ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI

SOSYAL MEDYA DÜZENLEMELERİ; AVRUPA BİRLİĞİ ÜLKELERİNDEN ÖRNEKLER VE TÜRKİYE İÇİN ÖNERİLER

Akif MANAV

Ulaştırma ve Haberleşme Uzmanlığı Tezi

2014

Ankara

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI

SOSYAL MEDYA DÜZENLEMELERİ; AVRUPA BİRLİĞİ ÜLKELERİNDEN ÖRNEKLER VE TÜRKİYE İÇİN ÖNERİLER

Akif MANAV

Ulaştırma ve Haberleşme Uzmanlığı Tezi

2014

Ankara

KABUL VE ONAY

Akif Manav tarafından hazırlanan "Sosyal Medya Düzenlemeleri; Avrupa Birliği Ülkelerinden Örnekler ve Türkiye İçin Öneriler" adlı bu tezin Ulaştırma ve Haberleşme Uzmanlığı tezi olarak uygun olduğunu onaylarım.

Daire Başkanı Gündüz ŞENGÜL
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından Ulaştırma ve Haberleşme Uzmanlığı Tezi olarak kabul edilmiştir.

Adı ve Soyadı İmzası

Başkan:_____

Üye :_____

Üye :_____

Üye :_____

Üye :_____

Bu tez, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı	
Tezin Adı	Sosyal Medya Düzenlemeleri; Avrupa Birliği Ülkelerinden Örnekler ve Türkiye İçin Öneriler
Türü	Ulaştırma ve Haberleşme Uzmanlığı Tezi
Yazar	Akif MANAV
Teslim Tarihi	2014
Anahtar Kelimeler	Sosyal Medya, Sosyal Medya Düzenlemeleri, İnternet Suçları, Sosyal Paylaşım Ağları
Tez Danışmanı	Daire Başkanı Gündüz ŞENGÜL
Sayfa Adedi	vii+103

İnternet kullanımının yaygınlaşmasıyla birlikte hayatımıza hızla giren sosyal medya siteleri, kullanıcılarına paylaştıkları içeriğin geniş kitlelere hızla ve kolayca ulaşması gibi konularda pek çok fırsat yaratmıştır. Ancak aynı mecraların bilinçsiz ya da kötü niyetli kişiler tarafından kullanılması gibi büyük risklerde söz konusudur. Bu noktada, sosyal medya platformlarında yapılan paylaşımlar sebebiyle hukuki ve cezai sorumluluğun sınırlarının neler olduğu son dönemlerde önemli bir gündem konusu olmuştur.

Bu çalışmada, internet ve sosyal medya alanına yönelik düzenlemeler Türkiye ve bazı Avrupa Birliği ülkeleri örnekleriyle birlikte incelenmiştir. Bazı AB ülkeleri ve Türkiye'de gerçekleştirilen uygulamalar incelenerek söz konusu alana yönelik düzenlemeler genel hatlarıyla ortaya koyulmuştur. Sonuç olarak, Türkiye ve AB ülkeleri arasında bir karşılaştırma yaparak AB'ye katılmayı hedefleyen Türkiye için yeni öneriler oluşturulmaya çalışılmıştır.

ABSTRACT

Ministry Of Transport, Maritime Affairs And Communications	
Thesis	Social Media Regulations; Examples from EU countries and Recommendations for Turkey
Type	Transportation and Communication Expertise Thesis
Author	Akif MANAV
Submission Date	2014
Keywords	Social Media, Social Media Regulations, Internet Crimes, Social Networks
Advisor	Head of Department Gündüz ŞENGÜL
Total Page	vii+103

With the widespread use of the internet into our lives,the newcomer social media sites has created many opportunities for the users to share the content in the areas of reaching a wide audience quickly and easily. However, there are great risks as the usage of the same medium by malicious or the unconscious people. At this point, due to sharing at the social media platforms,what are the limits of the civil and criminal liability in recent years has been an important item on the agenda.

In this study, the internet and social media regulations in Turkey with the examples in some EU countries were examined. By examining the practices some EU countries and Turkey outline of the regulations in question has been revealed. As a conclusion, by making a comparison beetween Turkey and EU countries, new proposals for Turkey that aims to join the EU have been attemted to establish.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Daire Başkanı Sn. Gündüz ŞENGÜL'e, tez verilerimin toplanmasında ve düzenlenmesinde büyük emeği olan Burcu ÖZTÜRK ve Mehmet RİGAN'a, tezde kullanılan görsellerin hazırlanmasında yardımcı olan Onur DEMİR'e ve tez yazma sürecinde desteklerini eksik etmeyen tüm mesai arkadaşlarıma, beni yetiştiren ve bugünlere gelmemi sağlayan sevgili anne ve babama ve bu süreçte hep yanımda olup beni destekleyen sevgili eşim Zaliha MANAV'a teşekkürü bir borç bilirim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği (European Union (EU))
ABD	Amerika Birleşik Devletleri
A.Ş.	Anonim Şirket
BTK	Bilgi Teknolojileri ve İletişimi Kurumu
DNS	Alan Adı Sistemi (Domain Name System)
DPT	Devlet Planlama Teşkilatı
DSL	Sayısal Abone Hattı (Digital Subscriber Line)
ENISA	Avrupa Ağ ve Veri Güvenliği Ajansı (European Network and Information Security Agency)
HTML	Zengin Metin İşaretleme Dili (Hyper Text Markup Language)
IAB	Etkileşimli Reklamcılık Bürosu (Interactive Advertising Bureau)
ICQ	Seni Arıyorum Programı (I Seek You)
IP	İnternet Protokolü (Internet Protocol Address)
İTÜ	İstanbul Teknik Üniversitesi
MEB	Milli Eğitim Bakanlığı
ODTÜ	Orta Doğu Teknik Üniversitesi
OECD	Ekonomik İşbirliği ve Kalkınma Teşkilatı (Organisation for Economic Co-operation and Development)
KDV	Katma Değer Vergisi
PTT	Posta ve Telgraf Teşkilatı
RTÜK	Radyo ve Televizyon Üst Kurulu
SSAK	Suç Sorunlarına Dair Avrupa Komitesi (European Committee on Crime Problems)
SSS	Siber Suçlar Sözleşmesi
S.R.G.	Sayılı Resmi Gazete
TBMM	Türkiye Büyük Millet Meclisi

TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
TMK	Türk Medeni Kanunu
TL	Türk Lirası
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
URL	Standart Kaynak Bulucu (Uniform Resource Locator)

GİRİŞ

Gerçek anlamda, 1970'li yılların başlarında ilk kez ortaya çıktığında önemi tam anlamıyla anlaşılamayan internet, bugün insanların günlük yaşamda en çok kullandığı ürün ve her geçen gün hızla küreselleşen dünyamızın en önemli evrensel gelişme aracı olmuştur.

Özellikle 1990'lı yılların başından itibaren kullanımı süratle artan ve geniş kitlelere yayılan internet, çeşitli tür ve içeriğe sahip web sitelerinin ortaya çıkmasıyla birlikte hızla yaygınlaşmış ve bu durum hiç şüphesiz interneti kitle iletişim araçları içinde özel bir yere taşımıştır.

İnternet ile birlikte paralel bir gelişim süreci gösteren "Sosyal Medya" kavramı da hayatımıza yeni giren bir olgudur.

Web 2.0 teknolojisinin ortaya çıkısıyla internet tek yönlü bir yayın alanı olmaktan çıkıp internet kullanıcılarının da paylaşım yapabildiği etkileşimli bir ortam olmuştur. Gelişen bu teknoloji ile birlikte sosyal paylaşım siteleri oluşmuş ve bu sitelerin yaygınlaşması sosyal medya kavramını doğurmuştur.

Günümüzde sosyal paylaşım ağları; haber, iş, sağlık, sanat, gezi gibi her türden konu üzerine sohbet edebileceğiniz blog ve forum siteleri, arkadaşlık kurma siteleri, ticari ürünler üzerine yorum ve şikâyet siteleri, video ve fotoğraf paylaşım siteleri gibi yaygın türlere sahiptir. Bu siteler; kullanım amacı, yapısı ya da hedef kitlesi itibariyle çeşitlilik göstermektedir. Örneğin bugün, özellikle gençler için Twitter, Facebook, Instagram gibi sosyal paylaşım sitelerinde aktif olarak yer almak, arkadaş çevresini genişletmenin en kolay yolu haline gelmişken, Linkedin gibi siteler ise iş hayatında güçlü bir ağ oluşturmanın en etkili yolu olmuştur.

Sosyal medya, kullanıcılarına paylaştıkları içeriğin geniş kitlelere kolayca ulaşması, demokrasi ve haber özgürlüğü gibi konularda pek çok fırsat yaratmaktadır. Ancak aynı mecranın bilinçsiz ya da kötü niyetli kişiler tarafından kullanılması gibi büyük riskler de söz konusudur. Örneğin; bir kurum ya da şahıs hakkında ortaya iftira atma, karalama ya da hakaret ve tehdit etme gibi benzeri suçlar işlenebilmekte, özel hayatın

ve kişisel verilerin gizliliği ihlal edilmekte ve devlet sırrı niteliğindeki bilgiler paylaşılabilmektedir.

Farklı boyutları olan bu yeni medya mecrasının geleneksel hukuk sistemi ile düzenlenemeyeceği tartışılmaktadır. Basın, yayın ve diğer iletişim araçlarını düzenleyen klasik hukuk normlarının sosyal medyanın yarattığı fırsatlar ve tehditler karşısında yeniden gözden geçirilmesi bir zorunluluk haline gelmiştir. Bu tür ve benzeri suçların kovuşturulmasına, bilgi güvenliğinin sağlanmasına kadar çok çeşitli yeni sorunlar gün yüzüne çıkmış ve tüm dünyada olduğu gibi Türkiye'de de sosyal medya kullanıcılarının hukuki ve cezai sorumluluklarının hangi esaslara tabi olacağı önemli bir tartışma konusu olmuştur.

Bu tez çalışmasının amacı; Avrupa Birliği'ne katılmayı hedefleyen ülkemiz için belli başlı bazı Avrupa Birliği ülkelerinin sosyal medya alanına yönelik düzenlemelerini inceleyerek Türkiye'deki düzenlemeler ile bir karşılaştırma yapmak ve ülkemiz için söz konusu alana yönelik önerileri değerlendirmektir.

Bu çalışma kapsamında; sosyal medyanın tanımı, tarihçesi ve gelişimine değinilmiş, dünyada yaygın olan sosyal paylaşım ağları ile Türkiye'deki sosyal medya kullanım hareketleri incelenmiş ve kitlesel örgütlenmede sosyal medyanın etkisine dikkat çekilmeye çalışılmıştır. Avrupa Birliği'nde internet ve sosyal medya alanına ilişkin düzenlemeler ile bazı AB ülkelerinde internet ve sosyal medya aracılığıyla işlenen suçlara dair düzenlemeler incelenmiş, dava örnekleri verilmiş ve Türkiye'de bu alana yönelik düzenlemeler araştırılarak, söz konusu alana yönelik sosyal ve hukuki alanda yapılabilecek çalışmalar konusunda öneriler sunulmuştur.

I. SOSYAL MEDYA KAVRAMI, KULLANIMI ve KİTLESEL ETKİSİ

İnternet ile birlikte paralel bir gelişim süreci gösteren "Sosyal Medya" kavramı hayatımıza yeni giren bir olgudur.

Haber siteleri, arkadaşlık kurma siteleri, video ve fotoğraf paylaşım siteleri gibi çeşitli türlere sahip olan sosyal medya ağlarını, kısaca kullanıcıların kendi ürettiği içeriği, paylaştığı ve yayınladığı her türlü internet kökenli platformun genel adı olarak tanımlayabilir ve sağladığı bilgi aktarımı niteliğiyle de bir kitle iletişim aracı olarak görebiliriz.

Sosyal meydanın radyo, televizyon ve gazete gibi geleneksel medya mecralarından farkı ise karşılıklı bir iletişimin söz konusu olmasıdır. Bu mecra, kişilerin birbirleriyle ya da kurumların kişilerle doğrudan iletişim kurabildiği ve hızla geri dönüş alabildiği kolay ve kullanışlı bir platformdur. Ayrıca kullanıcıya dayanan üretimin sürekli güncellenme olanağı vardır.

Sosyal medyanın, kullanıcılarının hayatları üzerinde büyük etkisi olduğu hemen hemen tüm akademik çalışmaların içeriğinde yer almaktadır. Sosyal medya üzerinden yaratılan bağların internet üzerinde sağlanan platformun sanallığını sosyalliğe doğru dönüştürdüğü söylenmektedir. Böylelikle güçlü değilmiş gibi gözüken bağların farklı alanlarda kuvvetli olabileceklerine de değinilmektedir. (Gençlik ve Spor Bakanlığı, 2013, s. 25)

1.1.Sosyal Medya ile İlgili Tanımlar ve Kavramlar

Sosyal medya, tanımlanması zor bir kavram olarak karşımıza çıkmaktadır. Özel sektör firmaları, akademisyenler ve aynı zamanda kullanıcılar "sosyal medya" kavramını farklı şekillerde tanımlamaktadırlar. Tanımlamada karşılaşılan bu farklılaşmanın, sosyal medya şemsiyesi altında nelerin kapsanması gerektiğine karar verememekten ve de birbiriyle ilintili iki kavram arasındaki (Web. 2.0 ve Kullanıcı Tarafından Oluşturulmuş İçerik) ayrışmadan ileri geldiği görülmektedir. 2004 yılında ortaya çıkan Web 2.0 tanımını yaparken dikkat edilmesi gereken noktanın WWW'nin (World Wide Web) yani dünya çapında ağın, eskiden olduğu gibi yalnızca kişiler tarafından oluşturulan ve yayımlanan verilerin olduğu bir platform olmaktan çıkıp,

sürekli olarak kullanıcıların katılımıyla birlikte ortak çalışmaya dayalı olarak değiştirilen verilerin olduğu bir alana dönüşmesi olmuştur. Örneklendirmek gerekirse online olarak erişilebilir kişisel web sayfaları, ansiklopediler ve klasik anlamda kullanıcılar tarafından yayımlanan bilgiler Web 1.0 dönemine ait görülürken bunların yerini yeni dönemde bloglar, wikiler ve ortak olarak ortaya çıkartılmış projeler almaktadır. Bu bağlamda Web 2.0 fikirsel ve teknolojik anlamda oluşturulan alanı temsil etmekteyken, "Kullanıcı Tarafından Oluşturulmuş İçerik" ise internet kullanıcılarının sosyal medyadan yararlandıkları her şekli temsil ettiği belirtilmektedir (Gençlik ve Spor Bakanlığı, 2013, sf.25).

Bu tanımdan anlaşıldığı üzere interneti paylaşım ortamına çeviren "Web 2.0 akımı" sosyal ağları, iletişimi ve etkileşimi üst düzeye çıkarmıştır. Bu noktadan hareketle sosyal medyanın en belirli özelliği; veri yükleyeninin sadece kurum değil birey de olabilmesidir. Sosyal ağlarda yer alan sayfaların içerikleri yalnızca kurumlar tarafından değil kişinin kendisi tarafından da yüklenmekte, yönlendirilmekte ve yönetilebilmektedir. Ayrıca söz konusu içerik kesintisiz olarak güncellenebilmektedir.

Türk Dil Kurumu'nun Büyük Sözlüğü'nde "Sosyal Medya" kavramına dair henüz bir tanım bulunmamaktadır. Ancak hayatımıza nüfuz eden bu kavram üzerine birçok akademik çalışma gerçekleştirilmiş ve çeşitli sosyal medya tanımları yapılmıştır. Bu tezin ana konusu sosyal medya kavramı üzerine şekillendiği için bazı başka sosyal medya tanımlarına da yer verilmesi uygun görülmüştür.

Bireylerin sınırları belirlenmiş bir sistem içinde halka yarı/açık profil oluşturmasına, bağlantıda olduğu diğer kullanıcıların listesini açıkça vermesine, bu diğer kullanıcıların sistemdeki listelenmiş bağlantılarını görmesine ve aralarında gezmesine izin veren web tabanlı hizmetlerin tümüne "Sosyal Medya" denmektedir. (Büyükşener, 2009, sf.1)

Anthony Mayfield (2008), sosyal medya türlerini sosyal ağlar, bloglar, wikiler, podcastler, forumlar, içerik toplulukları ve mikrobloglar olmak üzere 6'ya ayırmaktadır. Sosyal ağlar insanların kişisel web siteleri kurarak, arkadaşlarıyla iletişim kurmalarına ve içerik paylaşmalarına olanak sağlamaktadır. Facebook,

MySpace, Wikipedia, Apple iTunes, YouTube, Twitter gibi internet siteleri sosyal ağlara örnek olarak gösterilebilmektedir. Mayfield'e göre sosyal medya insan olma özellikleriyle yakından ilişkilidir. Yazar sosyal medyayı düşünceleri paylaşmak, biraraya gelmek, ticaret yapmak, arkadaşlar aramak, tartışmalar yapmak gibi insani özelliklerin internete yansıması olarak görmekte ve çok hızlı bir şekilde yayılmasını da bu özelliğine bağlamaktadır. Teknolojilerin gelişmesiyle, dijital kameraların, fotoğraf makinelerinin ucuzlaması, hızlı internet erişiminin artması gibi bu alandaki maliyetlerin azalması ve kullanımın basitleştirilmesiyle insanlar kendi fotoğraflarından, videolarından, düşüncelerinden, sözlerinden kendi içeriklerini oluşturarak bunları yayabilme şansı elde etmiştir. Bu özellikleri sayesinde sosyal medya siteleri çok kısa süre içerisinde tüm küreye yayılmıştır (Başlar, 2013, s.4).

Araştırmalar sosyal medya tanımlanmasında farklı mecralar olduğuna işaret etmektedir. Örneğin, bloglar, şirketlerin başlattığı tartışma platformları, chat odaları, tüketiciler arasında e-postalar, tüketicilerin ürün değerlendirmeleri, internet üzerindeki tartışma platformları ve forumlar farklı mecralar olarak anlatılmaktadır. Ancak genel olarak sosyal medya mecralarının 5 ana başlık altında toplandığı görülmektedir. Bunlar; ortaklaşa yapılan projeler, bloglar, mikroblog siteleri, içerik grupları ve sosyal ağ siteleri olarak belirtilmektedir. (Gençlik ve Spor Bakanlığı, 2013, s. 25).

Sosyal paylaşım ağları ile sosyal medya kavramının yoğun bir şekilde birbirinin yerine kullanıldığı ve zihinlerde aynı algıyı yarattığı görülmektedir. Ancak, sosyal paylaşım ağları ve sosyal medya kavramları, sıklıkla birbirinin yerine kullanılması ve benzerlikler göstermesine rağmen, aralarında büyük farklar bulunduğu belirtilmektedir. Sosyal medyanın paylaşım ve tartışma için bir araç iken, sosyal paylaşım ağlarının ise aynı ilgi alanları ve hobilere sahip kişileri birbirlerine bağlayan bir yapı olduğu görülmektedir. Birinde yayılan bilgilerin geneli ilgilendirirken, diğeri üzerinden yayılan bilgilerin daha kişisel ve hedef odaklı olduğu belirtilmektedir (Gürses, 2013, s. 5-6).

Bu çalışmada “sosyal medya” kısaca kullanıcıların kendi ürettiği içeriği paylaştığı ve yayınladığı her türlü internet kökenli platformun genel adı olarak kullanılacaktır.

1.2. Sosyal Medyanın Tarihçesi ve Gelişimi

Sosyal medya kavramının tarihçesi incelendiğinde günümüzdeki hâline gelene kadar birçok farklı aşamadan geçtiği görülmektedir. İlk olarak 1979 yılında TomTruscott ve Jim Ellis'in dünyanın farklı yerlerindeki internet kullanıcılarının herkes tarafından görülebilen mesajlar atabilmelerine olanak sağlayan Usenet'i oluşturdukları belirtilmektedir. Ancak günümüzde kullandığımız anlamıyla sosyal medya kavramının, bundan yaklaşık 20 yıl önce Bruce ve Susan Albeson'un çevrimiçi olarak günlük tutan internet kullanıcılarını bir araya toplayan "Açık Günlük" (Open Diary) platformu ile başladığı söylenmektedir. Oluşturulan bu online alan ile birlikte "blog" kavramının ortaya çıktığı belirtilmektedir. "Weblog" kelimesinin ilerleyen tarihlerde "weblog" (biz blogluyoruz) olarak kullanılmasıyla birlikte, bu platform üzerinde yazan kişilerin "blogcu" (blogger) olarak anılmaya başlandığı görülmektedir (Gençlik ve Spor Bakanlığı, 2013 sf. 25-26).

Birçok kaynakta da Ward Christensen ve Randy Suess adındaki iki teknoloji tutkununun, 1978 yılında arkadaşları ile irtibat halinde kalmak için BBS isimli bir yazılımı geliştirmelerini sosyal medyanın başlangıcı olarak değerlendirilmektedir (Çile, 2012).

Dilmen ve Öğüt (2010)'e göre gerçek anlamda ilk sosyal paylaşım ağı 1995 yılında lise veya üniversite arkadaşlarını arayıp bulmak amacıyla kurulan Classmates.com sitesidir (Gürses, 2013, s.9).

1995 yılında ortaya çıkan MIRC programı sosyal medya alanında adeta bir devrim etkisi yarattığı görülmektedir. MIRC programının sohbet odaları vasıtasıyla takma isimler kullanarak tanımadığımız kişiler ile iletişim kurmamızı sağladığı görülmektedir. Kullanıcılar kendileri hakkında detaylı bir bilgi vermek zorunda değillerdir. Yine o dönemlerde ortaya çıkan ICQ programının da çok popüler bir sohbet programı olduğu belirtilmektedir. ICQ' da, programın bize verdiği kullanıcı numaraları bizim ICQ kimliğimizi oluşturmaktadır. Bu dönemler sosyal medyanın tam anlamı ile sanal olduğu dönemler olarak değerlendirilmektedir. Zira kendimiz hakkında gerçek bilgiler vermemiz gerekmemektedir (Çile, 2012).

Heidemann vd. (2012, s.3866-3878), 1997 yılında Andrew Weinreich tarafından kullanıcının kendi profilini oluşturabildiği ve arkadaşlarını listeleyebildiği SixDegrees.com sitesini ilk gerçek zamanlı sohbet imkânı sağlayan paylaşım ağı olarak dikkat çekici bulmaktadır. Sitenin bir yıl içerisinde 1 milyon kullanıcıya ulaşmış olmasına rağmen gerekli değişimi zamanında yapamadığından dolayı 2000 yılında kapandığı görülmektedir (Gürses, 2013, s.9).

1999 yılında Microsoft tarafından geliştirilen Messenger programının kullanıcılara gerçek isimlerini kullanabilecekleri bir platform sunduğu görülmektedir. Yani artık çevrimiçi iletişimin sanallıktan kurtularak, gerçekliğe dönüşmeye başladığı belirtilmektedir. Fakat bu gerçek kimliğe geçişin hızlı olmadığı ve insanların takma isim kullanma alışkanlıkları uzun bir süre daha devam ettirdiği dile getirilmektedir. 2003 yılında da iş dünyasının profesyonellerini bir araya getirmeyi hedefleyen LinkedIn'in kurulduğu görülmektedir. Bu platformun gerçek bilgiler ve isim isteyen bir yapı ile karşımıza çıktığı ve internet kullanıcılarının LinkedIn'e ilk başlarda oldukça uzak kaldığı belirtilmektedir. Ancak kullanıcıların LinkedIn sayesinde iş hayatları ve kariyerleri için neler yapabileceklerini anladıklarında, sitenin üye sayısının oldukça arttığı görülmektedir (Çile, 2012).

Boyd (2007), 2003 yılında ünlü olmayan müzik grupları ve şarkıcılar için kurulduğu düşünülen MySpace.com sitesini de yüksek hızlı çıkış yapan bir sosyal paylaşım ağı olduğu için önemli bulmaktadır. Ancak bilinenin aksine MySpace'in ilk kurulurken bunu hedeflemediği zaman içinde bu alana yöneldiği belirtilmektedir (Gürses, 2013,s.11).

2004 yılının sosyal medya için tam bir dönüm noktası olduğu dile getirilmektedir. Bu yıl içerisinde resim paylaşma ağı olan Flickr faaliyete geçmiştir. Artık sosyal paylaşımın sadece sohbet üzerine olmadığı, insanların resim, fotoğraf gibi materyalleri de paylaşabileceği kanıtlanmıştır. Flickr'ın oldukça başarılı bir proje olarak sosyal medya tarihine adını yazdırdığı görülmektedir. Yine aynı yıl içerisinde Mark Zuckerberg, Facebook'u kurmuştur. İlk başlarda tek bir üniversite için kullanımda olan sitenin, zamanla başka üniversitelere de yayıldığı belirtilmektedir. Gerek alt yapısı gerekse kullandığı teknoloji bakımından, o günkü rakiplerine göre

tartışılmaz seviyede başarılı olan sitenin hızla dünyaya yayıldığı görülmüştür. Kullanışlı bir ara yüze sahip olmasının internet kullanıcılarını kendisine çektiği belirtilmektedir (Çile, 2012).

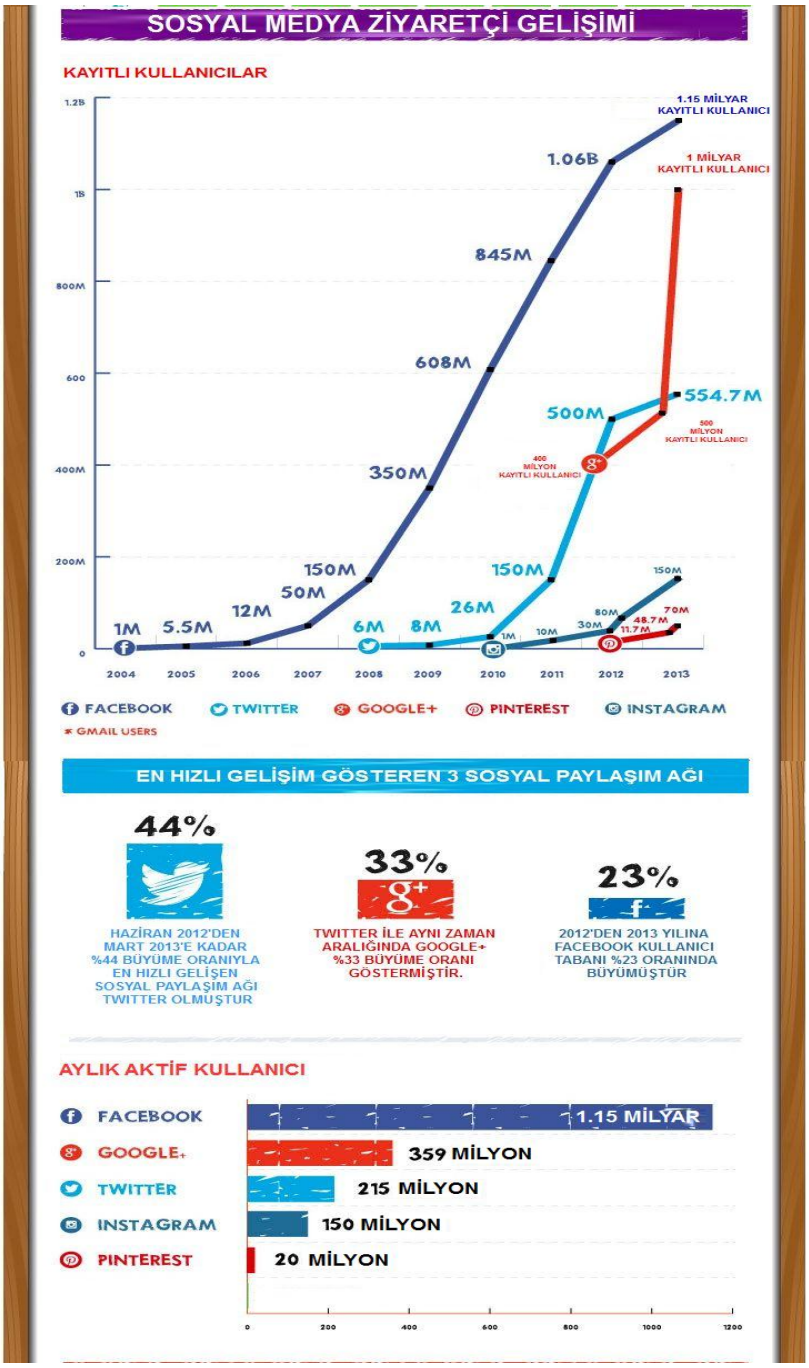
2005 yılında kurulan YouTube'un sosyal paylaşım mecrasının video ayağını oluşturarak, bu alana çok büyük bir katkı yaptığı görülmektedir. Google tarafından satın alınan sitenin, oldukça geliştirilerek başladığı günden bu yana dünyanın en popüler video platformu olmayı başardığı belirtilmektedir. 2006 yılında hayatımıza giren mikroblog sitesi Twitter'ın ise kısa zamanda kendi kültürünü oluşturduğu ve çok geniş kitlelere ulaştığı görülmektedir (Çile, 2012).

Örnekleri çoğaltılabilecek bu tür web siteleri sayesinde sosyal ağlara üye olan kullanıcıların sayısı giderek yükselmekte ve sosyal medya kavramı önemini arttırmaktadır. Dünyada bir milyardan fazla Facebook kullanıcısından bahsediliyorsa ve YouTube'da bir günde tam dört milyar video izleniyorsa ve her geçen saniye bu mecraya binlerce kişi katılıyorsa artık bambaşka bir iletişim evreninde olduğumuzu kabul etmemiz gerekmektedir.

Heidemann vd., (2012, s.3866-3878) özellikle Facebook ve Twitter'ın kullanıcılarına mümkün olduğunca fonksiyonellik sağlayarak kitlesini katladığına dikkat çekmiş ve günümüzün sosyal paylaşım ağı olarak milyarlarca insan tarafından kullanılmaya başlandığını belirtmiştir (Gürses, 2013, s.11) .

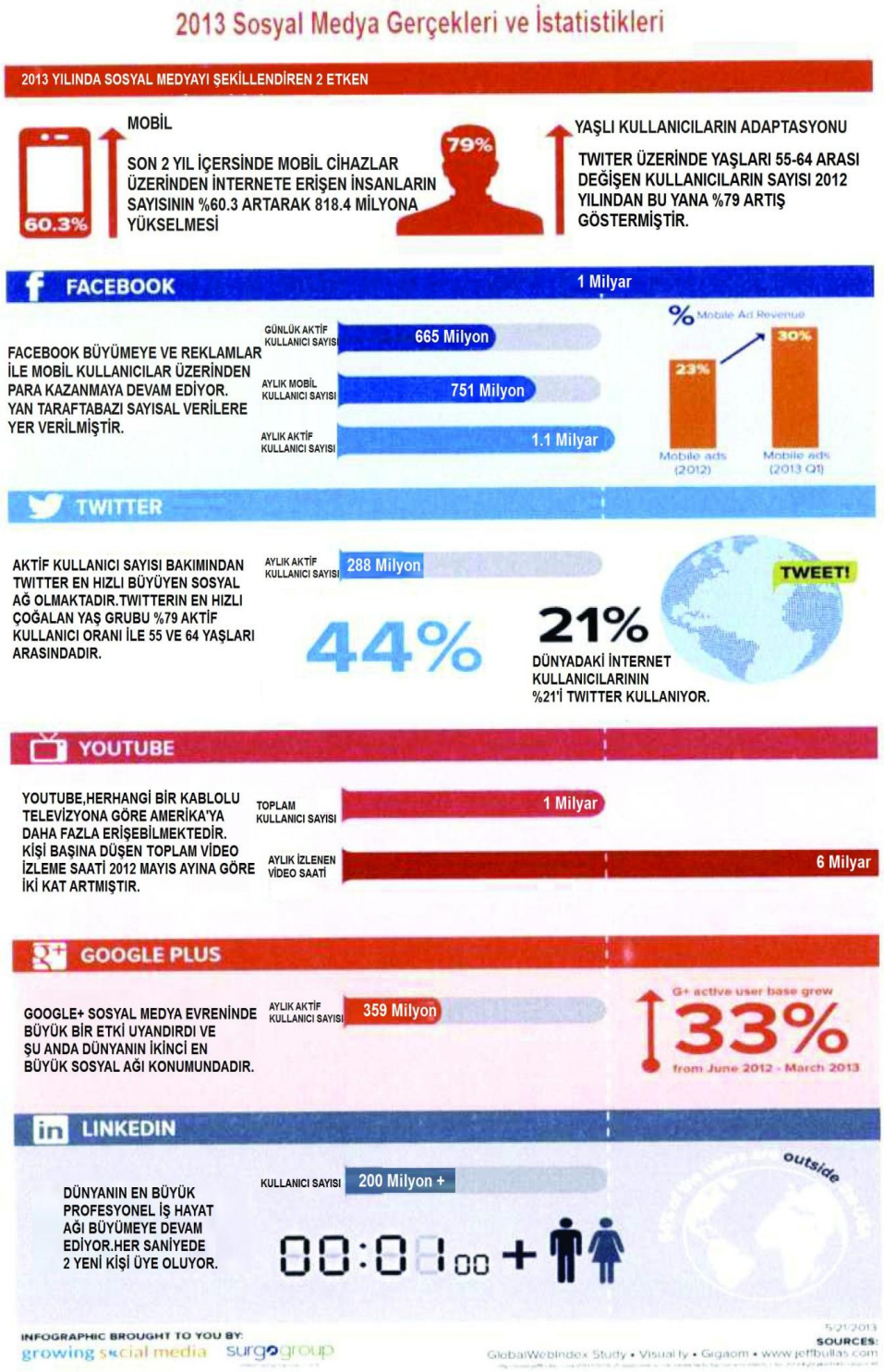
Bilinen en yaygın sosyal paylaşım ağlarının 2013 yılına kadar olan gelişimleri şekil 1.1 ve 1.2'de gösterilmektedir. Şekil 1.3.' de ise 2014 yılına ait güncel veriler bulunmaktadır.

Şekil 1.1. 2013 Yılı En Yaygın Sosyal Paylaşım Ağları- 1



Kaynak: Bullas, (The Growth Of Social Media,Temmuz 2014)

Şekil 1.2. 2013 Yılı En Yaygın Sosyal Paylaşım Ağları- 2



Kaynak: (Gürses, 2013)

Şekil 1.3. En Çok Kullanıcıya Sahip Sosyal Paylaşım Ağları 2014

Kaynak: Digital Insights, (Social-Media 2014 Statistics, Temmuz 2014)

1.3. Kitlesel Örgütlenmede Sosyal Medyanın Etkisi

Gerek ülkemizde örnekleri artarak görülen, gerekse dünyanın çeşitli bölgelerinde meydana gelen toplumsal hareketlerin eylem ve iletişim ortamı olması, sosyal medyanın önemini ve etkinliğini anlamamızı gerekli kılmaktadır.

Sosyal medya kullanımının yaygınlaşmasının ve kitlesel örgütlenmedeki etkisinin sorumluluk rejimine yeni bir boyut kazandırdığı dile getirilmektedir. Nihayetinde sosyal medya siteleri bireylere kendilerini ifade olanağı sağladığı gibi, farklı konumlardaki bireylerin hızlıca örgütlenmelerini, ortak bir payda altında ittifaklar kurmasını ve kitlesel tepki koymalarını sağladığı belirtilmektedir (Kaya).

Dünya siyaseti ve sosyal ağların kullanımı açısından 2010 yılının önemli bir dönüm noktası olduğu ve 2010 yılında Tunus, Mısır, Libya, Suriye, Bahreyn, Cezayir ve Ürdün gibi Arap ülkelerinde baş gösteren "Arap Baharı Olayları"nın sosyal medyanın kitlesel örgütlenmedeki rolünü ortaya çıkardığı belirtilmektedir (Babacan vd. 2012).

Bozkurt (2013) aşağıda yer alan değerlendirmesinde görüldüğü gibi, sosyal medyanın sivil toplumu organize ettiğini ifade etmektedir:

Dünya siyaseti ve sosyal ağlarının kullanımı açısından 2010 yılı önemli bir dönüm noktası oldu. Tunus'ta başlayıp Orta Doğu'yu önemli ölçüde etkileyen siyasi değişimlerinde sosyal medya, sivil toplumu organize etti, ortak hareket etmelerine zemin hazırladı ve kitleleri oldukça fazla etkiledi. Bu süreçte sosyal medya araçları kullanılarak atılan mesajlar, bir kartopu gibi büyüyerek insanları tetikleyip bir kelebek etkisi yarattı. Hatta kullanım kolaylığı ve etkili yayılımı nedeniyle bu ağlar, kullanıcılarına asimetrik bir güç kazandırdı.

Ortadoğu ve Kuzey Afrika'da başlayan halk hareketlerinin örgütlenme ve iletişim aracı olarak sosyal medya araçlarından yararlanılmasının ardından, yaşanan halk hareketlerine 'sosyal medya devrimi' gibi tanımlamaların yapılmasıyla, sosyal medyanın önemi ve etkisi tartışmasının artarak devam ettiği belirtilmektedir. İnsanların başta Facebook ve Twitter olmak üzere diğer toplumsal paylaşım ağları

yoluyla örgütlenerek toplantılar ve geniş katılımlı gösteriler organize ettikleri görülmektedir (Babacan vd. 2012, s15)

Washington Üniversitesi tarafından özellikle Tunus ve Mısır odaklı yapılan bir araştırmada, Facebook, Twitter, ve YouTube'da eşsiz bir veritabanı oluşturulduğu ve "Arap Baharı"nda sosyal medyanın kritik rol oynadığının kanıtladığı dile getirilmektedir (Bozkurt, 2013,s.51).

Papic ve Noonan (2011,s.166) Arap coğrafyasındaki halk hareketleriyle, sosyal medya ilişkisini bir sebep-sonuç ilişkisinden ziyade, sosyal medyayı yaşananlar bağlamında bir araç ve ortam olması bakımından ele almaktadır. Söz konusu halk hareketlerinin sosyal medyanın sunduğu özgür ortamdan dolayı olmadığı dile getirilmekte, sosyal medyanın toplumsal yaşanmışlığın dışa vurumu ve geniş kitlelere ulaştırılması anlamında bir araç işlevi gördüğü belirtilmektedir (Babacan vd. 2012, s.16).

Yapılan değerlendirmeden de görüldüğü üzere Arap Baharı Olayları gibi kitle hareketlerinin sebebinin sosyal medya olmadığı, sosyal medyanın katılım, örgütlenme ve paylaşılan içeriği geniş kitlelere ulaştırmada etkili bir araç olduğu ortaya koyulmaktadır.

2013 yılı Mayıs sonunda Türkiye'de cereyan eden "Gezi Parkı Olayları" diye adlandırılan kitle hareketleri de sosyal medyanın bahsettiğimiz örgütlenme etkisi için dikkat çekici bir örnektir.

Taksim Gezi Parkı eylemleri sürecinde sosyal medya kullanımı adeta bir patlama etkisi yapmıştır. Eylemlere katılmak isteyenler tarafından toplu hareket etmek ve bilgi akışını sağlamak için çok yoğun bir şekilde kullanılmıştır. Türkiye gerçek anlamda ilk kez sosyal medyanın gücüne ve yayılma etkisine bu olay ile şahit olmuştur.

Bu yayılmada, TV kanallarında eylemle ilgili yeterli ve ayrıntılı haberleri bulamayanların kapsamlı bilgiyi almak amacıyla sosyal medya sitelerine göz atmayı tercih etmesi ile özellikle sanat ve siyaset dünyasının ünlü isimlerinin eylemlerle ilgili paylaşımlarda bulunmasının büyük katkısı olduğu görülmektedir. 31 Mayıs

2013'te eylemlerin yoğunlaştığı saatlerde #direngeziparkı başlıklı twitterhashtag'i dünya listesinde popüler konularda (trendingtopics-TT) zirveye yerleştiği görülmektedir. Sosyal medyanın ciddi etkisini gören Türkiye'nin ilk defa "sanal olanın" etkisini derinden hissettiği belirtilmektedir. Sosyal medyanın paylaşım ve bilgi akışındaki yoğun kullanımı, "yalan haber", "provakatif bilgi" ve "enformasyon kirliliği" iddialarıyla birlikte bu alanın düzenlenmesi gerektiği tartışmalarını gündeme getirdiği görülmektedir (Bozkurt, 2013,s.52).

Kimi kesimler sosyal medya alanına kesinlikle müdahale edilmemesini dile getirirken, kimileri düzenlemelerin kısıtlama yönünde olmaması gerektiğini dile getirmiştir. Ancak ortada bir gerçek var ki o da sosyal medya etkilerinin tamamen kullanıcıların niyetine bağlı olduğudur. Çünkü kimi kullanıcılar gerçek dışı bir bilgiyle, iftirayla ya da içeriği değiştirilmiş maksatlı bir fotoğrafla kamuoyunu provoke edip çatışma iklimine sürükleyebilmektedir. Başkasının hesabını çalıp onun adına paylaşımlar yapabilmekte, birilerinin özel hayatının veya kişisel verilerinin gizliliğini ihlal edebilmektedir. Hatta devlet sırrı niteliğindeki bilgiler dahi bu tür sosyal medya siteleri aracılığıyla ifşa edilebilmektedir.

Babaoğlan (2013) aşağıda yer alan değerlendirmesinde görüldüğü gibi, sanal platformlarda yapabileceklerimizin sınırının olmadığını ifade etmektedir:

> Bulduğunuz yerin, yaşamakta olduğunuz zamanın ve en önemlisi gerçekte kim olduğunuzun hiç bir önemi olmayan bu sanal platformda yapabileceklerinizin sınırı net değildir. Bilgiyi üretmek ve çok hızlı yaymak bu yapı ile artık herkesin elindedir. Gerçek bir haberci olmanız, haber kaynağına ulaşmanız vs.. gibi kavramlara gerek bile yoktur. Sadece bir akıllı cihazınızın ve internet bağlantınızın olması yeterlidir.

Görüldüğü üzere sosyal medya ortamlarının hızlı ve kolay bilgi karmaşalarına ve hatalı yönlendirmelere açık olduğu dile getirilmektedir.

Aşağıda yer alan şekillerde "Gezi Parkı Olayları" süresince gerçek dışı bilgi ya da içeriği değiştirilmiş maksatlı fotoğraflara ve o fotoğrafların orijinal hallerine dair örnekler bulunmaktadır.

Şekil 1.4. Avrasya Maratonu Koşusunun Gezi Parkı Yürüyüşü Gibi Gösterilmesi

Kaynak: Yenişafak, 2013

Şekil.1.5. Panzerin Taksimde Vatandaşı Ezdiği İddiası

Kaynak: Yenişafak, 2013

Şekil 1.6. Türk Polisinin Köpeğe Dahi Biber Gazı Sıktığı İddiası

Provoke Amaçlı Fotoğraf **Fotoğrafın Orijinali**

Kaynak: Yenişafak, 2013

Görüldüğü üzere günümüz teknolojisinin geldiği noktada örneklerdeki gibi gerçekdışı içerikler üretmek çok kolaylaşmıştır.

II. AVRUPA BİRLİĞİ'NİN İNTERNET VE SOSYAL MEDYAYA İLİŞKİN DÜZENLEMELERİ

Avrupa Birliğine katılmaya aday olan her ülkenin dolayısıyla Türkiye'nin de tam üyelik için Kopenhag Kriterlerini yerine getirmesi gerektiği bilinmektedir. Kopenhag Kriterlerinin en önemlisinin de "Acquis Communautaire" denilen Avrupa Birliği Müktesebatının üstlenilmesi yani aday ülkelerde bulunan mevcut düzenlemelerin Avrupa Birliğindeki düzenlemelerle uyumlaştırılarak bir standart sağlanması olduğu belirtilmektedir (Nizam, 2009,s.1).

Türkiye için 39 ana başlıkta düzenlenen Avrupa Birliği Müktesebatı başlıklarından birisinin de "Telekomünikasyon ve Bilişim Teknolojileri Politikası" (Telecommunication and Information Technologies Policy) adıyla düzenlenmiş olduğu görülmektedir (Nizam, 2009, s.1).

Nizam'a göre Avrupa Birliği Bilişim Politikasının telekomünikasyon ile birlikte anılmasının sebebi birlik bünyesinde telekomünikasyonun bireysel haberleşmenin ötesinde bilişim toplumunun temel altyapısını oluşturması felsefesidir ve bu felsefeye dayanarak Avrupa Birliği Bilişim Politikasının temellerini aşağıdaki belgeler oluşturmaktadır;

- Telekomünikasyon ve Bilişim hizmetleri ve araçları için ortak bir iç pazar oluşturulmasını öngören 1987 tarihli Yeşil Kitap,
- Sektörün eşitlikçi bir şekilde düzenlenmesini ve liberalleşmesini öngören 1998 Avrupa Birliği Düzenleyici Çerçevesi
- 13 Aralık 1999 tarihli Elektronik İmza için Topluluk çerçevesini oluşturan Avrupa Parlamentosu ve Konsey Direktifi
- 23-24 Mart 2000 Lizbon Zirvesi ile başlatılan "e-Avrupa Hareketi"
- 15-16 Haziran 2001 Göteborg Zirvesinde kabul edilen "e-Avrupa+ Hareket Planı"
- 29 Haziran 2001 tarihinde Strasbourg'ta kabul edilen "Avrupa Siber Suçlar Konvansiyonu"

Ayrıca bunların yanı sıra Avrupa Birliği tarafından kişisel verilerin korunması ve siber güvenliğin sağlanması başta olmak üzere, bilgi güvenliğinin sağlanması için birçok direktif ve tavsiye kararı hazırlandığı görülmektedir (Henkoğlu ve Yılmaz, 2013, s.9).

Henkoğlu ve Yılmaz (2013), 24 Ekim 1995 tarih ve 95/46/EC sayılı AB direktifinin; AB'nin veri koruma hukukunda temel direktifi olduğunu belirtmektedir. Ayrıca söz konusu direktifin, 97/66/EC sayılı direktif ile 95/46/EC sayılı direktifin telekomünikasyon alanındaki tamamlayıcısı olduğunu belirterek bilgi güvenliği ile ilgili konuları içeren temel AB direktifleri ve tavsiye kararlarını şu şekilde sıralamışlardır;

- Bilgi Güvenliği Alanındaki 92/242/EEC Sayılı Karar
- Kişisel Verilerin İşlenmesi ve Kişisel Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayılı Direktif
- 97/66/EC Sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi
- 2000/31/EC Sayılı Elektronik Ticaret Direktifi
- 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi
- 1151/2003/EC Sayılı Yasadışı ve Zararlı İçerikle Geniş Ağ Üzerinde Mücadele Kararı
- 854/2005/EC Sayılı Güvenli İnternet Kullanımına Geçiş Kararı
- 2006/24/EC Sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif

AB bilgi güvenliği politikalarına ışık tutan önemli belgelerden biri de "Yeşil Kitap (Green Paper)" olarak görülmektedir. Söz konusu kitabın; AB Komisyonu tarafından belirli bir konuyu tüm AB genelinde tartışmaya açmak ve alınan fikirlerle konunun

olgunlaşmasını sağlamak için yayımlandığı ve hukuki bağlayıcılığı bulunmadığı belirtilmektedir (Henkoğlu ve Yılmaz, 2013, s.9-10).

Çalışma konusu kapsamında bu belgeler arasından 2001 yılında kabul edilen "Avrupa Siber Suçlar Konvansiyonu" ya da diğer adıyla "Avrupa Siber Suçlar Sözleşmesi" büyük önem arz etmektedir.

Avrupa Komisyonu tarafından bu alana yönelik yapılan düzenlemelerin AB üye ülkelerinin yanı sıra, evrensel düzenlemelerle de paralellik göstermekte olduğu ve internet suçlarına genel yaklaşımı ortaya koyduğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Avrupa Komisyonu'nun 1996 yılında yayımladığı bu alandaki ilk düzenleme olan 487 sayılı İnternet Üzerinden Yasadışı ve Zararlı İçeriğe İlişkin Tebliğinde (COM/96/487) ve Avrupa Komisyonu'nun "İnternetin Yasadışı ve Zararlı Kullanımı Çalışma Grubu-1" raporunda, internetin ortaya çıkardığı olumsuzluklara ilişkin olarak bir sınıflandırma yapıldığı ve suç potansiyeli barındıran alanların 8 sınıfa ayrıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013). Bunlar;

- Ulusal güvenliği tehdit eden internet yayınları (terörist faaliyetlere altyapı sunması vb)
- Küçüklerin fiziki, ahlaki ve zihinsel gelişmelerini olumsuz etkileyen yayınlar
- İnsan onurunu tehdit eder nitelikte yayınlar (ırk, cinsiyet, milliyet ayrımı)
- Ekonomik olumsuzluklar (kredi kartı, banka bilgilerinin çalınması)
- Bilgi gizliliğine yönelik olumsuzluklar
- Özel hayatın gizliliğine yönelik olumsuzluklar
- Kişi saygınlığına yönelik olumsuzluklar
- Telif hakları ihlalleri

İnternet düzenlemelerine ilişkin AB Müktesebatının, hukuka aykırı içerik ile zararlı içerik arasında bir ayrım yaptığı görülmektedir. Hukuka aykırı içerik, ulusal kanunların suç saydığı unsurların internet yayınları içerisindeki varlığını ifade ederken, zararlı içerik, ebeveynlerin çocuklarının internette ulaşmalarını istemeyecekleri içerik olarak tanımlanmaktadır (Avrupa Birliği Bakanlığı, 2013).

Avrupa Birliği; özgürlük, temel haklar, demokrasi ve hukukun üstünlüğü gibi değerlerin ve normların, gerçek hayatta korunduğu gibi internet ve sosyal medya alanında da aynen korunması gerektiğini belirtmektedir. Söz konusu alandaki özgürlüğün güvenlik tedbirleriyle teminat altına alınması gerektiği ve kötü amaçlı etkinliklerden, istismardan korunması vurgulanmaktadır (Avrupa Birliği Bakanlığı, 2013).

2.1. Avrupa Konseyi Siber Suçlar Sözleşmesi ve Ek Protokol

Uluslararası bilişim suçları ve bilgi güvenliği politikaları ile ilgili olarak Avrupa Konseyi tarafından hazırlanan en önemli hukuki belgelerden biri 185 sayılı Siber Suçlar Sözleşmesi (SSS) olarak kabul edilmektedir (Henkoğlu ve Yılmaz, 2013, s.12).

Siber suç olgusuyla mücadele etmek bakımından en önemli husus, uluslararası adli yardımlaşma olarak düşünülmektedir. Bunun bilincinde olan ülkeler, uluslararası örgütler ve sivil toplum kuruluşları, toplu ve standartlaşmış bir mücadeleyi mümkün kılmayı amaçlayan sayısız girişimlerde bulunmuşlardır. Bu girişimlerden en önemlisi, Avrupa Konseyi bünyesinde kabul edilen 2001 tarihli Siber Suç Budapeşte Sözleşmesi ya da diğer adıyla Avrupa Konseyi Siber Suçlar Sözleşmesi olarak görülmektedir (Önok, 2013, s.1232).

AB ve hatta dünya genelinde "sosyal medya mecralarının kullanımı" değil de "siber suç" konusu genel olarak ele alındığında, bu konuyu düzenleyen söz konusu sözleşmenin getirdiği en büyük unsur olarak; ortak bir siber suç tanımı yapması ve bu suçların sözleşmeye taraf ülkelerde cezaya tabi olduğunu hüküm altına alması görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Sözleşme'nin ortaya çıkışı, Suç Sorunlarına Dair Avrupa Komitesi'nin (SSAK-European Committee on Crime Problems) 1996' da, Avrupa Konseyi'ne siber suçlara ilişkin bir komite kurmasını tavsiye etmesine dayanmaktadır ve bu öneriye uygun olarak, Şubat 1997'de "Siber-uzay Suçları Uzman Komitesi" (Committee of Experts on Crime in Cyber-space) kurulduğu görülmektedir (Önok, 2013,s.1241).

Söz konusu komitenin dört yıl boyunca sözleşme tasarısını hazırladığı ve nihai tasarının Haziran 2001'de SSAK tarafından onaylandığı belirtilmektedir. Daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 8 Kasım 2001'de kabul edilen ve 23 Kasım 2001'de Budapeşte'de devletlerin imzasına açılan Siber Suç Sözleşmesi, 1 Temmuz 2004'te yürürlüğe girmiş olup bu alandaki ilk uluslararası antlaşma olmuştur (Önok, 2013, s.1241).

Bozkurt (2010), 2004 yılında yürürlüğe giren ve sonradan Türkiye'nin de katıldığı ve içinde ABD, Japonya, Kanada, Güney Afrika, Avrupa Konseyi üyeleri ve diğer Avrupa ülkeleri olmak üzere 47 ülke tarafından imzalanan Siber Suçlar Sözleşmesinin; bilgi merkezlerini ve bireyleri korumayı hedef almakta ve zararlı kodların üretilmesi/dağıtılması konusunda uluslararası bir çerçeve oluşturduğunu belirtmektedir (Henkoğlu ve Yılmaz, 2013, s.12).

Türkiye'nin de imzaladığı ancak henüz yürürlüğe koymadığı bu sözleşme bilgisayar ve internet suçlarına ilişkin ulusal mevzuatların uyumlulaştırılarak bu konu hakkındaki uluslararası işbirliğinin arttırılmasını amaçlamaktadır (Avrupa Birliği Bakanlığı, 2013).

Roscini (2010), sözleşmenin aynı zamanda, yetkisiz erişim ve fikri mülkiyet hakları ile ilgili düzenlemeler içerdiğini de belirtmektedir. Ayrıca sözleşmenin bilgi güvenliği politikaları açısından; içeriğinde yasal düzenlemeler, alınacak teknik önlemler ve uluslararası işbirliği seçenekleriyle birlikte sunulmasını en önemli özelliği olarak görmektedir (Henkoğlu ve Yılmaz, 2013, s.12).

28.1.2003 tarihinde bilgisayar sistemleri aracılığıyla işlenen, ırkçı ve yabancı düşmanlığı güden nitelikli eylemlerin cezalandırılmasını düzenlemek amacıyla Strazburg'da Siber Suç Sözleşmesine ek bir protokolün kabul edildiği görülmektedir.

Bu konunun ayrı bir protokol ile düzenlenmesinin sebebi; bazı devletlerin ifade özgürlüğünün kısıtlanmasına dönük endişeleri sebebiyle, ırkçılık ve yabancı düşmanlığının bilişim sistemleri aracılığıyla işlenmesinin cezalandırılması konusunda uzlaşı sağlamaması olarak belirtilmektedir (Önok, 2013, s.1242).

Türkiye'nin Siber Suçlar Sözleşmesini 2011 yılında imzaladığı, fakat ek protokolü daha imzalamadığı görülmektedir (Henkoğlu ve Yılmaz, 2013, s.12).

Henkoğlu ve Yılmaz (2013), aşağıdaki değerlendirmede de görüldüğü üzere Türkiye'nin sözleşmenin yaptırım gücünden faydalanabilmesi için, sözleşmeyi iç hukukuna uyarlaması gerektiğini ifade etmektedir:

Türkiye'nin sözleşmenin yaptırım gücünden faydalanabilmesi için, sözleşmeyi iç hukuka uyarlaması ve TBMM onayından geçirmesi gerekmektedir. SSS'nin iç hukuka uyarlanarak yürürlüğe girmesi, emniyet teşkilatları arasında bilgi alışverişine imkân tanıması yönüyle de önemlidir. Fakat bu konuda yapılacak çalışmalar, "Kişisel Verilerin Korunması" kanunu ile ilgili çalışmalarla birlikte yürütülmelidir. Çünkü iç hukukunda kişisel verilerin korunması hakkında düzenlemeye sahip olmayan ve kişisel verilerin hangi şartlarda paylaşılacağını belirlemeyen ülkeler; SSS'yi uygulamaya başladıklarında, bireylerin kişisel verilerini sözleşmeyi onaylayan diğer ülkelerle paylaşmak zorunda kalmaları söz konusu olabilecektir.

Önok (2013, s.1242), aşağıdaki maddelerde görüldüğü üzere Budapeşte Sözleşmesi'nin başlıca üç amacı olduğunu belirtmektedir. Bunlar;

1) Bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını mümkün kılmak.

2) Siber suçların soruşturulması açısından, bilişim ortamına uygun düşen ortak yetkileri tanımlayarak, devletler arasındaki muhakeme kurallarının yeknesaklaştırılmasını mümkün kılmak.

3) Hem geleneksel hem de yeni türden uluslararası işbirliği yöntemlerini belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını mümkün kılmak.

Söz konusu sözleşmenin belli ortak tanımlar ve suç tipleri belirleyerek yargı denetimi bakımından bir uyum düzeyi yakalanmasına yardımcı olduğu ve internet suçlarında ortak bir tutumun benimsenmesi durumunda siber suçlarla istenilen düzeylerde baş edilebileceği öngörülmektedir (Avrupa Birliği Bakanlığı, 2013).

Yine sözleşmenin getirdiği en büyük yeniliklerden biri olarak; siber suçlar üzerine ortak tanımlar getirmesi görülmektedir ve bu suçlara Maddi Ceza Hukuku başlığını taşıyan Sözleşme'nin 2. Bölüm, 1. Kısmı'nda değinilmektedir (Avrupa Birliği Bakanlığı, 2013, s.18). Bunlar;

Başlık 1 - Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar:

- Yasadışı Erişim
- Yasadışı Müdahale
- Verilere Müdahale
- Sistemlere Müdahale
- Cihazların Kötüye Kullanımı

Başlık 2 - Bilgisayarla İlişkili Suçlar

- Bilgisayarla İlgili Sahtecilik Fiilleri
- Bilgisayarla İlgili Dolandırıcılık Fiilleri

Başlık 3 - İçerikle İlişkili Suçlar

- Çocuk Pornografisi ile İlişkili Suçlar

Başlık 4 - Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar

- Telif Haklarının ve Benzer Hakların İhlaline İlişkin Suçlar

Ayrıca Sözleşme'nin 11. maddesinde bu suçlara kasıtlı olarak yardım ve yataklık edilmesinin de ulusal mevzuat kapsamında bir suç olarak tanımlanması gerektiğine işaret edilmektedir (Avrupa Birliği Bakanlığı, 2013).

Helvacıoğlu (2004), söz konusu sözleşmenin 4. maddesinde belirtilen veriyi bozma, değiştirme ve silme işleminin haksız, bilerek ve isteyerek gerçekleştirilmiş olması durumunda; 5. maddesinde ise, bilişim sistemine veri ilâve edilmesi, verilerin silinmesi, bozulması, değiştirilmesi ve başka bir yere aktarılması durumlarında yaptırıma tabi tutulduğunu belirtmiştir (Henkoğlu ve Yılmaz, 2013, s.12).

Sözleşmeye taraf olan ülkelerin iç hukuklarında sözleşmeye uygun olarak söz konusu suçlar için çeşitli yaptırımlar getirdiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Siber Suçlar Sözleşmesinin çalışmamız ile kesiştiği en önemli nokta yukarıda bahsettiğimiz "Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanıma Açık Bulunmasına Yönelik Suçlar" başlığı altındaki suçlardır.

Bu bağlamda özellikle Avrupa Birliğinde Kişisel Verilirin Güvenliği konusu derinlemesine irdelenecek ve başka bir ana başlıkta bazı belli başlı Avrupa Birliği ülkelerinden detaylı örnekler verilecektir.

2.2. Avrupa Birliği ve Avrupa Konseyi'nde Kişisel Verilerin Korunması

Kalkınma Bakanlığı (2013), Birleşmiş Milletler, OECD, APEC ve Avrupa Konseyi olmak üzere, pek çok uluslararası kuruluşun kişisel verilerin korunmasına yönelik önemli çalışmalar yürüttüğünü ve kişisel verilerin korunması konusunda temel oluşturacak belgeler hazırladığını belirtmektedir (Gürses, 2013, s.67).

Avrupa Komisyonu (1981), veri koruma alanında Avrupa Konseyi tarafından imzaya açılan ilk uluslararası hukuk düzenlemesi olarak, 1981 yılında yapılan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkındaki Sözleşme"sini dile getirmektedir. Söz konusu sözleşme ile sözleşmeyi imzalayan ülkelerdeki gerçek kişilerin, temel hak ve özgürlüğü ve kişisel nitelikteki verileri yasal olarak güvence altına alınmaya çalışılmaktadır ve sözleşmede yer alan

kişisel nitelikteki verilerin tanımının günümüzde de geçerliliğini sürdürdüğü görülmektedir (Henkoğlu ve Yılmaz, 2013, s.11).

Ayrıca 108 sayılı sözleşmede yer alan bireylerin hak ve özgürlükleri ve kişisel mahremiyet hakkındaki esasların, 1995 yılında 95/46/EC sayılı AB direktifi ile genişletildiği belirtilmektedir (Henkoğlu ve Yılmaz, 2013).

Kişisel Verilerin İşlenmesi ve Bu Tür Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayı ve 24/10/1995 Tarihli Avrupa Birliği Yönergesi'nde kişisel nitelikli verinin tanımı şu şekilde yapılmaktadır; *"Kişisel nitelikli veri, belirli ya da belirlenebilir gerçek kişilere ait bütün bilgileri ifade eder; bir gerçek kişinin belirlenebilir olması, özellikle şifre numarasına göre ya da psişik, psikolojik, fiziksel, ekonomik, kültürel veya sosyal benliği ifade eden bir veya birden fazla unsura aidiyeti aracılığı ile doğrudan veya dolaylı olarak teşhis edilebilmesi anlamına gelmektedir "* (Koç,2013,s.47-48).

Şahin (2011), kişisel verilerin korunması konusunda en geniş yasal altyapı olarak Avrupa Birliği tarafından; 1995 yılında yayınlanan 95/46/EC sayılı Veri Koruma Direktifi'nin yanı sıra; 2002 yılında yayınlanan 2002/58/EC sayılı E-Gizlilik Direktifi'nin, 2006 yılında yayınlanan 2006/24/EC sayılı Veri Saklama Direktifi'nin, ve 2009 yılında yayınlanan 2009/136/EC sayılı Vatandaş Hakları Direktifi'nin düzenlemelerine de dikkat çekmiştir (Gürses, 2013, s.70).

Ayrıca 2001 yılında 108 sayılı sözleşmeye ek olarak; "Denetleyici Makamlar ve Sınır ötesi Veri Akışına İlişkin Protokol" adıyla bulut bilişim hizmetlerini de yakından ilgilendiren 181 sayılı Ek Protokol'ün kabul edildiği belirtilmektedir (Henkoğlu ve Yılmaz, 2013,s.12).

108 sayılı sözleşme ve 181 sayılı protokolü imzalayan 46 ülkeden Türkiye ve Rusya olmak üzere 2 tanesi hariç tüm ülkelerin, iç hukuklarında kişisel verilerin korunması için uygulamaya başladıkları görülmektedir (Henkoğlu ve Yılmaz, 2013). Türkiye'nin 1981 yılında sözleşmeyi imzaladığı fakat daha onaylamadığından dolayı Türkiye'de kişisel verilerin korunmasına ilişkin henüz açık ve yeterli bir yasa ve veri

işlemlerini kontrol edecek, denetleyecek bir kuruluş mevcut olmadığı belirtilmektedir (Gürses, 2013,s.69) .

Şimşek (2001), ayrıca söz konusu belgede üye devletlerin veri işlem faaliyetleri sırasında bireylerin özel yaşamlarını korumaları ve riayet etmeleri yükümlülüğüne de dikkat çekmektedir (Koç, 2013, s.48).

Civelek (2011)'ten alınan aşağıdaki tabloda Avrupa Konseyi Üyesi olan bazı ülkelerin "Karşılaştırmalı Hukukta Kişisel Verilerin Korunması" bilgileri yer almaktadır (Gürses, 2013, s.70-76).

Tablo 2.1. Karşılaştırmalı Hukukta Kişisel Verilerin Korunması/Avrupa Konseyi Ülkeleri

Devlet	108 Sayılı Sözleşme		İlgili Ulusal Mevzuat	Kayıt veya Bildirim	Veri Koruma Otoritesi
	İmza Tarihi	Onay Tarihi			
Arnavutluk	14.02.2004	09.06.2004	9887 Sayılı Kişisel Verilerin Korunması Hakkında Kanun, 2008	Yok	Veri Koruma Komiseri
Ermenistan					
Avusturya**	28.01.81	30.03.88	Kişisel Verilerin Korunmasına İlişkin Kanun	Tüm Veriler	Veri Koruma Komisyonu
Azerbaycan			Veri, Veri İşleme ve Veri Koruma Hakkında Azerbaycan Cumhuriyeti Kanunu		
Belçika**	07.05.82	28.05.93	-Kişisel verilerin Korunması Kanunu -95/46 Sayılı VKD'nin Uygulanmasına İlişkin Kanun-Kişisel Verilerin Korunması Kararnamesi	Tüm Veriler	Mahremiyet Koruma Komisyonu
Bosna Hersek	02.03.2004	-	Kişisel verilerin Korunması Kanunu	-	Veri Koruma Komisyonu
Bulgaristan	02.06.1998	18.09.2002	Kişisel verilerin Korunması Kanunu	Tüm Veriler	Kişisel Verilerin Korunması Komisyonu
Hırvatistan	05.06.2003	21.06.2005	Kişisel verilerin Korunması Kanunu	Tüm Veriler (Önemli	Kişisel Verilerin Korunma Ajansı

				İstisnalar)	
Güney Kıbrıs Rum	**25.07.86**	**21.02.02**	**Kişisel Verilerin İşlenmesi(Bireylerin Korunması)Kanunu,2001**	**Bazı Verileri**	**Kişisel Verileri Koruma Komitesi**
Almanya**	**28.01.81**	**19.06.85**	**Federal Veri Koruma Kanunu(95/46 Sayılı VKD'nin Uygulanmasına Yönelik)**	**Bazı Verielr**	**Federal Veri Koruma Komiseri**
Yunanistan**	**17.02.83**	**11.08.95**	**1997 Tarihli ve 2472 Sayılı Kişisel Verilerin İşlenmesi ile İlgili Bireyin Korunması Hakkında Kanun -Kişisel Verilerin ve Mahremiyetin Elektronik Haberleşme Sektöründe Korunması ve 2472/1997 Sayılı Kanunu Değiştiren Kanun**	**Tüm Veriler**	**Kişisel Veri Koruma Kurumu**
Macaristan	**13.05.93**	**08.10.97**	**LXIII Sayılı Kişisel Verilerin Korunması ve Kamuyu İlgilendiren Bilgilerin Açıklanması Hakkında Kanun**	**Tüm Veriler**	**Veri Koruma Ombudsmanı**
İzlanda	**27.09.82**	**25.03.91**	**Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunmasına İlişkin Kanun**	**Tüm Veriler**	**Kişisel Veri Koruma Kurumu**
İrlanda*	**18.12.86**	**25.04.90**	**1988 Tarihli Veri Koruma Kanunu(2003'te Değişti)**	**Bazı Veriler**	**Veri Koruma Komiseri**
İtalya**	**02.02.83**	**29.03.97**	**196/2003 Sayılı Kişisel Veri Koruma Kanunu**	**Bazı Veriler**	**Kişisel Verileri Koruma Kurumu**
Letonya	**31.10.2000**	**30.05.2001**	**Kişisel Veri Koruma Kanunu**	**Bazı Veriler**	**Devlet Veri Denetim Otoritesi**
Lihtenştayn	**02.03.2004**	**11.05.2004**	**-Veri Koruma Kanunu,2002 -Veri Koruma Üzerine 9 Temmuz 2002 Tarihli Yönetmelik**	**Bazı Veriler**	**Veri Koruma Komiseri**
Litvanya	**11.02.2000**	**01.06.2001**	**Kişisel Verilerin Yasal Olarak Korunması Hakkında Kanun**	**Bazı Veriler**	**Devlet Veri Denetim Otoritesi**

Lüksemburg	**28.01.81**	**10.02.88**	**Kişisel Verilerin İşlenmesi Halinde Bireyin Korunması Hakkında Kanun -Telekomünikasyon Kanunu**	**Tüm Veriler (İstisnaları Var)**	**Veri Koruma Ulusal Komisyonu**
Malta	**15.01.2003**	**28.02.2003**	**Veri Koruma Kanunu, 2001**	**Tüm Veriler**	**Veri Koruma Komiseri**
Moldova	**04.05.98**	**28.02.08**	**-**	**-**	**-**
Monako	**01.10.08**	**24.12.2008**	**İsimsel Bilginin İşlenmesi Hakkında Kanun**	**Tüm Veriler**	**-**
Karadağ	**06.09.2005**	**06.09.2005**	**-**	**-**	**-**
Hollanda**	**21.01.88**	**24.08.93**	**Kişisel Veri Koruma Kanunu**		**Veri Koruma Komisyonu**
Norveç	**13.03.81**	**20.02.84**	**Kişisel Veri Kanunu**	**Tüm Veriler**	**Veri Müfettişliği**
Polonya	**21.04.99**	**23.05.2002**	**Kişisel Verilerin Korunması Hakkında Kanun**	**Bazı Veriler**	**Kişisel Veri Koruma Genel Müfettişliği**
Portekiz**	**14.05.81**	**02.09.93**	**Kişisel Verilerin Korunması Kanunu(95/46 Sayılı VKD'nin Uygulanmasına İlişkin)**	**Bazı Veriler**	**Ulusal Veri Koruma Komisyonu**
Romanya	**18.03.97**	**27.02.02**	**Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında 677/2001 Sayılı Kanun 102/2005 ve 506/2004 Sayılı Kanunlar**		**Kişisel Verilerin İşlenmesinin Denetlenmesi Hakkında Ulusal Otorite**
Rusya	**07.11.2001**				
San Marino			**Sayısallaştırılmış Kişisel Verilerin Toplanması, İşlenmesi ve Kullanılması Hakkında Kanun**	**Tüm Veriler**	**Gizli ve Kişisel Verilerin Korunmasından Sorumlu Garantör**
Sırbistan	**06.09.2005**	**06.09.2005**	**Kişisel Veri Koruma Kanunu**		
Slovakya	**14.04.2000**	**13.09.2000**	**Kişisel Veri Koruma Kanunu**	**Bazı Veriler**	**Slovak Cumhuriyetini ve Kişisel Verileri Koruma Ofisi**
Slovenya	**23.11.93**	**27.05.94**	**Kişisel Veri Koruma Kanunu**	**Tüm Veriler**	**Bilgi Komiserliği**

İspanya**	**28.01.82**	**31.04.84**	**Kişisel Verilerin Korunması Hakkında 15/99 Sayılı Kanun**	**Tüm Veriler**	**Veri Koruma Ajansı**
İsveç**	**28.01.81**	**29.09.82**	**Kişisel Veri Kanunu**		**Veri Teftiş Kurulu**
Makedonya	**24.03.2006**	**24.03.2006**	**Kişisel Veri Koruma Kanunu**		**Kişisel Veri Koruma Müdürlüğü**
Türkiye	**28.01.81**				
İsviçre	**02.10.97**	**02.10.97**	**Federal Veri Koruma Kanunu Yönetmelikler: OLPD,OALSP**	**Bazı Veriler**	**Federal Veri Koruma ve Bilgi Komiseri**
Ukrayna	**29.08.2005**		**Bilgi ve Telekomünikasyon Sistemlerinde Ukrayna Veri Koruma Kanunu,2006 Kişisel Verilerin Korunması Hakkında Taslak Kanun, 09.01.2007**		
İngiltere**	**02.10.97**	**02.10.97**	**Veri Koruma Kanunu**		

Kaynak: Gürses, (2013)

Yukarıdaki tabloda da görüldüğü üzere Türkiye'nin Avrupa Konseyine Üye Olan ülkeler gibi doğrudan kişisel verileri korumaya yönelik kanunu bulunmamaktadır.

2.3. Avrupa Ağ ve Veri Güvenliği Ajansı (ENISA)

Avrupa Birliği içinde özel bir görevi yerine getirmek, belirli bir alandaki sorunlara çözüm aramak ve kurumlar arasında koordinasyonu sağlamak amacıyla tüzel kişiliğe sahip ajanslar oluşturulmaktadır ve merkezi Yunanistan'da bulunan ENISA (European Network and Information Security Agency), AB içinde ağ ve bilgi güvenliğinin sağlanması amacıyla kurulan önemli bir uzmanlık kuruluşu olarak tanımlanmaktadır (Henkoğlu ve Yılmaz,2013, s.13).

Avrupa Ağ ve Veri Güvenliği Ajansı'nın 2004 yılında 5 yıllığına EC/460/2004 Sayılı Tüzük ile kurulduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013, s.20).

ENISA'nın AB çatısı altındaki tüm kurum ve kuruluşların ağ ve bilgi güvenliği konusunda bilgi paylaşımında bulunduğu bir merkez statüsünde olduğu ve asıl sorumluluğunun, AB içinde en üst seviyede ve en etkin şekilde ağ ve bilgi güvenliğini sağlamak olduğu belirtilmektedir (Henkoğlu ve Yılmaz, 2013,s.13).

ENISA'nın AB enstitüleri ve üye ülkelerle de işbirliği yaparak; AB içinde yer alan tüm kullanıcılar, çeşitli organizasyonlar ve iş dünyasıyla bilgi güvenliği kültürü oluşturduğu belirtilmektedir. Bulut bilişim alanında hem kamu kurumlarına, hem de özel sektör temsilcilerine yeni bilişim teknolojileri ve servislerine güvenli geçiş için rehberlik hizmeti sağladığı da görülmektedir. Ayrıca kurumlar arası koordinasyonu sağlama ve farkındalık çalışmaları yapmasının yanı sıra; kullanıcılara uyguladığı anketlerle mevcut durumun analizini de sık aralıklarla yaparak, yeni bilgi güvenliği politikalarının üretilmesine katkı sağladığı da belirtilmektedir (Henkoğlu ve Yılmaz, 2013, s.13).

Avrupa Birliği Bakanlığı'nın 2013 yılında yayınladığı rapora göre ENISA'nın temel amacı; AB düzeyinde ağ ve veri güvenliğinin arttırılması olarak tanımlanmaktadır ve Ajans, aşağıda sayılan konularda faaliyetler yürütmektedir:

- Avrupa Komisyonu'na ve üye devletlere bilgi güvenliği ile donanım ve yazılımların güvenliğine ilişkin özel sektörle iletişim hususlarında danışmanlık hizmetlerin verilmesi,
- AB'de karşılaşılan ağ ve veri güvenliği sorunlarına ilişkin verilerin toplanması, analizi ve muhtemel tehlikelerin belirlenmesi,
- Bilgi güvenliği sorunları ile başa çıkma kapasitesinin güçlendirilmesi için risk değerlendirme ve risk yönetme yöntemlerinin tanıtımının yapılması,
- Bilgi güvenliği alanındaki aktörlerin işbirliğini güçlendirme, bunlar arasında farkındalık yaratma, kamu-özel sektör ortaklığını destekleme faaliyetleridir.

Yukarıda bahsedilen çalışmaların yanı sıra; ENISA'nın AB içerisinde ve üye ülkelerde oluşturulan "Bilgisayar Olaylarına Müdahale Ekipleri" (Computer

Emergency Response Team, CERT) ile ortak çalışmalar yaptığı da görülmektedir (Henkoğlu ve Yılmaz, 2013, s.13).

2009 yılında faaliyetlerine son vermesi beklenilen ENISA'nın faaliyetlerine son verilmediği ve 2010 yılında alınan bir kararla faaliyetlerinin 3 yıl daha uzatıldığı ve en son 2013 Mayıs ayında Ajans'ın kurucu tüzüğü değiştirilerek görev süresinin 2020 yılına kadar uzatıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

2.4. Avrupa Birliği Ağ ve Veri Güvenliği Direktifi

Avrupa Birliği'nin ağ ve veri güvenliği konusunda yeni bir direktif hazırlığı içerisinde olduğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013, s.20).

Çalışmamızın önceki bölümlerinde bahsettiğimiz 108 sayılı sözleşmede ve 95/46/EC sayılı direktifte; üye ya da sözleşmeye taraf ülkeler arasında kişisel nitelikteki verilerin transferinin yasaklanamayacağı hükmü bulunduğu görülmektedir. Bu nedenle AB'nin bilgi güvenliği politikalarını geliştirirken; Avrupa Ekonomik Alanı'nı bir bütün olarak ele aldığı ve üye ya da taraf ülkeler arasında bütünleştirici bir tutum sergilediği görülmektedir (Henkoğlu ve Yılmaz 2013,s.12).

Ocak 2012 tarihli ve IP/12/46 referans numaralı yeni veri koruma direktifi taslağına ihtiyaç duyulmasının nedenleri arasında üye ülkelerin ulusal veri koruma düzenlemeleri arasındaki belirsizlik ve farklılıkların görülmesinin, bu düşünceyi doğruladığı düşünülmektedir (Henkoğlu ve Yılmaz, 2013,s.12).

Taslağın nihai hali 7 Şubat 2013 tarihinde yayımlanmış olup, gelinen aşamada AB Konseyi'ndeki görüşmelere devam edildiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013,s.20).

Bilgisayar ağları ve veri sitemlerinin bugün toplumsal ve ekonomik anlamda kazandığı önem nedeniyle, üye devletlerin bu sistemlerin güvenliği hususunda hazırlıklı olması gerektiği dile getirilmektedir ve direktifin amacının eş ve yüksek düzeyde ağ ve veri güvenliğini sağlaması olduğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Direktif taslağının 3 temel yaklaşım benimsediği dile getirilmektedir (Avrupa Birliği Bakanlığı, 2013, s.21). Bunlar;

1. Üye devletlerin ağ ve veri güvenliği stratejisi başta olmak üzere, bu alanda işbirliği planlayan Bilgisayar Acil Durum Müdahale Ekipleri kurarak ulusal kapasitelerini geliştirmelerini sağlamak.

2. Üye devletlerin AB düzeyinde işbirliği ağı kurmaları ve ağ ve veri güvenliğine yönelik tehditlerin tespiti ve bertaraf edilmesi için işbirliği yapmasını sağlamak.

3. Elektronik Haberleşme Direktifi temelinde bir risk yönetim modelinin oluşturulması ve kamu-özel sektör ortaklığının geliştirilmesi sağlamak.

Yine direktifle birlikte tüm üye devletlerin Ulusal Ağ ve Veri Güvenliği Stratejisi geliştirmelerinin zorunlu hale getirilmesi istenmektedir. Bu stratejinin, güncel öncelikleri ve hedefleri ortaya koyması, kamunun rol paylaşımını belirlemesi ve yönetişim çerçevesini ortaya koyması istenmektedir. Ayrıca hazırlık, müdahale ve kurtulma gibi tanımlamaları yaparak, kamu-özel sektör işbirliği mekanizmalarını ortaya koyması, eğitim ve farkındalık yaratma faaliyetlerine ilişkin planlar ile Ar-Ge planlarını içermesi gerektiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Yine bu strateji içersinde, risk analizleri, yol haritası gibi içeriği haiz işbirliği planlarının da bulunması gerektiği belirtilmektedir. Ayrıca üye devletlerin, ağ ve veri güvenliği konularında yetkili olacak kurumları belirlemesi gerektiği ve bu kurumların yeterli insan kaynağı ve teknik altyapıyla donatılarak, gerektiğinde adli makamlarla işbirliği yapmaya yetkili olarak yapılanması gerektiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013). Ayrıca ağ ve veri güvenliği sorunlarıyla mücadele etmek üzere, her üye devletin, Bilgisayar Acil Müdahale Ekipleri kurmaları

istenmektedir ve bu ekiplerin ağ ve veri güvenliği konusunda yetkili kuruma bağlı olarak gerçekleştirdikleri faaliyetlere ilişkin Komisyon'a rapor sunması beklenmektedir (Avrupa Birliği Bakanlığı, 2013).

III. BAZI AVRUPA BİRLİĞİ ÜLKELERİNDE İNTERNET VE SOSYAL MEDYA ÜZERİNDEN İŞLENEN SUÇLAR VE ALINAN TEDBİRLER

3.1.İtalya

İtalya Anayasası'nın 21. maddesine göre herkesin özgür biçimde düşüncelerini sözlü, yazılı veya diğer iletişim biçimleri ile ifade etme hürriyeti bulunduğu belirtilmektedir. Medya, yine aynı maddede yazan istisna hariç olmak üzere (gerekçeli biçimde medyaya yönelik kanunlarda yazan suçların takibinde) herhangi bir izne veya sansüre tabi kılınamamaktadır. Yine aynı maddede kamu ahlakına aykırı yayınların ve gösterilerin yasaklandığı görülmektedir. Bunlara yönelik önlemlerin ise ancak kanun ile konabileceği dile getirilmektedir (Avrupa Birliği Bakanlığı, 2013, s.24).

3.1.1. İnternet Siteleri ve Sosyal Medya Üzerinden Yapılan Hakaretler

İtalyan Ceza Kanunu'nun 594. ve 595. maddelerinde, onur kırıcı davranışta bulunma ve hakaret suçlarının, düzenlendiği görülmektedir. 595. maddede hakaret suçunun basın yolu ile işlenmesinin, cezayı (hapis ve para cezasını) artırıcı nitelikte olduğu belirtilmektedir. Yine "596-bis" maddesinin, baskı araçları ile işlenen hakaret suçlarına yönelik düzenlendiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

İtalya'da Yargıtay'ın verdiği 46504 sayılı karara göre web sitelerinin de diğer iletişim araçları gibi Ceza Hukuku kurallarına tabi olduğu görülmektedir. Ayrıca hakaretin, Anayasa'nın 21. maddesinde düzenlenen ifade özgürlüğü kapsamında değerlendirilmediği görülmektedir. Bu karardan hareketle web siteleri aracılığıyla hakaret etmenin Ceza Kanunu kapsamında cezalandırıldığı sonucuna ulaşılabilmektedir (Avrupa Birliği Bakanlığı, 2013).

"G.I.P. di Livorno con la sentenza n. 38912 del 02 ottobre - 31 dicembre 2012" sayılı mahkeme kararıyla, Facebook üzerinden eski çalıştığı şirkete hakaret eden bir kullanıcının suçlu bulunduğu görülmektedir. Kararda, internet aracılığıyla hakaret etmenin, Ceza Kanunu'nun 595. maddesinde düzenlenen hakaret suçu kapsamında değerlendirildiği görülmüş ve suçun bahse konu maddenin 3. paragrafı uyarınca

reklam ve diğer araçlarla yayma yoluyla yapıldığına kanaat getirilerek ağırlaştırıcı bir etken olduğu ifade edilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.1.2.Siber Suçlar

İtalya'nın 2008 yılında Siber Suçlar Sözleşmesi'ni imzaladığı ve onayladığı bilinmektedir. Ayrıca İtalyan Ceza Kanunu'nda siber suçlara ilişkin hükümLER bulunduğu görülmektedir. İtalya Ceza Kanunu'nun "615. ter" maddesi, bir bilgisayar veya iletişim aracına izinsiz girmeye ve bulunmaya ilişkin olup madde uyarınca, bu suçun 3 yıla kadar hapis ile cezalandırıldığı belirtilmektedir. Eğer bu suç; bir kamu görevlisi veya sistem işletmecisi tarafından görevi kötüye kullanılarak işleniyorsa, fail suçu şiddet ile veya silahlı olarak işliyorsa, sisteme, veriye veya bilgiye zarar geliyorsa, cezanın 1 ile 5 yıl hapis cezası olduğu belirtilmektedir. İlk iki halde izinsiz girilen sistem kamu düzenini ilgilendiriyorsa, cezaların arttırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Yine görevlilerce işlenme hali hariç olmak üzere sayılan fiillerin, re'sen soruşturulduğu görülmektedir. "615. quater" maddesinde, kendine çıkar sağlamak veya başkasına zarar vermek üzere kodları, anahtar kelimeleri veya korunan bir sistem veya bilgisayara girmek üzere gereken öğeleri yasadışı olarak eline geçiren, çoğaltan, yayan, ileten veya sayılan amaçlarla bunlara yönelik bilgi veya talimat alan kimselerin, 1 yılı aşmayan hapis cezası ve para cezası ile cezalandırıldığı belirtilmektedir. "615. quinquies" maddesinde de, bilgisayar veya telekomünikasyon sistemlerini veya bunlarda bulunan verileri zedeleme amacı ve etkisi taşıyan, kendisi veya başkasının hazırladığı bilgisayar programlarını, yayan, ileten veya ulaştıran kimselerin, iki yıla kadar hapis ve para cezası ile cezalandırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.1.3 Kişisel Verilerin İzinsiz veya Hukuka Aykırı Olarak Elde Edilmesi ve Kullanılması

30 Haziran 2003 tarihli ve 196 sayılı İtalyan Kişisel Verilerin Korunması Kanunu uyarınca bu kanuna aykırılıktan özel hukuk hükümlerine başvurulabildiği, idari hükümlerin ihlali halinde de para cezası uygulanabildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Bunlara ek olarak 167. madde uyarınca kendisine kazanç sağlamak veya başkasına zarar vermek üzere kişisel verileri işleyen kişilerin, zararın gerçekleşmesi halinde bazı maddelerin ihlali sebebiyle 6 ile 18 ay hapis cezasına, işlemenin veri paylaşımını veya dağıtımını içermesi halinde 6 ile 24 ay hapis cezasına, bazı maddelerin ihlali sebebiyle ise 1 ile 3 yıl hapis cezasına çarptırıldığı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.1.4. İnternet Ortamına Yönelik Kısıtlayıcı Önlemler

İtalya'da 2009 yılında internet servis sağlayıcılarına, içerisinde suça teşvik eden ve suçu savunan paylaşımların bulunduğuna inandıkları Facebook veya Youtube gibi bir sosyal medya sitelerini bütün olarak filtreleme/ karartma/ bloke etme/ erişime engelleme yükümlülüğü getiren bir mevzuat değişikliği gündeme geldiği görülmektedir. Bu değişikliğin, ifade hürriyeti kapsamında eleştirilere maruz kaldığı belirtilmektedir. Yine aynı sene, bu tip sosyal paylaşım sitelerinde yer alan saldırgan nitelikli içeriklerin siteden kaldırılmasının hızlandırılması için bazı değişikliklerinde gündeme geldiği görülmektedir. Bu öneriler arasında, polisin savcıya gitmeksizin hâkimden talepte bulunabilmesi, nefret suçu işleyenlere para cezası getirilmesi ve şiddeti teşvik eden sitelere erişimin engellenmesi gibi yaptırımları içerdiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Yine 2010 yılında internetin belirli sebeplerle filtrelenmesine yönelik mevzuat değişikliklerine gidilmek istendiği ve sosyal medya sitelerinde yapılan paylaşmalara yönelik olarak tartışmalara halen devam edildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Günümüzde İtalya'da ayrı bir internet kanunu olduğu görülmemektedir. (2007 yılında, Levi-Prodi Kanunu adı altında bir taslak hazırlanmış olsa dahi yasalaştığına dair bir bilgiye ulaşılamamıştır). Bunun yerine internetin, yazılı ve görsel-işitsel basının tabi olduğu düzenlemelere tabi tutulduğu görülmektedir. Örneğin; geleneksel basında, yayıncının yayın içeriğinden sorumlu olması gibi web sitesi sahiplerinin de kullanıcılarının paylaşımlarından sorumlu olduğuna dair bir yaklaşım olduğu ve bu yönde mahkeme kararları alındığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

İtalya'da medyaya yönelik düzenlemelerin ise 1848 tarihli Albertine Kanunu, Ceza Kanunu, Kamu Güvenliği Kanunları ve 1963 tarihli Basın Mensuplarına Yönelik Kurallardan oluştuğu görülmektedir. Ayrıca 2002 yılında kurulan Ulusal Güvenlik Komitesi'nin internetle ilgili güvenlik meseleleri ile ilgilendiği ve komitenin akademi, ordu ve hukuk sektörü üyelerinden oluştuğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

İtalya mahkemelerince genellikle, aracıların/servis sağlayıcıların, site kullanıcılarının paylaşımlarından/yorumlarından (özellikle telif haklarına yönelik davalarda) sorumlu tutulmadığı görülmektedir. Özellikle iftira davaları nedeniyle bazı sitelerin mahkeme kararı ile kapatıldığı bilinmektedir. İtalya'da 2010 yılında çıkarılan bir düzenleme uyarınca internet üzerinden habercilik yapması gereken kimselerin de haberci olarak kayıtlı bulunması gerekmekteyken, günümüzde bu hükümlerin sayıları milyonları bulan bloglar için uygulanmamakta olduğu ve kimi kullanıcıların bu hükümlere tabi olmamak için gazeteciler ile birlikte çalıştığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Tüm bu veriler ışığında İtalya'da tüketici organizasyonları, çevrimiçi fuhuş siteleri ve dosya paylaşım siteleri gibi çeşitli konularda olmak üzere çok sayıda siteye siyasi olmayan amaçlar ya da sosyal amaçlar ile engelleme getirildiği görülmektedir. Ayrıca kumar siteleri, ya da çocuk pornosu içeren siteler gibi bazı konularda kara listeler olduğu görülmektedir. Çeşitli idarelerin talebi ile yargı tarafından siteler bloke edilebilmekte veya servis sağlayıcıya bloke yükümlülüğü getirilebilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.2.Hollanda

Hollanda'da, internet suçlarına ilişkin düzenlemelerin Hollanda Ceza Kanunu'nun muhtelif maddelerinde bulunduğu görülmektedir. Söz konusu düzenlemelerin 2006 yılında Ceza Kanunu'nda değişiklik yapılan Bilgisayar Suçları Kanunu ile gerçekleştirildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013, s.26).

3.2.1.Bilgisayar Sistemlerine Müdahale Suçu

Hollanda Ceza Kanunu'nun 138ab maddesinin, başkasının bilgisayarına kasten ve hukuka aykırı şekilde girilmesi suçunu düzenlendiği görülmektedir. Söz konusu suçun oluşması için gereken unsurlara bakıldığında fiilin; bir güvenliği devre dışı bırakarak, teknolojik araçlarla, sahte sinyal ya da sahte bir kimlik ile gerçekleştirilmesi gerektiği ve bu halde kişinin para cezası ile 1 yıla kadar hapis cezası arasında cezalandırılacağı belirtilmektedir. Söz konusu maddenin 2. fıkrası uyarınca bu kapsamda ele geçirilen bilgiler saklanır, işlenir ya da başka bir ağa aktarılırsa cezanın, para cezası ile 4 yıla kadar hapis cezası arasında olduğu görülmektedir. Aynı cezanın, bir kamu telekomünikasyon şebekesi aracılığıyla gerçekleştirilmesi durumunda da uygulanacağı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Hollanda Ceza Kanunu'nun 350a maddesine göre, bilgisayar ya da telekomünikasyon aracılığı ile kasten ve hukuka aykırı olarak bilgilerin saklanması, işlenmesi, iletilmesi, değiştirilmesi, silinmesi, engellenmesi ya da başka bir bilgi konulması durumunda kişinin para cezası ile 2 yıla kadar hapis cezası arasında cezalandırıldığı görülmektedir. Anılan suçun, hukuka aykırı olarak bir kamu telekomünikasyon ağı aracılığı ile işlenmesi ve söz konusu bilgilerde ciddi zarara sebep olunması halinde ise cezanın, para cezası ile 4 yıla kadar hapis cezası arasında değiştiği görülmektedir. Aynı cezanın, kasıtlı ve hukuka aykırı olarak elde edilen bilginin erişime açılması ya da dağıtılması halinde de geçerli olduğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.2.2.Suça Teşvik

Hollanda Ceza Kanunu'nun 131. Maddesinde, sözlü veya yazılı olarak ya da bir görüntü ile suça ya da kamu görevlilerine karşı şiddete teşvik etmenin para cezası ile 5 yıla kadar hapis cezası arasında cezalandırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.2.3.Hakaret ve İftira Suçları

Hollanda Ceza Kanunu'nun 111. maddesi uyarınca, krala yönelik hakaretin para cezası ile 5 yıla kadar hapis cezası arasında cezalandırıldığı, kanunun 112. maddesi uyarınca ise kralın; eşine, halefine ve onun eşine yönelik hakaretin para cezası ile 4 yıla kadar hapis cezası arasında cezalandırıldığı görülmektedir. Ayrıca Kanun'un 113. maddesi uyarınca kralı ya da sayılan yakınlarını aşağılayan bir belge ya da görüntünün dağıtılması, teşhiri veya yayılması hallerinde para cezası ile 1 yıla kadar hapis cezası arasında cezalandırılacağı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Kanunun 261. maddesine göre bir kişinin onuruna ve itibarına yönelik olarak alenen iftira eden kişinin para cezası ile 6 aya kadar hapis cezası arasında cezalandırıldığı görülmektedir. Bu suçun, yazı ya da görüntülerin dağıtılması, ifşa edilmesi suretiyle işlenmesi halinde ise para cezası ile 1 yıla kadar hapis cezası arasında bir cezalandırma gerçekleştirildiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.2.4. Ayrımcılık Suçları

Bilişim ve iletişim teknolojilerini kullanarak bazı gruplara karşı ayrımcılık yapmanın ya da onları kasti olarak aşağılamanın, Hollanda Ceza Kanunu'nun muhtelif maddelerinde düzenlendiği görülmektedir. Kanun'un 137c maddesi uyarınca sözlü veya yazılı olarak ya da bir görüntü ile bir grubu, ırkı, dini, inancı vb. alenen aşağılayan birinin para cezası ile 1 yıla kadar hapis cezası arasında cezalandırıldığı belirtilmektedir. Suçun, bunu meslek ya da alışkanlık haline getirmiş biri tarafından ya da daha çok kişi tarafından işlenmesi halinde cezanın, para cezası ile 2 yıla kadar hapis cezası arasında ağırlaştırıldığı görülmektedir. Kanun'un 137d maddesinde ise aynı hususların, bu kişilere karşı nefreti, ayrımcılığı ya da şiddeti teşvik edecek

şekilde gerçekleştirilmesi halinde, para cezası ile bir yıla kadar hapis cezası arasında bir ceza öngörüldüğü belirtilmektedir. Bu suçun ağırlaştırıcı sebebi de 137c maddesi ile aynı olup, bu halde cezanın üst sınırının 2 yıla kadar hapis cezasına çıkarıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Kanunun 137e maddesi uyarınca, bu kişilere karşı nefreti ya da ayrımcılığı teşvik eden bir açıklama yapan, böyle bir açıklamanın yer aldığı bir metni karşı tarafın rızası olmaksızın ileten, yayan, dağıtan ya da ifşa eden kişinin para cezası ile 6 aya kadar hapis cezası arasında cezalandırıldığı belirtilmektedir. Yukarıda yer verilen maddelerde belirtildiği gibi, bu suçun ağırlaştırılmış halinde de azami cezanın 1 yıla kadar hapis cezası olacak şekilde düzenlendiği görülmektedir. Kanun'un 137f maddesi uyarınca ise ayrımcılığa yönelik bu suçların mali ya da diğer maddi şekillerde desteklenmesine katılan kişilerin para cezası ile 3 aya kadar hapis cezası arasında cezalandırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.2.5.Kişisel Verilerin Korunması

Hollanda Ceza Kanunu'nda münhasıran verilerin korunmasının ihlaline ilişkin hüküm olmadığı görülmektedir. Veri Koruma Kanunu adı altında ayrı bir düzenlemenin olduğu görülmekte ve kişisel verilere ilişkin ihlaller bakımından ağırlıklı olarak idari tedbirler öngörüldüğü belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.3.Almanya

Almanya'da internet suçlarına ilişkin ayrı bir kanun olmadığı, konunun Alman Ceza Kanunu'nun (Strafgesetzbuch/ StGB) muhtelif hükümlerinde düzenlendiği görülmektedir. Kanun'un tanımlara ilişkin 11. maddesinin 3. fıkrasında, görsel - işitsel kitle iletişim araçlarının, veri saklama ortamlarının, resim ve görsellerin de yazılı belgelerle eşdeğer olarak düzenlendiği belirtilmektedir. Söz konusu tanımdan, internet aracılığı ile yayınlanan bilgilerin de bu kapsamda olduğu anlaşılmaktadır. Dolayısıyla, kanunun yazılı belgelerden bahsettiği maddelerinde bu tanıma atıf yapılıyorsa internet aracılığı ile gerçekleştirilen fiillerin de söz konusu madde kapsamında değerlendirileceği düşünülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.3.1.Bilgisayar Sistemlerine Müdahale Suçu

Alman Ceza Kanunu'nun 202a maddesine göre, kendisine ait olmayan ve izinsiz erişime karşı korunan bir bilgiyi hukuka aykırı şekilde elde eden kişinin, para cezası ile en fazla 3 yıla kadar hapis cezası arasında cezalandırıldığı görülmektedir. Bu çerçevede Kanun'un 303a maddesine göre verileri silen, engelleyen, kullanılmaz hale getiren ya da değiştiren kişinin cezasının ise para cezası ile en fazla 2 yıla kadar hapis cezası arasında olacağı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013, s.28).

3.3.2.Gizliliğin İhlali

Kanun'un 201-207. maddelerinde gizliliğin ihlaline ilişkin hükümler yer aldığı görülmektedir. Örneğin 201. maddede, konuşulanların gizlice kaydedilmesi veya bu kaydın kullanılması veya üçüncü bir kişiye verilmesi durumunda para cezası ile en fazla 3 yıla kadar hapis cezası, kanunun 201a maddesinde ise kapalı bir alanda izinsiz fotoğraf çekilmesi suretiyle gizliliğin ihlali durumunda para cezası ile en fazla 1 yıla kadar hapis cezası arasında bir ceza öngörüldüğü belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.3.3. Ayrımcılığa Dayalı Olarak Halkın Kışkırtılması Suçu

Alman Ceza Kanunu'nun 130. maddesinde halkı nefrete teşvik suçunun düzenlendiği görülmektedir. Maddenin 2. fıkrasında yapılan atıf sebebiyle internet aracılığı ile işlenen suçların da madde kapsamında ele alındığı görülmektedir. Milliyet, ırk, din gibi unsurlara dayanarak halkı bu gruplara karşı nefrete teşvik eden, şiddete davet eden veya kasten aşağılayarak kişiliğine bağlı temel haklarını ihlal eden ve bu bilgileri dağıtan, halka ifşa eden ya da onların erişimine açan kişinin; para cezası ile en fazla 3 yıla kadar hapis cezası arasında cezalandırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.3.4. İftira ve Tahkir Suçları

Alman Ceza Kanunu'nun 186. maddesinin genel olarak iftira suçunu düzenlediği görülmektedir. Kanunun 188/1. maddesinde ise iki farklı hal bakımından, iftira suçunun bir siyasetçiye karşı alenen işlenmesi durumunu düzenlediği görülmektedir.

Bunların ilkinde kişinin, kamuya açık bir toplantıda iftirayı gerçekleştirmekte olması, ikincisinde ise iftira içeren yazılı bir metin oluşturması durumu belirtilmektedir. Böyle bir metnin internet aracılığı ile yayınlanmasının da bu kapsamda olduğu görülmektedir. Suçun oluşması için iftiranın, siyasetçinin siyasi pozisyonu ile ilgili olması ve bundan dolayı görevini zorlaştırması gerektiği ve anılan unsurlarının oluşması halinde 3 aydan 5 yıla kadar hapis cezası öngörüldüğü belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Söz konusu kanunun 187. maddesinde ise iftira suçunun bilerek ve kasıtlı olarak ve halkın kişi hakkındaki görüşlerini olumsuz etkileyecek ya da güvenilirliğini tehlikeye atacak şekilde gerçek olmayan bir bilgiyi yaymak suretiyle işlenmesinin düzenlendiği görülmektedir. Bu suçun, siyasetçiye karşı işlendiğinde 188/2. maddesi uyarınca 6 aydan 5 yıla kadar hapis cezası öngörüldüğü belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Kamuya açık bir toplantıda ya da yazılı bir metin veya internet aracılığı ile devlet başkanına tahkirin madde 90'da 3 aydan 5 yıla kadar, devleti, anayasal düzeni, bayrağı ve devletin sembollerini tahkirin madde 90a'da 3 yıla kadar ve devletin mevcudiyetine veya anayasal ilkelere karşı gelecek şekilde yasama, yürütme ve yargıyı tahkirin ise madde 90b'de 3 aydan 5 yıla kadar hapis cezası gerektirdiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.3.5.Toplantı ve Gösteri Yürüyüşüne Davet

Almanya'nın, toplantı ve gösteri yürüyüşlerine ilişkin Federal Kanunu'nun 23. maddesi uyarınca, kişileri, -icra edilebilir bir kararla- önceden yasaklanmış bir eyleme, yazılı bir metin veya internet aracılığı ile davet etmenin cezasının, para cezası ile bir yıla kadar hapis cezası arasında olduğu görülmektedir. Ayrıca, Ceza Kanunu'nun 111. Maddesinde kamuya açık bir toplantıda ya da yazılı bir metin veya internet aracılığı ile hukuka aykırı bir fiilin gerçekleştirilmesi için kişileri teşvik eden birinin suçu azmettiren gibi sorumlu tutulduğu görülmektedir. Maddenin ikinci fıkrasında söz konusu teşvikin başarısız olması halinde dahi para cezası ile 5 yıla kadar hapis cezası arasında değişen bir ceza öngörüldüğü ancak kanun uyarınca bu halde verilecek cezanın, söz konusu teşvik başarılı olsaydı gerçekleşecek suçun

cezasından daha ağır olmaması gerektiği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.4.İngiltere

3.4.1.İnternet Ortamında İşlenen Suçları Düzenleyen Kanunlar

İngiltere'de bilgisayar üzerinden işlenen suçlara ilişkin 1990 tarihli Bilgisayarın Kötüye Kullanımı Kanunu'nun uygulandığı görülmektedir. Bu kanunun, hackleme, verilerin sızdırılması ve suç işleme amacıyla izinsiz şekilde verilere erişim gibi siber suçları kapsadığı belirtilmektedir. Söz konusu kanunun, 2006 ve 2008 yıllarında revize edildiği bilinmektedir (Avrupa Birliği Bakanlığı, 2013, s.29).

İngiltere'de bilgisayar ve internet vasıtasıyla işlenen geleneksel suçların ise mevcut ceza kanunu ve ilgili diğer kanunlarda ele alındığı görülmektedir. Örneğin, çocuk pornografisi kapsamına giren suçların 1978 tarihli Çocukların Korunması Kanunu kapsamında, internette yolsuzluk suçlarının 2006 tarihli Yolsuzluk Kanunu kapsamında, telif haklarının ihlaline ilişkin suçların ise 1988 tarihli Telif, Tasarım ve Patent Kanunu altında değerlendirildiği görülmektedir. İngiltere'de çocuk pornografisi, uyuşturucu ve intiharı teşvik, terörizmi teşvik gibi suçlar işlendiğinde sitelere erişimin engellenmesi gibi çeşitli kısıtlayıcı önlemlere başvurulabildiği de görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.4.2.İngiliz Ceza Kanununda Sanal Ortama İlişkin Düzenlemeler

İngiltere'de siber suçların 1990 tarihli Bilgisayarın Kötüye Kullanımı Kanunu kapsamında, sanal ortamda işlenen geleneksel suçlarla ilgili kanunlar çerçevesinde düzenlendiği görülmektedir. İngiltere Ceza Kanunu'nda sanal ortamda işlenen suçlara yönelik özel bir düzenlemeye rastlanmadığı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.4.3.İnternet Sitelerine Yönelik Düzenlemeler, İnternet Üzerinden Yapılan Hakaretler

2003 tarihli İletişim Kanunu'nun (Communication Act) elektronik iletişim ağlarının uygunsuz kullanımına ilişkin düzenlemeleri içerdiği görülmektedir. Bu kapsamda,

Facebook, Twitter, Linkedln ve Youtube gibi mecralar üzerinden ağza alınmaz, çirkin, saldırgan, tehdit edici ya da yalan içerikli paylaşımların cezalandırılmasının mümkün kılındığı görülmektedir. İlgili madde altında sayılan fiillerden birini işlediği tespit edilen kişilere 6 aya kadar hapis cezası, adli para cezası veya her ikisinin birden uygulanabildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.4.4. Sosyal Medya Aracılığıyla Gönderilen Mesajların Soruşturulması Hakkında Yönerge

20 Haziran 2013 tarihinde savcıların sosyal medya aracılığıyla gönderilen mesajların soruşturulması amacıyla hazırlanan yönergenin kamuoyu ile paylaşıldığı görülmektedir. Söz konusu yönerge kapsamında, şiddet çağrısı yapan, bir veya birden fazla kişiyi hedef gösteren ya da mahkeme kararlarını ihlal etmeye yönelik sosyal medya paylaşımları yapan kişilerin 2003 tarihli İletişim Kanunu'nun 127. maddesi kapsamında cezalandırıldığı belirtilmektedir. İlgili madde altında sayılan fiillerden birini işlediği tespit edilen kişilere 6 aya kadar hapis cezası, adli para cezası veya her ikisinin birden uygulanabildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Ancak sadece rahatsızlık verici, rencide edici ve yalan içerikli paylaşım yapan kişi "içten bir pişmanlık gösterdiği" ya da "paylaşımı internet ortamından kaldırmak için etkili bir çabada bulunduğu" takdirde olayın yargıya intikal etmeyeceği belirtilmektedir. Ayrıca eğer söz konusu paylaşımın geniş bir kitleye ulaşması amaçlanmamışsa da dava açılmayacağı görülmektedir. Savcıların sosyal medya üzerinden yapılan paylaşımlara ilişkin dava açılması gerekip gerekmediği hakkında karar verirken "kamu yararı" ilkesini de gözetecekleri belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.5.Fransa

Fransa'da siber suç olarak ifade edilen internet yoluyla işlenen suçların, çok sayıda kanun ve düzenleyici işleme konu olduğu görülmektedir. Söz konusu düzenlemelerin ağırlıklı olarak, banka hesapları gibi kişisel verilerin kullanılmasına yönelik olan suçlar, fikri mülkiyet haklarının ihlaline yönelik suçlar ve bilgi teknolojisini

kullanarak iletişim sağlamak yoluyla ırk düşmanlığı ya da bir kişiye yönelik saldırı gibi konularda işlenen suçlar olmak üzere üç grup suça ilişkin olduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013, s.31).

3.5.1.Verilerin İzinsiz veya Hukuka Aykırı Olarak Elde Edilmesi ve Kullanılmasına İlişkin Suçlar

Fransız Hukuku'nda internet kullanımına ilişkin temel kanuni düzenlemenin 78-17 sayı ve 6 Ocak 1978 tarihli Bilgisayarlar, Dosyalar ve Özgürlükler ile İlgili Kanun olduğu görülmektedir. Söz konusu kanunun, özellikle Avrupa Birliği'nin kişisel verilerin korunmasına ilişkin mevzuatına paralel olarak çok sayıda değişiklik geçirmiş olduğu ve temel olarak kişisel verilerin kullanımına ilişkin usul ve esasları düzenlediği belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

Fransız Ceza Kanunu'nun kişilere karşı suçlara ilişkin 2. kitabının, kişiliğe karşı saldırıları düzenleyen 6. başlığında; bilgi teknolojilerinin ve iletişim araçlarının kullanılması yoluyla işlenen suçlara yer verildiği görülmektedir. Bu bölümde kişisel verilerin, 78-17 Sayılı Kanun'da düzenlenen usullere aykırı olarak veya kişinin muhalefetine rağmen ya da hukuka aykırı olarak elde edilmesi, işlenmesi, kullanılması ve açıklanmasının 5 yıl hapis cezası ve 300 bin Avro para cezası yaptırımına tabi tutulduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Buna benzer cezaların, suçun, özel hayatın gizliliğine karşı işlenmesi halinde 226-3. maddede yer aldığı da görülmektedir. Bir sosyal paylaşım ağında, bir kişi adına, sahte bir profil yaratılması Fransa Ceza Kanunu'nun 226-4-1. maddesi kapsamında değerlendirilmektedir. Bu kapsamda yaratılan sahte profil, kişinin hayatında olumsuz etki yaratır, onurunu zedeler veya huzurunu bozacak sonuçlara yol açarsa bu hareketin, ceza kovuşturmasının konusu olacağı belirtilmektedir. Bu suçun, 1 yıl hapis ve 15 bin Avro para cezasıyla cezalandırıldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Fransa Ceza Kanunu'nun "Ulusa, Devlete ve Kamu Barışına Karşı Suçlar" başlıklı 4. kitabında aynı suçun devlet güvenliğine ilişkin sırlar hakkında işlenmesi halinde, 5 ile 7 yıl arasında hapis ve 75 ile 100 bin Avro arasında para cezasıyla

cezalandırılacağı düzenlenmesi olduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Fikri Mülkiyet Kanunu'nun 335-1 vd. maddelerinde, fikri mülkiyet haklarının siber suç yoluyla ihlal edilmesi, yani fikri mülkiyete konu olan malların, internet gibi bilgi ve iletişim teknolojilerinin kullanılmasıyla elde edilmesi, çoğaltılması, dağıtılması gibi vb. fiillerin suç olarak tanımlandığı görülmektedir. Bu Kanun'da, suçun işleniş biçimine göre, 6 ay ile 3 yıl arasında değişen hapis cezaları ve 300 bin Avroya kadar çıkan para cezaları bulunduğu belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

3.5.2.Hakaret ve Sövme Suçları

Fransız hukukunda, hakaret ve sövme suçunun unsurlarını taşımayan hallerde, internet üzerinden yerme, aleyhte söz söyleme, eleştiri yapma gibi hareketler Fransa Ceza Kanunu'nu maddelerine değil, şartları oluşursa Fransız Medeni Kanunu'nun 1382. maddesine tabi olduğu görülmektedir. Bu kapsamda bir kişi veya işletme aleyhine hakaret niteliği taşımasa da olumsuz görüş ve ifadelerde bulunmak, sorumluluğa sebep olan fiil olarak belirtilmektedir. Ancak tazminat sorumluluğunun diğer klasik şartlarının yanında, bu hareketin zarar vermek kastıyla yapılması gerektiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Hakaret suçunun ise 29 Temmuz 1881 tarihli Basın Özgürlüğü Kanunu'nda düzenlendiği görülmektedir. Buna göre internetten yapılan tüm yayınların, toplumun sınırlı bir bölümüne ulaşıyor olsa bile hakaret sayılabileceği belirtilmektedir. Söz konusu suç, ifade özgürlüğünün sınırını göstermekte olup, ifade özgürlüğünün başkasına zarar vermek amacıyla kullanılması hukuka aykırı bulunmaktadır. Basın Özgürlüğü Kanunu'nun 29. maddesinin birinci fıkrası uyarınca bir kişinin onurunu veya itibarını zedeleyen iddia veya isnatların hakaret olarak nitelendirildiği görülmektedir. Söz konusu fiiller elektronik iletişim araçlarıyla kamuya yayınlamak yoluyla işlenebilir. Suç niteliğindeki fiiller, somut bir olaya ilişkin bir iddia, belirli veya belirlenebilir bir kişinin tartışma konusu yapılması şeklinde gerçekleştirilebilir. Hakaret suçunun oluşması için, bu fiillerin, zarar verme ya da tahkir etme kastıyla işlenmiş olması gerektiği belirtilmektedir. Bununla birlikte basit bir eleştiri veya

değerlendirmenin bu suçun oluşmasına yol açmadığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Basın Özgürlüğü Kanunu'nun 65. maddesine göre hakaret suçunun, ilk yayım tarihinden itibaren 3 ay içerisinde kovuşturulması gerektiği belirtilmektedir. Hakaret suçu için hapis cezası bulunmayıp, sadece 12 bin Avro para cezası olduğu belirtilmektedir. Diğer taraftan mağdurun, hukuk davası açarak tazminat talep etmesinin de mümkün olduğu belirtilmektedir. Ancak Basın Özgürlüğü Kanunu'nun 32. maddesinde, ırk veya dine dayalı hakaret suçu için 1 yıl hapis ve 45 bin Avro para cezası olduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.5.3. Suça Teşvik Suçları

Basın ve iletişim araçlarıyla kişileri suça teşvik etme suçunun Fransız Basın Özgürlüğü Kanunu'nda düzenlendiği görülmektedir. Kanunun 24. maddesine göre yaşama, kişinin vücut bütünlüğüne, cinsel eğilimine karşı suçlar ile hırsızlığa, tehdit etmeye, savaş suçlarına ve insanlığa karşı suçları övmeye teşvik ve tahrik eden hareketlerin suç teşkil ettiği belirtilmektedir. Maddede suça tahrik ve teşvik suçu için 5 yıl hapis ve 300 bin Avro para cezası olduğu öngörülmektedir (Avrupa Birliği Bakanlığı, 2013).

3.6. Finlandiya

Finlandiya'da internet ortamında işlenen suçlara ilişkin ayrı bir kanun olmadığı, bu tür suçların Finlandiya Ceza Kanunu hükümlerine tabi olduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013, s.33).

3.6.1.Ceza Kanunundaki Düzenlemeler

Finlandiya Siber Suçlar Sözleşmesi'ne taraf bir ülke olduğundan Siber Suçlar Sözleşmesi'nde belirtilmiş olan suç gruplarına ilişkin düzenlemelerin Finlandiya Ceza Kanunu'nda da (515/2003) bulunduğu görülmektedir. Ayrıca yine Siber Suçlar Sözleşmesine taraf bir ülke olmasından hareketle, normalde suç olarak kabul edilen bütün davranışların internet olanakları kullanılarak gerçekleştirilmesinin de suç olarak değerlendirileceği mütalaa edilmektedir (Avrupa Birliği Bakanlığı, 2013).

Örnek olarak Fin Ceza Kanunu'nun 17. Fasıl, 1. Kısmında (515/2003) bir suça toplu medya olanakları kullanılarak veya bir topluluk içerisinde açık olarak teşvikte bulunmanın maddi ceza ya da 2 yıla kadar hapis cezası ile cezalandırılabildiği görülmektedir (Avrupa Birliği, 2013)

3.6.2. Kişisel Hesapları Hackleme ya da Kişisel Verileri Sızdırmaya Karşı Alınan Önlemler

Veri ve iletişime ilişkin suçların Fin Ceza Kanunu'nun 38. faslında düzenlendiği görülmektedir. Sadece başkasına ait bilgisayara hackleme yoluyla girmenin para veya 1 yıla kadar hapisle cezalandırıldığı görülmektedir. Suçun büyüklüğü ve verilerin ifşa edilip edilmemesine göre suç ve cezasının arttığı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

IV. TÜRKİYE'DE İNTERNET ve SOSYAL MEDYA KULLANIMI ve BU ALANA İLİŞKİN DÜZENLEMELER

Leiner vd.(2009)'ye göre internetin en hassas özelliği olarak, sansürden uzak bir kitle iletişim ortamı olması görülmektedir. Ancak bu özelliği, hiçbir zaman internetin hukuk dışı bir kullanım aracı olmasına dayanak oluşturacak şekilde yorumlanmayacaktır. İnternet, her biri kendi içinde bağımsız yönetilen ve denetlenen; yani otonom olan ağların bütününden oluşmaktadır. Bu açıdan bakıldığında: bireysel olarak denetlenebilen ancak küresel bağlamda denetimi ve yönetimi tam anlamıyla mümkün olmayan bir yapı olarak düşünülmektedir (Koç ve Kaynak, 2010, s.3).

Yazıcıoğlu (1997)'na göre internet bugün sayılamayacak veya sınıflandırılamayacak kadar çok alanda kullanılmaktadır. E-posta göndermek ve almak, haber grupları oluşturmak, eş zamanlı sohbet etmek, video konferanslar düzenlemek, ticaret yapmak, eğitim ve askeri amaçlar için kullanmak gibi örneklere her geçen gün yenileri eklenmektedir. İnternet, ulusal ve uluslararası alandaki işleyiş biçimi ile bir taraftan ceza kanunlarında yer alan klasik suç tiplerinin gerçekleştirilmesine uygun bir ortam yaratırken, kendine özgü ve yeni suçları yaratan bir faaliyet alanı da olmuştur. Bu noktada: internet üzerinden gerçekleştirilen ve suç unsuru taşıyan eylemler gerek nitelik gerekse nicelik olarak artan bir öneme sahip olarak değerlendirilmektedir. İnternet üzerinden yapılan bir yayının ulusal sınırları aşarak diğer kitle iletişim araçlarına oranla çok daha geniş kitlelere ulaşması nedeniyle etkilerinin de aynı oranda büyük olduğu gözlemlenmektedir. Bu gücün kötüye kullanılmasının suç içerikli içeriğin aynı hız ve etkiyle tüm dünyaya yayılması gibi son derece ciddi ve tehlikeli bir sonucun ortaya çıkacağı düşünülmektedir. Bu durumun, suç işleyenler açısından interneti kullanma sıklığını ve yaygınlığını artırdığı vurgulanmaktadır (Koç ve Kaynak, 2010).

İnsanların birbirleriyle iletişim kurma kanalı, hatta sosyalleşme yolu olarak daha çok interneti tercih etmeye başlamaları ile beraber, sosyal medya gerek sosyolojik, gerekse hukuki olarak toplum hayatının önemli bir parçası haline gelmiştir. İnternette yayın yapan ve kullanıcılarının artık yüz milyonları bulduğu sosyal medya siteleri

sosyal hayatın bizzat kendisine tekabül eder hale geldiğinden, hukuki olmasının yanı sıra sosyolojik birer olgu olan suçların da çok farklı tezahürlerine sosyal medyada rastlamanın mümkün hale geldiği dile getirilmektedir (Özocak 2012, s.1).

İnternet yayıncılığındaki hukuk ihlallerinin genel olarak; kişilik haklarının ihlali, özel hayatın gizliliği ilkesinin ihlali, gerçek dışı haber ve yorumlarla yapılan ihlaller ile cevap ve düzeltme hakkının ihlali gibi konularda gerçekleştiği belirtilmektedir (Nizam ve Biçer, s.2).

Sosyal medya üzerinden işlenen suçların, günlük somut hayattan farklı olarak, maddi varlığı bulunmayan soyut ortamlar üzerinde gerçekleştiğinden, bunların işlenme yolları ve suçluların tespiti yöntemlerinin geleneksel ve klasik suçlara göre farklılık göstereceği dile getirilmektedir (Özocak 2012).

Özdilek (2006), bilişim suçlarını "bilişim sistemleri aracılığıyla işlenen suçlar" ve "bilişim alanındaki suçlar" olarak ikiye ayırmaktadır. İlk gruptaki suçlar "geleneksel" ya da "klasik" suçlar olarak tanımlanmakta, ancak bir bilişim sistemi aracılığıyla işlenmektedir. Örneğin; internet siteleri üzerinden işlenen cinsel taciz, halkı kin ve düşmanlığa tahrik etme gibi suçlar bu grupta sayılmaktadır. İkinci gruptaki suçlar ise, kanunda sınırlı sayıda düzenlenen ve ilk gruptaki suçlara göre teknik özellikler arz eden suçlar olarak sınıflandırılmıştır. 5237 Sayılı Türk Ceza Kanunu'nda bu suçlar, 243 ila 246. maddeler arasında, "Bilişim Alanında Suçlar"" başlığıyla düzenlenmektedir (Özocak, 2012, s.2).

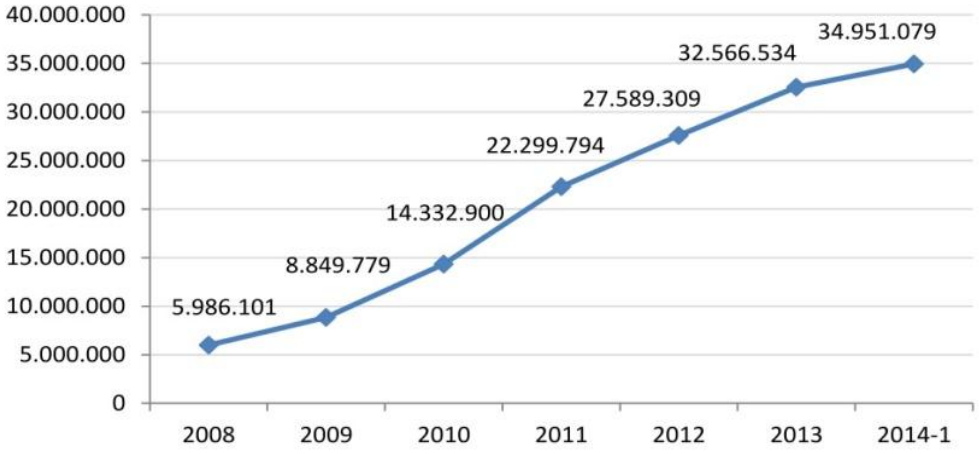
Sosyal medya üzerinde işlenen suçların, her iki grup suçun kapsamına da girdiği görülmektedir. Örneğin, bir kimsenin bir sosyal paylaşım sitesi hesabı şifresinin kırılarak hesabına yetkisiz bir biçimde girilmesi durumunda ikinci grup olan "bilişim alanında suç" söz konusuyken, buna karşın, sosyal paylaşım sitesindeki bir hesap üzerinden bir kimseye hakaret edilmesi durumunda, ilk grup olan klasik ya da geleneksel suçlardan olan hakaret suçunun bilişim sistemleri aracılığıyla işlenmesinden bahsetmek gerekeceği dile getirilmektedir (Özocak, 2012, s.2).

Ancak Türkiye'de söz konusu alana yönelik düzenlemelere geçmeden önce Türkiye'de internet ve sosyal medya kullanımının hangi boyutlara ulaşmış olduğunun anlaşılması çalışmamız açısından önemli görülmektedir.

4.1.Türkiye'de İnternet ve Sosyal Medya Kullanımı

Şekil 4.1' de görüldüğü üzere 2008 yılından başlayarak Türkiye'de genişbant internet abonesi sayısının hızlı bir şekilde arttığı görülmektedir.

Şekil 4.1. Genişbant İnternet Abone Sayısı



Kaynak: BTK (2014)

Bilgi Teknolojileri ve İletişimi Kurumu'nun (BTK) yayınladığı 2014 yılı ilk çeyrek raporu verilerine göre bugün Türkiye'de toplamda 34 milyon 951 bin 79 genişbant internet abone sayısına ulaşılmıştır.

Aşağıdaki tabloda da Türkiye'de bağlantı çeşidine göre internet abone sayıları ile çeyrek (2013-4. ve 2014-1.) ve yıllık bazda artış oranlarına yer verilmiştir.

Tablo 4.1. Toplam İnternet Abone Sayıları

	2013-1	2013-4	2014-1	Çeyrek Büyüme Oranı (2013-4...2014-1)	Yıllık Büyüme Oranı (2013-1...2014-1)
xDSL	6.678.907	6.644.543	6.671.447	0,4%	-0,11%
Mobil Bilgisayardan İnternet	1.780.790	1.701.014	1.541.425	-9,4%	-13,44%
Mobil Cepten İnternet	21.408.431	22.472.129	24.902.577	10,8%	16,32%
Kablo İnternet	501.201	486.497	492.288	1,2%	-1,78%
Fiber	741.675	1.193.704	1.277.711	7,0%	72,27%
Diğer	137.366	116.043	112.808	-2,8%	-17,88%
TOPLAM	31.248.370	32.613.930	34.998.256	7,3%	12,00%

Kaynak: BTK (2014)

Türkiye'de 6 milyon 671 bin 447 xDSL,1 milyon 541 bin 425 mobil bilgisayardan internet, 24 milyon 902 bin 577 mobil cepten internet, 492 bin 288 kablo internet, 1 milyon 277 bin 711 fiber internet ve 112 bin 808 diğer internet aboneleri bulunmaktadır.

Burada dikkat çeken husus yaklaşık 25 milyon abonesi ile diğer genişbant internet bağlantılarının abone sayılarını büyük bir farkla geçen mobil cepten internete bağlanan abonelerin sayısıdır.

Bu veri bize akıllı telefonların özellikle internet kullanımında ne kadar önemli olduğunu göstermektedir.

Ipsos (2013)'un 24 ülkede online olarak yürüttüğü Global Advisor Socialogue araştırması, 35 yaşın altında olan kişilerin sosyal medyada daha aktif olduklarını göstermektedir (Gençlik ve Spor Bakanlığı, 2013, s.27).

Benzer bir eğilim Türkiye'de de gözlemlenmektedir. Ipsos (2012) tarafından yapılan BrandPuls Türkiye'de İnternet Kullanım Alışkanlıkları 2012 araştırması, tüm internet kullanıcılarının % 81'inin sosyal medyayı aktif kullandığını, 14-24 yaş grubundaki gençlerde bu oranın % 91'e çıktığını göstermektedir (Gençlik ve Spor Bakanlığı, 2013, s.40).

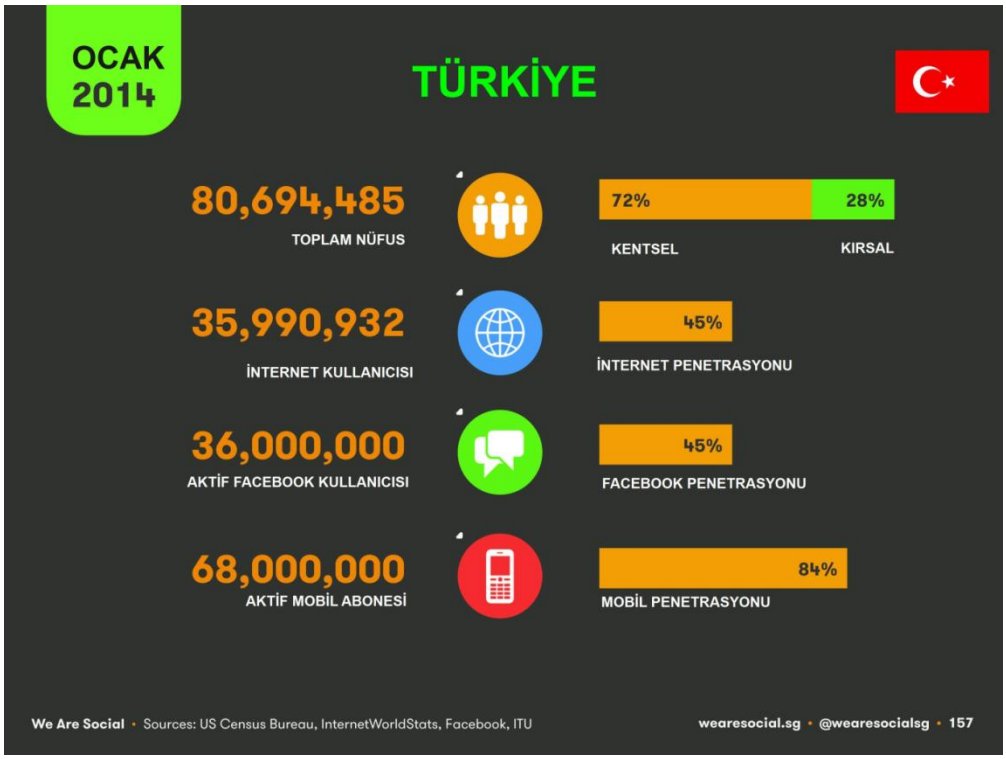
IAB Türkiye İnternet Ölçümlemesi Araştırması, Facebook'un Türkiye'de en popüler sosyal medya sitesi olduğunu belirtmektedir. Araştırma, Temmuz 2013 döneminde 15 yaş üzeri nüfusta Facebook'u birden fazla ziyaret edenlerin oranının % 84

olduğunu ortaya koymaktadır. İkinci sırada ise Youtube'un geldiği ve internet kullanıcısı nüfusun % 70'inin Youtube'u ziyaret ettiği dile getirilmektedir. Araştırma, Facebook kadar olmasa da Twitter'ın da Türkiye'de yaygın bir şekilde kullanıldığını belirtmektedir. 15 yaş üzeri internet kullanıcısı olan her 3 kişiden birisinin (% 32) Temmuz 2013 döneminde Twitter'ı ziyaret ettiği belirtilmektedir (Gençlik ve Spor Bakanlığı, 2013).

2014 yılı Ocak ayı içerisinde "wearesocial.sg" internet sitesinde yayınlanan "Küresel Sayısal İstatistikler 2014" (Global Digital Statistics 2014) raporunda da yukarıda paylaşılan verilere paralel ve daha güncel bilgiler bulunmaktadır.

Aşağıda yer alan ve açıklamaları yapılan Şekil 4.2, Şekil 4.3, Şekil 4.4, Şekil 4.5 ve Şekil 4.8 bu rapordan alınmış ve Türkçeye çevrilmiştir.

Şekil 4.2. Türkiye Anlık Bilgi



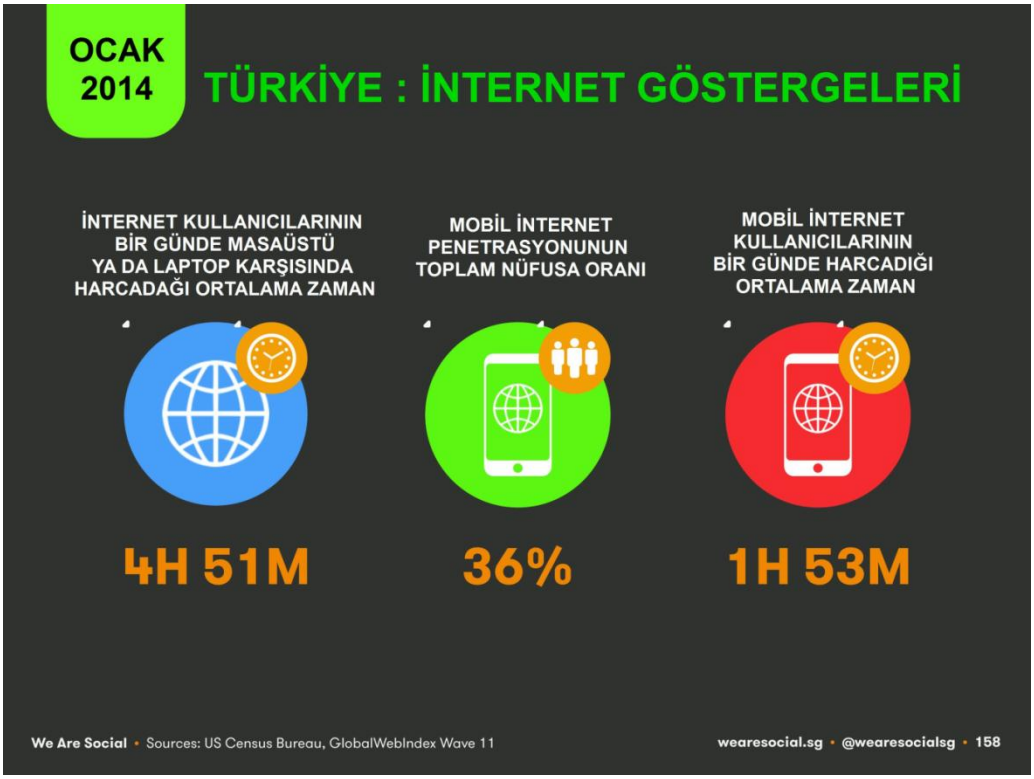
Kaynak: Global Digital Statistics (2014)

Şekil 4.2'de görüldüğü üzere söz konusu rapor Türkiye'nin toplam nüfusunu 80 milyon 694 bin 485 olarak kabul etmektedir. Türkiye'de 35 milyon 990 bin 932

internet kullanıcısı ve 68 milyon aktif cep telefonu abonesi olduğunu belirtmekte ve sırasıyla toplam nüfusa oranla %45 internet penetrasyonu, %84'te mobil penetrasyonu olduğunu göstermektedir (Global Digital Statistics ,2014).

Şekil 4.2'de bulunan veriler söz konusu rapordan alınan diğer şekillerde bulunan bilgilere temel oluşturmaktadır. Yani diğer şekillerde bulunan bilgiler Şekil 4.2'de yer alan verilerden yola çıkılarak hesaplanmıştır.

Şekil 4.3. Türkiye İnternet Göstergeleri- 1



Kaynak: Global Digital Statistics (2014)

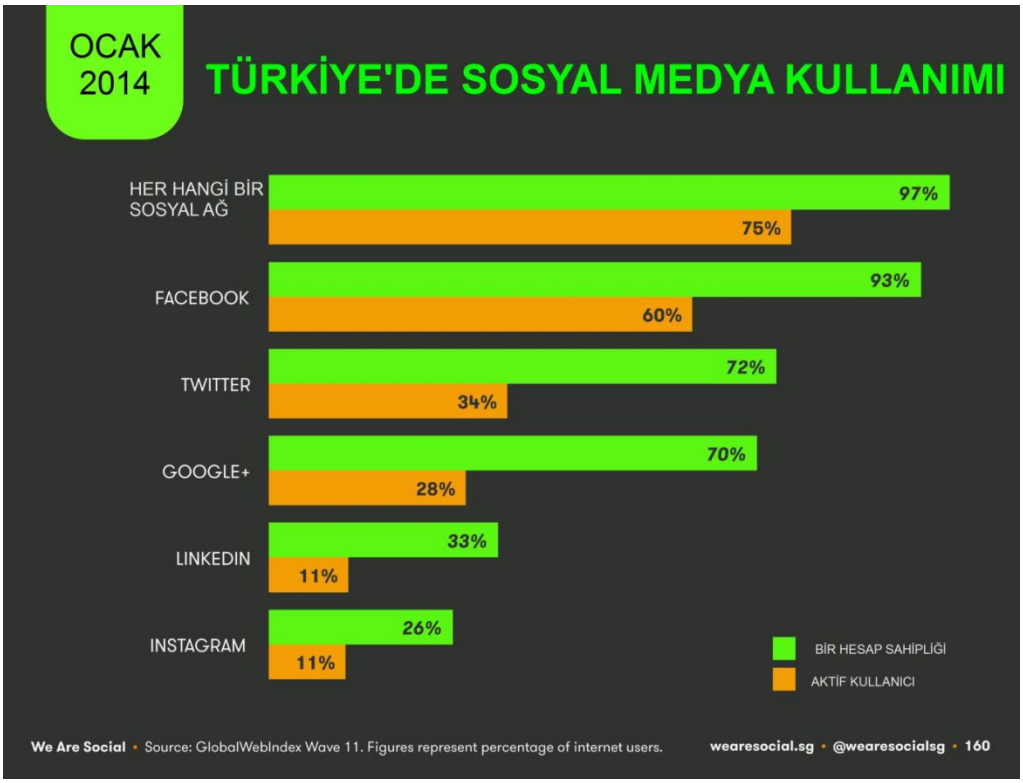
Şekil 4.3'te görüldüğü üzere Türkiye'deki internet kullanıcıları bir günde bilgisayar karşısında ortalama 4 saat 51 dakika zaman harcamaktadır. Mobil internet penetrasyonunun toplam nüfusa oranı ise %36'dır. Bu yaklaşık 29 milyon kullanıcı etmektedir. Mobil internet kullanıcılarının bir günde harcadığı ortalama zaman 1 saat 53 dakika olarak gösterilmiştir.

Şekil 4.4. Türkiye'de İnternet Göstergeleri-2

Kaynak: Global Digital Statistics (2014)

Şekil 4.4'te gösterildiği üzere Türkiye'de sosyal medya kullanımı toplam nüfusun %44'üne yayılmış ve sosyal medya kullanıcıları günde ortalama 2 saat 32 dakika sosyal medya sitelerinde vakit geçirmektedir. Cep telefonları vasıtasıyla sosyal medya uygulaması kullananların oranı %51'dir.Yer bildirim servisi kullanan mobil kullanıcıların oranı ise %26'dır.

Şekil 4.5. Türkiye'de Sosyal Medya Kullanımı



Kaynak: Global Digital Statistics (2014)

Şekil 4,5'te Türkiye'de en yaygın olarak kullanılan sosyal medya sitelerinin toplam kullanıcı ve bir önceki ay girenlerin yüzdesi üzerinden aktif kullanıcı sayısı belirtilmiştir.

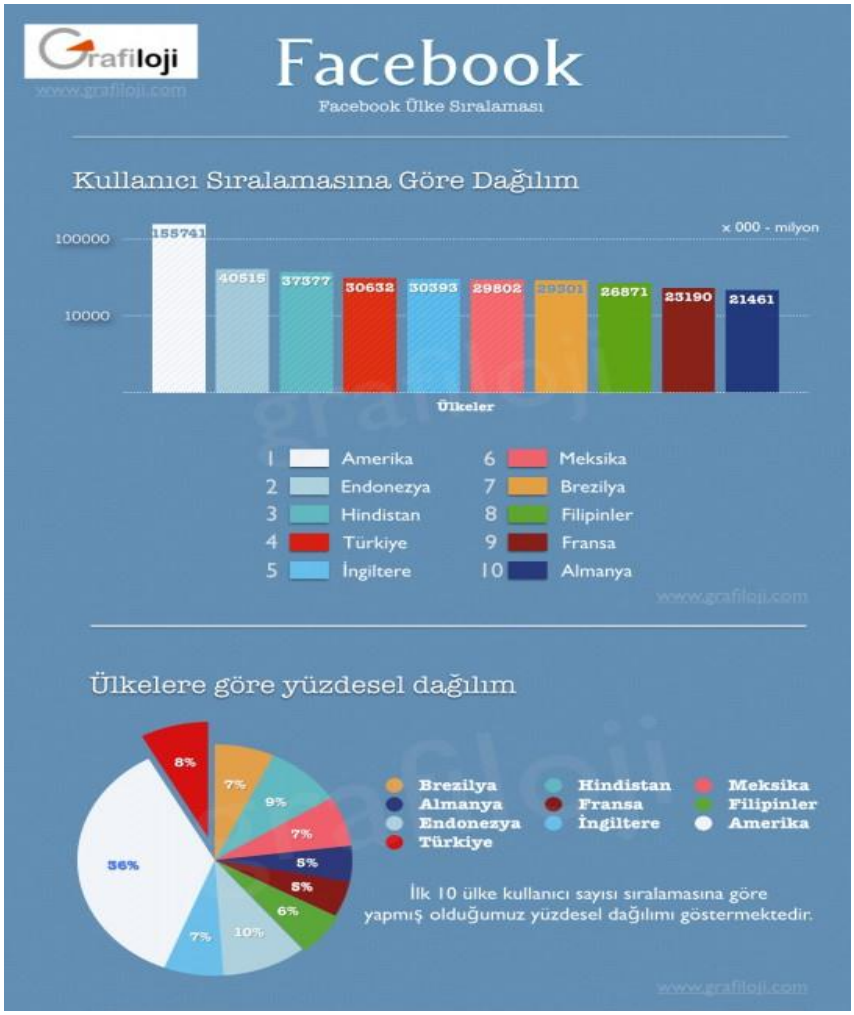
Rapora göre söz konusu sitelerin toplam kullanıcı sayıları Türkiye'nin toplam internet kullanıcısı sayısına oranla gösterilmiştir. Aşağıda verilen kullanıcı sayıları bu şekilde bulunmuştur.

Türkiye'de 36 milyon aktif Facebook kullanıcısı vardır. Bunu yaklaşık 25 milyon hesap ve 12 milyon üstünde aktif kullanıcı ile Twitter takip etmektedir. Twitter'ı yaklaşık 24 milyon hesap ile GOOGLE+ izlemektedir. Profesyonel iş ağı olarak yaygınlaşan LinkedIn'in de 11 Milyon 800 binin üstünde hesap sahibi ve Türkiye genelinde yaklaşık 4 milyon aktif kullanıcısı vardır. Çok popüler bir fotoğraf paylaşım sitesi olan Instagram'ın ise 9 milyon 300 bin civarında hesap sahibi ve yaklaşık 4 milyon aktif kullanıcısı bulunmaktadır (Global Digital Statistics 2014).

Raporda görüldüğü üzere Türkiye'deki en yaygın ilk iki sosyal paylaşım ağı Facebook ve Twitter'dır. Marketingland (2013)'ten alınan bilgiye göre de, Gigya adlı araştırma şirketinin yaptığı Temmuz 2013 istatistiklerinde Facebook ve Twitter'ın en çok içerik paylaşımının yapıldığı platformlar olduğu gösterilmiştir (Gürses,2013).

Social Boomer'dan alınan 2014 verilerine göre Türkiye, Facebook'ta ilk 10 ülke kullanıcı sayısı sıralamasında %8'lik yüzdesel dağılım ile 4. sırada bulunmaktadır. (Grafiloji,2014)

Şekil 4.6. Social Boomer'ın 2014 Verilerine Göre Facebook'ta İlk 10 Ülkenin Kullanıcı Sayıları



Kaynak: Grafiloji, (Temmuz, 2014)

AddThis'ten alınan 2013 verilerine göre Facebook'ta olduğu gibi Twitter'da da içerik paylaşımı konusunda ABD %27 ile ilk sırada yer almaktadır. Türkiye ise %4 ile altıncı sırada yer bulmaktadır (Gürses, 2013).

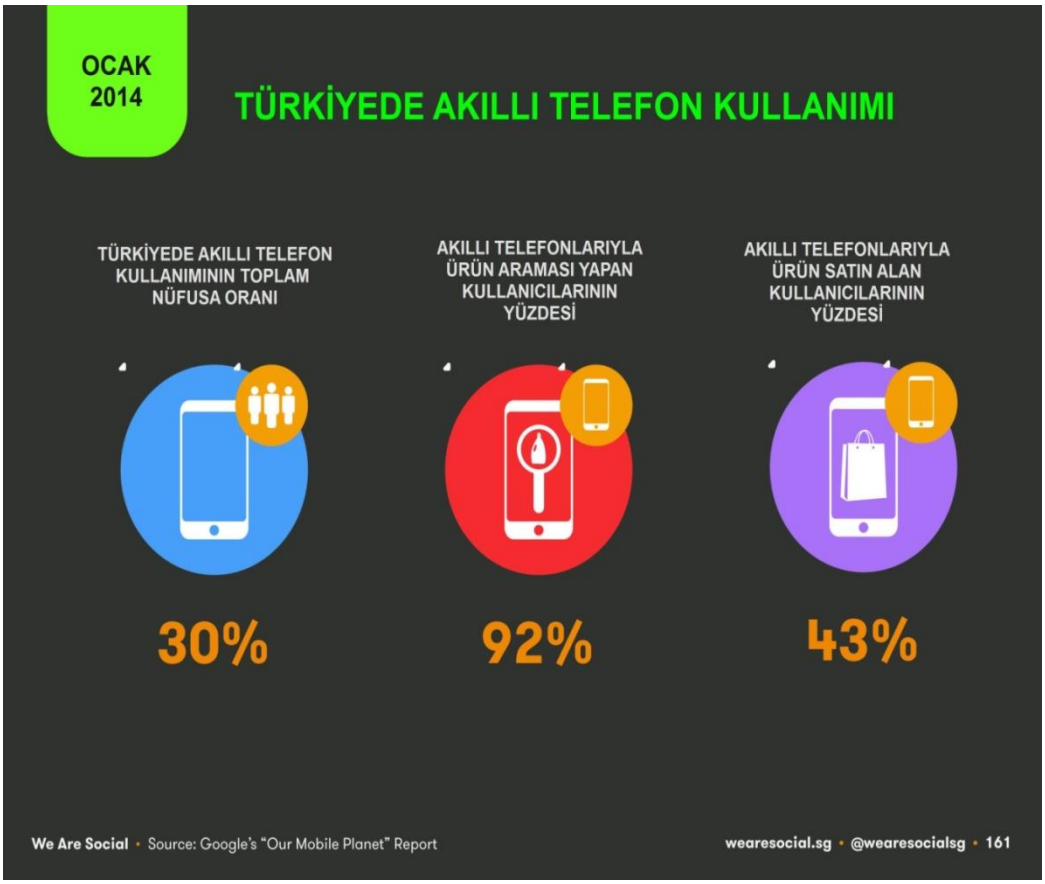
Şekil 4.7. AddThis'in 2013 Verilerine Göre Twitter Üzerinden Paylaşılan İçeriklerin Ülkelere Göre Dağılımı

Ülke	%
Amerika Birleşik Devletleri	% 27
Büyük Britanya	% 5
İspanya	% 5
Brezilya	% 4
Kanada	% 4
Türkiye	% 4
Fransa	% 4
İtalya	% 3
Hindistan	% 2
Venezuela	% 2
Hollanda	% 2
Meksika	% 2
Mısır	% 2
Japonya	% 2
Endonezya	% 2
Almanya	% 2
Suudi Arabistan	% 2
Arjantin	% 1
Avustralya	% 1
Rusya	% 1

Kaynak: (Gürses,2013)

Global Dijital Statistics 2014 raporunda Türkiye'de akıllı telefonların kullanımına dair verilerde sunulmuştur.

Şekli 4.8. Türkiye'de Akıllı Telefon Kullanımı



Kaynak: Global Digital Statistics (2014)

Şekil 4.8'de görüldüğü üzere Türkiye'de toplam nüfusun % 30'unda akıllı telefon bulunmaktadır. Akıllı telefon kullanıcılarının %92'si ürün aramalarını akıllı telefonları üzerinden yapıp % 43'ü alışverişlerini bu telefonları üzerinden gerçekleştirmektedir (Global Digital Statistics 2014).

Tüm bu veriler Türkiye'de sosyal medya kullanımının hiç de azımsanamayacak bir boyutta olduğunu ve her geçen gün daha da büyüyerek hayatımızın her alanında daha fazla yer almaya başladığına işaret etmektedir.

4.2. Türk Ceza Kanunu'nda Bilişim Alanında İşlenen Suçlar

Bilişim suçu kavramının, Türk Ceza Hukukuna ilk defa 1991 yılında 3756 sayılı Kanunla girmiş olup, Bilişim Alanında Suçlar başlığı altında şu an mülga durumdaki 765 Sayılı Kanun'un (Eski Türk Ceza Kanunu'nun) 525 inci maddesinde yasa koyucunun, bilişim alanı ihlallerini, bilişim suçu olarak isimlendirmeyi tercih ettiği görülmektedir (Koç ve Kaynak, 2010,s. 8). Bu kanun, 13/11/2005 tarih ve 25642 S.R.G. de yayımlanan 04/11/2004 tarih ve 5252 Sayılı Kanun'un 12. maddesi ile 1 Haziran 2005 tarihi itibariyle tüm ek değişiklikleriyle birlikte yürürlükten kaldırılmıştır.

Bugün yürürlükte olan 5237 sayılı TCK' nın 243 - 246. maddeleri arasında "Bilişim Alanında Suçlar" başlığı altında düzenlenen suçlar, klasik suçların aksine, sadece bilişim vasıtasıyla işlenen suçlar değil, aynı zamanda bütün hareket ve neticenin de bilişim alanında doğduğu suçlar olarak görülmektedir. Bugün TCK, Bilişim Alanında Suçları; "Yetkisiz Erişim", "Sisteme Müdahale", "Veriye Müdahale (Değiştirme, Bozma, Yok Etme, Erişilmez Kılma)", "Bilişim Sistemleri Aracılığıyla Yarar Sağlama" ve "Banka ve Kredi Kartlarının Kötüye Kullanımı" olarak sınıflandırmaktadır (Özocak, 2012).

4.3. Türk Ceza Kanunu'nda Bilişim Sistemleri Aracılığıyla İşlenen Suçlar

Bilişim teknolojilerinin yalnızca suç işlemenin bir aracı olarak kullanıldığı düşünüldüğünde, pek çok klasik ya da geleneksel suçun bilişim sistemleri aracılığıyla işlenebildiği görülmektedir. Örneğin, kalp rahatsızlığı olduğu bilinen bir kimsenin bilgisayarına kurulacak bir programla, korkutma yoluyla kalp krizi geçirmesini sağlanarak insan öldürme suçunun dahi bilişim sistemleri aracılığıyla işlenebileceği düşünüldüğünde, bu suçlar bakımından herhangi bir sınır konulmasının mümkün olmadığı düşünülmektedir (Özocak 2012).

Bilişim sistemleri aracılığıyla işlendiği sıkça görülen klasik suçlar ve TCK'da alınan tedbirler aşağıdaki bölümlerde irdelenecektir.

4.3.1. Hakaret ve Tehdit

Sosyal medyada en çok gerçekleştirilen suçların başında hakaret ve tehdit suçları görülmektedir. Hakaret suçunun TCK'nın 125. Maddesinde *"Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırmak",* tehdit suçunun ise TCK' nın 106. Maddesinde "Bir *başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit etmek"* şeklinde düzenlendiği görülmektedir (Özocak 2012).

Son yıllarda verilen yargı kararlarına bakıldığında, sosyal medya üzerinden, özellikle de Facebook ve Twitter gibi neredeyse herkesin kullanmakta olduğu sosyal ağlar üzerinden işlenen suçların, büyük bir çoğunluğunun hakaret ve tehdit suçları olduğu görülmektedir (Özocak 2012).

Sözlü, yazılı veya görsel biçimde işlenen klasik hakaret ve tehdit suçları gibi, sosyal medya üzerinden işlenen hakaret ve tehdit suçlarının da, tipik fiilde belirtilen unsurları taşıdıkları sürece, bu hükümlere göre cezalandırılacağı belirtilmektedir. Ancak, burada farklılık arzeden bir husus olarak, eğer fail tehdit suçunu sosyal medya üzerinden kendini tanınmayacak bir hale sokarak işlerse, örneğin, sahte isimle bir Facebook ya da Twitter hesabı açarak bir kişiyi ölümle tehdit ederse, bu fiilin tıpkı imzasız bir mektup gibi değerlendirileceği ve failin cezasının TCK m. 106/2(b)' deki *"Kişinin kendisini tanınmayacak bir hâle koyması suretiyle..."* düzenlemesi nedeniyle, ağırlaştırılacaktır" ifadesiyle cezalandırılacağı görülmektedir (Özocak 2012).

Sancar (2006, s.69), özellikle hakaret suçu bakımından değinilmesi gereken bir hususun da, fiilin TCK' da belirtilen bazı suçlardaki özel kasıtla işlenmesine haline dikkat çekmektedir. Örneğin, kişi bir sosyal ağdaki hesabı üzerinden cumhurbaşkanına hakaret ediyor yahut kanun koyucunun korunacak değer açısından özel önem yüklediği Türklüğü, Cumhuriyeti veya Devletin kurum ve kuruluşlarını aşağılıyorsa, burada artık TCK m. 125'den değil, özel düzenleme söz konusu olduğu

için TCK m. 299 veya 301'den ceza sorumluluğu doğacağını belirtmektedir (Özocak 2012).

4.3.2. Kişisel Verilerin Hukuka Aykırı Kaydedilmesi ve Yayılması

Sosyal medyada sıkça görülen suç tiplerinden biriside kişisel verilerin hukuka aykırı olarak kaydedilmesi ve yayılması olarak belirtilmektedir (Özocak 2012).

Şahin (2011) Civelek (2011) ve Kılınç (2012), ülkemizde kişisel verilerin korunmasına ilişkin yeterli yasal bir düzenleme ve yetkili bir kuruluş bulunmadığına dikkat çekmekte ve bu hususta farklı hukuksal düzenlemeler bulunduğunu belirtmektedir (Gürses, 2013) . Bunlar;

- Anayasa
- Türk Medeni Kanunu
- Türk Borçlar Kanunu
- Türk Ceza Kanunu
- Ceza Muhakemesi Kanunu
- Vergi Usul Kanunu
- İş Kanunu
- Nüfus Hizmetleri Kanunu
- Bilgi Edinme Kanunu
- Polis Vazife ve Salahiyet Kanunu
- 5809 Sayılı Elektronik Haberleşme Kanunu
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 5070 sayılı Elektronik İmza Kanunu
- Ceza Muhakemesinde Beden Muayenesi, Genetik İncelemeler ve Fizik Kimliğin Tespiti Hakkında Yönetmelik
- Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan iletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla izleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik
- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"

Özocak (2012),Türk Ceza Kanunundaki 135 ve 136 maddelere değinerek;

> Tipik fiillerin düzenlendiği TCK m. 135' *"Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir. Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır",* TCK m. 136 ise *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır"* hükümlerini ihtiva etmektedir.

Küzeci (2010.s.288), yasa koyucunun TCK 135. Maddesinin ilk fıkrasında kişisel verilerin hukuka aykırı olarak kaydedilmesini ararken, ikinci fıkrasında hukuka aykırı kayıt şartını aramamasına dikkat çekmiştir. Bu durumda, siyasi, felsefi veya dini görüşlere yahut ırksal kökenlere ilişkin verilerin kaydedilmesinde hukuka aykırı kayıt şartı aranmayacağını, bu tür kayıtların her halükarda suça vücut vereceğini belirtmektedir (Özocak 2012).

Dolayısıyla sosyal paylaşım sitelerinde kişilerin isim, kimlik bilgileri, cep telefonu numaraları, fotoğrafları gibi kişisel verilerinin rızaları dışında kaydedilmesinin veya yayılmasının suç sayılacağı dile getirilmektedir. Ancak kişilerin Facebook, Twitter vb. gibi herkesin görebileceği sosyal ağlarda fotoğraf veya saklamaya gerek duymadıkları kişisel bilgilerini yayınladıklarından, bunların kaydedilmesi TCK m. 135 kapsamında suç oluşturmayacağı belirtilmektedir. Fakat, kendi rızasıyla fotoğraflarını veya kişisel bilgilerini bu mecralarda paylaşan kişilerin bu rızası, söz konusu kişisel verilerin yayılmasını kapsamadığından, kaydedilen bu fotoğraf ve bilgilerin, veri sahibinin rızası dışında paylaşılmasının TCK m. 136 anlamında *"kişisel verilerin hukuka aykırı yayılması"* suçunu oluşturacağı belirtilmektedir (Özocak, 2012).

4.3.3. Özel Hayatın Gizliliğini İhlal

1982 Anayasasında, " kişinin hak ve ödevleri başlıklı II. Bölümünün IV. başlığında "özel hayatın gizliliği ve korunması" kavramına yer verildiği görülmektedir ve özel hayatın gizliliği ve korunması kavramının her fert için tartışmasız nitelikte temel bir hak olduğu belirtilmektedir (Koç, 2013,s.45).

Günümüzde gelişen bilişim teknolojisi ile kişilere ait bilgilerin, rızası olmaksızın siber uzay ortamına aktarılması ve böylece internet üzerinden herkes için ulaşılabilir kılınmaları olanaklı hale gelmiştir. Kişinin özel hayatına yönelik bu tarz haksız hareketlerin telafisi olanaksız zararlar meydana getirebileceği düşünülmektedir. Teknik olanaklar sayesinde kişinin özel hayatına ait bilgilerden oluşan kişisel verilerin; dinlenmesi, kaydedilmesi, değiştirilmesi, silinmesi, hatta ortadan kaldırılmasının mümkün olabileceği belirtilmektedir (Koç, 2013, s.46).

TCK'nın 134. maddesinde "Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır" ifadesi bulunmaktadır. Yani bir sosyal medya ağında bir kimseye ait özel görüşmeler yayınlanır ya da o kimsenin özel hayatına ilişkin özel bilgiler paylaşılırsa, fail TCK m. 134/1 uyarınca sorumlu tutulacağı görülmektedir. Maddenin ikinci fıkrasında ise, suçun ağırlaştırıcı halinin düzenlendiği ve özel hayata ilişkin görüntü veya seslerin ifşasında, cezanın ağırlaştırılacağı ifade edildiği görülmektedir (Özocak, 2012).

4.3.4. Cinsel Taciz

Sosyal medyada en sık görülen suçlardan birisinin de cinsel taciz suçu olduğu dile getirilmektedir. Suçu düzenleyen TCK'nın 105. maddesinde, cinsel taciz suçu için failin fiziksel temasını aramamakta, mağduru "cinsel amaçlı olarak taciz etmek" davranışını suç için yeterli gördüğü belirtilmektedir. Bu nedenle, sosyal medya ağları üzerinden, bir kimseye karşı cinsel içerikli sözler söylemek veya bu amaçla görseller paylaşmak gibi fiillerin, TCK m. 105 açısından cinsel taciz suçu sayılacağı görülmektedir (Özocak, 2012).

4.4.5. Müstehcenlik - İnternette Çocuk Pornografisi

Müstehcenlik konusunun TCK'nın 226. Maddesinde düzenlendiği görülmektedir. Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişinin, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılacağı belirtilmektedir. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişinin ise iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılacağı görülmektedir (Koç ve Kaynak, 2010).

Sosyal medyanın da bu suçun sıkça işlendiği mecralardan birisi olarak karşımıza çıktığı görülmektedir. Günümüzde çocukların küçük yaştan itibaren iyi düzeyde bilgisayar kullanabilir hale geldiği ve sosyal ağlarda hesap açarak tanımadıkları kişilerle iletişime geçebildiği dile getirilmektedir. Bu bağlamda, sosyal ağlarda çocuklarla iletişime geçen yetişkinlerin, çocuklara müstehcen görüntüler göstermeleri yahut çocukları müstehcen ses veya yazılara maruz bırakmaları durumunda, bu suçun meydana geleceği belirtilmektedir (Özocak,2012).

TCK'nın 226. maddesinin, gerek çocukları müstehcen görüntü, ses ya da yazıya maruz bırakmayı, gerekse de müstehcen görüntü, ses ya da yazı içeren ürünlerde çocukları kullanmayı suç olarak tanımlamadığı görülmektedir (Özocak,2012).

Çocuk pornografisinin, ülkemizde yeni bir kavram olmasına karşın bütün Dünyada kararlılıkla üzerine gidilen bir suç olduğu dile getirilmektedir. Başta Amerika, Almanya, İspanya gibi ülkelerin üzerinde önemle durduğu ve tahkikatların İnterpol dairelerince yapıldığı önemli bir suç olarak görülmektedir. Bu tür sitelerin %60'ının ABD'de yapıldığı belirtilmektedir. Türkiye'de bu anlamda üretim olmadığı ve sadece izlenme ile yetinildiği konusunda bilgilendirmeler bulunmaktadır. Genelde bu sitelerden yalnızca meraktan birkaç resim indirene işlem yapılmadığı ancak çocuk pornografisi ile ilgili koleksiyon yapan bağımlıların tespiti ile yakalanması yoluna gidildiği bilinmektedir (Koç ve Kaynak, 2010).

4.4. Türkiye'de İnternet Alanına Yönelik Düzenlemeler Kapsamında 5651 Sayılı Kanun

4 Mayıs 2007 tarihinde kabul edilen 5651 Sayılı " İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 23 Mayıs 2007 tarihli resmi gazetede yayımlanmak suretiyle yürürlüğe girmiştir.

5651 Sayılı Kanun'un; içerik, yer ve erişim sağlayıcı gibi temel internet aktörlerinin sorumluluk rejimi ile belli suç tiplerine ilişkin içerik barındıran web sitelerine erişimin nasıl engelleneceği olmak üzere iki temel hususu düzenlediği görülmektedir. Bu nedenle 5651 Sayılı Kanun'un içerik sağlayıcılara ilişkin getirdiği hüküm dolayısıyla, sosyal medya paylaşımları sebebiyle hukuki sorumluluğun tespitinde büyük önem taşıdığı düşünülmektedir (Kaya).

5651 Sayılı Kanun'un, içerik sağlayıcıyı internet ortamında kullanıcılara her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımladığı görülmektedir (Kaya).

İçerik sağlayıcının sorumluluğu 5651 Sayılı Kanunun 4. maddesinde şu şekilde düzenlenmiştir (TİB, 2014);

> MADDE 4-
>
> (1) İçerik sağlayıcı, internet ortamında kullanıma sunduğu her türlü içerikten sorumludur.
>
> (2) İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur.
>
> (3) (Ek: 6/2/2014-6518/87 md.) İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır.

Kanunun, içerik sağlayıcılarının internet ortamında kullanıma sunduğu her türlü içerikten sorumlu olduğunu kabul ettiği belirtilmektedir. İçerik sağlayıcının bu

doğrultuda "ürettiği, değiştirdiği veya sağladığı" her türlü içerikten dolayı hem cezai hem de hukuki sorumluluğu olduğu görülmektedir (Kaya).

5651 sayılı yasa çerçevesinde internet ortamında yapılan ve erişimi engellenebilen yayınlar aşağıda belirtilmiştir (TİB, 2014);

a) 5237 sayılı Türk Ceza Kanununda yer alan;

1) İntihara yönlendirme (madde 84),

2) Çocukların cinsel istismarı (madde 103, birinci fıkra),

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),

4) Sağlık için tehlikeli madde temini (madde 194),

5) Müstehcenlik (madde 226),

6) Fuhuş (madde 227),

7) Kumar oynanması için yer ve imkân sağlama (madde 228), suçları.

b) 25.7.1951 tarihli ve 5816 sayılı Atatürk Aleyhine işlenen Suçlar Hakkında Kanunda yer alan suçlar"

5651 sayılı Kanun'da belirtilen katalog suçlar kapsamında verilen erişimin engellenmesi kararlarının, kararı veren hâkim, mahkeme veya Cumhuriyet Savcısı tarafından gereği yapılmak üzere Telekomünikasyon İletişim Başkanlığına gönderildiği ve kararların Telekomünikasyon İletişim Başkanlığınca yerine getirileceği belirtilmektedir. Ayrıca yukarıda anılan suçların oluşması halinde ilgili içerik veya yer sağlayıcının yurtdışında olması durumunda TİB tarafından re'sen erişimin engellenmesinin yapılabileceği; müstehcenlik ve çocukların cinsel istismarı suçlarının oluşması ve içerik veya yer sağlayıcının yurt içinde bulunması durumunda yine Başkanlıkça re'sen erişimin engellenmesi yapılıp mahkeme onayına sunulabileceği görülmektedir (Gürses, 2013).

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"da öngörülen

engelleme işlemlerinin yasada sayılan katalog suçlar kapsamında gerçekleştirildiğinde, ifade özgürlüğünün anılan koşullar bağlamında sınırlandırılması olarak değerlendirilerek bu konuda verilecek tedbir kararının sınırlandırma ölçütlerine uygun olduğu sonucuna varıldığı belirtilmektedir. Zira 5651 sayılı Kanun'da düzenlenen erişimin engellenmesi tedbirinin Anayasada belirtilen sınırlama nedenlerinden biri olan "suçların önlenmesine" yönelik olduğu görülmektedir (Dülger ve Beceni, 2011, s.14).

Etkileri itibariyle son dönemde tartışmalara konu olan sosyal medya kavramı bahse mevzu kanunun yeniden gözden geçirilmesini gerekli kılmıştır. Nitekim 5651 Sayılı Kanun'da 6495, 6518 ve 6527 Sayılı Kanunlarla özellikle kişilik hakkı ve özel hayatın gizliliği ile ilgili konularda değişiklikler yapılmıştır.

5651 Sayılı Kanun'da değişikliğe gidilmesini gerektiren başlıca nedenleri aşağıdaki başlıklar altında özetlemek mümkündür (TİB, 2014) :

1- Sorumluluğunu yerine getirmeyen "Erişim ve İçerik Sağlayıcılara" hapis cezasının verilmesi mümkündü.

2- Bir kişinin kendisiyle ilgili bir içeriği çıkarmak istemesi halinde, bu süreç çok uzundu ve genellikle sonuç alınamamaktaydı.

3- Mahkeme kararlarının genelde "Erişimin engellenmesine" değil, "İçeriğin çıkarılmasına" yönelik olması nedeniyle, bu kararların uygulanması genellikle mümkün olmuyordu.

4- İçeriğin çıkartılması ile ilgili mahkeme kararında genellikle "URL Adresinin" yerine "IP Adresi" veriliyordu. Bunun sonucunda da içerik çıkarılması yerine tüm site kapatılıyordu.

6495, 6518 ve 6527 Sayılı Kanunlarla yapılan değişiklikler ile yukarıdaki konularda aşağıdaki düzenlemeler yapılmıştır (TİB,2014):

1- Erişim ve İçerik Sağlayıcılar için geçerli olan "hapis cezası" kaldırılmış, bunun yerine "para cezası" getirilmiştir.

2- “Trafik Bilgilerinin Saklanması” konusunda AB mevzuatı dikkate alınmış ve “Trafik bilgisinin” belirli bir süre saklanması istenmiştir. Saklanan bilgi “İçerik Bilgisi” değildir. Trafik Bilgisi; arayan ve aranan IP numaralarının hangi tarih ve saatte irtibat kurduklarına ilişkin bilgidir. Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ancak mahkeme kararı olması halinde istenebilecektir.

3- “Erişim Sağlayıcılar Birliği’nin” kurulması kararlaştırılmıştır. Bu Birlik koordinasyon amaçlıdır. Bu Birlik bünyesinde Kamu Kurumları bulunmayacaktır. Birliğin üyeleri;“İnternet Servis Sağlayıcıları ve Erişim Sağlayıcıları”dır. Erişim Sağlayıcılar Birliği 19 Mayıs 2014’te faaliyetlerine başlamıştır.

4- Kişilerin internetteki mağduriyetleri; “Kişilik Haklarının İhlali” ve “Özel Hayatın Gizliliğinin İhlali” olarak 2 temel grupta toplanmaktadır. Bu iki ihlalin engellenmesinde “Mahkeme Kararı”nın alınması esastır.

5- İnternet ortamında “Kişilik Haklarının İhlal” edildiğini iddia eden ve bu içeriğin çıkarılmasını isteyen kişilerin hareket şekli, aşağıda belirtilen şekilde olacaktır:

-Kişi; bu içeriğin çıkarılması için “İçerik veya Yer Sağlayıcısına” müracaat edebileceği gibi, doğrudan Sulh Ceza Mahkemesine de başvurabilecektir.

-Kişi; eğer “Sulh Ceza Mahkemesine” müracaat etmişse, hâkim bu başvuruya 24 saat içinde karar verecektir.

-Hâkim; kişinin müracaatını haklı bulursa, “Kişilik İhlalinin” gerçekleştiği yayının “URL Adresine Erişiminin Engellenmesine” ilişkin karar verecektir.

-Bu karar hâkim tarafından doğrudan “Erişim Sağlayıcılar Birliği’ne” gönderilecektir.

-Erişim Sağlayıcılar Birliği bu kararı 4 saat içinde tüm “Erişim Sağlayıcılarına” ileterek, bu URL’ye erişimi engelleyecektir.

-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.

-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.Bu kararda; söz konusu içeriğin öncelikle "engellenmesi" istenmekte, içeriğin çıkarılmasının daha sonra yapılması hedeflenmektedir. Hâkimin vereceği karar; yalnızca "Kişilik Hakkının İhlal" edildiği kısım veya sayfaya ilişkin "URL Adresi" olacağı için, bütün bir sitenin kapanması önlenecektir. Kişiye ilişkin aynı mahiyette içerikler başka internet adreslerinde de yayınlanabilir. Bu durumda ilgili kişinin müracaatı halinde; hâkimin verdiği "Erişimin Engellenmesi" kararı, Erişim Sağlayıcıları Birliği tarafından tüm adresler içinde uygulanacaktır.

6- İnternet ortamında "Özel Hayatının Gizliliğinin İhlal Edildiğini" iddia eden ve bu içeriğin çıkarılmasını isteyen kişilerin hareket şekli ise aşağıda belirtildiği gibi olacaktır:

-Kişi; söz konusu içeriğin çıkarılması için bu içeriğe ilişkin "URL Adresi" ve "kimliğini ispatlayıcı bilgiler" ile Telekomünikasyon İletişim Başkanlığı'na başvuracaktır.

-Telekomünikasyon İletişim Başkanlığı, müracaat eden kişinin Kimlik bilgilerini doğruladıktan sonra, bu talebi hemen "Erişim Sağlayıcılar Birliğine" iletecek, Birlik 4 saat içinde bu URL adresine erişimi engelleyecektir. Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

- Başvuru sahibi; erişimin engellenmesinden sonra en geç 24 saat içinde "Sulh Ceza Mahkemesi'ne" başvurmak zorundadır.

- Hâkim; kişinin müracaatını haklı görürse, “Özel Hayatın Gizliliğine” ilişkin yayının “URL Adresine Erişiminin” engellenmesine ilişkin karar verecektir.

- Bu karar hâkim tarafından” Erişim Sağlayıcılar Birliği’ne” gönderilecek ve belirtilen URL adresine erişimin engellenmesine devam edilecektir.

- Hâkimin kararı olumsuz olursa, yine bu karar “Erişim Sağlayıcılar Birliği’ne” gönderilecek ve engelleme kaldırılacaktır.

- Sulh Ceza Mahkemesi’nin bu konudaki olumlu/olumsuz kararının 48 saat içinde verilmesi gerekmektedir.

- Özel Hayatın Gizliliği” ile ilgili konularda istisnai olarak Telekomünikasyon İletişim Başkanı tarafından da erişimin engellenmesi yapılabilecektir. Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar.

5651 sayılı Kanunda yapılan bu düzenlemeler ile (TİB,2014):

1- Erişim Sağlayıcılar Birliği Kurularak internet üzerinde kamunun müdahalesi azaltılmıştır. Erişim Sağlayıcılar Birliği” tamamen sivil bir kuruluş olup, bu organizasyon içinde kamu kuruluşları bulunmamaktadır.

2- İnsanların internette en çok mağdur oldukları “Kişilik Haklarının İhlali” ve “Özel Hayatın Gizliliğinin İhlali” gibi iki önemli konuda çok hızlı ve sonuç alınabilir çözümler getirilmiştir.

3- Her iki durumda da kişinin bizzat kendisinin müracaatı gerekmektedir. Müracaat yöntemi oldukça basit ve sonuç odaklıdır.

4- Telekomünikasyon İletişim Başkanı’nın müdahale yetkisi çok sınırlıdır. Bu yetki; "Özel Hayatın Gizliliğine ilişkin olan ve gecikmesinde sakınca bulunan haller ile kısıtlanmıştır.

5- Erişim ve İçerik sağlayıcılardan bir yıldan az iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklanması istenilen bilgiler

“arayan ve aranan IP adresleri, arama tarih saat bilgisi” gibi trafik bilgileri olup, kesinlikle “İçerik Bilgisi” değildir.

6- Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ancak mahkeme kararı olması halinde istenebilecektir.

7- Erişim ve içerik sağlayıcılar için mevcut kanunda bulunan hapis cezası kaldırılarak, uluslararası büyük internet oyuncularının Türkiye’de faaliyet göstermelerinin önündeki en önemli engel aşılmıştır.

V. TÜRKİYE ve AVRUPA ÜLKELERİNDEN MAHKEME KARARI ÖRNEKLERİ

5.1. Emre Ersöz Davası

Türkiye'de bir kullanıcıya kendi yazdığı bir içerikten dolayı açılan ilk dava, 1998'de çevrimiçi bir Türk forumunda yaptığı yorumun ardından, "devletin emniyet kuvvetlerini alenen tahkir" suçundan 10 aya mahkûm edilen ve sonra bu cezası ertelenen Emre Ersöz'e açılan dava olarak belirtilmektedir (Koç, 2013).

18 yaşındaki Ersöz'ün Ankara'da, açık bırakılan çukurlar yüzünden gösteri yapan kör vatandaşlara karşı polisin sert müdahale ettiği iddialarını içeren bir mesajı forum sayfalarına gönderdiği ve bunun üzerine Savcının Ersöz aleyhine TCK'nın 159. maddesinin 1. fıkrası uyarınca dava açtığı ve sanığın bir yıldan dört yıla kadar hapis cezasına çarptırılmasını talep ettiği belirtilmektedir. Ersöz'ün yazdıklarının kamuya açık olmadığını ileri sürerek beraat talep ettiği ve duruşma sırasında, forumun yalnızca İnternet kullanıcılarına açık bir ortam olması nedeniyle kendisinin çevrimiçi yorumlarının aleni sayılamayacağını belirttiği görülmektedir (Koç, 2013).

Ersöz'ün yargılama sonunda suçlu bulunduğu, ancak beş yıl içinde benzer bir ceza almaması koşuluyla 10 aya indirilen cezasının ertelendiği belirtilmektedir (Koç, 2013).

5.2. Türkiye'de Twitter Üzerinden Yapılan Tehdit ve Hakaret Suçlamalarına İlişkin Hapis Cezası Verilen İlk Dava

Manken Nilay Dorsa ile Twitter'dan hakaret ettiği gerekçesiyle mahkemeye verilen menajer Sercan Dinçşahin arasındaki dava Türkiye'de twitter üzerinden yapılan tehdit ve hakaret suçlamalarına ilişkin hapis cezası verilen ilk dava olması açısından önemli bir örnektir.

Nilay Dorsa'ya gönderdiği "Sen her yüzüne güleni, dostun sanma ama beni has düşmanın bil bundan böyle" ve "Ben seni mahkemeye vereceğim. Sen dua et ki karşıma bu yakınlarda çıkmayasın pislik" şeklindeki tweetleri nedeniyle suçlu bulunan Sercan Dinçşahin'in bugüne kadar Twitter'da tehdit ve hakaret suçundan ceza alan ilk kişi olduğu görülmektedir (Kural, 2013).

İstanbul 18. Sulh Ceza Mahkemesi'nin sosyal paylaşım sitesi "Twitter" üzerinden manken Nilay Dorsa'ya "tehditte bulunduğu" gerekçesiyle Sercan Dinçşahin'in 5 ay hapis ve "hakaret ettiği" gerekçesiyle de bin 500 TL para cezasına çarptırılmasına karar verdiği görülmektedir. Ancak sanığa verilen bu cezanın açıklanmasının, 5 yıllık denetimli serbestlik süresi ve bir daha suç işlememe şartıyla geri bırakılmasına hükmedildiği belirtilmektedir (AA, 2013).

5.3. Coşkun Ak Davası

İlkiz, Nebil ve Tozkoparak, çevrimiçi yayıncılık konusunda Türkiye'de kullanıcıya değil de yayıncıya açılan ilk dava olan Coşkun Ak davasının, forum yöneticisi (moderator) Ak'ın beraat etmesiyle sonuçlandığını ve iki kere temyize giden bu davanın kararının internet sektöründe ve kullanıcı çevrelerinde de memnuniyet yarattığını dile getirmektedir (Koç,2013).

Coşkun Ak'ın Superonline şirketinin interaktif bölümler koordinatörü olduğu dönemde, internet sitesinde okuyucuların düşüncelerini aktardığı Türkiye'deki insan hakkı ihlalleri hakkında açılmış Superonline forumuna kimliği tespit edilemeyen bir üye tarafından yazılan bir mesaj nedeniyle, başka bir okuyucu tarafından savcılığa şikayet edildiği görülmektedir (Koç,2013).

Konuyu inceleyen Cumhuriyet Savcısının İnternet üzerinde işlenen suçlara ilişkin bir düzenleme olmadığını kabul ettiği ancak, Coşkun Ak'ın görevinin tıpkı bir gazetenin yazı işleri müdürününkine benzediğini belirterek, davanın görüldüğü sırada geçerli olan kuralların "kıyasen" Coşkun Ak aleyhinde de uygulanabileceği sonucuna ulaştığı belirtilmektedir (Koç,2013).

İstanbul 4. Ağır Ceza Mahkemesi'nde, Basın Kanunu çerçevesinde açılan davanın 27 Mart 2001'de sonuca ulaştığı görülmektedir. Coşkun Ak'a 40 ay ağır hapis cezası verildiği ancak bu cezanın ilk temyizde 14 Kasım 2001'de 6 milyon TL ağır para cezasına çevrildiği ve Yargıtay 9. Ceza Dairesi'nin bu hükmü bozduğu belirtilmektedir. Yargıtay'ın Ak davasını, suç içeren içerikten onun ya da bir başkasının sorumlu tutulup tutulamayacağı konusunda üniversitelerden seçilecek

bilirkişilerin vereceği karara bakılarak incelenmesini istediği görülmektedir (Koç,2013).

Yargıtay'ın kararı bozmasından sonra davayı yeniden inceleyen ilk derece mahkemesi olan İstanbul 4. Ağır Ceza Mahkemesi'nin Mart 2002'de Coşkun Ak aleyhine verdiği kararda direndiği görülmektedir. Bununla birlikte Basın Kanunu'nun ilgili 159. maddesinde yapılan değişikliğe dayanarak cezayı 40 aylık hapis cezasını 6 milyon TL (yaklaşık 4 $) ağır para cezasına çevirdiği ve bunun üzerine Coşkun Ak ve Avukatı Fikret İlkiz'in yeniden temyize başvurdukları görülmektedir. Yeniden değerlendirilen davanın 24 Nisan 2003 tarihinde sonuca vardığı ve kararın Yargıtay Ceza Genel Kurulu tarafından bozulmuş olduğu belirtilmektedir (Koç, 2013).

Coşkun Ak için verilen beraat kararına Ak'ın avukatı tarafından ileri sürülen hususlardan dolayı değil, 159. maddede yapılan değişiklik sayesinde varıldığı belirtilmektedir. Genel Kurul'un maddeye eklenen "sadece eleştirmek maksadıyla yapılan yazılı, sözlü veya görüntülü düşünce açıklamaları cezayı gerektirmez" kuralını Ak davasına da uyguladığı görülmektedir (Koç, 2013).

5.4. Türkiye'de Twitter'ın Kapatılması Süreci ve Anayasa Mahkemesi'nin Kararı

Tezimizin bütünlüğü açısından 2014 yılı Mart ayı içerisinde ülkemizde vuku bulan Twitter'in kapatılması ve ardından yaşanan sürecin incelenmesi büyük önem arz etmektedir.

Yaşanan süreç kısaca aşağıdaki gibi özetlenebilir:

Adı geçen firma içeriğinde bulunan bazı hesaplar hakkında, vatandaşlarımızın yaptığı şikâyetler üzerine kişilik haklarının ve özel hayatın gizliliğinin ihlali nedeniyle Türkiye Cumhuriyeti Mahkemelerince URL bazlı olarak erişimi engelleme kararı verilmiştir.

Mahkeme kararları çerçevesinde URL bazlı engelleme talepleri, Twitter'in sunduğu içeriklere ait adreslerin tamamının, "güvenli-security-https" kodlu olması nedeniyle

karşılanamamıştır. Güvenli kodlu adresler doğrudan ilgili firmanın işbirliğini gerektirmektedir.

Erişimi engelleme talepleri, elektronik ortamda bahsi geçen firmaya iletilmiş, fakat iyi niyetli çabalara rağmen, adı geçen firma bu kararlara duyarsız kalmış, içerikler çıkarılmamış ve mahkeme kararları yerine getirilmemiştir.

Bu nedenle mahkeme kararlarıyla mağdur oldukları tespit edilen vatandaşlarımızın ileride telafisi mümkün olmayacak sorunlarla karşılaşmaması ve mağduriyetlerinin önlenmesi için, TİB tarafından söz konusu firmanın internet sayfasına 21.03.2014 tarihinde bütünüyle erişim engellenmesi tedbiri uygulanmıştır.

Bu olay hem yurt içinde hem de yurt dışında büyük ses getirmiştir.

Ancak erişim engellemesi sonrasında Türkiye'de Ofisi ya da temsilcisi olmayan Twitter firması Türkiye'de bir temsilci belirlemiş ve bu çerçevede bir takım görüşmeler başlatmıştır.

22.03.2014 tarihinde yapılan ilk görüşmede mevcut mahkeme kararlarından 4 tanesinin gereği yerine getirilmiştir. 01.04.2014 tarihinde yapılan ikinci görüşmede ise, 01.01.2014 tarihinden beri vatandaşlarımızın bireysel müracaatlarına dayalı engelleme talepleri ve diğer Mahkeme karalarının gereğinin yapılması Twitter firmasından talep edilmiştir.

BTK tarafından yapılan 21.03.2014 tarihli basın bildirisinde Twitter tarafından mahkeme kararlarının gereğini yerine getirmek üzere bir mekanizma kurulması halinde söz konusu tedbirin kaldırılacağı öngörülmüştür.

Ancak o dönemde İdari Mahkemelerde yargı süreci devam eden dosyalar olduğu halde Twitter'ın engellenmesiyle ilgili bireysel başvuruları görüşen Anayasa Mahkemesi "Twitter.com sitesine erişimin tamamen engellenmesini öngören işlemin kanuni dayanağının bulunmadığı ve bu sosyal paylaşım sitesine erişimin kanuni dayanağı olmaksızın ve sınırları belirsiz bir yasaklama kararı ile engellenmesinin demokratik toplumların en temel değerlerinden biri olan ifade özgürlüğüne ağır bir müdahale olduğu açıktır" ifadeleri ile Twitter'ın açılmasına karar vermiştir. Anayasa

Mahkemesine uyma zorunluluğu gereğince, Twitter firmasının internet sayfasından erişim engellemesi kaldırılmıştır.

Burada dikkat çekici bir hususta sitenin kapanması sonrası Türkiye'de her hangi bir ofisi ya da temsilcisi bulunmayan Twitter'ın hemen bir temsilci belirlemesi ve yetkili makamlarla görüşmeye başlamasıdır.

5.5. Fransa'da Yaşanan Bir Dava Örneği

Fransa Temyiz Mahkemesi'nin bir kadın işçinin kendisine ait Facebook ve msn profili üzerinden "hayatımızı zehir eden onun gibi yöneticilerin ve patronların sonu gelmeli" şeklindeki ifadesine yönelik olarak, 10 Nisan 2013 tarihinde aldığı kararda, kişinin profilinin sadece arkadaşlarına ve temaslarına açık bir alan olduğu belirtilerek, söz konusu kişinin bu tür sözlerinden dolayı kamuya bir açıklama yapmış olarak suçlanamayacağı kararını vermiş olduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Bu karar ile Temyiz Mahkemesi'nin özellikle Facebook gibi sosyal ağlar üzerinden kişilerin yayımladıkları içeriklerin kamuya yönelik değil, özel olduğunu kabul ettiği görülmektedir. Böylece, Facebook profili üzerinden yayımlananlar hakaret ya da kamu istismar gerekçeleriyle bundan böyle davaya tabi olmayacaktır. Bu karar ile Temyiz Mahkemesi'nin içtihat oluşturduğu görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Ancak bu kararda yargıçların iki sınırlama belirledikleri görülmektedir. İlk olarak Adaletin önünde Facebook profilinin "özel" olarak kabul edilebilmesi için Facebook profilinin herkese açık olmaması gerektiği belirtilmektedir. İkinci husus olarak ise Facebook profili üzerinden arkadaş sayısının dikkate alındığı görülmektedir. Facebook profili üzerinden yayımlananların özel olarak kabul edilebilmesi için, yayımlananların sadece sınırlı sayıda kişi tarafından erişilebilir olması gerekmektedir ancak mahkemenin bu konuda sayısal bir sınır belirtmediği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Karara göre "Birbirlerine ortak aidiyet, özlem ve hedefler" ile bağlanan kişilerin bir araya geldikleri ifade alanı "özeldir" ve mahkemenin aldığı kararda kişinin Facebook

profili üzerinden ulaşılabilen arkadaşlarının bu tanıma denk düştüğü görülmektedir. Bu içtihat ile Fransa'da sosyal ağ kullanıcılarının, hakaret ya da kamu istismarına dayalı kovuşturmaya konu olmalarının zorlaştığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

5.6. Avrupa Adalet Divanı'nın Vermiş Olduğu Google Kararı

Avrupa Adalet Divanı'nın bir şahsın kendisi ile ilgili bilgilerin arama motorlarından çıkarılması talebi üzerine vermiş olduğu kararın tezimiz konusu açısından önemli bir örnek olduğu düşünülmektedir.

Kararın ortaya çıkması özetle şöyledir:

Hugo Guidotti isimli Madridli cerrahın İspanyol gazetesi El País'da 1991 yılında yayınlanmış olan bir habere yönlendirilen linklerin çıkartılması için Google'a başvurduğu görülmektedir. Haber doktorun sözde yanlış yaptığı bir ameliyat ile ilgilidir. Ancak Google'dan sonuç alamayan kişi, kendisi ile ilgili bilgilerin arama motorlarından çıkarılmasını talep etme hakkı tanınması için mahkemeye başvurmuştur (Robinson, 2014).

Bunun üzerine, Avrupa Adalet Divanı'nın; bireylerin kendi isimlerinin yer aldığı haberlerin, yargı kararlarının ve diğer dokümanların arama sonuçlarından çıkarılmasını Google'dan talep edebileceği kararına vardığı görülmektedir. Yani Avrupa Adalet Divanı kararında arama motoru şirketlerinin kişinin bilgilerinin bulunduğu internet sayfalarına yönlendiren linklerin arama motorunda çıkmasından sorumlu olduğuna hükmetmiştir. Karar, bireylerin isimleri ile arama yapıldığında gazeteler gibi üçüncü parti sitelerde yer alan kendilerine ait bilgilere yönlendiren linklerin çıkartılması için Google ve diğer arama motorlarından talepte bulunabileceği anlamına gelmektedir ve buna dava sonuçları ve yasal duyurular da dâhil edilebilmektedir (Robinson, 2014).

Mahkeme kararında, arama sonuçlarında çıkan sonuçların etkisinin büyük olduğu ve bu nedenle kişilerin bazı materyalleri çıkarma haklarının olması gerektiği belirtilirken aynı zamanda toplum içerisinde belirli rolleri olan kişiler söz konusu

olduğunda kamu çıkarının da gözetilerek denge kurulması gerektiği belirtilmektedir (Robinson, 2014).

5.7. İngiltere'de Yaşanan Bir Dava Örneği

2010 yılında İngiltere'de gerçekleşen olayda, Twitter üzerinden yapılan bir paylaşımın 2003 tarihli İletişim Kanunun 127. maddesi kapsamında yargılandığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

2 Haziran 2010 günü yoğun kar yağışı sebebiyle Robin Hood Havaalanının kapandığını öğrenen Paul Chambers adlı kişi kızgınlığını, Twitter üzerinden "Lanet olsun! RobinHood havaalanı kapandı. Bir hafta süreniz var... Aksi halde hava alanını havaya uçuracağım" içerikli tweet ile dile getirdiği belirtilmektedir.

Chambers'ın İngiltere'nin 2003 tarihli İletişim Kanunu'nda (2003 Communications Act) yer alan elektronik iletişim ağlarında tehdit unsuru içeren mesajların gönderilmesini yasaklayan 127. maddeden yargılandığı ve para cezasına çarptırıldığı görülmektedir. Ancak temyiz sürecinde hâkimlerin mesajın "tehdit unsuru" içermeyen bir şaka olduğunu kabul ederek davayı düşürdükleri görülmektedir (Avrupa Birliği Bakanlığı, 2013).

İki yıl süren dava süreci boyunca, Chambers'ın farklı kesimlerden ifade özgürlüğünün kısıtlanamayacağına dair destek aldığı belirtilmektedir. Ayrıca, Kraliyet Savcılık Servisi (Crown Prosecution Service) adıyla anılan kurumun süreci uzattığı, kamu kaynaklarını böyle davalarla boşa harcadığı iddia edilerek eleştirilere maruz kaldığı görülmektedir. Bunun üzerine Kraliyet Savcılık Ofisi tarafından Aralık 2012 tarihinde sosyal medya aracılığıyla gönderilen mesajların soruşturulması hakkında usullerin belirlenmesi amacıyla bir yönerge hazırlanmasına ilişkin çalışmalar başlatıldığı belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

VI. AVRUPA BİRLİĞİ VE TÜRKİYE'DE İNTERNET VE SOSYAL MEDYA EĞİTİMİ

Günümüzde görsel ve işitsel paylaşımın sayısal teknolojiler sayesinde baş döndürücü bir hız ve kapasiteye ulaştığı dile getirilmektedir. Bireyin bu sürece bilgi ve erişim olanakları dâhilinde katılmakta olduğu ve çoğu zaman da oluşturduğu iletiler ile kaynak rolünü üstlendiği belirtilmektedir. Buckingham (2003), uzmanların, bireyin sayısal paylaşımda yer alması için öncelikle teknolojik yatırımın gerekli olduğunu belirttiklerini ancak, bireyin yeni medyadan yani sosyal medyadan etkin bir biçimde yararlanabilmesi için teknolojiye erişimin sağlanmasının ötesinde verilecek eleştirel medya eğitimi ile mümkün olabileceğini söylemektedir. Aksi takdirde görsel-işitsel paylaşımdaki kirliliğin doğru okuma biçimleri geliştiremeyen bireyin sömürülmesine ve yanlış yönlendirilmesine neden olacağını vurgulamaktadır (Akkor Gül, 2013, s.16).

Bu kapsamda sosyal medya alanına ilişkin eğitim çalışmalarının irdelenmesi çalışma bütünlüğü açısından önemli görülmektedir.

6.1. Avrupa Birliği'nde İnternet ve Sosyal Medya Alanına Yönelik Bilinçlendirme Çalışmaları

Avrupa Birliği (AB) düzleminde 2000 yılında Lizbon'da yapılan Avrupa zirvesinde "bilgi toplumu" ile bilgi ve iletişim teknolojileri arasındaki bağın, sunulan fırsatlar yanında, karşılaşılacak tehditlerin de gündeme getirilerek tartışıldığı görülmektedir. Bu çerçevede de medya okuryazarlığının önemine vurgu yapıldığı belirtilmektedir. Lizbon stratejisi çerçevesinde, geleceğin Avrupa'sının, yeni iletişim teknolojilerine dayanacağı, buna bağlı olarak enformasyon teknolojilerini kullanma becerilerinin artırılması yanında, bu eğitimle ilgili bütçenin de genişletilmesi gerektiği belirtilmektedir. Zirvede ayrıca e-öğrenme girişiminin, Avrupa Komisyonu tarafından benimsendiği görülmektedir (Asrak Hasdemîr, 2012).

Avrupa Komisyonu'nun Avrupa Birliği vatandaşlarının yeni medyada daha faal olabilmeleri ve özellikle gizli reklamlar ve mahremiyet ihlali gibi potansiyel risk teşkil eden konularda farkındalık geliştirebilmeleri için üye ülkelerin eğitim

programlarında medya eğitiminin zorunlu hale getirilmesi için çalışmalar yaptığı görülmektedir (Euractiv,2009).

Gül ve Tekinalp (2011), Avrupa Birliği'nin özellikle son beş senedir 'medya eğitimi' konusunda yürüttüğü çalışmaların, üyeliğe aday konumundaki Türkiye için ayrı bir önem taşıdığını çünkü Türkiye'deki medya eğitimi uygulamalarının henüz istenen düzeye ulaşamadığını dile getirmektedir. Ayrıca Avrupa Birliği'nin tavsiye kararları ve yönergeler ile çizdiği politikaların, üye ve üyeliğe aday devletlerin politikalarının şekillendirilmesinde önemli bir rol üstlendiği görülmektedir (Akkor Gül, 2013,s.16).

Livingstone, (2006), bireyin artık yeni medya ortamında salt tüketici konumundan sıyrılıp üreten kaynak rolünü üstlendiğini ve bunun çevrimiçi ortamda her an artan içerik, öngörülemeyen miktarda gerçek veya gerçek dışı enformasyon paylaşımına neden olduğunu belirtmektedir. Bu bağlamda medya okuryazarlığının, yeni medyanın eleştirel bir biçimde takip edilebilmesi için bir gereklilik olarak ortaya çıktığını vurgulamaktadır. Bu yaklaşıma göre Avrupa Birliği'nin medya okuryazarlığına yönelişinin özellikle 'yeni medyanın gelişimi' ve 'bireyin yeni konumu' ile ilintili olduğu görülmektedir (Akkor Gül, 2013, s.16).

Avrupa Birliği'nin özellikle sosyal medya alanını içeren 'medya okuryazarlığı' konusu ile ilgili düzenlemeleri olarak; 2007 yılında gerçekleştirdiği "Sayısal Ortamda Medya Okuryazarlığına Bir Avrupa Yaklaşımı" başlıklı bildirim ve 2009 yılında yayınladığı "Rekabet Edebilirliği Daha Yüksek Bir Görsel-İşitsel İçerik Sanayi ve Kapsayıcı Bir Bilgi Ekonomisi için Sayısal Ortamda Medya Okuryazarlığı" başlıklı tavsiye kararı gibi iki önemli yasal çalışmaya rastlanmaktadır (Akkor Gül, 2013, s.16).

20 Aralık 2007 tarihinde *Sayısal Ortamda Medya Okuryazarlığına Bir Avrupa Yaklaşımı* başlığıyla yayımlanan bildirimde özetle medya okuryazarlığının hem Avrupa Birliği hem de üye devletlerin politikalarında giderek önem kazandığı belirtilmektedir. Avrupa vatandaşlarının demokratik ve kültürel hayata etkin bir biçimde katılımları açısından medya okuryazarlığı eğitiminin artık bir gereklilik olduğu bildirilmektedir. Teknolojik gelişmeler ile değişen medya ekonomisinin yeni aktörlerinin kimler olduğu, sayısal medya tüketiminin getirdiği imkân ve aynı

zamanda tehlikelerin neler olabileceği gibi konular hakkında tüketicilerin bilgilendirilmesi gerektiği işaret edilmektedir (Akkor Gül, 2013, s.22).

Bildirimde medya okuryazarlığının "medyaya ulaşmak, medya endüstrisini tanımak ve sunumları eleştirel bir biçimde değerlendirmek ve ayrıca farklı ortamlarda ileti oluşturabilmek" şeklinde tanımlandığı görülmektedir. Planlanan medya okuryazarlığı eğitiminin başlıca üç alanda yoğunlaşacağı bildirilmektedir. Bunların, 'ticari iletişim', 'görsel-işitsel eserler' ve 'çevrimiçi içerik' olduğu belirtilmektedir. Özellikle gençlerin eleştirel bakışlarının geliştirilip bilinçli seçimler yapmalarını hedefledikleri vurgulanmaktadır (Akkor Gül, 2013,s.22). Çünkü Avrupalı gençlerin % 89'undan fazlasının internet vasıtasıyla sohbet odaları, bloglar, sosyal iletişim ağları gibi yeni medya mecralarını düzenli olarak kullandığı belirtilmektedir. Komisyon'un hedef kitlelerinden birinin özellikle gençler olmasının sebebi olarak birçoğunun yeni teknolojilerin tehditlerini göz ardı etmeleri gösterilmektedir (Euractiv,2009).

Yine aynı bildirimde 'çevrimiçi içerik' konusundaki medya okuryazarlığı hedefleri ve alanla ilgili olarak değerlendirmeler yapıldığı da görülmektedir. İnternetin medya tüketim alışkanlıklarını tamamen değiştirdiği ve geleneksel medyaya ulaşımın IPTV ve internetten radyo gibi yeni seçeneklerle de mümkün olabildiği dile getirilmektedir. Dünyanın her köşesinden gelen metin, görsel ve işitsel içeriğe farklı ortamlarda etkileşimli erişim sağlanabildiği vurgulanmaktadır. Ayrıca mevcut koşulların internet kullanıcılarına birçok imkânlar sağladığı gibi çeşitli tehlikelere de yol açabileceği belirtilmektedir. Medya okuryazarlığının bu alandaki hedefinin ise, internet kullanıcılarını çevrimiçi içerikleri eleştirel bir biçimde değerlendirmelerini sağlayacak çeşitli araçlar ile donatılması olduğu vurgulanmaktadır. Tüm bunların yanında söz konusu bildirimde; sayısal yapım ve yaratım becerilerinin geliştirilmesi, telif hakları konusunda tüketicilerin bilinçlendirilmesi ve arama motorlarının doğru kullanımının teşvik edilmesi gibi diğer başlıklarında yer aldığı görülmektedir (Akkor Gül, 2013, s.23).

Avrupa Birliği Komisyonu'nun 20 Ağustos 2009 tarihinde yayımladığı *Rekabet Edebilirliği Daha Yüksek Bir Görsel-İşitsel İçerik Sanayi ve Kapsayıcı Bir Bilgi Ekonomisi için Sayısal Ortamda Medya Okuryazarlığı* başlıklı tavsiye kararı

Komisyonun 2007 yılında başlattığı süreci somutlaştırması ve bu konudaki kararlılığını ortaya koyması açısından önemli bulunmaktadır (Akkor Gül, 2013, s.23).

Akkor Gül (2013) aşağıda da görüldüğü gibi, düzenleme incelendiğinde, Komisyonun üye devlet ve ilgili otoriteler ile medya sanayi olmak üzere başlıca iki gruba önerilerde bulunduğuna değinmiştir. Üye devletlere ve ilgili otoritelere kısaca şunlar önerilmektedir:

- Paydaşların etik kurallar gibi ortak düzenlemeler geliştirmeleri ve uygulamalar başlatmalarını sağlamak, özdenetim girişimlerini desteklemek,
- Komisyonun Avrupa'daki medya okuryazarlığı düzeyini değerlendirmek üzere yaptığı güncel çalışmayı takip ederek, sayısal medya okuryazarlığının farklı boyutlarını araştırmak üzere çalışma ve projeler başlatıp teşvik etmek,
- Medya okuryazarlığının zorunlu eğitimin bir parçası haline gelmesi için konferans ve çeşitli sosyal etkinlikler düzenleyerek bu konuda bir müzakere ortamının gelişmesine olanak sağlamak; medya okuryazarlığını 18 Aralık 2006 Avrupa Parlamentosu ve Avrupa Konseyi'nin ilgili tavsiye kararına dayanarak hayat boyu eğitimi temel yetkinliklerden biri olarak değerlendirmek,
- Vatandaşlara yönelik ulusal kampanyalar ile hem ulusal hem de Avrupa görsel-işitsel mirası hakkında bilinç oluşturmak,
- Kişisel verilerin bilgi ve iletişim ağlarına aktarımındaki olası riskler hakkında gençleri, öğretmen ve ebeveynleri çeşitli eğitim ve bilgilendirme kampanyaları ile uyarmak.

Medya sanayine ise şu önerilerde bulunulmuştur:

- Enformasyon ve yaratıcı içeriğin sayısal dünyada nasıl oluşturulduğu, kurgulanıp dağıtıldığı ve arama motorlarının nasıl kullanılması gerektiği hakkında kampanyalar düzenleyerek halkı bilgilendirmek,
- Ürün yerleştirme, çevrimiçi reklamcılık gibi ticari iletişimde kullanılan teknikler hakkında kampanyalar düzenleyerek vatandaşları kullanabilecekleri bilgiler ile donatmak; ayrıca reklam ve içerik arasındaki sınırı ayırt etmelerine yardımcı olacak bilgiler vermek,

- Etkileşimli reklamlar hazırlanırken özellikle gençlere yönelik enformasyon paketlerinin nasıl tasarlandığı hakkında mevcut yasal hükümlere değinerek bilgi vermek,
- Telif hakları gibi konuları da kapsayacak şekilde alanın ekonomi politiği hakkında bilgilendirici günler düzenlemek,

Ayrıca komisyonun medya okuryazarlığının sosyal dışlamanın yeni bir şekli olduğunu düşündüğü ve üye devletleri gelişmekte olan teknolojilerin nesiller arasında, farklı gelir ve sosyal konumdaki grubundaki insanlar arasında yaratacağı boşluğu gidermesi için çaba sarf etmeye yönelttiği görülmektedir. Ayrıca blogların hızla çoğalması ve içeriğin kontrol edilememesi gibi nedenlerle bilgi sağlayıcıların veya kaynakların amaçlarını sorgulamaksızın Web'de gezinen kullanıcıların kitle halinde yanlış bilgilenmeye yol açılabileceğine dikkat çekilmektedir (Euractiv, 2009).

6.2. Türkiye'de Medya Okuryazarlığı Kapsamında İnternet ve Sosyal Medya Alanına Yönelik Eğitim Çalışmaları

Türkiye'de söz konusu alana yönelik eğitim çalışmalarının medya okuryazarlığı kapsamı altında ele alındığı görülmektedir. Medya okuryazarlığı konusunun ise kamusal düzlemde 2000'li yıllarda ele alınmaya başladığı belirtilmektedir (Asrak Hasdemîr, 2012).

Türkiye'de medya okuryazarlığının ilk olarak 2003 yılındaki İletişim Şurasında gündeme getirildiği, 2004 yılında ise Eylem Planı düzeyinde çalışan Medya ve Şiddet Çalışma Grubunun sonuç raporunda Radyo Televizyon Üst Kurulu (RTÜK) önerisiyle gündeme alındığı görülmektedir. Bu çalışmalar doğrultusunda RTÜK ve Milli Eğitim Bakanlığı'nın (MEB) işbirliği ile 2006-2007 öğretim yılında Ankara, İstanbul, İzmir, Adana ve Erzurum olmak üzere beş pilot ilde okutulmaya başlanan medya okuryazarlığı dersinin, 2007-2008 öğretim yılında ilköğretim II. kademede seçmeli ders olarak okutulmaya başladığı görülmektedir (Kurt ve Kürüm, 2010, s.24).

Medya Okuryazarlığı dersinin amacının; medya karşısında etkiye en açık, en hassas grubu oluşturan çocukların, medya kurumunun yapısını, işleyişini, kurgulanmış içeriğin bilinçli bir şekilde değerlendirilmesini ve eleştirel olarak izlemesini, özetle, medya ile ilgili doğru soruları sorup, doğru yanıtları bulabilmesini sağlamak olarak tanımlandığı görülmektedir (RTÜK, 2014).

Bu çalışmanın, bilinçli bir medya kültürünün oluşturulması açısından önemli bir girişim olduğu ancak amaca ulaşmada tek başına yeterli olmayacağı dile getirilmektedir. Çocukların erken yaşlarda medyayla tanıştıkları dikkate alındığında bu becerilerin daha erken yaşlarda kazandırılması gerekli bulunmaktadır. Bunu sağlamanın bir yolu olarak çocuklara erken yaşlarda sorgulama, araştırma gibi becerilerin kazandırılması görülmektedir. Bu kapsamda da 2006 yılında uygulamaya konan yeni ilköğretim programının ortak temel becerileri arasında eleştirel düşünme bir beceri olarak tanımlanmaktadır ve bu becerinin öğrencilere kazandırılması gerekli görüldüğü belirtilmektedir (Kurt ve Kürüm,2010, s.24).

Diğer bir ifadeye göre, Medya Okuryazarlığı projesiyle, medyayı doğru okuyan, yaşadığı çevreye duyarlı, ülkesinin sorunlarını bilen, medya mesajlarını akıl süzgecinden geçirebilen bireyler yetiştirilmesi amaçlanmaktadır (RTÜK,2014).

Ders içeriğinde; İletişime Giriş, Kitle İletişimi, Etkili Bir Kitle İletişim Aracı Olarak Televizyon, Türkiye'de Televizyon Yayıncılığı, Televizyon Program Türleri, Aile, Çocuk ve Televizyon, Bir Kitle İletişim Aracı Olarak Radyo, Gazete ve Dergi ile İnternetin Özellikleri ve İşlevleri, İnternet Kullanımında Dikkat Edilmesi Gereken Hususlar gibi konu başlıkları bulunmaktadır (RTÜK,2014).

Görüldüğü gibi, söz konusu ders içerisinde internete yer verilmektedir. İnternet ünitesinde verilecek becerilerin ise "gözlem, eleştirel düşünme, yaratıcı düşünme, problem çözme, iletişim, bilgi teknolojilerini kullanma, Türkçeyi doğru, güzel ve etkili kullanmadır. Söz konusu ünitede verilecek temel değerler ise, "etik kurallara bağlılık, farklılıklara saygı duyma, sorumluluk, dürüstlük" olarak sıralandığı görülmektedir (Asrak Hasdemîr,2012, s.33).

Livingstone ve Haddon (2009), Türkiye'nin de aralarında bulunduğu 25 Avrupa ülkesinde yapılan bir çalışmanın sonuçlarına göre internet kullanımının tamamıyla çocukların günlük yaşantısının bir parçası haline geldiğini ve 9-16 yaş arasındaki çocukların %93'ünün en az haftada bir kez çevrimiçi olduklarını dile getirmiştir. (Asrak Hasdemîr,2012, s.33).

Livingstone vd. (2011, s.27), Türkiye, Romanya ve Macaristan'daki çocukların interneti güvenli bir biçimde kullanma, istenmeyen mesaj ve reklamları engelleme, istenmeyen/tanınmayan kişilerden gelecek mesajları önleme, fıltreleme seçeneklerini değiştirme, enformasyonu farklı internet sitelerinden doğrulama gibi dijital medya okuryazarlığı becerilerinin diğer ülkelere göre daha düşük olduğunu dile getirmektedir (Asrak Hasdemîr,2012,s.33).

Bu nedenle yeni medya okuryazarlığı kapsamında internet okuryazarlığını da içine alacak ve uygulamalarla destekleyecek bir medya okuryazarlığı müfredatının, çocukların bu konudaki bilgi ve becerilerini geliştirmesi açısından çok önemli olduğu görülmektedir. Böylece çocukların diğer medya araçlarının yanı sıra interneti de daha bilinçli ve etkin biçimde kullanabileceği belirtilmektedir (Asrak Hasdemîr,2012, s.35).

Bu aşamada dersin müfredatı ve kaynaklarının gözden geçirilmesi yanında dersin alanın uzmanı olan öğretmenler tarafından verilmesinin de çok önemli olduğu dile getirilmektedir. İletişim fakültesi mezunlarının pedagojik formasyon alarak dersin öğretmenliğini üstlenmeleri en uygun çözümlerden biri olarak değerlendirildiği görülmektedir (Asrak Hasdemîr,2012, s.35).

VII. SOSYAL MEDYA DÜZENLEMELERİ KAPSAMINDA AVRUPA BİRLİĞİ ve TÜRKİYE MUKAYASESİ ve ÖNERİLER

Günümüzde internet üzerinde oluşan trafiğin en büyük kısmını sosyal paylaşım ağlarının oluşturduğu belirtilmektedir. İnsanların sosyal paylaşım ağları üzerinden bilgi, haber veya ilgi alanlarına yönelik paylaşımlar yaptığı ve video, fotoğraf veya haber paylaşmanın bunların başında geldiği görülmektedir (Gürses, 2013).

Bu çalışma kapsamında gerçekleştirilen incelemeler doğrultusunda sosyal medyanın gerek yasal, gerek sosyal hayat anlamında önemli bir yer tuttuğu görülmektedir. Bu çalışmada temel olarak, sosyal medya ağlarının kullanım yaygınlığı incelenmiş olup, son yıllarda kullanımı giderek artan bu yeni medya mecrası ile işlenebilecek suçlara karşı alınan tedbirler ve yapılan düzenlemeler ele alınmıştır. Bu çerçevede, Avrupa Birliği'nde ve Türkiye'de internet ve sosyal medyaya ilişkin bazı düzenlemelere yer verilmiş olup, bu bölümde yukarıda yer verilen değerlendirmelere dayanılarak Türkiye ile Avrupa Birliği arasında karşılaştırma yapılarak Türkiye için bazı önerilerde bulunulacaktır.

7.1. Hukuksal Açıdan Mukayese ve Öneriler

İncelenen AB ülkelerindeki örneklerden de görüldüğü üzere, sosyal medya platformlarında işlenen suçların, geleneksel yöntemlerle işlenmiş olan suçlardan ayrı tutulmayarak "Gerçek Hayatta Suç Olan, Sanal Dünyada da Suçtur" ilkesinin, genel geçer uygulama haline geldiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Bu ilkeye paralel olarak, AB ülkelerinde, geleneksel suçların düzenlendiği ceza kanunlarında internet ortamında işlenen suçların da düzenlendiği görülmektedir. Siber suç olarak tanımlanan, internet, bilgisayar ve veri sistemlerine yönelik işlenen suçlar için özel kanuni düzenlemelere gidildiği veya yine ceza kanunları içinde bu suçlara yönelik güncellemeler gerçekleştirildiği görülmektedir. Ancak, ülkemizde örneği görülen "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında 5651 Sayılı Kanun" benzeri doğrudan internet ortamına yönelik yürürlüğe konmuş kanun örnekleri olmadığı görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Avrupa Birliği ülkelerinin siber suçla mücadele içinse buna yönelik mevzuat oluşturma yoluna gittikleri görülmektedir. Veri güvenliği, kişisel verilerin korunması gibi alanlarda yapılan düzenlemeler ise Avrupa Konseyi Siber Suçlar Sözleşmesi paralelinde yürütüldüğü belirtilmektedir (Avrupa Birliği Bakanlığı, 2013).

AB ülkelerine bakıldığında, internet ortamında işlenen hakaret/aşağılama gibi fiillerin yaptırıma tabi tutulduğu görülmektedir. İngiltere bu fiilleri kabahatler arasında sayıp para cezaları ile cezalandırırken; Fransa, Almanya, İtalya gibi örneklerde ise fiilin ağırlığına göre para ve hapis cezaları verilebildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Ülke örneklerindeki yasadışı içeriğin sorumluluğuna yönelik değerlendirmelerde ise içeriği ilk olarak üretenin sorumlu olduğu ilkesinin kabul edildiği görülmektedir. Bu içeriğin internette yayınlanmasına aracılık eden "ara hizmet sağlayıcıların" ise sorumsuzluğu esas olarak görülmektedir. Buna paralel olarak da erişim yasakları gibi uygulamalara ancak çocukların ve gençlerin cinsel istismarı gibi sebeplerle yer verildiği görülmektedir (Avrupa Birliği Bakanlığı, 2013).

Görüldüğü üzere internet ve sosyal medya alanında yapılan düzenlemeler için Avrupa Birliği ülkeleri ile Türkiye'nin "Gerçek Hayatta Suç Olan, Sanal Dünyada da Suçtur" ilkesinde hemfikir oldukları açıkça ortadadır. Her iki tarafında internet ve sosyal medya alanında getirdiği düzenlemeler bu ilke paralelinde gelişmektedir.

AB ülkelerinde, ülkemizdeki 5651 Sayılı Kanun benzeri doğrudan internet ortamına yönelik bir kanun bulunmamakla birlikte, internet ve sosyal medya vasıtasıyla işlenebilecek suçlar için bazı ülkelerin bu yönde çalışmaları olduğu görülmektedir.

Avrupa Birliği ülkeleri 1981 yılında "Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşmeyi kabul etmiş ve iç hukuklarında bu sözleşmeye uygun düzenlemeleri yapmışlardır. Ancak Türkiye, 1981 yılında sözleşmeyi imzalamış fakat henüz iç hukukuna dair düzenlemeleri yapmadığından onaylamamıştır. Bu yüzden de Türkiye'de kişisel verilerin korunmasına ilişkin henüz açık ve yeterli bir yasa ve veri işlemlerini kontrol edecek, denetleyecek bir kuruluş bulunmadığı görülmektedir (Gürses, 2013). Ancak

5651 Sayılı Kanun'da yapılan değişiklikler ile insanların internette en çok mağdur oldukları "Kişilik Haklarının İhlali" ve " Özel Hayatın Gizliliğinin İhlali" gibi iki önemli konuda çok hızlı ve sonuç alınabilir çözümler getirildiği görülmektedir. Ancak kişisel verilerle ilgili tüm hususları kapsayan yasal düzenlemenin biran evvel çıkartılmasına ve kişisel verilerin işlenmesi, korunması vb. süreçlerini kontrol edecek, denetleyecek "düzenleyici ve denetleyici" bir kurum kurulmasına ihtiyaç olduğu görülmektedir (Gürses, 2013).

Sosyal medya davalarına yönelik verilen örneklerde Avrupa Birliği ülkelerinde bu alandaki davaların uzun sürebildiği görülmektedir. İngiltere'de yaşanan bir dava örneği başlığı altında incelediğimiz Chambers Davası da bu durum için güzel bir örnektir. İki yıl süren dava süreci boyunca, Chambers farklı kesimlerden ifade özgürlüğünün kısıtlanamayacağına dair destek aldığı, Kraliyet Savcılık Servisi (Crown Prosecution Service) adıyla anılan kurumun ise süreci uzattığı ve kamu kaynaklarını böyle davalarla boşa harcadığı iddia edilerek eleştirilere maruz kaldığı görülmektedir (Avrupa Birliği Bakanlığı, 2013). 5651 Sayılı Kanun'daki son değişikliklerle, Türkiye'nin zaten bu tür davaların hızla sonuca ulaştırılabilmesi için önemli bir adım attığı görülmektedir. Ancak internet ve sosyal medya alanı için özel mahkemelerin kurulması bu tür davalardaki çözüm sürecini daha da hızlandırmak adına Türkiye için gerçekten de yerinde ve faydalı bir adım olabilir. Ayrıca Türkiye, bu girişimiyle AB ülkeleri için iyi bir örnek teşkil edebilir.

Sosyal medya alanına yönelik mahkemelerin kurulmasına ek olarak bilişime ilişkin bilgi sahibi olan hukukçuya ve hukuk bilen bilişimciye ihtiyaç olduğundan üniversitelerde bu konuyla ilgili olarak eğitim veren bölümlerin, kürsülerin kurulmasının teşvik edilmesinin de büyük önem arz ettiği düşünülmektedir (Gürses, 2013).

Bu noktada dile getirilebilecek diğer bir öneride bilişim ve hukuk bilimleri arasında terminolojik yapının kurulmasıdır. Türkiye'nin bilişim alanında önde gelen bir üretici ülke konumunda olmamasının bilişim alanında yabancı terminoloji kullanılmasına sebep olduğu görülmektedir. Bu nedenle, bilişim suçuyla ilgili birçok yabancı terminolojik kavram yasalarımızda mevcuttur. Bunların öz dilimizde ve

herkesin anlayacağı şekilde karşılıklarının bulunması büyük önem arz etmektedir (ntvmsnbc, 2011).

Tüm bunların yanında belki de sosyal medya alanında Türkiye'ye getirilebilecek en büyük öneri; milyon hatta milyarları bulan kullanıcı sayıları ile dev sosyal medya şirketlerinin Türkiye'de temsilcilik ve/veya ofis açmaları için gerekli yasanın ivedilikle çıkarılması olacaktır.

Gürses (2013), internet ortamında geniş kitlelere hizmet veren şirketlerin, bulunduğu ülkelerde ofis açmasının kanun ile belirtilmesini ifade ederek:

> Günümüzde internetin hayatımızda hızla yaygınlaşması sonucu hukuk dışı pek çok faaliyet hızlı bir şekilde yaygınlaşmaktadır. İnternet erişiminde rol oynayan "Sunucu (Server)" olarak adlandırılan ana bilgisayarların belli başlı ülkelerin tekelinde olması ve bulunduğu ülkelerin yasalarına tabi tutulması internet aracılığı ile ortaya çıkan kanunsuz oluşumlara imkân sağlamaktadır. İnternet ortamında geniş kitlelere hizmet veren şirketlerin bulunduğu ülkelerde ofis açması ve o ülkenin kişisel verilerinin bulunduğu sunucuların o ülkede bulundurulması yasa ile belirtilmelidir. Örneğin Facebook, Twitter, Google+, Youtube'un, çeşitli gerekçelerle (ülkemizden kazandığı gelirin vergisini ödememek vb.) için bir ofis açmaması dikkat çekmektedir. Bu gibi ofislerin açılması durumunda yaşanan bürokratik işlemlerin çok daha hızlı gerçekleşeceği yadsınamaz bir gerçektir.

Görüldüğü üzere internet ortamında geniş kitlelere hizmet veren şirketlerin ofis bulundurmamalarının Türkiye için hem ekonomik hem de bürokratik olumsuz sonuçları vardır.

Ekonomik açıdan bakıldığında Türkiye'de ofis bulundurmayan sosyal medya şirketleri, büyük kazançlar sağladıkları reklam hizmetlerini yurtdışından faturalandırmadıkları için Türkiye'ye vergi ödememekte ve bu durum Türkiye cari açığına olumsuz etki etmektedir.

Babaoğlan (2014, sözlü görüşme), bu alanda hizmet veren şirketlerin Türkiye'yi "ne gelirse kar sayılacak" bir pazar olarak gördüklerini ifade ederek:

> Türkiye'de durum çok farklı. Bu firmalar Türkiye'yi yatırım yapılacak bir pazar olarak değil, "ne gelirse kar sayılacak" bir pazar olarak görüyor. Google dışında birçoğu herhangi bir stratejik hamle ve adım bile atmıyor. Google bu konuda ufak tefek şeyler yapsada halen standardın çok gerisinde. Bu firmalar Türkiye'de bulunmama nedenlerini 5651 sayılı kanunun bir önceki halinde öngörülen hapis cezası maddesine vurgu yaparak açıklasalar da aslında onlara göre ana neden pazarın stabilizasyon sorunu. Bu nedenle burada bir ofis ve temas noktası bulundurmayı red ediyorlar.

Ofisi bulunmadığı halde Türkiye'de 5 yıldır faaliyet gösteren ve kullanıcı sayısını her geçen gün arttıran Twitter, Türkiye'den çok ciddi bir reklam geliri elde etmektedir. 2013 yılında 400 milyon doların üzerinde ciro yapan şirketin bu kazancının 35 milyon doları yani neredeyse 10/1'i Türkiye üzerinden kazanılmıştır. 2014 için 600 milyon dolara yakın bir ciro bekleyen şirketin Türkiye'den elde ettiği gelirin de 50 milyon dolara yaklaşması beklenmektedir. Bu da ortalama net kar olarak 100 milyon TL kazanç anlamına gelmektedir. Twitter'ın Türkiye'de ofis açması halinde ise kazancının yüzde 20'si kurumlar vergisi adı altında kesintiye uğrayacaktır. Bu da 100 milyon TL'de 20 milyon TL'nin devletin kasasına gireceği anlamına gelmektedir. Bunun yanı sıra gider tablosuna açılacak ofisin maliyeti ve ortalama 50 ile 100 personelin maaşı da eklenecektir. Tüm bu maliyetler göz önünde bulundurulduğunda Twitter'ın Türkiye'den elde ettiği yıllık kazancın neredeyse yarı yarıya azalmış olacağı öngörülmektedir (Haber 7, 2014).

Bu alanda hizmet veren Türk şirketleri hem KDV hem kurumlar hem de gelir vergisi öderken yukarıda verilen Twitter örneğinde de görüldüğü üzere Türkiye'de ofis açmayı ve vergi ödemeyi kabul etmeyen şirketler haksız rekabete ve Türkiye'nin cari açığının büyümesine yol açmaktadır.

Dünyanın Çin hariç internet erişiminin sağlanabildiği hemen hemen her ülkesinde toplam 250 milyon aktif kullanıcı ile faaliyet gösteren Twitter'ın sadece 13 ülkede ofisi bulunmaktadır. Twitter hesaplarının yüzde 77'sinin ABD dışında olmasına rağmen ofislerin 1'i merkez olmak üzere 11'i Amerika'dadır. Diğer ofislerin ise çoğu Avrupa'da olmak üzere sırasıyla Hollanda (Amsterdam), Almanya (Berlin), İrlanda

(Dublin), İngiltere (Londra), Fransa (Paris), İspanya (Madrid), Brezilya (Rio de Janeiro - SãoPaulo), Singapur, Avustralya (Sidney), Güney Kore (Seul), Japonya (Tokyo) ve Kanada'da (Toronto, Vancouver) yer almaktadır (Haber 7, 2014).

Twitter'ın ofis açtığı ülkelere bakıldığında ortaya çok çarpıcı bir tablo ortaya çıkmaktadır. Ortadoğu ve Afrika'da tek bir ofisi dahi bulunmayan Twitter'ın öte taraftan açtığı ofislerinin bulunduğu bazı ülkelerin nüfusu Türkiye'deki kullanıcı sayısının neredeyse yarısına bile denk gelmemektedir. Örneğin Singapur'un 5 milyon 312 bin, İrlanda'nın ise 5 milyon 589 bin nüfusu bulunmaktadır (Haber 7, 2014).

Twitter'ın 12 milyon aktif kullanıcısı olan Türkiye'de ofis açmazken nüfusu 5 milyon civarında olan İrlanda'da ya da 17 milyon olan Hollanda gibi Avrupa ülkelerinde ofis açması dikkat çekmektedir. 12 Milyon aktif kullanıcısı olan Türkiye'nin Twitter'a ofis açtırma konusunda çok geç kaldığı görülmektedir.

Twitter sadece bir örnektir. Facebook, Youtube, Google+ gibi daha nice dev sosyal medya şirketi Türkiye'de faaliyet gösterdiği unutulmamalıdır.

Bu tür şirketlerin Türkiye'de bir ofis açmamaları için öne sürdükleri en büyük savlarından birisinin 5651 Sayılı Kanun'daki erişim ve içerik sağlayıcıları için geçerli olan "Hapis cezası" maddesi olduğu belirtilmektedir (Babaoğlan, 2014). Ancak, 5651 Sayılı kanunda yapılan değişiklikle hapis cezasının para cezasına çevrildiği tezimizin bu konuyla ilgili bölümlerinde belirtilmiştir. Yani artık Twitter gibi Türkiye'de ofis ya da temsilcilik kurmak istemeyen sosyal medya şirketlerinin öne sürecekleri hukuki bir çekince kalmadığı görülmektedir.

Ayrıca sosyal medya şirketlerinin her ülke için aynı olaylarda farklı davranışlar sergilemesi, devletler tarafından bu şirketlere olan güvenirliliğin azalmasına neden olmaktadır. Ayrıca, uluslararası arenada da sosyal medya alanında ciddi bir denetimsiz yapının olduğunu göstermektedir. Bu denetimsizliğin ve söz konusu alana yönelik ülkelerin birbirinden farklılık gösteren uygulamalarının ortadan kaldırılması için, aynı "Avrupa Konseyi Siber Suçlar Sözleşmesi" gibi internet alanında bir denetim mekanizması oluşturacak uluslararası bağlayıcılığı olan ortak bir anlaşmaya ihtiyaç vardır. Bu tür bir uluslararası düzenleme hem anlaşmaya taraf devletler hem

de sosyal medya alanında faaliyet gösteren şirketler için karşılıklı güven ortamını tahsis edecek ve bu alana denetim getirecektir.

Bu noktada Türkiye böyle bir sözleşmenin amacı ve söz konusu alanda yaratacağı güven ortamı konusunda farkındalık oluşturmalıdır. Türkiye'nin sosyal medya şirketlerinin ofis açmadığı ülkelere yönelik yoğun lobicilik çalışması yapması yerinde bir adım olacaktır.

7.2. Sosyal Açıdan Mukayese ve Öneriler

Avrupa Komisyonu'nun Avrupa Birliği vatandaşları için sosyal medya platformlarında daha faal olabilmeleri ve özellikle gizli reklamlar, mahremiyet ihlali gibi potansiyel risk teşkil eden konularda farkındalık geliştirebilmeleri için üye ülkelerin eğitim programlarında medya eğitiminin zorunlu hale getirilmesi için yaptığı çalışmalar çok önemlidir. Avrupa Parlamentosu'nun da desteğiyle, Komisyon üye ülkeler için bir tavsiye mektubu yayınlamış ve yetişkinler için yeni medya eğitimine tabi tutabilecek kurslar düzenlenmesini ve okul eğitim müfredatlarında bu eğitim türünün zorunlu hale getirilmesini istemiştir.

Türkiye'de yetişkinler için sosyal medya alanına yönelik eğitim çalışmaları yapıldığı görülmemektedir. Bu nedenle Türkiye'de de Avrupa Komisyonu'nun dile getirdiği gibi sosyal medya kullanıcıları için eğitici kurslar düzenlenmesi yerinde olacaktır. Türkiye'deki kullanıcıların, kişisel bilgilerin önemi konusunda bilinçlendirilmesi ve sosyal paylaşım ağları üzerinde paylaşılan kişisel verilerin başka kimseler tarafından görülebileceği, yorumlanabileceği ve paylaşan kişinin bundan ileride zarar görebileceği gibi konuların göz önünde tutulması büyük önem arz etmektedir.

Ayrıca orta öğretim çağındaki öğrencilerin, bilinçlenmeleri ve farkındalıklarının artırılması için bilişim suçları ve sosyal paylaşım ağlarının güvenli kullanımı ile ilgili seminerler verilmesi veya müfredata bu konu ile ilgili dersler eklenmesi yerinde bir adım olacaktır (Gürses, 2013). Çünkü Türkiye'de okutulan medya okuryazarlığı dersinin içeriğinde bu konulara yönelik bir çalışma olmadığı ilgili konunun irdelendiği bölümde görülmektedir. Ayrıca Avrupa Komisyonu'nun da tavsiyesinde

görüldüğü üzere okul eğitim müfredatlarında bu eğitim türünün zorunlu hale getirilmesi Türkiye içinde önemli bir adım olacaktır.

Tüm önerileri kısaca özetleyecek olursak;

- Kişisel verilerle ilgili tüm hususları kapsayan yasal düzenlemenin biran evvel çıkartılması ve kişisel verilerin işlenmesi, korunması vb. süreçlerini kontrol edecek, denetleyecek "düzenleyici ve denetleyici" bir kurum kurulması gerekmektedir.
- İnternet ortamında işlenen suçların hızlıca karara bağlanması için özel mahkemelerin kurulması yerinde olacaktır.
- Bilişime ilişkin bilgi sahibi olan hukukçuya ve hukuk bilen bilişimciye ihtiyaç olduğundan üniversitelerde bu konuyla ilgili olarak eğitim veren bölümlerin, kürsülerin kurulmasının teşvik edilmesi gerekmektedir.
- Bilişim ve hukuk bilimleri arasında terminolojik yapının kurulması önem arz etmektedir.
- Sosyal medya kullanıcıları için eğitici kurslar düzenlenmesi, kullanıcıların, kişisel bilgilerinin önemi konusunda bilinçlendirilmesi, ortaöğretim çağındakiler için müfredata bu konu ile ilgili dersler eklenmesi Türkiye için yerinde bir adım olacaktır.
- Sosyal medya şirketlerinin Türkiye'de temsilcilik ve/veya ofis açmaları için gerekli yasanın ivedilikle çıkarılması gerekmektedir.
- Türkiye internet ve sosyal medya alanında denetim mekanizması oluşturacak uluslararası bağlayıcılığı olan bir sözleşmenin oluşturulması için farkındalık oluşturmalıdır. Bu kapsamda Türkiye'nin sosyal medya şirketlerinin faaliyet gösterip ofis açmadığı ülkelere yönelik yoğun lobicilik çalışması yerinde bir adım olacaktır.

SONUÇ

Sosyal medyanın çalışmamız içersinde değindiğimiz Arap Baharı ve Taksim Gezi Parkı Olayları gibi kitlesel halk hareketlerinde, bir örgütlenme ve iletişim aracı olarak ne kadar etkili olduğu görülmektedir. Sosyal medya platformlarının haber alma özgürlüğü gibi konularda fırsat yarattığı ancak bilinçsiz veya kötü niyetli kişiler tarafından kullanılmasının ise büyük riskleri ve olumsuzlukları beraberinde getirdiği belirtilmektedir. Kimi kullanıcıların, birilerinin özel hayatının gizliliğini ihlal edip, doğruluğu ispatlanmamış ya da devlet sırrı niteliğindeki bilgileri ifşa edebileceği ya da içeriği değiştirilmiş maksatlı paylaşımlar, yalan haber ve iftiralar ile suç işleyip, başka insanları suça teşvik edebileceği görülmektedir. Bu noktada, bu denli önemli etkileri olan ve mağduriyetlere neden olabilen sosyal medya alanına yönelik düzenlemelerin olmaması gibi bir durum söz konusu değildir.

İncelediğimiz örneklerde de görüldüğü üzere, AB ülkelerinde de sosyal medya ortamlarında ortamda işlenen suçlara karşı, "Gerçek Hayatta Suç Olan, Sanal Dünyada da Suçtur" ilkesi ile hareket edildiği görülmektedir. Bu ilkeye paralel olarak, geleneksel suçlarını düzenlendikleri ceza kanunlarında internet ortamında işlenen suçları da düzenledikleri anlaşılmaktadır. Bu çalışma kapsamında gerçekleştirilen incelemeler doğrultusunda Türkiye'nin sosyal medya alanında AB ülkeleriyle hemen hemen aynı şekilde hareket ettiği görülmektedir.

Türkiye'nin bu alanda en büyük sorunu olarak karşımıza sosyal medya şirketlerinin Türkiye'de ofis bulundurmamaları çıkmaktadır. Türkiye'de faaliyet gösteren bir sosyal medya platformunun aktif kullanıcı sayısı Avrupa Birliği'ndeki bazı ülkelerin toplam nüfusunu ikiye katlarken, sosyal medya şirketlerinin bu tutumları karşımıza şu iki soruyu çıkmaktadır. Bu dev sosyal medya şirketleri ofis açtıkları ülkeleri neye göre belirlemektedir ve ofis açmadan faaliyet gösterdikleri ülkelerin böyle bir durumda yaptırım olanakları nedir? İşte bu iki sorunun cevabı sadece Türkiye'yi değil bu tür şirketlerin ofis açmadan faaliyet gösterdikleri tüm ülkeleri ilgilendirmektedir. Çünkü her hangi bir sosyal medya şirketinin her ülke için aynı olaylarda farklı davranışlar sergilemesi bu şirketlere olan güvenirliliğin azalmasına neden olmaktadır. Ayrıca, uluslararası arenada da sosyal medya alanında ciddi bir

denetimsiz yapının olduğunu göstermektedir. Bu denetimsizliğin ve söz konusu alana yönelik, ülkelerin birbirinden farklılık gösteren uygulamalarının ortadan kaldırılması için bu alanı düzenleyecek uluslararası bir kural metnine, küresel koordinasyonunun ve güvenliğinin devamı açısından ihtiyaç duyulduğu açıkça ortadadır. Bu tür bir uluslararası düzenleme hem anlaşmaya taraf devletler hem de sosyal medya alanında faaliyet gösteren şirketler için karşılıklı güven ortamını tahsis edecek ve bu alana denetim getirecektir.

KAYNAKLAR

AKKOR GÜL Ayşen, 2013, Avrupa Birliği'nde Medya Okuryazarlığı: Düzenleme ve Çalışmalarda Gözlemlenen Eğilimler, İstanbul Üniversitesi İletişim Fakültesi, İstanbul, s.16, www.ajit-e.org/download_pdf.php?id=63&f=63_rev1.pdf (18.08.2014)

ASRAK HASDEMİR Tuba, 2012, Gelenekselden Yeni Medya Okuryazarlığına: Türkiye Örneğinde Bir Değerlendirme, Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı 2, Aralık 2012, Çorum, s.23-40, www.sbedergi.hitit.edu.tr/files/tuba%20hasrakdemir.pdf (18.08.2014)

AVRUPA BİRLİĞİ BAKANLIĞI, 2013, AB'de ve Diğer Belli Başlı Ülkelerde İnternet ve Sosyal Medya'ya İlişkin Düzenlemeler, Haziran 2013, Ankara, s.18-33

BABACAN Mehmet Emin vd., 2012, Sosyal Medya ve Arap Baharı, s.15-16 http://sosyal medya akademi.com /dokumanlar /arap_bahar %C4%B1_sosyal_medya.pdf (21.04.2014)

BABAOĞLAN Ali Rıza, 2013 Gezi Parkı Olayları ve Dijital Kaos, Haziran 2013, http://www.alibabaoglan.com/blog/gezi-parki-olaylari-ve-dijital-kaos/, (03.04.2014)

BABAOĞLAN Ali Rıza, 2014, Sözlü Görüşme, Twitter'ın Kapatılması Üzerine, 26 Mart 2014, http://www.alibabaoglan.com/blog/twitterin-kapatilmasi-uzerine, (13.06.2014)

BAŞLAR Gülşah, 2013, Yeni Medyanın Gelişimi ve Dijitalleşen Kapitalizm, 1 Marmara Üniversitesi, Radyo TV ve Sinema Bölümü, 2013, İstanbul, s.4, http://ab.org.tr/ab13/bildiri/247.pdf

BOZKURT Aslıhan, 2013, Sosyal Medya'nın "Gezi"deki Rolü…, Bilişim Dergisi, Sayı:156, s.51-54 http://www.bilisimdergisi.org/s156 (21.05.2014)

BULLAS Jeff, 2014, The Growth Of Social Media, http://www.jeffbullas.com/2014/01/17/20-social-media-facts-and-statistics-you-should-know-in-2014/ (07.08.2014)

BÜYÜKŞENER Ercüment, 2009, Türkiye'de Sosyal Ağların Yeri ve Sosyal Medyaya Bakış, inet-tr '09 - XIV. Türkiye'de İnternet Konferansı Bildirileri, 12-13 Aralık 2009, İstanbul, s.1, http://inet-tr.org.tr/inetconf14/kitap/buyuksener_inet09.pdf

BTK, 2014, Türkiye Elektronik Haberleşme Sektörü, Üç Aylık Pazar Verileri Raporu, 2014 Yılı 1. Çeyrek Ocak- Şubat- Mart, Sektörel Araştırma ve Strateji Geliştirme Dairesi Başkanlığı, Mayıs 2014, Ankara, s.26-27

ÇİLE Ahmet, 2012, Sosyal Medya Tarihçesi, http://sosyaling.com/sosyal-medya-tarihcesi/ (05.05.2014)

DIGITAL INSIGHTS, 2014, http://socialtimes.com/social-media-facts-figures-stats-infographic_b200159 (07.08.2014)

DÜLGER Murat Volkan, BECENİ Yasin, 2011, Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler, Yayın No: TÜSİAD-T/2011,03; 512, Mart 2011, İstanbul, s.14, http://www.tusiad.org.tr/__rsc/shared/file/InternetErisimi-rapor.pdf (12.07.2014)

EURAKTİV, 2009, Medya Eğitimi Avrupa'da Zorunlu Olacak, 25.08.2009, http://www.euractiv.com.tr/yazici-sayfasi/article/ab-medyanin-okullarda-ders-olarak-ogretilmesini-istiyor-006725 (06.07.2014)

GENÇLİK VE SPOR BAKANLIĞI,2013, Gençlik ve Sosyal Medya Araştırma Raporu, T.C. Gençlik Ve Spor Bakanlığı Eğitim, Kültür Ve Araştırma Yayın No: 79, Aralık 2013, Ankara, Gençlik Araştırmaları Yayın No: 4, s.25-26

GLOBAL DIGITAL STATISTICS 2014, http://www.slideshare.net/wearesocialsg/social-digital-mobile-around-the-world-january-2014 (04.06.2014)

GÖKSU Yunus, 2013, Sosyal Medya Yalanın Dibini Gördü,01 Haziran 2013, http://www.yenisafak.com.tr/gundem/sosyal-medya-yalanin-dibini-gordu-528657 (11.06.2014)

GÜRSES Binnur, 2013, Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri, BTK İdari Uzmanlık Tezi, Ağustos 2013, Ankara, s.5-6, http://212.175.164.17/ekDosyalar/tezler/Binnur_GURSES.PDF

HABER 7, 2014, Twitter Neden Türkiye'de Ofis Açmıyor, 21 Nisan 2014 http://www.ajanshaber.com/twitter-neden-turkiyede-ofis-acmiyor-haberi/55381 (13.06.2014)

HENKOĞLU Türkay, YILMAZ Bülent, 2013, Avrupa Birliği (AB) Bilgi Güvenliği Politikaları, Türk Kütüphaneciliği 27, s.9 www.tk.org.tr/index.php/TK/article/download/384/377 (23.07.2014)

KAYA MEHMET BEDİİ, Sosyal Medya Paylaşımları Sebebiyle Hukuki Sorumluluğun Esasları, http://www.ankara.diplo.de/contentblob/4057082/ Daten /3714633/mehmetbediikaya.pdf (13.04.2014)

KAYA Murat, CAN Enes, 2013, Twitter"dan tehdit ve hakarete ilk ceza, 15 Şubat 2013,İstanbul, http://www.aa.com.tr/tr/rss/133706--twitterdan-tehdit-ve-hakarete-ilk-ceza (06.08.2014)

KOÇ Serhat, 2013, Hukuksal Bağlamda Sosyal Medya Analizi ve Kıyaslamalı Mevzuat Önerileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Tezi, İstanbul, s.45-48, www.serhatkoc.com/uploads/tez.pdf (12.07.2014)

KOÇ Serhat, KAYNAK Selva, 2010, Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik, Akademik Bilişim 10-XII. Akademik Bilişim Konferansı Bidirileri, 10-12 Şubat 2010, Muğla, s.3, www.ab.org.tr/ab10/kitap/koc_kaynak_AB10.pdf (12.07.2014)

KURAL Salih, 2013, Twitter'da Hakaret ve Tehdide İlk Kez Ceza Geldi, 16 Şubat 2013, http://sosyalmedya.co/twitterda-ceza-hakaret-ilk-ceza/ (06.08.2014)

KURT Adile Aşkım, KÜRÜM Dilruba, 2010, Medya Okuryazarlığı ve Eleştirel Düşünme Arasındaki İlişki: Kavramsal Bir Bakış, Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, ISSN: 1309-1387 Yıl: 2 Sayı: 2 Bahar 2010, Burdur, s. 20-34, www.oaji.net/articles/1037-1405507239.pdf (19.08.2014)

NİZAM Feridun, 2009, Avrupa Birliği Bilişim Politikası ve Türkiye'nin Uyumu, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2009, Ankara,s.1 http://www.ab.org.tr/ab05/tammetin/89.doc (25.07.2014)

NİZAM Feridun, BİÇER Serkan, İnternet Yayıncılığında Etik ve Hukuki İhlaller, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, s.2, www.inet-tr.org.tr/inetconf10/bildiri/28.doc (13.07.2014)

NTVMSNBC, 2011, Analog Düşünceyle Bilişim Hukuku Yapılmaz, 20 Haziran 2011 , http://www.ntvmsnbc.com/id/25225095/ (09.06.2014)

ÖNOK Murat, 2013, Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Hukuk Fakültesi Dergisi, İstanbul, s.1232-1242, www.dosya.marmara.edu.tr/huk/fakültedergisi/nurcentel/muratonok.pdf (11.07.2014)

ÖZOCAK Gürkan, Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti, http://www.koksalpartners.com/files/7413/6923/9762/OZOCAK_Sosyal-Medyada-Islenen-Suc-Tipleri.pdf

ROBINSON Frances, 2014, AB: Talep Edildiğinde Google Linkleri Çıkarmalı, The Wall Street Journal, 13 Mayıs 2014, http://www.wsj.com.tr/article/SB10001424052702303627504579559472418712230.html (06.06.2014)

RTÜK,2014, Medya Okuryazarlığı, http://www.rtuk.org.tr/Home/SolMenu/89 (19.08.2014)

TİB, 2014, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, http://www.tib.gov.tr/tr/tr-menu-42-kanunlar.html (05.08.2014)

ÖZGÜNLÜK BİLDİRİMİ

Uzmanlık tezi olarak sunduğum bu çalışmayı, bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde değinme yaparak yararlandığımı ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Ulaştırma ve Haberleşme Uzman ve Uzman Yardımcılarının Sınav, Atama, Çalışma Usul ve Esasları Hakkında Yönetmeliğine uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığını tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Akif MANAV

ÖZGEÇMİŞ

1984 yılında Kocaeli'nin Gölcük ilçesinde doğdu. İlkokul, ortaokul ve lise öğrenimini Gölcük'te tamamladı. 2007 yılında Ankara Üniversitesi, İletişim Fakültesi, Halkla İlişkiler ve Tanıtım Bölümünden mezun oldu. 2010-2011 yılları arasında Güney Marmara Kalkınma Ajansında Reklam ve Halkla İlişkiler Sorumlusu olarak görev yaptı. 2011 yılı Mart ayından itibaren Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nda Ulaştırma ve Haberleşme Uzman Yardımcısı olarak görev yaptı. Halen Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Basın ve Halkla İlişkiler Müşavirliği'nde çalışmaktadır.