA	1	,4	32,2
ARDAHAN	1	,4	32,6
ARTVİN	2	,8	33,3
AYDIN	2	,8	34,1
BİLECİK	1	,4	34,5
BURSA	5	1,9	36,4
ÇANAKKALE	1	,4	36,7
ÇANKIRI	1	,4	37,1
ÇORUM	6	2,3	39,4
DENİZLİ	4	1,5	40,9
DİYARBAKIR	1	,4	41,3
EDİRNE	1	,4	41,7
ELAZIĞ	1	,4	42,0
ERZİNCAN	2	,8	42,8
ERZURUM	4	1,5	44,3
ESKİŞEHİR	4	1,5	45,8
GAZİANTEP	2	,8	46,6
GİRESUN	1	,4	47,0
HATAY	1	,4	47,3

Tablo 9.2: Devam.

İĞDIR	1	,4	47,7
ISPARTA	1	,4	48,1
İSTANBUL	58	22,0	70,1
İZMİR	11	4,2	74,2
KAHRAMANMARAŞ	2	,8	75,0
KARS	1	,4	75,4
KAYSERİ	6	2,3	77,7
KIRKLARELİ	1	,4	78,0
KIRŞEHİR	1	,4	78,4
KOCAELİ	2	,8	79,2
KONYA	6	2,3	81,4
KÜTAHYA	1	,4	81,8
MALATYA	3	1,1	83,0
MANİSA	1	,4	83,3
MARDİN	2	,8	84,1
MERSİN	2	,8	84,8
MUĞLA	2	,8	85,6
MUŞ	1	,4	86,0
NEVŞEHİR	2	,8	86,7
NİĞDE	1	,4	87,1
ORDU	2	,8	87,9
OSMANİYE	2	,8	88,6
SAKARYA	2	,8	89,4
SAMSUN	10	3,8	93,2
SİVAS	1	,4	93,6
ŞIRNAK	1	,4	93,9
TEKİRDAĞ	1	,4	94,3

Tablo 9.2: Devam.

TOKAT	2	,8	95,1
TRABZON	8	3,0	98,1
ŞANLIURFA	1	,4	98,5
VAN	1	,4	98,9
ZONGULDAK	2	,8	99,6
YURTDIŞI	1	,4	100,0
TOPLAM	264	100,0	

Toplam 264 katılımcının %27,3 oranındaki bölümü Ankara doğumludur. 1 katılımcı yurt dışı doğumlu olduğunu belirtmiştir.

Tablo 9.3: Katılımcıların Doğum Yılları.

	Frekans	Yüzde	Kümülatif Yüzde
1944	1	,4	,4
1950	1	,4	,8
1952	1	,4	1,1
1955	1	,4	1,5
1956	2	,8	2,3
1958	3	1,1	3,4
1960	1	,4	3,8
1961	5	1,9	5,7
1963	2	,8	6,4
1964	2	,8	7,2
1965	5	1,9	9,1
1966	1	,4	9,5
1967	6	2,3	11,7
1968	2	,8	12,5
1969	4	1,5	14,0
1970	1	,4	14,4
1971	6	2,3	16,7
1972	5	1,9	18,6
1973	6	2,3	20,8
1974	7	2,7	23,5
1975	6	2,3	25,8
1976	6	2,3	28,0
1977	10	3,8	31,8
1978	5	1,9	33,7
1979	7	2,7	36,4
1980	6	2,3	38,6

Tablo 9.3: Devam.

1981	7	2,7	41,3
1982	17	6,4	47,7
1983	12	4,5	52,3
1984	10	3,8	56,1
1985	13	4,9	61,0
1986	13	4,9	65,9
1987	13	4,9	70,8
1988	17	6,4	77,3
1989	13	4,9	82,2
1990	15	5,7	87,9
1991	15	5,7	93,6
1992	13	4,9	98,5
1993	4	1,5	100,0
TOPLAM	264	100,0	

Katılımcıların ortalama yaşı 33 olarak hesaplanmıştır. En genç katılımcının 20 en yaşlı katılımcının ise 69 yaşında olduğu tespit edilmiştir.

Tablo 9.4: Katılımcıların Eğitim Durumları.

	Frekans	Yüzde	Kümülatif Yüzde
Lise	19	7,2	7,2
Üniversite / Y.Okul	165	62,5	69,7
Y.Lisans	66	25,0	94,7
Doktora	14	5,3	100,0
TOPLAM	264	100,0	

Katılımcıların eğitim durumları en yüksek %62,5 oranı ile Üniversite ve Yüksek okul, en düşük %5,3 ile Doktora seviyesinde bulunmaktadır.

Tablo 9.5: Katılımcıların Meslekleri.

	Frekans	Yüzde	Kümülatif Yüzde
Öğrenci	61	18,1	23,1
Öğretim Üyesi / Görevlisi	16	6,1	29,2
Uzman	29	26,0	40,2
Avukat	18	6,8	47,0
Tıp doktoru	2	,8	47,7
Girişimci / İşyeri sahibi	16	6,1	53,8
Memur / Ücretli çalışan	53	20,1	73,9
Serbest meslek	9	3,4	77,3
Sanatçı	2	,8	78,0
Diğer	58	12,0	100,0
TOPLAM	264	100,0	

Katılımcılar mesleklerine göre incelendiğinde en büyük oran %26 ile uzmanlar; en düşük oran ise %0,8 ile sanatçılar ve tıp doktorlarından oluşmaktadır.

Tablo 9.6: Katılımcıların Medeni Durumları.

	Frekans	Yüzde	Kümülatif Yüzde
Bekar	144	54,5	54,5
Evli	115	43,6	98,1
Ayrılmış / Dul	5	1,9	100,0
TOPLAM	264	100,0	

Katılımcılar %54,5 oranı ile evli, %43,6 oranı ile bekar ve %1,9 oranı ile ayrılmış veya dul bireylerden oluşmaktadır.

Tablo 9.7: Çocuk Sahibi Katılımcılar.

	Frekans	Yüzde	Kümülatif Yüzde
Yok	179	67,8	67,8
Var	85	32,2	100,0
TOPLAM	264	100,0	

Tablo 9.8: Katılımcıların Gelir Seviyeleri.

	Frekans	Yüzde	Kümülatif Yüzde
1.000 TL veya altı	47	17,8	17,8
1.001 - 3.000 TL	97	36,7	54,5
3.001 - 5.000 TL	59	22,3	76,9
5.001 - 10.000 TL	38	14,4	91,3
10.000 TL veya üzeri	23	8,7	100,0
TOPLAM	264	100,0	

Katılımcılar gelir seviyelerine göre %36,7 oranda 1001 – 3000 TL aylık gelir elde eden bireylerden oluşmaktadır. Katılımcıların %8,7 oranındakileri 10.000 TL ve üzeri aylık gelire sahip olduklarını belirtmiştir.

Tablo 9.9: Katılımcıların İnternet Kullanıcısı Oldukları Süreler.

	Frekans	Yüzde	Kümülatif Yüzde
2 - 5 yıldır İnternet kullanıcısıyım.	11	4,2	4,2
6 - 9 yıldır İnternet kullanıcısıyım.	60	22,7	26,9
10 yıldan uzun süredir İnternet kullanıyorum.	193	73,1	100,0
TOPLAM	264	100,0	

Katılımcıların %73.1'lik bölümü 10 yıl ve daha uzun süreler İnternet kullanıcısı olduklarını belirtmiştir. 2-5 yıldır İnternet kullanıcısı olan katılımcıların oranı %4.2 olarak tespit edilmiştir.

Tablo 9.10: Katılımcıların İnternet Kullanım Amaçları

Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (Facebook)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	44	16,7	16,7
Nadiren	33	12,5	29,2
Ortalama	45	17,0	46,2
Sık	45	17,0	63,3
Çok Sık	97	36,7	100,0
TOPLAM	264	100,0	
Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (Google+)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	64	24,2	24,2
Nadiren	48	18,2	42,4
Ortalama	25	9,5	51,9
Sık	25	9,5	61,4
Çok Sık	102	38,6	100,0
TOPLAM	264	100,0	

Tablo 9.10: Devam.

Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (Linkedin)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	114	43,2	43,2
Nadiren	59	22,3	65,5
Ortalama	44	16,7	82,2
Sık	26	9,8	92,0
Çok Sık	21	8,0	100,0
TOPLAM	264	100,0	
Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (Twitter)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	83	31,4	31,4
Nadiren	41	15,5	47,0
Ortalama	35	13,3	60,2
Sık	44	16,7	76,9
Çok Sık	61	23,1	100,0
TOPLAM	264	100,0	
Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (Forumlar)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	47	17,8	17,8
Nadiren	89	33,7	51,5
Ortalama	66	25,0	76,5
Sık	35	13,3	89,8
Çok Sık	27	10,2	100,0
TOPLAM	264	100,0	

Tablo 9.10: Devam.

Aşağıdaki uygulamaları ne sıklıkla kullanıyorsunuz? (E-posta grupları)			
	Frekans	Yüzde	Kümülatif Yüzde
Hiçbir Zaman	43	16,3	16,3
Nadiren	56	21,2	37,5
Ortalama	53	20,1	57,6
Sık	52	19,7	77,3
Çok Sık	60	22,7	100,0
TOPLAM	264	100,0	

Tablo 9.11: Katılımcıların İnternet’e Eriştikleri Ortamlar.

İnternete hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)1					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Ev	249	94,3	100,0	100,0
Boş		15	5,7		
TOPLAM		264	100,0		
İnternete hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)2					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	İşyeri / Okul	231	87,5	100,0	100,0
Boş		33	12,5		
TOPLAM		264	100,0		

Tablo 9.11: Devam.

İnternete hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)3					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	İnternet evleri (İnternet cafeler)	20	7,6	100,0	100,0
Boş		244	92,4		
TOPLAM		264	100,0		
İnternete hangi ortamlardan bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)4					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Ortak erişim alanları (Kafeterya, havaalanı terminal)	141	53,4	100,0	100,0
Boş		123	46,6		
TOPLAM		264	100,0		

Katılımcıların %94.3'lük oranı İnternete evden; %87.5'lik oranı işyeri ve okullardan, %7.6'lık oranı İnternet evlerinden, %53.4'lük oranı ise Ortak erişim alanlarından İnternete bağlandıklarını ifade etmiştir.

9.3.Analizler

Tablo 9.12: Katılımcıların İnternet’i Kullanım Amaçları.

İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)1					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	İşimle / derslerimle ilgili konularda araştırma	235	89,0	100,0	100,0
Boş		29	11,0		
TOPLAM		264	100,0		
İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)2					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Kişisel olarak ilgi duyduğum konularda araştırma	249	94,3	100,0	100,0
Boş		15	5,7		
TOPLAM		264	100,0		
İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)3					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Haber ve güncel gelişmeleri takip etme	243	92,0	100,0	100,0
Boş		21	8,0		
TOPLAM		264	100,0		

Tablo 9.12: Devam.

İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)4					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	İletişim	229	86,7	100,0	100,0
Boş		35	13,3		
TOPLAM		264	100,0		
İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)5					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Sosyal çevre edinme	90	34,1	100,0	100,0
Boş		174	65,9		
TOPLAM		264	100,0		
İnterneti hangi amaçlar için kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)6					
		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Oyun ve eğlence	123	46,6	100,0	100,0
Boş		141	53,4		
TOPLAM		264	100,0		

Katılımcıların %89'luk bölümü İnterneti iş ve derslerle ilgili konularda araştırma yapmak için; %94.3'lük bölümü kişisel konularda araştırma yapmak için; %92'lik bölümü haber takibi için; %86.7'si iletişim amacıyla %34.1'lik bölümü sosyal çevre edinmek için ve %46.6'lık bölümü ise oyun ve eğlence amacıyla kullandıklarını belirtmiştir.

Tablo 9.13: Katılımcıların Güncel Gelişmeleri Takip Etme Durumu.

Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?						
		Konulara ilgi duymuyorum ve gelişmeleri takip etmiyorum.	Konulara ilgi duymuyorum fakat gelişmeleri yazılı ve görsel basından takip ediyorum	Konulara ilgi duyuyorum fakat gelişmeleri takip etmiyorum.	Konulara ilgi duyuyorum ve gelişmeleri yakından takip ediyorum	TOPLAM
Erkek	Frekans	10	15	34	106	165
	Yüzde	6,1%	9,1%	20,6%	64,2%	100,0%
Kadın	Frekans	4	14	32	49	99
	Yüzde	4,0%	14,1%	32,3%	49,5%	100,0%
TOPLAM	Frekans	14	29	66	155	264
	Yüzde	5,3%	11,0%	25,0%	58,7%	100,0%

Erkek katılımcıların %64.2'lik bölümü teknoloji, bilgisayar ve internet konularına ilgi duyup gelişmeleri yakından takip ettiklerini belirtmiştir. Bu oran kadın katılımcılarda %49.5 olarak hesaplanmıştır.

Tablo 9.13: Devam.

Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?						
		Konulara ilgi duymuyorum ve gelişmeleri takip etmiyorum.	Konulara ilgi duymuyorum fakat gelişmeleri yazılı ve görsel basından takip ediyorum	Konulara ilgi duyuyorum fakat gelişmeleri takip etmiyorum.	Konulara ilgi duyuyorum ve gelişmeleri yakından takip ediyorum	TOPLAM
Lise	Frekans	2	3	6	8	19
	Yüzde	10,5%	15,8%	31,6%	42,1%	100,0%
Üniversite / Y.Okul	Frekans	12	18	46	89	165
	Yüzde	7,3%	10,9%	27,9%	53,9%	100,0%
Y.Lisans	Frekans	0	8	11	47	66
	Yüzde	,0%	12,1%	16,7%	71,2%	100,0%
Doktora	Frekans	0	0	3	11	14
	Yüzde	,0%	,0%	21,4%	78,6%	100,0%
TOPLAM	Frekans	14	29	66	155	264
	Yüzde	5,3%	11,0%	25,0%	58,7%	100,0%

Teknoloji, bilgisayar ve internet konularına ilgi duyup gelişmeleri yakından takip etme konusunda sırasıyla doktora eğitimine sahip katılımcıların %78.6 lık oranı, Yüksek lisans eğitilmiş katılımcıların %71.2 lik oranı, üniversite eğitimine sahip katılımcıların %53.9 luk oranı ve lise mezunu katılımcıların %42.1 lik oranı dikkat çekmektedir. Eğitim seviyesi ile teknoloji konularına ilgi konusunda doğru orantı olduğunu söylemek mümkündür.

Benzer bir orantı katılımcıların gelir seviyesinde de tespit edilmiştir. Bu tespiti göre teknolojiye yönelik ilgi ve gelişmeleri takip etme davranışı;

- i) 1000 TL ve altı gelir grubunda %40.4
- ii) 1.001-3.000 TL gelir grubunda %49.5
- iii) 3.001-5.000 TL gelir grubunda %67.8
- iv) 5.001-10.000 TL gelir grubunda %76.3
- v) 10.000 TL ve üzeri gelir grubunda ise %82.6

olarak hesaplanmıştır.

Tablo 9.13: Devam.

Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?						
		Konulara ilgi duymuyorum ve gelişmeleri takip etmiyorum.	ilgi duymuyorum gelişmeleri yazılı ve görsel basından takip ediyorum	Konulara ilgi duymuyorum fakat gelişmeleri takip etmiyorum.	ilgi duyuyorum ve gelişmeleri yakından takip ediyorum	TOPLAM
Bekar	Frekans	8	18	43	75	144
	Yüzde	5,6%	12,5%	29,9%	52,1%	100,0%
Evli	Frekans	5	11	22	77	115
	Yüzde	4,3%	9,6%	19,1%	67,0%	100,0%
Ayrılmış / Dul	Frekans	1	0	1	3	5
	Yüzde	20,0%	,0%	20,0%	60,0%	100,0%
TOPLAM	Frekans	14	29	66	155	264
	Yüzde	5,3%	11,0%	25,0%	58,7%	100,0%
Teknoloji, Bilgisayar ve İnternet konularına ilgili misiniz? Bu konularla ilgili güncel gelişmeleri takip ediyor musunuz?						
		ilgi duymuyorum ve gelişmeleri takip etmiyorum.	ilgi duymuyorum gelişmeleri yazılı ve görsel basından takip ediyorum	İlgi duyuyorum fakat gelişmeleri takip etmiyorum.	İlgi duyuyorum ve gelişmeleri yakından takip ediyorum	TOPLAM
1.000 TL veya altı	Frekans	3	4	21	19	47
	Yüzde	6,4%	8,5%	44,7%	40,4%	100,0%

Tablo 9.13: Devam.

1.001 - 3.000 TL	Frekans	6	11	32	48	97
	Yüzde	6,2%	11,3%	33,0%	49,5%	100,0%
3.001 - 5.000 TL	Frekans	3	8	8	40	59
	Yüzde	5,1%	13,6%	13,6%	67,8%	100,0%
5.001 - 10.000 TL	Frekans	2	3	4	29	38
	Yüzde	5,3%	7,9%	10,5%	76,3%	100,0%
10.000 TL veya üzeri	Frekans	0	3	1	19	23
	Yüzde	,0%	13,0%	4,3%	82,6%	100,0%
TOPLAM	Frekans	14	29	66	155	264
	Yüzde	5,3%	11,0%	25,0%	58,7%	100,0%

Tablo 9.14: Akıllı Cep Telefonu Kullanımı.

Akıllı cep telefonu kullanıyor musunuz?			
	Frekans	Yüzde	Kümülatif Yüzde
Evet	228	86,4	86,4
Hayır	36	13,6	100,0
TOPLA M	264	100,0	

Katılımcıların %86.4'lük bölümü akıllı cep telefonu kullandıklarını ifade etmiştir.

Tablo 9.15: Antivirüs Yazılım Kullanımı.

Cep Telefonunuzda Antivirüs Kullanıyor musunuz?			
	Frekans	Yüzde	Kümülatif Yüzde
Evet	51	19,3	19,3
Hayır	213	80,7	100,0
TOPLAM	264	100,0	

Katılımcıların %80.7'lik bölümü cep telefonlarında antivirüs yazılımı kullanmadıklarını ifade etmiştir.

Tablo 9.16: İnternet Dolandırıcılığı.

Siz veya bir yakınınız İnternet yoluyla dolandırıcılığa maruz kaldı mı?			
	Frekans	Yüzde	Kümülatif Yüzde
Evet	59	22,3	22,3
Hayır	205	77,7	100,0
TOPLAM	264	100,0	

Katılımcıların %22.3'lük kesimi kendilerinin veya yakınlarının İnternet dolandırıcılığı maruz kaldıklarını belirtmiştir.

Tablo 9.17: İnternet ve Özgürlük.

Sizce İnternet tamamen özgür bir ortam mı olmalıdır?			
	Frekans	Yüzde	Kümülatif Yüzde
Evet	130	49,2	49,2
Hayır	134	50,8	100,0
TOPLAM	264	100,0	

Katılımcıların %49.2’lik bölümü İnternetin tamamen özgür bir ortam olması gerektiğini; %50.8’lik bölümü ise tamamen özgür olmaması gerektiğini ifade etmiştir.

Tablo 9.18: Güvenli İnternet Hizmeti.

Güvenli internet hizmeti (çocuk ve aile profili) kullanıyor musunuz?				
	Frekans	Yüzde		Kümülatif Yüzde
Evet	61	23,1		23,1
Hayır	203	76,9		100,0
TOPLAM	264	100,0		
Güvenli internet hizmeti (çocuk ve aile profili) kullanıyor musunuz?				
		Evet	Hayır	TOPLAM
Erkek	Frekans	45	120	165
	Yüzde	27,3%	72,7%	100,0%
Kadın	Frekans	16	83	99
	Yüzde	16,2%	83,8%	100,0%
TOPLAM	Frekans	61	203	264
	Yüzde	23,1%	76,9%	100,0%
Güvenli internet hizmeti (çocuk ve aile profili) kullanıyor musunuz?				
		Evet	Hayır	TOPLAM
Çocuksuz	Frekans	24	155	179
	Yüzde	13,4%	86,6%	100,0%
Çocuklu	Frekans	37	48	85
	Yüzde	43,5%	56,5%	100,0%
TOPLAM	Frekans	61	203	264
	Yüzde	23,1%	76,9%	100,0%

Katılımcıların %23.1'lik oranı Güvenli İnternet Hizmeti kullandıklarını ifade etmiştir. Bu oran erkek katılımcılarda %27.3 ve kadın kullanıcılar da %16.2 olarak hesaplanmıştır. Aynı oran çocuklu katılımcılarda %43.5 ve çocuksuz kullanıcılar da %13.4 olarak karşımıza çıkmaktadır. Güvenli İnternet Hizmeti kullanımının çocuklu ailelerde daha yaygın olduğunu söylemek mümkündür.

Tablo 9.19: Çapraz Tablo Analizleri Cinsiyet

Cinsiyet * Sizce İnternet tamamen özgür bir ortam mı olmalıdır?				
		Evet	Hayır	TOPLAM
Erkek	Frekans	84	81	165
	Yüzde	50,9%	49,1%	100,0%
Kadın	Frekans	46	53	99
	Yüzde	46,5%	53,5%	100,0%
TOPLAM	Frekans	130	134	264
	Yüzde	49,2%	50,8%	100,0%

İnternetin tamamen özgür olması konusunda görüş bildiren erkek katılımcıların oranı %50.9 kadın katılımcıların oranı ise %46.5 olarak hesaplanmıştır. Tamamen özgür İnternet görüşünü savunanların örneklem içerisindeki oranı ise %49.2 olarak karşımıza çıkmaktadır.

Tablo 9.20: Çapraz Tablo Analizleri Çocuk bilgisi

Çocuğunuz var mı? * Sizce İnternet tamamen özgür bir ortam mı olmalıdır?				
		Evet	Hayır	TOPLAM
Hayır	Frekans	98	81	179
	Yüzde	54,7%	45,3%	100,0%
Evet	Frekans	32	53	85
	Yüzde	37,6%	62,4%	100,0%
TOPLAM	Frekans	130	134	264
	Yüzde	49,2%	50,8%	100,0%

İnternetin tamamen özgür olması konusunda çocuklu bireylerin %62.4'lük kesimi "hayır" yanıtını verirken aynı yanıtı veren çocuksuz katılımcıların oranı %45.3 ve örneklem genelindeki "hayır" yanıtının oranı %50.8 olarak hesaplanmıştır.

Tablo 9.21: Anket Soruları Karşılaştırmalı Analizler.

	KK +	%	K+	%	E D	%	K-	%	K K-	%
Antivirüs yazılımları bilgisayarları bütün tehlikelerden korur.	13	4,9	67	25,4	89	33,7	65	24,6	30	11,4
Lisanslı yazılımlarla lisansı kırılmış yazılımlar eşit derecede güvenlidir.	14	5,3	40	15,2	92	34,8	76	28,8	42	15,9
İnternette işlenen suçların failleri genellikle tespit edilemez.	5	1,9	58	22,0	51	19,3	112	42,4	38	14,4
İnternet aboneliğini başkasıyla paylaşmak tehlikelidir.	124	47,0	99	37,5	19	7,2	17	6,4	5	1,9
Şifresiz erişilen kablosuz ağlardan İnternete bağlanmak tehlikelidir.	90	34,1	86	32,6	52	19,7	27	10,2	9	3,4
İnternet siteleri aracılığıyla kumar oynamak suçtur	77	29,2	50	18,9	60	22,7	46	17,4	31	11,7

Tablo 9.21: Devam.

Pornografik fotoğraf ve videolar bulundurmak suçtur.	64	24,2	30	11,4	65	24,6	63	23,9	42	15,9
Sosyal medya platformlarını 13 yaşından küçük çocukların kullanmaması gerekmektedir.	107	40,5	72	27,3	48	18,2	18	6,8	19	7,2
İnternette içerik filtrelemesi aboneler tarafından uygulanmalıdır	96	36,4	76	28,8	31	11,7	32	12,1	29	11,0
İnternet sitelerine erişim engelleme tedbir kararları uygulamadan kalkmalıdır.	67	25,4	56	21,2	51	19,3	42	15,9	48	18,2
İnternet bankacılığı dolandırıcılık olaylarında bütün sorumluluk bankalara aittir.	66	25,0	50	18,9	72	27,3	57	21,6	19	7,2
Tahmin edilmesi zor şifreler tam anlamıyla güvenlidir.	17	6,4	41	15,5	85	32,2	79	29,9	42	15,9
Güvenli İnternet hizmeti bilgisayarı tehditlerden korur.	41	15,5	74	28,0	78	29,5	46	17,4	25	9,5

Tablo 9.21: Devam.

	KK +	%	K+	%	E D	%	K-	%	K K-	%
Güvenli İnternet hizmeti temiz bir İnternet içeriği sağlar.	47	17,8	89	33,7	74	28,0	30	11,4	24	9,1
Gelişmiş ülkelerde İnternet sitelerine erişim engellenmez.	58	22,0	59	22,3	72	27,3	45	17,0	30	11,4
Her ülkede İnternet içeriğini denetleyen kurumlar olmalıdır.	90	34,1	96	36,4	33	12,5	19	7,2	26	9,8
İnternet üzerinden işlenen suçlar özel kanunlarla düzenlenmelidir.	152	57,6	89	33,7	12	4,5	5	1,9	6	2,3
İnternet bankacılığı dolandırıcılık olaylarında bütün sorumluluk kullanıcılara aittir.	7	2,7	13	4,9	71	26,9	112	42,4	61	23,1
Spam (yığın) e-postalar çözülmesi gereken önemli bir sorundur.	135	51,1	91	34,5	27	10,2	6	2,3	5	1,9
Tanımadığım kişi ve firmalardan gelen e-posta ve sms mesajlarından rahatsız oluyorum.	165	62,5	76	28,8	11	4,2	6	2,3	6	2,3

Tablo 9.21: Devam.

Güvenli İnternet hizmeti temiz bir İnternet içeriği sağlayamaz	38	14,4	51	19,3	67	25,4	77	29,2	31	11,7
İnternette kullanıcılar genellikle kendi kimliklerini saklarlar	39	14,8	111	42,0	83	31,4	29	11,0	2	0,8
(KK+ : Kesinlikle Katılıyorum. K+:Katılıyorum. ED: Emin Değilim. K-: Katılmıyorum. KK-: Kesinlikle Katılmıyorum)										

Antivirüs yazılımlarının bilgisayarları bütün tehlikelerden koruması konusunda katılımcıların %33.7'si emin olmadığını ifade etmiştir. Benzer biçimde lisanslı yazılımlarla lisansı kırılmış (crack edilmiş) yazılımların eşit derecede güvenli olup olmadığı konusunda da %34.8'lik kesim emin olmadığını ifade etmiştir.

Katılımcıların %56,6'sı "İnternette işlenen suçların failleri genellikle tespit edilemez." ifadesine katılmadıklarını belirtmiştir. Katılımcıların %47'lik bölümü İnternet aboneliğini başkasıyla paylaşmanın tehlikeli olduğunu düşünmektedir. Şifresiz erişilen kablosuz ağlardan İnternete bağlanmanın tehlikeli olduğunu düşünen katılımcıların oranı %34 olarak tespit edilmiştir.

Katılımcıların %48,1'lik bölümü İnternet aracılığıyla kumar oynamanın suç olduğunu düşünmektedir. Ancak ülkemizde yürürlükte bulunan Türk Ceza Kanunu'na göre kumar oynamak değil, oynanmasına yer ve imkan sağlamak suç olarak kabul edilmiştir. Kumar oynanması fiili Kabahatler Kanunu tarafından düzenlenmiştir.

Benzer bir bilgi eksikliği de bilgisayarda pornografik yayınların bulundurulması konusunda görülmektedir. Katılımcıların %35.6'sı söz konusu materyallerin suç kapsamında olduğu görüşünderken %24.6'sı emin olmadıklarını ifade etmiştir.

Facebook ve Twitter gibi sosyal ağ platformlarına kayıtlı olmak için dünyanın her yerinde 13 yaş sınırı bulunmaktadır. Buna rağmen katılımcıların %67.8'i söz konusu sitelerin 13 yaşından küçükler için sakıncalı olduğunu düşünmektedir.

Katılımcıların %65.2'si İnternette içerik filtrelemelerinin servis sağlayıcılar tarafından değil aboneler tarafından uygulanması gerektiği görüşündedir. Katılımcıların %46.6'sı yürürlükteki erişim engelleme tedbir kararlarının kaldırılması gerektiğini ifade etmişlerdir.

Katılımcılar, İnternet bankacılığı dolandırıcılığı konusunda kusur ve sorumluluğun bankalarda olduğu konusunda %27.3 oranı ile emin olmadıklarını; sorumluluğun kullanıcılar üzerinde olduğu konusuna ise %65.5 oranı ile katılmadıklarını belirtmişlerdir.

Katılımcılar, güçlü şifre tercihinin sistem güvenliğini sağlaması konusunda %32.2 oranı ile emin olmadıklarını; %45.8 oranı ile bu görüşe katılmadıklarını ifade etmişlerdir.

Güvenli İnternet Hizmeti'nin kullanıcıları teknik risklerden koruması konusunda katılımcıların %29.5'luk kesimi emin olmadıklarını belirtirken; temiz içerik sağlaması konusunda ise %51.5'lik kesim katıldıklarını belirtmişlerdir.

Katılımcıların %70.5'lik kesimi her ülkede İnternet içeriğini düzenleyen kurum ve kuruluşlar olması gerektiğini; %91.3'lük kesimi ise bilişim suçlarının özel kanunlarla düzenlenmesi gerektiği görüşündedirler.

Yığın (spam) e-postalar konusunda katılımcıların %85.6'sı konunun çözülmesi gereken önemli bir sorun olduğu görüşündeyken; %91.3'ü Tanımadığı kişi ve firmalardan gelen e-posta ve sms mesajlarından rahatsız olduğunu belirtmiştir.

Katılımcıların %56.8'lik bölümü ise İnternette kimlik saklama davranışının yaygın olduğu görüşündedir. Kimlik saklama davranışının yaygın olmadığını düşünenler %11.8'lik bölümü oluştururken; katılımcıların %31.4'lük bölümü konu hakkında emin olmadıklarını ifade etmişlerdir.

10. SONUÇLAR VE YORUMLAR

Örnekleme üzerinde yapılan çalışmalarda, teknoloji konularına ilgi seviyesi ve bilişim okuryazarlığıyla eğitim ve gelir düzeyi parametreleri arasında doğru orantı olduğu bulgusuna ulaşılmıştır.

Bilişim suçları konusunda ise her eğitim ve gelir düzeyinde bilgi ve farkındalık eksikliği tespit edilmiştir. Özellikle kumar, pornografi gibi konularda ve İnternet bankacılığı dolandırıcılığı konularında hangi fiilin suç olduğu ya da kusur ve sorumluluk dağılımı konularında katılımcıların büyük çoğunluğu fikir beyan edememişlerdir.

Ülkemizdeki bilişim mevzuatının gelişmiş ülkelere göre yetersiz ve eksik oluşu, özellikle de bilişim suçlarına özgü yasaların bulunmayışı da katılımcıların hemfikir olduğu konular arasındadır.

Ülkemizde mevcut bulunan yasalar tarafından daha önce düzenlenemeyen yığın (spam) e-posta ve sms gönderimi konusunda 1 Mayıs 2015 tarihinde yürürlüğe giren “Elektronik Ticaretin Düzenlenmesi Hakkında Kanun” un bu soruna etkin çözümler üretmesi beklenmektedir. Katılımcıların en çok fikir birliğinde olduğu (%91.3) konu olarak yığın e-posta ve SMS’lerden duyulan rahatsızlık olarak öne çıkmaktadır.

Bireysel İnternet güvenliği konusunda Katılımcıların yaklaşık olarak yarısı (%47) İnternet aboneliğini başkasıyla paylaşmanın tehlikeli olduğunu düşünmektedir. Şifresiz erişilen kablosuz ağlardan İnternete bağlanmanın tehlikeli olduğunu düşünen katılımcıların oranı ise yaklaşık olarak üçte bir oranında (%34) olarak tespit edilmiştir.

Katılımcıların yaklaşık olarak üçte biri (%33.7) Antivirüs yazılımlarının bilgisayarları bütün tehlikelerden koruması konusunda emin olmadığını ifade etmiştir. Benzer biçimde lisanslı yazılımlarla lisansı kırılmış (crack edilmiş) yazılımların eşit derecede güvenli olup olmadığı konusunda da aynı üçte birlik (%34.8) emin olmayan oranda katılımcı karşımıza çıkmaktadır. İnternette kimlik saklama davranışı konusunda da yaklaşık üçte birlik (%31.4) oranda katılımcı fikir sahibi olmadığını beyan etmiştir.

Özet olarak kullanıcıların yaklaşık olarak üçte birinin İnternet güvenliği ve güvenli İnternet konularında bilinç sahibi olmadığını söylemek mümkündür.

Güvenli İnternet konusunda yapılan analizlerde ise Katılımcıların yaklaşık olarak yarısı (%49.2) İnternetin tamamen özgür bir ortam olması gerektiğini

savunmaktadır.

Katılımcıların %23.1'lik oranı Güvenli İnternet Hizmeti kullandıklarını ifade etmiştir. Aynı soruya yanıt veren çocuklu katılımcılarda bu oran %43.5 ve çocuksuz katılımcılarda ise %13.4 olarak karşımıza çıkmaktadır. İnternetin tamamen özgür olması konusunda çocuklu bireylerin %62.4'lük kesimi “hayır” yanıtını verirken aynı yanıtı veren çocuksuz katılımcıların oranı %45.3 ve örneklem genelindeki “hayır” yanıtının oranı %50.8 olarak hesaplanmıştır.

Güvenli İnternet Hizmeti kullanım tercihinin çocuklu ailelerde istatistiksel olarak anlamlı bir biçimde daha yaygın olduğunu söylemek mümkündür.

Katılımcıların büyük bir çoğunluğu (%70.5) her ülkede İnternet içeriğini düzenleyen kurum ve kuruluşlar olması gerektiğini düşünmektedir. Aynı şekilde katılımcıların %65.2'si İnternette içerik filtrelemelerinin gerekliliğini vurgulamıştır.

Güvenli İnternet Hizmeti'nin kullanıcıları teknik risklerden koruması konusunda katılımcıların %29.5'luk kesimi emin olmadıklarını belirtirken; temiz içerik sağlaması konusunda ise %51.5'lik kesim bu görüşe katıldıklarını belirtmiştir.

Sonuç olarak ülkemizde uygulanan Güvenli İnternet Hizmeti'nin toplumsal bilişim okuryazarlığı düzeyine uygun bir proje olduğunu, özellikle çocuklu aileler için tercih ve tavsiye edilebilir bir uygulama olduğunu söylemek mümkündür. Bilgisayar ve İnternet konularındaki bilgi ve bilinç düzeyi geliştikçe çocukları olumsuz içeriklerden ve bütün yaş kesimlerindeki kullanıcıları teknik tehditlerden korumak için farklı proje ve yöntemlerin uygulanması düşünülebilir.

KAYNAKLAR

- [1] Web 1, (2017) <https://www.merriam-webster.com/dictionary/Internet> (Erişim Tarihi: 01/05/2017).
- [2] İnternet 12 Yaşında (2011), Elektrik Mühendisliği Dergisi 442. Sayı, 21-24.
- [3] Web 2, (2017) http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/55.html (Erişim Tarihi: 01/05/2017).
- [4] Web 3, (2017) <http://www.google.com.tr/safetycenter/families/start/basics/> (Erişim Tarihi: 01/05/2017).
- [5] İlbaş Ç., (2006), Bilişim Suçlarının Tespitinde Kablosuz İnternet Engeli, Bilişim ve Hukuk Dergisi, 17-18.
- [6] Mitnick K., (2002), The Art of Deception, John Wiley and Sons.
- [7] Microsoft, (2017), Güvenlik Danışma Belgesi (Sayı:912920).
- [8] İlbaş Ç. (2009), “Bilişim Suçlarının Sosyo Kültürel Seviyelere Göre Algı Analizi”, Yüksek Lisans Tezi, Başkent Üniversitesi.
- [9] A. Hussain, J. Heidemann, C. Papadopoulos, (2004), “Distinguishing between Singel and Multisource, Computer Networks, Volume 46, Issue 4, 479–503.
- [10] Web 3, (2017), http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php (Erişim Tarihi: 08/05/2017).
- [11] Siber Güvenlik Kurulu, (2012), Ulaştırma Denizcilik ve Haberleşme Bakanlığı 3. Toplantı raporu.
- [12] Siber Güvenlik Kurulu, (2012), Milli Savunma Bakanlığı 3. Toplantı raporu.
- [13] Web 4, (2017), <http://www.idare.gen.tr/akillioglu-idariusul.htm> (Erişim Tarihi: 08/05/2017).
- [14] Web 5, (2017), <http://www.kgmd.adalet.gov.tr/kisiselverilerinkorunmasikanunu.htm> (Erişim Tarihi: 08/05/2017).
- [15] Koç S., (2013), “Hukuksal Bağlamda Sosyal Medya Analizi ve Kıyaslamalı Mevzuat Önerileri” Yüksek lisans Tezi, Bilgi Üniversitesi.
- [16] Web 6, (2017), http://www.tib.gov.tr/tr/tr-menu-36-guvenli_internet_hizmeti.html (Erişim Tarihi: 01/05/2017).
- [17] BTK, (2012), Çocuk ve Aile Profil Kriterleri Çalışma Kurulu 4. Toplantı Raporu.

[18]BTK, (2012), Çocuk ve Aile Profil Kriterleri Çalışma Kurulu 1. Toplantı Raporu.

ÖZGEÇMİŞ

Aslen İzmirli olan ve ailesinin memuriyet hayatı dolayısıyla Çankırı Ilgaz'da doğan Serhat Özeren, lisans eğitimini İstanbul Teknik Üniversitesi Uçak ve Uzak Bilimleri Fakültesi Uçak Mühendisliği bölümünde tamamlamıştır.

İş yaşamına 1989 yılında Lever Bilgi İşlem bölümünde IT Sistemleri ve AS/400 sistemlerinin güvenliğinden ve işletiminden sorumlu çalışmalarda bulunarak başlamıştır. Lever'den ayrıldıktan sonra Erenet Bilgisayar Otomasyon Sistemleri'ni kuran Özeren, Lever'e Bilgi Teknolojileri konusunda dış kaynak kullanımı hizmeti vermiştir. Özeren, Erenet' ten sonra, 1995 yılında Türkiye'nin ilk SAP (Systems Applications and Products) uygulama ortağı olan Eresoft'un kuruluşunda yer almıştır. 1997 yılında ise Oracle iş ortağı olan Ereteam şirketini kurmuştur.

Özeren, 2005-2008 yılları arasında C5 Elektronik'te Yönetim Kurulu Üyesi ve Genel Müdür olarak görev yapmıştır. 2010-2015 tarihlerinde C5 Elektronik Yönetim Kurulu Başkan Vekili olarak görev yapmıştır. Aynı zamanda İTÜ Geliştirme Vakfı Okulları Yönetim Kurulu Başkanlığı, İTÜ Geliştirme Vakfı iştiraki olan Arı Kültürel A.Ş. ve Kültürel A.Ş.'nin Yönetim Kurulu Başkanlığını, İstanbul Teknik Üniversitesi Arı-Teknokent Yönetim kurulu üyeliği, Atlas Telekomünikasyon Ltd Yönetim Kurulu Başkanlığı, Biztech Teknoloji Yönetim Kurulu Başkanlığı görevini sürdürmektedir.

Özeren, Ticari hayattaki tecrübesinin yanı sıra, sivil toplum faaliyetlerinde de oldukça aktif rol almaktadır. Özeren, 2002 yılında Telekomünikasyon ve Enerji Hizmetleri Tüketici Hakları ve Sektörel Araştırmalar Derneği'ni (TEDER) kurmuştur. Halen TEDER Yönetim Kurulu Başkanlığı görevini yürütmektedir. 2008 yılında Devlet Planlama Teşkilatı'nda gerçekleştirilen seçimde Türkiye E-Dönüşüm Danışma Kurulu Başkanı seçilmiştir. E-Dönüşüm Danışma Kurulu Başkanı sıfatıyla Türkiye E-Dönüşüm İcra Kurulu'nda da yer almıştır. Tüm Telekomünikasyon İşadamları Derneği (TÜTED) Yönetim Kurulu Üyeliği, Türkiye Bilişim Derneği (TBD) Yönetim Kurulu Üyeliği ve Ulaştırma Denizcilik ve Haberleşme Bakanlığı'nın düzenlediği Ulaştırma Şurası Koordinasyon Kurulu Üyeliği görevlerinde bulunmuştur.

Halen, Teknoloji Bilgilendirme Platformu Başkanlığı, TOBB Telekomünikasyon Sektör Meclisi Başkan Yardımcılığı görevlerini devam ettirmektedir.

2010 yılında Sivil Toplum Kuruluşları ve özel sektör temsilcilerinin desteği ve oy birliğiyle İnternet Kurulu Başkanlığı'na seçilmiştir. Ulaştırma Bakanlığı'nın adında ve yapısındaki değişiklik sonrası 2012 Eylül'den itibaren T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı İnternet Geliştirme Kurulu Başkanlığı görevine yeniden atanmıştır. Bu görevi de 2016 haziran ayına kadar sürdürmüştür.

Ek A: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun üzerinde yapılan değişiklikler

MADDE 85 – 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 2 nci maddesinin birinci fıkrasına aşağıdaki bentler eklenmiştir.

“n) Birlik: Erişim Sağlayıcıları Birliğini,

o) Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

ö) İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,

p) URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,

r) 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,”

MADDE 86 – 5651 sayılı Kanunun 3 üncü maddesine aşağıdaki fıkra eklenmiştir.

“(3) 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.”

MADDE 87 – 5651 sayılı Kanunun 4 üncü maddesine aşağıdaki fıkra eklenmiştir.

“(3) 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.”

MADDE 88 – 5651 sayılı Kanunun 5 inci maddesinin ikinci fıkrası aşağıdaki şekilde değiştirilmiş ve aynı maddeye aşağıdaki fıkralar eklenmiştir.

“(2) Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.”

“(3) 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) Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

(5) Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.

(6) 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.”

MADDE 89 – 5651 sayılı Kanunun 6 ncı maddesinin birinci fıkrasının (a) bendindeki “ve teknik olarak engelleme imkânı bulunduğu ölçüde” ibaresi çıkartılmış, aynı fıkra aşağıdaki (ç) ve (d) bentleri eklenmiş, üçüncü fıkrasında geçen “(b) ve (c)” ibaresi “(b), (c), (ç) ve (d)” şeklinde değiştirilmiştir.

“ç) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla,”

MADDE 90 – 5651 sayılı Kanunun 6 ncı maddesinden sonra gelmek üzere aşağıdaki 6/A maddesi eklenmiştir.

“Erişim Sağlayıcıları Birliği

MADDE 6/A – (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 katılımıyla oluşan ve koordinasyonu sağlayan bir kuruluştur.

(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.”

MADDE 91 – 5651 sayılı Kanunun 7 nci maddesinin ikinci ve üçüncü fıkraları aşağıdaki şekilde değiştirilmiş ve maddeye aşağıdaki fıkra eklenmiştir.

“(2) 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) Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.”

“(4) 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.”

MADDE 92 – 5651 sayılı Kanunun 8 inci maddesinin ikinci fıkrasının dördüncü cümlesinden sonra gelmek üzere “Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir.” cümlesi eklenmiş, dördüncü fıkrasında yer alan “(2) ve (5)” ibaresi “(2), (5) ve (6)” şeklinde değiştirilmiş, onuncu fıkrasındaki “altı aydan iki yıla kadar hapis cezası” ibaresi “beş yüz günden üç bin güne kadar adli para cezası” şeklinde değiştirilmiştir.

MADDE 93 – 5651 sayılı Kanunun 9 uncu maddesi başlığıyla birlikte aşağıdaki şekilde değiştirilmiştir.

“İçeriğin yayından çıkarılması ve erişimin engellenmesi

MADDE 9 – (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.

(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.”

MADDE 94 – 5651 sayılı Kanunun 9 uncu maddesinden sonra gelmek üzere aşağıdaki 9/A maddesi eklenmiştir.

“Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi

MADDE 9/A – (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. Bu karara karşı sulh ceza mahkemesine itiraz edilebilir.”

MADDE 95 – 5651 sayılı Kanunun 10 uncu maddesinin dördüncü fıkrasının (a)

bendinde yer alan “yayınları önlemeye” ibaresinden sonra “, internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye” ibaresi eklenmiş, beşinci fıkrası aşağıdaki şekilde değiştirilmiş, maddeye aşağıdaki fıkralar eklenmiştir.

“(5) 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) 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) Başkanlık kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurabilir.”

MADDE 96 – 5651 sayılı Kanunun 11 inci maddesinin ikinci fıkrasında yer alan “yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine” ibaresi “yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine” şeklinde değiştirilmiştir.

MADDE 97 – 5651 sayılı Kanunun ek 1 inci maddesinin dördüncü fıkrasından sonra gelmek üzere aşağıdaki fıkralar eklenmiş ve diğer fıkra buna göre teselsül ettirilmiştir.

“(5) 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) 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.”

MADDE 98 – Ekli (2) sayılı listedeki kadrolar ihdas edilerek öncelikle Telekomünikasyon İletişim Başkanlığı hizmetlerinde kullanılmak üzere 5651 sayılı Kanuna ekli (I) sayılı listeye eklenmiştir.

MADDE 99 – 5651 sayılı Kanuna aşağıdaki ek madde eklenmiştir.

“EK MADDE 2 – 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 fıkra da belirtilen ücret dışında herhangi bir ödeme yapılamaz.”

MADDE 100 – 5651 sayılı Kanuna aşağıdaki geçici madde eklenmiştir.

“GEÇİCİ MADDE 3 – (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 Tüzüğü'nün 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.”

Ek B: İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik

Amaç ve kapsam

MADDE 1 – (1) Bu Yönetmeliğin amacı; içerik sağlayıcıların, yer sağlayıcıların ve erişim sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Yönetmelik; 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 – (1) Bu Yönetmeliğin uygulanmasında;

- a) Abone: Herhangi bir sözleşme ile erişim sağlayıcılarından internet ortamına bağlanma hizmeti alan gerçek veya tüzel kişileri,
- b) Başkan: Telekomünikasyon İletişim Başkanını,
- c) Başkanlık: Telekomünikasyon İletişim Başkanlığını,
- ç) Bilgi: Verilerin anlam kazanmış biçimini,
- d) Dosya bütünlük değeri: Bir bilgisayar dosyasının içindeki bütün verilerin matematiksel bir işlemde geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değeri,
- e) Erişim: Herhangi bir vasıta ile internet ortamına bağlanarak kullanım olanağı kazanılmasını,
- f) Erişim sağlayıcı: İnternet toplu kullanım sağlayıcılarına ve abone olan kullanıcılarına internet ortamına erişim olanağı sağlayan işletmeciler ile gerçek veya tüzel kişileri,
- g) Erişim sağlayıcı trafik bilgisi: İnternet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgileri,
- ğ) Faaliyet belgesi: Erişim sağlayıcı veya yer sağlayıcı olarak faaliyette bulunabilmek için Kurum tarafından verilen Kanun kapsamındaki yetkilendirmeyi içeren belgeyi,

h) IP adresi: Belirli bir ağı bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adresi,

ı) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri,

i) İnternet ortamı: Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı,

j) İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini,

k) Kanun: 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu,

l) Kullanıcı: Aboneliği olup olmamasına bakılmaksızın internet ortamından yararlanan gerçek veya tüzel kişileri,

m) Kurum: Telekomünikasyon Kurumunu,

n) Sabit IP adresi: Belirli bir ağı bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, zamana, oturuma göre değişmeyen ve sistem yöneticisi tarafından belirlenip tanımlanan ve değiştirilebilen IP adresini,

o) Ticari amaçla internet toplu kullanım sağlayıcı: İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek veya tüzel kişileri,

ö) Vekil sunucu trafik bilgisi: İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri,

p) Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri,

r) Yayın: İnternet ortamında yapılan yayını,

s) Yer sağlayıcı: İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,

ş) Yer sağlayıcı trafik bilgisi: İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri, ifade eder.

İlkeler

MADDE 4 – (1) Yayınlar;

- a) İnsan onuruna, temel hak ve hürriyetlere saygılı olmalıdır.
- b) Gençlerin ve çocukların fiziksel, zihinsel ve ahlakî gelişimini zedeleyecek türden içeriklere yer vermemelidir.
- c) Ailenin huzur ve refahını sağlayan hususlara zarar verecek nitelikte olmamalıdır.
- ç) Kişileri, uyuşturucu madde bağımlılığı, fuhuş, müstehcenlik ve kumar gibi kötü alışkanlıklara teşvik edici olmamalıdır.

(2) Herkesin kendisine yönelik haklarını ihlal eden internet yayınlarının içeriklerinden dolayı cevap ve düzeltme hakkı olmalıdır.

İKİNCİ BÖLÜM

İçerik Sağlayıcıları, Yer Sağlayıcıları ile Erişim Sağlayıcılarının

Sorumluluk ve Yükümlülükleri

Bilgilendirme yükümlülüğü

MADDE 5 – (1) Ticari veya ekonomik amaçlı içerik sağlayıcıları, yer sağlayıcıları ve erişim sağlayıcıları, aşağıda belirtilen tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür:

- a) Gerçek kişi ise; adı ve soyadı, tüzel kişi ise; unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası,
- b) Yerleşim yeri, tüzel kişi ise merkezinin bulunduğu yer,
- c) Elektronik iletişim adresi ve telefon numarası,
- ç) Sunduğu hizmet, bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapılıyor ise, yetkili denetim merciine ilişkin bilgiler.

(2) Ticari veya ekonomik amaçlı içerik sağlayıcı, birinci fıkradaki bilgilerle birlikte, yer sağlayıcıya ilişkin tanıtıcı bilgileri, doğru, eksiksiz ve güncel olarak ana sayfasında bulundurmakla yükümlüdür.

İçerik sağlayıcının sorumluluğu

MADDE 6 – (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.

Yer sağlayıcının yükümlülükleri

MADDE 7 – (1) Yer sağlayıcı;

a) Yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, Kanun ve ilgili mevzuat hükümlerine göre Başkanlık, adli makamlar veya hakları ihlal edilen kişiler tarafından haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla,

b) Sunucu barındırma hizmeti dâhil, yer sağlamakla ilgili hizmetlerinde (a) bendindeki hükümlere uymakla,

c) Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle,

yükümlüdür.

(2) Yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir.

Erişim sağlayıcının yükümlülükleri

MADDE 8 – (1) Erişim sağlayıcı;

a) Herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, Kanun ve ilgili diğer mevzuat hükümlerine göre, Başkanlıkça haberdar edilmesi halinde ve teknik olarak en-gelleme imkânı bulunduğu ölçüde erişimi engellemekle,

b) Sağladığı hizmetlere ilişkin olarak, Başkanlığın Kanunla ve ilgili diğer mevzuatla verilen görevlerini yerine getirebilmesi için; erişim sağlayıcı trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle, internet trafik izlemesinde Başkanlığa gerekli yardım ve desteği sağlamakla, faaliyet belgesinde yer alan Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirmekle ve ticari amaçla internet toplu kullanım sağlayıcılar için belirli bir IP bloğundan sabit IP adres planlaması yapmakla ve bu bloktan IP adresi vermekle,

c) Faaliyetine son vereceği tarihten en az üç ay önce, durumu Kuruma, içerik sağlayıcılarına ve müşterilerine bildirmekle, Kuruma bildirilen kapanma tarihinden geriye doğru bir yıllık süredeki trafik bilgilerine ilişkin bütün kayıtları metin dosyası olarak, log formatlarını açıklamalarıyla birlikte, abone kütük bilgilerini Başkanlığa cd, dvd gibi optik medya ortamında teslim etmekle,

ç) Faaliyete başlamasından itibaren her ay düzenli olarak, her erişim yöntemine ilişkin kullanacağı erişim numaralarını ve toptan hizmet verdiği abonelere ilişkin

bilgileri Başkanlığa göndermekle,

d) Başkanlık ile aralarındaki bağlantıdan erişimi engellenecek adreslere ilişkin gönderilecek bilgileri kendi sistemlerinde derhal uygulanabilmesi için, gerekli olan donanım ve yazılımı kurarak lazım olan düzenlemeleri yapmakla,

e) Kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte muhafaza etmek ve gizliliğini temin etmekle,

yükümlüdür.

(2) Erişim sağlayıcı, verdiği hizmeti kullananlara ilişkin bilgilerin başkaları tarafından elde edilmesini ilgili mevzuatta belirlenen esas ve usullere uygun olarak engeller.

(3) Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadığını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.

İdari para cezaları

MADDE 9 – (1) Bu Yönetmeliğin 5 inci maddesinde belirtilen yükümlülüğü yerine getirmeyen içerik sağlayıcı, yer sağlayıcı veya erişim sağlayıcıya Başkanlık tarafından ikibin Yeni Türk Lirasından onbin Yeni Türk Lirasına kadar idarî para cezası verilir.

(2) Bu Yönetmeliğin 8 inci maddesinin birinci fıkrasının (b) ve (c) bentlerinde yer alan yükümlülüklerden birini yerine getirmeyen erişim sağlayıcısına, Başkanlık tarafından onbin Yeni Türk Lirasından ellibin Yeni Türk Lirasına kadar idarî para cezası verilir.

ÜÇÜNCÜ BÖLÜM

İçeriğin Yayından Çıkarılması ve Cevap Hakkı

İçeriğin yayından çıkarılması ve cevap hakkı

MADDE 10 – (1) İçerik nedeniyle hakları ihlâl edildiğini iddia eden kişi, içerik sağlayıcıya, buna ulaşamaması halinde yer sağlayıcıya, internet ortamından veya bizzat başvurarak, kendisine ilişkin içeriğin yayından çıkarılmasını ve yayındaki kapsamından fazla olmamak üzere hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasını isteyebilir. İçerik veya yer sağlayıcı, kendisine ulaştığı tarihten itibaren iki gün içinde talebi yerine getirir. Bu süre zarfında talep yerine getirilmediği takdirde reddedilmiş sayılır.

(2) Talebin reddedilmiş sayılması halinde, kişi onbeş gün içinde yerleşim yeri sulh ceza mahkemesine başvurarak, içeriğin yayından çıkarılmasına ve yayındaki kapsamından fazla olmamak üzere, hazırladığı cevabın bir hafta süreyle internet ortamında yayımlanmasına karar verilmesini isteyebilir. Sulh ceza hâkimi bu talebi üç gün içinde duruşma yapmaksızın karara bağlar. Sulh ceza hâkiminin kararına karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(3) Sulh ceza hâkiminin kesinleşen kararının, birinci fıkraya göre yapılan başvuruyu yerine getirmeyen içerik sağlayıcıya veya yer sağlayıcıya tebliğinden itibaren iki gün içinde, içerik yayından çıkarılarak hazırlanan cevabın yayımlanmasına, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve tekzip başlığı altında başlanır.

Cezai yaptırım

MADDE 11 – (1) Sulh ceza hâkiminin kararını, 10 uncu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. İçerik veya yer sağlayıcının tüzel kişi olması halinde, bu fıkra hükmü yayın sorumlusu hakkında uygulanır.

DÖRDÜNCÜ BÖLÜM

Erişimin Engellenmesi

Erişimin engellenmesi kararının konusunu oluşturan suçlar

MADDE 12 – (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),

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

Koruma tedbiri olarak erişimin engellenmesi kararı

MADDE 13 – (1) 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.

(2) Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara, Başkanlıkça ve Ceza Muhakemesi Kanunu hükümlerine göre ilgililer tarafından itiraz edilebilir.

İdari tedbir olarak erişimin engellenmesi kararı

MADDE 14 – (1) İçeriği 12 nci maddede belirtilen suçları oluşturan yayınlarda, içerik sağlayıcının veya yer sağlayıcının yurt dışında bulunması halinde veya içerik sağlayıcı veya yer sağlayıcı yurt içinde bulursa bile, içeriği Türk Ceza Kanununun 103 üncü maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226 ncı maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesine Başkanlıkça re’sen karar verilir. Türk Ceza Kanununun 103 üncü maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226 ncı maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak içerik veya yer sağlayıcının yurt içinde bulunması durumunda bu karar, yirmidört saat içinde hâkimin onayına sunulur ve hâkim kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Başkanlık tarafından derhal kaldırılır ve erişim sağlayıcılara bildirilerek gereğinin yerine getirilmesi istenir.

(2) Başkanlık tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Cumhuriyet başsavcılığına suç duyurusunda bulunulur. Başkanlık, suç duyurusuna esas teşkil edecek verilerin elde edilebilmesi için kamu kurum ve kuruluşlarından bilgi ve belge talep edebilir.

Erişimin engellenmesi kararında belirtilmesi gerekli hususlar

MADDE 15 – (1) Koruma tedbiri olarak verilen erişimin engellenmesi kararında;

- a) Kararı veren merciin adı,
- b) Karar tarihi ile soruşturma numarası veya kovuşturmayla geçilmişse mahkeme esas numarası,
- c) Tedbirin hangi suç için istendiği, bu suça ilişkin yeterli şüphe sebeplerinin neler olduğu,

ç) "URL adresi: <http://www.abcd.com/abcdefgh.htm>" şeklinde örneklenen, suça ilişkin bilgilerin bulunduğu tam web adresi,

d) "www.abcd.com" şeklinde örneklenen, hakkında tedbir uygulanacak internet yayınlarının alan adı,

e) Hakkında tedbir uygulanacak internet yayınlarının bulunduğu yer sağlayıcıya ait IP adresi,

f) Alan adı veya IP adresi olarak erişim engelleme yöntemi, belirtilir.

Erişimin engellenmesi usulü

MADDE 16 – (1) Yönetmeliğin 13 üncü maddesi gereğince, hâkim, mahkeme veya Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararı Başkanlığa gönderilir. Kararlar, doğrudan erişim sağlayıcılara gönderilemez. Başkanlık, kararlara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

(2) Kişiler veya kurumlar tarafından Başkanlığın kurduğu bilgi ihbar merkezine yapılan ihbarlar, teknik ve hukuki incelemeye alınır. Söz konusu içerikte bu suçlardan birisinin olduğu konusunda yeterli şüphe sebebi tespit edildiği takdirde, 14 üncü maddeye göre işlem yapılır. Suça ilişkin yeterli şüphe sebebi tespit edilemediği takdirde işlem yapılmaz.

(3) 13 üncü ve 14 üncü maddeler kapsamındaki erişimin engellenmesi kararlarına ilişkin bilgiler, Başkanlıkça ilgili erişim sağlayıcılara elektronik ortamda bildirilir ve kararların gereği erişim sağlayıcılar tarafından derhal ve en geç kararın bildirilmesi anından itibaren yirmidört saat içinde yerine getirilir. 13 üncü maddeye göre erişimi engellenen yayınlar, Başkanlık tarafından hazırlanan ve mevcut sayfa yerine kararı veren merciin adı ile karar tarih ve sayısını belirten uyarı sayfasına yönlendirilir.

(4) Erişim sağlayıcılar, Başkanlık ile aralarındaki bağlantıdan aktarılabilecek erişimin engellenmesi kararlarının, kendi sistemlerinde derhal uygulanabilmesi için gerekli olan donanım ve yazılımı kurarak lazım olan düzenlemeleri yapar.

(5) Erişimin engellenmesi kararı kapsamında, erişimin engellenmesi kararına konu olan suçun olduğu konusunda yeterli şüphe sebebinin tespiti sürecinde, erişim engellenmeden önceki yayının durumu elektronik ortamda Başkanlıkça arşivlenir.

(6) Gerekliğinde Başkanlık, erişimin engellenmesi kararlarına konu olan içeriğin yayından kaldırılmasını, 7 nci maddenin birinci fıkrası uyarınca yer sağlayıcıdan isteyebilir.

Erişimin engellenmesinin hükümsüz kalması

MADDE 17 – (1) Soruşturma sonucunda kovuşturmayaya yer olmadığı kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda Cumhuriyet savcısı, kovuşturmayaya yer olmadığı kararının bir örneğini Başkanlığa gönderir. Başkanlık, karara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

(2) Kovuşturma evresinde beraat kararı verilmesi halinde, erişimin engellenmesi kararı kendiliğinden hükümsüz kalır. Bu durumda mahkemece beraat kararının bir örneği Başkanlığa gönderilir. Başkanlık, karara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

(3) Başkanlıkça resen verilen erişimin engellenmesi kararı, hâkim tarafından onaylanmadığı takdirde hükümsüz sayılır. Başkanlık, karara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

Erişimin engellenmesinin kaldırılması

MADDE 18 – (1) Konusu bu Yönetmeliğin 12 nci maddesinde sayılan suçları oluşturan içeriğin yayından çıkarılması halinde; erişimin engellenmesi kararı, soruşturma evresinde Cumhuriyet savcısı, kovuşturma evresinde mahkeme tarafından kaldırılır. Bu kararın bir örneği Başkanlığa gönderilir. Başkanlık, karara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

(2) 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. Bu kararın bir örneği Başkanlığa gönderilir. Başkanlık, karara ilişkin bilgileri gereği derhal yapılmak üzere elektronik ortamda erişim sağlayıcılara bildirir.

İdari ve cezai yaptırımlar

MADDE 19 – (1) İdarî tedbir olarak verilen erişimin engellenmesi kararının Başkanlıkça bildirilmesinden itibaren yirmidört saat içinde 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 faaliyet belgesinin iptaline karar verilebilir.

(2) Soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme; soruşturma

evresinde gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini Başkanlıkça bildirilmesinden itibaren yirmidört saat içinde yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, altı aydan iki yıla kadar hapis cezası ile cezalandırılır.

BEŞİNCİ BÖLÜM

Çeşitli ve Son Hükümler

Kanun yolu

MADDE 20 – (1) Bu Yönetmelikte 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.

Çalışma kurulları

MADDE 21 – (1) Başkanlık, Ulaştırma Bakanlığı, 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 Kanun kapsamına giren suçları oluşturan içeriğe sahip faaliyet ve yayınları önlemeye yönelik çalışmalar yapmak amacıyla çalışma kurulları oluşturabilir. Çalışma kurulları, Başkanın görevlendireceği personelin başkanlığında çalışmalarını yürütür. Kurulların çalışma usul ve esasları Başkanlıkça belirlenir. Çalışma kurullarının her türlü giderleri Kurum tarafından karşılanır.

(2) Başkanlık bu Yönetmelikle verilen görevlerini yerine getirirken danışman kullanma, hizmet satın alma, tanıtma, kiralama gibi faaliyetlerde bulunabilir.

İşbirliği ve koordinasyon çalışmaları

MADDE 22 – (1) Başkanlık, bilişim ve internet alanındaki gelişmeleri izlemek amacıyla, uluslararası kurum ve kuruluşlarla, gerek Türkiye’de gerekse yurt dışında, giderleri Kurum tarafından karşılanan işbirliği ve ortak çalışmalar yapar.

(2) Başkanlık, 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 bulunur veya koordinasyonu sağlar. Bu doğrultuda Başkanlık, soruşturma mercileri ile yetkili ve görevli kolluk

kuvvetleri tarafından intikal ettirilen talepleri inceler, deęerlendirir ve Kanunda öngörölen suçların önlenmesini teminen gerekli tedbirlerin alınmasını sağlayabilir.

(3) Başkanlık, İnternet Kurulu ile gerekli işbirlięi ve koordinasyonu sağlar; bu Kurulca izleme, filtreleme ve engelleme yapılacak içerięi haiz yayınların tespiti ve benzeri konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır. Başkanlık görevlerinin yerine getirilmesi amacıyla, Başkan veya görevlendireceęi daire başkanı ile ilgili daire başkanları İnternet Kurulu toplantılarına katılır. İnternet Kurulu, Başkanlığın Kanundaki görevlerine ilişkin hususlarda Başkanlığın görüşünü alarak karar verir.

Yürürlük

MADDE 23 – (1) Bu Yönetmelik yayımı tarihinde yürürlüęe girer.

Yürütme

MADDE 24 – (1) Bu Yönetmelik hükümlerini Başbakan yürütür.