BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

SOSYAL PAYLAŞIM AĞLARINDA KİŞİSEL VERİLERİN GÜVENLİĞİ; SORUNLAR VE ÇÖZÜM ÖNERİLERİ.

Binnur GÜRSES

İdari Uzmanlık Tezi

Ağustos 2013

Ankara

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

Bu yayında öne sürülen fikirler eserin yazarına aittir;

Bilgi Teknolojileri ve İletişim Kurumunun görüşlerini yansıtmaz.

BTK ISBN 978-605-345-086-3

BTK Yayın No T 0197

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

SOSYAL PAYLAŞIM AĞLARINDA KİŞİSEL VERİLERİN GÜVENLİĞİ; SORUNLAR VE ÇÖZÜM ÖNERİLERİ.

Binnur GÜRSES

İdari Uzmanlık Tezi

Ağustos 2013

Ankara

Binnur GÜRSES tarafından hazırlanan "**Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri**" adlı bu tezin İdari Uzmanlık tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Mustafa ALKAN
Tez Danışmanı

Bu çalışma, tez savunma komisyonumuz tarafından İdari Uzmanlık tezi olarak kabul edilmiştir.

Başkan : _____

Üye : _____

Üye : _____

Üye : _____

Üye : _____

Bu tez, Bilgi Teknolojileri ve İletişim Kurumu tez yazım kurallarına uygundur.

İÇİNDEKİLER

ÖZET

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU	
Tezin Adı	Sosyal Paylaşım Ağlarında Kişisel Verilerin Güvenliği; Sorunlar ve Çözüm Önerileri
Türü	İdari Uzmanlık Tezi
Yazar	Binnur GÜRSES
Teslim Tarihi	Ağustos 2013
Anahtar Kelimeler	Sosyal Paylaşım Ağları, Kişisel Veriler, Güvenlik
Tez danışmanı	Prof. Dr. Mustafa ALKAN
Sayfa Adedi	vi + 100

Bu çalışmada, sosyal paylaşım ağlarının kullanımında oluşabilecek güvenlik açıkları, tehlikeleri, alınması gereken güvenlik önlemleri ve uygulanmasına ilişkin olarak yaşanılan sorunlarla ilgili çözüm önerilerinde bulunulmaktadır.

Bu çalışma, son yıllarda Dünya'da ve Türkiye'de artış gösteren sosyal paylaşım ağlarında kişisel verilerin doğru ve güvenli kullanımı konusunda Dünya'da ve Türkiye'de gerçekleştirilen faaliyetlerin incelenmesini amaçlamaktadır. Bu çalışma kapsamında Türkiye'de ve dünyada yaygın olan sosyal paylaşım ağları incelenmiş, kişisel verinin tanımı yapılmış, sosyal paylaşım ağlarındaki güvenlik tehditlerine dikkat çekilmeye çalışılmıştır. Sosyal paylaşım ağlarının hayatımıza getirdiği birçok faydalar yanında sebep olduğu riskler ortaya konmaya çalışılmış, dünyada başta ABD ve AB ülkelerinin kişisel verilerin güvenliği konusunda yapmış oldukları çalışmalar incelenmiş ve Türkiye'de bu konuda yapılan uygulamalar anlatılmaya çalışılmıştır.

Ayrıca, sosyal paylaşım ağlarında kişisel verilerin güvenliğini sağlamak amacıyla alınabilecek önlemler kapsamında kişisel, sosyal ve hukuki alanda yapılabilecek çalışmalar konusunda öneriler sunulmuştur.

ABSTRACT

INFORMATION AND COMMUNICATION TECHNOLOGIES AUTHORITY	
Thesis	The Security of Personal Data in Social Networks; Issues and Solution Proposals
Type	Administrative Expertise Thesis
Author	Binnur GÜRSES
Submission Date	August 2013
KeyWords	Social Networks, Personal Data, Security
Advisor	Prof. Dr. Mustafa ALKAN
Total Page	vi + 100

In this thesis safety gaps and threats associated with social media usage, possible solutions for safety problems and the practical problems faced while applying safety solutions for social media applications will be considered.

This thesis aims to examine the personal data protection and privacy of personal data in social networks, which are widely used throughout the world and Turkey. Within the scope of this thesis; the popular social networks are analysed, "personal data" paradigm is defined and the security threats regarding social networks are highlighted.While social networks come up with several benefits for individuals, they also cause safet risks regarding personal data shared in the social media environments. . Within this scope, worldwide efforts (particularly in USA and EU) which aims to ensure personal data protection are reviewed and Turkey case for the aforementioned problem is described.

Additionally, social, technical and legal suggestions are proposed so as to ensure personal data protection and to make social networks safer.

TEŞEKKÜR

Çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren tez danışmanım Prof. Dr. Mustafa ALKAN'a, görüş ve değerlendirmeleri ile sağladıkları destekten dolayı Daire Başkanım Özgür Fatih AKPINAR'a ve Cafer CANBAY, K. Sacid SARIKAYA, Müberra OĞUZ, Mustafa ÜNVER, Başkanlarıma, çalışma arkadaşlarıma, çeviri konusunda destek veren Fatih GENÇ, Özgür PEKÇAĞLAYAN ve Ali ERSOY'a, manevi desteklerinden güç aldığım aileme, bu süreçte beni hiç yalnız bırakmayan, sürekli destekleyen değerli eşim Birol GÜRSES'e, sabır ve anlayışlarından dolayı oğullarım Batur Kaan ve Bora GÜRSES'e teşekkür ederim.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	Avrupa Birliği (European Union (EU))
ABD	Amerika Birleşik Devletleri
ASP	Etkin Sunucu Sayfası (Active Server Page)
API	Uygulama Programlama Arayüzü (Application Programming Interface)
APEC	Asya Pasifik Ekonomik İşbirliği (Asia Pacific Economic Cooperation)
BTK	Bilgi Teknolojileri ve İletişim Kurumu
DNS	Alan Adı Sistemi (Domain Name System)
HTML	Zengin Metin İşaretleme Dili (Hyper Text Markup Language)
ID	Kimlik (Identy)
IOS	Ağlar Arası İşletim Sistemi (Internetwork Operating System)
IP	İnternet Protokolü (Internet Protocol)
JS	Java Betiği (Java Script)
OECD	Ekonomik İsbirliği ve Kalkınma Teşkilatı (Organisation for Economic Co-operation and Development)
RFC	Açıklama İsteği (Request for Comments)
SSL	Güvenli Soket Katmanı (Secure Socket Layer)
XSS	Siteler Arası Kod Çalıştırma (Cross-Site Scripting)
XSRF	Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery)
TBMM	Türkiye Büyük Millet Meclisi
T.C.	Türkiye Cumhuriyeti
TCK	Türk Ceza Kanunu
TİB	Telekomünikasyon İletişim Başkanlığı
URL	Standart Kaynak Bulucu (Uniform Resource Locator)
TMK	Türk Medeni Kanunu
IWF	İnternet İzleme Kurumu (Internet Watch Foundation)

GİRİŞ

İnternetin yaygınlaşması insanların bilgisayar kullanım alışkanlıklarını ve şeklini de değiştirmiştir. Önceleri sadece araştırma veya eğlence amaçlı kullanılan İnternet günümüzde ise bazen bir kütüphane, bazen bir televizyon, bazen bir eğlence ortamı, bazen de bir eğitim ortamı olarak kullanılabilmektedir. Web 2.0 teknolojisi ile beraber internet, tek taraflı bir yayın ortamı olmaktan çıkıp internet kullanıcısının da fikirlerini paylaşabildiği, geri dönüş yapabildiği etkileşimli bir ortam olmuştur.

İnternet kullanıcısının da internet ortamında kendi düşüncelerini paylaşabilmesini sağlayan Web 2.0 teknolojinin yaygınlaşması ile beraber sosyal paylaşım ağları denilen olgunun doğmasına ve hızla yaygınlaşmasına ortam hazırlanmıştır. Çünkü kullanıcılar beğenmedikleri, yanlış buldukları veya destekledikleri herhangi bir konuda düşüncelerini başka insanlarla paylaşma imkânı bulmaktadır. Bu da sosyal paylaşım ağlarının çok hızlı gelişmesine imkân tanımıştır. Öyle ki sosyal paylaşım ağları çoğunluğu genç olan milyarlarca kişi tarafından kullanılmaktadır. İnsanların birbirleri ile bu kadar erken yaşlarda bu kadar kolay iletişim kurması sosyal paylaşım ağlarını güçlendirmektedir. Bugün gelinen noktada sosyal paylaşım ağlarının gücü artık iktidarları bile tehdit eder boyuta gelmiştir. Ortadoğu'da ortaya çıkan ve birçok ülkeyi etkileyen Arap Baharı buna en iyi örnektir. Arap ülkelerinde sivil halk sosyal paylaşım ağları üzerinden örgütlenerek iktidarlara karşı çok etkin protestolar yapabilmişlerdir. Türkiye'de ise yakın zamanda ortaya çıkan ve günlerce devam eden Gezi Parkı olayları da sosyal paylaşım ağları üzerinden örgütlenen gençlerin gerçekleştirdikleri eylemler olarak tarihteki yerini almıştır.

Sosyal paylaşım ağları kullanım amacı, hedef kitlesi veya yapısı itibariyle çeşitlilik göstermektedir. Facebook, Twitter, YouTube, Google+, LinkedIn vb. sosyal paylaşım ağlarına örnek olarak verilebilir.

Sosyal paylaşım ağları kötü niyetli kullanıcılar veya yeterli bilgi seviyesine sahip olmayan kişilerin kullanımları sonucunca bireysel veya kamusal açıdan istenmeyen durumların ortaya çıkmasına neden de olabilmektedir. Bu nedenle anti-sosyal paylaşım ağları diyebileceğimiz sosyal paylaşım ağı karşıtı grupların da ortaya çıktığını söylemek mümkündür.

Bu çalışmanın amacı, sosyal paylaşım ağlarında kişisel verilerin mevcut durumuna ve önemine değinmek, yaşanan sorunları irdelemek ve alınabilecek önlemleri değerlendirmektir.

Bu çalışma kapsamında; Türkiye'de ve dünyada yaygın olan sosyal paylaşım ağları incelenmiş, kişisel verinin tanımı yapılmış, sosyal paylaşım ağlarındaki güvenlik tehditlerine dikkat çekilmeye çalışılmıştır. Sosyal paylaşım ağlarının hayatımıza getirdiği birçok faydalar yanında sebep olduğu riskler ortaya konmaya çalışılmış, dünyada başta ABD ve AB ülkelerinin kişisel verilerin güvenliği konusunda yapmış oldukları çalışmalar incelenmiş ve Türkiye'de bu konuda yapılan uygulamalar araştırılarak, sosyal paylaşım ağlarında kişisel verilerin güvenliğini sağlamak amacıyla alınabilecek önlemler kapsamında kişisel, sosyal ve hukuki alanda yapılabilecek çalışmalar konusunda öneriler sunulmuştur.

1. SOSYAL PAYLAŞIM AĞLARI

İnsanlar arasındaki iletişim şekli internetin yaygınlaşması ile beraber değişiklik göstermiştir. İnternet ortamında iletişim klasik iletişim ortamlarına göre bazı avantajlara sahip olduğundan dolayı hızla yaygınlaşmaktadır. Maliyetinin diğer iletişim ortamlarına göre çok ucuz olması, yeni insanlarla tanışma ve istenilen bilgiyi ulaşılabilir kılıp istemeyeni gizleme gibi imkânlar; telefon, radyo veya televizyon gibi iletişim ortamlarına göre birer avantaj olarak kabul edilmektedir.

İnternet ortamındaki sosyal paylaşım ağlarında iletişim; ilk önceleri sohbet, yeni insanlarla tanışma gibi amaçlarla gerçekleştirilirken zaman içinde, uzun süredir haber alınamayan arkadaşlar ile iletişim kurma, arkadaş çevresiyle bir şeyler paylaşma, iş çevresi ile iletişim halinde olma, hayranlık duyulan bir ünlüyü takip etme veya fotoğraf, video gibi hobiler üzerine bir şeyler paylaşma şeklini almıştır. Hatta ticari şirketler için müşteri kitlesine kolay ulaşma gibi daha profesyonel bir yapıya da büründüğü kabul edilmektedir.

İnternet ortamındaki iletişim olarak da nitelendirilebilen sosyal paylaşım ağları günümüzde milyarlarca insan tarafından kullanılmaktadır. 2010 yılında yapılan bir çalışmada yetişkin insanların %61'inin, gençlerin ise %73'ünün sosyal paylaşım ağları üzerinden iletişimi kullandığını ortaya koymaktadır (Ferriter, 2010, s.87-88). Bugün en yaygın olarak kullanılan sosyal paylaşım ağları olarak kabul edilen Facebook, Twitter ve Youtube'un 2004'ten sonra ortaya çıkmış olmasına rağmen milyarlarca insan tarafından kullanılması da ilginç bir noktadır (Boyd, 2007, s.210-230).

Bilişim teknolojilerinin gelişmesi ile beraber internet ortamında bilgi, fotoğraf, ses ve video gibi kişisel bilgilerin paylaşımı da artmıştır. Sosyal paylaşım ağları insanlar arasındaki mesafeye bakmaksızın iletişim kurmalarını sağlayan, insan iletişimine yeni bir boyut kazandıran ve hızla gelişen sosyal ve ekonomik bir olgu olarak tanımlanmaktadır.

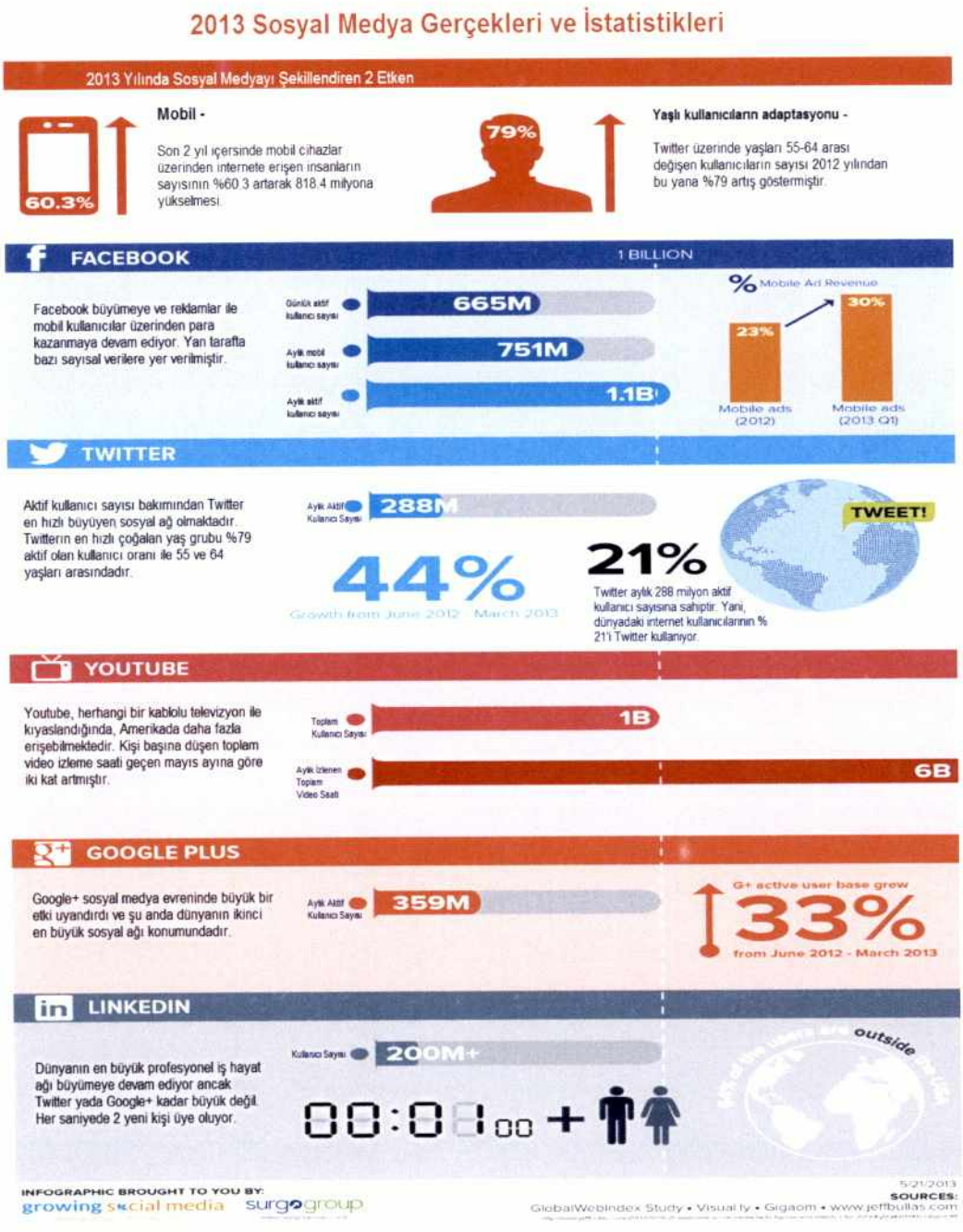
Sosyal paylaşım ağları bilgi paylaşımının olduğu çevrim içi (online) sistemler olarak ifade edilebilir. Bunun ilk ayağı da kişisel verilerin bir profilde paylaşılmasıdır. Sosyal paylaşım ağlarına ilk kayıt yapıldığında kişisel bilgilerin girilmesi istenir. Bu bilgiler genelde ad, soyad, yaşanılan yer, yaş, iş tecrübeleri, hobiler, favori filmler ve ilgi alanları gibi bilgilerdir (Chang, 2013, s.311-321).

Sosyal paylaşım ağları kullanım amacına göre de çeşitlilik göstermektedir. Bazı sosyal paylaşım ağları fotoğraf paylaşımı temeline dayanırken, bazıları video veya bilgi paylaşımı temeline dayanmaktadır. Belli bir gruba hitap eden sosyal paylaşım ağları olduğu gibi, her kesime hitap edenleri de bulunmaktadır. Hatta mekândan bağımsızlığı sağlayarak öğretmen ve öğrenci için bir eğitim platformuna dönüşebilen sosyal paylaşım ağları da bulunmaktadır. Örneğin Heather Rogers Haverback Towson Üniversitesi öğrencileri tarafından Facebook'ta bir grup oluşturulmuş ve bu grup okuma dersinin ödevlerinin tartışıldığı ve görüşlerin paylaşıldığı bir eğitim ortamı olarak kullanılmıştır (Haverback, 2009; Everson, 2013, s.A61-A81).

Sosyal paylaşım ağlarının kullanım miktarı ve türü ülkeden ülkeye farklılık arz etmektedir. Çok ilginçtir ki, Türk bir mühendis tarafından geliştirilen Orkut adlı sosyal paylaşım ağı Türkiye'de hiç kullanılmamasına rağmen günümüzde Hindistan'da %20 oran ile en yaygın sosyal paylaşım ağı olmuştur. 2009 verilerine göre Cyworld Güney Kore'de nüfusun %50'si tarafından kullanılmakta iken 2010 verilerine göre Japonya'da 14 milyon kişi Mixi denilen sosyal paylaşım ağını kullanmaktadır (Vasalou vd., 2010 s.719-728). Çin'de ise en fazla kullanım oranına sahip sosyal paylaşım ağı Qzone'dur. Bütün bunların yanında dünya genelinde en çok kullanılan sosyal paylaşım ağları; Facebook, Twitter ve Youtube' dur.

2013 itibariyle en çok kullanıcı sayısına sahip sosyal paylaşım ağları Şekil 1.1'de görülmektedir.

Şekil 1. 1. En Çok Kullanıcıya Sahip Sosyal Paylaşım Ağları



Kaynak: Growing Social Media, Mayıs 2013

Sosyal paylaşım ağları ve sosyal medya kavramları, sıklıkla birbirinin yerine kullanılması ve benzerlikler göstermesine rağmen, aralarında büyük farklar

bulunmaktadır. Sosyal medya paylaşım ve tartışma için bir araç iken, sosyal paylaşım ağları ise aynı ilgi alanları ve hobilere sahip kişileri birbirlerine bağlayan bir yapıdır. Birinde yayılan bilgiler geneli ilgilendirirken, diğeri üzerinden yayılan bilgiler daha kişisel ve hedef odaklıdır Sosyal medya ile sosyal paylaşım ağları arasında beş temel farklılık bulunmaktadır. Bunlar;

> "**1) Tanım:** Sosyal medya, bilgiyi aktarmak veya dağıtmak için kullanılan bir araçtır. Sosyal paylaşım ağları ise, bir bağlılıktır, benzer ilgi alanlarına sahip insanların oluşturduğu guruplardan meydana gelir.
>
> **2) İletişim yöntemi:** Sosyal medya, belirlenmiş mesajları ve haberleri, televizyon ve radyo gibi bireylere ileten bir haberleşme kanalıdır. Sosyal medyada amaç bireyin ne yediği, nerede olduğu gibi kişisel verilerin değil, doğrudan doğruya haberlerin iletilmesidir. Sosyal paylaşım ağlarında ise haberleşme iki yönlüdür, konuya ve atmosfere göre farklı bireyler dahil olup mesajlaşırlar.
>
> **3) Geri bildirim:** Sosyal medyada geri bildirim olmaz veya ölçülemeyecek kadar küçük olur. Yayılmış bir haberin herhangi bir getirisi olmayabilir, kaç kişi tarafından anlaşıldığı yada beğenildiği gibi veriler üretmesi güç olmaktadır. Öte yandan, sosyal paylaşım ağlarında ise geri bildirimler daha belirgindir. Paylaşılanları insanlar beğenir, arkadaş olmak isterler ve sitenin ziyaretçi sayısı artar, bu durumda bireyin sosyal ağının büyüdüğü ve güçlendiği yorumuna varılabilir.
>
> **4) Cevap süreleri:** Sosyal medya yavaş büyür. Bireyin sadece bir haber yayması ve onunla ilgili insanların tartışmaya başlaması için bireyin bu alanda ünlenmiş olması ve güven kazanmış olması gerekir. Sosyal paylaşım ağlarında ise iletişim iki yönlüdür. Bireyler iletişim kuracakları kişileri kendileri belirler ve paylaşımlar bu kişilere özgün olduğu için daha kişiseldir.
>
> **5) Ricalar:** Bireyler paylaşımları ile ilgili ricalarda bulunabilirler. Yeni iş kurmuş bir birey, sosyal medya üzerinden takipçilerine beğenmesi ricasında bulunursa firmasının itibarını zedeleyecek ve güvenilirliğini kaybedecektir. Ancak, sosyal paylaşım ağları üzerinden, arkadaşlarına bu tarz bir rica da bulunması bunu daha kişisel kılacaktır, arkadaşlarıyla nasıl başarıya ulaşabileceği konusunda tartışmalar yürütebilecek ve bu da firmanın kazancı şeklinde sonuçlanacaktır" (Examiner, 2013; Lonscohen, 2013; Socialmedyatoday 2013; a.g.e.).

1.1. Sosyal Paylaşım Ağları ile İlgili Tanımlar ve Kavramlar

Sosyal paylaşım ağları çeşitli amaçlarla kurulmuş ve kullanılmakta olan web-tabanlı sistemlerdir. Bu nedenle tüm sosyal paylaşım ağlarını tek bir tanımla sınırlamak zor olsa da bireylerin, web-tabanlı sistemlerin izin verdiği ölçüde profillerinin bir kısmını veya tamamını paylaştıkları, çeşitli bağlantılar paylaşabildiği ve iletişim halinde olduğu diğer kişilerin paylaşımlarını görebildikleri sistemler olarak tanımlanabilir (Boyd, 2007, s.210-230). Tanımdan da anlaşılacağı gibi, bir sosyal paylaşım ağının üç temel bileşene sahip olması gerekir. Bunlar;

1) Profillerinin tamamının veya bir kısmının paylaşılması,
2) Bir arkadaş grubuna sahip olmak,
3) Arkadaş grubu arasında yetki veya izin çerçevesinde belli bağlantı veya paylaşımların görüntülenebilmesidir.

Günümüz sosyal paylaşım ağları sadece bu üç hizmet ayağıyla yetinmemektedir. Yapılan bir çalışmada sadece Facebook'a günde 20 milyon uygulamanın yüklendiği ortaya konulmaktadır (Li vd., 2013, s.18-30).

Başka bir çalışmada sosyal paylaşım ağları insanların iletişim kurmalarını sağlayan herhangi bir konuda birbirleri ile etkileşim içerisinde oldukları sanal ortamlar olarak tanımlanmaktadır (Murray and Waller, 2007, s.56-59). Bunun yanında sosyal paylaşım ağlarını grafik teorisine göre tanımlayan çalışmalar da mevcuttur. Grafik teorisine göre bireyler birer düğüm ve bireyler arasındaki bağlantı veya paylaşımlar da birer kenar olarak tanımlanıp sosyal paylaşım ağlarının analizi yapılmaktadır (Ni vd., 2010, s.2514–2527).

Sosyal paylaşım ağları, Avrupa Konseyi'nin Bilgi Toplumu Hizmetleri Hakkındaki 1998/48 sayılı direktifinde ve değişik 1998/34 sayılı Avrupa Direktifinin 1'inci maddesinin 2'nci paragrafında bilgi toplumu hizmeti olarak nitelendirilmektedir. Özetle; Sosyal paylaşım ağları, insanları internet

ortamında buluşturan, kullanıcılarının arkadaş çevresi veya benzer ilgi alanlarına sahip kişilerle iletişim kurmalarını sağlayarak birbirleri ile tanışıp, bilgi, fotoğraf ve video gibi veri paylaşımına olanak tanıyan ve herhangi bir konuda tartışma ortamı sağlayan internet tabanlı yeni nesil iletişim araçları olarak tanımlanabilir.

İnternet ortamında sosyalleşirken bireysel kullanıcının kendini normal sosyal hayattaki gibi ifade edebilmesi modellenmektedir. Yapılan bir çalışmada sosyal paylaşım ağlarının normal yaşamda yapılan çeşitli jestleri sembolize eden çeşitli ikonlar ile gerçek hayatı modellediği ve kullanıcının kendini gerçek hayattaki gibi ifade etmesinin amaçlandığı vurgulanmaktadır (Yavanoğlu ve Sağıroğlu, 2010).

Yapılan bir diğer çalışmada sosyal paylaşım ağları türlerine göre; iş, arkadaşlık, fotoğraf, randevu, yüz yüze görüşmeyi kolaylaştırma ve genel ilgi odaklı sosyal paylaşım ağları olarak gruplandırılmıştır (Chen ve Shi, 2009).

Şekil 1. 2. Sosyal Paylaşım Ağlarının Sınıflandırılması

Kaynak: Hiedemann vd., 2011 103-112

Sosyal paylaşım ağlarının belli başlılarından bahsetmek gerekirse Facebook, Twitter, Google+, Youtube, MySpace, LinkedIn, Flickr, Friendster, Bebo, Blogger, Hi5, Orkut, Netlog vb. bunların başında gelir.

1.2. Sosyal Paylaşım Ağlarının Tarihçesi

Sosyal paylaşım ağları internet ortamında ortaya çıkan insanlar arası iletişim ile doğmuş ve gelişim göstermiştir. 1990'lı yılların ortasından sonra ortaya çıkan ve o dönemlerde küçük kullanıcı kitlelerini hedefleyen sosyal paylaşım ağlarını kullanan insan sayısı günümüzde milyarlarla ifade edilmektedir.

Gerçek anlamda ilk sosyal paylaşım ağı olarak tanımlayabileceğimiz çalışma 1995 yılında yapılmıştır. Classmates.com sitesi, lise veya üniversite arkadaşlarını arayıp bulmak amacıyla kurulmuş bir sosyal paylaşım ağıdır (Dilmen ve Öğüt, 2010).

1997 yılında Andrew Weinreich tarafından kullanıcının kendi profilini oluşturabildiği ve arkadaşlarını listeleyebildiği SixDegrees.com sitesi kurulmuştur. Site bir yıl içerisinde 1 milyon kullanıcıya ulaşmıştır (Heidemann vd., 2012, s.3866-3878). Bu özellik ilk defa SixDegrees.com ile ortaya çıkmış olan bir özellik değildir. Daha önce kurulmuş olan AIM ve ICQ, kullanıcılarına profil oluşturma imkânı verebilmiştir. Fakat SixDegrees.com ilk gerçek zamanlı sohbet imkânı da sağlayan ilk paylaşım ağı olarak dikkat çekmektedir. SixDegrees.com milyonlarca kişi tarafından kullanılmasına rağmen gerekli değişimi zamanında yapamadığından 2000 yılında kapanmıştır (Heidemann vd., 2012, s.3866-3878).

1997-2001 yılları arasında çeşitli sosyal paylaşım ağları kurulmuş ve farklı kullanıcı toplulukları tarafından kullanılmıştır. AsianAvenue, BlackPlanet ve MiGente bunların başında gelir. Bu ağlar ile ilk defa profesyonel amaçlı sosyal paylaşım ağları ortaya çıkmıştır. Bu sosyal paylaşım ağlarında kullanıcılar profillerini profesyonel amaçlarla kullanabilmişlerdir. Profillerini ve

arkadaş listelerini oluşturan kullanıcılar, ziyaretçi defterini de kullanmışlardır. Ancak bu dönemde kurulan sosyal paylaşım ağlarının yeterli kullanıcı sayısına ulaşmamasının ve kapanmalarının nedenlerinin başında web teknolojilerinin zayıf olması ve bugünün reklam endüstrisinin henüz oluşmamış olması gelmektedir (Boyd, 2007, s.210-230).

1999 yılında Friend Journal kurulmuştur. Bu ağda kullanıcı, başka bir kullanıcıyı arkadaşı olarak seçerek yazdıklarını takip edebilmiştir (Boyd, 2007, s.210-230). Yine aynı tarihte bir Kore sosyal paylaşım ağı olan Cyworld kurulmuş ve sosyal paylaşım ağı özelliklerini 2001 yılında kazanmıştır. Bir İsveç sosyal paylaşım ağı olan LunarStorm'a 2001 yılında arkadaş listesi, ziyaretçi defteri ve günlük tutma özellikleri eklenmiştir.

AdrianScott tarafından 2001 yılında San Fransisco'da kurulan Ryze.com daha önce kurulan sosyal paylaşım ağlarından farklı olarak iş hayatına yönelik geliştirilmiş bir sosyal paylaşım ağıdır. Benzer şekilde kurulan Tribe.net, LinkedIn ve Friendster kurucuları birbirileri ile iş birliği ile daha da büyüyebileceklerini düşünerek hareket etmişlerdir. Bu da başarılarını artırmıştır. Özellikle Friendster çok hızlı bir yükseliş göstermiştir (Chafkin M., 2013).

2002 yılında kurulan ve çok kısa zamanda hızlı bir gelişim göstererek, çok yaygın bir sosyal paylaşım ağı olan Friendster'in düşüşü de yine aynı hızda olmuştur. Friendster Ryze'e bir ek olarak geliştirilmiş randevulaşma tabanlı bir sosyal paylaşım ağıdır. Klasik sosyal paylaşım ağları birbirlerini hiç tanımayan insanları tanıştırmayı hedeflerken Friendster, ortak arkadaşları olan insanları tanıştırmayı hedeflemekte ve bu özelliği ile de diğer sosyal paylaşım ağlarından ayrılmaktadır. Bu da daha romantik bir ortam oluşması açısından etkili bir yöntemdir (Boyd ve Heer, 2006). Ancak Friendster kullanıcılara bazı kısıtlamalar getirmiştir. Bunların başında kullanıcılara diğer kullanıcıların profil sayfalarına ulaşmada getirilen kısıtlamalar gelmektedir. Buna göre bir kullanıcı en fazla dördüncü seviyeden bir arkadaşının profil

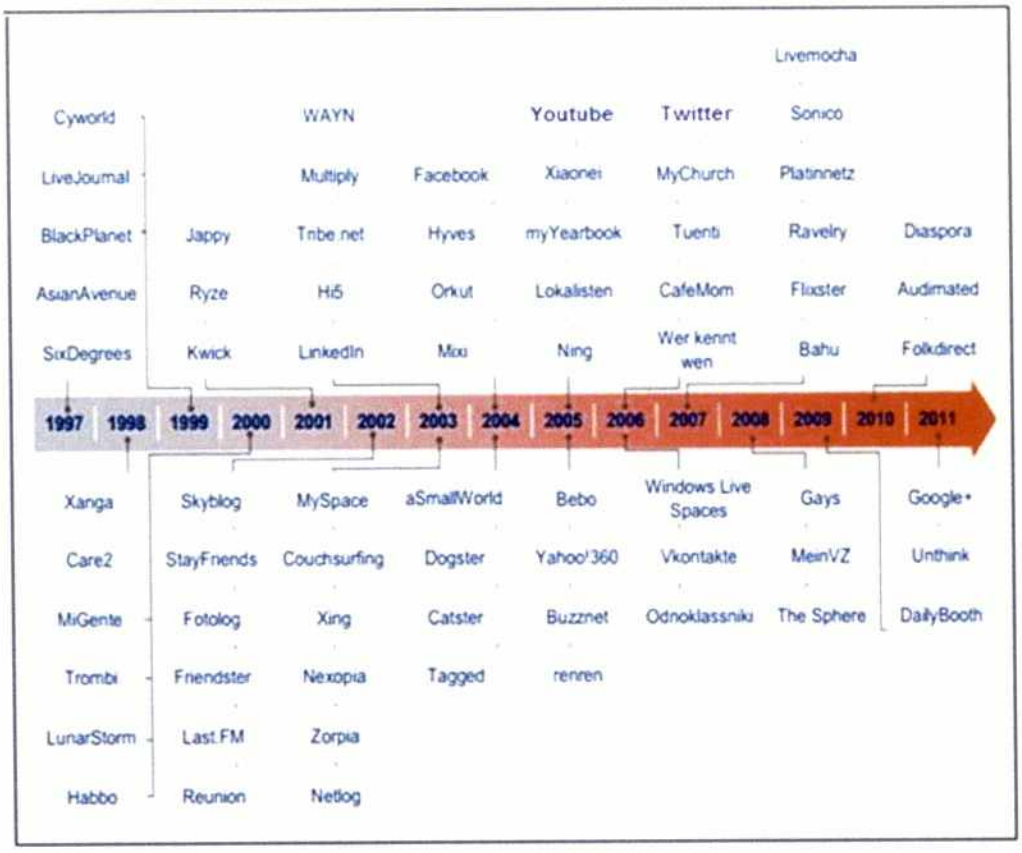
sayfasına ulaşabilmektedir. Yani bir kullanıcı ancak arkadaşının-arkadaşının-arkadaşının-arkadaşının profiline ulaşabilmektedir. Bu tür kısıtlamalar ve sahte hesap oluşturan kullanıcıları engellemek için sürekli artırılan güvenlik önlemleri yüzünden büyük düşüş yaşayan Friendster, çok hızlı yükseliş gösterip yine çok hızlı düşüş yaşaması açısından incelenmeye değer bir sosyal paylaşım ağıdır (Dilmen ve Öğüt, 2010).

2003 yılında California'da Friendster'e göre kullanıcılara daha fazla imkân sunan MySpace kurulmuştur. Friendster'den kaçan kullanıcıların çoğu MySpace'e geçmiştir. Bu nedenle Myspace çok hızlı bir yükseliş yaşamıştır. MySpace'in daha çok müzik grupları için kurulduğu düşünülmektedir. Ancak bilinenin aksine MySpace ilk kurulurken bunu hedeflememiştir. Ancak zaman içinde bu alana yönelmiştir (Boyd, 2007, s.210-230).

Daha sonra kurulan Facebook ve Twitter günümüzün sosyal paylaşım ağı olarak milyarlarca insan tarafından kullanılmaya başlanmıştır. Tarihsel açıdan bakıldığı zaman Facebook ve Twitter kullanıcılarına mümkün olduğunca fonksiyonellik sağlamayı amaçlayarak kitlesini katlamaktadır (Heidemann vd., 2012, s.3866-3878).

Şekil 1.3'te de görüldüğü gibi pek çok sosyal paylaşım ağı zaman içinde geliştirilmiştir. Ancak bunların çoğu ya yeterince ilgi görmemiş ya da belli bir süre kullanılmasına rağmen zaman içinde popülaritesini kaybetmiştir. Son yıllarda büyük sosyal paylaşım ağları küçükleri satın alarak pastadan aldığı payı artırmaktadır.

Şekil 1. 3. 1997-2011 Yılları Arası Sosyal Paylaşım Ağlarının Zaman Çizelgesi



Kaynak: Hiedemann vd., 2011 103-112

1.3. Günümüzde Yaygın Olan Sosyal Paylaşım Ağları

1.3.1. Facebook

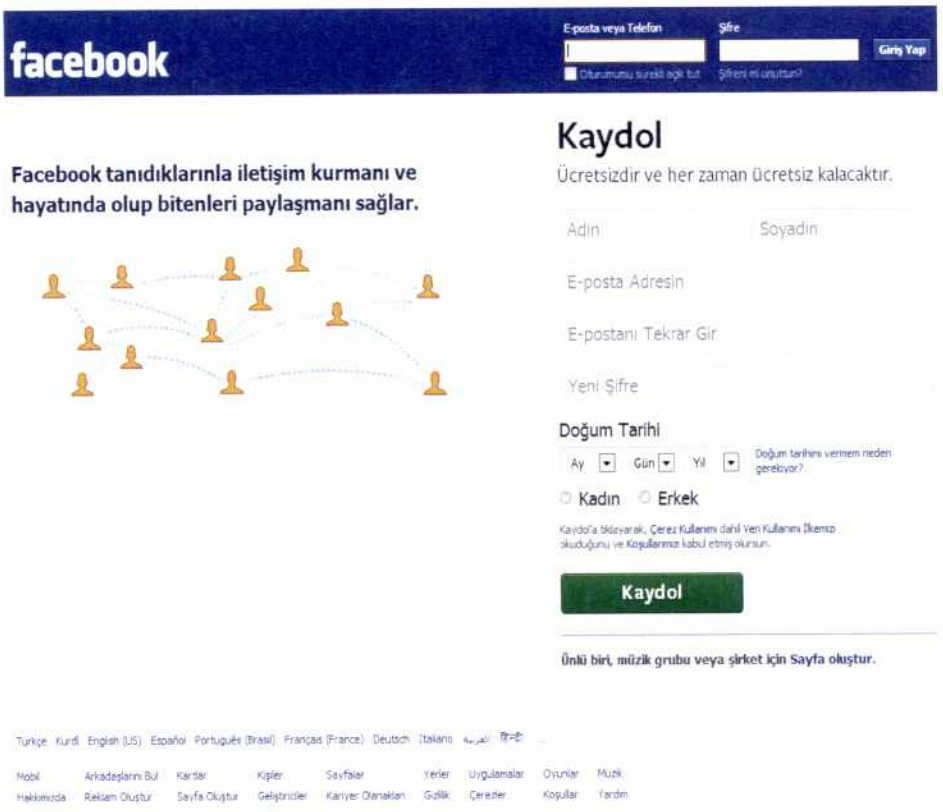
Facebook 2004 yılında Mark Zuckerberg tarafından geliştirilmiştir. İlk kuruluşunda Facebook'un hedef kitlesini Harvard Üniversitesi öğrencileri oluşturmuş, bir süre sonra Amerika Birleşik Devletleri (ABD)'ndeki tüm eğitim kurumlarını içerisine almış olan Facebook 2005 yılında bütün dünyanın kullanımına açılmıştır. Dünyanın en çok kullanıcısına sahip sosyal paylaşım

ağı olan Facebook'un bugünkü sloganı "Dünyayı daha açık ve birbirine bağlı yapmak "tır (Heidemann vd., 2012, s.3866-3878).

Günümüzde Facebook en yaygın kullanılan sosyal paylaşım ağıdır. 2013'ün ilk çeyreği için açıklanan Facebook istatistikleri de bu gerçeği onaylar niteliktedir. 70 dilde hizmet veren Facebook kullanıcı sayısı Mart 2013 itibariyle 1.11 milyar kişiye ulaşmıştır (Facebook, 2013d). Bu da dünyada her 7 kişiden birinin Facebook kullandığını ortaya koymaktadır. 10 yıl gibi çok kısa bir sürede Facebook'un bu kadar kişi tarafından kullanılacak seviyeye ulaşması inanılmaz bir durumdur. Facebook'un günlük aktif kullanıcı sayısı 665 milyon, mobil kullanıcı sayısı ise 751 milyon kişi iken kullanıcılar arasında 150 milyar arkadaşlık bağlantısı bulunmaktadır. Bu da kişi başına 141,5 arkadaş anlamına gelmektedir. Yine aynı rapora göre üzerindeki uygulama sayısı 10 milyona ulaşmış olan ve 240 milyar fotoğraf içeren Facebook'a günlük 350 milyon fotoğraf yüklenmektedir. Ortalama her Facebook'a girişte 20 dakika zaman harcanmaktadır. Facebook'ta günlük beğenme sayısı ise 4.5 milyardır. Bütün bu istatistikler Facebook'un popülaritesini ortaya koymak açısından yeterlidir (Facebook, 2013d).

Facebook'un dünya genelindeki kullanım istatistikleri böyle iken, Türkiye'de ki durumunu da irdelemek gerekmektedir.

Şekil 1. 4. Facebook'un Kullanıcı Ara Yüzü (2013)



Kaynak: Facebook, 2013c

Türkiye toplam Facebook kullanıcı sayısı bakımından dünyada ABD, Brezilya, Hindistan, Endonezya ve Meksika'nın ardından 6. sırada bulunmaktadır. Mart 2013 itibariyle Türkiye'de 32.849.260 Facebook kullanıcısı mevcut iken, Haziran 2013 itibariyle bu sayı 32.775.240 kişidir. Yani Türkiye'de Facebook kullanıcı sayısı 3 ayda %0,023 oranında 74.020 kişi azalmıştır. Şubat-Mart aylarına ve Mayıs-Haziran aylarına göre değişimler Şekil 1.5 ve 1.6'da görülmektedir. Bu azalmanın nedeni sahte hesapların silinmesi ve çok az da olsa bazı kullanıcıların hesaplarını dondurması olarak değerlendirilmektedir (Quintly, 2013). Yine aynı araştırma şirketinin Ekim 2012'ye ait istatistiklerinde Türkiye'de 32.177.280 Facebook kullanıcısı olduğu görülmektedir (Quintly, 2013; a.g.e.).

Şekil 1. 5. Facebook'un Mart 2013 İtibariyle Ülkelere Göre Kullanıcı Sayıları

	Ülkeler	Kullanıcı Sayısı	Değişim	+/- %
	Dünya	967,777,300	-3,648,160	-0.38 %
1.	ABD	160,372,040	-4,586,480	-2.78 %
2.	Brezilya	67,886,280	+2,228,460	+3.39 %
3.	Hindistan	62,615,300	+917,540	+1.49 %
4.	Endonezya	47,926,500	-881,080	-1.81 %
5.	Meksika	40,894,260	+1,084,040	+2.72 %
6.	Türkiye	32,849,260	+588,340	+1.82 %
7.	Büyük Britanya	31,771,120	-826,340	-2.53 %
8.	Filipinler	30,065,320	-148,820	-0.49 %
9.	Fransa	25,208,600	-293,760	-1.15 %
10.	Almanya	25,090,540	-193,700	-0.77 %

Kaynak: Quintly, 2013

Şekil 1. 6. Facebook'un Haziran 2013 İtibariyle Ülkelere Göre Kullanıcı Sayıları

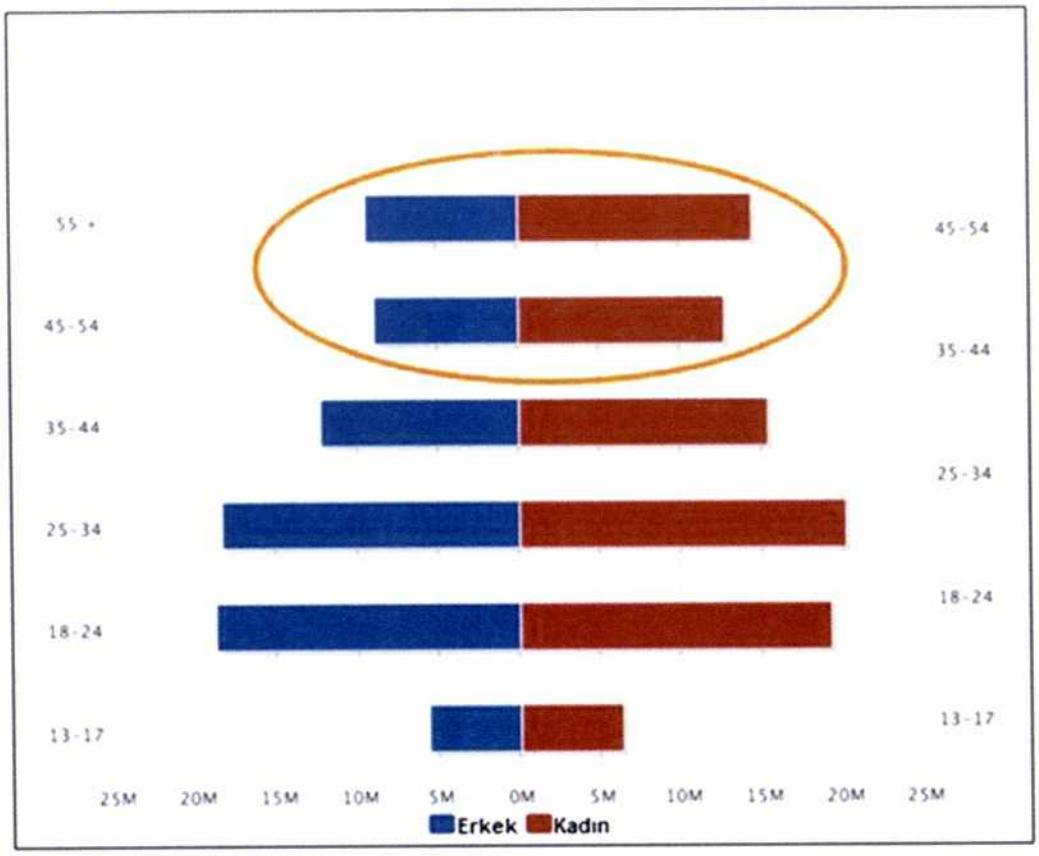
	Ülkeler	Kullanıcı Sayısı	Değişim	+/- %
	Dünya	982,605,720	+417,680	+0.04 %
1.	ABD	158,922,860	+94,360	+0.06 %
2.	Brezilya	71,864,860	+114,160	+0.16 %
3.	Hindistan	63,792,680	-115,660	-0.18 %
4.	Endonezya	47,971,440	-12,220	-0.03 %
5.	Meksika	42,571,360	+186,840	+0.44 %
6.	Türkiye	32,775,240	-22,260	-0.07 %
7.	Büyük Britanya	31,130,260	-34,260	-0.11 %
8.	Filipinler	30,284,820	-80,300	-0.26 %
9.	Fransa	25,392,200	+42,860	+0.17 %
10.	Almanya	24,970,100	+11,640	+0.05 %

Kaynak: Quintly, 2013

İstatistikler incelendiğinde bazı ülkelerde Facebook kullanıcı sayısı artarken bazı ülkelerde ise azalma eğilimindedir. Ancak milyarlarca kullanıcıya sahip Facebook'un kullanıcı sayısındaki bu küçük değişiklikler çok önemli değerler değildir.

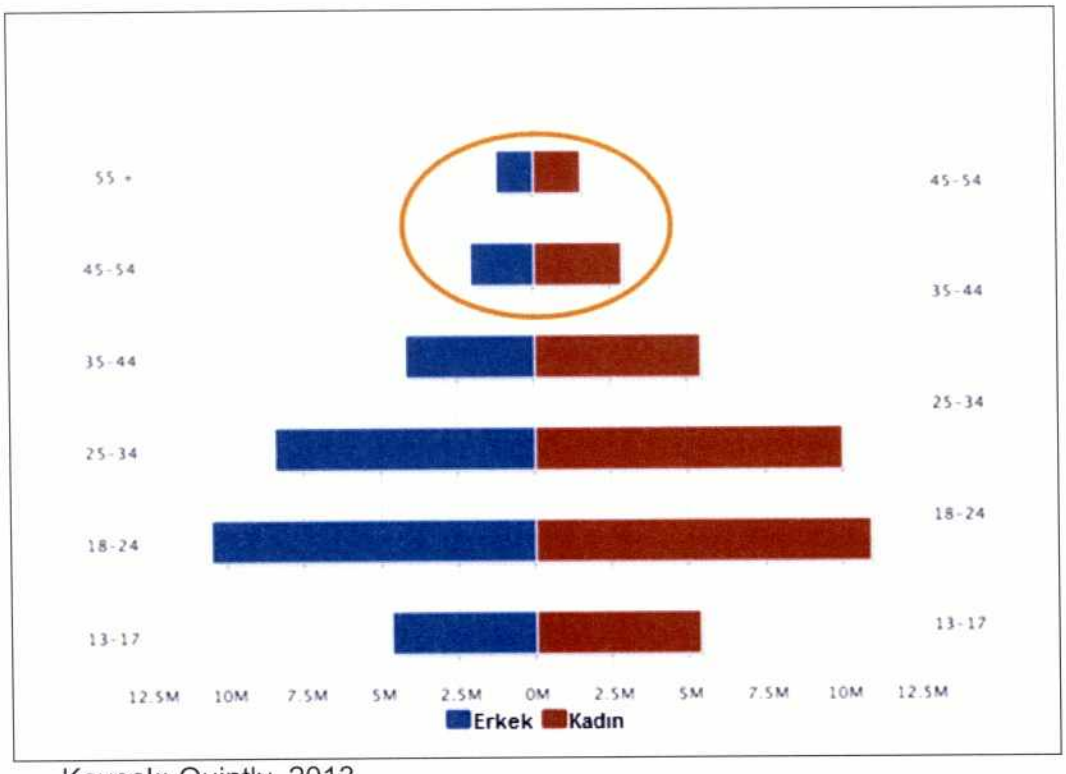
Facebook'un kullanıcıları incelendiğinde en yoğun yaş aralığının 18-34 olduğu görülmekte olup, ABD'de orta yaş ve üstü de önemsenecek derecededir. Bunun yanında Dünya genelinde erkek kullanıcıların sayısı kadınlara göre daha fazladır.

Şekil 1. 7. ABD'de Facebook Kullanıcılarının Yaş Açısından Dağılımı



Kaynak: Quintly, 2013

Şekil 1.8. 2013 Yılı İtibariyle Brezilya'da Facebook Kullanıcılarının Yaş Açısından Dağılımı



Kaynak: Quintly, 2013

Facebook daha önce kurulmuş sosyal paylaşım ağlarına göre kullanıcılarına çok daha fazla hizmet sunmaktadır. Bunlar; fotoğraf ve video paylaşma, fotoğrafta yüz etiketleme, haber veya link paylaşma, pazar yeri ile alışveriş imkânı, dürtmeler ve hediye verme şeklinde sıralanabilir. Bireysel kullanıcıların yanında profesyonel kuruluşlar da kullanıcı kitlesine ulaşmak, iletişim içerisinde olmak ve gelişmelerden haberdar etmek için Facebook'u aktif olarak kullanmaktadır (Facebook, 2013e).

Fotoğraf Paylaşımı: Facebook'un en çok rağbet gören uygulamalarından biridir. Bu uygulama ile kullanıcılar arkadaşları ile fotoğraf paylaşabilmektedir. Paylaşılan fotoğraflar üzerinde yorum yapma veya beğenme de kullanıcılar arasında en çok kullanılan fonksiyonlardır. Bunların yanında daha sonra eklenen fotoğrafta kişi etiketleme de kullanıcıların fotoğraf uygulamalarına

olan taleplerini artırmaktadır. Kullanıcıların etiketlendikleri fotoğraflar üzerinde gizlilik ayarları yapabilmesi de kullanıcıların memnuniyetlerini kazanan bir diğer konudur.

Video Paylaşımı: Facebook kullanıcılarına Youtube veya diğer video paylaşım siteleri üzerinden video paylaşımına olanak tanımaktadır. Kullanıcıların birbirlerine video gönderme veya paylaşılan videolar üzerinde yorum veya beğeni yapma gibi imkânları da mevcuttur.

Etkinlikler: Kullanıcılar arkadaşları ile Facebook üzerinden etkinlik davetleri oluşturabilmekte ve organizasyon yapma imkânına sahip olmaktadır.

Dürtmeler: Dürtme fonksiyonu kullanıcıların arkadaşlarını iletişim kurmaya çekmek adına gerçek dünyadan sanal ortama uyarlanan bir fonksiyondur. Dürtme anlamında çeşitli uygulamalar da geliştirilmiştir.

Uygulamalar: Uygulama oluşturma veya uygulama yükleme Facebook'a sonradan eklenen ve kullanıcıların oluşturdukları uygulamaların paylaşılmasına, kullanılmasına olanak tanıyan Facebook fonksiyonudur. Bu uygulamalar Facebook API aracılığı ile geliştirilmekte ve Facebook'a yüklenmektedir.

Hediyeler: Kullanıcıların birbirlerine belli bir ücret dahilinde gönderdikleri armağanlardır. Bu hediyeler genelde özel bir günü kutlama veya sevgililer arasında sıkça kullanılmaktadır.

Pazar Yeri: Pazar yeri Facebook kullanıcılarının Facebook ortamında satış yapmalarına olanak tanıyan bir Facebook fonksiyonudur. Facebook bu hizmeti kullanıcılarına şimdilik ücretsiz olarak sunmaktadır.

Facebook dünyanın en çok kullanıcıya sahip sosyal paylaşım ağı olmasına rağmen akademik çevrelerce sıkça eleştirilmektedir. Bu eleştirilerin başında

kullanıcı bilgilerinin üçüncü kişilerle paylaşılması ve sürekli kullanılması durumunda bir bağımlılık haline gelmesi bulunmaktadır. Facebook'a yöneltilen eleştirilerden bir diğeri de kullanıcı ayarlarının yanlış yapılması durumunda kullanıcı bilgi güvenliğinin yeterli seviyede sağlanamamasıdır. Şubat 2009 yılında Lordlar Kamarasında bir konuşma yapan Oxford Üniversitesi profesörlerinden Lady Greenfield'e göre Facebook'un uzun süre kullanılması kişilik bozukluklarına ve beyinde küçülmeye neden olmaktadır (Guardian, 2013). Kullanıcı sayısının milyarlarla ifade edilmesi dünya genelinin siyasi, ekonomik veya dini tercihleri üzerinde etki yapabileceği açısından da sıkça tartışma konusu olmaktadır. Arap baharı olarak tanımlanan Ortadoğu'nun en büyük siyasi ayaklanmasına yaptığı etki bu gerçeği ortaya koymak açısından çok çarpıcı bir örnektir.

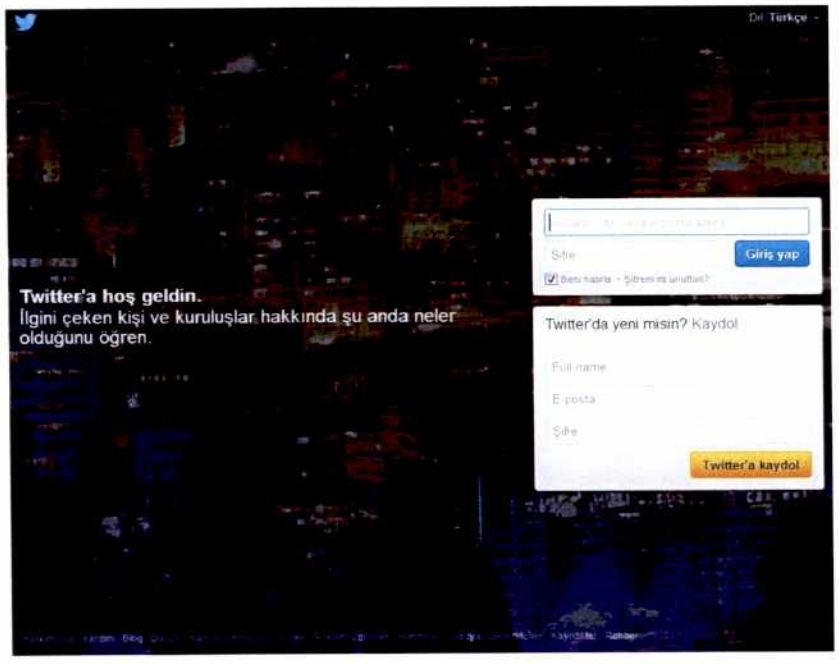
1.3.2. Twitter

Twitter bir mikroblog sitesidir. 2006 yılında Jack Dorsay, Evan Williams ve Biz Stone tarafından kurulmuştur. Twitter insanların internet ortamında duygu ve düşüncelerini, haber, link veya bilgi paylaştıkları bir sosyal paylaşım ağıdır. Twitter kullanıcıları, takip etmek istedikleri kişileri listelerine ekleyerek onların paylaştıkları 'tweet' denilen ve maksimum 140 karakterden oluşan paylaşımları takip edebilmektedir. Twitter'ı sadece bir paylaşım ağı olarak ifade eden olduğu gibi bir haber paylaşım ağı olarak da tanımlayanlar bulunmaktadır. Her iki tanım da yanlış değildir. Çünkü insanlar Twitter'da sıkça haber de paylaşmaktadır (Campo-Avila vd., 2013, s.437-444).

Twitter'ı diğer sosyal paylaşım ağlarından ayıran en önemli fark, takip işleminin tek taraflı olmasıdır. Yani bir kullanıcı binlerce hatta milyonlarca kişi tarafından takip edilebilir, ancak hiç kimseyi takip etmeyebilir. Bu, en çok ünlü isimlerin beklentilerini karşılamaktadır. Twitter, akıllı telefonların gelişmesi ile tıpkı Facebook gibi cep telefonları aracılığı ile de milyonlarca kişi tarafından kullanılmaktadır (Campo-Avila vd., 2013, s.437-444).

Twitter, pek çok açıdan Facebook'a benzemektedir. Her iki sistem de insanların iletişim kurmalarını ve bir şeyler paylaşmalarını sağlamaktadır. Ancak iki sosyal paylaşım ağının kullanım şekli birbirinden farklılık göstermektedir. Kimi kullanıcı için Twitter'ın her bir Tweet'i 140 karakter ile sınırlaması çok yanlış bulunmakla beraber, kimisi için ise bu en büyük avantaj olarak nitelendirilmektedir. Çünkü bu özelliğin insanları daha rahat bir ortamda hissetmelerini sağladığı düşünülmektedir (Dunlap vd., 2011, s.292-315).

Şekil 1. 9. Twitter'ın Kullanıcı Ara Yüzü (2013)

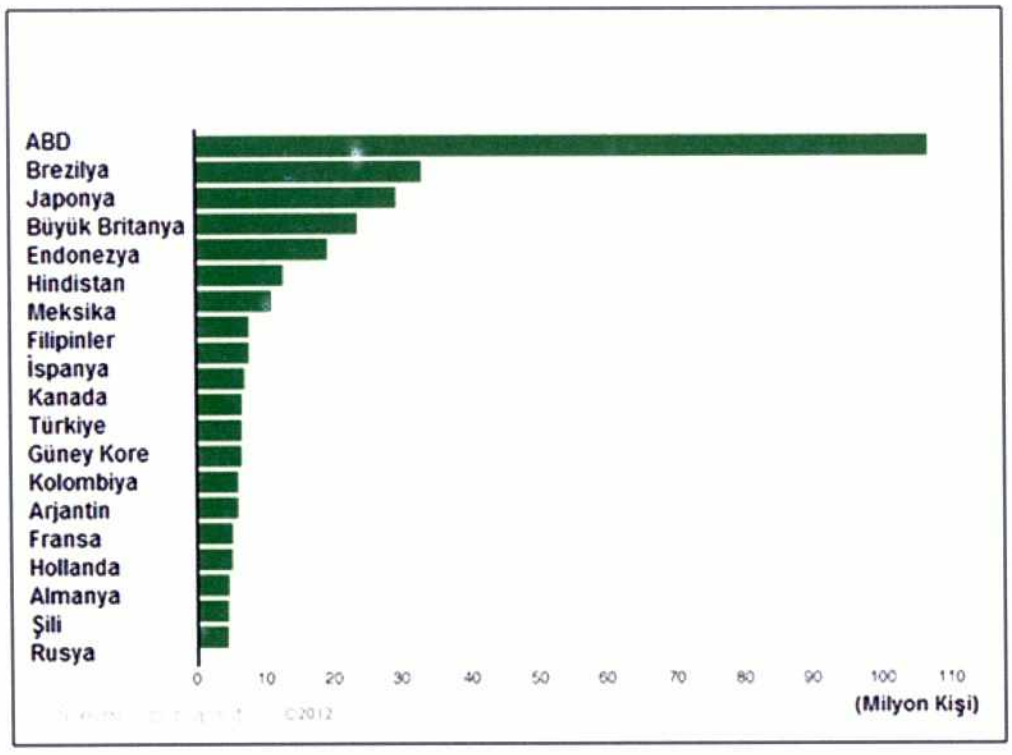


Kaynak: Twitter 2013c

Twitter da Facebook gibi çok kısa bir geçmişe sahip olmasına rağmen yüz milyonlarca kişi tarafından kullanılmaktadır. Mayıs 2013 itibariyle 554 milyon Twitter kullanıcısı bulunmakta ve bunların 135 milyonu her gün hesabına giriş yapmaktadır. Yine aynı araştırmaya göre günde ortalama 58 milyon tweet atılırken, Twitter kullanıcılarının %43'ünün tweet atmak için cep telefonlarını kullandığı ve saniyede 9.100 tweet atıldığı görülmüştür. Kuruluşundan beri atılan tweet sayısı 170 milyara ulaşan Twitter'ın 2013 yılı içinde

$399.500.000 reklam geliri elde edeceği tahmin edilmektedir (Statistic Brain, 2013a; a.g.e.).

Şekil 1. 10. 2012 İtibariyle Twitter'ın Kullanıcı Sayılarının Ülkelere Göre Dağılımı



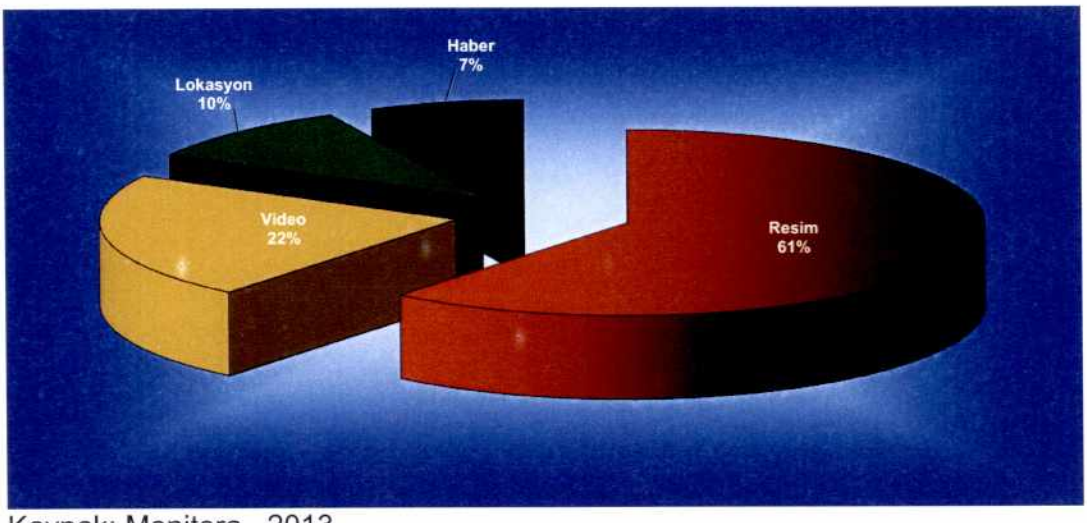
Kaynak: The Next Web, 2013

Montera adlı bir araştırma şirketinin yaptığı bir araştırmaya göre 2012 itibariyle Twitter'ın Türkiye'de 7.2 milyon kullanıcısı bulunmaktadır. Bunların 5.3 milyonu Twitter hesaplarını aktif olarak kullanmaktadır. Türkiye'de günlük atılan tweet sayısı ise 1.7 milyondur. İllere göre bakıldığında ise İstanbul'un %58 ile ilk sırada bulunduğu, İstanbul'u, %13 ile Ankara, %11 ile İzmir'in takip ettiği görülmüştür. (Sabah, 2012).

Aynı şirketin 2013 yılında yaptığı araştırmaya göre ise Türkiye'deki Twitter kullanıcı sayısı 9.6 milyondur. Yani bir yılda kullanıcı sayısı %33 oranında artmıştır. Bu kullanıcıların 6.3 milyonu Twitter'ı aktif olarak kullanmaktadır.

Aktif kullanıcı sayısı aylık 6.2 milyon kullanıcı iken haftalık 4.3 milyon kullanıcıya ulaşmaktadır. Bir Tweet ortalama 70 karakterden oluşmakta olup, saniyede 92 Tweet atılmaktadır. Atılan Tweet'lerde En çok kullanılan saat diliminin 22:00-23:00 arası olduğu, en çok kullanılan günün çarşamba günü olduğu ortaya konulmuştur. Araştırmanın en ilginç detayı ise Türkiye'de günde 8 milyon adet Tweet'in atılmasıdır. Bu sayı bir önceki yıla göre %470 oranında artış anlamına gelmektedir (Monitera, 2013).

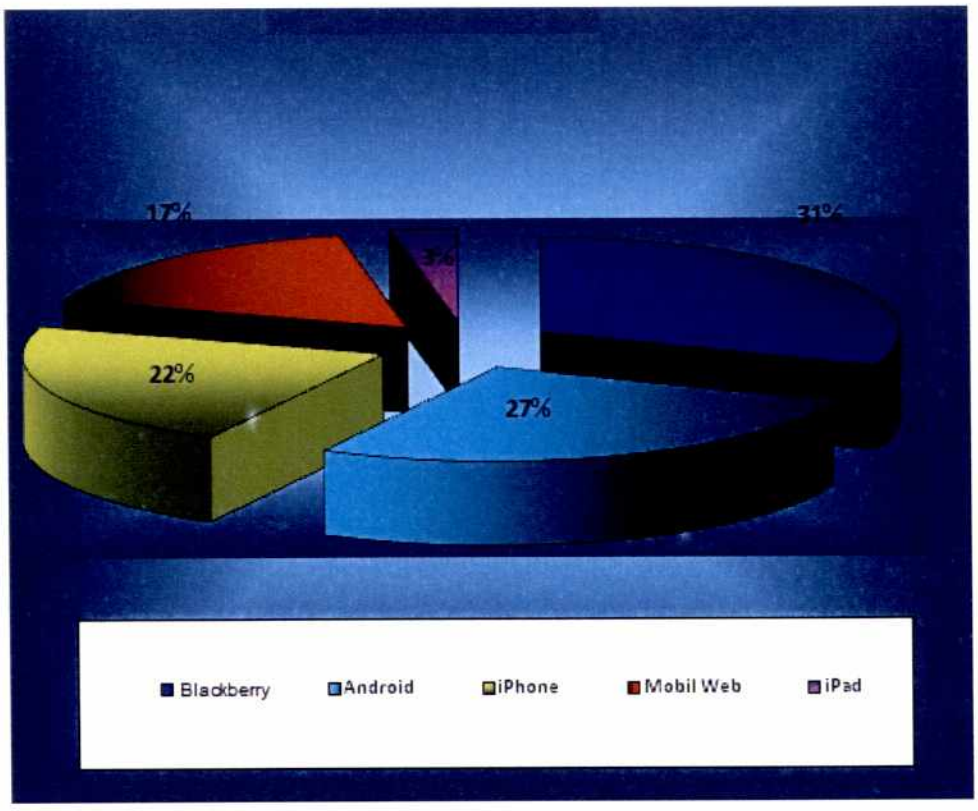
Şekil 1. 11. Twitter' da 2013 Yılı İçinde Paylaşım Yüzdeleri



Kaynak: Monitera, 2013

Şekil 1.11.'de Türkiye'de Twitter'daki paylaşım yüzdeleri gösterilmiştir. Aynı arastırmaya göre %39 oranında web, %61 oranında mobil cihazlar kullanılmıştır. Markalara göre mobil cihaz kullanımları şekil 1.12'de belirtilmiştir.

Şekil 1. 12. Twitter' da 2013 Yılı İçinde Markalara Göre Mobil Cihaz Kullanımları



Kaynak: Monitera, 2013

1.3.3. Youtube

Youtube 2005 yılında kurulmuş olan bir video paylaşım sitesidir. Youtube temelde bir video paylaşım sitesi olsa da pek çok açıdan bir sosyal paylaşım ağı olarak nitelendirilebilir. Kullanıcılar Youtube'a video, animasyon, slayt veya amatör çekimlerini ekleyebilmektedirler. Yüklenen videoları izleyerek üzerinde yorum yapabilmekte, hatta bir tartışma ortamı yaratabilmektedirler. Bu özellikler Youtube'un daha çok kullanıcıya hitap etmesini sağlamaktadır.

Youtube teknolojisi incelendiğinde Adobe Flash Player tabanlı olduğu ve SorensonSpark H.263 video kodeğini kullandığı görülmektedir. Videolar 320'ye 240 ebatında gösterilmektedir. Youtube, video yüklerken WMA, AVI, MOV ve MPG formatlarını kabul etmekte iken bu formatları FLV formatına çevirerek kullanıcılarına sunmaktadır. Youtube'un popülaritesini ve kullanıcı sayısını artıran en önemli etkenlerden biri de Youtube dışındaki sitelerde yayınlanmasına izin veren HTML kodlarını kullanıcılarına sunmasıdır. Bu özellik videoların diğer sosyal paylaşım ağlarında da kolayca paylaşılmasına imkân sunmaktadır (Cheng vd., 2008).

Youtube istatistikleri incelendiğinde ne kadar çok kullanılan bir ağ olduğu daha net anlaşılmaktadır. 2012 yılı verilerine göre Youtube'a günde 4 milyar video eklenirken, Youtube üzerinden izlenen toplam video sayısı 3 milyar saate ulaşmıştır. Her gün 800 milyon kişi Youtube'u ziyaret ederken bunların %70'i ABD dışından oluşmaktadır. Youtube 54 dilde hizmet vermekte iken 2011 yılına kadar 1 trilyon kere ziyaret edilmiştir. Google 2006 yılında Youtube'u satın almak için 1.65 milyar dolar ödemiştir (Statistic Brain, 2013b).

Youtube'un açıkladığı 2013 verilerine göre ise ayda 1 milyar kişi Youtube'u ziyaret etmektedir. Ayda 6 milyar saat video izlenmektedir. Bu da dünyada yaklaşık kişi başı bir saat Youtube üzerinden video izlenmesi anlamına gelmektedir ki bu inanılmaz bir rakam olarak nitelendirilebilir. Her dakikada 100 saatlik video yüklenmekte iken yine oluşan trafiğin %70'i ABD dışından kaynaklanmaktadır. Youtube 56 bölgede yerelleşme faaliyeti gerçekleştirmiş olup, 61 dilde hizmet vermektedir. Youtube Türkçe dil desteğini ise Ekim 2012 tarihinden itibaren vermeye başlamıştır. Videolara yapılan yorumlar milyonlarla ifade edilirken bu sayı her sene katlanmaktadır (Youtube, 2013).

1.3.4. Google+

Google+ 2011 yılında, Google'ın Facebook ve Twitter'a rakip olması hedefiyle kurulmuş bir sosyal paylaşım ağıdır. Daha sonra kurulmasına rağmen kullanıcı sayısı hızla artmaktadır. Google+'ı diğer sosyal paylaşım ağlarından ayıran en önemli fark ve avantaj Google'ın Gmail, Youtube gibi diğer hizmetleri ile entegre olması ve uyumlu şekilde paylaşılmasıdır. Bir başka deyişle Google+ kullanıcılarına bir sosyal paylaşım ağından daha fazlasını sunmaktadır. Bu da kullanıcı sayısını hızla artırmaktadır.

2013 verilerine (StreamSocial Q1 2013 raporu) göre Google+ aylık 359 milyon kişi tarafından kullanılmaktadır. Google+, Twitter'dan (%44) sonra yıllık büyümede % 33 ile en hızlı büyüyen ikinci sosyal paylaşım ağı konumundadır. Google'ın aktif kullanıcı sayısı, Facebook (%82) ve Twitter'ın (%62) ardından %60 ile üçüncü sırada bulunmaktadır (Global Web Index, 2013).

1.3.5. LinkedIn

2003 yılında kurulan LinkedIn dünyadaki en büyük iş ağı konumundadır ve büyümeye devam etmektedir. Ancak Twitter veya Google+'a göre bu büyüme çok hızlı bir büyüme olarak değerlendirilemez. Bununla beraber 200 milyondan fazla kişi tarafından kullanılmaktadır. LinkedIn'i Facebook, Twitter ve Google+'tan ayıran en önemli özellik tamamen iş hayatına odaklanmış bir sosyal paylaşım ağı olmasıdır. Sistem aynı zamanda iş arayanlarla işverenleri buluşturan bir platformdur (Yavanoğlu vd., 2012).

İstatistiklere bakıldığı zaman Visual.ly raporuna göre saniyede 2 kişi LinkedIn'e üye olmaktadır. Kullanıcılarının %64'ü Amerika dışından olan LinkedIn'in kullanıcılarının %42'si profillerini düzenli bir şekilde güncellemektedir. LinkedIn kullanıcılarının %35'i her gün sayfalarına giriş

yapmaktadır. Kullanıcılarının %39'u profesyonel kullanım hesapları için ücret ödemektedir. LinkedIn kullanıcılarının %81'i en az bir ağ grubuna üye konumundadır (Visual, 2013).

1.3.6. Instagram

2010 yılında Mike Krieger ve Kevin Systrom tarafından kurulan Instagram, fotoğraf filtreleme temeline dayanmaktadır. Kullanıcılar çektikleri fotoğrafları Instagram'da çeşitli filtrelerden geçirerek fotoğraflarını paylaşabilmektedirler. Amaro, Mayfair, Rise, Walden, Kelvin bu filtrelemelerden bazılarıdır. Facebook tarafından 1 milyar dolarla satın alınan Insatagram'a fotoğrafları etiketleme özelliği de eklenmiş ve bu durum kullanıcı sayısını hızla artırmıştır. Kullanıcıları tarafından kullanımını kolaylaştırmak için mobil cihazlar üzerinden kullanıma olanak tanıyan sosyal paylaşım ağlarından biri de Instagram'dır. Bu şekilde Instagram kullanıcılarına cep telefonları aracılığıyla çektikleri fotoğrafları kolay bir şekilde Instagram ve diğer paylaşım ağları üzerinden paylaşma olanağı tanımaktadır. Instagram'ın fotoğrafları filtreleyebilme imkânı daha çok kullanıcıya hitap etme olanağı tanımaktadır.

Instagram; iletişim içerisinde olduğunuz arkadaşlarınızdan hangilerinin Instagram kullanıcısı olduğunu görme ve fotoğraf paylaşımı yaparken resimleri etiketleme imkânı ile daha etkileşimli bir iletişim ortamı sunmaktadır. Etiketlendiğiniz fotoğraflar üzerinde gizlilik ayarları yapabilmek de bir diğer avantaj olarak tanımlanabilir (Sosyal Medya Kulübü, 2013).

1.3.7. MySpace

2003 yılında kurulan MySpace daha çok müziğe ilgi duyan kullanıcıları ve müzik gruplarını bir araya getiren bir sosyal paylaşım ağıdır. Kullanıcılar

müzik ile ilgili paylaşımlar yaparken videolarını, fotoğraflarını ve müzikleri ile ilgili paylaşımlarını yapmaktadır. Bu durum amatör müzisyenler için bulunmaz fırsatlar doğurabilmektedir. Bunun yanında profesyonel müzisyenlerin de hayranları ile iletişim kurmalarına da olanak tanımaktadır.

2013 verilerine göre MySpace'in 32.6 milyon kullanıcısı bulunmaktadır. MySpace'in piyasa değerinin 12 milyar dolar olduğu düşünülmektedir. MySpace üzerindeki şarkıcı sayısı 14.2 milyon iken 53 milyon şarkı bulunmaktadır (Digital Marketing Ramblings, 2013).

1.3.8. Flickr

2004 yılında Ludicorp tarafından kurulan Flickr daha çok fotoğraf paylaşımını temel alan bir sosyal paylaşım ağıdır. Kullanıcılarının bol bol fotoğraf paylaştıkları Flickr kullanıcılarına aylık 100 MB fotoğraf yükleme sınırı koymaktadır. Önceleri sadece fotoğraf yüklenmesine izin veren Flickr, 2008 yılından itibaren video yüklemeye de izin vermeye başlamıştır. Fotoğraf ve video yüklemeye sınır koyan Flickrpro kullanıcılarına bu anlamda daha fazla imkân sunmaktadır (Yavanoğlu vd., 2012; Flickr, 2013).

1.3.9. Diğer sosyal paylaşım ağları

Facebook, Twitter, Google+ dünya çapında çok geniş kitlelere ulaşan sosyal paylaşım ağlarıdır. Ancak alan olarak daha dar fakat kullanıcı sayısı bakımından çok büyük kitlelere hitap eden sosyal paylaşım ağları da mevcuttur. Bunların başında Qzone ve Orkut gelmektedir.

Qzone Tencent tarafından 2005 yılında kurulmuştur. Qzone daha çok Çin'de çok sayıda kullanıcıya ulaşmış bir sosyal paylaşım ağıdır. 2013 verilerine göre 599 milyon kullanıcısı bulunmaktadır. Kullanıcılarının bloglarını yazabildikleri, günlüklerini tutabildikleri, fotoğraf gönderebildikleri ve müzik

dinleyebildikleri Qzone, kullanıcılarına profil arka planlarını değiştirme gibi kişileştirme imkânları da sunmaktadır (China Internet Watch, 2013).
2004 yılında Google'ın Türk çalışanlarından Orkut Büyükkökten tarafından kurulan Orkut yine Qzone gibi bazı ülkelerde sıkça kullanılan sosyal paylaşım ağlarından biridir. Ekim 2012 itibarıyla Dünya çapında 33 milyon aktif üye sayısına ulaşmış olsa da üyelerin çoğunluğu sadece Brezilya, Hindistan ve Japonya'dan gelmektedir. Daha sonra Google'a satılan Orkut Google+ ile paralel çalışmaktadır (Tübitak, 2013).

Yeni nesil sosyal paylaşım ağlarına bir diğer örnek de Zello Walkie Talkie'dir. Bu sosyal paylaşım ağı, kullanıcılarının akıllı telefonlarına kurdukları uygulama ile telsiz gibi haberleşmelerini sağlamaktadır. Kullanıcılar bu uygulamayı iPhone, Android veya BlackBerry gibi farklı platformlar üzerine kurarak kullanabilmektedir. Bu sosyal paylaşım ağı Türkiye'de Gezi olayları ile adını duyurmuştur. Gezi Parkı eylemcileri bu uygulama ile birbirleriyle anlık iletişim kurarak kalabalığın nerede olduğu veya güvenlik güçlerinin konumu hakkında bilgi paylaşımı yapmışlardır. Eylemciler "Taksim Direniş", "Ankara Direniş" ve "İzmir Direniş" gibi gruplar kurmuşlar ve bu gruplar üzerinden iletişim kurmuşlardır (Milliyet, 2013).

Üzerinde durduğumuz sosyal paylaşım ağları dışında Renren, Cyworld, Mixi, Skyrock, Badoo, Netlog, Hi5, Pinterest bunlardan bazılarıdır. Bu sosyal paylaşım ağlarından Renren Çin'de, Mixi Japonya'da, Skyrock Fransa'da, Cyworld Güney Kore'de çok yaygın olan sosyal paylaşım ağlarıdır (Onat Ferah, Alikılıç özlem, 2008).

2. KİŞİSEL VERİLER

Bu bölümde, kişisel verilerin tanımından, öneminden ve korunması için alınması gereken güvenlik önlemlerinden bahsedilecektir.

2.1. Kişisel Veri Nedir?

Bilgi; telefon, radyo ve televizyon gibi haberleşme araçlarının icat edilmesi ve kullanılmaya başlanmasından itibaren önem kazanmaya başlamış, bilgisayar teknolojileri ve internetin yaygınlaşması ile herkes tarafından ulaşılabilir bir hale gelmiştir. Günümüzde bireyler özel ve resmi her türlü işlemlerini internet üzerinden gerçekleştirebilmektedirler (Civelek, 2011; GAO, 2008; Chen ve Shuo 2009). Bireyler mutfak alışverişlerini, değerli eşyalarının ve elektronik eşyalarının alım satım işlemlerini yerlerinden kalkmadan, rahatlıkla internet üzerinden yapabildikleri gibi (Gittigidiyor, 2013) özel işlemleri haricindeki, resmi işlerini de internet üzerinden yapabilmektedirler. Günümüzde adli sicil kaydı bilgisi edinmek, birey hakkında sürmekte olan davaları takip etmek, askerlik durumunu, sigorta bilgilerini ve tıbbi bilgileri görüntülemek gibi işlemler internet üzerinden oldukça kolay gerçekleştirilebilmektedir (Chen ve Shuo 2009; Türkiye, 2013a; Türkiye, 2013b). Bu durum kişisel bilgilerin önemini ortaya koymaktadır. Bir bireyin kişisel bilgilerinin, başka bir birey tarafından ele geçirilmesi durumunda, kişisel bilgilerini kaybeden kişinin hayatına müdahale edilmesi, maddi ve/veya manevi zarar verilmesi mümkün hale gelecektir.

Kişisel verilerin neler olduğu bilgisi bireylerin yorumlarına göre değişiklik gösterebilir, bir birey doğum tarihinin kişisel veri olduğunu söylerken, bir diğeri ise bunun kişisel veri olmadığını savunabilir. Bu karışıklığın giderilmesi için kişisel verinin tanımının mevzuatlarca yapılması gereği ön plana çıkmış ve birçok devlet tarafından kanunlar veya Uluslararası sözleşmelerle bu tanım yapılmıştır (Koç ve Kaynak, 2010).

Kişisel bilgi ya da kişisel veri ile ilgili olarak, Avrupa Konseyi (1981) 108 sayılı sözleşmesinin ikinci maddesinde şu tanıma yer verilmiştir: Kişisel nitelikteki veriler; kimliği belirten veya belirtebilen, gerçek kişi ile ilgili tüm bilgileri ifade eder (Avrupa Konseyi, 1981; TBMM, 2013a).

Amerika Birleşik Devletlerine göre kişisel bilgiler şu şekilde tanımlanmıştır; Kişisel bilgiler, isim, soysal güvenlik numarası, doğum tarihi ve yeri, anne kızlık soyadı, biyometrik kayıtları gibi bireyin kimliğini ortaya çıkarabilecek her türlü bilgi ve birey ile bağlantılı veya bağlantı kurulabilecek, tıbbi kayıtlar, eğitim ve finansal durum gibi bilgilerdir (NIST, 2010).

Birleşik Krallık ise şu tanıma yer vermiştir; Kişisel kayıtlar bir bireyin, fiziksel ve zihinsel sağlığını, aldığı ruhsal danışmanlığı, herhangi bir organizasyon ya da kişi tarafından refah için verilen danışmanlığı belirtebilecek her türlü veriden oluşur (Legislation, 2013).

Avustralya ise şu şekilde tanımlamaktadır. Doğru olup olmadığı ve bir ortama kaydedilip kaydedilmediği önemsiz olarak, bir bireyin kimliğini ortaya çıkaran ya da ortaya çıkmasına neden olabilecek her türlü bilgi ve görüş kişisel bilgidir (Pla, 2013).

Türkiye Cumhuriyeti'nde ise, Türkiye Cumhuriyeti Anayasası (TBMM, 2013a) ve 5237 sayılı Türk Ceza Kanunu (TBMM, 2013c) ile korunmakta olan kişisel bilgiler, Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından hazırlanarak 06/02/2004 tarihli ve 25365 sayılı Resmi Gazetede yayınlanan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması hakkında yönetmeliğe göre; "tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası veya fiziksel, psikolojik, zihinsel, ekonomik, kültürel ve sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgiyi" ifade ederken, 24/07/2012 tarihli ve 28363 sayılı Resmi Gazetede yayınlanan ve ocak 2013 tarihinde

yürürlüğe giren Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması hakkında yönetmeliğe göre ise "kişisel veri; belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler olarak" (BTK, 2013a), ifade edilmektedir.

Bu tanımlara istinaden, elektronik posta adresleri ve bilgisayarların ağ (internet) bağlantılarında kullandıkları IP adresleri de kişisel veri olarak sınıflandırılabilir çünkü bu adresler sayesinde bireylerin bilgisayarlarına ve dolayısıyla bireylere ulaşmak mümkündür (Fenafil, 2013).

2.2. Kişisel Verilerin Önemi

Genel yaşam, kişisel ve sektörel mahremiyet ihtiyaçlarından yola çıkılarak kişisel veri olarak değerlendirilebilecek veriler ve önemleri (Slideshare, 2013) aşağıda belirtilmektedir:

"1) **Hayata ilişkin veriler:**
Ayrımcılığa uğramamak için din, dil, ırk, sicil bilgisi, siyasi eğilimi ve özel hayata ilişkin bilgilerdir.

2) **Maddi veriler:**
Bireyin mal varlığı, borçları, gelirleri, yaptığı alış verişler, kredi kartı gibi, maddi durumunu gösteren bilgilerdir.

3) **Internet kullanımına ilişkin kişisel veriler:**
Internet üzerindeki yazışmalar, ziyaret edilen web siteleri ve internette paylaşılan veriler özel olarak değerlendirilebilir. Ayrıca internet erişimine ilişkin IP kayıtlarının, internet servis sağlayıcısının sunucuları üzerinde tutulabiliyor olması da mahremiyeti artırmaktadır.

4) **Sağlıkla ilgili kişisel veriler:**
Sağlık ile ilişkili veriler, kişilerin toplum ile olan ilişkilerini, sigorta kapsamlarını ve bankalardan alacakları kredi hususlarını etkileyebileceğinden hassas kabul edilebilir. Biyometrik veriler de, kişilerin kimliklerini ortaya çıkaracağından kişisel veriler arasındadır.

5) **Politik kişisel veriler:**
Toplum barışı ve seçme özgürlüğü açılarından politik veriler mahrem verilerdir.

2.3. "Kişisel Verilerin Korunması", "Veri Güvenliği" İlişkisi

"Kişisel verilerin korunması" ve "veri güvenliği" kavramlarının nereden geldiği tam olarak bilinmemekle beraber, ilk defa Almanca'da kullanıldığı ve buradan diğer dillere geçtiği düşünülmektedir. Bu kavramlar Avrupa'da yaygın olarak kabul görmesine rağmen, ABD ve Kanada gibi diğer ülkelerde ise "özel yaşamın gizliliğinin" korunması kavramı ortaya çıkmaktadır (Kaya, 2005).

Kişisel verilerin korunmasından kasıt, verilerin kendisinin korunmasından daha çok kişinin korunması, bu bilgilerle, kişiye doğrudan ulaşılmasının önüne geçilmesidir. Dolayısıyla, kişisel veri korunması ile veri güvenliği arasında bir ayrım bulunmaktadır. Veri, her türlü bilgiyi kapsarken, kişisel veriler, sadece bireylerin kimliklerine doğrudan veya dolaylı olarak ulaşılmasına imkân veren bilgilerdir (Avrupa Konseyi, 1981; NIST, 2010; Legislation, 2013; Pla, 2013; Kaya, 2005; Bygrave, 2002; Gola ve Rudolf 2007). Örneğin, meteorolojik bilgileri içeren verilerin saklanması ve başkalarının görmesine karşı önlemler alınması halinde, bu, veri güvenliği olarak değerlendirilecektir. Ancak, bir bireyin ismi, Türkiye Cumhuriyeti (T.C.) kimlik numarası gibi bilgilerin saklanması ve korunması, kişisel verilerin korunması olarak sınıflandırılabilir.

2.4. Kişisel Verilerin Güvenliği ve Güvenlik Önlemleri

Kişisel veriler, gerek bireyler hakkında istihbarat bilgisi toplamak, gerek maddi kazanç sağlamak maksatlı, kötü niyetli kişilerin hedefi konumundadırlar. Bu bilgileri içeren verilerin elde edilmesinde pek çok yöntem kullanılmaktadır. Genellikle kullanıcının bilinçsizliğinden faydalanan bu yöntemlerden en yaygın olanları ve bu saldırı yöntemlerine karşı uygulanabilecek gerek bireysel gerek sunucu odaklı koruma yöntemlerinden bazıları aşağıda sıralamıştır (Yavanoğlu vd., 2012);

" - Kimlikleri Taklit Etmek

- Yemleme (Phishing) Saldırısı
- İstenmeyen E-Postalar (Spam)
- Kötü Amaçlı Sosyal Ağ Uygulamaları
- Siteler Arası Kod Çalıştırma (XSS) ve Siteler Arası İstek Sahteciliği (XSRF)
- Casusluk/Casus Yazılımlar
- Sahte Linkler
- DNS Yanıltma (Spoofing) Saldırıları"

2.4.1. Kimlikleri taklit etmek

Sosyal paylaşım ağlarında bir başkasının yerine geçerek, yerine geçilen kişi gibi davranmak, onu taklit etmek ve bu yönde sosyal paylaşım ağları üzerinde hesap açmak işlemlerine denmektedir. Bu yöntemle birey, sevdiği bir şarkıcıyı, siyasetçiyi, sanatçıyı övüp yüceltebilmekte, hayran kitlesini artırabilmekte ya da sevmediği bir kişiyi yererek kişiliğine zarar verebilmekte, hayranlarını kaybetmesine ve gerek maddi gerek manevi zarar görmesine neden olabilmektedir.

Bu saldırı yöntemine karşı alınabilecek etkili bir önlem bulunmamasına karşın bireyler, kendi kimliklerini çalan saldırganlara karşı koymak için kendi profillerinin özgün olduğunu belirtecek işaretler kullanabilirler. Bu işaretlere örnek olarak, profillerinin adresini yazan ve orijinal olduğunu gösteren bir fotoğraf yayınlamak verilebilir (Yavanoğlu vd., 2012).

2.4.2. Yemleme (Phishing) saldırıları

Bu tarz saldırılarda, genellikle kurbana güvenilir kaynaktan olduğunu iddia eden bir e-posta gönderilmektedir. Bu e-posta ile kullanıcıların kişisel bilgileri (kullanıcı adı, şifre, kredi kartı bilgileri, telefon numaraları) talep edilmektedir (Merwe, Loock ve Dabrowski, 2005). Bunu yaparken, güvenilir ve çok kullanılan bir bankanın posta tasarımı taklit edilmekte ve uydurma bir haber yazılarak kullanıcıdan bilgiler talep edilmektedir. Bu yöntemin diğer yöntemlerle beraber kullanıldığı da gözlemlenmektedir. Örneğin, güvenilir bir

bankadan gelen bir e-posta içerisinde, yeni bir kampanyadan söz edilebilir ve bu kampanyadan faydalanmak için belli bir adrese tıklanması istenilebilir. Tıklanılan adres, bankanın kendi internet sitesi yerine, başka bir siteye gidebilir ve bankanın arayüzüne çok benzeyen bir arayüz ile kullanıcıdan kişisel bilgilerini talep edebilir (Bilgigüvenliği, 2013b).

Yemleme saldırılarına karşı en etkili önlem, bireylerin eğitilmesi ve bilinçlendirilmesi olarak karşımıza çıkmaktadır. Bu eğitim günümüzde kullanıcıların, linklere tıklamaması, linki adres çubuğuna doğrudan yazması, müşteri hizmetlerini araması ve kişisel bilgileri vermemesi şeklinde şekillenmiştir (Kumaraguru vd., 2007).

Teknik çözüm olarak ise, tarayıcı geliştiricileri tarafından, internet tarayıcılarına anti-yemleme uygulamaları gömülü olarak eklenmektedir (Blogspot, 2013). Ayrıca, e-posta hizmeti yazılımları da SPAM e-postaları işaretleyerek kullanıcıları uyarmaktadırlar (Squirrelmail, 2013).

2.4.3. İstenmeyen e-postalar (Spam)

Bu saldırılar, yemleme saldırıları ile benzerlik göstermektedirler. Bu saldırılarda, saldırgan ele geçirdiği e-posta hesaplarını kullanarak, kurbanın adres defterindeki herkese posta gönderir ve uydurma bir bahane ile kişisel bilgilerini veya doğrudan para göndermelerini talep edebilir (Bilgigüvenliği, 2013b; BGA, 2013).

Bu saldırılara karşı, yemleme saldırılarına karşı alınan önlemlerin alınması gerekmektedir.

2.4.4. Kötü amaçlı sosyal paylaşım ağ uygulamaları

Facebook ve benzeri sosyal paylaşım ağlarında kullanıcılara yönelik geliştirilen pek çok uygulama ve oyun bulunmaktadır. Bu uygulamalar,

kullanıcıdan habersiz olarak veya kullanıcının bilinçsizliğinden faydalanarak (okumadan onaylama gibi), kullanıcının kişisel bilgilerini alabilmekte veya kullanıcının arkadaş listesinde bulunan herkese e-posta gönderebilmektedir (Yavanoğlu vd., 2012).

Bu tarz bazı uygulama ve oyunlar, kullanıcılara ücretsiz hediyeler (örneğin oyunda fazladan bazı haklar) vermeyi teklif etmektedirler. Bu tekliflere tıklanıldığında, genellikle kullanıcı, farklı bir web sayfasına yönlendirilmekte ve bu sayfa üzerinden bir anket doldurması istenmektedir. Doldurulan bu anket üzerinde kullanıcıların kişisel bilgilerine yönelik sorular bulunmaktadır (Itnewsafrica, 2013).

Kullanıcıların, sosyal ağlar üzerinden oyun ve uygulama kullanacakları zaman, bu uygulamalarının talep ettikleri yetkilere ve kullanıcı sözleşmelerine dikkat etmeleri gerekmektedir. Uygulamada gerekmediği halde profilleri üzerinden kullanıcıların kişisel bilgilerine erişmek isteniyorsa, bu uygulamanın kullanılmaması gerekmektedir. Aynı şekilde uygulama içinden tıklanılarak takip edilen bağlantılarda, kullanıcıdan kişisel bilgilerinin talep edildiği formların doldurulması da risk yaratmaktadır (Itnewsafrica, 2013; Techrepublic, 2013).

2.4.5. Siteler arası kod çalıştırma (XSS) ve siteler arası istek sahteciliği (XSRF)

Siteler arası kod çalıştırma yönteminde saldırı, betik kodları kullanılarak gerçekleştirilir. Saldırgan, bu yöntemi kullanarak sosyal ağ sitesine betik kodu yerleştirir ve bu kod aracılığı ile kurbanın çerez (cookie) oturum (session) bilgilerini almaya (Joomla, 2013), yine bu yöntemi kullanarak, kurbanın bilgisayarında bulunan dosyaları silmeye ya da değiştirmeye çalışabilir, klavye darbelerini kaydederek bilgilerini öğrenebilir ve bu yolla şifrelerini ele geçirebilir ya da zararlı yazılımlar içeren başka bir web sitesi açılmasına neden olabilir (Techrepublic, 2013).

Siteler arası istek sahteciliği ise, siteler arası kod çalıştırmanın aksine, kullanıcının siteye olan güveni yerine, sitenin kullanıcının internet tarayıcısına olan güvenini kullanmaya yöneliktir. Örneğin, bu yöntem kullanılarak gerçekleştirilecek bir saldırıda, saldırgan web sitesine internet tarayıcısı tarafından getirileceği kesin olan bir URL yerleştirir (örneğin resim adresi), bu adres bir bankanın internet adresini, banka kullanıcılarının giriş (Login) bilgilerini çerezlerde tutmakta ve adreste saldırganın banka hesabına para transferi için gerekli bilgiler yer almakta ise, kurban farkında olmadan isteği dışında saldırganın hesabına kendi hesabından para transferi işlemini onaylamış olmaktadır (Shiftleft, 2013).

XSS ve XSRF saldırılarından korunmak ancak sunucu bazlı çözümler ile mümkün olabilmektedir. Kullanıcı kendi internet tarayıcısı üzerinden çerezleri (cookies) iptal edebilir, ancak bu durum, kullanıcının web sitesinden istediği performansı alamamasına neden olacaktır.

Sunucu tarafında, site yöneticileri sitelerini geliştirirken bir kaç temel şeye dikkat etmelidirler. Bunların en başında, gerekli olmadıkça GET yöntemi (verilerin adres çubuğuna yazılarak, herkes tarafından okunulabilir şekilde sunucuya taşındığı yöntemdir) kullanarak kullanıcıdan girdi almamak gelmektedir. GET metodu yerine daha çok POST yöntemi (verilerin, arka planda işlenerek, kullanıcıya gösterilmeksizin sunucuya taşındığı yöntemdir) kullanılması, XSS saldırılarında en temel ve basit yöntem olan adres değiştirerek kullanıcıya saldırmayı engellemektedir. Bunun yanı sıra, kullanıcının sitenin kendisine ait olan formları kullanarak veri gönderdiğinden emin olunmalıdır. Eğer kullanıcı, önceden herhangi bir form talebinde bulunmamışsa ve veri gönderiyorsa, burada şüpheli bir durum olduğunu değerlendirmeli ve işlem yapılmamalıdır. Bunun için, her formun içerisine rastgele üretilmiş bir form ID' si yerleştirilmeli, daha sonra kullanıcıdan veri alınırken, form içersindeki ID ile beraber göndermesi talep edilmelidir. Karşılaştırılan ID' lerde farklılık olması durumunda ise bir problem olduğu var

sayılarak, sunucu tarafında işlem durdurulmalıdır (Shiftleft, 2013; Techrepublic, 2013).

En etkili yöntemlerden bir diğeri ise, sunucuya gelen her türlü veriden, her türlü kodu silmek veya bu kodları tarayıcının yorumlayacağı şekilde değil, kullanıcıya göstereceği şekilde işlemektir (Techrepublic, 2013).

Sonuç olarak XSS ve XSRF saldırılarına karşı en etkili yöntemlerin sunucu tarafında alınabileceği ortaya çıkmaktadır. Geliştirilen web sitelerinin mümkün olduğunca sunucu taraflı kodlar ile çalışması ve istemci taraflı kodları kullanmaması gerekmektedir. Böylelikle, bir kullanıcı kendisini koruma altına almak adına, tarayıcısından Java Script'i devre dışı bıraktığında, site üzerindeki yeteneklerden kayıp olmaksızın faydalanmaya devam edebilecektir (Techrepublic, 2013).

2.4.6. Casusluk / casus yazılımlar

Genellikle internet üzerinden indirilen ücretsiz yazılımlar ile kurbanın bilgisayarına casus yazılımlar kurulabilmekte ve bu yazılımlar ile kurbanın bilgisayarda gerçekleştirdiği işlemler, internet üzerinden uzaktaki bir sunucuya taşınarak izlenebilmektedir. Bu yazılımlar vasıtasıyla saldırgan, kurbanın kişisel bilgilerini (kullanıcı adı, şifre, kimlik no vb.) ele geçirebilmekte ve maddi kazanç sağlayabilmektedir (Federal Trade Commision, 2013; Blogspot, 2013; Onguardonline, 2013).

Kritik kurumlarda görev yapan personelin sosyal paylaşım ağlarında bulunan üyelikleri kurumsal açıdan tehdit oluşturabilmektedir. Üyelik veya profil bilgilerinden, kişilerin arkadaşlıkları, fotoğrafları, yazdıkları veya paylaştıkları bilgiler sayesinde kişisel zafiyetleri ortaya çıkmaktadır. Bu zafiyetler üzerinden farkında olunmadan kurumsal bilgi varlıklarını tehdit eden ve casusluk için iyi bir altyapı oluşturan sorunlar ortaya çıkmaktadır (Yavanoğlu, vd., 2012).

Casus yazılımlar, kurbanın bilgisayarından dışarıya bilgi çıkarabilmek için öncelikli olarak, bilgisayarın ve bulunduğu ağın zafiyetlerinden faydalanmaktadırlar. Bu yazılımların işlevlerini yerlerine getirebilmeleri için, bir şekilde kurbanın bilgisayarına bulaşmaları gerekmektedir. Bulaşma işlemi genellikle kullanıcının internetten ücretsiz indirdiği yazılımlar ve filmler aracılığı ile gerçekleşmektedir. Kullanıcıların bu konuda bilinçlendirilmesi ve internet üzerinden, kaynağından emin olmadıkları hiç bir şeyi indirmemeleri konusunda yetiştirilmeleri gerekmektedir.

Bu yazılımlar farklı olarak, bilgisayarlara, web sitelerinden rastgele fırlayan pop-up pencereler (kullanıcının isteği dışında açılan tarayıcı pencereleri) içerisine gömülmüş scriptlerle, istenmeyen e-postalar (spam) içerisinde (ek olarak veya link olarak) ve işletim sisteminin üzerine kurulu olan yazılımların açıklarını kullanarak da bulaşabilmektedir.

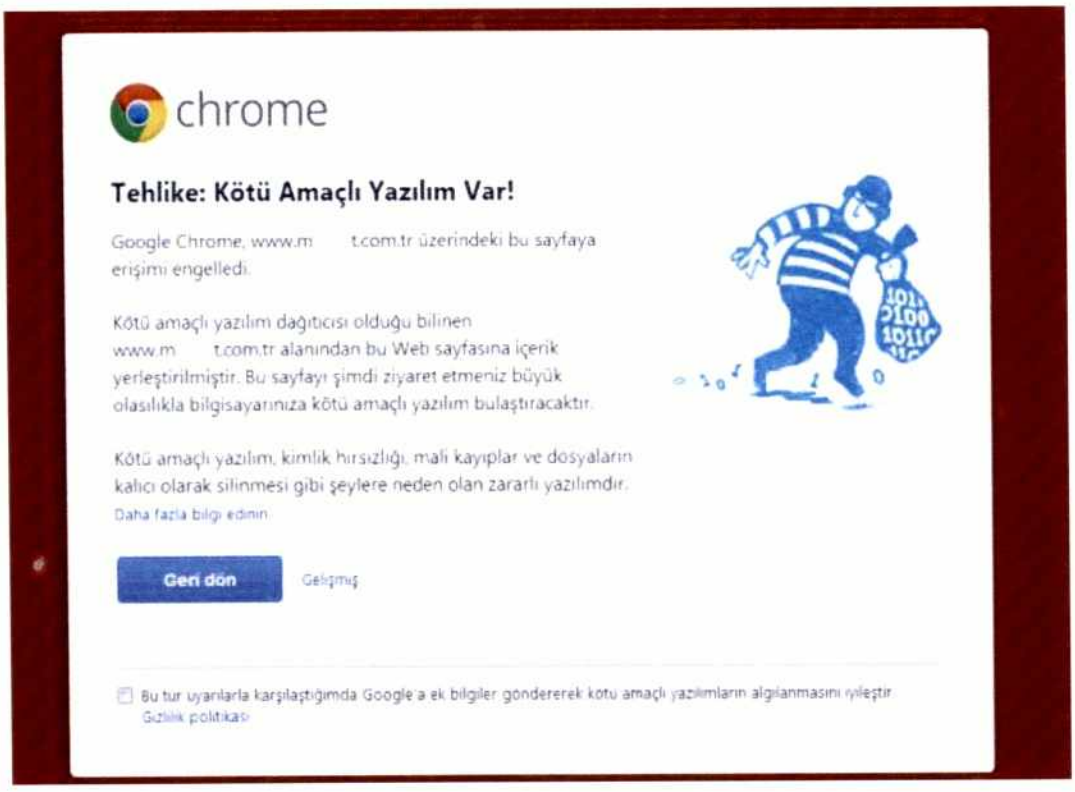
Bu tarz yazılımlara karşı mücadele edebilmek için;

- İşletim Sisteminin ve üzerinde kurulu olan yazılımların güncelleştirmelerinin zamanında yapılması ve daima güncel tutulmasının sağlanması gerekmektedir.
- Bilgisayar üzerinde, işletim sistemini koruyacak bir anti-virus yazılımı, anti-spyware yazılımı ve benzeri yazılımlar kurulması ve bunların güncelleştirmelerinin düzenli olarak yapılması tavsiye edilmektedir.
- Lider internet tarayıcılarının hepsinde açılan pop-up pencereleri engelleme özelliği bulunmaktadır. Bu özelliğin pasif olması durumunda aktif hale getirilmesi gerekmektedir.
- Gelen istenmeyen e-postaların (spam), posta sunucusuna istenmeyen posta olarak bildirilmesi ve bir daha ki gelişlerinde otomatik olarak istenmeyen posta olarak işaretlenmesinin sağlanması gerekmektedir.
- Gelen e-postalarda ve gezilen internet sitelerinde, güvenilmeyen hiç bir bağlantının tıklanmaması ve indirilmemesi gerekmektedir.
- Bilgisayara casus yazılım bulaşmış olsa dahi, bu yazılımın internete bilgi sızdırmasını zorlaştırmak için ağ üzerinde güvenlik duvarı

(firewall) yazılım kurulması tavsiye edilmektedir (F-Secure, 2005; Onguardonline, 2013; a.g.e.).

Bu çözümlere ek olarak, günümüzde lider internet tarayıcılar ve arama motorları, daha önceden zararlı içerik veya casus yazılım barındırdığı tespit edilmiş web sayfalarını kaydetmekte ve kullanıcılar bu sayfalara ulaşmak istedikleri takdirde onları uyarmaktadır (Blogspot, 2013).

Şekil 2. 1. Chrome İnternet Tarayıcısı, Zararlı Yazılım İçeren Web Sitesi Uyarısı



Kaynak: Technopat, 2013

2.4.7. Sahte linkler

Bu yöntem yemleme saldırılarında olduğu gibi kullanıcının sahte bir linke tıklamasını sağlamak üzerine kuruludur. Bu link bir e-posta ile gönderilebileceği gibi, sosyal paylaşım ağı üzerinde kullanıcının

tıklayabileceği bir link paylaşımı olarak da kullanılabilmektedir. Örneğin, yemleme saldırısında olduğu gibi bankadan gelecek e-posta yerine, kurbanın bir arkadaşının ya da üye olduğu grubun profilinde tıklayacağı ve bankaya aitmiş gibi gözüken bir link olabilmektedir Tıklanıldığı takdirde, bankanın kendi internet sitesi yerine, başka bir siteye gidebilmekte ve bankanın arayüzüne çok benzeyen bir arayüz ile kullanıcıdan kişisel bilgilerini talep edebilmektedir (Bilgigüvenliği, 2013b).

Sahte linkler daha çok yemleme yöntemiyle beraber kullanılmaktadır. Kullanıcıların bir linke tıklamadan önce o linkin doğruluğundan emin olmaları gerekmektedir. Eğer imkân varsa, linke tıklamak yerine, doğrudan adres çubuğuna yazılarak sayfaya ulaşılması gerekmektedir (Bilgigüvenliği, 2013b).

Bu durumda kullanıcılar linke ulaştıklarında, meşhur bir bankanın arayüzünü görürlerken, adres çubuğunda "www.examplebank.com" yerine "www.examplephishingbank.com" gibi bir farklı bir adres görüyorlarsa, bu fark ulaştıkları adresin sahte bir linkten geldiğini anlamalarına yardımcı olacaktır. Çözüm yöntemi olarak kullanıcıların bilinçlendirilmesi ve eğitilmesi, sahte link saldırılarından kurban olmalarının önüne geçecektir (Merwe vd., 2005; Gunter, 2004).

2.4.8. DNS yanıltma (Spoofing) saldırıları

Bu saldırı yönteminde, kurbanın bilindik ve güvenilir DNS sunucuları yerine, saldırganın DNS sunucusunu kullanması sağlanmaktadır. Böylelikle kurban örneğin www.example.com adresine ulaşmak istediğinde 192.0.43.10 IP adresi yerine, saldırganın sunucusunun IP adresine yönlendirilecek ve neredeyse hiç farkında olmadan, güvenilir banka sitesinde olduğunu zannederek, saldırganın sitesine her türlü kişisel bilgilerini verecektir (Dnscurve, 2013; IETF, 2013a; IETF, 2013b).

Kullanıcı bir internet sitesine ulaşmak istediği zaman (örnek: www.example.com), bilgisayar ilgili DNS sunucusuna bu sitenin IP adresini sorarak isteği o adrese göndermektedir (IETF, 2013a; IETF, 2013b).

DNS yanıltma saldırılarında ise saldırgan, kullanıcı yerine bu DNS sunucusunu hedef alarak, üzerinde kayıtlı olan adres bilgilerini değiştirmekte ve kendi sunucusuna yönlendirmektedir (Dnscurve, 2013). Bu saldırı karşısında, doğrudan hedef kendisi olmadığı için, kullanıcının bireysel olarak alabileceği pek fazla önlem bulunmamaktadır. Sunucu yöneticilerinin ilgili dokümanlarda belirtilen önlemleri almaları ve DNS sunucusu hizmeti veren yazılımları (BIND, Microsoft DNS Server vb.) güncel tutmaları gerekmektedir. Bunun yanı sıra, kullanıcıların bireysel olarak herhangi bir DNS sunucusunu kullanmamaları, internet servis sağlayıcıları tarafından önerilen veya bilindik ve güvendikleri DNS sunucuları kullanmaları gerekmektedir (Itnewsafrica, 2013).

Genel olarak savunma yöntemleri incelendiğinde insanların bilinçlenmesi gerektiği, sistemlerin ve yazılımların güncel olması gerektiği ön plana çıkmaktadır. Kimlik ihlali, saldırganın, sosyal ağdaki bir kullanıcı ile gerçek hayattaki bir oluşum eşleştirmesiyle olmaktadır (Techrepublic, 2013). Yapılan araştırmalara göre, sosyal paylaşım ağlarını kullanan kullanıcıların basit ve sözlük saldırıları kullanarak kolaylıkla bulunabilecek şifreler kullandıkları tespit edilmiştir (Bilgigüvenliği, 2013a).

Kullanıcıların şifrelerinin, uzun, büyük/küçük harf, sayı ve karakter karışımından oluşması tavsiye edilmektedir (howsecureismypassword, 2013; Microsoft, 2013).

Kullanıcıların, kullandıkları uygulamaların ve sosyal paylaşım ağlarının kullanıcı sözleşmelerini okumaları ve kişisel bilgilerine nasıl işlem yapıldığını incelemeleri gerekmektedir. Sosyal paylaşım ağları üzerinde paylaşılmış hiç bir bilgi artık özel değildir. Kurban, kişisel bilgilerini korumak adına, paylaşım

ayarlarını ne kadar özel sınırlamış olursa olsun, saldırganlar, kurbanın arkadaşları aracılığı ile bu bilgilere ulaşabilmektedirler (FBI, 2013). Örneğin Facebook, kendi sistemine yüklenmiş her türlü resim bilgi ve belgenin kullanım hakkının kendisinde olduğuna dair bir sözleşme kullanmaktadır (Facebook, 2013b). Bu gibi durumlarda, kullanıcıların bireysel olarak alacakları önlemler yetersiz kalmakta ve sunucu tarafında hizmet aldıkları kurumlar, kişisel bilgilerini para karşılığı 3. kişi ve/veya kuruluşlarla paylaşabilmektedirler. Bu gibi durumların önüne geçilebilmesi için ilgili mevzuatlarda, kişisel bilgilerin paylaşılmasını ve işlenmesini kısıtlayıcı maddeler eklenmiştir (TBMM, 2013a; TBMM, 2013b). Türkiye Cumhuriyeti Anayasası'nda şu ifadelere yer verilmiştir;

> "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" (TBMM, 2013c).

Türkiye'de son yıllarda, kişisel verilerin korunması ve güvenliğinin sağlanması ile ilgili hususlar öne çıkmaya başlamıştır. Anayasamızda belirtilen, kişisel verilerin korunması hususunun hukuksal bir önemi bulunmakla beraber, son yıllarda bu alanda akademik çalışmalarda artış gözlemlenmektedir (Küzeci, 2010).

Temel olarak bakıldığı zaman Kişisel verilere karşı üç farklı gruptan saldırırlar gelmektedir. Bu saldırılar;

- Bireyler
- Kurumlar veya kuruluşlar (şirketler, bankalar)
- Devletler

tarafından gerçekleştirilebilmektedir.

Bireysel anlamda bu saldırıların, saldırganın kendi egosunun tatmini, bir arkadaşından intikam alma ya da ufak çaplı maddi gelir sağlamak olabilir. Ancak, kurumlar, kuruluşlar ve devletler açısından düşündüğümüzde ise, büyük çaplı maddi gelir sağlama ve istihbarat amaçlı bilgiler toplamak olarak düşünülebilir. Bu durumda kişisel verilerin korunması ancak, Kanunlar ve Uluslararası sözleşmelerle garanti altına alınabilecektir (Küzeci, 2010).

3. SOSYAL PAYLAŞIM AĞLARINDA KİŞİSEL VERİLERİN KULLANIMI, PAYLAŞIMI, GİZLİLİK POLİTİKALARI VE İHLALLERİ

Bu bölümde bireylerin sosyal paylaşım ağları kullanım alışkanlıklarına, sosyal paylaşım ağlarındaki gizlilik politikalarına ve sosyal paylaşım ağlarında kişisel verilerin kullanım ihlallerine ilişkin örneklere değinilecektir.

Kişisel verilerin kullanımı; ilgili kanunlar ve kullanıcı sözleşmeleriyle belirlenir (Facebook, 2013b; Twitter, 2013b). Türkiye Cumhuriyetinde kişisel verilerin kullanımı ile ilgili kanun hazırlanmış, ancak henüz taslak olarak beklemektedir (TBMM, 2013b), ancak, Türkiye Cumhuriyeti Anayasası, kişisel verilere yönelik anayasal koruma sağlamıştır. Anayasada, "kişisel verilerin kullanımı kanunlarca düzenlenir" ibaresi yer almaktadır, buna göre taslak kanunda;

> "MADDE 5-
> (1) Kişisel verilerin;
> a) Hukuka ve dürüstlük kurallarına uygun olarak işlenmesi,
> b) Belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi,
> c) Toplandıkları amaçla bağlantılı, yeterli ve orantılı olması,
> ç) Doğru olması ve gerektiğinde güncellenmesi,
> d) İlgili kişilerin kimliklerini belirtecek biçimde ve kaydedildikleri veya yeniden işlenecekleri amaç için gerekli olan süre kadar muhafaza edilmesi zorunludur.
> (2) Kişisel veriler, ilgili mevzuatta yeniden işlenme amacına yönelik yeterli koruma tedbirleri getiren düzenlemenin bulunması veya kişisel verileri kontrol eden tarafından bu yönde gerekli tedbirlerin alınması şartıyla tarihî, istatistikî veya bilimsel amaçlarla yeniden işlenebilir veya birinci fıkranın (d) bendinde öngörülenden daha uzun bir süre saklanabilir" (TBMM, 2013c).

İbareleri yer almaktadır. Aynı şekilde TCK'nın "Kişisel Verilerin Kaydedilmesi" başlıklı 135. maddesi de kişisel verileri hukuka aykırı olarak kaydedenlerin ve işleyenlerin 6 aydan 3 yıla kadar hapis cezası ile cezalandırılmalarını hükmetmektedir (TBMM, 2013a).

3.1. Sosyal Paylaşım Ağlarında Kişisel Verilerin Kullanımına Örnekler

Bireyler sosyal paylaşım ağlarında genellikle;

-İsimleri
-Fotoğrafları
-Doğum tarihleri
-Okulları
-Yaşadıkları şehirleri
-İlişki durumları
-E-Posta adresleri
-Cep telefonu numaraları

gibi bilgileri paylaşmaktadırlar. Bireylerin büyük çoğunluğunun gerçek isimlerini sosyal ağlarda paylaştığı görülürken, yalnızca %20'sinin cep telefonu bilgilerini paylaştıkları görülmektedir (Pewinternet, 2013). Buradan bireylerin, yabancı kişilerin, doğrudan kendilerine ulaşabilecekleri bilgileri paylaşmak istemedikleri ve bir anlamda kendilerince kişisel bilgilerini korumaya çalıştıkları çıkarımı yapılabilir. Aşağıdaki tabloda, 17 yaşına kadar olan gençlerin, cinsiyet ve yaşlarına göre sosyal ağlarda gerçekleştirdikleri paylaşımlar görülebilmektedir (Pewinternet, 2013).

Tablo 3. 1. Sosyal Paylaşım Ağlarında Paylaşılan Kişisel Bilgilerin Yaş ve Cinsiyete Göre Dağılımı

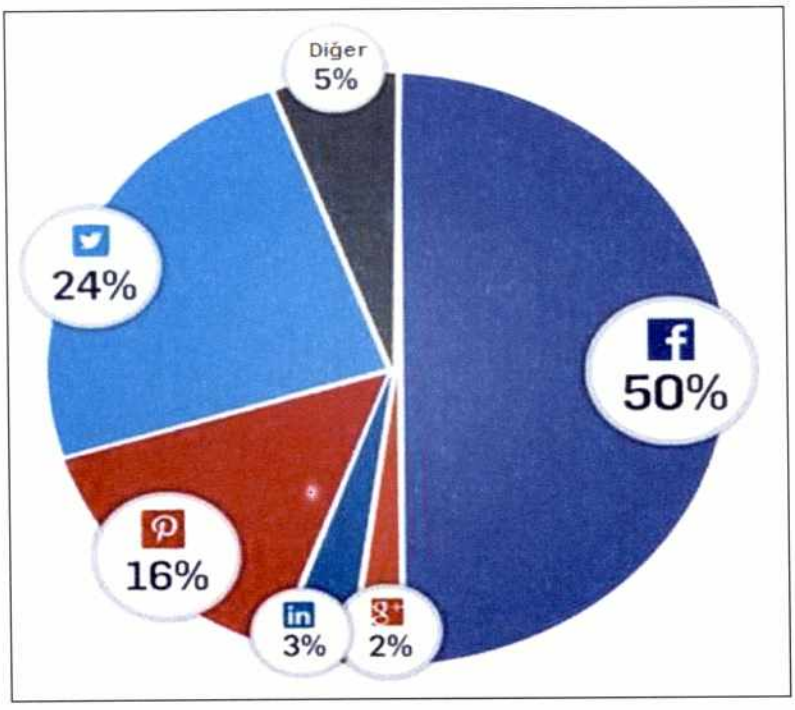
Paylaşılan Bilgi	Genç SPA Kullanıcıları (%)	Erkekler (%)	Kızlar (%)	12-13 Yaş Arası Gençler (%)	14-17 Yaş Arası Gençler (%)
Gerçek İsim	92	92	92	89	93
Kendi Fotoğrafı	91	89	94	82	94
Hobiler (Film, müzik, kitap vb)	84	84	85	81	85
Doğum Tarihi	82	81	83	79	83
Okul Adı	71	73	69	56	76
Yaşadığı Şehir	71	73	69	67	72
İlişki Durumu	62	62	61	50	66
E-posta Adresi	53	57	49	53	53
Kendisiyle İlgili Video	24	27	21	25	24
Cep Telefonu Numarası	20	26	14	11	23

Kaynak: Pewinternet, 2013

3.2. Sosyal Paylaşım Ağları Açısından İnternette İçerik Paylaşımı

Son yıllarda internet kullanım ve bilgi paylaşım şekli değişmektedir. Yeni dönem iletişimde sosyal paylaşım ağları üzerinden bilgi paylaşımı hızla gelişmektedir. Artık oluşan trafiğin en büyük kısmını sosyal paylaşım ağları oluşturmaktadır. Yapılan istatistikî bilgiler de bunu göstermektedir. Gigya adlı araştırma şirketinin yaptığı Temmuz 2013 istatistiklerine göre Facebook ve Twitter en çok içerik paylaşımının yapıldığı platformlar olarak dikkat çekmektedir (Marketingland, 2013).

Şekil 3. 1. Sosyal Paylaşım Ağlarında İçerik Paylaşımı (2013)



Kaynak: Marketingland, 2013

Facebook paylaşılan içeriğin %50'sini oluşturarak bu alandaki liderliğini sürdürürken Twitter ve yeni nesil içerik paylaşım ağlarından olan Pinterest bu alanda hızlı yükselişlerini sürdürmektedir.

İnternet ortamında içerik paylaşımı için paylaşım butonu sağlayan kuruluşlardan biri AddThis'dir. AddThis kullanıcılara beğendikleri haber veya içerikleri sosyal paylaşım ağları üzerinden paylaşma olanağı tanıyan 600.000'den fazla kullanıcıya sahip bir araçtır.

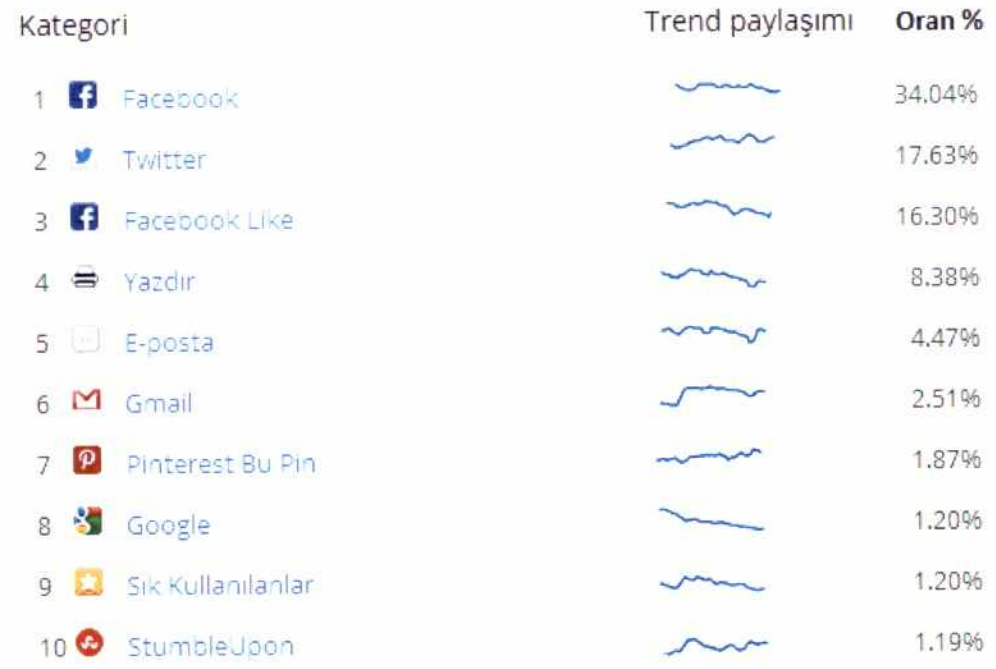
Şekil 3. 2. AddThis'in 2013 Verilerine Göre İçerik Paylaşımı

Kategori	Trend paylaşımı	**Oran %**
1 Sosyal ağ		57.83 %
2 Bloglama platformu		19.21 %
3 Tools		8.77 %
4 E-posta/IM hizmeti		8,08 %
5 Site bookmarking		4.52 %
6 Sosyal haber		1,50 %
7 Diğer		% 0.05
8 Alışveriş sitesi		% 0.05

Kaynak: AddThis, 2013

AddThis'in 2013 verilerine göre sosyal paylaşım ağları %57,83 ile en fazla içeriğin paylaşıldığı platformlar olarak dikkat çekerken, bloglar %19,21 ile ikinci sırada gelmektedir (AddThis, 2013).

Şekil 3. 3. AddThis'in 2013 Verilerine Göre Sosyal Paylaşım Ağlarında İçerik Paylaşımı



Kaynak: AddThis, 2013

Bu içeriklerin hangi sosyal paylaşım ağı üzerinden ne kadar paylaşıldığına bakıldığı zaman bu alanda da yine Facebook'un lider olduğu görülmektedir. "Şekil 3.3" 'te Facebook'taki içerik paylaşımı %34,04 ile ilk sırada yer alırken, Twitter üzerindeki içerik paylaşımının %17,63 ile ikinci sırada yer aldığı görülmektedir.

Facebook'ta paylaşılan içeriklerin ülkelere göre dağılımı incelendiğinde; ABD %22 ile ilk sırada yer alırken, Brezilya %7 ile ikinci ve Türkiye %6 ile üçüncü sırada bulunmaktadır. Mısır %5 ile dördüncü ve İtalya %4 ile beşinci sırada yer alarak ilk beş sırayı oluşturmaktadır.

Şekil 3. 4. AddThis'in 2013 Verilerine Göre Facebook Üzerinden Paylaşılan İçeriklerin Ülkelere Göre Dağılımı

Ülke	%
Amerika Birleşik Devletleri	22%
Brezilya	% 7
Türkiye	% 6
Mısır	% 5
İtalya	% 4
Fransa	% 3
Büyük Britanya	% 3
İspanya	% 3
Kanada	% 2
Hindistan	% 2
Pakistan	% 2
Meksika	% 2
Arjantin	% 2
Almanya	% 2
Yunanistan	% 2
Endonezya	% 2
Hollanda	% 1
Suudi Arabistan	% 1
Kolombiya	% 1
Vietnam	% 1

Kaynak: AddThis, 2013

Yine aynı şirketin 2013 verilerine göre Twitter'da içerik paylaşımı konusunda ABD %27 ile ilk sırada yer alırken, Büyük Britanya %5 ile ikinci, İspanya %5 ile üçüncü, Türkiye ise %4 ile altıncı sırada yer almaktadır.

Şekil 3. 5. 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: AddThis, 2013

3.3. Sosyal Paylaşım Ağlarının Gizlilik Politikaları

Sosyal paylaşım ağlarının hepsi olmasa da çoğunluğu kullanıcılarına ücretsiz hizmet vermekte iken Facebook ve LinkedIn gibi sosyal paylaşım ağları ise

bazı hizmetleri belli ücret karşılığında vermektedir. Facebook'un yakın geçmişte tanınmayan kişilere mesaj atmayı ücretli hale çevirmesi bunlara örnek olarak verilebilir.

Sosyal paylaşım ağlarının bir diğer gelir kaynağı ise reklam gelirleridir. 2000'lerden önce kurulan sosyal paylaşım ağlarının yeterli gelir elde edememeleri ve sonuç olarak da kapanmalarının başında o zaman bugünkü gibi geçerli olan bir reklam sektörünün henüz oturmaması gelmektedir. Bu bile sosyal paylaşım ağlarının ne kadar büyük bir reklam gelirine sahip olduğunu göstermek adına yeterli bir veridir.

Sosyal paylaşım ağlarının başka bir gelir kaynağı ve en tartışmalı olanı kullanıcılarının bazı bilgilerinin üçüncü kişilerle paylaşımı konusudur. Bu konuda çok fazla eleştiri olmasına rağmen sosyal paylaşım ağları buna devam etmektedir. Bunu yapma adına da kullanıcılarından "Gizlilik Politikası", "Kullanıcı Sözleşmesi" veya "Hizmet Şartları" adları altında çeşitli kullanım sözleşmeleri ile kendilerini garanti altına almaktadır. Bu konuda yapılan tartışmaların yoğunlaştığı bir diğer nokta ise kullanıcı bilgilerinin istihbarat teşkilatları veya hükümetlerle paylaşılması konusudur. Her ne kadar sosyal paylaşım ağları bunları inkâr etse de Facebook'un bölge yöneticisi Richard Allan'ın TBMM "İnternet Araştırma Komisyonu"na Haziran 2012'de "Özel durumlarda bilgileri gizli servislerle paylaşıyoruz" itirafı sosyal paylaşım ağlarının gerektiğinde bilgileri üçüncü kişilerle paylaştığının net bir itirafı gibidir (Gantep, 2013).

Genel anlamda bakıldığı zaman sosyal paylaşım ağları kullanıcılarının çoğunun sosyal paylaşım ağlarının hak ve sorumluluklar hakkında kullanıcılarına verdiği haklar ve sorumluluklardan habersiz olduğu görülmektedir. Zaten kullanıcılardan sayfalarca maddeleri okumayı, okunsa bile tamamını anlamayı beklemek çok da gerçekçi bir yaklaşım değildir. Google, Facebook ve Twitter'ın en geniş kullanıcı kitlelerine sahip olduğu

düşünüldüğünde bu şirketlerin gizlilik politikalarını incelemekte fayda bulunmaktadır.

Google+, Orkut ve Youtube, Google'ın sosyal paylaşım ağlarıdır. Ancak Google kullanıcı hesaplarını tek çatı altında topladığından kullanıcılarına da tek gizlilik politikası ile şartları belirtmektedir. Google söz konusu politika ilkelerini açıklarken pek çok alanda kullanıcılarına hizmet verdiğini ve daha iyi hizmet vermek amacıyla kullanıcı bilgilerini kullanabileceğini belirterek kullanıcının hangi bilgilerinin kullanıldığının bilinmesi amacıyla bu politikayı düzenlediklerini belirtmektedir (Google, 2013a).

Google "Bilgi Toplama" başlığı altında kullanıcılardan iki şekilde bilgi toplandığını belirtmektedir. Birinci bilgi toplama şekli Google'ın herhangi bir hizmetini kullanırken profil oluşturmak için girilen ad, soyad, e-posta ve kişisel fotoğraf gibi bilgilerin toplanması durumudur. Bu bilgiler gerekli durumlarda üçüncü kişilerle paylaşılabilmektedir (Google, 2013a).

İkinci bilgi toplama şekli ile Google hizmetini kullanan kullanıcıların girdikleri sitelerde etkileşimli reklamlarla etkileşimlerde bulunmaları durumunda cihaz bilgileri (donanım türü, işletim sistemi vb.), konum bilgileri, veri önbelleği, çerez ve tanımlayıcılar gibi bilgiler yine Google tarafından toplanabilmektedir (Google, 2013a).

Toplanan bilgiler başlığı altında bilgilerin sunulan hizmetleri iyileştirmek, yeni hizmetler geliştirmek, istatistiksel veya reklam amaçlı olarak kullanılabildiği belirtilmektedir. Çerezler aracılığıyla toplanan bilgiler verilen hizmeti geliştirmek veya istatistiksel açıdan sonuç çıkarmak ve reklam amacıyla kullanılabilmektedir. Bu verilerin işlenmesi sonucunda da kullanıcıya özel reklamların görülmesi amaçlanmaktadır. Ayrıca kişisel bilgilerin bunlara benzer amaçlar dışında kullanılması durumunda öncelikle kullanıcıdan izin alınacağı belirtilmektedir. Kişisel bilgilerin farklı ülkelerdeki sunucularda

tutulduğu ve gerektiğinde farklı ülkelerde işlenebileceği iletilmektedir (Google, 2013a).

"Şeffaflık ve Seçim" başlığı altında Google, kullanıcılarına bilgilerini kullanma açısından bazı kısıtlamaları getirme hakkı tanımaktadır. Örneğin profil bilgilerinin görünürlüğü kısıtlanabilir, Google reklamcılık hizmetleri devre dışı bırakılabilir, tarayıcı bilgilerine ulaşma hakkı kısıtlanabilir ve bunlara benzer işlemler yapılarak Google'ın istenmeyen bilgilere ulaşması önlenebilmektedir. Ancak bu Google'ın hiçbir bilgiye ulaşamayacağı anlamına gelmemektedir (Google, 2013a).

"Kişisel Bilgilere Erişme ve Bunları Kullanma" başlığı altında Google kullanıcıların bilgilerini güncelleme imkânlarının olduğunu belirtirken aynı zamanda kullanıcı hesaplarını silme olanakları olduğunu, ancak kullanıcı hesabını silse de kullanıcı verilerinin bir süre daha sistemde kayıtlı tutulacağını belirtmektedir (Google, 2013a).

"Diğer Kişilerle Paylaşılan Bilgiler" başlığı altında Google bazı bilgilerin üçüncü kişilerle paylaşılabileceğini net olarak ifade etmektedir. İzin alınması durumunda, alan adı yöneticisine bağlı olan hizmetlerin kullanılması, bilgilerin harici kuruluşlarla paylaşılması durumu (verilerin işlenmesi amacıyla) veya yasal nedenlerden dolayı bilgilerin üçüncü kişilerle paylaşılabileceği belirtilmektedir. Bilgi güvenliğinin sağlanması amacıyla SSL'in kullanılmakta olduğu, hesap erişimi açısından iki adımlı doğrulama ve sistemlere erişimi engellemek açısından gerekli tüm fiziki güvenlik tedbirlerinin alınmakta olduğu belirtilmektedir (Google, 2013a).

Yukarıdaki veriler ışığında Google'ın kullanıcıların bazı bilgilerini üçüncü kişilerle paylaşabildiği ortaya çıkmaktadır. Üçüncü kişiler olarak belirtilen kuruluşların bazen reklam amaçlı şirketler, bazen hükümetler ve bazen de istihbarat teşkilatı olabileceği sonucuna varılmaktadır (Google, 2013a).

Facebook yine Google gibi kullanıcı bilgilerini gerektiğinde üçüncü kişilerle paylaşmaktadır. Facebook kullanıcı hesabını silse bile belli bir süre kullanıcı bilgilerini tutmakta ve bazı paylaşımlarını ise hiç silmemektedir. Bunların başında arkadaşları ile yapılan paylaşımlar ve bu paylaşımlara arkadaşlarının da bir yorum veya beğenide bulunması gibi bir durumda bu paylaşım bireye ait olmaktan çıkıp bir ortak paylaşım olarak değerlendirildiğinden silinmemektedir (Facebook, 2013a).

Facebook kullanıcıların paylaştığı bilgiler üzerinde çok geniş yetki hakkını kullanıcı sözleşmesi ile garanti altına almaktadır. "Aldığımız Bilgileri Nasıl Kullanıyoruz" başlığı altında Facebook kullanıcı bilgilerini ortakları, sitede reklam yayınlayan reklam veren şirketlerle, sistem üzerinde oyunlarla veya Facebook'u kullanan girişimcilerle paylaşabileceğini net ifadelerle belirtmektedir. Bu başlık altında Facebook hizmet geliştirme, reklam kişileştirme veya analiz ve test amacı gibi pek çok nedenden dolayı kullanıcı verilerini kullanabileceğini ifade etmektedir (Facebook, 2013a).

Facebook kullanıcı bilgilerini gerektiğinde hükümetlerle paylaşabilmektedir. Ancak hangi bilgilerin kimlerle paylaşılabildiğini veya hangilerinin kiminle paylaşılmadığını belirtmediği gibi herhangi bir kişi veya kuruluşla paylaştığı bilgiler hakkında kullanıcıyı da bilgilendirme gereği duymamaktadır (Facebook, 2013f).

Facebook kullanıcıların paylaştıkları fotoğraf veya video gibi paylaşımları üzerinden kullanıcı tarafından paylaşılabilmek üzere telif hakkı kazandığını "İçeriklerinizi ve Bilgilerinizi Paylaşma" başlığı altında açıklamaktadır. Yani Facebook herhangi bir kullanıcının bir video veya fotoğrafı alt lisans ile satma hakkı ile üçüncü kişilerle paylaşabilir. Kullanıcı bu hakkı bu sözleşme ile Facebook'a vermektedir (Facebook, 2013a).

Facebook'un mobil uygulamaları kullanıcıların rehber veya mesaj gibi özel bilgilerine ulaşabilmektedir. Facebook bunu da mobil uygulama kullanıcı

sözleşmesi ile garanti altına almaktadır. Bu tür uygulamaları kuran kullanıcı bunları peşinen kabullenmiş sayılmaktadır (Facebook, 2013a).

Twitter da Facebook ve Google gibi kullanıcı haklarını üçüncü kişilerle paylaşabilmektedir. Twitter da Facebook gibi kullanıcıların attığı Tweet'leri kullanıcı silse bile sistemden silmemekte ve bu Tweet'leri gerektiğinde üçüncü kişilerle paylaşabilmektedir.

Twitter da mobil uygulamalar yoluyla kullanıcının adres defterine ulaşabilmekte ve adres defterinde kayıtlı kişilere kişinin Twitter hesabı hakkında bilgilendirme yapabilmektedir. Bu uygulamalar ayrıca kullanıcıların lokasyon bilgileri gibi bilgileri de kayıt altına almaktadır.

Twitter geçmişe dönük iki haftalık tweet kaydı tutmaktadır. Daha önce paylaşılan Tweet'ler ise kullanıcı tarafından silindi olarak bilinmekle beraber sunucularda tutulmakta ve gerektiğinde üçüncü kişilerle paylaşılabilmektedir (Twitter, 2013a).

Twitter'ın kullandığı bir diğer bilgi kullanıcılara ait çerezlerdir. Bu bilgiler yine veri olarak değerlendirilmekte ve bu veriler üzerinde çeşitli analizler yapılabilmektedir. Her ne kadar Twitter bu verileri hizmetlerini geliştirmek için kullandığını söylese de aslında başka amaçlarla da kullanılabilmektedir (Twitter, 2013a).

Herhangi bir nedenden dolayı kullanıcı bir şikâyeti için merci aradığında sosyal paylaşım ağları adres olarak ABD mahkemelerini adres göstermektedir. Bu kullanıcılar için çok zor bir durumdur. Çünkü ABD'de dava açmak ve bu davayı kazanmak için yapılacak masraflar kullanıcılar için çok masraflı harcamalar olduğundan çoğu kullanıcı bu yola başvurmaktan vazgeçmektedir.

Yapılan bir çalışmada sosyal paylaşım ağları aşağıda belirtildiği gibi güvenlik özelliklerine göre karşılaştırılmıştır. Sosyal paylaşım ağları gizlilik ayarları, fotoğraf yükleme, yaş sınırı, 3. parti uygulamalar, grup oluşturma, arkadaşlıklar kurma vb. açısından karşılaştırılmaktadır. Tablo 3.2'de bu karşılaştırmaların detayları görülmektedir. Kullanıcı yaş sınırının 13-14 'ten başlaması ve reşit olmayan kullanıcıların oranının %30'larda olması çok dikkat çekici verilerdir (Yavanoğlu ve Sağıroğlu, 2012 s.15-27).

Tablo 3. 2. Sosyal Paylaşım Ağlarının Güvenlik Özelliklerine Göre Karşılaştırılması

	Facebook	MySpace	Bebo	Friendster	Hi5	Orkut	PerfSpot	Yahoo! 360	Zorpia	Netlog
Yaş Sınırı	13	14	13	16	13	18	13	18	16	13
Reşit Olmayan Kullanıcı yüzdesi	36	33	54	3	24	4	32	16	15	31
Profil Editörü (WYSIWYG)	Var	Var	-	Var	Var	-	Var	Var	Var	Var
Kullanıcı Bağıl Kod (HTML or CSS)	-	Var	-	Var	-	-	-	-	-	-
Kişisel Bağlantı Kısayolu	-	Var	Var	Var	Var	-	-	Var	Var	Var
Fotoğraf Yükleme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Yorum Yazma	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Arkadaşlıklar	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Günlük Hazırlama	-	Var	Var	Var	Var	-	Var	Var	Var	Var
3.Parti Uygulamalar	Var	Var	Var	Var	Var	Var	Var	-	-	-
Gizlilik Ayarları	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Kullanıcı Engelleme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Spam Bildirme	Var	Var	Var	Var	Var	Var	-	-	Var	
Kötüye Kullanım bildirme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Güvenlik Önerileri	Var	Var	Var	-	Var	Var	Var	Var	-	-
Kişileri Etiketleme	Var	Var	Var	Var	Var	-	-	-	Var	Var
Gruplar	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Grup Oluşturma	Var	Var	Var	-	Var	Var	Var	Var	Var	Var
Tartışma Forumu	Var	Var	-	Var	-	-	-	-	Var	-
E-Posta Gönderme	Var	Var	Var	-	Var	Var	Var	Var	Var	Var
Fotoğraf Paylaşma	Var	Var	Var	-	Var	-	Var	-	Var	-
Kişisel Video yükleme	Var	Var	Var	Var	-	Var	-	-	Var	Var
İsme Göre Arama	Var	Var	Var	-	-	-	Var	-	Var	Var
E-Posta Adresine göre Arama	Var	Var	Var	Var	Var	-	-	-	Var	-
Okul Adına Göre Arama	Var	Var	-	Var	-	-	-	-	Var	-
Şehir Adına Göre Arama	-	Var	-	Var	Var	-	Var	-	Var	Var
İlgili Alanlarına Göre Arama	Var	Var	-	Var	-	-	-	-	Var	-
İstenilen Kelimelere Göre arama	-	Var	-	Var	Var	Var	-	Var	Var	Var
Üye Olmadan Arama Yapma	-	Var	-	-	-	-	Var	-	Var	-

Kaynak: Yavanoğlu ve Sağıroğlu, 2012 s.15-27

Genel anlamda sosyal paylaşım ağlarının gizlilik politikalarının karşılaştırılması durumunda hemen hepsinin kullanıcı bilgilerini üçüncü kişilerle paylaşabildiği, çoğunun kullanıcı profilleri üzerinden özel reklam profili oluşturduğu ve hiçbirinin yerel mahkemeleri kabul etmediği ABD veya AB mahkemelerinde dava açılmasına izin verdiği görülmektedir. Bazı sosyal paylaşım ağlarının kullanıcının hesabını silmesi durumunda belli bir süre daha bilgilerini tuttuğu, bazılarınınsa hiç silmediği görülmektedir. Tablo 3.3'de sosyal paylaşım ağlarının gizlilik politikalarının karşılaştırılmasının detayları görülmektedir (Yavanoğlu ve Sağıroğlu, 2012).

Tablo 3. 3. Sosyal Paylaşım Ağlarının Gizlilik Politikalarının Karşılaştırılması

	Facebook	Twitter	Myspace	Yonja	Reunited Friends	Linked-in	Friendster	Buzz	Blogger	Bebo	Hi5	Perfspot	Zorbia	Netlog	Badoo
Özel Bilgilerin 3. Kişilerce Paylaşımı	K	K	K	K	K	K	K	K	K	K	K	K	H	K	H
Kişisel Bilgilerden Özel Reklam Profil Oluşturma	E	-	E	E	E	E	E	E	-	E	E	E	E	E	E
Arama Motorlarına Tarama Hakkı	K	E	-	-	-	E	E	-	-	-	-	-	-	-	-
Kanunen Mahkemelere Destek Ulusal/Uluslararası	ABD	-	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	-	AB	AB
Profil Öğeleri Gizleme Desteği	E	-	E	E	E	E	E	E	E	E	E	E	-	E	E
Hesap Pasifleştirme	E	-	-	H	-	-	-	-	-	-	-	-	-	-	-
Hesap Silme	E	-	-	E	E	E	-	-	E	E	-	-	-	E	E
Silinen Hesap Bilgi Tutma Süres	90 gün	-	-	-	1 Yıl	-	-	-	-	-	-	-	-	6 Ay	-
Bilgilerin Tutulduğu Ülke	ABD	ABD	ABD	ABD	UK	ABD	ABD	ABD	ABD	ABD	ABD	ABD	Çin	AB	Güney Kıbrıs
Güvenli Sunucu Desteği	E	-	-	E	E	E	E	E	E	E	E	E	E	-	E
IP Tabanlı Loglama	E	E	E	-	-	E	E	-	-	-	E	E	E	-	E
Çerez Tabanlı Denetim	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Anonim İstatistik Toplama	-	-	E	-	-	E	-	-	-	E	E	E	-	E	-
Anadilde Kural Yayınlama	H	H	E	H	H	H	H	E	E	H	H	H	H	E	E

K:Kısıtlı, E: Evet, H: Hayır, ABD: Amerika Birleşik Devletleri, UK: Birleşik Krallık, AB:Avrupa Birliği Üyesi Ülke

Kaynak: Yavanoğlu ve Sağıroğlu, 2012

Genel anlamda bakıldığı zaman bütün sosyal paylaşım ağları kullanıcı bilgilerini işlemekte, analiz etmekte, gerektiğinde reklam kuruluşları veya farklı şirketlerle paylaşabilmektedir. Çoğu inkâr etse de gerektiğinde kullanıcı bilgilerini hükümetlerle veya istihbarat teşkilatları ile de paylaşabilmektedir. Bunun yanında çoğu kullanıcının bilmediği veya farkında olmadığı pek çok bilgi kayıt altına alınmakta ve kullanıcı hesabını silse bile kayıt altında tutulmaya devam etmektedir.

3.4. Sosyal Paylaşım Ağlarında Kişisel Verilerin Kullanım İhlalleri Örnekleri

Geçmişten günümüze kişisel verilerin kullanımları hususunda pek çok ihlal yaşanmıştır. Bunlardan bazıları aşağıda listelenmiştir;

-PATH: PATH uygulaması, kullanıcıların izinleri olmaksızın rehberlerindeki kişilerin listesini kendi sunucularına göndermiş ve ABD mahkemelerince cezalandırılmıştır. Bu olaydan sonra IOS işletim sistemlerinde, bir uygulama herhangi bir yetkiyi almak istediğinde kullanıcı onayına sunma zorunluluğu getirilmiştir (Donanımhaber, 2013).

-Phorm: 2012 yılı içerisinde, TTNET A.Ş.'nin'in kişisel verilerin işlenmesine ilişkin olarak Gezinti.com hizmeti aracılığıyla abonelerden/kullanıcılardan alınan onay sürecinde abonelerin/kullanıcıların kişisel bilgilerinin hangi kapsamda ve hangi süre ile işleneceğine ilişkin gerekli açıklamaları yapmayarak ve aboneleri/kullanıcıları eksik bilgilendirerek Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin "Şeffaflık ve bilgilendirme" başlıklı 6'ncı maddesini, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin "Telekomünikasyonun Gizliliği" başlıklı 8'inci maddesini ve aynı yönetmeliğin "İzin ve Süre" başlıklı 9'uncu maddesi ve ilgili diğer mevzuat hükümleri kapsamında ihlal ettiği değerlendirilen TTNET A.Ş. hakkında BTK,

soruşturma başlatmıştır.(BTK, 2013b). Soruşturma sonucunda, TTNet A.Ş. hakkında, 2011 yılı net satışlarının (3.150.975.726,02) %0,05 (onbinde beş) i oranında idari para cezası uygulanması hususuna karar verilmiştir (BTK, 2013c). Phorm örneği doğrudan sosyal paylaşım siteleri ile ilgili bir örnek olmamakla birlikte, kişisel verilerin gizliliğinin sağlanması konusunda alınmış Kurul Kararları bulunduğundan tezde yer verilmesi uygun bulunmuştur.

-RSA: Mart 2011 yılında saldırganlar iki çalışana yemleme postası göndererek çalışanlardan yalnızca birinin e-postadaki linke tıklaması ile beraber casus yazılımın sisteme dahil olmasını sağlayarak RSA güvenlik anahtarını nasıl kıracaklarını öğrenmişlerdir (FBI, 2013).

-2010 Dünya Kupası: 2010 yılında saldırganlar rastgele istenmeyen postalar göndererek, insanlara ücretsiz bilet kazandıklarını söylemiş ve kişisel bilgileri çalmayı hedeflemişlerdir (FBI, 2013).

-Usama Bin Ladin: Usama Bin Ladin'in öldürülmesinden sonra, yakalama videosu olduğu idda edilen bir video Facebook' a yüklenmiştir. Kullanıcılar bu videoyu izlemek istediklerinde, bir java script kodunun adres çubuğuna kopyalanarak çalıştırılması talep edilmiş, bunu yapan kullanıcıların Facebook hesaplarının tüm kontrolü saldırganların eline geçmiştir (FBI, 2013).

4. SOSYAL PAYLAŞIM AĞLARINDA KİŞİSEL VERİLERİN GÜVENLİĞİ

Bu bölümde, sosyal paylaşım ağlarında güvenlik zafiyetlerinden ve alınması gereken önlemlerden, kişisel veriler ile ilgili hukuki düzenlemelerden ve bu düzenlemelerin diğer ülkeler ile kıyaslamasından bahsedilecektir.

4.1. Sosyal Paylaşım Ağlarında Güvenlik Zafiyeti Oluşturabilecek Hususlar

Şirketler, müşterileri ile iletişim kurmak, onların ihtiyaçlarını belirlemek ve bu ihtiyaçlara uygun çözümler üretebilmek için her geçen gün sosyal paylaşım ağlarını daha fazla kullanmaktadırlar. Ancak şirketler için sosyal paylaşım ağları, paylaşmak ve başkalarının paylaşımlarını beğenmenin çok daha ötesinde yer almakta ve bu durum, şirketlerin imajı için oldukça büyük riskler yaratabilmektedir (Networkworld, 2013a).

Siber suçlular, kişilerin sosyal paylaşım ağları üzerinde kurdukları profilleri aracılığı ile kişisel bilgilerini çalabilirler ve bu bilgilere dayanarak, kişiye özel saldırı yöntemleri ile saldırıya geçebilirler. Örneğin, kurbanın sosyal paylaşım ağları sayfasından öğrendiği bilgiler ile saldırgan, bir bankadan aradığını, kişinin son gittiği yerleri, işini vb. bilgileri teyit amaçlı karşı tarafa söyleyerek güven kazanabilir, sonrasında banka hesap bilgilerini isteyebilir (Sophos Social Networking Security Thread, 2013a; Symantec Internet Security Thread Report, 2013).

Sosyal paylaşım ağlarında herkes arkadaş olarak eklenebilmektedir. Ancak, arkadaş tanımına baktığımızda bu herhangi biri olabilir. Bireyler, yalnızca bir defa tanıştıkları veya hiç tanışmadıkları kişileri arkadaş olarak sayfalarına ekleyebilmektedir. Sosyal paylaşım ağları arkadaş olarak eklenen kişilere, bireyin paylaştığı her türlü bilgiyi göstermektedir. Bunlara fotoğraflar, durum güncelleştirmeleri, grup üyelikleri, yorumları da dahildir. Ayrıca bu paylaşımlar sadece kendi arkadaş listesi ile kalmamaktadır. Örneğin

facebook, bireylerin, arkadaşlarının arkadaşlarını da görüntülemesine izin vermektedir. Bu da hiç tanımadığınız kimselerin sizin kişisel paylaşımlarınızı görmesi anlamına gelmektedir.

Örneğin, facebookta aşağıdakilere benzer iletiler paylaşılmaktadır.

-Yaşasın yeni bir iş teklifi aldım :))
-Yağmurdan bıktım usandım artık, biraz güneş açsın.
-Antalya'yı iple çekiyorum, haftaya kumsallardayım :)

Bu paylaşımlar zararsız görünse de birey, paylaşımı ile tüm arkadaş çevresine ve onun arkadaşlarına, gelecek hafta evinde olmayacağını duyurmuş, her ne kadar evde bir alarm sistemi bulunsa bile, evine kötü niyetli kişileri açık bir şekilde davet etmiştir. Herhangi bir hırsızlık ve alarm çalması durumunda, bireyin Antalya'dan kalkıp, evine ulaşması saatler alacaktır ve evdeki değerli eşyaları çoktan çalınmış olacaktır.

Ayrıca, sosyal paylaşım ağları üzerinde pek çok istenmeyen paylaşım da gezinebilmektedir. Örneğin bir dönem Facebook üzerinde yaygınlaşan "Benim hakkımda bilmedikleriniz" uygulaması ile bireylerin kendilerine sorulan soruları cevaplaması ve uygulamayı arkadaş listelerine göndererek, onların da cevap vermesi sağlanmıştır. Böylece herkes birbiri hakkında hiç bilmediği farklı şeyler öğrenmiştir. Bu sorular, "En utanç verici anınız, ilk okulunuzun adı, en sevdiğiniz hayvanınızın adı" gibi masum görünüşlü sorulardan oluşmuştur.

İnternette herhangi bir siteden hesap yaratırken, site size şifrenizi unutmanız durumunda hesabınıza ulaşabilmeniz için gizli soru belirlemenizi istemektedir. Genel olarak önceden kayıtlı gizli soruların bazıları şunlar olabilmektedir;

-İlk okul öğretmeninizin adı nedir?
-İlk okulunuzun adı nedir?
-İlk evcil hayvanınızın adı nedir?
-Doğduğunuz şehir neresidir?

Bu sorularla, Facebook üzerindeki uygulamanın sorduğu sorular kıyaslandığında, benzerlik gösterdiği dikkat çekmektedir. Bu uygulamayı kullanan birisinin arkadaş listesindeki herhangi biri, kişinin posta hesabına gizli soruyu cevaplayarak erişim sağlayabilir. Bireyin arkadaşlarının yanı sıra, uygulama geliştiricisi kişinin de bu bilgileri toplayıp kaydetmediğinden emin olmak mümkün olmayabilir. Bu durumda birey, hiç tanımadığı bir başka kişi ile kişisel bilgilerini gönüllü olarak paylaşmış olacaktır (Dinerman, 2011).

Sosyal paylaşım ağları ve internet üzerindeki bir başka yaygın tehdit de kısaltılmış web adresleridir. Kısaltılmış web adreslerinde asıl amaç, çok uzun web sitesi adreslerinin yerine bir kaç karakterden oluşan kısa web adresleri üretmek ve bunları diğer kişilerle paylaşırken kolaylık sağlamaktır (Google, 2013b). Ancak, bu üretim esnasında, yeni oluşturulan adreslerin isimlerinden, asıl hedefin anlaşılması mümkün olmamaktadır. Sosyal paylaşım ağları üzerinden paylaşılan bu tarz kısaltılmış adreslerin, kimlik hırsızlığına yönelik olarak herhangi bir siteye, virüs içerikli sayfalara yönlendirme ihtimali bulunmaktadır (Dinerman, 2011).

4.2. Sosyal Paylaşım Ağlarında Alınması Gereken Güvenlik Önlemleri

Sosyal paylaşım ağları kişisel bilgiler açısından tehdit yaratmasına karşılık, kullanıcılarına eğlenceli ve güzel zaman geçirtmektedirler. Kullanıcılardan kişisel verilerinin güvenlikleri için, Facebook, Twitter ve benzeri Sosyal paylaşım ağları kullanmalarını bırakmalarını talep etmek doğru olmayacaktır, ancak, bazı önlemler alınması akıllıca olacaktır;

-Kullanıcıların, kullandıkları sosyal paylaşım ağlarının gizlilik ayarlarını gözden geçirmesi ve kendi ihtiyaçlarına göre belirlemesi,

-Arkadaş listesi oluşturulurken herkesin arkadaş olarak eklenmesindense, gerçekten tanınan insanların eklenmesi,

-Kişisel sayfaların, arkadaş listesi dışında kalanlar için kısıtlanmış olarak yayınlanması,

-Her türlü ön tanımlı ayarın iptal edilip, tek tek gözden geçirilerek açılması,

-Durum güncelleştirmelerinde paylaşılanlara dikkat edilmesi,

-Sosyal paylaşım ağları üzerindeki uygulamalarda cevaplanılan sorulara şüphe ile yaklaşılması,

-Kısaltılmış adreslere tıklanılırken, adresin güvenilirliğinin kontrol edilmesi tavsiye edilmektedir (Networkworld, 2013b; a.g.e.).

Temel olarak;

-Bir teklif, doğru olamayacak kadar iyiyse, muhtemelen altında yatan bir şey vardır.

-E-posta ve internet sitelerinde yazan her şeye inanılmaması gerekmektedir.

-Riskli görünen adreslere tıklanılmamalıdır.

-Kişisel bilgilerin asla e-posta veya internet sitesinde yayınlanmaması gerekmektedir.

-Eğer bir paylaşımın ya da e-postanın doğruluğundan şüphe duyulursa, göndericisi ile başka bir kanal üzerinden iletişim kurularak, doğrulanması iyi olacaktır.

-Kişisel bilgi talep eden telefon çağrıları, e-postalar ve uygulamalardan kaçınılması gerekmektedir (Sophos Social Networking Security Threads, 2013b; a.g.e.).

4.3. Kişisel Verilerin Korunmasına İlişkin Hukuki Düzenlemeler

"Kişisel verilerin korunmasına yönelik, Birleşmiş Milletler, Avrupa Konseyi, OECD ve APEC olmak üzere, pek çok devletlerarası kuruluş önemli çalışmalar yürütmüş ve kişisel verilerin korunması konusunda çerçeve niteliğinde belgeler hazırlamışlardır. Tablo 4.1'de görüleceği üzere, bu çalışmalar pek çok ülke için yol gösterici oldukları gibi aynı zamanda ülkeler arası veri transferini kolaylaştıran bir uyum sağlanmasına da ön ayak olmuşlardır" (Kalkınma Bakanlığı, 2013).

Tablo 4.1. Devletlerarası Kuruluşların Kişisel Verilerin Korunmasına Yönelik Çalışmaları

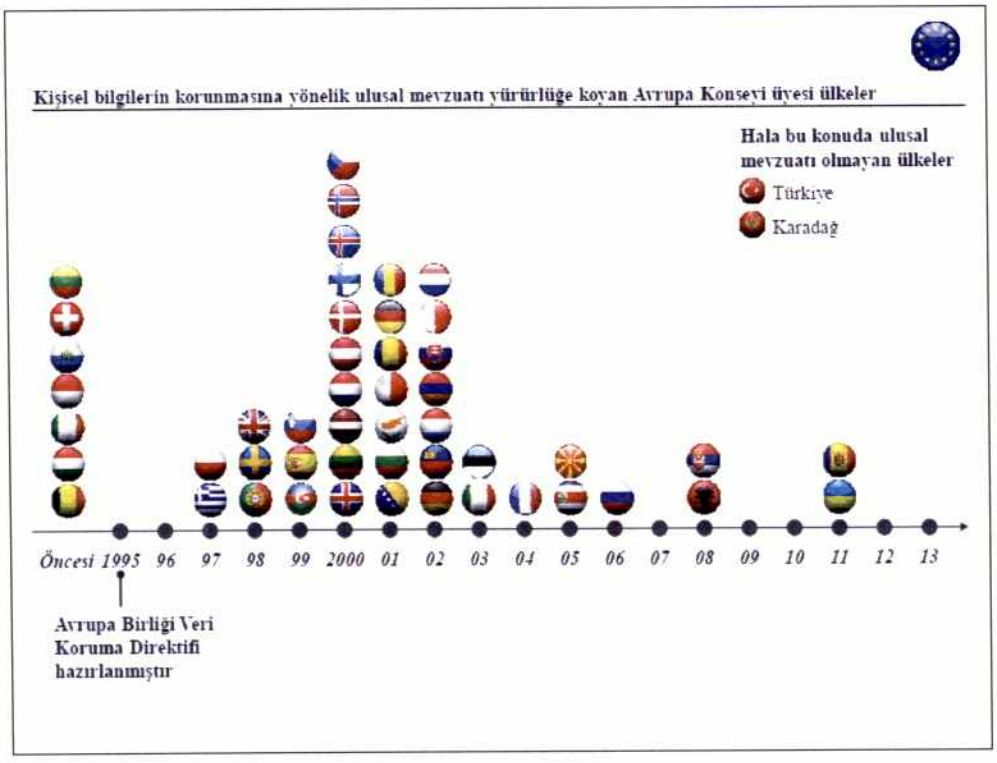
Devletlerarası Kuruluş	Başlıca Çalışmaları
Birleşmiş Milletler	• Birleşmiş Milletler tarafından 1948'de kabul edilen İnsan Hakları Bildirgesi aile hayatı, ev ve iletişim mahremiyetini temel hak sayarak güvence altına almıştır. • 1990'daki Çocuk Hakları Bildirgesi de çocukların mahremiyetini güvence altına almıştır. • 1990'da bilgisayarlardaki kişisel veri dosyaları ile ilgili Rehber İlkeler, bilişim dünyasında veri koruma anlamında bazı temel ilkeleri belirlemiştir.
Avrupa Konseyi	• 1950'de Avrupa İnsan Hakları Bildirgesi mahremiyetin korunmasını bir temel hak olarak kabul etmiştir. • Elektronik veri tabanlarının yaygınlaşması sonucunda 1973'teki bildirge ile bireylerin korunma altına alınmasına yönelik adım atılmıştır. • 1981'de "Kişisel Verilerin Otomatik Olarak İşlenmesi Sırasında Gerçek Kişilerin Korunmasına İlişkin Sözleşme" ilk uluslararası bağlayıcılığı olan belge olarak ortaya konmuş ve veri koruma ile sınır ötesi veri transferi konusunda temel ilkeler belirlenmiştir.
OECD	• 1969'dan itibaren çalışma grupları mevcuttur. • 1980'de sınır ötesi kişisel veri transferi ve bireylerin mahremiyet ve haklarının korunması konusunda rehber ilkeler yayımlamıştır. Söz konusu belgenin güncellenmesi için çalışmalar yapılmaktadır.
APEC	• Belli veri koruma ilkeleri çerçevesinde APEC Mahremiyet Çerçevesi ile 2004'te üye ülkeler arası uyum artırılmaya çalışılmıştır. • 2007'deki APEC Data Protection Pathfinder ile APEC üyesi ülkeler arasında kişisel veri transferi konusunda bir sistem kurulmuştur. • 2010'daki APEC Cross-Border Privacy Enforcement Arrangement ile birlikte ulusal kurumlar arası işbirliğinin artırılması hedeflenmiştir. • 2012'deki APEC Cross-Border Privacy Rules System ile "Safe Harbor" uygulamasına benzer, gönüllü bir sertifikasyon sistemi kurulmuştur.

Kaynak : Kalkınma Bakanlığı, 2013

Yukarıdaki tabloda görüldüğü üzere, kişisel verilerin korunması hakkında Avrupa Konseyi, yoğun bir çalışmanın sonucunda 1981 yılında *"Kişisel Verilerin Otomatik İşleme Tabi Tutulma Sürecinde Bireylerin Korunmasına İlişkin 108 sayılı Sözleşme"*yi kabul etmiştir. Sözleşme 1985 yılında yürürlüğe girerek kişisel verilerin korunması konusunda bağlayıcı ilk uluslararası belge olma niteliği kazanmıştır (Atak, 2010).

Bu sözleşmeye Avrupa Konseyi üyesi olmayan devletlerde taraf olabileceğinden, 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 bulunmamaktadır.

Tablo 4. 2. Avrupa Konseyi'nden Kişisel Verileri Koruma Kanununu Çıkaran Ülkeler



Kaynak : Kalkınma Bakanlığı, 2013

Kişisel verilerin korunması konusunda en geniş yasal altyapı Avrupa Birliği tarafından; 1995 yılında yayınlanan 95/46/EC sayılı Veri Koruma Direktifi, 2002 yılında yayınlanan 2002/58/EC sayılı E-Gizlilik Direktifi, 2006 yılında yayınlanan 2006/24/EC sayılı Veri Saklama Direktifi, ve 2009 yılında yayınlanan 2009/136/EC sayılı Vatandaş Hakları Direktifi ile düzenlenmiştir (Şahin, 2011).

ABD'de genel bir kişisel veri koruma sistemi geliştirilemezken, bu konudaki anayasal koruma da sınırlı kalmaktadır. Çünkü ABD anayasası gizliliği doğrudan güvence altına almamış ancak alınan kararlar ile birlikte gizlilik hakkı içtihatların bir parçası haline gelmiştir. İlave olarak özel sektördeki uygulamaları düzenlemek amacıyla sektörel kanunlar çıkartılmıştır. Ancak henüz Avrupa'daki gibi ulusal çapta bir veri koruma kanunu mevcut değildir. 2001 yılında 11 Eylül saldırılarının hemen ardından çıkartılan PATRIOT Act ile birlikte Amerikan hükümetinin özel hayata ve kişisel verilere erişim imkânları büyük oranda artırılmıştır (Kalkınma Bakanlığı, 2013).

Günümüzde teknolojinin gelişmesine paralel olarak kişisel verilerin korunması alanında birçok ülkede günün oluşan koşullarına uygun gelişmeler hızla devam etmektedir. Aşağıdaki Tablo 4.3 ve Tablo 4.4'de Avrupa Konseyi Üyesi Ülkeler ile üyesi olmayan bazı ülkelerin "Karşılaştırmalı Hukukta Kişisel Verilerin Korunması" bilgileri yer almaktadır (Civelek, 2011).

Tablo 4. 3. Karşılaştırmalı Hukukta Kişisel Verilerin Korunması/Avrupa Konseyi Üyesi Ülkeler

Devlet	108 Sayılı Sözleşme		İlgili Anayasa	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi	Hükümleri			Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Arnavutluk	14/02/2004	09/06/2004	1998 AY, md. 35	9887 sayılı Kişisel Verilerin Korunması Hakkında Kanun, 2008	10/03/2008	Var	Yok	Her ikisi	Yok	Yok	Veri Koruma Komiseri
Ermenistan			1995 AY, md. 20								
Avusturya**	28/01/81	30/03/88	Veri Koruma Kanunu 2000, md.1 Bölüm 1-3'teki anayasal koşul	Kişisel Verilerin Korunmasına İlişkin Kanun (Federal Act concerning the Protection of Personal Data –Implementation of Directive 95/46/EC9)	17/08/99	Var	Var	Her ikisi	Tüm veriler (önemli istisnalar)	Bazı veriler	Veri Koruma Komisyonu
Azerbaycan			1995 AY, md.32	Veri, Veri işleme ve Veri Koruma Hakkında Azerbaycan Cumhuriyeti Kanunu	07.12.99						
Belçika**	07/05/82	28/05/93	1970 AY, md. 22	-Kişisel Verilerin Korunması Kanunu -95/46 sayılı VKD''nin uygulanmasına ilişkin Kanun -Kişisel Verilerin Korunması Kararnamesi	08/12/92 11/12/98 13/02/2001	Var	Var	Her ikisi	Tüm veriler	Bazı verileri	Mahremiyet Koruma Komisyonu

* AB üyesi ülkelerden 95/46/AT sayılı Veri Koruma Direktifini uyumlaştıran ülkeler.

** AB üyesi ülkelerden 95/46/AT sayılı Veri Koruma DirektifiniVeri Koruma Direktifini uyumlaştırma sürecinde olan ülkeler.

(Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Bosna Hersek	02/03/2004		Bosna Hersek'in 1995 tarihli AY, md. II, paragraf 3f	Kişisel Verilerin Korunması Kanunu	20/12/2001	-	-	Her ikisi	-	Yok	Veri Koruma Komisyonu
Bulgaristan	02/06/98	18/09/02	1991 AY, md. 32	Kişisel Verilerin Korunması Kanunu	21/12/2001	Var	Var	Her ikisi	Tüm veriler	Evet	Kişisel Verilerin Korunması Komisyonu
Hırvatistan	05/06/2003	21/06/2005	1990 AY, md. 37 (1997 ve 2000'de değişen)	Kişisel Verilerin Korunması Kanunu	01/10/2005	Var	Yok	Her ikisi	Tüm veriler (önemli istisnalar)	Yok	Kişisel Verileri Koruma Ajansı
Güney Kıbrıs Rum Yönetimi	25/07/86	21/02/02	1960 AY, md.15	Kişisel Verilerin İşlenmesi (Bireylerin Korunması) Kanunu, 2001	2001	Var	Yok	Her ikisi	Bazı verileri	Evet	Kişisel Verileri Koruma Komiseri
Almanya**	28/01/81	19/06/85	1943 AY, md.10	Federal Veri Koruma Kanunu (95/46 sayılı VKD'nin uygulanmasına yönelik)	01/01/2002	Var	Yok	Her ikisi	Bazı veriler	Yok	Federal Veri Koruma Komiseri
Yunanistan**	17/02/83	11/08/95		1997 tarihli ve 2472 sayılı kişisel verilerin işlenmesi ile ilgili bireyin korunması hakkında kanun Kişisel verilerin ve mahremiyetin elektronik haberleşme sektöründe korunması ve 2472/1997 sayılı kanunu değiştiren kanun (2006)	26/03/1997	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Kişisel Veri Koruma Kurumu
Macaristan	13/05/93	08/10/97	149 AY, md. 59	LXIII sayılı kişisel verilerin korunması ve kamuyu ilgilendiren bilgilerin açıklanması hakkında kanun	17/11/92 Bölüm III Bölüm IV	Var	Yok	Her ikisi	Tüm veriler	Yok	Veri Koruma Ombudsmanı

(Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletimine) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
İzlanda	27/09/82	25/03/91		Kişisel verilerin işlenmesi karşısında bireylerin korunmasına ilişkin kanun	01/01/2000	Var	Var	Her ikisi	Tüm veriler	Tüm veriler	Kişisel Veri Koruma Kurumu
İrlanda*	18/12/86	25/04/90		1988 tarihli Veri Koruma Kanunu (2003'te değişti) Elektronik Mahremiyet Kanunu, 2003 (2008'de değiştirildi)	13/07/88 19/12/01	Yok	Yok	Her ikisi	Bazı veriler	Yok	Veri Koruma Komiseri
İtalya**	02/02/83	29/03/97		196/2003 sayılı Kişisel Veri Koruma Kanunu	01/01/2004	Var	Var	Her ikisi	Bazı veriler	Bazı veriler	Kişisel Verileri Koruma Kurumu
Letonya	31/10/00	30/05/01	1922 AY, m 96	Kişisel Veri Koruma Kanunu	23/03/00	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Devlet Veri Denetim Otoritesi (Data State Inspectorate)
Lihtenştayn	02/03/2004	11/05/2004	-	Veri Koruma Kanunu, 2002 Veri Koruma üzerine 9 Temmuz 2002 tarihli Yönetmelik	14/03/02 09/07/02	Var	Var	Evet	Evet Bazı veriler	Evet	Veri Koruma Komiseri
Litvanya	11/02/00	01/06/01	1992 AY, md. 22	Kişisel Verilerin Yasal olarak Korunması Hakkında Kanun	17/07/00	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Devlet Veri Denetim Otoritesi (State Data Protection Inspectorate)
Lüksemburg*	28/01/81	10/02/88	1868 AY, md. 28	Kişisel Verilerin İşlenmesi Halinde Bireyin Korunması Hakkında Kanun Telekomünikasyon Kanunu	02/08/2002	Var	Var	Her ikisi	Tüm veriler (istisnaları var)	Bazı veriler	Veri Koruma Ulusal Komisyonu

(Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Malta	15/01/2003	28/02/2003	1964 AY, bölüm 32	Veri Koruma Kanunu, 2001	14/12/2001	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Veri Koruma Komiseri
Moldova	04/05/1998	28/02/2008	1994 AY, md. 28			Yok	Yok	Her ikisi			
Monako	01/10/2008	24/12/2008	1962 AY, md.22	İsimsel bilginin işlenmesi hakkında Kanun İsimsel verinin işlenmesi hakkında kanunun uygulanmasıona ilişkin Yönetmelik	23/12/1993	Var	-		Tüm veriler	Yok	Kişisel Verilerin Denetlenmesi Hakkında Kanun
Karadağ	06/09/2005	06/09/2005									
Hollanda**	21/01/88	24/08/93	1989 AY, m.10	Kişisel Veri Koruma Kanunu	06/07/00	Var	Yok		Her ikisi	Bazı veriler	Veri Koruma Komisyonu
Norveç	13/03/81	20/02/84		Kişisel Veri Kanunu	14/04/00	Var	-	Her ikisi	Tüm veriler	Tüm veriler	Veri Müfettişliği
Polonya	21/04/99	23/05/02	1997 AY, m. 51	Kişisel Verilerin Korunması Hakkında Kanun	29/08/97	Var	Var	Her ikisi	Bazı veriler	Evet	Kişisel Veri Koruma Genel Müfettişi
Portekiz**	14/05/81	02/09/93	1976 AY, m. 35	Kişisel Verilerin Korunması Kanunu (95/46 sayılı VKD'nin uygulanmasına ilişkin)	28/10/1998	Var	Yok	Her ikisi	Bazı veriler	Bazı veriler	Ulusal Veri Koruma Komisyonu
Romanya	18/03/97	27/02/02	1991 AY, m.26	Kişisel Verilerin İşlenmesi Karşısında Bireylerin Korunması ve Bu Verilerin Serbest Dolaşımı Hakkında 677/2001 sayılı Kanun 102/2005 ve 506/2004 sayılı Kanunlar	12/12/2001	Var	Var	Her ikisi	Evet	Evet	Kişisel Verilerin İşlenmesinin Denetlenmesi Hakkında Ulusal Otorite
Rusya	07/11/01		1993 AY, m.24								

(Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
San Marino				Sayısallaştırılmış kişisel verilerin toplanması, işlenmesi ve kullanılması hakkında kanun	01/03/83	Yok	Var	Her ikisi	Tüm veriler	Bazı veriler	Gizli ve Kişisel Verilerin Korunmasından Sorumlu Garantör (Guarantor)
Sırbistan	06/09/2005	06/09/2005		Kişisel Veri Koruma Kanunu	/10/2008						
Slovakya	14/04/00	13/09/00	1992 AY, m. 19 ve 22	Kişisel Veri Koruma Kanunu	03/02/2005	Var	Yok	Her ikisi	Bazı veriler	Yok	Slovak Cumhuriyetini ve Kişisel Verileri Koruma Ofisi
Slovenya	23/11/93	27/05/94	1991 AY, m. 38	Kişisel Veri Koruma Kanunu	08/07/99	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Bilgi Komiserliği
İspanya**	28/01/82	31/04/84	1978 AY, m. 18	Kişisel Verilerin Korunması Hakkında 15/99 sayılı Kanun	13/12/99	Var	Yok	Her ikisi	Tüm veriler	Bazı veriler	Veri Koruma Ajansı
İsveç**	28/01/81	29/09/82	1989 AY, Bölüm 2, m. 3	Kişisel Veri Kanunu	29/04/1998	Var	Yok	Her ikisi			Veri Teftiş Kurulu
İsviçre	02/10/97	02/10/97	1999 AY, m. 13	Federal Veri Koruma Kanunu Yönetmelikler:OLPD, OALSP	19/06/92 Yönetmelikler 14/06/93'te kabul edildi.	Var	Var	Her ikisi	Bazı veriler	Bazı veriler	Federal Veri Koruma ve Bilgi Komiseri
Makedonya	24/03/2006	24/03/2006	1992 AY, m.18	Kişisel Veri Koruma Kanunu	25/01/2005	Var	Var	Her ikisi	Yok	Evet	Kişisel Veri Koruma Müdürlüğü (İdari organ)
Türkiye	28/01/81		1982 AY (2001 değ.) m. 20								

(Avrupa Konseyi Üyesi Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Ukrayna	29/08/2005		1996 AY, m.32	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	Bölge kanunları: Jersey Kanunu, Guernsey Kanunu, Isle of Man Kanunu	16/07/98	Var	Yok	Her ikisi	Tüm veriler	Evet

Tablo 4. 4. Karşılaştırmalı Hukukta Kişisel Verilerin Korunması / Avrupa Konseyi Üyesi Olmayan Bazı Ülkeler

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Vatikan											
ABD				1-Mahremiyet Kanunu 2-Kişisel verilerin korunmasında farklı sektörlere ait kanunlar[249] 3- Güvenli Liman Kuralları	1- 1974 3-2000						
Kanada			1982 AY, Bölüm 8	1- Mahremiyet Kanunu 2- Kişisel Verilerin Korunması ve Elektronik Belgelere İlişkin Kanun	01/07/83 13/04/00	Var		Kamu			Mahremiyet Komiseri Federal Kurumlar
Japonya				1-Kamu sektörü: Kamu kurumlarında sayısal ortamda tutulan kişisel verilerin korunması hakkında kanun 2-Kamu kurumlarında sayısal ortamda tutulan kişisel verilerin korunması hakkında kanunun uygulanmasına ilişkin yönetmelik	16/12/88 01/10/89	Yok	Yok	Kamu	Bazı veriler		İdari Yönetim Ofisi, İçişleri, Posta ve Telekomünikasyon
Meksika			1917 AY, m.16	Federal Şeffaflık ve kamu kurumlarındaki bilgilere erişim kanunu Federal Kanunlar	05/2002						Kamu Bilgilerine Erişim Enstitüsü
Arjantin			1853 AY, m.43	Kişisel Verilerin Korunması Kanunu	04/10/2000	Var		Her ikisi			
Avustralya				Federal Mahremiyet Kanunu	18/10/88 21/12/2002	Var	Yok	Kamu ve özel sektör			Mahremiyet Komiseri
Brezilya			1988 AY, m.5.X,	Habeas Veri Kanunu	1997						

(Avrupa Konseyi Üyesi Olmayan Bazı Ülkeler, devamı)

Devlet	108 Sayılı Sözleşme		İlgili Anayasa Hükümleri	İlgili Ulusal Mevzuat	Yürürlük tarihi	Kapsamı			Kayıt veya bildirim	Verinin ihracında (dışarı iletiminde) özel yetki	Veri Koruma Otoritesi
	İmza tarihi	Onay tarihi				Elle işleme	Tüzel kişiler	Kamu veya özel sektör			
Şili			1980 AY, m.19	Kişisel Verilerin Korunması Kanunu	28/08/99	Var	Evet	Her ikisi	Yok	-	
İsrail			1992, Bölüm 7, Temel Kanunlar; İnsan Onuru ve Özgürlüğü	5741 sayılı Mahremiyeti Koruma Kanunu 5746 sayılı İdari Verileri Koruma Kanunu	02/1981 1986	Yok	Yok				
Güney Kore			1948 AY, M.17	Kamu Kurumlarınca Yönetilen Kişisel Verilerin Korunması Kanunu	07/01/94	Yok	Yok	Kamu			
Tayland	06/09/2005	06/09/2005	1997 AY, Bölüm 34	Bilgi Kanunu no: B.E 2540	1997		-	Evet			Resmi Bilgi Komisyonu Ofisi
Yeni Zelanda			1990 Yeni Zelanda Haklar Kanunu, m.28	Mahremiyet Kanunu	17/05/93					Yok	Mahremiyet Komiseri

Ülkemizde kişisel verilerin korunmasına ilişkin yeterli yasal bir düzenleme ve yetkili bir kuruluş bulunmamasına rağmen, bu hususta farklı hukuksal düzenlemeler bulunmaktadır. 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 İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik
- Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" (Şahin, 2011; Civelek, 2011; Kılınç, 2012; a.g.e.).

Sosyal paylaşım ağlarında kişisel verilerin korunmasına yönelik hukuki düzenlemeleri işlemek gerekirse;

5237 sayılı TCK'da ve muhtelif maddelerde belirtilen suç tanımlamaları başlıklar halinde listelenebilir.

- **Bilişim sistemine girmek:**

  TCK 243/1'de belirtilen bir kişinin bir bilişim sistemine hukuka aykırı olarak girmesi ve kalması durumunda 1 yıla kadar hapis cezası, TCK 243/3' de sistemin içerdiği veriler yok olur veya değişirse, 6 aydan 2

yıla kadar hapis cezası öngörülmüştür. Bu yasalar ile bir sistemdeki kişisel veriler koruma altına alınmıştır (TBMM, 2013a).

- **Sistemi engellemek, bozma, verileri yok etme veya değiştirme:**
  Yukarda belirtilen suça ek olarak benzer bir şekilde bir kamu kurum veya kuruluşuna ait kişisel ya da bir banka ve kredi kurumunun verilerinin bilişim sistemi üzerinde işlenmesi halinde TCK 243/3 maddesinin 1. fıkrası gereğince 1.5 yıldan 7.5 yıla kadar hapis cezası belirtilmiştir (TBMM, 2013a).

- **Banka veya kredi kartlarının maddi kazanç doğrultusunda kötüye kullanımı:**
  TCK' nın 245. maddesi banka veya kredi kartlarının usulsüz kullanımını düzenleyen madde olma özelliğine sahiptir. Fakat 245. madde incelendiğinde suçun işlenmiş sayılması için gerçek bir kredi kartının kullanılması ya da kopyalanması fiziki olarak gerçekleştirilmesi gerekmektedir. Bu yüzden internet ortamında gerçekleştirilen bu suçları, normu uygulayan yargıcın bu durumları gözetmesi gerektiği açıktır (Koç ve Kaynak, 2010).

- **Nitelikli dolandırıcılık:**
  TCK' nın 158. maddesi 1. fıkrası gereği bilişim sistemleri aracılığı ile banka ve kredi kurumlarının kullanılması suretiyle işlenen suçlara 2 yıldan 7 yıla kadar hapis cezası düzenlenmiştir. Bu madde 243 ile 246 maddeleri arasında düzenlenen "Bilişim Alanında Suçlar" dışında muhtelif maddeler arasında yer almaktadır (TBMM, 2013a).

- **Hakaret, sövme ve şantaj:**
  Kişisel veriler kullanılarak şantaj yapılması durumunda TCK' nın 125. maddesi gereği 3 aydan 2 yıla kadar hapis cezası belirtilmiştir (Koç ve Kaynak, 2010).

- **E-posta, sosyal ağlardaki kişisel hesapların ele geçirilmesi:**
  E-posta ve sosyal ağlardaki kişisel hesapların haksız olarak ele geçirilmesi durumunda TCK'nın 243. Maddesi gereğince 2 yıla kadar hapis ya da adli para cezası verilmektedir. Eğer e-postası ele geçirilen kişinin verilerinde değişiklik yapılması durumunda bu ceza 2 yıldan 4 yıla kadar hapis cezasına dönüşmekte ve para cezası hükmü de ortadan kalkmaktadır (TBMM, 2013a).

Kişisel verilerin zorlama ve tehdit etmek için kullanılması durumunda TCK'nın 107. maddesi gereğince önceki cezaya ek olarak 5000 güne kadar adli para cezası ile birlikte 3 yıla kadar hapis cezası verilmektedir (TBMM, 2013a).

Eğer sadece kişiye sıkıntı vermek ve rahatsız etmek amacı ile yapılıyorsa yine önceki cezaya ek olarak TCK'nın 127. maddesi gereğince 3 aydan 1 yıla kadar hapis cezası verilmektedir (TBMM, 2013a).

TCK'nın 124. maddesi gereğince eğer kişisel haberleşme verileri hukuka aykırı olarak ifşa edilirse yine 1 yıldan 3 yıla kadar hapis cezası söz konusu olmaktadır. Ayrıca Skype gibi haberleşme programlarında konuşmaları kaydedip başkaları ile paylaşılması durumunda da bu cezai işlem uygulanmaktadır (TBMM, 2013a).

Sadece kişilerin siyasi, felsefi, dini görüşleri, ırki kökenleri, cinsel yaşamları, sağlık durumlarına yönelik belgelerin kayıt altında tutulması durumunda TCK'nın 135. maddesinin 1. ve 2. fıkralarına istinaden önceki cezalara ek olarak 6 aydan 3 yıla kadar hapis cezası verilmektedir (TBMM, 2013a).

Bütün bu düzenlemelerden hakkında soruşturma açılan kişinin ceza alması durumunda, özel bilgi ve beceri sayesinde gerçekleştirmiş olduğu için verilecek ceza yarısı oranında artırılır (TBMM, 2013a).

Bununla beraber, Telekomünikasyon İletişim Başkanlığının (TİB) internet ortamında yapılan yayınların düzenlenmesiyle ilgili faaliyetleri bulunmakta olup, konuyla ilgili mevzuata ve açıklamalara aşağıda yer verilmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da belirtilen katalog suçlar kapsamında verilen erişimin engellenmesi kararları, kararı veren hâkim, mahkeme veya Cumhuriyet Savcısı tarafından gereği yapılmak üzere Telekomünikasyon İletişim Başkanlığına gönderilmekte ve kararlar Telekomünikasyon İletişim Başkanlığınca yerine getirilmektedir. Ayrıca anılan Kanunun 8. maddesinde sayılan suçların oluşması durumunda ilgili içerik veya yer sağlayıcının yurtdışında olması durumunda TİB tarafından re'sen erişimin engellenmesi yapılabilmekte; 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 sunulmaktadır (TİB, 2013a).

5651 sayılı yasa çerçevesinde İnternet ortamında yapılan ve erişimi engellenebilen yayınlar aşağıda belirtilmiştir:

"...

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 İşlenen Suçlar Hakkında Kanunda yer alan,

c) 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlardır.

..." (TİB, 20113b)

Kısaca; 5651 sayılı Yasada belirtilen suçlar ve daha sonra ilave edilen yasadışı bahis ve şans oyunlarına ilişkin konularda erişimin engellenmesi kararı verilebilmektedir. Bununla birlikte, mevcut durum itibariyle erişimin engellenmesi uygulamasının sosyal medya ayağı bulunmamakta olup, sosyal paylaşım ağlarında yaşanacak kişisel veri ihlalleri veya kişilik hakkına saldırı gibi konularda TİB uygulaması bulunmamaktadır. Bu çerçevede, mevcut erişim engelleme uygulamasının ve ilişkili mevzuatın sosyal paylaşım ağlarının yaygınlığı göz önüne alınarak, sosyal paylaşım ağlarını da kapsayacak şekilde genişletilmesinin yerinde olacağı değerlendirilmektedir. (TİB, 20113b)

Bu bölümde kişisel verilerin korunması ile ilgili olarak ulusal ve uluslararası kurum ve kuruluşların uygulamaları incelenmiştir. Ülkemizde kişisel verilerin korunması kanununa olan ihtiyaçtan hareketle, 1989 yılından başlayarak 2000'li yıllara kadar bu konuda çeşitli taslaklar hazırlanmış, 02/05/2008 tarihinde oluşturulan tasarı Türkiye Büyük Millet Meclisi'ne sevk edilmesine rağmen bu güne kadar henüz çıkarılamamıştır. Tasarı halen Başbakanlık'ta bulunmaktadır.

AB vatandaşlarının kişisel verileri üzerindeki haklarını düzenleyen kanuna benzer şekilde Kişisel Verilerin Korunması Kanun Tasarısı hazırlanmıştır. Kişisel verilerin yasal, dürüst bir şekilde toplanması ve işlenmesi, belirli ve meşru amaçlar için güncelleştirilmesi, amacına uygun bir süre için muhafaza edilmesi, verilerin amaca aykırı olarak paylaşılmaması, veri sahibi kişinin hakkındaki verileri öğrenme, değiştirme ve gerekirse silme haklarını düzenleyen bu tasarı, kişisel veri sahibinin haklarını koruyucu nitelikte düzenlenmiştir (Beyli, 2004; Civelek, 2011). Bu sistemin işleyişini de yine oluşturulacak Kişisel Verilerin Korunması Kurul'u kontrol edecektir. Bu kurul ayrıca olası anlaşmazlıklarda veri kütüğü sahibine çeşitli yaptırımlar uygulayarak veri sahibinin haklarını koruyacaktır (Hukuktabilişim, 2013).

SONUÇLAR VE ÖNERİLER

Sosyal paylaşım ağları, 90'ların ortasından sonra hayatımıza giren ve günden güne kullanıcı sayılarını artıran yeni nesil iletişim araçlarıdır. İlk önceleri belli bir amaçla ve belli bir kesime hitaben ortaya çıkan sosyal paylaşım ağları, zaman içinde daha karmaşık bir yapıya ve milyarlara hitap eden devasa etkileşim platformları haline gelmiştir. Günümüzün en yaygın sosyal paylaşım ağları olan Facebook, Twitter ve Youtube bunların başında gelir.

İnsanlar sosyal paylaşım ağları üzerinden bilgi, haber veya ilgi alanlarına yönelik paylaşımlar yapmaktadır. Video, fotoğraf veya haber paylaşmak bunların başında gelir. Sosyal paylaşım ağlarının günden güne popülaritesini artırması amatör kullanıcıların yanında profesyonel kuruluşların da dikkatini çekmiş olup profesyonel şirketler de sosyal paylaşım ağları üzerinden hedef kitlesine ulaşmak amacıyla bu sistemleri aktif olarak kullanmaktadır.

Günümüzde internet üzerinde oluşan trafiğin en büyük kısmını sosyal paylaşım ağları oluşturmaktadır. İnternet kullanıcıları internet üzerinde gezinirken ilgi çekici her türlü haber veya içeriği arkadaş grubuyla paylaşmaktadır. Bu da sosyal paylaşım ağlarının oluşturduğu trafiği artırmaktadır. Bu anlamda Facebook ve Twitter yine başı çekmektedir.

Sosyal paylaşım ağları kullanıcılarına hizmet sunarken kullanıcı bilgileri üzerinden de maddi kazanç sağlamaktadır. Bu bilgileri kullanma hakkını ve inisiyatifini de gizlilik politikaları veya kullanıcı sözleşmeleri adı altında garanti altına almaktadır. Ancak bu sözleşmelerin çok uzun olması, yeteri kadar açık olmaması ve internet kullanıcılarının çok büyük bir kesiminin bu sözleşmeleri okumaması kullanıcı açısından bir problem olarak değerlendirilmektedir. Ayrıca yasal düzenlemelerin yetersiz olması nedeniyle sosyal paylaşım ağlarının kullanıcı bilgilerini gerektiğinde istihbarat kuruluşları ile

paylaşabilmesi çokça eleştirilen ve anti-sosyal paylaşım ağlarının ortaya çıkmasının en büyük nedeni olarak görülmektedir.

Kişisel veriler pek çok farklı saldırı yöntemleri ile hedef alınmaktadırlar. Bu yöntemler doğrudan sistemler üzerine, doğrudan kullanıcıya veya sistemler üzerinden dolaylı olarak kullanıcıya gerçekleştirilebilir. Kullanıcıların ve sistem yöneticilerinin bu saldırılara karşı bilinçli ve dikkatli olması gerekmektedir.

Bu tezde temel olarak, sosyal paylaşım ağlarının kullanım yaygınlığı incelenmiş olup, son yıllarda kullanımı giderek artan bu ağlarda ortaya çıkabilecek güvenlik açıkları kişisel bilgilerin gizliliğinin sağlanması açısından ele alınmıştır. Bu çerçevede, dünyada ve ülkemizde kişisel bilgileri gizliliğinin sağlanması ve korunması için yapılan bazı düzenlemelere yer verilmiş olup, bu bölümde yukarıda yer verilen değerlendirmelere dayanılarak bazı önerilerde bulunulacaktır.

Sosyal paylaşım ağları üzerinde gençlerin ağırlıklı olarak gerçek isimlerini ve fotoğraflarını paylaştıkları görülmektedir. İnternet üzerine konulmuş bir bilgiyi artık geri almak mümkün olmadığından, o bilgi herhangi (iyi veya kötü niyetli) bir kişi tarafından rahatlıkla okunabilecektir. Ayrıca, sosyal paylaşım ağları üzerinde paylaşılan durum güncelleştirmeleri, bireylerin hayatları ile ilgili pek çok ipucunu verebilecektir. Masum gözüken ve masum amaçlarla yazılmış bir durum güncelleştirmesi, kişinin evinin soyulmasına bile neden olabilmektedir.

Sosyal paylaşım ağları üzerinde geliştirilen uygulamalar, bireylerin kişisel bilgilerini hedef alabilmektedirler. Kişilerin bu uygulamalara girdiği verilerin neler olduğuna dikkat etmesi gerekir. Önemli olan kullanıcıların sosyal paylaşım ağlarını güvenli etkin ve bilinçli kullanımı konusunda bilgilendirilmesi gerektiğidir. Devletler ve özel kurumlar tarafından alınan önlemler sosyal paylaşım ağlarını kullanan kişileri belli bir noktaya kadar koruyabilmektedir. Bu yüzden toplumda güvenlik eksikliklerini minimize

edebilmek için bireysel anlamda farkındalık yaratmak yapılması gereken önlemlerin başında gelmektedir.

Taksim Gezi Parkı eylemleri ile birlikte sosyal paylaşım ağlarının toplumdaki ve güvenlik sektöründeki önemi ülkemizde etkin bir şekilde fark edilmeye başlanmıştır. Genç nüfusun fazla olması dolayısıyla sosyal paylaşım ağlarının ülkemizde yaygın bir şekilde kullanıldığı bir gerçektir.

Bu hususta ülkeler kendi toplumlarının sosyo-kültürel, dini, ideolojik özelliklerine göre bazı uygulamalara gitmiştir, fakat kişisel veriler için Devletlerce yapılan tanımlara bakıldığında, şu tanım ön plana çıkmaktadır: "kişisel veri; belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgilerden" oluşur. Kısaca kişisel bilgiler, isim, doğum tarihi, kimlik numarası, fotoğraf, tıbbi kayıtlar vb. verilerdir. Bundan dolayı, kişisel verilerin korunması, verinin kendisinin gizliliğinin korunmasından çok, bireyin kimliğinin korunmasıdır. Amerika ve Kanada'da bu durum, özel yaşamın gizliliğinin korunması olarak tasvir edilmektedir.

Bu çalışma kapsamında gerçekleştirilen incelemeler doğrultusunda kişisel bilgilerin gerek yasal, gerek sosyal hayat anlamında önemli bir yer tuttuğu görülmektedir. Bireylerin kişisel bilgilerinin çalınmasının hukuki sonuçları olacağı gibi, bireyin sosyal hayatı üzerinde de olumsuz etkileri bulunabilir. Bu yüzden bu bilgilerin sosyal, teknik ve hukuki çerçevelerde korunması önemlidir.

Yapılan incelemeler neticesinde, sosyal, teknik ve hukuki alanlarda aşağıda belirtilen önlemlerin alınmasının önemli olduğu değerlendirilmektedir.

Sosyal Önlemler

1- Kullanıcılar, kişisel bilgilerinin önemi konusunda bilinçlendirilmelidir. Bu amaç doğrultusunda kampanyalar ve ödüllü oyunlar düzenlenebilir.

Bilinçlenmiş kullanıcılar, yemleme, istenmeyen e-posta, sahte linkler gibi saldırılara karşı dikkatli olacaklarından, mağduriyetleri en aza inecektir.

2- Kullanıcılar, internette gezinirken, teknolojik olarak gerekli önlemleri almış veya alabilecek esnekliğe sahip tarayıcıları, e-posta hesapları için teknolojik olarak kullanıcının güvenliğini ön planda tutan hizmet sağlayıcılarını seçmelidirler.

3- Sosyal ağlarda paylaşılan verilerin neler olduğuna dikkat edilmesi gerekmektedir. Sosyal paylaşım ağları üzerinde paylaşılan kişisel verilerin başka kimseler tarafından görülebileceği, yorumlanabileceği ve paylaşan kişinin bundan ileride zarar görebileceği göz önünde tutulmalıdır.

4- Sosyal paylaşım ağları üzerinde oynanan oyun yazılımları ve eğlence amaçlı geliştirilen diğer uygulamaların, hangi yetkileri istediğine dikkat edilmesi gerekmektedir. İhtiyacından fazla yetki talebinde bulunan uygulamalara şüphe ile yaklaşılmalı, bu tarz uygulamalarda sorulan sorulara verilen cevapların kişisel bilgiler olduğu unutulmamalıdır.

5- Orta öğretim çağındaki öğrencilere, bilinçlenmeleri ve farkındalıklarının artırılması için bilişim suçları ve sosyal paylaşım ağlarının güvenli kullanımı ile ilgili seminerler verilmeli veya müfredata bu konu ile ilgili dersler eklenmelidir.

Teknolojik Önlemler

1- Kullanıcıların kişisel bilgilerinin güvenliği açısından, hem kullanıcıların kendi kişisel cihazlarında (bilgisayar, tablet, cep telefonu vb.), hem de hizmet alınan tüm sunucularda (Sosyal paylaşım ağları, internet servis sağlayıcıları, hastaneler, devlet sistemleri vb.) bulunan yazılımların güncel olması gerekmektedir.

2- Sosyal paylaşım ağları tarafından, kullanıcıların sayfalarına (kullanıcının parolası ele geçirilerek) yetkisiz erişimin engellenmesi amacıyla, kullanıcılar güçlü parola belirlemeye zorlanmalıdır. Belirlenecek bu parolaların karmaşıklığı arttıkça kaba kuvvet (kaba kuvvet yöntemi: her türlü şifre ihtimalini denemektir) vb. yöntemlerle kırılması bir o kadar zorlaşmaktadır.

3- Kullanılan e-posta sunucusunda veya e-posta istemci yazılımında, istenmeyen postaları (spam) ayırt edebilecek gerekli eklentiler kurulmuş olmalıdır.

4- Hem kullanıcının kişisel cihazında, hem de her türlü sunucu sisteminde anti-virus, anti-spyware vb. güvenlik yazılımları kurulmuş olmalı ve güncelleştirmeleri sıklıkla yapılmalıdır.

5- Sosyal paylaşım ağları tarafından XSS, XSRF ve benzeri saldırılara karşı gerekli her türlü önlem alınmış olmalıdır. Bu önlemler, GET yöntemi ile veri girişini engellemek, her sayfa ve formda ID kontrolü gerçekleştirmek, sunucuya gelen verilerden istenmeyen kodları (HTML, JS gibi) temizlemek ve benzeri yöntemleri uygulamak olacaktır.

6- Sosyal paylaşım ağlarının güvenlik politikalarının kullanıcı tarafından rahat anlaşılmasını sağlayacak şekilde basitleştirilmesi sosyal paylaşım ağlarından talep edilmelidir.

7- Sosyal paylaşım ağları gizlilik politikalarının uzun ve anlaşılması güç metinler olarak yayınlanması yerine basit ve görsel yöntemler kullanılarak oluşturulmuş objeler ve kişisel verilerin kullanılması durumunu otomatik olarak algılamak için geliştirilmiş olan Platform for Privacy Preferences (P3P) vb. yazılım teknolojilerinin kullanımı teşvik edilmelidir.

Yasal Önlemler

1- 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.

2- Yaşanan bu olumsuz gelişmelere önlem olarak pek çok ülke kendi mevzuatını geliştirmekte ve bu olumsuzluklara karşı önlemler almaktadır. Ülkemizde TCK'ya bilişim suçları bölümü ilave edilerek hukuki önlemler alınmıştır. Kaleme alınan 5237 sayılı yeni Ceza Kanunumuzda daha dikkatli olarak incelenmeye çalışılmış fakat etkin olmamıştır. Örneğin yukarıda belirtilen TCK'nın 245. maddesi gereği kredi kartının usulsüz kullanımına ilişkin düzenlemede bilişim aracılığı ile işlenen suçlar kapsam dışına alınmıştır. Başkasına ait kredi kartı, internet bankacılığı, şifre, parola ve diğer önemli kişisel bilgilerin, internet ortamında elde edilerek, çıkar sağlamak amacıyla bir başkası tarafından yetkisiz olarak kullanılmasının kimlik hırsızlığı dolandırıcılık yöntemi olması nedeniyle, TCK'nın 245. maddesi bilişim suçları kapsamında yeniden düzenlenmelidir.

3- Yeterli bilgi seviyesine sahip olmayan kullanıcıların da sosyal paylaşım ağlarını kullanabilecekleri düşünülerek kullanıcıların hakları yasalarla garanti

altına alınmalı, servis sağlayıcıların bu kurallara uymalarını sağlayacak yaptırımlar geliştirilmelidir.

4- Kullanıcıların mağduriyetleri durumunda yasal açıdan mağduriyetlerinin giderilmesini sağlamak amacıyla dava açma ve sonuçlandırma mekanizması basitleştirilmeli ve gerekli yurt dışı kurum veya kuruluşlarla gerekli işbirlikleri yapılmalıdır. Buna örnek olarak İngiltere' de faaliyet gösteren Internet Watch Foundation (IWF) adlı sivil toplum kuruluşu gösterilebilir. AB fonlarından desteklenen kuruluş "Uyar ve Kaldır" prensibi doğrultusunda mahkemelerin yükünü hafifleten bir bilirkişi durumundadır. Böylelikle mağdur olan kişilerin başvuruları ön elemeden geçerek haklı olup olmadıkları bir üst makama ve/veya mahkemelere bildirilmektedir.

5- Ülkemizde; bilişime ilişkin bilgi sahibi olan hukukçuya ve hukuk bilen bilişimciye ihtiyaç olduğundan üniversitelerde bu konuyla ilgili olarak eğitim veren bölümlerin, kürsülerin kurulması teşvik edilmelidir.

6- Diğer taraftan, kişisel verilerle ilgili tüm hususları kapsayan yasal düzenlemenin öncelikle yapılması ve kişisel verilerin işlenmesi, korunması vb. süreçlerini kontrol edecek, denetleyecek "düzenleyici ve denetleyici" bir kurumun kurulması sağlanmalıdır.

7- Son olarak, mevcut durum itibariyle TİB tarafından ilgili düzenlemeler çerçevesinde erişim engelleme uygulaması yapılmakta olup, bu uygulamanın sosyal paylaşım ağlarıyla ilgili genişletilmesinin yerinde olacağı düşünülmektedir. Diğer bir ifade ile, mevcut durumda sosyal paylaşım ağlarıya ilgili bir kişisel veri gizliliği ihlali veya kişilik haklarına saldırı yaşandığında bu durumun mağdurun kişisel başvurusu üzerine TİB tarafından ele alınması gibi bir yaklaşımın hukuki çerçevesi çizilmek koşuluyla hayata geçirilebileceği değerlendirilmektedir.

KAYNAKLAR

ADDTHIS, 2013, İnternette İçerik Paylaşımı, http://www.addthis.com/services#.Uez-qphrPcu, (14.07.2013)

ATAK Songül, 2010, TBB Dergisi, Sayı 87, s.90-120, Ankara http://tbbdergisi.barobirlik.org.tr/m2010-87-606, (10.07.2013)

AVRUPA KONSEYİ, 1981, 108 sayılı Avrupa Konseyi Sözleşmesi

BEYLİ Ceylin, 2004, "KİŞİSEL VERİLERİN KORUNMASI HAKKINDA KANUN TASARISI ÜZERİNE ELEŞTİRİLER" Türkiye Bilişim Şurası Hukuk Çalışma Grubu Kişisel Veriler Raporu'na ait görüş, http://www.ihop.org.tr/dosya/izleme/tbs_kisisel_veri_ceylin_beyli_gorus_1.pdf, (15.08.2013)

BGA(Bilgi Güvenliği Akademisi), 2013, http://www.bga.com.tr/, (20.07.2013)

BİLGİ GÜVENLİGİ, 2013a, http://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/en-buyuk-facebook-acigi-sizsiniz.html, (15.07.2013)

BİLGİ GUVENLİGİ, 2013b, http://www.bilgiguvenligi.gov.tr/son-kullanici/index.php, (15.07.2013)

BLOGSPOT, 2013, http://googleonlinesecurity.blogspot.jp/2012/06/safe-browsing-protecting-web-users-for.html, (17.07.2013)

BM Genel Kurulu, 1990, mevcut *Bilgisayarlı Kişisel Veri Dosyaları Yönetmeliği için rehber* 14 Aralık 1990,: http://www.refworld.org/docid/3ddcafaac.html, (12.08.2013)

BOYD, D. M., 2007, "Social Network Sites: Definition, Historyand Scholarship", Journal of Computer-Mediated Communication, s.210-230

BOYD D. M., Heer J., 2006, "Profiles as Conversation: Networked Identity Performance on Friendster", Hawaii International Conference on SystemSciences, HICSS 39

BTK, 2013a, http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSKVIGKHak_Yon_Konsolide_Metin_2013.pdf, (14.07.2013)

BTK, 2013b, http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf (14.07.2013)

BTK, 2013c, http://www.tk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2013%20DK-SDD-228.pdf (14.07.2013)

BYGRAVE Lee A, 2002, Data Protection Law, Kluwer Law International, ISBN-13:* 978-9041198709*, London

CAMPO Avila J., Moreno-Vergara N., Trella-Lopez M., 2013, "Bridging the Gap Between the Least and the Most Influential Twitter Users", ProcediaComputerScience 19, s.437-444

CHAFKİN M., 2013, "How toKill a Great Idea!", http://www.inc.com/magazine/20070601/features-how-to-kill-a-great-idea.html, (12.07.2013)

CHANG, C. C., 2013, "Examining Users' Intentionto Continue Using Social Network Games: A Flow experience Perspective", Telematicsand Informatics 30, s.311-321

CHEN Xi, Shuo Shi, 2009, A Literature Review of Privacy Research on Social Network Sites , International Conference on Multimedia Information Networking and Security, Vol. 1, s. 93 – 97

CHENG X., Dale C., Liu J., 2008 , "Statistics and Social Network of YouTube Videos", Quality of Service, IWQoS 2008, 16th International Workshop on,s. 229 - 238

CHINA INTERNET WATCH, 2013, http://www.chinainternetwatch.com/2054/tencent-active-im-users-close-to-800-million-social-network-qzone-over-600-million-in-2012/, (21.07.2013)

CİVELEK Dilek Yüksek, 2011, Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi, TC Başbakanlık, Devlet Planlama Teşkilatı Müsteşarlığı, Ankara

DIGITAL MARKETING RAMBLINGS, 2013, http://expandedramblings.com/index.php/myspace-stats-then-now/, (21.07.2013)

DINERMAN B., 2011, Social Networking and Security Risks, GFI White Paper,http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf, (23.07.2013)

DİLMEN N. E., Öğüt, S., 2010, "Sosyalleşmenin Yeni Yüzü: Sosyal Paylaşım Ağları", İkinci Yeni İletişim Ortamları ve Etkileşim Uluslararası Konferansı, İstanbul, s.237-242

DNSCURVE, 2013, http://dnscurve.org/forgery.html, (01.07.2013)

DONANIMHABER, 2013, http://www.donanimhaber.com/mac-os-x/haberleri/Path-yeni-bir-kisisel-bilgi-ihlali-suclamasi-ile-karsi-karsiya.htm, (01.07.2013)

DUNLAP J. C.,Lowenthal P. R., 2011, "Learning, Unlearning, and Relearning: Using Web 2.0 Technologies tu Supportthe Development of Lifelong Learning Skills", In Magoulas G. D., E-Infrastructures and Technologies forLifelong Learning: Next Generation Environments, s.292-315

EVERSON M., Gudlach E., Miller J., 2013, "Social Media and the Introductory Statisrics Course", Computer in Human Behavior 29, A61-A81

EXAMINER, 2013, http://www.examiner.com/article/social-media-vs-social-networking-what-s-the-difference, (10.08.2013)

FACEBOOK, 2013a, "Facebook Hak ve Sorumluluklar Bildirimi", https://www.facebook.com/legal/terms, (17.07.2013)

FACEBOOK, 2013b, https://www.facebook.com/about/privacy/your-info, (17.07.2013)

FACEBOOK, 2013c, https://www.facebook.com/, (15.07.2013)

FACEBOOK, 2013d, Facebook Reports First Quarter 2013 Results, http://investor.fb.com/releasedetail.cfm?ReleaseID=761090, (08.07.2013)

FACEBOOK, 2013e, https://www.facebook.com/business/overview, (27.07.2013)

FACEBOOK, 2013f, https://www.facebook.com/about/government_requests (27.07.2013)

FBI, 2013, http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks, (20.07.2013)

FEDERAL TRADE COMMISION, 2013, Monitoring Software on Your PC Staff Report

FENAFiL, 2013, http://fenafil.com/hukuk/internet/kisisel_veriler.htm, (15.07.2013)

FERRITER W. H., 2010, "Digitally Speaking", Educational Leadership, 68, s.87-88

FLICKR, 2013, http://www.flickr.com/about/, (13.08.2013)

F-SECURE, 2011, http://safeandsavvy.f-secure.com/2011/01/20/how-to-protect-from-malware/, (01.20.2011)

GANTEP, 2013, "Popüler Siteleri ve Ağları Ücretsiz Kullanarak Aslında Neleri BaştanKabulEdiyorsunuz?", http://gul6.bim.gantep.edu.tr/~bidb/index.php?option=com_content&view=article&id=205%3A2013-01-15-09-16-02&catid=18%3Ahaberler&Itemid=26&lang=tr, (17.07.2013)

GAO (U.S.Government Accountability Office), 2008, Alternatives Exist for Enhancing Protection of Personally Identifiable Information

GİTTİGİDİYOR, 2013, http://yardim.gittigidiyor.com/sozlesmeler-kurallar/gizlilik-politikasi, (03.07.2013)

GLOBALWEBINDEX, 2013, "StreamSocial Q1 2013: Facebook Active UsageBooms", https://www.globalwebindex.net/Stream-Social, (09.07.2013)

GOOGLE, 2013a, "Google Gizlilik Politikası", https://www.google.com.tr/intl/tr/policies/privacy/, (17.07.2013)

GOOGLE, 2013b, URL Shortener http://goo.gl/, (09.06.2013)

GOLA Peter, Rudolf SCHOMERUS, 2007, Bundesdantenschutzgesetz Kommentar, Verlag C., H. Beck, 9. Basım, Almanya

GROWINGSOCIALMEDIA, 2013, Social Media Statistics and Facts of 2013", http://growingsocialmedia.com/social-media-statistics-and-facts-of-2013-infographic/, (08.07.2013)

GUARDIAN, Facebook and Bebo risk 'infantilising' the human mind, http://www.guardian.co.uk/uk/2009/feb/24/social-networking-site-changing-childrens-brains, (20.07.2013)

GUNTER Ollman, 2004, The Phishing Guide - Understanding and Preventing Phishing Attacks. White Paper, Next Generation Security Software Ltd.

HAVERBACK Heather Rogers, 2009, "Facebook: Uncharted territory in a reading education classroom", Reading Today, Sayı 27, s. 34

HEIDEMANN J., Klier M., Probst F., 2012, "Online Social Networks: A Survey of a Global Phenomenon", Computer Networks 56, s.3866-3878

HOWSECUREISMYPASSWORD, 2013, https://howsecureismypassword.net/, (04.06.2013)

HUKUKTABİLİŞİM, 2013, Kişisel Verilerin Korunması Kanun Tasarısı Neleri Düzenliyor?, http://hukuktabilisim.blogspot.com/2013/02/kisisel-verilerin-korunmas-kanun-tasars_4.html, (17.06.2013)

IETF, 2013a, RFC 781, https://tools.ietf.org/html/rfc781, (07.06.2013)

IETF, 2013b, RFC 1034, https://tools.ietf.org/html/rfc1034, (07.06.2013)

ITNEWSAFRICA , 2013, http://www.itnewsafrica.com/2013/07/social-networking-poses-security-threats/, (13.07.2013)

JOOMLA, 2013, http://www.jt.gen.tr/makaleler/haberler/guvenlik/saldirilar/9-cross-site-scriting-attack.html, (16.07.2013)

KALKINMA BAKANLIĞI, 2013, Bilgi Güvenliği, Kişisel Bilgilerin Korunması ve Güvenli Internet Ekseni Küresel Eğilimler ve Ülke İncelemeleri Raporu

KAYA Cemil, 2005, İdare Hukukunda Bilgi Edinme Hakkı, Seçkin Kitapevi, Ankara

KILINÇ Doğan, 2012, Ankara Üniversitesi Hukuk Fakültesi Dergisi cilt 61,sayı 3, sayfa 1089-1169 http://dergiler.ankara.edu.tr/dergiler/38/1690/18020.pdf, (11.08.2013)

KOÇ Serhat, Selva Kaynak, 2010, Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet Ve Kişisel Güvenlik, XII Akademik Bilişim Konferansı Bildirileri

KUMARAGURU P., Y.W. Rhee, A. Acquisti, L. Cranor, J. Hong, E. Nunge, 2007, Protecting People from Phishing: The Design and Evolution of an Embedded Training E-mail System, , CyLab Carnegie Melon University

KÜZECİ Elif, 2010, Kişisel Verilerin Korunması, Turhan Yayımevi, Ankara

LEGISLATION, 2013, http://www.legislation.gov.uk/ukpga/1984/60/section/12, (23.06.2013)

LI Y. M., Hsiao H. W., Lee Y. L., 2013 , "Recommending Social Network Applications via Social Filtering Mechanisms", Information Sciences 239, s.18-30

LONSCOHEN, 2013, http://lonscohen.com/blog/2009/04/difference-between-social-media-and-social-networking/, (12.08.2013)

MARKETINGLAND, 2013, The Landscape of Social Login & Sharing: Consumers Want, http://marketingland.com/gigya-only-2-percent-of-social-sharing-happens-on-google-52184?utm_campaign=tweet&utm_source=, (20.07.2013)

MERWE Van der, A J, Loock, M, Dabrowski, M., 2005, Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town.

MICROSOFT, 2013, http://www.microsoft.com/security/online-privacy/passwords-create.aspx, (10.07.2013)

MİLLİYET, 2013, http://gundem.milliyet.com.tr/gostericiler-zello-ile-telsiz/gundem/detay/1719532/default.htm, (04.08.2013)

MONİTERA, 2013, "2013 Twitter Türkiye Profili", http://blog.monitera.com/, (09.07.2013)

MURRAY K. E.,Waller R., 2007, "Social Networking Goes Abroad", International Educator, 16(3), s.56-59

NEDİYOR, 2013, Facebook ve Twitter'dan Gezi Açıklaması, http://nediyor.com/2013/06/1379343/, (27.06.2013)

NETWORKWORLD, 2013a, 5 Top Social Security Threads http://www.networkworld.com/news/2011/053111-social-media-security.html, (15.07.2013)

NETWORKWORLD, 2013b, Social Media Security Threads Taken Too Lightly http://www.networkworld.com/news/2011/012011-social-network-security.html, (24.07.2013)

NIST, 2010, Guide to Protecting the Confidentiality of Personally Identifiable Information, Special Publication 800-122

Nİ Y., Xie L., Liu Z. Q., 2010, Minimizing the expected complete in fluence time of a social network, Information Sciences 180, s.2514–2527

ONAT Ferah, Alikılıç özlem, 2008, http://journal.yasar.edu.tr/wp-content/uploads/2012/05/no9_vol3_09_onat_alikilic.pdf, (13.08.2013)

ONGUARDONLINE, 2013, http://www.onguardonline.gov/, (11.06.2013)

PEWINTERNET, 2013, http://www.pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy/Main-Report/Part-2.aspx, (22.07.2013)

PLA (Prostitution Licensing Authority), 2013, http://www.pla.qld.gov.au/reportsPublications/ipp/what.htm, (15.07.2013)

QUINTLY, 2013, Facebook Country Statistics March 2013 – Top 10 Countries And A Comparison Of The U.S. And Brazil, http://www.quintly.com/blog/2013/03/facebook-country-statistics-march-2013/, (03.07.2013)

SABAH, 2012, "İşte Türkiye'nin Twitter istatistikleri", http://www.sabah.com.tr/Teknoloji/Haber/2012/03/16/iste-turkiyenin-twitter-istatistikleri, (16.03.2012)

SHIFLETT, 2013, http://shiflett.org/articles/cross-site-request-forgeries, (02.07.2013)

SLIDESHARE, 2013, http://www.slideshare.net/femiral/kiisel-verilerin-korunmas-ve-hasta-verilerinin-gvenlii, (16.07.2013)

SOCIALMEDIATODAY, 2013, http://socialmediatoday.com/index.php?q=SMC/194754, (14.08.2013)

SOPHOS Social Networking Security Thread, 2013a, http://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats.aspx, (14.06.2013)

SOPHOS Social Networking Security Threads, 2013b, http://www.sophos.com/en-us/security-news-trends/security-trends/social-networking-security-threats/protection-strategies.aspx, (14.06.2013)

SOSYAL MEDYA KULÜBÜ, 2013, http://sosyalmedya-tr.com/sosyalmedya/instagram-nedir-nasil-kullanilir.html, (04.08.2013)

SQUIRRELMAIL, 2013, http://squirrelmail.org/, (27.06.2013)

STATISTICBRAIN, 2013a, "Twitter Statistics", http://www.statisticbrain.com/twitter-statistics/, (02.05.2013)

STATISTICBRAIN, 2013b, "Youtube Statistics", http://www.statisticbrain.com/youtube-statistics/, (02.05.2013)

STUFF, 2013, Twitter Hükümetin Gezi Taleplerini Reddetti, http://www.stuff.com.tr/2013/06/twitter-hukumetin-gezi-taleplerini-reddetti.html, (27.06.2013)

SYMANTEC Internet Security Thread Report, Volume 18, April 2013

ŞAHİN Osman, 2011, Elektronik haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğinin Korunması, BTK Uzmanlık Tezi, Ankara

TBMM, 2013a, 5237 sayılı Türk Ceza Kanunu, http://www.tbmm.gov.tr/kanunlar/k5237.html

TBMM, 2013b, Kişisel Verilerin Korunması Kanunu Tasarısı, http://www2.tbmm.gov.tr/d23/1/1-0576.pdf

TBMM , 2013c, Türkiye Cumhuriyeti Anayasası http://www.tbmm.gov.tr/anayasa.htm, (09.04.2013)

TECHNOPAT, 2013, http://www.technopat.net/2013/01/20/google-chrome-milliyete-erisimi-engelledi/, (13.08.2013)

TECHREPUBLIC, 2013, http://www.techrepublic.com/blog/security/what-is-cross-site-scripting/426, (13.08.2013)

THENEXTWEB, 2013, "Studyshowsthatonly 27% of Twitter userstweetedduring a 3 monthperiod", http://thenextweb.com/socialmedia/2012/01/31/study-shows-that-only-27-of-twitter-users-tweeted-during-a-3-month-period/, (09.07.2013)

TİB, 2013a, http://www.tib.gov.tr/tr/tr-menu-30-erisimin_engellenmesi.html (30.10.2013)

TİB, 2013b,

http://www.tib.gov.tr/tr/tr-menu-47-

internet_icerik_duzenlenmesi_hakkindaki_sorular.html (30.10.2013)

TÜBİTAK, 2013, Bilim ve Teknik Dergisi, Sayı 544, s.17, Ankara

TÜRKİYE, 2013a, https://www.turkiye.gov.tr/bilgilendirme?konu=siteHakkinda, (08.5.2013)

TÜRKİYE, 2013b, https://www.turkiye.gov.tr/adli-sicil-kaydi, (08.05.2013)

TWITTER, 2013a, "Twitter Privacy Policy", https://twitter.com/privacy, (18,06.2013)

TWITTER, 2013b, https://twitter.com/tos, (18.06.2013)

TWITTER, 2013c, https://twitter.com/, (18.06.2013)

VASALOU A.,Joinson A. N., Couvisier D., 2010 ,"Cultural Differences, Experince with Social Networks andthe Nature of 'True Commitment' in Facebook", Human-ComputerStudies, 68, 719-728

VISUAL, 2013, "10 Amazing LinkedIn Statistics For 2013", http://visual.ly/10-amazing-linkedin-statistics-2013, (09.07.2013)

WSJ (Wall Street Journal), 2013, http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html, (26.07.2013)

YAVANOĞLU Uraz, Sağıroğlu Şeref, 2010, "Sosyal Ağlar ve Bilgi Güvenliği", 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Türkiye, Mayıs 2010

YAVANOĞLU Uraz, Sağıroğlu Şeref ve Çolak İlhami, 2012, Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler, Politeknik Dergisi, Cilt 15, Sayı 1

YOUTUBE, 2013, "Youtube Statistics", http://www.youtube.com/yt/press/statistics.html, (09.07.2013)

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 Bilgi Teknolojileri ve İletişim Kurumu Meslek Personeli Sınav, Görev, Çalışma Usul ve Esasları Hakkında Yönetmeliğe uygun olarak hazırladığımı belirtir, bunu onurumla doğrularım.

Bilgi Teknolojileri ve İletişim Kurumu 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.

Binnur GÜRSES

ÖZGEÇMİŞ

1968 yılında Ankara'da doğdu. İlkokul, orta ve lise öğrenimini Ankara'da tamamladı. Telsiz Genel Müdürlüğü'nün açmış olduğu sınavı kazanarak 1987 yılında çalışma hayatına başladı. Anadolu Üniversitesi İktisadi İdari Bilimler Fakültesi İktisat Bölümü'nden mezun oldu. Kuruluşundan itibaren Bilgi Teknolojileri ve İletişim Kurumu'nda çalışmaya devam etti. 2009 yılında şef kadrosuna atandı. Halen Tüketici Hakları Dairesi Başkanlığına bağlı Tüketici ile İlişkiler Müdürlüğü'nde bu görevi sürdürmekte olup; evli ve iki çocuk annesidir.