Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

GÜVENLİ İNTERNET MERKEZİ

Bilgi Teknolojileri ve İnternetin Bilinçli, Güvenli Kullanımı

Bilgi Teknolojileri ve İletişim Kurumu

İnternet Daire Başkanlığı

İçindekiler

ÖNSÖZ

Bilgi ve iletişim teknolojileri dijital çağın şüphesiz en önemli aracı haline gelmiştir. Özellikle iletişim teknolojilerinin geldiği nokta, dünyanın dört bir yanındaki vatandaşlar üzerinde olağanüstü bir etkisi olmuş, iletişim hatları; inovasyon, büyüme ve yeni iş modellerinin gelişmesine katkı sağlamıştır.

Fırsatlarıyla tehditleriyle içinde bulunduğumuz dönem artık dijital çağ dönemidir. Bilgi ve teknoloji çağında Endüsri 4.0, nesnelerin interneti, yapay zekâ ve inovasyonun konuşulduğu bir ortamda iletişim tam da merkezde yer almaktadır. İletişim tüm bu teknolojilerin birbirleri ile haberleşmesi, veri gönderimi, bilgi edinimi ve paylaşımı gibi teknoloji odaklı tüm faaliyetlerin merkezinde yer almaktadır.

İletişim teknolojileri içinde en önemli araç olan internet, dünyanın dört bir yanındaki insanlar üzerinde olağanüstü bir etkiye sahiptir. Bununla birlikte internet, insanların haberleşmesine ve kendilerini ifade etmelerine olanak vermesi nedeni ile de yaşam özgürlüğünün vazgeçilmez bir parçası haline gelmiştir. Dünyanın herhangi bir yerinde, bir insanın akıllı telefon ve internet bağlantısı ile kendi işini kurmasına ve dünyanın dört bir yanından insanlarla iletişime geçmesine olanak sağlamıştır.

İletişim teknolojilerindeki sürekli inovasyon şüphesiz tüm dijital vatandaşların ortak çalışmaları ile ortaya çıkmaktadır. Elektronik haberleşme araçlarında ülke genelinde hizmetlerin yaygınlaştırılması, kaynakların etkin ve verimli kullanılması, rekabetin tesisi ve bu konuda tüketici haklarının korunması devletlerin öncelikli sorumluluğu altındadır. Ayrıca tüm vatandaşlar tarafından erişilebilir, önceden belirlenmiş kalitede ve herkesin karşılayabileceği makul bir bedel karşılığında asgari standartlarda sunulacak olan internet erişimi de dâhil tüm elektronik haberleşme hizmetleri birer evrensel hizmet olarak tanımlanmıştır.

İnternet teknolojileri ve internet ile ilgili çalışma alanları oldukça geniştir. İnternet ile ilgili başlıklar spesifik bir disiplinin konusu olmaktan uzak disiplinler arası bir konudur. Bununla birlikte fırsatlarıyla tehditleriyle, yeni trendleri ve yaklaşımlarıyla, haklarıyla sorumluluklarıyla internet, bilişim uzmanlarından sağlık çalışanlarına, eğitimcilerden psikologlara kadar her branştan insanın katkılarıyla şekillenecek bir çalışma alanıdır.

Yapılan bu çalışmayla, yeni nesil internet teknolojilerinden internetin getirdiği fırsatlara, internette hak ve sorumluluklardan internet güvenliğine, internet bağımlılığından internet hukukuna varıncaya kadar internetin birçok yönü incelenmeye çalışılmıştır. Bu kitabın okuyucular ve kitaptan faydalanmak isteyen değerli araştırmacılar için yararlı olması en büyük dileğimizdir. Kitapla ilgili görüş ve önerileriniz de bizim için oldukça değerlidir. Bu yüzden olabilecek katkılarınız için şimdiden teşekkürü bir borç bilir, kitap içeriğinin herkese faydalı olmasını temenni ederiz.

BÖLÜM 1 İNTERNETTE AR-GE VE İNOVASYON

İçindekiler

Ar-ge ve inovasyon kavramları sıklıkla kullanılan kavramlar olmakla birlikte internette ar-ge ve inovasyon çok bilindik veya kullanılan bir tabir değildir. Oysa internet yapısı gereği sürekli değişen, yenilenen ve yeni fonksiyonların kazandırıldığı sistemler bütünüdür. Bir sene içerisinde en çok yenilenen teknolojiler sıralanmış olsa, internet teknolojileri en üst sıralarda kendine yer edinirdi. Artık internetin hızına hem altyapı hem içerik olarak erişmek oldukça zordur. Bu yüzden ar-ge ve inovasyon çalışmalarının en büyüğü aslında internet ortamında gerçekleştirilmektedir. Bu bölümde internetin kısa tarihi içerisinde, nereden nereye geldiği özetlenerek bu ekosistem içerisinde internetin fırsatları ve faydalarından bahsedilmeye çalışılacaktır.

1. İnternet Tarihi ve İnternetle İlgili Kavramlar

Bu bölümde internetin kısa tarihi içende ne gibi aşamalardan geçtiği özetlenecek internet deyince akla gelen kavramlardan bahsedilmeye çalışılacaktır.

1.1. İnternetin kısa tarihi

İnternet içinde bulunduğumuz dijital çağın vazgeçilmez bir aracı haline gelmiştir.1969 yılında çeşitli bilgisayar ve askeri araştırma projelerini desteklemek için Amerika Savunma Bakanlığı ARPANET (Gelişmiş Araştırma Projeleri Dairesi Ağı) adında paket anahtarlamalı bir ağ tasarlamaya başladığı zamandan Türkiye'de 1986 yılında ilk geniş alan ağı TÜVEKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) kurulmasına kadar geçen süre, internetin gelişimine giden yolda başlangıç aşamalarını oluşturmuştur. 1990'lı yıllara gelindiğinde ARPANET yerini World Wide Web'e bırakmıştır. İlk web sitesi Tim Berners Lee tarafından tek sayfada internetin ne olduğu ve nasıl kullanılacağını anlatması ile oluşturulmuştur.

1991 yılında ODTÜ-TÜBİTAK işbirliğiyle kurulan TR.NET ilk internet servis sağlayıcı olarak, ICANN (İnternet Tahsisli Sayılar ve İsimler Kurumu) ve ODTÜ ".tr" alan adı dağıtımına başlamıştır. 1992 yılında Hollanda'ya ilk deneysel bağlantı gerçekleştirilmiştir. 1993 yılında ODTÜ'den 64Kbps kapasiteli ilk internet bağlantısı gerçekleştirilmiştir. Türkiye'nin internete resmi bağlantısı ise Nisan 1993'te başlamıştır. 1994 yılında Ege Üniversitesi'nden internet bağlantısı gerçekleştirilerek, kurumlara ve firmalara ilk internet hesapları verilmeye başlanmıştır. 1995 yılında Bilkent ve Boğaziçi Üniversiteleri internet ağına bağlanan diğer üniversiteler olmuştur. 1996 yılında İstanbul Teknik Üniversitesi de internet ağına dâhil olmuştur. Yine bu tarihte Türkiye'nin ilk internet altyapısı olan TURNET oluşturulmuştur. 1997 yılında akademik kuruluşların internet bağlantısını sağlayan omurga olan ULAKNET (Ulusal Akademik Ağ) oluşturulmuştur. 1998 yılında Ulaştırma Bakanlığı bünyesinde İnternet Üst Kurulu kurulmuştur. 1999 yılında TTNET, TURNET'in yerini alarak internet omurgasını oluşturdu. 2000 yılına kadar geçen süre içerisinde Türkiye'de internetin özellikle üniversitelerde kullanıldığı ve internet altyapısının Türkiye'de oluşturulmaya başlandığı gözlenmiştir.

Bununla birlikte, dünyada 1972 yılında ilk e-posta alınmıştır. 1981 yılında IBM ilk kişisel bilgisayarı tanıttı. 80'li yıllar dünyada internetin gelişiminde teknik altyapının güçlendirilmesi (TCP (İletim Kontrol Protokolü)/IP (İnternet Protokolü) protokolünün oluşturulması, DNS Sisteminin kurulması, ilk alan adının alınması) ile devam etmiştir.

1.2. İnternet teknolojileri ile ilgili kavramlar

İnternet bağlantısının kurulması ile birlikte çevrimiçi teknolojiler hayatımıza girmeye başlamıştır. Çevrimiçi (web) teknolojiler, internetin getirmiş olduğu yeniliklerle birlikte 1990'lı yılların başından itibaren yaşamımızda yer edinmeye başlamıştır. 2000'li yılların başına kadar çevrimiçi teknolojileri kullanarak çeşitli kurum ve kuruluşlar, şirketler, belediyeler, devletler, üniversiteler ve diğer organizasyonlar kendilerini dijital ortama taşımaya başlamışlardır.

İlk aşamada temel amaç, tüm evrene oluşturulan içerikleri sunmaktı. Bu içerikler HTML (Köprü Metni Biçimlendirme Dili) ve HTTP (Hiper Metin Aktarım Protokolü) gibi birtakım teknolojiler vasıtasıyla çevrimiçi ortama aktarılmaya başladı. 1991 senesinde HTML ve HTTP ile birlikte kısa adı WWW (World Wide Web) olan ve çevrimiçi ortamda oluşturulan bu içeriklerin bir sayfa olarak görüntülenmesini sağlayan bir servis teknolojisi doğmuştur. 1993 yılında Mosaic ve 1994 yılına gelindiğinde "Netscape Communications Corporation" firmaları tarafından üretilen, şimdi AOL firması tarafından geliştirilen Netscape internet tarayıcısı hizmet vermeye başlamıştır. Tarayıcılar, web sayfalarını incelemek ve web sayfaları arasında gezinebilmek için gerekli olan programlara verilen genel ad olup, HTML tabanlı yazılan ve içeriğinde bilgiler bulunduran sayfaların bir ağ sunucusuna internet vasıtasıyla bağlanarak ulaşıp açılmasını sağlayan yazılımlar olarak hizmete başlamıştır. Sonra da sırasıyla Opera ve Internet Explorer tarayıcıları geliştirilmiştir.

1990'lı yılların ortalarından 2000'li yılların başlarına kadar çevrimiçi içerikler sırasıyla HTML 2, çerezler, SSL, HTML 3, Javascript, Java, Flash, XML, HTML 3.2, HTML 4, CSS ve HTLML 5 gibi web teknolojileri ile geliştirilmeye devam edilerek kullanıcılara sunulmuştur. Bu teknolojiler internet sayfalarını daha sistematik ve görsel yanı güçlü hale getirmiştir.

2. Dünden Geleceğe İnternet

İnternet sürekli değişen ve yenilenen bir teknoloji özelliğine sahiptir. İnternet kısa sürede önceden öngörülemeyen bir noktaya gelmiştir. Bundan sonraki süreçte, internet teknolojilerinin hangi yöne evirileceğini kestirmek oldukça zordur. Dünden bugüne internet, bir tarih olmakla birlikte bugünden geleceğe internet, sadece bir tahmin olabilecektir. Çünkü internet ile ilgili kavramlar, kullanılan teknoloji, sosyal ağlar veya sosyal beğeniler çok kısa bir süre öncesine kadar hayatımızda değildi. Çok alışılagelmiş gibi durumlar aslında tarih içerisinde çok küçük bir bölüm veya anı kapsamaktadır. Bu yüzden internet başlı başına bir devrim olarak nitelendirilebilir.

2.1. Dünden bugüne internet

İnternet tabanlı çevrimiçi teknolojiler kısa bir zaman içinde büyük değişim ve yenileşime girmiştir. İlk defa 2004 yılında isminden bahsedilmeye başlayan web 2.0 teknolojileri ile internet teknolojileri kendi içinde dönemlere ayrılmaya başlamıştır. 90'lı yıllarda sadece durağan internet siteleri ile tek taraflı bilgi akışı sunulurken; 2000'li yıllarla birlikte etkileşimli ve herkesin içerik oluşturabildiği web 2.0 teknolojileri ortaya çıkmaya başlamıştır (Şekil-2).

2000'li yıllar ile birlikte internet kullanıcıları Web 2.0 teknolojisi ile tanışmaya başlamıştır. Web 2.0 teknolojisi ile web platformunda sadece içeriklere ulaşmak değil o içerikleri yönetmek, değiştirmek, ekleme yapmak veya silmek gibi aktivitelerin yanında tamamen yeni içerikler geliştirme imkanı da kullanıcılara sunulmaya başlamıştır. Kişisel web sayfalarında oluşan bloglar, içerik yönetimi sistemi sağlayan wiki'ler, kullanıcıların fotoğraflarını milyonlarca kullanıcı ile buluşturan Flickr, yine kullanıcıların başka kullanıcıların bilgisayarlarındaki içerikleri indirmelerine olanak tanıyan P2P (Peer to Peer –Eşten eşe) programları gibi servisler web 2.0 teknolojilerine geçişi hızlandırmıştır.

Web 2.0 teknolojileri sosyal ağlar ile daha da boyut değiştirmeye başlamıştır. 1997 yılında Six.Degrees.com sosyal ağının kurulmasının ardından bunu Livejournal, Friendster, Myspace gibi popüler sosyal ağlar izlemiştir ve son olarak 2004 yılında kurulan Facebook çok kısa zamanda büyük bir kullanıcı kitlesine ulaşmıştır.

Web 2.0 teknolojileri özellikle sosyal iletişim olarak adlandırılan MySpace ve Facebook gibi daha çok arkadaş ve akraba arama ve onlarla iletişim kurma platformlarının doğmasına sebep olmuştur. 2000'li yıllardan 2010'lu yıllara geçerken sosyal iletişim mantığı ile kurulan sosyal ağlar, sosyal medya platformlarına kaymaya başlamıştır. Böylece kapalı gruplar arasındaki iletişim birden hiç tanımadığımız bir insanın bile paylaşımını görebilme imkânını doğuran sosyal medya platformlarına evrilmeye başlamıştır (Şekil-1).

Şekil 1 – Web Teknolojilerinin Gelişimi

Web 1.0	Web 2.0
Statik bannerlar.	Sitedeki içeriğe göre reklam gösteren hizmetler (Google AdSense).
Fotoğraflarınızı sadece kendi kullanımınız için depolayabileceğiniz hizmetler (Ofoto).	Fotoğraflarınızı milyonlarca kullanıcı ile paylaşabileceğiniz hizmetler (Flickr).
Belirli sunucuları kullanarak erişime olanak tanıyan dosya depolama servisleri (Akamai).	Kullanıcıların başka kullanıcıların bilgisayarlarındaki içerikleri indirmelerine olanak tanıyan servisler (Bittorrent).
Belirli listelerden mp3 indirmenizi sağlayan web siteleri (mp3.com).	Şarkı ya da şarkıcı adını aratarak farklı platformlardan mp3 indirmenizi sağlayan servisler (Kazaa, Napster, Emule vb.).
Ansiklopedik bilgi içeren siteler (Britannica Online).	Ansiklopedik bilginin kullanıcı katkılarıyla aşamalı bir şekilde oluşturulduğu siteler (Wikipedia).
Kişisel web sayfaları.	Bloglar.
Akılda kalıcı domain adları seçmek.	Arama motorlarına uygunluğa dikkat etmek.
Reklamlarda sayfa görüntüleme sayısının önemli olması.	Reklamlara tıklama sayısının önemli olması.
İçerik yönetim sistemleri.	Wikiler.
Klasör tabanlı dizin yapıları (taxonomy).	Anahtar kelime tabanlı etiket yapıları (tagging, folksonomy).

Şekil 2 – Web 1.0 ile Web 2.0 Arasındaki Farklar (Kaynak: Durusoy, 2011)

2.2. Bugünden geleceğe internet

İnternet teknolojileri sürekli bir gelişim içindedir ve bu gelişimin sürekli olarak devam etmesi beklenmektedir. Gelecekte nasıl bir internet teknolojisinin bizleri beklediğini kestirmek ise zordur; ama bu konuda bazı tahminler ve teknolojinin seyri bazı ipuçlarını da beraberinde getirmektedir.

Tek yönlü bilgi akışı sunan web 1.0 ile etkileşimli bir bilgi akışı sunan web 2.0'dan sonra web 3.0 ve hatta web 4.0 teknolojilerinden bahsedilmeye başlanmıştır.

Web 3.0 ile internete bağlanan makinelerin daha da akıllı hale gelmesi öngörülmektedir. Nesnelerin interneti ve yapay zeka teknolojilerinin doğuşu bunun en belirgin

örneğidir. Teknolojik cihazların akıllanması söylemi her ne kadar mecazi bir anlam ifade ediyor olsa da, internet platformları aracılığıyla kullanıcılardan artık birçok veri toplanmaktadır. Bu da büyük veri olarak ifade edilen başka bir kavramın doğmasına sebep olmuştur. Büyük veri ile kullanıcı davranışları daha da anlamlandırılabilmektedir. Bu da pazarlamadan imalat teknolojisine kadar birçok sektörde değişimin yaşanacağının bir göstergesidir.

Web 4.0 ise web 3.0'ın devamı olarak düşünülebilir. İnternetin akıllı cihazlar yaratmasının yanında artık tüm iş ve işlemlerde yeni web teknolojilerinin her alanda etkin rol oynayacağı öngörülmektedir. Bu durum her şeyin sanallaşacağını, birçok eylemin internet üzerinden gerçekleştirileceğini göstermektedir. Bununla birlikte, yapılan birçok aktivenin gerçek zamanlı olarak sanal ortamda da yapılabileceği tahmin edilmektedir.

Web 3.0 ve web 4.0 kısaca; akıllı robotlar, kişiye özel internet içeriği, kişiyi daha yakından tanıyan makineler ile şu an internette yapılamayan ama kısa zamanda yapılabilir olacak birçok aktiviteyi de kapsamaktadır.

3. İnternet Kaynakları ve Yönetimi

İnternetin tarihi ve geleceği ile birlikte diğer önemli bir konu, internet kaynakları ve bu kaynakların yönetimi mevzusudur. Hem altyapı hizmetleri hem de internet erişiminin sağlanabilmesi için gerekli protokoller, tahsisler ve teknolojiler ile birlikte internet içeriği de bu kaynakların bir bileşenidir diyebiliriz.

3.1. İnternet yönetişimi

İnternet yönetişimi kavramı, Birleşmiş Milletler (BM) himayesinde internetin bütün yönleriyle işbirliğine dayalı, çok paydaşlı ve katılımcı bir politika oluşturabilmesi amacıyla 2006 yılında başlatılan ve her sene düzenlenen İnternet Yönetişim Forumu (Internet Govarnance Forum – IGF) ile daha fazla gündeme gelmeye başlamıştır. Yine, BM himayesinde ve BM'ye bağlı Uluslararası Telekomünikasyon Birliği (ITU)'nin öncülüğünde ilki 2003 yılında Cenevre'de gerçekleştirilen Dünya Bilgi Toplumu Zirvesi (World Summit on Information Society-WSIS) internetin geleceği ile ilgili birçok alt başlığı tartışmaya açmış; fakat söz konusu zirvede tam bir uzlaşma sağlanamamıştır. Bununla birlikte, zirveden çıkan önemli bir karar, işbirliği ve diyaloğun sürdürülmesi ve İnternet Yönetişimi Çalışma Grubu'nun (Working Group on Internet Governance -WGIG) kurulması kararı olmuştur (WSIS-03/GENEVA/DOC/5-E).

WGIG internet yönetişimini, internet kullanımı ile ilgili ilke, norm, kurallar ile tüm bu süreçlerin uygulanmasında çeşitli programların geliştirilmesi ve uygulanması olarak tanımlamıştır. Bu çerçevede yönetişim, hem internetin altyapı seviyesinde yönetimi hem de başta bu altyapının geliştirilmesi ile içerik yönünden güvenli, doğru ve yenilikçi bir şekilde kullanımı ile ilgili tüm aşamaları kapsamaktadır. Bu doğrultuda WGIG, 4 ana başlıkta 'internet yönetişim politikaları' belirlemiştir. Bunlar:

1) **İnternet ve Kritik Altyapıların Yönetimi:** Başta alan adları ve IP (Internet Protocol)'lerin tahsisi ve kök sunucu-

ların yönetimi olmak üzere spesifik teknik düzenlemeleri kapsamaktadır.

2) **İnternetin Güvenli Kullanımı:** Siber güvenlik ve kritik altyapıların korunması başta olmak üzere internet ve ağ güvenliği ile ilgili başlıkları kapsamaktadır.

3) **İnternet Kullanımının Yaygınlaştırılması:** İnternette bilginin serbest bir şekilde akması ve kullanıcı verilerinin çevrimiçi ortamda korunumu dengesinde, dijital ortamın e-ticaret ve e-devlet gibi daha rekabetçi ve daha yenilikçi sistemlerle kullanımının sağlanması hedeflenmektedir.

4) **İnternet Kaynaklarının Geliştirilmesi:** Ülkelerin kaynak politikalarını doğru koordine ederek internetin gelişimine evrensel hizmet kapsamında destek sağlanması gerekmektedir.

3.2. İnternet altyapısının yönetimi

İnternet, yerel bilgisayarların birbirlerine bağlanabildiği ve haberleşebildiği; bu haberleşmenin açık ağ mimarisinde TCP/IP olarak standart sunulan bir protokol eşliğinde verilerin iletilerek yapılabildiği küresel bir şebeke olarak teknik yönden tanımlanabilmektedir. İnternete bağlanan her cihaza belirli bir sistematik dâhilinde kendine has bir numaralandırma sistemi olan IP adresi (Internet Protocol Address) verilmekte ve yerel bilgisayarlar bu adresler aracılığıyla birbirleriyle haberleşebilmektedirler.

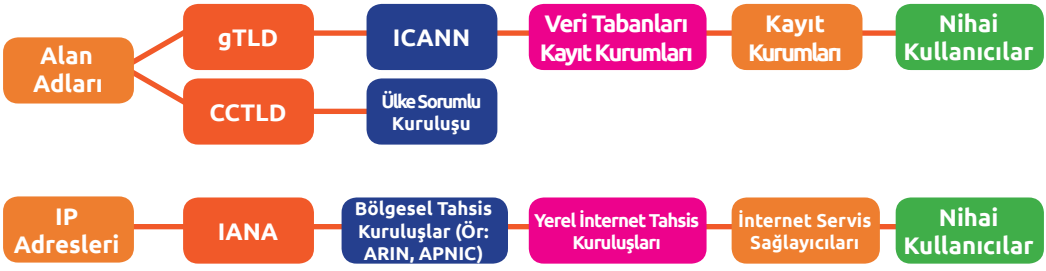
TCP/IP protokolü üzerinde gerçekleşen veri iletişimi ile birlikte internetin birçok ses, veri iletişimi ve dosya paylaşımı gibi özel protokolleri de destekleyebilen bir platform ile arkasında büyük bir ağ mimarisi barındırıyor olması, internet yönetişiminin önemini daha da artırmaktadır.

İnternetin mucidinin veya sahibinin kim olduğuna dair efsanevi sorular yıllardır gündeme gelmektedir. İnternet ağını tek başına yaratabilecek, genişletebilecek veya kontrol edebilecek bir güç yoktur. İnternetin yönetimi ve işlerliği büyük bir işbirliği içerisinde sağlanmaktadır. Aynı zamanda internetin belirli prosedürler çerçevesinde kullanımının sağlanması amacıyla yetkilendirilmiş birkaç kurum mevcuttur. Bunlardan en önemlisi 1998 yılında alan adlarının ilgililere tahsisi ve dağıtımının koordinasyonunun sağlanması amacıyla yetkilendirilmiş İnternet Tahsisli Adlar ve Sayılar Kurumu (Internet Corporation for Assigned Names and Numbers - ICANN)'dur. Bu yetkilendirme ile birlikte internet yönetişimi gündeme gelmeye başlamış; daha sonraları internetin getirmiş olduğu yenilikler ve web 2.0 teknolojileri ile birlikte internetin altyapısı yanı sıra sosyo-kültürel, ekonomik ve teknolojik yönden de yönetişimi önem kazanmaya başlamıştır.

ABD'de faaliyetlerine başlayan ICANN'in temel görevleri, IP adreslerinin tahsisinin koordinasyonunu sağlamak, protokol tanımlayıcıları atamasını yapmak, Genel Üst Düzey Alan (gTLD) ve Ülke Kodu Üst Düzey Alan (ccTLD) ad sunucuları ile kök sunucuların kontrolünü sağlamak olarak tanımlanmıştır. Yine ICANN ile koordinasyon içerisinde çalışan İnternet Tanım-

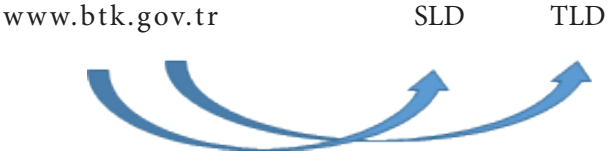
lanmış Sayılar Otoritesi (IANA - Internet Assigned Numbers Authority) mevcuttur.

IANA, ABD'de internetin özerk bir yapıda devletten bağımsız bir yapıda çalışabilmesi amacıyla ABD Ticaret Bakanlığı tarafından yetkilendirilmiş ve daha sonraları ICANN ile birlikte koordineli bir şekilde çalışmalarına devam etmiştir. IANA, IP yönetimi ile ilgili politikaları tarafsız bir şekilde yürütmekle ve IP numaralarının tahsisini yapmakla görevlidir. IP adreslerinin tahsislerinde ise IANA koordinasyonunda çeşitli kıta ve bölgelerde kurumlar yetkilendirilmiştir. Örneğin Amerika'da ARIN (American Registry for Internet Numbers) ve Asya'da APNIC (Asia Pacific Network Information Centre) gibi kuruluşlar vasıtasıyla IP numaralarının tahsisi yerel kurumlara yapılabilmektedir (Şekil-3).



Şekil 3 - Alan Adları ve IP Tahsis Prosedürü

İnternet alan adları birinci (TLDs) ve ikinci (SLDs) derece alan adlarından oluşmakta olup birinci derece alan adları ülke kodu içeren (country code top level domains -ccTLDs) ve içermeyen (generic top level domains -gTLDs) alan adları olarak iki kategoriye ayrılmaktadır (Şekil-4). İkinci derece alan adları www'dan sonra gelen kısım olarak belirtilmektedir. Birinci derece alan adlarının (Türkiye'de örneğin: com.tr, net.tr vs.) tahsisi ICANN tarafından akredite edilmiş organizasyonlarca yürütülmektedir.



Şekil 4 - Birinci ve İkinci Derece Alan Adları

Birinci derece alan adlarının tahsisi ülke kodları içerdiği için alan adlarının yönetimi devletlere bırakılmıştır. Devletler de bu yetkiyi kendileri veya özel kuruluşlar vasıtasıyla kullanabilmektedir. ".com", ".net" ".org" ve ".info" talep eden herkesin kullanımına açıkken ".int", ".edu", ".gov", ".mil", ".aero", ".biz", ".coop", ".name", ".pro" ve ".museum" belirli kriterleri sağlayan kurumlara tahsis edilebilmektedir.

Ülkemizde ".tr" uzantılı alan adlarının yönetimi 5809 sayılı Elektronik Haberleşme Kanunu'nun 35. maddesi ile belirlenmiştir. Bu doğrultuda "Nic.tr" sistemi üzerinden alan adlarının tahsisi gerçekleştirilmektedir. 7.11.2010 tarihli ve 27752 sayılı İnternet Alan Adları Yönetmeliği ile ".tr" uzantılı internet alan adları yönetimine ilişkin usul ve esaslar tekrar düzenlenmiştir. Bilgi Teknolojileri ve İletişim Kurumu (BTK) bu yönetmeliğin 14. maddesinin birinci fıkrasının (a) bendi uyarınca TRABİS ("tr" ağ bilgi sistemi)'i kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde TRABİS'in üçüncü bir tarafça kurulması ve işletilmesini sağlamakla görevlendirilmiştir. TRABİS, ".tr" uzantılı internet alan adı sisteminin ve buna ait merkezi veritabanının işletilmesine, rehberin oluşturulmasına, güncellenmesine ve rehberlik hizmetinin sunulmasına ve alan adı başvuru işlemlerinin gerçek zamanlı olarak yapılmasına imkân veren, tüm bu faaliyetlerin güvenli ve iş sürekliliğini sağlayacak şekilde gerçekleştirildiği sistem olarak tanımlanmıştır.

4. Yeni Nesil İnternet Teknolojileri

İnternetin dinamik yapısı ve internet teknolojilerindeki sürekli inovasyon yeni nesil internet teknolojilerinin ortaya çıkmasına sebep olmuştur. Bu teknolojilerden başlıcaları Nesnelerin İnterneti, Endüstri 4.0, Bulut Bilişim, Büyük Veri ve 4.5 G Teknolojileridir.

4.1. Nesnelerin interneti

Aklınıza hiç buzdolabınızın yumurtalığındaki yumurta bittiği zaman sizi uyarabileceği ve hatta uyarmakla da kalmayıp marketinize yumurta siparişi verip bir de sizi bu konuda bilgilendirebileceği gelebiliyor mu? Veya soğuk kış aylarında arabanıza ilk bindiğiniz anda arabanızın sıcacık olması? Sabah yatağınızdan kalkmadan çayın suyunu ısıtabilecek bir sistem olması, 1 haftadır spor yapmadığınız ve yemeği çok kaçırdığınız zaman sağlığınızın kötüye gittiğini size hatırlatan bir kol saatinin olması gibi durumları hiç düşündünüz mü? Bunlar nesnelerin interneti ile gerçekleşebilecek sadece birkaç örnek olarak düşünülebilir. Nesnelerin interneti (IoT) kavramı ilk kez 1999 yılında Kevin Ashton tarafından kullanılmış olsa da ilk örneği 1990 yılında kahve makinesinin boş olup olmadığını kontrol edebilmek için kurulan kameralı sistem ile fikir olarak ortaya çıkmıştır.

Nesnelerin internetine, nesnelerin, eşyaların birbiriyle haberleşmesine olanak sağlayan ve kendi aralarında bilgi aktarımı gerçekleştirerek akıllı bir ağ oluşturmuş cihazlar sistemidir diyebiliriz. Yani gündelik hayatta kullanılan nesnelerin kablolu veya kablosuz bir ağa bağlanarak veri gönderip almasını sağlayan kabiliyetler bütünüdür. Akıllı evler, akıllı saatler, akıllı telefonlar ve akıllı tüm cihazlar nesnelerin interneti ile hayatımıza girmiş durumdadır.

Bugün birçok işletme nesnelerin interneti tabanlı birçok ürün ve hizmet üretebilmektedir. Nesnelerin interneti tabanlı pazar payının 2020 yılına kadar 7.1 trilyon dolara yükseleceği tahmin edilmektedir. Bugün çok sınırlı sayıda olarak günlük hayatta

kullanılabiliyor olsa da IoT birçok uygulama alanı ile yakın zamanda hayatımızda önemli bir yer tutacaktır. Bu çerçevede, IoT ve uygulama alanlarını şu 4 başlıkta toplamak mümkündür:

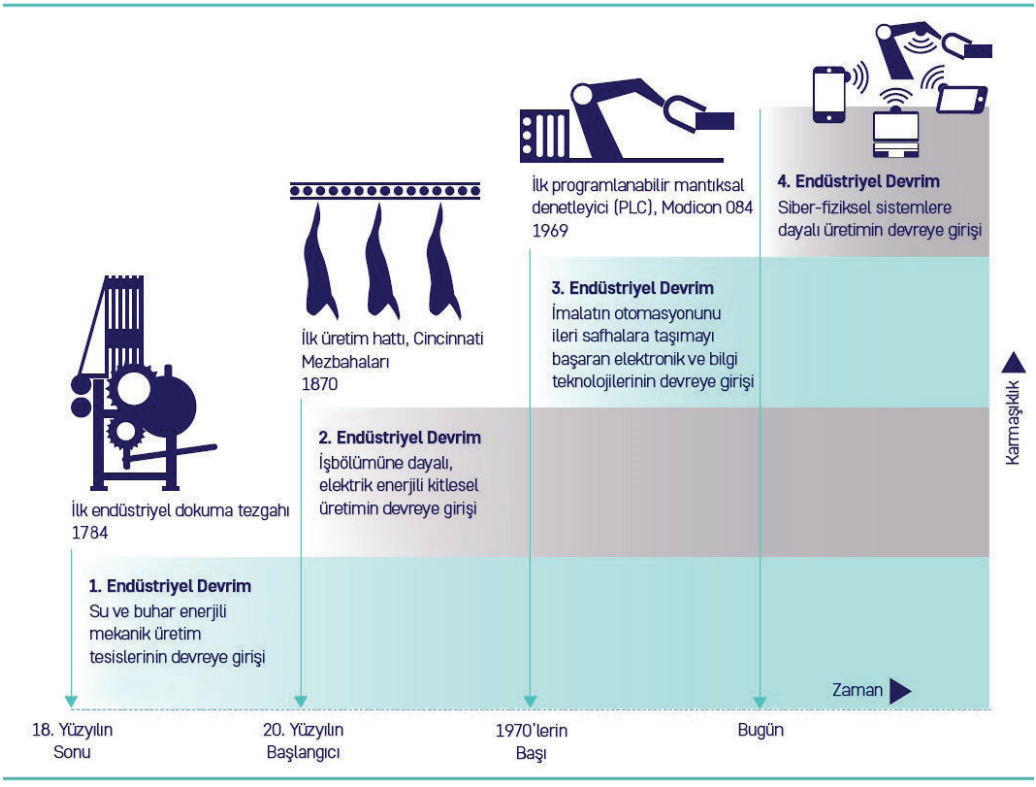
1. Taşımacılık ve lojistik
2. Sağlık
3. Akıllı çevre (ev, ofis, şehir)
4. Kişisel ve sosyal alan

Iot uygulamalarına sadece yukarıda ki 4 başlık altında bile on binlerce örnek verilebilir. Bu örneklerin hepsi de hayatı kolaylaştıran, belki de zaman, maliyet ve verimlilik yönünden tasarruf sağlayan uygulamalar olacaktır.

En basit olarak günlük hayatta sıklıkla kullandığımız akıllı telefonların 5 yıl önceki hali ile şimdiki hali arasında sizce en büyük fark kamera çözünürlüğü veya hızı mı? Bugün birçok akıllı telefon parmak izi, el hareketleri ve kalp atış hızının ölçülmesi gibi farklı fonksiyonları cihazlara yerleştiren sensörler aracılığı ile yapabilmektedir.

4.2. Endüstri 4.0

Endüstri 4.0 kavramı nesnelerin interneti ile yakından ilişkilidir. Endüstri 4.0 işin daha çok sanayi yani üretim tarafını ilgilendiren bölümüdür. 1712 yılında buhar makinelerinin icadı ile başlayan sanayileşme dönemi, bilgi ve iletişim teknolojilerinin sanayide kullanılmaya başlamasına kadar (Endüstri 3.0) günümüze uzanmıştır (Şekil-5). Endüstri 4.0 ise çoğunlukla dijital teknolojilere dayalı bir üretimin gerçekleştirilmesi üzerinde durmaktadır. Bu sadece nesnelerin internetini değil sanayide kullanılan hizmet gücü ve fiziksel sistemlerin de internet teknolojileri ile akıllılaşmasını öngörmektedir. Bugünden geleceğe internet bölümünde incelenen web 3.0 ve web 4.0 ile de endüstri 4.0 bu yönden yakından ilişkilidir.

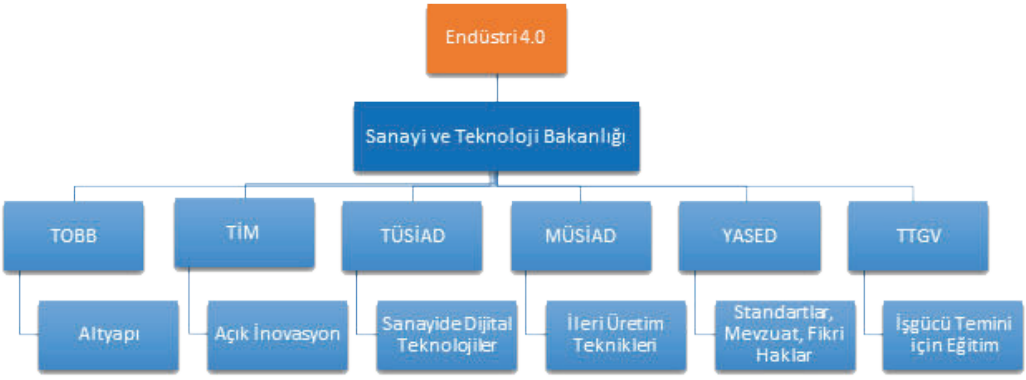


Şekil 5 – Sanayi Devrimi Aşamaları (Kaynak: http://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/)

Daha da anlamlandırmak için Endüstri 4.0'a şöyle bir örnek verilebilir. Klasik üretim anlayışında bir üretim hattı, o hatta üretilecek ilgili ürün ve o ürünün üretilmesinden sorumlu bir de insan gücü vardır. Endüstri 4.0 bu insan gücünü en aza indir-

meyi amaçlamaktadır. Ürünler ile üretim hattının yani üretimi yapacak makinelerin birbiri ile haberleşerek üretimi kendi aralarında tamamlamasını veya büyük bir bölümünü tamamlamasını öngörür.

Ülkemizde de Endüstri 4.0'a giden yolda Sanayide Dijital Dönüşüm Platformu; Bilim, Sanayi ve Teknoloji Bakanlığı bünyesinde kurulmuş ve aşağıda görüldüğü üzere çeşitli kurum ve kuruluşlara ilgili konu başlıklarında görevler verilmiştir (Şekil-6).



Şekil 6 – Sanayide Dijital Dönüşüm Platformu Görev Dağılımı

4.3. Bulut bilişim

İnternette birçok veri üretilmektedir. Bu veriler de depolama alanlarına ihtiyaç duymaktadır. Bu veriler kişisel bilgisayarlar ya da bu iş için oluşturulmuş özel bilgisayarlar olan sunucularda depolanmaktadır. Bulut bilişim ise bu verilerin fiziki makineler yerine internet yani bulut ortamında saklanılması mantığına dayanır. Günümüzde kullanılan bulut uygulamalarından en bilinenleri, Oracle, Microsoft Office 365, Google Drive ve Apple Icloud'dur.

Bulut bilişimde üç temel modele göre hizmet sunulmaktadır. Bunlar SaaS, PaaS, IaaS olarak isimlendirilir. Bunlardan en çok kullanılan Software as a Service kısaltması olan SaaS, Türkçe'ye "Bir Yazılım Olarak Servis" şeklinde veya "Yazılım Hizmeti" olarak çevrilmiştir. SaaS, bir hizmet veya yazılımı satın alan kullanıcılar, PaaS ve IaaS modelleri üzerine kurulan yazılıma erişirler. Böylece kullanıcının yönetmek, izlemek, çalıştırmak zorunda olduğu bir altyapı ya da platform bulunmaz. Böylelikle kullanıcılar pek çok operasyonel işten kurtulmuş, bakım ve destek maliyetleri kolaylaşmış veya ortadan kalkmış olur. Sonuç olarak yine dijital veriye ulaşmak için fiziki bir sistem kullanılır ama bu sistemi, hizme-

ti satın alan kullanıcının bulundurmasına ihtiyaç duymaz. PaaS (Platform as a Service) ve IaaS (Infrastructure as a Service) ise sırasıyla platform ve altyapı hizmeti sunulmasını ifade eder.

Bulut teknolojisi altyapı yatırımlarını azaltır, maliyetleri genel olarak düşürür ve istenildiği zaman bilgiye ulaşma kolaylığı sunar ama bu karşı tarafta saklanan verinin güvenliği ve gizliliği sorumluluğunu da getirir.

4.4. Büyük veri

Büyük verinin gündeme gelmesinde en önemli aşama web 2.0 teknolojileridir. Başta sosyal medya olmak üzere etkileşimli platformlar internet üzerinden akıl almaz bir şekilde verinin üretilmesine olanak sağlamıştır. Örneğin, her bir dakika içerisinde Youtube'a 500 saatten daha fazla video yüklendiği tahmin edilmektedir.

Veri, günümüzün en değerli aracı haline gelmiştir. Birçok teknoloji şirketi platformlarını kullanıcılarına ücretsiz sunmaktadır. Bunun nedeni ise, karşılığında bu platformların kullanıcı verilerini rahatlıkla alıp işlemesidir. Bugün toplanan bu devasa veri, veri madenciliği ve veri analistliği gibi yöntemlerle anlamlı hale getirilmektedir. Bu veriler de aslında büyük bir ticari enstrüman haline gelebilmektedir.

4.5. Yeni nesil mobil telekomünikasyon sistemleri

İnternet, mobil teknoloji dünyasında da büyük değişimlere yol açmıştır. Cep telefonlarının ilk çıktığı zamanlar sadece konuşma servisinin olduğu internetsiz dönem 1. Nesil (1G) olarak adlandırılabilir. Bunu mesajlaşma servisi ile birlikte kısıtlı internet hizmetlerinin getirildiği 2. Nesil (2G) hizmetler takip etmiştir. 2000'li

1G	2G	3G	4G	5G
• Konuşma	• Konuşma • Veri taşıma (SMS + MMS)	• Konuşma • Veri taşıma • Mobil internet • Görüntülü arama	• Konuşma • Veri taşıma • Hızlı mobil internet • Görüntülü arama	• Konuşma • Veri taşıma • Daha hızlı mobil İnternet • Görüntülü arama

Şekil 7 - Yeni Nesil Mobil Teknolojiler

yılların başında ise Japonlar cep telefonlarından rahatlıkla ses, video ve diğer iletişim verilerini gönderebilmeye ve hatta internet erişim hizmetlerini de sunmaya başlamıştır. Cep telefonlarından rahatlıkla internete bağlantı sağlanabilen bu dönem 3. Nesil (3G) hizmetler olarak anılmaya başlamıştır.

4. Nesil (4G) hizmetler ise, 3. Nesil hizmetlerin hızlandırılmış versiyonu olarak iletişim teknolojileri içerisinde yerini almıştır. Böylelikle, daha hızlı veri gönderme ve karşı taraftan bu verileri çağırma dönemi hayatımıza girmiştir. 4.5G olarak adlandırılan teknoloji ise 4G'nin de biraz daha hızlandırılmış versiyonu olarak bir nevi 5G'ye geçiş dönemi olarak kabul edilmektedir. 5. Nesil (5G) hizmetler ile de en yüksek hız kapasitesi ile 4G'ye göre tahmini 10 kat kadar daha hızlı iletişim ağı öngörülmektedir (Şekil-7).

5. İnternet Girişimciliği

İnternetin gelişimi ile birlikte kullanıcılara sunduğu en büyük fırsat internet girişimciliği olmuştur. Bugün dijital pazarlama, sosyal medya pazarlamacılığı, e-ticaret ve dijital girişimcilik gibi farklı isimler altında anılabilmekte veya gruplanabilmektedir.

Bugün gerek işletmeler gerekse kullanıcılar çevrimiçi ortamda varlıklarını oluşturmaktadır. Bu varlıkların çoğu sosyalleşme dışında genellikle ticaret, finans ve pazarlama gibi faaliyetleri de kapsamaktadır. Dijital platformlarda varlıklarını oluşturmak ve bunları sürdürülebilir kılmak günümüz rekabet koşullarının vazgeçilmez bir zorunluluğu halini almıştır.

Günümüzde tüketiciler artık üreticilere internet üzerinden ulaşmaktadır. Telefon, adres ve ürün bilgisi gibi pek çok işletme özelliği öncelikle internet üzerinden araştırılmaktadır. Kullanıcılar fiziki bir alışveriş yapacak olsalar bile öncelikli olarak internet üzerinden ilgili ürün veya hizmeti araştırmaktadırlar.

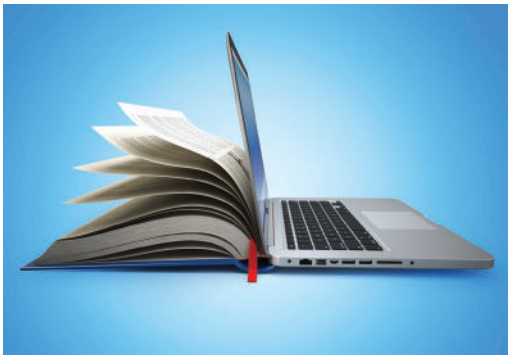
Dijital pazarlama günümüz rekabet koşullarının vazgeçilmez bir aracı haline gelmiştir. E-Posta pazarlama, arama motoru optimizasyonu, arama motoru pazarlaması, web ve sosyal medya analizleri, e-ticaret, dijital reklamcılık ve mobil pazarlama gibi kavramlar hep internetin getirdiği fırsatların doğal olarak işletmelere zorunlu bir yansıması olarak ortaya çıkmıştır.

Fiziki işletme sahibi olmayan internet kullanıcıları bile web 2.0 teknolojileri sayesinde internet girişimciliği faaliyetlerini yürütebilmektedirler. Sosyal medya, blog ve kendi sayfaları aracılığı ile kullanıcılar pazarlama faaliyetlerini gerçekleştirebilmektedirler. Dünyayı gezerek ve gezdikleri yerleri diğer insanlara internet ve sosyal medya üzerinden tanıtan insanlar için bile internet bir girişimcilik ve para kazanma kapısı haline gelmiştir. Bu ve bunun gibi birçok girişimcilik fırsatını internet tüm kullanıcılarına sunmuş durumdadır.

6. İnternet Okur-Yazarlığı

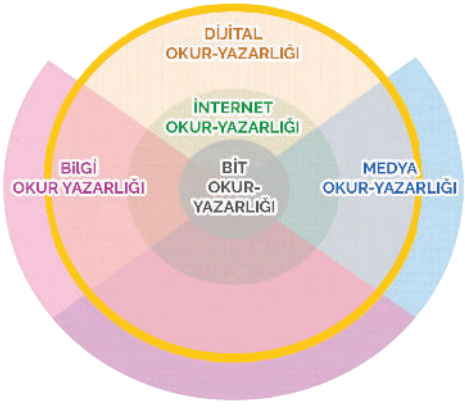
Bilgi teknolojileri ve başta internet olmak üzere iletişim araçlarının toplumsal tabana daha hızlı bir şekilde nüfus etmeye başlaması ile bu araçlara ve bilgiye ulaşım her geçen gün kolaylaşmış, bireylerin diji-

tal dünya ile etkileşimleri hızlı bir şekilde artmaya başlamıştır. Bilgi çağının getirmiş olduğu inovatif yaklaşımlarla dijital teknolojiler, hem yeni fırsatlar sunmakta hem de bireylerin bilişsel ve duygusal zekâlarını birçok açıdan etkilemektedir.



Günlük hayatta yapılabilen birçok iş ve işlemin artık internet üzerinden yapılabiliyor olması, ilk kullanılmaya başlandığında sanal dünya olarak adlandırılan bu platformun zamanla sanallıktan çıkmaya başlamasına sebep olmuştur. İnternet kullanıcısı olan ve potansiyel internet kullanıcısı olmaya aday olan bir vatandaşın gerçek hayatta sahip olduğu birçok hak ve sorumluluklar artık çevrimiçi ortamda da geçerli olmaya başlamıştır. İnternetin zaman içerisinde bireylerin yaşamlarını olumlu ve olumsuz birçok yönden etkilemeye başlaması dijital okur-yazarlık ve dijital vatandaşlık kavramlarının oluşmasına zemin hazırlamıştır. Önceden dijital ortamın olumlu ve olumsuz yönlerini iyi süzebilen sınırlı sayıdaki bireyler için geçerli olan dijital vatandaşlık ve dijital okur-yazarlık gibi kavramlar, birçok vatandaş için dijital teknolojilerin anlık olarak ulaşılabilir noktaya gelmesiyle, tüm bireyler için geçerli olan kavramlara dönüşmeye başlamıştır.

İnternet okur-yazarlığı dijital okur-yazarlığın önemli bir bölümünü oluşturmaktadır. Hatta internet teknolojilerinin yaygınlaşmasıyla dijital okur-yazarlık internet okur-yazarlığının tamamına yakın bir bölümünü oluşturmaya başlamıştır. Şekil 8'de görüldüğü üzere dijital dünyada okur-yazarlık; medya okur-yazarlığı, bilgi okur-yazarlığı ve dijital okur-yazarlık gibi bileşenlere sahip olmakla birlikte internet ve bilgi teknolojileri okur-yazarlığı bu bileşenlerin merkezinde yer almaktadır.



Şekil 8 – Dijital Dünyada Okur-Yazarlık (Kaynak: Ala-Mutka, 2011)

İnternet okur-yazarlığı, dijital okur-yazarlığın bir bileşeni olmakla birlikte dijitalleşme çağının internet teknolojilerine kayması ile birlikte dijital okur-yazarlık internet okur-yazarlığı ile hemen hemen aynı şeyleri ifade eder hale gelmeye başlamıştır. Bununla birlikte medya, bilgi ve BİT okur-yazarlıkları da hemen hemen aynı şeyleri ifade etmeye başlamıştır. Medya okur-yazarlığı gazete, radyo ve televizyon gibi geleneksel yayıncılık platformlarını da kapsarken BİT okur-yazarlığı hepsinin merkezinde bilişim ve iletişim teknolojilerini kullanıldığı platformlardaki okur-yazarlıkları kapsamaktadır. Bilgi okur-yazarlığı kapsamındaki bilgi edinim ve üretimi ağırlıkta internet ve geleneksel medya araçları kullanılarak gerçekleştiği için BİT okur-yazarlığı hepsinin merkezinde yer almaktadır.

6.1. Dijital okur-yazarlık kavramı

Dijital okur-yazarlık; bilgi teknolojilerinin getirmiş olduğu fırsat, inovasyon ve yaratıcılığın farkında olma, bilginin geçerlilik ve güvenilirliğinden emin olma ve bu teknolojilerin kullanımının etik sorumluluğunu bilme ve bilgiyi eleştirel ve sistematik bir şekilde arama, toplama ve işleme fonksiyonlarını kapsamaktadır.

Dijital okuryazarlık, dijital teknolojilerinin sadece etkin kullanımı değil; aynı zamanda bu teknolojilerin doğru ve etik kullanımı gerekliliğini de beraberinde getirmiştir (Şekil-9). Bu da 'dijital yerli' ve 'dijital göçmen' kavramlarının ortaya çıkmasına neden olmuştur. Bu açıdan günümüz çocuk ve gençlerinin internete yerli, bir önceki neslin ise televizyona yerli, internete göçmen olduğunu söylemek gerekir. İki nesil öncesi ise radyoya yerli, televizyona göçmendi. Dijital göçmen ve dijital yerli kavramları yanı sıra dijital dünya sessiz kuşak, baby boomers, x, y ve z kuşakları olarak adlandırılan kuşakların da oluşmasına zemin hazırlamıştır. Bu kuşakların birbirleri arasındaki fark aşağıda Tablo 1'de özetlenmiştir.

Şekil 9 – Dijital Okur-Yazarlık Boyutları

Tablo 1. Dijital Kuşaklar Arasındaki Farklılıklar

	Sessiz Kuşak	Baby Boomers	X Kuşağı	Y Kuşağı	Z Kuşağı
Doğum Aralığı	1923 - 1945	1946 - 1964	1965 - 1980	1981 - 1997	1998 - 2017
Dünya Nüfusu	0,3 Milyar	1,1 Milyar	1,5 Milyar	2 Milyar	2,4 Milyar
Nüfus Oranı	%5	%15	%20	%27	%32
İletişim Şekli	Mektup	Telefon	E-Mail/SMS	Anlık Mesaj	Emoji
Teknoloji Merakı	Araba	Televizyon	Bilgisayar	Akıllı Telefon	Sanal Gerçeklik/
Hobi	Okuma	TV İzleme	İnternette Gezinme	Video İzleme	Sosyal Medyanın Gücünden Faydalanma
Dijital Yetkinlik	Dijital Öncesi	Dijital Göçmen	Erken Uyum Sağlayanlar	Dijital Yerli	Dijital Mahkûm
Müzik	Safiye Ayla Müzeyyen Senar	Zeki Müren Emel Sayın	Coşkun Sabah Cengiz Kurtoğlu	Britney Spears Justin Timberlake	Justin Bieber Taylor Swift
Facebook Harici Kullandığı Sosyal Ağ	Sosyal Kulüpler	Match.com	LinkedIn	Tinder	Snapchat
Hayata Bakış Açısı	Ülke neden bu kadar kötüye gitti?	Eski bayramlar yok azizim.	Sonuç olarak ne demek istiyorsun?	Kariyer nasıl yapılır?	Her şey çok kötü. Hiçbir şeyi beğenmiyorum.

Dijital okur-yazarlığı üç aşamada incelemek, kapsamını belirlemek adına önemlidir.

a) Teknoloji

Dijital okur-yazarlık, dijital alt yapının ve teknolojik araçların gelişmesiyle hız kazanmıştır. Bu açıdan dijital okur-yazarlık günümüzde teknolojik araçların gelişmesi ve gelişen teknolojik araçların etkin kullanılmasıyla ortaya çıkmaktadır.

b) Eğitim-öğretim

Dijital okur-yazarlığın diğer bir boyutu eğitim ve öğretim faaliyetleridir. İster bireysel bazda öğrenim olsun, ister sistematik olarak eğitim kurumlarında bir program

veya müfredat bazında olsun, dijital vatandaşlık ve dijital okur-yazarlık direkt olarak toplumsal anlamda eğitimli olmaya ve eğitim aracılığıyla toplumsal bilincin oluşturulmasına dayanmaktadır.

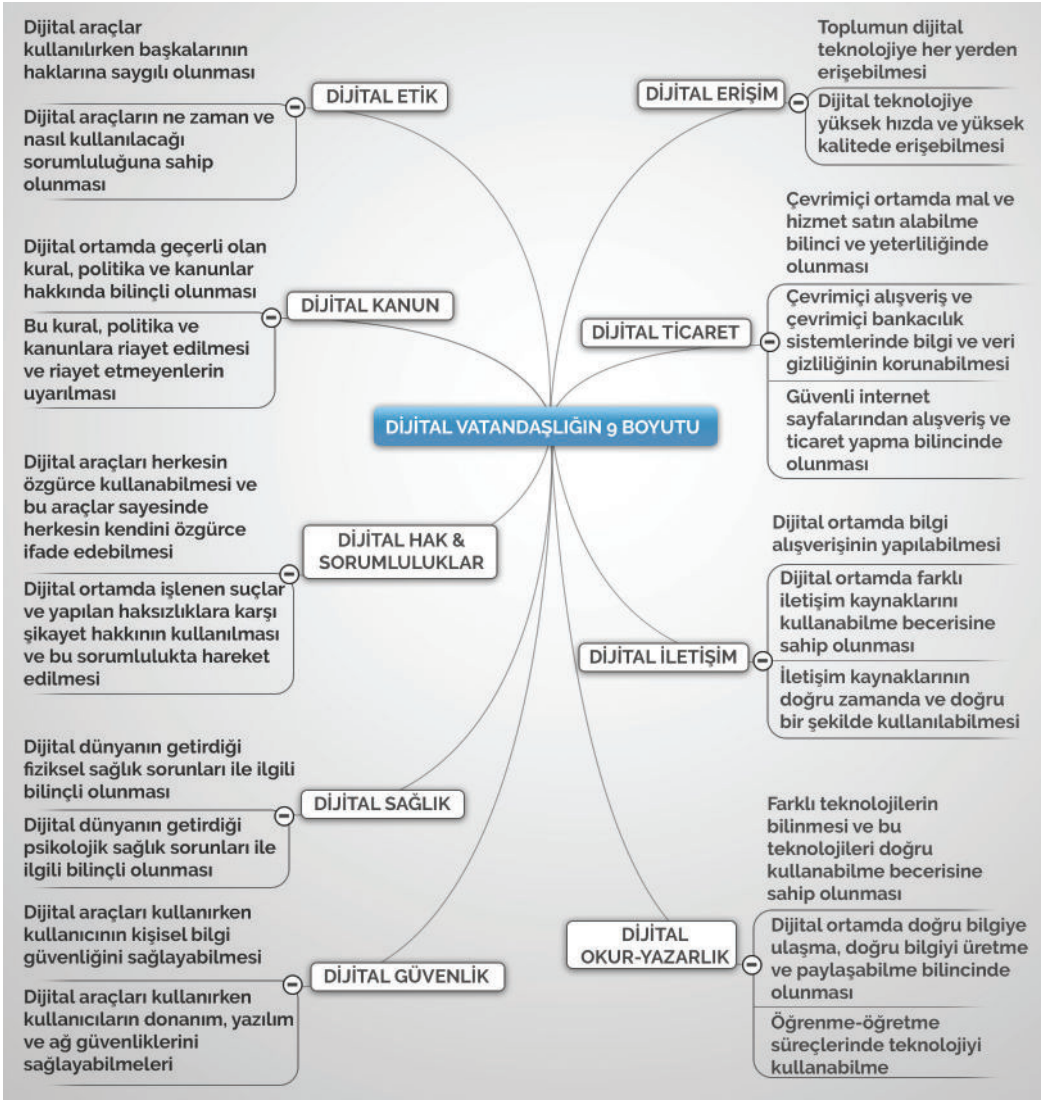
c) Etkileşim-iletişim

Etkileşim boyutu, dijital okur-yazarlığın son aşamasıdır. Dijital kaynakları kullanırken başkalarına zarar vermemek, bireysel yaşamı kolaylaştıracak şekilde kullanmak ve bu dijital araçları kullanırken iletişimin kurallarını bilmeyi gerektirmektedir. Başkalarıyla sanal ortamlarda iletişime geçerken iletişimin kimle gerçekleştiğinden emin olmak ve ileride gerçek hayatı etkileyecek, sıkıntı çıkaracak iletişimlerde ve yayınlarda bulunmamaktır.

Dijital okur-yazarlığın boyutları incelendiği ve kuşaktan kuşağa dijitalleşmenin getirdiği sonuçlar analiz edildiği zaman aslında iyi bir vatandaş olmanın iyi bir dijital vatandaş olmaya evrildiği gözlemlenmiştir. Bu yüzden internet okur-yazarlığında dijital okur-yazarlık kadar önem kazanan kavram dijital vatandaşlık olmuştur.

6.2. Dijital vatandaşlık kavramı

Bilişim ve iletişim teknolojileri gün geçtikçe gelişmekte, bu teknolojilerin kullanıldığı araçlar yaygınlaşmaktadır. Bu gelişmelere bağlı olarak bu araçlar sayesinde bilgiye her yerden ulaşılabilmekte ve her birey dünyanın farklı bir coğrafyasındaki ülke vatandaşı ile iletişim kurabilmektedir. Dijital vatandaşlık kavramı bu gelişmelerin bir sonucu olarak çıkmıştır. Diğer bir ifade ile internetin iletişim ve haberleşme noktasında ülke sınırlarını ortadan kaldırması, dünyayı küreselleştirmesi bu kavramın ortaya çıkmasına sebep olmuştur. Teknolojiyi ve teknolojiyle beraber hayatımıza giren dijital araçları doğru kullanmasını bilen, etik kurallara ve kişi haklarına dijital platformda da saygı duyan ve bu araçları güvenlik ve sorumluluk bilinciyle kullanmasını bilen kişiye dijital vatandaş denilmektedir. Dijital vatandaşlık ise kısaca, teknoloji kullanımı ile ilgili dijital vatandaşların sorumluluk sahibi davranış normları olarak tanımlanmaktadır.



Şekil 10 - Dijital Vatandaşlığın 9 Boyutu (Kaynak: Çubukcu & Bayzan, 2013)

Dijital vatandaşlığın Şekil 10'da görüldüğü üzere 9 boyutu tanımlanmıştır. Bu 9 boyut kısaca aşağıda açıklanmıştır.

1. *Dijital erişim:* Üretken vatandaşlar olmak için, eşit olarak teknolojik imkanlara dijital erişim sağlanması anlamına gelir. Örneğin, cinsiyet, ırk, yaş, etnik kimlik, fiziksel ve zihinsel farklılıklara aldırış etmeden elektronik topluma tam katılımın sağlanmasıdır.

2. *Dijital ticaret:* Elektronik ortamlarda satma ve satın alma işlemlerini yapacak yeterliliğe sahip olmak anlamına gelir.
3. *Dijital iletişim:* İletişim biçimlerinin değişikliğe uğrayarak elektronik araçlar vasıtasıyla da yapıldığının farkında olmaktır. Örneğin, e-posta, cep telefonu, anlık mesajlaşma gibi teknolojiler kullanıcıların iletişim yolunu değiştirmiştir.
4. *Dijital okur-yazarlık:* Öğrenme–öğretme sürecinin artık teknoloji kullanılarak da gerçekleştirildiğinin farkında olunmasıdır.
5. *Dijital etik:* Sanal dünyada gösterilen davranışın ya da işin elektronik standardının da olduğunun farkında olmaktır. Örneğin, siber zorbalık, sanal küfürleşme, sexting (mobil küfürleşme) gibi birçok olumsuz kavram sunan dijital dünya, her bireyin bilinçli bir internet kullanıcısı olması gerekliliğini kaçınılmaz hale getirmiştir.
6. *Dijital kanun:* Sanal dünyada yapılan işlerin elektronik sorumluluğunun olduğu ve kanunlarla yaptırım altına alındığı anlamına gelir. Örneğin, ülkemizde bazı yasadışı faliyetlerin (çocuk pornografisi, yasadışı organ ve uyuşturucu satışı, intihara meyilli hale getiren web siteleri ve kumar gibi faaliyetleri içerenler) sanal dünyada yapılması kanunen yasaktır.
7. *Dijital haklar/sorumluluklar:* Herkesin sanal dünyada kendini özgürce ifade edebilecek haklara sahip olduğu ve bunun da yasaklanamayacağı anlamına gelir. Örneğin, sanal ortamda formlarda görüş bildirme, grup oluşturma, tartışma ortamlarına katılma vb. temel haklar kısıtlanamaz. Bunun yanısıra vatandaşların dijital ortamda sorumlulukları da mevcuttur.
8. *Dijital sağlık:* Dijital dünyada hem fiziksel, hem ruhsal hem de psikolojik yönden sağlığı direkt ya da dolaylı olarak etkileyecek etmenlerin bulunduğunun farkında olunmasıdır. Örneğin, göz sağlığı, tekrarlayan stres sendromu, a-sosyal yaşam, içe kapanıklık ve fiziksel bozukluklar (bel ve sırt ağrıları) yeni teknolojik dünyada ele alınması gereken konulardır.
9. *Dijital güvenlik:* Bireyin sanal ortamda kendi güvenliğini sağlayacak önlemleri alması demektir. Örneğin, başkalarının bilgilerini izinsiz kullanmak, solucan, virüs veya truva atı oluşturmak, spam göndermek, birilerinin bilgilerini veya mallarını çalmak vb. faaliyetlerin farkına vararak gereken gizlilik ve güvenlik tedbirlerinin alınmasıdır (virüs programları, filtreleme programları vb.).

Dijital vatandaşlık ve yaklaşım alanları genellikle ilköğretim ve lise kademelerindeki öğrencilerin teknolojik ihtiyaçları çerçevesinde özellikle çevrimiçi teknolojileri ve diğer dijital platformları bilinçli ve doğru kullanımı aşamasında öğrencilere, eğiticilere ve sektör temsilcilerine tavsiyeler sunan bir yöntem bilim olarak literatüre dâhil olmuştur. Bununla birlikte, dijital vatandaşlığa sadece yeni yetişen genç neslin ihtiyaçları gözetilerek ortaya konması ge-

reken yaklaşımlar olarak bakılmamalı; teknolojiyle sonradan tanışan ve dijital araçları kullanmaya yeni başlayan jenerasyonun da ihtiyaçları doğrultusunda ortaya konması gerekenler olarak ele alınmalıdır. Bu çerçevede dijital teknolojiler ile ilgilenen her kesim ile bu kesimin dijital ihtiyaçlarına cevap verecek kanun koyucular, sektör ve sivil inisiyatiflerin de dijital vatandaşlığın her bir boyutunda aktif katılım ve düzenleme yapılması gerektiğini ortaya koymaktadır.

6.3. İnternet okur-yazarlığında internet araçları ve kaynaklarının kullanımı

Okur-yazarlık normalde hem okuduğunu anlama hem de okunabilir bilgi üretme anlamına gelmektedir. İnternet okur-yazarlığı da internet üzerinden bir bilgiye ulaşma, o bilgiyi analiz etme ve yorumlayabilme ile birlikte internette bilgi oluşturabilme becerilerini de kapsamaktadır.

İnternet okur-yazarlığı sadece sosyal ağ hesapları oluşturma ve arama motorları üzerinden birkaç bilgiye ulaşma becerisi ile başarılabilecek bir şey değildir. Örneğin Google her ne kadar bir arama motoru olarak bilinse de Google'un bugün pek çok kullanım alanı vardır. Örneğin Google Scholar, Google'un önemli servislerinden birisidir. https://scholar.google.com adresinden yapılan aramalar ile sadece akademik çalışmalara erişilebilmektedir. Ayrıca https://news.google.com adresinden ulaşılan Google News ile istediğiniz ülkeyi tanımlayarak, ilgili ülkelere ait güncel haberlere erişilebilmektedir. Yine https://books.google.com adresinden ulaşılan Google Kitaplar ile birçok farklı kitaba ulaşmak mümkündür.

İnternet okur-yazarlığı için temel aramalarda bile birçok yol ve yöntem mevcuttur. İyi bir okur-yazar hem doğru ve güvenli arama yöntemlerini bilmeli hem doğru bilgiye ulaştığından emin olmalı hem de arama sonuçlarına yeni bilgiler ekleyebilmelidir. Basit gibi görünen bir Google aramasında bile birçok farklı özellik mevcuttur. Bunun için https://support.google.com/ adresinden Google Arama seçilerek aramalar ile ilgili makaleler okunabilir.

Google bugün reklamcılıktan iş fırsatlarına varıncaya kadar pek çok servis sunmaktadır. Bunun gibi diğer arama motorlarında da benzer servisler mevcuttur. Bu yüzden internet kaynaklarının ve internet araçlarının getirmiş olduğu yeniliklerden haberdar olmak ve bunları kullanabilmek gerekmektedir.

İnternetin fırsatları pek çok alanda yeniliklerin doğmasına olanak sağlamıştır. Bankacılık sektöründe çevrimiçi ve mobil bankacılık hizmetleri; üretim sektöründe kurumsal kaynak yazılımları, hizmet sektöründe bilgilendirme ve şikâyet sistemleri; kamu sektöründe vatandaş-devlet ilişkisini kolaylaştıran e-Devlet ve CİMER gibi hizmetler; eğitim sektöründe FATİH projesi internet ile gelen yeniliklerden sadece birkaçıdır. Bu tarz sistem, yazılım ve araçların farkında olmak ve kullanabilmek, internet okur-yazarlığının en önemli aşamalarını oluşturmaktadır.

Web 2.0 teknolojileri internet kullanıcılarını sadece tüketen değil üreten bireyler

olmaya da teşvik etmeye başlamıştır. İnternette bugün herkes içerik oluşturabilmektedir. Bunun için belirli yazılım veya donanımlara hâkim olma zorunluluğu da azalmıştır. Bugün bir bölgeye turistik amaçlı yapılacak bir seyahatte bile farklı blog, forum ve sosyal medya platformlarında diğer internet kullanıcılarının paylaşımları, yorumları veya görüşleri dikkate alınarak karar verilmektedir. İnternetin anlık etkileşimli bir platform haline gelmeye başlaması içerik sayısının günden güne artmasına sebep olmuştur. İnternet, bir bilgiye ulaşma noktasında belirli kaynaklara ihtiyacı azaltarak anlık çözümler sunan bir araç haline gelmiştir. Burada en büyük katkı ise her kullanıcının aynı zamanda birer üretici olmaya başlaması ile mümkün olmuştur. Yani her okur aynı zamanda yazar da olabilmektedir. Yalnız bu durum internet okur-yazarlığı için yine kâfi değildir. Hem üreten hem tüketen bireyler yanında üretilen ve/veya tüketilen bilginin taranması, değerlendirilmesi, analizi ve doğruluğunun teyidi internet okur-yazarlığının diğer önemli bileşenlerini oluşturmaktadır.

İyi bir internet okur-yazarlığına giden yolda internet kullanıcıları için birçok boyut ve bileşen söz konusudur. Bunları aşağıdaki gibi derlemek ve yorumlamak mümkündür.

1. İnternetin Teknoloji Boyutunu Anlamak

1.1. İnternet Teknolojilerini Anlama

1.1.1. İnternet ve kullanım alanlarını anlamak

1.1.2. İnternet bağlantısı için gereken bileşenleri tanımlamak

1.1.3. World wide web, web adresleri ve web'de gezinmek

1.1.4. Web adreslerinin nasıl çalıştığını anlamak

1.1.5. Web 2.0 teknolojilerini anlamak

1.1.6. Web tarayıcıları ve eklentilerini yönetebilmek

1.1.7. Bir web sitesinin içeriğinin nasıl değerlendirileceğini tanımlamak

1.1.8. İnternet üzerinden iletişim yapabilmek

1.1.9. E-postanın nasıl çalıştığını anlamak, e-posta iletilerini yönetebilmek

1.1.10.E-ticareti anlamak

1.2. İnternette İçerik Geliştirebilme

1.2.1. İçeriğin üretilmesi

1.2.1.1. İnternette pozitif içerik üretebilme, dijital metin, ses, video ve fotoğraf üretebilmek

1.2.1.2. Dijital medyayı kullanarak zihin haritaları, diyagramlar oluşturabilmek

1.2.1.3. Yaratıcılığı teşvik edecek internet platformlarını kullanabilmek

1.2.2. İçeriğin entegre edilmesi ve yeniden düzenlenmesi

1.2.2.1. İnternette bilgi alanlarına (web siteleri, sosyal ağlar, forumlar, wikiler vs.) katkıda bulunabilmek

1.2.2.2. Katkıda bulunulan bilgiyi gerektiği zaman çağrılarak yeniden düzenleyebilmek

1.2.3. Telif hakkı ve lisans bilgilerini anlamak

1.2.3.1. İçerik yazımı ve paylaşımı için uygun lisansları kullanabilmek

1.2.3.2. Kendi dijital üretimlerini nasıl lisanslayacağını öğrenmek

1.2.3.3. Telif hakkı ve lisans kurallarıyla ilgili bilgileri nasıl bulacağını öğrenmek

1.2.4. Programlama

1.2.4.1. Dijital bilgiyi kullanarak gerçek dünyadaki karmaşık modelleri, simülasyonları ve görselleştirmeleri yaratabilmek

1.2.4.2. Dijital cihaz yazılımlarını kodlayıp programlayabilmek

1.3. Problem Çözebilme

1.3.1. Teknik problemleri çözebilme,

1.3.1.1. Sorun çözme ve sorun giderme konularında yardım bulabileceği bilgi kaynaklarını öğrenmek

1.3.1.2. Teknik bir sorunu çözebilmeyi veya teknoloji çalışmadığında yapılacak şeyleri öğrenme

1.3.2. İhtiyaçların ve teknolojik cevapların belirlenmesi

1.3.2.1. Dijital cihazların ve kaynakların potansiyelini ve kısıtlamalarını kavramak

1.3.2.2. Teknolojiyi kullanarak yapılabilecek şeylerin çeşitliliğini öğrenme,

1.3.2.3. Soruna göre en uygun teknolojileri seçebilmek

1.3.3. Teknolojinin yenilikçi ve yaratıcı kullanımı

1.3.3.1. Çözüm ararken, web veya değişik çevrimiçi ağını nasıl keşfedeceğini öğrenmek

1.3.3.2. Kendini yaratıcı biçimde ifade etmek için çeşitli ortamları (metin, görüntüler, ses ve film) kullanabilmek

1.3.4. Dijital uçurumun giderilmesi

1.3.4.1. BİT'in nereden geldiğini, onu kimin geliştirdiğini ve hangi amaca yönelik olduğunu öğrenmek

1.3.4.2. Bilgiyi transfer edebilme

1.3.4.3. Yeni teknolojiye sorunsuz uyum sağlayabilme ve teknolojiyi kendi çevresi ile bütünleştirebilmek

1.3.4.4. Dijital yetkinliklerde diğer kullanıcıları desteklemeyi öğrenmek

2. İnternetin Etik Boyutunu Anlamak

2.1. İnternet İletişimini Sağlayabilme

2.1.1. E-posta, VoIP ve çeşitli video konferans programlarını kullanabilmek

2.1.2. Başkalarıyla iletişim kurabilmek

2.1.3. Uygun iletişim türünü belirleyip, iletişimden aldığı veriyi filtreleyebilmek

2.1.4. Tanımadığı kişilerle iletişim risklerinin farkında olmak

2.1.5. Başta sosyal medya olmak üzere Web 2.0 teknolojilerini kullanarak içerik paylaşımında bulunabilmek

2.1.6. Paylaştığı içeriğin uygunluğunu ve doğruluğunu kavrayabilme

2.1.7. Paylaştığı içeriğin içerdiği telif ve lisans bilgilerine hâkim olma

2.1.8. Başkaları ile iletişimde geri besleme kanallarını öğrenme, başkaları ile yardımlaşabilmek

2.2. İnternette Güvenlik ve Gizliliği Sağlayabilme

2.2.1. Dijital cihazları koruma

2.2.1.1. Virüsler ve zararlı yazılımlar ile ilgili bilgi sahibi olmak

2.2.1.2. Anti-virüs programları hakkında bilgi sahibi olmak

2.2.1.3. Şifre güvenliği hakkında bilgi sahibi olmak

2.2.1.4. Çevrimiçi dolandırıcılık ve korunma yöntemleri hakkında bilgi sahibi olmak

2.2.1.5. Siber ataklar ve korunma yöntemleri hakkında genel bilgi sahibi olma

2.2.1.6. Mobil uygulamalar, web tarayıcıları, işletim sistemleri ve e-posta güvenlik /gizlilik ayarlarını öğrenme

2.2.2. Kişisel verileri koruma

2.2.2.1. Kişisel verilerin ne olduğu, çevrimiçi ortamda nasıl oluşturulduğu ve işlendiğini kavrama

2.2.2.2. Kişisel veriler mevzuatı hakkında genel bilgiye sahibi olma

2.2.2.3. Kişisel bilgi güvenliğinin nasıl sağlanacağını öğrenme,

2.2.3. Kişisel sağlığı koruma,

2.2.3.1. Bilgisayar ve internet kullanımının fiziksel sağlığa etkilerini öğrenme

2.2.3.2. Bilgisayar ve internet kullanımının psikososyal sağlığa etkileriniöğrenme

2.2.4. Çevreyi koruma,

2.2.4.1. Bilgisayarların ve elektronik cihazların çevresel etkilerini analiz edebilme

2.2.4.2. Bu cihazların parçalarını verimli bir şekilde geri dönüştürerek bunların daha uzun süre nasıl sürdürebileceğini kavrama

2.2.4.3. Dijital cihazların maliyet etkin bir şekilde ve zaman açısından verimli bir şekilde nasıl kullanılacağını öğrenme

2.2.4.4. Dijital cihazlara bağımlı hale gelmeden ihtiyaç dâhilinde kullanımını öğrenme

2.3. İnternette Hak ve Sorumlulukları Bilme

2.3.1. Hakları bilme

2.3.1.1. İnternette herkesin ifade özgürlüğünün olduğunun farkında olma

2.3.1.2. İnternette herkesin eşit haklarla bağlantı ve içerik üretme hakkına sahip olduğunu bilme

2.3.1.3. İnternetin katılımcı ve demokratik bir hak olduğunun farkında olma

2.3.1.4. Çevrimiçi topluluk ve sosyal ağların eleştirel anlayışta olduğunun farkında olma

2.3.2. Sorumlulukları bilme

2.3.2.1. Bilişim ve internet hukuku mevzuatlarını öğrenme ve kavrama

2.3.2.2. Siber suçlar, siber zorbalık ve diğer siber tehditleri kavrama, anlama ve sonuçları hakkında farkında olma

2.3.2.3. İnternette karşılaşılan olumsuzluklar, riskler ve yasadışı paylaşımlara karşı izlenecek yol ve yöntemleri öğrenme

3. İnternetin Bilişsel Boyutunu Anlamak

3.1. İnternette Bilgiyi Tarayabilme ve Filtreleyebilme

3.1.1. Çevrimiçi bilginin nasıl üretildiğini, yönetildiğini ve kullanılabilir hale getirildiğini kavrama

3.1.2. Arama motorlarının çalışma prensiplerini anlama, indeksleme ilkelerini öğrenme

3.1.3. Farklı arama motorlarını kullanmasını öğrenme

3.1.4. Hangi arama motorlarının veya veri tabanlarının kendi bilgi ihtiyaçlarına en iyi cevap verdiğini anlama

3.2. İnternette Bilgiyi Değerlendirebilme

3.2.1. Çevrimiçi ortamda bulunan bilgiyi yargılayabilme, söz konusu içerik ile o içeriğin sunuluş biçimi arasındaki farkı yargılayabilme

3.2.2. Edinilen bilgiyi çeşitli kaynaklardan toplayarak tarafsız bir şekilde değerlendirebilme ve bu sayede güvenilir bir bilgi ortamı oluşturabilme

3.2.3. Farklı kaynakların güvenilirliği ile çevrimiçi ve çevrimdışı bilgi kaynaklarını kavrama

3.2.4. Yeni nesil terminolojileri öğrenme.

3.3. İnternette Bilgiyi Saklayabilme ve Geri Çağırabilme

3.3.1. Bilgilerin farklı cihazlarda / servislerde nasıl saklandığını kavrama

3.3.2. Farklı saklama seçeneklerini ve en uygun olanı seçebilmeyi kavrama

3.3.3. Saklama seçeneklerinin güvenlik ve gizliliğini göz önüne alarak istediği zaman bilgiyi çağırabilmesini öğrenme

4. Sosyal Medya Araçlarını Etkin Kullanabilme

4.1. Sosyal Medyanın Teknoloji Boyutunu Anlayabilme

4.3.1 Geleneksel medya ile yeni medya arasındaki farkı anlama

4.3.2 Web 2.0 ile medyanın dönüşümünü analiz etme

4.3.3 Yeni medyanın geleceğini anlama

4.3.4 Yeni medyanın fırsatlarını yakalama

4.3.5 Sosyal medyayı kavrama, platformlarını anlama

4.3.6 Popüler sosyal medya platformları ve kullanım amaçlarını kavrama

4.3.7 Sosyal medya kampanyalarının yürütülmesi

4.3.8 Sosyal medya ve topluluk yönetimini anlama

4.3.9 Sosyal medya ve dijital pazarlamayı anlama

4.3.10 Sosyal medya ve seedingi (yemleme) anlama

4.3.11 Sosyal medyanın dinamiklerini öğrenme

4.3.12 Sosyal medya takibi ve raporlama yapabilme

4.2. Sosyal Medyanın Etik Boyutunu Anlayabilme

4.2.1. Sosyal medyaya giriş ve şifre işlemlerini anlama

4.2.2. Sosyal medya profilinin oluşturulması ve hesap yönetimini sağlama

4.2.3. Sosyal medya hesaplarını güvenli tutma yollarını öğrenme

4.2.4. Sosyal medya hesaplarını gizli tutma yollarını öğrenme

4.2.5. Sosyal medya hesaplarının reklam tercihleri ve kişisel bilgilere erişiminin denetlenmesini yapabilme

4.2.6. Sosyal medyada güvenli iletişim kanalları oluşturma

4.2.7. Sosyal medyada kriz yönetimi (başkalarının eline geçen hesaplar, kötüye kullanım, telif ihlalleri vs.) sağlama

4.3. Sosyal Medyanın Bilişsel Boyutunu anlayabilme

4.3.1. Sosyal medya ve ihtiyaçların belirlenmesi

4.3.2. Sosyal medya ve uygun kaynakların belirlenmesi

4.3.3. Sosyal medya ve içerik tercihlerinin belirlenmesi

4.3.4. Sosyal medya ve bilgi kirliliğinden korunma

4.3.5. Sosyal medyada bilgi edinimi, paylaşımı ve eleştirel yaklaşım stratejilerini anlama.

6.4. Yerel ve pozitif içerik kavramı

İnternetin faydalarından daha çok istifade etmek ve zararlarından korunmak için en etkili yöntem internetin yerel ve pozitif içeriğini güçlendirmekten geçmektedir. Avrupa Komisyonu tarafından desteklenerek kurulan 'Çocuklar İçin Daha İyi Bir İnternet (Better Internet For Kids)' girişimi sayfasında çevrimiçi pozitif içerik çocukların hem öğrenip hem eğlenip hem de yaratıcılıklarını geliştirebilecekleri bakış açısı ile sunulan herhangi bir içerik olarak tanımlanmıştır. Bununla birlikte pozitif içerik, çocukların bireylere saygı duyan bir yapı içerisinde toplumdaki katılımcılıklarını artıran ve diğer toplum bireyleri içerisinde ürettikleri bu içeriklerle üretkenlik ve motivasyon duygularını geliştiren bir kavram olarak belirtilmiştir.

İnternet tüm dünya vatandaşlarını aynı platform içerisinde eşit haklarla buluşturmuştur. İnternet ortamında yer alan bilgilerden herkesin eşit hak ve sorumluluklarla faydalanma hakkı vardır. Çevrimiçi paylaşılan her bilgi çevrimiçi topluluğa bir katkı sunmakla birlikte o bilgiyi herkesin etik değerler gözeterek kullanma hakkı da mevcuttur. Bu yüzden coğrafi sınırlamalara bağlı kalmadan ve dil, din, ırk farkı gözetmeden dünyanın herhangi bir yerinde üretilen pozitif bir içeriği yerelleştirmek gerekmektedir. Yerelleştirme işlemi sadece tercümeden oluşmakla kalmayıp o içeriğin bulunduğu coğrafi yapıya göre de konumlandırılması ve uyarlanmasını kapsamaktadır. Bu yüzden pozitif içerik konusunda hem üretken hem de farklı platformlarda yer alan doğru bilgiye ulaşma, paylaşma ve yerelleştirme konularında da etik değerler çerçevesinde farkında olunması gerekmektedir.

Web 2.0 teknolojileri artık tüm internet kullanıcılarını birer içerik üreticisi haline getirmiştir. İçerik üretmek için artık bir web sitesi tasarlamak veya oluşturmak gerekmemektedir. İnternet teknolojilerinin her geçen gün gelişmesi internetin sunduğu fırsatları artırmakta ve yürütülen işlemleri her geçen gün kolaylaştırmaktadır. Bugün hazır blog siteleri, sosyal ağlar, sosyal medya, sözlükler ve diğer hazır platformlar sayesinde içerik her an üretilebilmektedir.

İnternette içerik üretebilmek oldukça önem arz eden bir konudur. Yalnız üretilen içeriğin katma değeri ve kalitesi de en az üretim kadar önemli diğer bir konudur. Bugün başta Instagram ve Facebook olmak üzere kullanıcılar tarafından üretilen içeriklerin önemli bir bölümü kişisel amaçlar ve tatmin duygusu ile oluşturulan içeriklerdir. Maalesef bugün internet kullanıcılarının internette harcadıkları vaktin önemli bir bölümü de bu amaç ve hırslar bütününde oluşturulan içerikler ile geçmektedir. Bu yüzden her bir dijital vatandaş internette harcadığı vaktin kendine ne gibi bir katma değer yarattığını sorgulamalıdır. Bu dengede bakıldığında internet hem çok faydalı bir platform hem de çok zararlı bir platform olarak insan hayatında yer edinebilir. Bu da pozitif içeriğin önemini bir kez daha ön plana çıkarmaktadır.

7. Bölüm Kazanımları

Ar-ge ve inovasyon işletmeler açısından sıklıkla kullanılan kavramlar olmakla birlikte internet teknolojileri açısından bir yandan oldukça yeni bir yandan da oldukça eski kavramlardır. İnternet çok kısa geçmişine rağmen en büyük yenilik teknolojilerinden biri olarak kullanıcıların hayatlarında oldukça önemli bir yer tutmuştur. İnternet ve araçları doğru ve etkin kullanıldığı zaman kullanışlı ve yeni fırsatlara açık bir platform iken yanlış ve riskli kullanımlarda da olabildiğince kötü sonuçlar doğurabilecek bir platformdur. Bu yüzden internete iki ucu keskin bir bıçak diyebiliriz. Bu bölümde internetin tarih sahnesindeki kısa yolculuğu incelendikten sonra internet kaynakları ve yeni nesil internet teknolojilerinden bahsedilerek internetin geldiği ve geleceği nokta özetlenmeye çalışılmıştır. Bu geçmiş ve devam edecek yolculukta internetten doğru bir şekilde yararlanabilmek için internet girişimciliği, dijital okur-yazarlık, dijital okur-yazarlık çerçevesinde internet okur-yazarlığı ve boyutları derinlemesine incelenerek internet araç ve kaynaklarının doğru kullanılması için gerekli bileşenler ortaya çıkarılmıştır.

KAYNAKLAR

Ala-Mutka, K. (2011). Mapping digital competence: towards a conceptual understanding. Institute for Prospective Technological Studies. Available at: ftp://ftp. jrc. es/pub/EURdoc/JRC67075_TN. pdf (Erişim 15/01/2013).

Cubukcu, A., & Bazyan, S. (2017). A Study Regarding the Perception of Digital Citizenship Among Adults and the Assessment of This Perception. Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications, 47.

Çakır, H., Kılıç, M.S ve Diğerleri (2014). Güncel Tehdit Siber Suçlar, Seçkin Yayınevi, Ankara

Durusoy, O. (2011). Öğretmen yetiştirmede web 2.0 ve dijital video teknolojilerinin kullanılarak öğretmenlik öz-yeterliğinin geliştirilmesi.

Çubukcu, A. (2014). Çevrimiçi Ortamda Çocukların Korunumuna İlişkin Yapılan Çalışmalar ve Çocuklarda Dijital Vatandaşlık Algısının Geliştirilmesine Yönelik Çevrimiçi Modüllerin Geliştirilmesi, İletişim Uzmanlığı Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara

Durusoy, O. (2011). Öğretmen Yetiştirmede Web 2.0 ve Dijital Video Teknolojilerinin Kullanılarak Öğretmenlik Öz-Yeterliliğinin Geliştirilmesi, Yüksek Lisans Tezi, Balıkesir Üniversitesi, Fen Bilimleri Enstitüsü.

Çubukcu, A., & Bayzan, Ş. (2013). Türkiye'de Dijital Vatandaşlık Algısı ve Bu Algıyı İnternetin Bilinçli, Güvenli ve Etkin Kullanımı ile Artırma Yöntemleri. Middle Eastern & African Journal of Educational Research, 5, 148-174

Türkiye ve Dünyada İnternetin Kısa Tarihi,

URL:https://medyaglob.wordpress.com/2012/04/19/turkiye-ve-dunyada-internetin-kisa-tarihi/, Son Erişim tarihi, 23.05.2018.

Web Teknolojilerinin Kurumsal Kimlik Kazanması,

URL:http://innocentrum.com/blog/kurumsalwebteknolojileri.php, Son Erişim tarihi, 18.03.2018.

Yeşil, S., & Alkan, M. (2007). İnternet Yönetişimi ve İçerik Düzenlemeleri, XII. Türkiye'de İnternet Konferansı, Ankara.

Darici, A., (2005). İnternet Arabağlantısı: Çevirmeli İnternet Arabağlantısı, AB Uygulamaları ve Türkiye İncelemesi, Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu.

Kaya,M.B. (2010). Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi, On İki Levha Yayıncılık.

Mossberger, K., Tolbert, C., & S. McNeal, R. (2007). Digital Citizenship: The Internet, Society, and Participation. London, England: The MIT Press.

Ribble, M., & Bailey, G. (2007). Digital citizenship in schools. Washington, DC.

Ribble, M. S., Bailey, G. D., & Hall, B. (2005). Teaching digital citizenship: when will it become a priority for 21st century schools. School Business Affairs, 71(3), 11-14.

Yeşilyurt,N.(2007). ICANN Tartışmaları ve Uluslararası Politika, Akademik Bilişim 2007, Dumlupınar Üniversitesi, Kütahya.

BTK(2014). İnternet Alan Adları Yönetimi, Mevcut Sorunlar ve Çözüm Önerileri, btk.gov.tr sitesinden 24 Şubat 2014 tarihinde

Ashton, K. (2009). That 'internet of things' thing. RFiD Journal, 22(7), 97-114.

The Trojan Room Coffee Pot,

URL: http://www.cl.cam.ac.uk/coffee/qsf/coffee.html, Son Erişim tarihi, 15.04.2018.

Nesnelerin İnterneti,

URL: https://haleurun.wordpress.com/, Son Erişim tarihi, 09.04.2018.

Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.

Atzori, L., Iera,A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

Endüstri Tarihine Kısa Bir Yolculuk,

URL: http://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/, Son Erişim tarihi, 10.04.2018.

Bulut Bilişim Nedir?

URL: https://www.netinternet.com.tr/bulut-bilisim-nedir, Son Erişim tarihi, 10.04.2018.

YouTube - Statistics & Facts,

URL: https://www.statista.com/topics/2019/youtube/, Son Erişim tarihi, 03.05.2018.

Promoting Positive Online Content Across Europe, Son Erişim tarihi, 19.04.2018.

URL:https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2173627

An Internet Search Engine Operator is Responsible for the processing that it carries out of personal data which appear on web pages published by third parties,

URL: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf, Son Erişim tarihi, 10.04.2018.

Google EU Privacy Removal,

URL:https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=en, Son Erişim tarihi, 03.03.2018.

Request to Block Bing Search Results In Europe,

URL: https://www.bing.com/webmaster/tools/eu-privacy-request, Son Erişim tarihi, 03.03.2018.

BÖLÜM 2 İNTERNET VE GÜVENLİK

İçindekiler

Günümüzde masaüstü bilgisayarlardan mobil cihazlara kadar birçok cihazdan ve hemen her yerden bağlanılan internet, sadece insanların değil nesnelerinde bağlandığı ve birbirleriyle haberleştiği iletişim ağı haline gelmiştir. Bu kadar hızlı büyüyen ve gelişen internet, sunduğu fırsatlar sayesinde insanların hayatını kolaylaştırmış ve vazgeçilmezi olmuştur. Gerçek hayatta çok zaman alan işlerin çok kısa bir süre içerisinde yapılabilmesi, istenilen bilgiye bir tıklamayla ulaşılabilmesi, farklı coğrafyalardaki insanlarla iletişim kurulabilmesi, farklı kültürleri tanımaya olanak sunması, dünyanın bir ucundaki anlık haberlere hızlıca ulaşmayı sağlaması, istenilen ürünü alabilmeye ve satabilmeye imkân sunması, bankacılık işlemlerinde sunduğu işlem kolaylığı ve daha birçok özelliği interneti vazgeçilmez kılmaktadır.

Bu kadar güzel fırsatlar sunan internetin, sevindiren yüzü yanında bir de üzen yüzü bulunmaktadır. Gerçek hayatta yaşanan birçok olumsuzluklar ne yazık ki internet ortamında da yaşanabilmektedir. Hırsızlık, dolandırıcılık, hakaret, taciz, istismar, kişilik haklarının ihlali, özel hayatın gizliliğinin ihlali, suç olan içeriklerin üretilmesi ve paylaşılması, vatandaşa faydalı olan sistemleri devre dışı bırakmaya yönelik siber saldırılar, insanların hesaplarının ele geçirilmesi, insanların yalan haberlerle ve paylaşımlarla itibarlarının zedelenmesi, internet yoluyla insanların bilgisayarlarına virüs bulaştırılması, zararlı internet içeriklerinin oluşturulması gibi birçok başlığı da internetin üzen yüzü ve barındırdığı olumsuzluklar olarak sıralamak mümkündür.

İnternette güvenlikten bahsederken olayı geniş bir bakış açısından ele almak gerekmektedir. Hem sunduğu imkânlar ve getirdiği fırsatlar açısından yani gülen yüzünü, hem de sebep olduğu mağduriyetler ve verebileceği zararlar açısından da üzen yüzünü göstermek gerekmektedir. Yaşanılan mağduriyetlerin ve olumsuzlukların, internette nasıl davranılması gerektiğine yönelik kuralların bilinmemesinden ya da bilindiği halde bunlara uyulmamasından kaynaklandığı göz ardı edilmemelidir.

Bu bölümde; bilgisayarda ve internette gezinirken dikkat edilmesi gereken güvenlik konularında bilgilendirmeler yapılacaktır. Çünkü internette güvende olmak, internete çıkış yapılan cihazın güvenliğinden başlamaktadır. İlk çıkış noktasında güvenlik sağlanmazsa ideal bir güvenlikten bahsetmek zorlaşır.

1. Bilgi Güvenliği

Bilgi güvenliği, bir varlık türü olarak kabul edilen bilginin başkaları tarafından izinsiz ya da yetkisiz bir şekilde erişilmesini, kullanılması, değiştirilmesini, herkese açık olarak paylaşılmasını, yok edilmesini, başkalarına verilmesini veya bu bilgilere kullanılamayacak şekilde hasar verilmesini önlemek ve bu varlık türünü korumak olarak tanımlanabilir. Bilgi güvenliğinde "gizlilik", "bütünlük" ve "erişilebilirlik" unsurları son derece önemlidir. Gizlilik; bilginin yetkisiz kişilerin eline geçmemesi ve yetkisiz erişime karşı korunmasıdır. Bütünlük; bilginin yetkisiz kişiler tarafından değiştirilmemesidir. Erişilebilirlik; bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Mobil telefonlar ve tabletler mini birer bilgisayardırlar. Bu araçları ve diğer bilgisayarları kullananların alması gereken önlemler, güvenliğin ilk ayağını oluşturmaktadır. Bunlar bir kullanıcı için zor olan şeyler değildir. İşletim sisteminin güncel tutulması, bu cihazlara lisanslı antivirüs uygulamalarının yüklenmesi, şüpheli içeriğe sahip internet sitelerine bağlanılmaması, bilinmeyen adreslerden gelen ve merak uyandıran e-postaların açılmaması, kullanılmadığı durumlarda ekranların kapalı tutulması istenmeyen durumların ortaya çıkma olasılığını tamamen ortadan kaldırmasa da azaltacaktır.

Bilgi güvenliği zafiyeti durumunda olabilecek birçok durum söz konusudur: Kişisel bilgilerin internet ortamında yayınlanması, internet bankacılığı sistemini kullanan kişilerin hesaplarının boşaltılması, öğrenci bilgi sistemlerindeki öğrenci notlarının değiştirilmesi, hastane sistemindeki hasta bilgilerinin ele geçirilmesi, başkasına ait bilgisayarların ele geçirilerek saldırı ve suç amaçlı kullanılması, ele geçirilen bilgisayar ve hesaplardan toplu olarak istenmeyen mesajların gönderilmesi gibi durumlar sayılabilir. Bunlar bireylerin her açıdan mağduriyet yaşamasına sebep olabilmektedir. Bireylerin toplum içinde imaj ve itibarının zedelenmesi, maddi kayıplar, zaman ve emek kaybı, başkalarının işlediği suçlardan dolayı suçsuz kişilerin suçlanması ve mağdur olması, bilgisayardaki hayati önemdeki verileri kaybetme, kişisel bilgilerin çalınması gibi durumlar yaşanan olumsuzluklar olarak sayılabilir. Bireylerin bu konuda yapması gereken en önemli şey bilgi edinerek güvenliklerini artırmaları diğer bir ifadeyle bu konuda bilinçli olmalarıdır.

Bilgi güvenliği konusunda en fazla yapılan hatalardan birisi "Bana bir şey olmaz. Bugüne kadar bir şey olmadı, bundan sonra da olacağını düşünmüyorum" yaklaşımıdır. Ne yazık ki en fazla mağduriyeti de bu şekilde düşünenler yaşamaktadırlar. Yani aşırı güven aslında güven zafiyeti oluşturmaktadır. Bu yaklaşımın dışında aşağıdaki yanlış yaklaşımlara rastlamak da mümkündür.

- Antivirüs yazılımım var, korunuyorum, güvendeyim,
- Güvenlik duvarım var, sıkıntı yok güvendeyim,
- Zaten bilgisayarda fazla bir şey yapmıyorum, internete fazla girmiyorum,
- Bilgisayarın yedeğini zaten alıyorum, güvenlik önlemine gerek yok,
- Aşırı şüpheci ve paranoyak olmak anlamsız, olsa olsa birkaç dosyam silinir,
- Güvenlikten bana ne, zaten bilgi işlem bakıyor, evde ve ofiste bununla ilgilenen var, ben bilmesem de olur gibi yaklaşımlar.

Bu yaklaşımlardan kurtulmak veya bunların farkında olmak için aşağıdakileri bilmek, konunun öneminin anlaşılması açısından son derece önemlidir;

- Kullanıcıdaki güvenlik ve olayları hafife almama bilinci bilgi güvenliğinin en önemli parçasıdır.
- Güvenlik açıklıklarının en önemli kısmı kullanıcı hatalarından kaynaklanmaktadır.
- Saldırganlar genellikle kullanıcı hatalarını kullanmaktadır.
- Kullanıcı, bilgi güvenliğinin en zayıf halkasıdır.
- Bir kullanıcının güvenlik ihlali tüm sistemin zarar görmesine sebep olabilir.
- Teknik önlemler kullanıcı hatalarını önlemede yeterli olmayabilir.
- Kullanıcı dikkati, kurallara riayet sistem güvenliği açısından önemlidir.

Bununla birlikte 2016 yılında Resmi Gazetede yayınlanarak yürürlüğü giren 6698 sayılı Kişisel Verilerin Korunumu Kanunu ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlenmiştir.

2. Kişisel Verilerin Korunması

Pek çok AB ülkesi ve ABD kişisel verileri koruma hakkında kanunlarını ulusal mevzuatlarına adapte etmiş olsalar da Türkiye ancak yakın bir zamanda kişisel verilerin korunması yasa tasarısını kanunlaştırabilmiştir. Örneğin, Türkiye'nin 1949 yılında katıldığı Avrupa Konseyi, 1980 yılında sınır ötesi veri işleme ile ilgili uluslararası alanda mahremiyetin korunmasına yönelik bir sözleşme kabul etmiştir. Avrupa Konseyi, 1981 yılında ise veri koruma alanında ilk uluslararası hukuk belgesi olan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkında Sözleşme"yi (108 no'lu Sözleşme) imzaya açmıştır. Daha sonraki yıllarda ise hem üyesi olduğumuz Avrupa Konseyi hem de Avrupa Birliği siber ortamda yaşanan gelişmelere bağlı olarak pek çok direktif, sözleşme ve protokolü imzaya açmıştır.

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" (108 sayılı Sözleşme), veri koruma alanındaki ilk uluslararası hukuk belgesidir. Bu Sözleşme, 1 Ekim 1985 yılında yürürlüğe girmiştir. Ülkemiz, anılan Sözleşmeyi 28 Ocak 1981 tarihinde imzalamış; ancak onaylayarak iç

hukukta geçerli hale uzun bir süre getirememiştir. Bu sözleşme 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanarak iç hukuka dahil edilmiştir. Zira söz konusu sözleşmenin 4'üncü maddesi gereğince, sözleşmenin onaylanabilmesi için, imzalayan devletin, sözleşmede öngörülen ilkeler çerçevesinde bir yasa kabul etmesi zorunludur. Türkiye ta ki, uzun süren çalışmalar neticesinde 6698 sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde kabul etmiş ve 7 Nisan 2016 tarihinde Resmi Gazete'de yayınlanarak yürürlüğe girmiştir. Söz konusu yasada, kişisel verilerin işlenmesi, silinmesi, yok edilmesi, anonim hale getirilmesi ve aktarılması gibi hükümler tanımlanmıştır. Kanunda kişisel veri ise kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır.

Dünyada ve ülkemizde giderek artan internet kullanımı, birçok kolaylığı beraberinde getirirken kişisel verilerin korunumu konusu da daha önemli hale gelmiştir. Kişisel veriler, kişinin kimlik yapısını ortaya koyan ve kişiye özel bilgiler olarak tanımlanabilir. İlk başta kişisel veriler olarak doğum tarihi, açık ev adresi, anne kızlık soyadı ve vatandaşlık numarası gibi kişisel bilgiler akla gelmektedir. Yalnız internet teknolojilerinin gelişmesi internetin fırsatları yanı sıra veri gizliliği ve veri güvenliği gibi konuları da gündeme taşımaya başlamıştır. Bugün birçok internet kaynağı ve internet aracı ister pazarlama ve reklam faaliyetleri kapsamında olsun ister spam ve oltalama gibi istenmeyen kötü niyetli internet içerikleri aracılığı ile olsun kişisel bilgileri elde etme noktasında birçok iz sürmektedir. Bugünün internet kullanıcıları kişisel bilgilerini sosyal medya ve diğer internet platformlarında paylaşmama noktasında oldukça bilinçlenmiş durumdadırlar. Diğer açıdan bakılacak olursa farklı yöntemlerle doğrudan paylaşılmayan kişisel bilgiler dolaylı paylaşımların harmanlanması ile büyük veri ve veri madenciliği gibi yöntemlerle de artık elde edilebilmektedir. Buna dijital çağda dijital ayak izleri denmektedir. Örneğin kişisel bilgilerini hiçbir şekilde internet ortamında paylaşmamış bir internet kullanıcısının, sosyal medyada yaptığı her türlü kişisel (sevinç, acı, hüzün, eğlence, iş, tatil, aile vs.) paylaşımlar sonucunda zamanla kişisel bilgilerin başkalarının eline geçmesi gibi.

Kişiye ait, kişiye özel internet içeriklerine kişisel paylaşım denilmektedir. Bu içerikler sosyal medya hesaplarının önemli bir bölümünü oluşturmaktadır. Günümüzde bu konuya ilişkin yapılan en büyük hatalardan biri aileler tarafından gerçekleştirilmektedir. Günümüzün dijital aileleri çocuklarının bebeklikten beri gelişim evrelerine ilişkin her türlü görsel ve işitsel içeriğini internete yüklemektedirler. Bu durumdan normal olarak bebek ve küçük yaştaki çocuklar farkında bile olamamaktadırlar. İnternet teknolojileri henüz yeni bir teknoloji olduğu için ailelerin çocukları üzerine yıllar boyunca yapacakları kişisel paylaşımların o çocukların ilerideki yaşamını nasıl etkileyeceğini şimdiden kestirmek ise oldukça zordur. Ama gerçek olan şudur ki, her bir kişisel paylaşımın önemli bir dijital ayak izi olduğu ve bu paylaşımlardan çocuğun özel hayatı ve kişisel bilgilerine ilişkin zamanla ciddi bilgiler elde edilebileceğidir.

Kişisel verilerin korunumu genelde hukuki ve teknik bir konudur. Yukarıdaki örnekte görüldüğü üzere ise her ne kadar yasalarla ve teknik araçlarla önlem alınsa da veri gizliliği ve güvenliği internet kullanıcılarının kendisinde bitmektedir. Bu yüzden bu konuda bilinç oluşumu ve bilinçlendirme çalışmaları oldukça önemli bir konu başlığıdır.

Bilgi ve iletişim teknolojilerinin gelişmesiyle özellikle internet ortamında kişisel verilerin korunumu internet ortamının dağıtık ve dinamik yapısı gereği daha da zor hale gelmiştir. Belirtildiği üzere birçok bilginin ve paylaşılan bilgilerin harmanlanması ile kişisel veriler oluşturulabilmektedir. Hatta bu bilgilerin birçoğu web 2.0 teknolojilerinin getirmiş olduğu kolaylıklar ile internet kullanıcılarının kendileri tarafından da paylaşılabilmektedir. Bugün sosyal ağlarda birçok kullanıcı kendini tanımlayıcı ve tasvir edici içerikli resim, video ve çeşitli diğer görsel ve işitsel araçları çok rahatlıkla paylaşabilmektedir. Dijital okur-yazarlığı düşük bireylerin bunun daha da ötesine geçerek adres, doğum tarihi, cep telefonu numarası gibi doğrudan kişisel veriler sınıfına girecek bilgileri bile rahatlıkla paylaşabildiği görülebilmektedir.

Kişisel verilerin korunmasında yasaların ve uluslararası sözleşmelerin getirmiş olduğu birtakım uygulama ve yaptırımlar olsa da temel gizlilik ve güvenlik kişinin kendisinde başlamaktadır. Bu yüzden kişisel bilgi güvenliği önemli hale gelmektedir. Bu güvenlik ve gizliliğe özellikle internet ortamında dikkat edilmesi gerekmektedir. Bu konuda da kullanıcıların şu önerileri dikkate almasında fayda bulunmaktadır:

- İnternette ve sosyal ağlarda tasvir edici, betimleyici bilgiler paylaşılmamalıdır. Çok fazla konum bilgisi, adres bilgisi verilmemelidir.
- Bilinen ve güvenli sitelerden işlem (alışveriş, iletişim, ticaret, dosya indirme vs.) yapılmalıdır.
- Başka bir internet sayfası üzerinden, arama motoru ya da e-posta ile gelen linklerden değil, doğrudan internet adresi yazılarak işlem yapmak istenilen sitelere bağlanılmalıdır. Bunun için web tarayıcıda sık kullanılanlar oluşturulmalıdır.
- İnternet kafe ve alışveriş merkezleri gibi internetin ortak kullanıldığı alanlar yerine kişisel bilgisayarlardan işlemler yapılmalıdır. Bu gibi yerlerdeki internet bilgi alma ve eğlence gibi temel amaçlar için kullanılmalıdır.
- İşlem yapılan web sitelerin https bağlantısına sahip olduğu ve geçerli bir sertifikasının olup olmadığı kontrol edilmelidir.
- İnternetten yapılan ödemeler mutlaka kredi kartı hesap özetinden kontrol edilmelidir. Bunun için sanal kredi

kartı veya sanal limit oluşturulmalıdır. Bilgisayarda da sanal klavye kullanılmalıdır.

- Gerek internette işlem yapılan sayfalarda gerekse bilgisayarda tahmin edilmesi güç şifreler belirlenmeli ve bu şifreler belirli aralıklarla değiştirilmelidir.
- Lisanssız yazılımlar kullanılmamalı, işletim sistemi güncel tutulmalı ve lisanslı anti-virüs yazılımlar kullanılmalıdır.
- Dışarıdan (harici bellekler) veya internetten bilgisayara yüklenilen dosyalar virüs ve casus yazılım taramalarından geçirilmelidir.
- Telefon yoluyla veya internette sosyal ağlar aracılığı ile telefon numarası isteme, hediye çeki, para talebi gibi tuzaklara dikkat edilmelidir. Hatta bu istek yakın arkadaştan veya kendisini polis olarak tanıtan kişilerden gelmiş olsa bile buna şüphe ile yaklaşılmalıdır. Bu durumda arkadaşın hesabı büyük bir ihtimalle ele geçirilmiştir. Kendini polis gibi göstermeye çalışan kişilerin tuzağına düşürülme ihtimali var demektir. Böylesi bir durumda hemen ihbar ve uyarı yöntemlerini kullanılmalıdır.
- Akıllı cep telefonlarınıza gereksiz ve birçok bilgiye ulaşan uygulamalar-yüklenmemelidir. Uygulama marketlerinin izin vermediği uygulamalar kullanılmalıdır ve telefona da zor tahmin edilebilir bir ekran kilidi belirlenmelidir.

Kişisel veriler ulusal mevzuat ve uluslararası sözleşmelerle korunma altına alınmaya çalışılsa da internet teknolojileri ile kişisel veriler dünyanın bir ucundan diğer ucuna çok rahatlıkla aktarılabilmektedir. Bunun takibi oldukça zor olmakla birlikte her ülkenin bu konudaki yaptırımı da farklı olabilmektedir. Bununla birlikte devletler tabi ki de önlemlerini almaya devam etmelidir. Çünkü kişisel verilerin yurtiçinde de işlenmesi ve üçüncü sahıslarla paylaşılması oldukça önemli bir konudur. Bu konuda Türkiye Avrupa Konseyi'nin üye bir ülkesi olarak kendi mevzuatını yeni olsa da çıkarmıştır. Bununla birlikte Türk Ceza Kanunu'nun 135. ve 136. maddeleri de kişisel verilerin kaydedilmesi ve ele geçirilmesi suçlarını düzenlemektedir. Ayrıca yine yakın zamanda kanunlaşan Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 10. Maddesi kişisel verilerin korunmasını düzenlemiştir. Bu maddenin b bendinde "Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz." İfadesi e-ticarette kişisel verilerin korunmasında oldukça önem teşkil eden bir yükümlülüktür.

3. Bilgisayar ve İnternet Güvenliği

Bilgisayarda ve internette yüzde yüz bir güvenlik sağlamak ve güvenli bir ortam oluşturmak oldukça zordur. Alınması gereken bazı tedbirleri alarak yüksek düzeyde güvenlik sağlamak ise mümkündür. Bilgisayar derken sadece masaüstü bilgisayarın algılanmaması gerekmektedir. Taşınabilir bilgisayarlar, tabletler ve akıllı telefonların hemen hepsi günümüzde bilgisayar özelliği taşıyan teknolojik aletler olarak değerlendirilmektedir. Bunların çalışabilmesi için mutlaka bir işletim sistemine gereksinim duyarlar.

Bu cihazların içlerinde yer alan özel ve paylaşılmaması gereken bilgilerin artmaya devam etmesi bu cihazlar için güvenlik tedbirlerini almayı gerekli kılmaktadır.

İşletim sistemleri, bir anlamda donanımların fonksiyonlarını yerine getirmeleri için tasarlanmış yazılımlardır. Dolayısıyla işletim sisteminde meydana gelebilecek hatalar donanımların çalışmasını, görevlerini yerine getirmesini engelleyecektir. Her ne kadar kullanıcılar, bilinen güvenlik tedbirlerini aldıklarını düşünseler de, güvenlik açıkları günden güne çoğalmakta ve tam bir korunma sağlanması zorlaşmaktadır.

Güvenlik tedbirleri almadan bilgisayar başta olmak üzere internete bağlanılan teknolojik aletleri yani bilişim teknolojilerini kullanmak günümüzde bir risk unsuru olarak karşımıza çıkmaktadır. Bireyler her ne kadar bu konunun uzağında dursalar bile bu durum onların yakasını bırakmamaktadır. Çünkü hemen her anında insanlar akıllı telefonlarıyla, tabletleriyle ve diğer teknolojik aletleriyle internete giriyorlar, bunlara çok farklı mobil uygulama yüklüyorlar, mobil uygulamaların istediği izinleri, sonucunun ne olacağını düşünmeden kabul ediyorlar.

Bu noktada risklerin farkında olmak ve buna göre tedbir almak çözüm noktasında alınabilecek en önemli önlem olarak karşımızda durmaktadır. Farkında olmak önemlidir, çünkü farkında olanları bir şekilde önlem almaya iten çok önemli gerekçeler bulunmaktadır. Farkında olmayanlarda ise böyle bir kaygı bulunmamakta ve bu durum mağduriyetlere yol açmaktadır. Sonrasında ben bilmiyordum pişmanlığı da pek bir işe yaramamaktadır. Bilgisayarda günlerce uğraşılarak oluşturulan belgelerin dışarıdan yapılan bir müdahale ile bozulması veya değiştirilmesi, çok büyük bir emek ve zaman kaybıdır. Hatta bu müdahaleyi yaparak dosyalara virüs bulaştıran ya da onları şifreleyen bilgisayar korsanlarının bunun karşılığında kişilerden yüklü miktarda para talep etmesi, para verilse bile çözüm üretilememesi mağduriyetin boyutunu daha da artırmaktadır. Onun için, bozulan bir sistemi ya da değiştirilen bir bilgiyi düzeltmek önlem almaktan oldukça zor, hatta bazen imkânsız da olabilir. Bilgi, belge ve dosyaların alınacak küçük önlemlerle korunabileceğini bilmek gerekir.

Bilgisayar giriş güvenliğinin sağlanması noktasında kullanıcının olmazsa olmazları olmalıdır. Mesela kimse evinden çıkarken evinin kapısını açık bırakmaz. Aynı mantık ve yaklaşım bilgisayar için, akıllı telefonlar için de geçerlidir. Bilgisayar ve bilgisayar özelliği taşıyan cihazların giriş güvenliği, içinde saklanan bilgilerin de güvenliği anlamına gelmektedir ve bu açıdan önemlidir.

Hiçbir birey, fiziksel olarak bu cihazlara ulaşabilen birinin bu bilgilere ulaşmasını arzu etmez. Onun içindir ki öncelikli ola-

rak bu tür cihazların fiziksel güvenliğini almak gerekir. Sonraki aşamada ise bu tür cihazlara erişim için kimlik doğrulaması yani kullanıcı adı ve parolanın olması gerekir. Bu tedbirler alındığında, yabancı kişiler fiziksel olarak bilgisayarınıza veya bilgisayar özelliği taşıyan mobil telefon, tablet gibi diğer cihazlara erişebilseler de bilgilerinize erişemeyeceklerdir. Bu cihazlar bir bilgisayar ağına veya internete bağlı olsa da, ağ üzerinden bilgilerinize erişim olmayacaktır.

Özetle, bilgisayar güvenliği açısından işletim sisteminin güncelliği, bilgisayara kurulan yazılımların orijinalliği yani lisanslı olması ve yine bunların güncelliği önemlidir. Benzer şekilde kaynağından emin olunmayan yazılımların bilgisayar sistemlerinden uzak tutulması, internette tehlikeli sitelerden uzak durulması da bir o kadar önemlidir.

Bilgisayar güvenliğinde en önemli konulardan biri de kötücül yazılımlar yoluyla bir bilgisayarın kötü niyetli bir başkası tarafından ele geçirilerek suç amaçlı yani başka sistemlere saldırı amaçlı kullanılmasıdır. Bilgisayar kullanımının yaygınlaşması ile bilgisayarlara yapılan saldırı ve teknikler de gün geçtikçe artmaktadır. Ağ saldırılarının en tehlikelilerinden olan Botnet saldırısı ile bilgisayar korsanları kişisel bilgisayarları ele geçirebilmektedir.

Botnet, siber saldırganların ele geçirdiği ve internete bağlanabilen her türlü cihazların tümünü ifade etmektedir. Siber saldırganlar ele geçirip köleleştirdikleri, sahibinin bile haberi olmayan binlerce bilgisayarı kontrol altında tutarak zararlı yazılımları yaymakta, ağlarına yeni köle bilgisayarlar eklemekte ve bunlarla da başka sistemlere saldırıda bulunmaktadırlar. Sistemleri devre dışı bırakmayı amaçlayan tek bir kaynaktan olabileceği gibi ele geçirilmiş bilgisayarlar ile çoklu kaynaktan hedef sistemlere yapılan DDoS olarak adlandırılan siber saldırılarda botnetler kullanılmaktadır. Tüm bunlar dikkate alındığında bilgisayar ve internet güvenliğinin ne denli önemli olduğu daha iyi anlaşılacaktır.

4. Parola ve Şifre Güvenliği

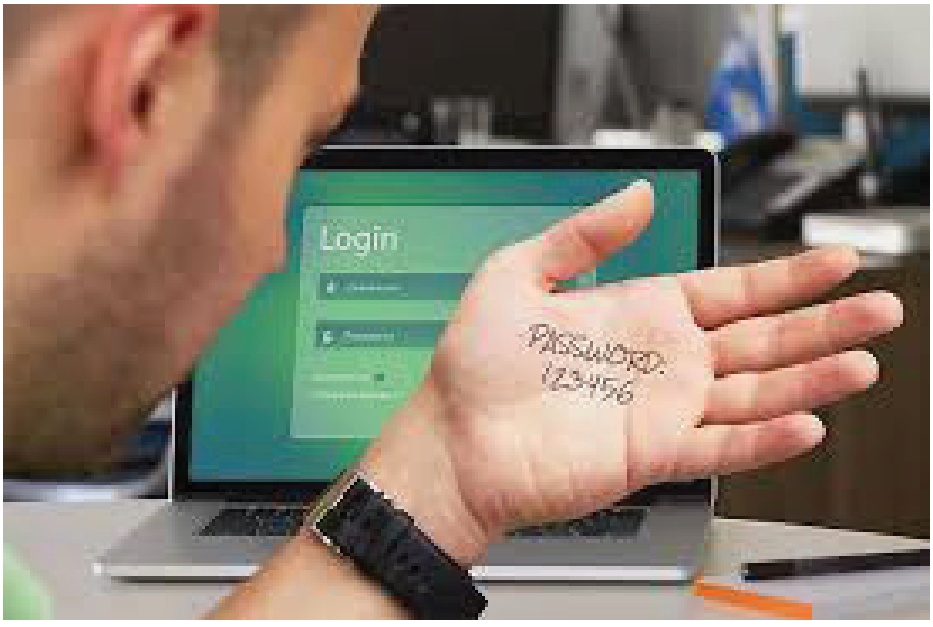
Kullanıcı adı ve şifreler yani parolalar bir kapının anahtarı gibidir. Kapı kullanıcı adıysa anahtar da şifredir ve bunların her ikisi de güçlü olmak zorundadır. Şifrenin güçlü kapının zayıf olması da bir zafiyettir. İkisi de bir bütün olarak güçlü olmalıdır. Şifreler iki şekilde başkaları tarafında ele geçirilmektedir. Bunlardan birincisi, tahmin ederek ya da deneme yanılma yoluyla elde edilmesidir. İkincisi, açıkta bırakılan yani bir yerlere yazılan şifrenin hırsızlık yoluyla ele geçirilmesi, çalınmasıdır.

Kişinin başkası benim parolamı nasıl tahmin edebilir ya da deneme yoluyla nasıl elde edebilir diye düşünmesi bir zafiyettir. Hâlbuki bunun cevabı çok basittir. Sizi tanıyan birisi, hakkınızda bildikleriyle şifrenizi tahmin edebilir. Unutulmasın diye çok sık kullanılan bir şifre kullanılıyorsa bir başkası deneme yanılma yoluyla bu tür basit parolaları bulabilir. Bir parolayı bulmayı aklına koymuş sanal hırsız, özel programlar kullanarak sık kullanılan yüzlerce parola örneğini ya da sözlüklerdeki binlerce keli-

meyi hızlıca deneyerek parolayı belirleyebilir. İyi korunmayan, yazılı, mesaj yoluyla ya da sözlü ifade edilen parolalar kulak misafiri olan birileri tarafından ya da araya girerek mesajı okuyan kişiler tarafından ele geçirilebilir. Bilgisayara bulaştırılan ve klavyeden yazılan her karakteri kaydeden keylogger gibi virüslü uygulamalarla kişinin bilgisayardaki işlemleri izlenerek parola kolaylıkla elde edilebilir.

Böyle bir durumdan şüphelenilmesi durumunda yapılacak ilk iş kullanıcı adının ve parolanın değiştirilmesidir. Başka sistemlerde ya da hesaplarda aynı parola kullanılmış ise aynı şekilde bunların de ivedi olarak değiştirilmesi gerekir. Bunları yapmak tek başına yeterli olmayabilir. Bu güvenlik zafiyetinden etkilenebilme olasılığı olan diğer kişilere de bilgi vermek gerekir ki sizin yerinize geçebilecek sanal hırsızların onlara zarar vermesi engellenmiş olsun. Ayrıca benzer problemlerin tekrar yaşanmaması adına da tahmin edilmesi zor ve güçlü parolalar oluşturulmalıdır. Güçlü parola, tahmin edilmesi kolay olmayan, karmaşık karakter kombinasyonundan oluşturulmuş veya deneme yanılma yoluyla bulunması oldukça zor parola demektir. Oluşturulan bir parolanın güçlü olarak kabul edilebilmesi için;

- En az 8 karakterden oluşması,
- Harflerle birlikte rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermesi,
- Büyük ve küçük harflerin bir arada bulunduğu bir birleşimden oluşması gerekir. Bu kurallara uygun parola oluştururken kombinasyon içerisinde doğum tarihi, ad, soyad gibi kişisel bilgiler içeren ifadelerin olmaması



önemlidir. Sözlükte bulunabilen kelimeler ile birçok kişinin kullanma olasılığı yüksek veya aynı yöntem ile geliştirilmiş parolaların olmaması gerekmektedir. Örneğin; 'Ben 1996 yılının 7. ayında Trabzon'un Sürmene ilçesinde doğdum'. İfadesi B1996y7. aTSid şeklinde şifre haline getirilebilir. Güçlü gibi görünen fakat gerçekte zayıf olan parolalardan kaçınmak gerekir. Bu parolalar klavyedeki harf sırası, alfabedeki harf sırası gibi popüler kurallardan oluşturulmaktadır. Örneğin bunlar; "qweasd", "123QweAsd", "asd12345", "Asd123, "qwerty", "qwerty123", "qazwsx123", "abc123", "123abc", "1234abcd", "123456", "987654321", "1234qqqQ" gibi parolardır.

Güçlü bir parola oluştursanız bile eğer bu parolayı koruyamıyorsanız fazla anlamlı olmaz. Güçlü parolalar vermek gereklidir fakat tek başına yeterli değildir. Verdiğiniz parolanın korunması ve paylaşılmaması da bir o kadar önemlidir. Parolayı korumak için aşağıdaki kurallar uygulanmalıdır:

- Parola kâğıt ya da elektronik gibi açıkça yazılmış olarak bulundurulmamalı, eğer bulundurulması gerekiyorsa saklanılan fiziksel ve elektronik ortamın güvenliği sağlanmalıdır.
- Her sistemde ya da her hesapta aynı parola kullanılmamalıdır. Bu durum riski en aza indirecektir.
- Belirli zaman aralıklarında parolalar mutlaka değiştirilmeli, lisanslı antivirüs yazılımları kullanılmalı ve bunlar güncel tutulmalıdır.

Tüm bu kurallar dizisi, uygulaması basit kurallar olsa da, bu konuda çok sık hatalar yapılmakta ve dikkatsiz davranılmaktadır. Bu durum da farklı derecelerde ve şekillerde mağduriyetlere yol açmaktadır. Özetle; kolay tahmin edilemeyen (güçlü) parolalar kullanılmalı, kullanılan parolalar korunmalı ve paylaşılmamalı, periyodik olarak değiştirilmeli, herhangi bir yerde yazılı olarak bulundurulmamalı ve cihazdaki lisanslı antivirüs programı güncel tutulmalıdır.

Bilgisayarın işletim sisteminin güvenliği de bir o kadar önemlidir. Parola sadece internet ve sosyal medyada oluşturulan üyelikler için değil, akıllı telefonlar dâhil bilgisayarlardaki işletim sistemleri için de olmazsa olmaz bir güvenlik tedbiridir.

Bilgisayara girişte çoğu kişi sadece işletim sisteminin açılışı aşamasında kullanıcı adı ve parola giriliyor olduğunu düşünür. Hâlbuki onun öncesinde bilgisayarın her açılışında parola sorulmasını sağlayan BIOS parolası ayarlanabilmektedir. Bilgisayara BIOS parolasını koymak için aşağıdaki adımlar takip edilebilir.

Bilgisayara BIOS parolası koymak için;

1. Öncelikle bilgisayarınızı yeniden başlatmalı ve BIOS ayarlarına girmelisiniz. Bunun için bilgisayarınızı açtığınızda ekrana ilk görüntü geldikten sonra 'Delete' veya 'F2' tuşuna basınız. (BIOS'a göre değişebilir, hangi tuş olduğu, BIOS ayarlarına girebileceğinizi belirten ekranda gösterilecektir.)
2. BIOS ayarlarındaki seçeneklerden "Güvenlik" (Security) ile ilgili olan seçeneği seçtiğinizde "Kullanıcı Paro-

lası" (User Password) ve "Yönetici Parolası" (Supervisor Password) olmak üzere iki farklı parola türü (BIOS'a göre değişebilmektedir) karşımıza gelecektir.

3. "Yönetici Parolası" sadece BIOS'a girmek istendiğinde sorulur. "Kullanıcı Parolası" ise hem BIOS'a girmek istendiğinde, hem de bilgisayarın her açılışında sorulacaktır. Eğer sizden başka kimsenin makinanızı açmasını istemiyorsanız bu seçeneği seçmeniz daha uygun olacaktır. Bu seçeneklerden herhangi birini seçtiğinizde koymak istediğiniz parola sorulacaktır.

4. Parolayı girdikten sonra kontrol amacıyla parolanız tekrar sorulacaktır. Burayı da doldurduktan sonra 'Esc' tuşuyla ana menüye çıkın. F10 veya Tekrar 'Esc' ye bastığınızda yapmış olduğunuz değişiklikleri kaydetmek isteyip istemediğiniz sorulacaktır. Değişiklikleri kaydederek çıkın.

Bu aşamadan sonra bilgisayarda kurulu olan işletim sisteminin açılışında parola sorulmasını sağlayarak ikinci güvenlik önlemi alınabilir. Windows işletim sisteminin açılışına parola tanımlamak için aşağıdaki adımlar takip edilmelidir.

1. "Başlat" menüsünden "Ayarlar" ve sonrada "Denetim Masası" tıklatılır.

2. Açılan "Denetim Masası" penceresinde "Kullanıcı Hesapları" seçilir.

3. Açılan "Kullanıcı Hesapları" penceresinde "Hesap değiştir" ile hesabın üzerine tıklatılır.

4 Hesap değiştir ifadesi tıklatıldığında bilgisayardaki kullanıcılar listelenir. Bu hesaplardan işlem yapılmak istenen hesap seçilir.

5 Açılan penceredeki "Parola oluştur" linki tıklatılır.

6 Açılan parola oluşturma ekranında " Yeni bir parola yazın" kutusuna şifrenizi girin ve "Onaylamak için şifrenizi yeniden girin" ve alttaki parola oluştur butonuna basınız.

7. Şifreniz oluşturulmuş oldu. Windows her açılışta şifrenizi soracaktır.

Bilgisayara kullanıcı adı ve parola tanımlamak tek başına yeterli olmayabilir. Çünkü işletim sistemine parola verseniz de gün içinde her zaman bilgisayarın başında durulmaz. Sadece bilgisayarları açarken değil gün boyunca parola yardımı ile erişimi denetlemek gerekir. Bu nedenle, bilgisayarın başından kısa bir süre için kalkılacaksa da bilgisayarı kilitlemek gerekir. Bilgisayarınızın başından ayrılırken hesabınızı kilitlemeyi alışkanlık haline getirmek diğer bir ifade ile bilgisayar başından kalkarken mutlaka oturumu kilitlemek, unutulan durumlar için parolalı ekran koruyucusu ayarlamak, hiç kimse ile kullanıcı adı ve parolayı paylaşmamak son derece önemlidir.

Benzer şekilde mobil cihazlarda da giriş şifresini, cihazın ayarlar seçeneği bölümünden tanımlamak mümkündür. Parolasız sistemler ve cihazlar, anahtarsız ev gibidir. Bu da hırsızlar için bulunmaz bir fırsattır. Hiçbir birey evinini hırsızlar tarafından soyulmasını istemediği gibi mobil cihazındaki ve bilgisayarındaki bilgilerinin çalınmasını da istemez.

5. Kötücül Yazılımlar

Zararlı, kötücül yazılımlar veya zararlı programlar, bilgisayar ve bilgisayar özelliği gösteren sistemlere zarar verebilen, bunları olumsuz etkileyerek etkili kullanılmasına engel olan yazılımlardır. Güvenli olmayan bu tür yazılımların en önemli özelliği lisanslı olmamalarıdır. Günümüzde bilgisayar sistemlerinde oldukça fazla lisanssız ve zararlı yazılımlar bulunmakta ve bunlar ciddi boyutlarda maddi ve veri kayıplarına neden olmaktadırlar. Lisanslı olmayan zararlı yazılımlarda virüs, casus yazılım ve solucan gibi isimler altında eklentiler bulunmaktadır. Bu durum, gerekli önlemler alınmadığında kişisel bilgi güvenliği, sistem güvenliği ve veri güvenliği açısından çok ciddi sonuçlar doğurmaktadır.

Zararlı kötücül yazılımlar birkaç başlık altında toplanabilir. Bunlar; virüsler, solucanlar (Wormlar), truva atları (Trojanlar), tuş kaydediciler (Keylogger), casus yazılımlar (Spyware)dır.

Virüsler, bilgisayar ve bilgisayar özelliği taşıyan cihazlardaki dosyalara tutunabilen ve kendini çoğaltarak bilgisayardaki diğer dosyalara da bulaşma özelliği gösteren zararlı yazılımlar, programlardır. En belirgin özellikleri çoğalarak yayılmak ve bulaştığı dosyalara, sistemlere zarar vermek amacıyla üretilmeleridir. Virüslerin bir sisteme bulaşabilmesi için kullanıcının etkisi oldukça büyüktür. Çünkü bir virüsün aktif olabilmesi için bir şekilde kullanıcı tarafından çalıştırılmasına gereksinim vardır. Dolayısıyla eğer bilgisayarda ya da bilgisayar özelliği taşıyan cihazda otomatik çalıştırma (autorun) açık değilse, virüsün bilgisayara bulaşmasında ilk derece sorumlu olan kullanıcıdır. Eğer otomatik çalıştırma özelliği açıksa herhangi bir kullanıcı etkisi olmadan da virüs aktif olabilir. Bunun için özellikle istenmeyen e-posta (spam) ile gönderilen ve virüs bulunma olasılığı yüksek olan exe, scr, zip, rar uzantılı dosyaları kaynak güvenilir değilse açmamak gerekmektedir.

Solucanlar; kopyalanma ve yayılma özelliği olan ve aynı zamanda çalışması için virüsteki gibi bir kullanıcı tarafından aktif edilmeye ihtiyaç duymayan zararlı yazılımlardır. Özellikle ağ üzerinde ve bilgisayarda kaynakların tüketilerek bazı işlemlerin sonlandırılmasına neden olmaktadırlar. Bu zararlı, sistemlerde açık bir kapı bırakmak suretiyle saldırganın veya diğer zararlı yazılımların sistemlere sızmasına, erişmesine olanak sağlarlar. Bilgisayar sistemlerindeki yavaşlıklar bu tür bir zararlı sebebiyle olabilmektedir. Virüslerde olduğu gibi dosya silme gibi bir özellikleri bulunmamaktadır. Örneğin, internette karşılaşılan "1.000.000 uncu kişisiniz", "ödül kazandınız", veya "Amerika'ya gitme şansı" gibi dikkat çeken açılır reklam ekranlarına tıklanması bu tür zararlıların bilgisayar sistemlerine bulaşmasına neden olabilmektedir.

Truva atı; bilgisayar için yararlı gibi gözükse de kullanıcının çalıştırması sonucu aktif hale gelen zararlı yazılımlardır. Adını da zaten efsanevi Truva atından almaktadır. Çünkü kullanıcı Truva atını kendi isteği ile

bilgisayara almaktadır. Bunların virüsler gibi kendini kopyalama özellikleri olmadığı gibi kullanıcı bilgisayara truva atı içeren bir program yüklemedikçe zarar vermezler.

Tuş kaydedici, kullanıcının bilgisayarda yazdığı her şeyi kaydederek, bunu bilgisayara bulaştıran ya da kopyalayan kişiye gönderen program ya da donanımlardır. Amaç kullanıcıların, kullanıcı adları ile şifrelerini ele geçirmektir. Ayrıca mahrem olabilecek yazışmalar da bu şekilde ele geçirilebilir. Örneğin, yazılan bir mail, arkadaşla yapılan özel sohbet bu şekilde kaydedilebilmektedir.

Casus yazılım; kullanıcıya ait bilgileri çalmayı, ele geçirmeyi amaçlayan zararlı bir yazılım, programdır. Eğer bilgisayarda arka arkaya ve bitmek bilmeyen bir şekilde açılır pencereler sorunu varsa yüksek ihtimalle bilgisayarda casus bir yazılım vardır. Casus yazılımlar, özellikle internete girmek için kullanılan tarayıcıya kullanıcının istemi dışında araç çubukları kurabilmekte ve web tarayıcısının açılış sayfasının değişmesine sebep olabilmektedirler. Tüm bunlarla birlikte zararlı yazılım derken akla aşağıdaki kavramlar da gelebilmektedir;

- Korsan yazılımlar (virüs, worm, trojan, keylogger spyware),
- Korsan müzik ve film dosyaları,
- Kırılmış (crack) programlar ve yazılımlar,
- Kaynağı bilinmeyen yerden edinilmiş herhangi bir program,

Güvenli olmayan yazılımların kaynakları ya belirsizdir ya da güvensizdir. Bunların geldikleri kaynakların bilinmesi korunmak açısından kritik öneme sahiptir. Bu tür yazılımlar bilgisayarlara bilerek ya da bilmeyerek kurulabilmektedir. Bilgisayardaki programların çalışmasında bozukluklar varsa, istem dışı dosya silinmesi ya da eklenmesi gibi bir durum yaşanıyorsa, bilgisayarda gözle görülür bir yavaşlık söz konusu ise kötücül yazılımın varlığından şüphelenmek gerekmektedir. Bu tür yazılımlar bilgisayarlara genellikle aşağıdaki şekilde yüklenebilmektedir.

- E-posta ile gönderilen bir dosya ekinin kontrol edilmeden açılmasından veya e-postada yer alan şüpheli bir bağlantının tıklatılmasından,
- Güvenli olmayan bir internet sitesinden yazılım indirilmesinden veya güvenilir olmayan bir yerden CD satın alınmasından,
- Başka bir bilgisayara takılarak kullanılmış olan USB yani harici bellek, güncel ve aynı zamanda lisanslı bir antivirüs programı ile taratmadan kullanıldığında,

Bu tür zararlı yazılımlar özellikleri itibariyle birçok şeyi yapabilme kabiliyetine sahiptirler. Bunları aşağıdaki şekilde sıralamak mümkündür:

- E-posta hesapları, banka şifreleri ve diğer kişisel bilgiler gibi bilgisayar ve bilgisayar özelliği taşıyan mobil cihazlardaki bilgileri çalarak başkalarına gönderebilirler.
- Bilgisayar ve bilgisayar özelliği taşıyan mobil cihazlardaki işletim sistemi başta olmak üzere diğer programların ya

çalışmamasına ya da hatalı çalışmasına sebep olabilirler.

- Bilgisayar ve bilgisayar özelliği taşıyan mobil cihazlardaki dosya veya klasörleri silebilirler, şifreleyebilirler, kopyalayabilirler, yerlerini değiştirebilirler ya da yeni dosyalar ekleyebilirler. Hatta böyle bir durumda bilgisayardaki diskteki tüm verilerin silinmesi ya da formatlanması gibi bir durum da söz konusu olabilir.
- Kişinin klavyeden yazdığı her şeyi, fare ile yaptığı her şeyi kaydederek bu zararlıyı bilgisayara bulaştıran kişiye gönderebilirler.
- Kişinin internete girmesi durumunda bilgisayar ekranında hiç de hoş olmayan can sıkıcı ve kötü amaçlı internet sitelerine yönlendiren istem dışı açılır pencerelerin çıkmasına sebep olabilirler.
- Bilgisayar ve bilgisayar özelliği taşıyan mobil cihazlarda, saldırganlar için güvenlik açıkları oluşturabilir ve bu cihazlar üzerinden başka sistemlere saldırı gerçekleştirebilirler.
- Başka zararlı kötücül yazılımların da sisteme bulaşmasına neden olarak bilgisayarın ya da mobil cihazın kaynaklarını tüketebildikleri gibi, internet kaynaklarını da kullanarak bilgisayarın ya da mobil cihazların yavaşlamasına sebebiyet verebilirler.

Bu tür güvensiz yazılımlardan korunmak için dikkat edilmesi gereken kuralları şu şekilde ifade etmek mümkündür.

- Kırılmış yani crack denilen program sitelerinden, oyun sitelerinden, sohbet sitelerinden, pornografik içerik barındıran sitelerden, zararlı yazılım barındırdığından şüphelenilen risk oranı oldukça yüksek internet sitelerinden kaçınılmalı,
- İnternet sitelerinde dolaşırken açılır pencere şeklinde çıkan mesajları okumadan "evet" ya da "tamam" düğmesi tıklatılmamalı, "bedava kazandınız, tıklayın" benzeri mesajların olduğu pencerelerin açıldığı internet sitelerinden uzak durulmalı,
- E-posta ile gelen bir eklentiyi açmadan önce kaynağı kontrol edilmeli, eklenti virüs taramasından geçirilmeli ve e-posta içinde gelen bağlantıları açmadan önce hedef internet sitesi veya sayfası kontrol edilmeli,
- Kaynağı belli olmayan ya da kaynağından emin olunmayan korsan yazılım içerebilen USB bellekler veya CD'ler bilgisayardan uzak tutulmalı,
- Eğer kurumsal alanlardaki sistemler kullanılıyorsa kurum politikalarına uygun hareket edilmeli, kurum tarafından belirlenmiş yazılımların dışında bilgisayarlarda program bulundurulmamalı, kurumdaki ilgili birimin haberi olmadan yazılım kurulum yapılmamalı ve gereksiz yazılımlar sistemden kaldırılmalı,

Yazılımlar her ne kadar iyi olsalar da bazı zamanlarda bunlarda da hatalar ve eksiklikler bulunabilir. Bu hatalar ve eksiklikler gerekli güncellemelerle düzeltilmez ve sis-

temlerdeki hatalar giderilmezse dışarıdan gelebilecek virüs ve benzeri saldırılara açık hale gelebilir. Bu durum güvenlik açığı gibi zafiyetlere sebebiyet verir. O açıdan bir sistemde ya da uygulamadaki bir açığın tespit edildiği andan itibaren en kısa zamanda kapatılması gerekir. Onun için gerekli güncellemelerin yapılarak sistemin ya da uygulamanın güncelliğinin sağlanması son derece önemlidir. Kullanıcıların sistemlerindeki ya da uygulamalarındaki güncelleme özelliğini açık tutmaları ya da yayınlanan güncellemelerin sürekli takip edilerek bilgisayarlara gerekli kurulumların hızla yapılması gerekir.

Tüm tedbirlerin alınmasına rağmen bilgisayara ya da bilgisayar özelliği gösteren cihaza zararlı program bulaştıysa ya da bulaşıldığından şüphe duyuluyorsa zaman kaybetmeden eğer kurumsal bilgisayar ise kurumdaki sorumlu birime haber vermek, kişisel bilgisayarsa işin uzmanından destek almak gerekmektedir. Bu durumda ilgili uzman kişilerce bilgisayardaki durum tespit edilerek gerekli temizleme işlemi yapılacaktır. Bireysel olarak kullanıcı, lisanslı ve güncel bir antivirüs programı ile tarama yaparak bilgisayardaki virüslerin temizlenmesini, silinmesini, silinemiyorsa da karantinaya alınmasını sağlayabilmektedir. Tedbir olarak sonraki aşamada da bilgisayardaki güvenlik duvarının (firewall) aktif edilmesi, güncel değilse güncellenmesi, işletim sistemindeki güncellemelerin yapılması gerekmektedir.

Sonuç olarak kötücül yazılımlardan korunmak için;

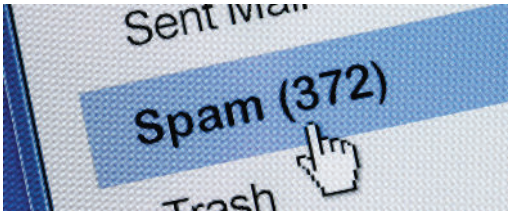
- Virüslerden korunmak için antivirüs, casus yazılımlardan korunmak için antispyware programların kullanılması,
- Kullanılan antivirüs ve antispyware programların periyodik olarak güncellemelerinin yapılması,
- Bilgisayar veya mobil cihazlardaki işletim sistemlerinin güncelliğinin sağlanması, işletim sistemindeki güvenlik duvarının aktif hale getirilmesi, lisanslı programların kullanılması,
- İnternette girilen sitelere ve indirilen dosyalara dikkat edilmesi, kaynağı belli olmayan adreslerden gelen e-postaların ve eklerinin açılmaması ve bunların antivirüs programı ile taranması gerekmektedir.

6. Spam & Phishing

Sanal ortamın siber suçluları, internet üzerinden insanları tuzağa düşürmek, e-posta yoluyla veya bir mesaj yoluyla gönderdikleri bağlantıları açtırmak ya da içeriği zararlı olan herhangi bir yasadışı veya kötü amaçlı bir siteye yönlendirmek konusunda oldukça profesyonel ve başarılıdırlar. Öyle ki, gönderilen e-postalar, e-posta linkleri veya diğer yollarla iletilen açılır (pop-up) pencereler bir finans kurumu, e-ticaret sitesi, devlet kurumu veya herhangi bir işletme veya işyerinden gönderilmiş masum içerikler gibi görünebilir. Emin olunmadan ve doğruluğu araştırılmadan açılan e-posta linkleri kişinin mağduriyetine sebebiyet verebilmektedir.

Spam, istenmeyen önemsiz posta demektir. Diğer bir ifadeyle tanınmayan kişilerden veya üye dahi olunmayan web sitelerinden ve bilgi paylaşımında bulunulmayan kuruluşlardan gelebilmektedir. Genellikle bu e-postalar, reklam amaçlı veya kişiye maddi/manevi zarar vermek amaçlı gönderilen e-postalardır. Diğer bir ifade ile spam, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi olarak adlandırılır.

Spam genel olarak ise istenmeyen veya zarar veren davranışlar bütünü olarak da özetlenebilir. Buna, toplu mesaj göndermek, sosyal medyada yabancı kişilerle bilerek iletişim kurmak ve kötücül yazılım içeren bağlantıları başkalarına göndermek gibi birçok faaliyeti dâhil etmek mümkündür. Spam e-postaların bazen kötü amaçlı bağlantılara tıklamak veya kötü amaçlı yazılım indirmek aracılığıyla yayıldığını da unutmamak gerekir. Bir e-posta gönderisinin spam olup olmadığını anlamak için çok kısa bir araştırma yapmak yeterlidir. Bu araştırma için; e-posta gelen şirket araştırılıp şirketle iletişime geçilebilir.



Spam e-postaları azaltmak için alınabilecek birkaç önlem bu tür e-postaları tamamen bitirmese de azaltacaktır. Bu önlemler şu şekilde sıralanabilir:

- **E-posta programlarındaki filtrelerin etkinleştirilmesi:** Çoğu internet servis sağlayıcısı ve e-posta sağlayıcısı spam filtresi sunar. Ancak ayarlanan seviyeye bağlı olarak spam olmayan postaların engellenmesiyle de sonuçlanabilir. Bunun için filtrenin istenilen şekilde çalıştığından emin olmak için arada sırada önemsiz postaları kontrol etmek faydalı olabilir.
- **Spam ihbar edilmeli**: Çoğu e-posta sağlayıcısı e-postayı spam olarak işaretlemenin veya spam örneklerini ihbar etmenin yollarını sunmaktadır. Spam'i ihbar etmek aynı zamanda o mesajın doğrudan gelen kutusuna düşmesini de engeller.
- **Çevrimiçi ortamda bilgilerin kimle paylaşıldığından emin olunması:** Kişi e-posta adresini internet ortamındaki özellikle sosyal ağ profilinde saklamadığından veya kişisel bilgilerini sadece belirli kişilerle paylaştığından emin olmalıdır. İnternet ortamındaki üye olunan platformlarda gizlilik ayarları yapılarak e-posta adresinin herkesçe görülmesi önlenebilir.
- Gönderilen spam e-postalarda listeden çıkmak için remove yazıp cevaplayın yazsa bile kesinlikle bu e-postaların yanıtlanmaması gerekmektedir. Bu büyük olasılıkla bir işe yaramayacağı gibi aynı zamanda adresin doğruluğunun tespitine ve daha fazla spam iletisi alınmasına sebep olacaktır. Ayıca, bazı sitelere kayıt olurken verilen e-posta adreslerinin o kurum tarafından paylaşılabilme olasılığını göz ardı etmemek gerekir.

- E-posta adresini herkese açık haber grupları, sohbet odaları, internet sayfaları ve sosyal paylaşım sitlerinde herkesin görebileceği şekilde yayınlamamak gerekir. Açıktan yayınlamak gerekirse, adresi maskeleyerek yayınlamak gerekir. Çünkü bu davranış kişiyi internet sayfalarında dolaşan ve otomatik olarak e-posta adresi toplayan programlardan korumaktadır.

- Birden çok kişiye veya bir gruba e-posta gönderilirken kişilerin e-posta adreslerini gizli karbon kopya (BCC) bölümüne yazmak gerekir. Çünkü bu adresleri kimse göremediğinden, e-posta adresi toplamak için gönderilen mesajlar da amacına ulaşamamış olur.

- Bir internet sitesinde yapılan işlemden dolayı e-posta adresi istenildiğinde, sitenin gizlilik politikasını kontrol etmek gerekir. Çünkü e-posta adresi gönderilirken, diğer firma/kişilerle paylaşmaları için de izin veriliyor olabilir. Bir internet sitesine gönderilen bilginin başkalarıyla paylaşılmadığına dair bir ifade veya seçili bir kutucuk olup olmadığının mutlaka kontrol edilmesi gerekir.

- Kullanım amacına göre farklı e-posta adresleri kullanılabilir. Yani aile ve arkadaşlarla haberleşme için kişisel iletişim amacıyla sohbet odalarında, haber grupları veya sosyal ağlarda, alışveriş sitelerinde kullanmak gibi ayrı e-postalar oluşturulabilir.

Phishing, diğer adıyla oltalama; internet teknolojilerini kullanarak yasadışı yollardan internet kullanıcılarının kişisel bilgilerini, şifrelerini, kredi kartı bilgilerini ve kişilere e-posta yoluyla gönderilen sahte bağlantılar aracılığıyla ele geçirmesine denilmektedir. Yani bu yöntem, spam e-posta veya açılır pencere yoluyla yapılan bir aldatma yöntemidir.

Genellikle saldırgan önceden kurgulanan bir hikâye üzerinden, kullanıcıyı e-postanın güvenilir bir kaynaktan geldiğine inandırıp, özel bilgilerini (kredi kartı, şifre bilgileri gibi) ele geçirmeye çalışır. Bu tür oltalamalardan korunmak için dikkat edilmesi gerekenleri aşağıdaki şekilde sıralamak mümkündür:

- Kişisel ve mali bilgilerin bilinen/tanınan kişiler dâhil hiç kimseye e-posta yoluyla gönderilmemesi gerekir. Çünkü istekte bulunanlara güvenilse bile e-posta iletişimine güvenemezsiniz. Teknik olarak e-posta içeriğine izlediği yol boyunca erişilebilme olasılığı vardır.

- E-posta mesajlarındaki internet bağlantılarına tıklanılmaması gerekir. Gönderilen bağlantıları kontrol etmek ve internet sitesi adreslerini ziyaret etmek gerekir. E-posta ile gönderilen internet sitesinde şifreleme kullanıp

kullanılmadığı yani adresin başında "http" yerine "https" olup olmadığı kontrol edilmelidir.

- Zararlı programlara karşı korunma programları (Antivirüs, anti-spyware, güvenlik duvarı) gibi güvenlik yazılımları kullanmak ve bu programları sık sık güncellemek gerekmektedir. Çünkü bazı taklit (oltalama) e-postaları, bilgisayara zarar verecek veya yapılan işlemleri izleyebilecek yazılımlar içeriyor olabilir. Kişi fark etmeden bulaşan zararlı yazılımlar varsa güncel korunma programları bunları yakalayabilir.

- Düzenli olarak kredi kart hesap özeti, banka bildirimleri gibi bilgilendirme dokümanlarını gözden geçirmek gerekmektedir. Taklit e-postalar ve taklit web siteleri hiç şüphe çekmemek için son derece profesyonel olarak hazırlanmış olabilir. Hatta kişi fark etmeden bilgileri ele geçirilmiş olabilir. Şüphelenilen kullanımlar olursa, hemen yetkililere bildirilmesi gerekir.

Tüm bunlarla birlikte bazı e-postalar ilginç ve merak uyandıran konu başlıkları (ölümcül hastalık, hediye, acil haber, uyarı, komplo teorisi gibi) ile duygu sömürüsü yaparak e-postanın başkalarına gönderilmesini ya da herhangi başka bir eylemde bulunulmasını talep edebilirler. Ayrıca bu tür mesajlarda bedava tekliflere, yardım taleplerine rastlamak mümkündür. Bu tür mesajların sonlarında genellikle gönderenin adı ve soyadı yazmaz veya yazar fakat araştırıldığında isim ile ilgili somut bilgiler bulunmaz. E-posta içerisinde bunu tanıdıklarına gönder, bu mesaj aldatmaca ya da şehir efsanesi değildir şeklinde ifadeler bulunabilir. Mesajın dilinde anlamsal olarak bozukluklar, dil ve mantıksal açıdan hatalar bulunur. Ayrıca mesajı gönderen, kişide güven duygusu oluşturmak için bu mesajın kişiye ulaşana kadar birçok kişiye gönderildiğine dair bilinçli olarak mesajda bulundurur. Böyle durumlarda mesajın hemen silinmesi gerekir.

7. Modem ve Kablosuz Ağlarda Güvenlik

Günümüzde internetsiz bir hayat düşünülemez hale gelmiştir. Bir anlamda internet bireylerin olmazsa olmazlarından olmuştur. Dünya nüfusunun yarıdan fazlası internete bağlıdır ve tüm dünyanın internete erişebilmesi için de yapılmakta olan çalışmalar ve projeler devam etmektedir. Günümüz teknoloji çağında artık birçok ev ve işyerinde internet bağlantısı bulunmaktadır. Masaüstü bilgisayarların, dizüstü bilgisayarların, tabletlerin, mobil aygıtların, televizyonların ve hatta nesnelerin bile internete bağlanabildiği bir çağın içindeyiz. İnternet güvenliğine, işletim sistemi güvenliğine, bilgi güvenliğine, parola ve şifre güvenliğine dikkat edildiği kadar internete bağlanma için kullanılan kablosuz ağ ve modem güvenliğine de dikkat edilmelidir.

Günümüzde evlerde kullanılan birçok modem kablosuz özelliğe sahiptir. Çünkü artık bir evde internete sadece bir birey değil evin diğer bireyleri de mobil cihazlarını kullanarak kablosuz modem aracılığıyla

bağlanmaktadır. Birden çok kişinin kullandığı bir kablosuz ağ üzerinden işlenebilecek bir suç durumunda ilk sorumlu internet abonesi olmaktadır. Bu tek başına büyük bir risktir. Bu açıdan kablosuz modemin tanınmayan kişilerce kullanılmaması önemli hale gelmektedir. Bununla birlikte bilinmeyen kablosuz ağlar kullanılarak internete girilmesi de bunun kadar riskli bir durumdur. Nasıl ki bir bilgisayarı virüsler, saldırılar gibi tehditlerden korumak için tedbir alınıyor ise modemi de farklı tedbirler alarak korumak gerekir. Örneğin, şifreli olmuş olsa bile kablosuz modemlerin kullanılmadığı zaman kapatılması hem güvenlik hem de sağlık açısından önemlidir. Bu kişinin evden çıkarken ocağı, kapıları, pencereleri kapatmasına benzetilebilir.

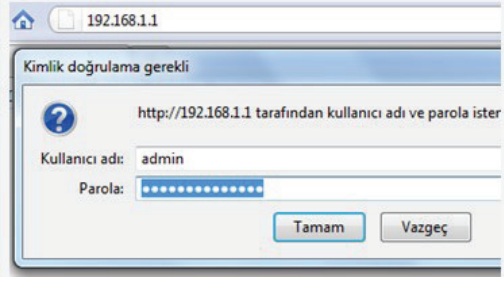
Siber saldırganların bilgisayar ile bilgisayarı internete bağlayan modem arasına girerek iletişimi dinleyebilme olasılıkları bulunmaktadır. İletişimi dinleyen bir saldırganın kişinin internette yaptığı işlemleri görmesi, kişisel bilgilerini ele geçirmesi ve hatta değiştirmesi mümkündür. Modemin yönetimini ele geçiren saldırgan, modem sahibinin yani abonenin haberi olmadan sakıncalı internet sitelerine erişebilir veya diğer sistemlere yönelik zararlı olabilecek eylemlerde bulunabilirler ki bu saldırganı değil aboneyi suçlu duruma sokar. Ayrıca bilgisayara erişme olanağı olmayan saldırganlar, modemdeki açıklardan faydalanarak kişinin bilgisayarına dolayısıyla kişisel verilerine de ulaşabilir. Bu sebeplerden dolayı modemlerin güvenliği önemlidir. Modemin kablosuz özelliği varsa, kablosuz yayın için gerekli olan güvenlik önlemleri de göz önünde bulundurulmalıdır.

Kablosuz modemin başkalarıyla paylaşılmasının birçok açıdan zararı söz konusu olabilmektedir. İyi niyetli olarak yapılan bu tür paylaşımlar, abonenin mağduriyetine kadar giden bir sürecin ortaya çıkmasına sebep olabilir. Eğer kotalı bir internet varsa, paylaşımdan kaynaklanan aşırı dosya indirme kotanın aşmasına, dolayısıyla fazladan bir ödemenin oluşmasına neden olacak ve abone ekonomik anlamda zarar görecektir. Kotalı ya da kotasız olsun kablosuz modemin paylaşılması çok fazla kişinin bağlanmasından kaynaklı olarak hızın azalmasına ve bağlantı veriminin düşmesine sebep olacaktır. Güvenlik boyutunda düşünüldüğünde, modemdeki açıklardan faydalanarak modemi ele geçiren saldırganın sistemlere siber saldırıda bulunması durumunda abonenin sorumlu tutulmasına, zararlı içeriklere, özellikle çocukların cinsel istismarı, çocuk pornografisi gibi tüm dünyaca suç kabul edilen sitelere girilmesi abonenin suçlu duruma düşmesine dolayısıyla mağdur olmasına sebep olur.

Modemlerden kaynaklı mağduriyet yaşamamak için, kablosuz modemlerin güvenlik tedbirlerinin alınması, kablosuz olsun ya da olmasın modemlerin yönetim paneline erişim parola ve şifrelerinin düzenlenmesi gerekmektedir. Genelde modemlerin ön tanımlı bir kullanıcı adı ve şifresi olduğu unutulmamalı ve mutlaka gerekli değişiklikler yapılmalıdır. Çünkü internette yapılacak küçük bir araştırma ile modemler için ön tanımlı gelen parolalar ve kullanıcı adlarının bulunması oldukça kolaydır. Diğer bir ifade ile modemlerin web üzerinden yönetilebilmesi için kullanıcı adı ve parola ile erişilen bir yönetim arayüzü vardır. Birçok

modem için ön tanımlı olarak gelen web yönetim arayüzü parolaları internette kolayca bulunabilmektedir. Bunun için bu parolaların mutlaka değiştirilmesi gerekir. Bir modemin web parola ve şifresini değiştirmek için aşağıdaki adımlar takip edilebilir.

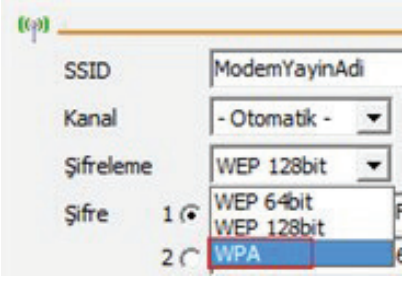
- Modemin kullanıcı kılavuzunda kullanıcı adı ve parolası ile ilgili bilgiler bulunmalıdır. Eğer öncesinde değiştirilmediyse genellikle kullanıcı adı "admin" olmakta ve modemin modeline göre şifresi aynı şekilde "**admin**", "**password**", "**12345**" gibi olabilmektedir. Modemin web yönetim ara yüzüne bağlanmakta kullanılan IP numarası ise genellikle "192.168.1.1" veya "10.0.0.1" şeklinde olabilmektedir.



- Modemin web ara yüzüne bağlanmak için internet tarayıcısının (browser) adres satırına IP numarası yazılır ve gelen kimlik doğrulama ekranından modemin kullanıcı kılavuzunda ifade edilen kullanıcı adı ve parolası girilir. Bu işlemden sonra modemle ilgili yönetim seçenekleri ekranı gelir. Bu ekran kullanılarak birçok ayarın değişikliğini yapmak mümkündür. Bu ara yüzde kullanıcı ve parolayı değiştirecek alan bulunarak gerekli değişiklikler yapılır ve değişiklikler kaydedilir.

Modemin web yönetim arayüzünden modemin kablosuz özelliği varsa onunda şifresi ve parolası belirlenebilir. Kablosuz modemler her yöne yayın yapan cihazlar olduğundan bu yayın herkes tarafından dinlenebilmektedir. Eğer şifre konulmamışsa herkes bunu kullanarak internete bağlanabilir. Kablosuz bağlantı için bir parola belirlenmiş olsa da eğer bilgiler şifrelenerek gönderilmezse (örneğin sohbet ederken) konuşmalar dinlenilebilir, parolalar görülebilir, gönderilen e-posta mesajları okunabilir. Bu nedenle şifreleme ayarı mutlaka belirlenmelidir. Kablosuz modemlerde şifreleme yapmak için WEP (Wired Equivalent Privacy - Kabloluya Eşit Güvenlik), WPA (Wi-Fi Protected Access - Wi-Fi Korumalı Erişim) , WPA2 (Wi-Fi Protected Access 2 - Wi-Fi Korumalı Erişim 2) olmak üzere üç standart şifreleme seçeneği sunulmaktadır. Bu seçenekler web yönetim arayüzünden belirlenebilir. WEP eskiden kullanılan bir yöntem olarak WPA kadar güvenli değildir ve artık pek kullanılmamaktadır. WEP şifreleme yönteminde yabancı birisi kolaylıkla şifreyi çözebilir. Bu nedenle modem ayarlarında şifreleme yöntemi olarak WEP yerine daha güvenli olan WPA veya WPA2 standardının seçilmesi tavsiye edilir. Bununla birlikte modemlerin birçoğunda sınırlı kabiliyete sahip olsa da yabancı kişilerin, davetsiz misafirlerin modeme ulaşmasını engelleyen bir güvenlik duvarı bulunmaktadır. Modemin web yönetim ekranından güvenlik duvarını aktif hale getirmek için "güvenlik duvarı etkin" olarak işaretlenmesi ve kaydedilmesi gere-

kir. Ayrıca kullanılmayan ve modeme internet üzerinden erişim için kullanılan tüm dış ağ servisler (ftp, snmp, telnet, icmp gibi) kapatılmalıdır. Bu da aynı şekilde modemin web yönetim ekranından yapılmaktadır. Tüm bunlara ek olarak MAC adresleri tanımlanarak fazladan güvenlik önlemi de alınabilir. MAC adresi, internete bağlanmak isteyen donanımın fiziksel adresi yani bir nevi kimliğidir. Modem yönetim ekranında MAC adresleri tanımlanarak, bunların dışındaki cihazların modemi kullanarak internete erişimi engellenmiş olur.



Modem güvenliği sağlanmazsa internete ve bilgisayara giren saldırganlar kişiye farklı şekillerde zararlar verebilir, bu kişilerin işlediği suçlardan modemin sahibi yani abone sorumlu tutulabilir. Bunun için, modemler gerekli tedbirler alınmadan asla kullanılmamalıdır. Sadece modemi korumak yetmez, yapılan kablosuz yayın için de güvenlik tedbirleri almak gerekir. Özetle:

- Kullanılmadığı zamanlar kablosuz modemler kapalı tutulmalıdır,
- Varsayılan parola kullanılmamalı ve modem yönetime ekranına ulaşmak için güçlü bir parola belirlenmelidir,
- Modemin varsayılan SSID (Hizmet Kümesi Tanımlayıcısı) adı yani diğer adıyla kablosuz ağ ismi değiştirilmeli ve kolaylıkla tahmin edilebilecek bir ad kullanmaktan kaçınılmalıdır,
- Kablosuz modemlerin şifrelemesi mutlaka açılmalıdır (WPA ya da WPA2 seçilmeli),
- Güvenlik duvarı aktif hale getirilmelidir,
- Uzaktan erişimi devre dışı bırakılmalı ve kullanılmayan servisler kapatılmalıdır,
- MAC adres filtrelemesi özelliği kullanılmalıdır.

8. İnternet Bankacılığı

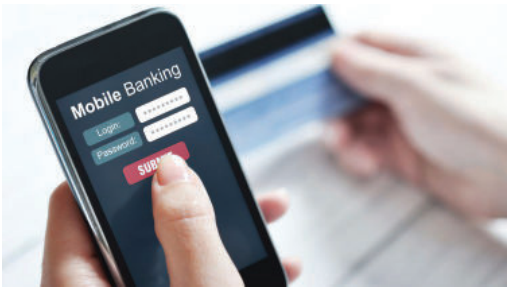
İnternet bankacılığı, banka şubesine gitmeden, çoğu bankacılık işleminin bilgisayar veya bilgisayar özelliği taşıyan mobil cihazlar kullanılarak internet üzerinden gerçekleştirilmesidir. Bir bankada yapılabilecek hemen her işlemi internet bankacılığı sayesinde daha kolay ve hızlı bir şekilde yapabilmek mümkündür. Bankacılığın geçmişine dönüp bakıldığında para göndermek, para almak, çek tahsil etmek, kredi kullanmak ve bunun gibi birçok işlemin süresi bir, iki haftayı hatta ayı bulabiliyordu. Her şeyin yazılı olarak yapılması ve uzun zaman alması gibi bir durum söz konusuydu. İnternetin gelişiyle birlikte bu yapılan işler elektronik ortama aktarılarak işlemler daha hızlı yapılmaya başlanmıştır. Bir kaç tıkla saatler alabilecek işlemler bitirilebilmektedir. Vakitten kazanç sağlaması, işlem masraflarının azlığı, istenilen her saatte işlem yapılabilmesi internet bankacılığını avantajlı kılmaktadır.

İnternet bankacılığı kişinin hayatına birçok açıdan kolaylıklar getirmiş olsa da bunu suistimal etmek isteyenler de olmaktadır. İnternet bankacılığını kullanan kişilerin kimlik bilgileri, hesap bilgileri, kart bilgileri çeşitli yöntemler (malware, botnet, spam, phishing, kimlik hırsızlığı, sosyal mühendislik) ile ele geçirilerek insanlar mağdur edilmektedir. İnternet bankacılığını kullananların güvenlik önlemlerinden ve yaşanabilecek risklerden haberdar olması ve buna göre davranması mağduriyet yaşanmaması açısından son derece önemlidir.

İnternet bankacılığı içerisine kredi kartlarını da dahil etmek gerekir. Çünkü kredi kartları, sanal kredi kartları, akıllı kartlar, şifrematikler de internet bankacılığının araçları durumundadır.

İnternet bankacılığında hem bankanın hem de kişinin yani internet bankacılığını kullanan müşterinin alması gereken önlemler bulunmaktadır. Genel olarak bankalar, benzer güvenlik önlemleri almaktadır. İnternet bankacılığında maksimum güvenliğin sağlanması için her iki tarafın yani bankanın ve müşterinin üzerine düşen sorumlulukları yapması gerekir.

Bankanın sorumlulukları Bankacılık Denetleme ve Düzenleme Kurumu'nun internet bankacılığı ile ilgili yasal düzenlemeleri ile ortaya konmuştur. Bankalar, sunmakta oldukları internet bankacılığı hizmetleri için, bu hizmetlerin arz ettiği risk seviyelerine uygun ve güvenilir bir kimlik doğrulama mekanizması tesis etmekle yükümlü kılınmıştır. Müşterilerin, kurulan kimlik doğrulama mekanizmasından geçmeden hizmetlerden yararlanmasına müsaade etmeyecek bir yapının bankalar tarafından kurulması öngörülmüştür. Ayrıca bankalar, internet bankacılığı servisi için beyan ettiği veya müşterilerine taahhüt ettiği düzeyde servis sürekliliğini sağlayarak servis kesintisinin doğurabileceği hukuki sorumlulukları en aza indirmek üzere gerekli önlemleri almak zorundadır.



İnternet bankacılığında müşterinin yani kullanıcının da bazı sorumlulukları bulunmaktadır. Kullanıcılar ilk olarak çevrimiçi olarak gerçekleştirdikleri tüm işlemler için kullandıkları kullanıcı adı ve şifrelerinin güvenliğini sağlamak amacıyla bu bilgilerin 3. şahısların eline geçmemesi için gerekli önlemleri almalıdırlar. Bankalar yapılan sözleşmelerde müşterileri bu konuda uyarır ve müşterinin gerekli özeni göstermemesi sonucu ortaya çıkan durumlarda sorumluluğun tamamen müşteriye ait olduğunu bildirirler.

Nasıl ki bankalar hizmet sundukları bankamatiklerin güvenliğinden sorumlu iseler kullanıcılar da internet bankacılığı hiz-

metine giriş yaptıkları cihazların güvenli olduğunu kontrol etmekten sorumludurlar. İnternet bankacılığına giriş yapılan bir bilgisayarın, tabletin ya da cep telefonunun güvenliğini sağlamak için bir antivirüs programı kullanmak her zaman yeterli olmayabilir, kullanılan programların, tarayıcının ve işletim sisteminin üreticileri tarafından yayımlanan güvenlik güncellemelerinin de sürekli kontrol edilip kurulması gerekir. Kullanıcıların ortak kullanıma açık cihazlardan internet bankacılığı hizmetlerine erişim yaptığı durumlarda giriş bilgilerinin güvenliğinin sağlanması daha zor olacağından bu hizmetten faydalanırken kişisel cihazlarını kullanmaları önerilir.

Güvenliği sağlanmamış bir cihazdan giriş bilgileri kullanılarak internet bankacılığı hizmetinden faydalanıldığında gizli bilgiler 3. şahıslar tarafından rahatlıkla ele geçirilebilir. Kullanıcı adı ve şifrelerin bilgisayar ya da herhangi bir cihazda kayıtlı bulundurulması güncel bir antivirüs programına sahip olunsa dahi güvenli olmayabilir. Farklı yollardan kayıtlı bu bilgilere ulaşan 3. şahısların verdiği zarar tamamen kullanıcının sorumluluğundadır ve bankalar bu konuda alınmış mahkeme kararları sonucunda gerekli tüm önlemleri sağladığından kendileri tarafından herhangi bir mağduriyet giderme durumu söz konusu olmayabilir. İnternet bankacılığı giriş bilgilerinin 3. şahısların eline geçtiği düşünüldüğünde daha az zarar için banka bu konuda bilgilendirilmeli ve çevrimiçi işlemlerin banka tarafından kapatılmasının ardından yeni giriş bilgileri talep edilmelidir. Fakat bu bilgiler ile tekrar giriş yapmadan önce kullanılacak cihazların güvenliği gözden geçirilmelidir.

İnternet bankacılığı işlemlerinde kullanıcıların sorumluluğu az gibi görünse de en büyük sorumluluğun kullanıcılarda olduğu söylenebilir. Bu sorumluluğun yerine getirilmemesinden doğacak olumsuz durumlar ciddi maddi zararlara yol açabilir ve bunlar bankalar tarafından doğrudan kullanıcı hatası olarak görülebilir. Bu maddi zararın azaltılması için alınabilecek bir diğer önlem de çevrimiçi işlemlere getirilecek kısıtlamalardır. Bankalar çevrimiçi işlem yapılabilmesi için müşterilerinden onay aldıkları gibi internet bankacılığı hizmetleri üzerinden yapılabilecek işlemlerin kısıtlanması ile ilgili bir düzenleme de yapmaktadır. Havale ve EFT işlemlerinin boyutlarına ve kredi kartı harcamalarına günlük limit ya da miktar kısıtı getirildiğinde kullanıcı hatasından kaynaklanabilecek dolandırıcılıklarda zarar en aza indirilebilir. İnternet bankacılığında dikkat edilmesi gerekenleri aşağıdaki şekilde sıralamak mümkündür:

- İşletim sistemi düzenli olarak güncellenerek olası güvenlik açıklarının kapatılması sağlanmalı, işletim sisteminin varsa firewall özelliği açık tutulmalıdır.
- Kullanılan internet tarayıcının mobil ya da masaüstü en güncel sürümü kullanılmalı ve her zaman güncelliği sağlanmalıdır.

- Mutlaka otomatik güncelleme seçeneği açık olan bir antivirüs yazılımı kullanılmalı ve bu yazılım düzenli olarak güncellenmelidir.
- İnternet şubesine giriş yaparken kullanılan kullanıcı adı, şifre veya parola gibi bilgiler bilgisayarda kayıtlı tutulmamalı, ezberlenmelidir. Eğer kayıtlı tutulacaksa bu tür dosyaların tutulduğu dosya şifrelenmelidir.
- Bankanın müşteri hizmetleri telefonu not edilmelidir. Böylece mesai saatleri dışında oluşacak bir tehlikede de bankayla iletişim kurmak hızlı olacaktır.
- Düzenli olarak banka hesap hareketleri ve bakiye gözden geçirilerek şüpheli işlemlerin olup olmadığı kontrol edilmelidir.
- Site adresinin "https" ile başladığından emin olunmalı, tarayıcı adres satırında güvenlik kilidi olup olmadığı kontrol edilmelidir. Bir anlamda İnternet sitesinin güvenlik sertifikası olup olmadığı kontrol edilmelidir.
- Yabancı kişilerden gelen (özellikle ilişiğinde dosya bulunan) e-postaları açılmamalı; bankadan gelmiş gibi görünüp, şifre, kullanıcı kodu, finansal bilgi, hesap numarası / kredi kartı ya da banka kartı numarası soran ya da kişisel bilgileri güncellemeyi isteyen e-postalar asla dikkate alınmamalıdır.
- İnternet şubesi şifresini belirlerken doğum yılı gibi kolay tahmin edilebilecek bir rakam birleşimi oluşturulmaması ve şifrenin düzenli olarak değiştirilmesi güvenlik için gereklidir. Bu şifrenin, diğer bankacılık şifreleriyle aynı olmamasına da ayrıca özen gösterilmelidir.
- Akıllı şifre, tek kullanımlık şifre kullanılmalıdır. İnternet işlemlerinde ekstra güvenlik sağlayan ve kişiye özel PIN Koduyla çalıştırılabilen "Tek Kullanımlık Şifre" üretme uygulaması/cihazı tercih edilmelidir.
- İnternet bankacılığı işlemleri asla bilinmeyen yabancı bir bilgisayarda ya da internet kafelerde yapılmamalıdır.
- Gelen e-postalarda, "internet bankacılığı güvenlik güncellemesi" yapılması isteniyorsa, kesinlikle inanılmamalıdır. Çünkü bankalar güvenlik güncellemelerini e-posta üzerinden talep etmemektedir.
- Cep telefonlarına yüklenmek istenilen uygulamalar mutlaka resmi uygulama mağazalarından (Google Play, Apple Store gibi) indirilmelidir. Bankanın mobil uygulaması da bu şekilde indirilmelidir.
- Bankanın kişiye önemli durumlarda ulaşması gerekebilir. Bu nedenle cep telefonu ve e-posta bilgilerinin, banka kayıtlarında her zaman güncel olmasına dikkat edilmelidir.
- İnternet bankacılığı için kullanılan bilgisayarın güvenliği çok önemlidir. İnternet şubesini kullanırken bilgisayarın başından kalkılmamalıdır. İnternet bağlantısının kesilmesi durumunda İnternet şubesi ekranı da kapatılmalıdır.

- İnternet Şubesi işlemleri, güvenliğinden emin olunmayan ve herkesin kullanımına açık bilgisayarlardan yapılmamalıdır.

9. Çevrimiçi Alışveriş

İnternet üzerinden alışveriş diğer adlarıyla çevrimiçi alışveriş ya da e-ticaret, bir elektronik ağ üzerinden ürün ya da hizmetlerin alım satımının yapılmasıdır. İnternet sayesinde alışveriş sistemi ve imkânları değişmiştir. Fiziksel mağazada ulaşabilecek kişi sayısı sınırlıyken, internetteki bir e-ticaret sitesinde sınırsız kişiye ulaşabilmek mümkün hale gelmiştir. Fiziksel mağazalarda sunulabilecek ürün sayısı kısıtlıdır. Tüm ürünleri sergilemek olanaksızdır veya bu çok yüksek maliyetlere sebep olabilir. E-ticaret ile sınırsız ürün sergilenebilir, üstelik bunun için ekstra maliyet de olmaz.

İnternet ortamında çevrimiçi alışveriş oldukça büyük kolaylıklar getirmiş olsa da dikkat edilmediğinde internetten alışveriş yapan kullanıcıların dolandırılmasına, mağduriyetine sebep olmaktadır. İnternet bankacılığında gösterilen güvenlik önlemleri hassasiyetini internetten alışveriş yaparken de göstermek gerekmektedir. Çevrimiçi alışverişte internet bankacılığının bir aracı olarak değerlendirilen kredi kartları kullanmaktadır. Çevrimiçi alışverişte internet sitesinin güvenilirliği, ödeme aşamasında kredi kartı bilgilerinin güvenliğinin sağlanması, güvenli bir ödeme için oldukça önemlidir.

Bu konuda herhangi bir mağduriyetin yaşanması alınacak tedbirlerle en aza indirilebilmektedir. Kullanıcının internetten alışveriş yaparken nelere dikkat edeceğini bilmesi yani bilinçli bir müşteri olması son derece önemlidir. Çevrimiçi alışverişte aşağıdaki konulara dikkat edilmesi yaşanabilecek mağduriyetleri azaltacaktır.

Bazı e-ticaret siteleri, e-ticaret sitesi bile değildir. Kendisini "e-ticaret sitesi" gibi gösterip büyük indirimler sağlayarak ziyaretçilere telefon, bilgisayar gibi nispeten pahalı ürünleri 5'te bir, bazen 10'da bir fiyatına satmayı vaat ederler. Çoğunda güvenlik sertifikası da bulunmayan bu sitelerin iyi tarafı, sizin paranızı çalmanın peşinde olmamalarıdır. Ama kötü tarafı da, bu sitelerin asıl amacının sizin bilgilerinizi çalmak olmasıdır. Evet, bu siteler sizden kredi kartı bilgisi istemez, onun yerine "kapıda kredi kartıyla veya nakit ödeme" vaadiyle yalnızca isminizi, telefon numaranızı ve adresinizi ister ve ürünün size kargoya verileceğini müjdeledikten sonra başka hiçbir şey yapmazlar. Bu sitelerin sahipleri, elde ettikleri bilgilerle size masum ama rahatsız edici reklam SMS'leri yollayabilecekleri gibi, son yıllarda meşhur olan bir dolandırıcılık yöntemini uygulayıp sizi arayarak "Banka hesabınız teröristler tarafından ele geçirilmiş, ben savcıyım/polisim, bize şuradan para yollayın gereken işlemleri yapıp davayı kapatalım" diye insanları korkutarak paralarını alabilirler. Bu sitelerden kesinlikle uzak durulmalıdır.

Güvenli bağlantıya sahip olmayan sitelerden alışveriş yapılmamalıdır. Bütün e-ticaret siteleri, "SSL sertifikası" denen bir güvenlik sertifikasına sahip olmalıdır ve her türlü satış işlemini bu sertifikayla yapmak

zorundadır. E-ticaret sitelerinde bu sertifikanın olup olmadığını, adres çubuğunda yazan adresin başında "http" yerine "https" yazıyor oluşundan veya adresin hemen başında bulunan yeşil bir simgenin oluşuna bakılarak anlaşılabilir. Bu sertifika sayesinde gönderilen kredi kartı bilgileri şifrelendiği için, bu bilgilerin kötü niyetli kişilerin eline geçmesi daha zordur. Eğer bir e-ticaret sitesinde güvenlik sertifikası kullanılmıyorsa, o siteden alışveriş yapılmaması en doğru yaklaşım olacaktır.

Mesafeli Satış Sözleşmesi'ne uymayan yerli siteler yasal değildir: "Mesafeli Satış Sözleşmesi", Gümrük ve Ticaret Bakanlığı'nın yürürlüğe soktuğu 'Mesafeli Sözleşmeler Yönetmeliği'ne uygun bir sözleşme biçimidir ve Türkiye'de faaliyet gösteren bütün e-ticaret firmalarının bu sözleşmeye uyması ve her satışın son aşamasında kullanıcıya da bu sözleşmeyi onaylatması şartı bulunur. Eğer rastladığınız bir yerli e-ticaret sitesinde bir Mesafeli Satış Sözleşmesi yoksa satış tamamlanmadan önce müşteriye böyle bir sözleşme onaylatılmıyorsa, o e-ticaret sitesinin yasal bir site değildir. Sitenin yasal olup olmadığını Gümrük ve Ticaret Bakanlığı'nın oluşturduğu Elektronik Ticaret Bilgi Platformu'ndan (https://www.eticaret.gov.tr) öğrenmek mümkündür.

Bununla birlikte internet üzerinden alışveriş yaparken aşağıdaki uyarılar dikkate alınırsa yaşanabilecek mağduriyetler azaltılabilir.

- İnternetten alışveriş yaparken ürün alınacak e-ticaret sitesinin SSL sertifikası olup olmadığına dikkat edilmelidir. Bu sertifikaya sahip bir siteden alışveriş yapıldığında kredi kartı bilgileri özel bir şifreleme sistemi ile doğrudan bankaya aktarılır ve kesinlikle üçüncü şahısların eline geçme ihtimali bulunmaz. İnternet sitesinin SSL sertifikasına sahip olup olmadığı siteye girildiğinde ve ödeme sayfasına geçildiğinde adres çubuğunun sağ tarafında bulunan kilit işaretinden anlaşılabilir.
- Yaşanabilecek herhangi bir sorun neticesinde müşterinin başvurabileceği müşteri hizmetleri merkezinin açık adres ve telefonunun tüketici ile paylaşılması yasal bir zorunluluktur. Alışveriş yapılacak site bu şartları barındırmıyorsa oradan alışveriş yapılmaması önerilir.
- Hiçbir e-ticaret sitesi alışveriş esnasında kredi kartı şifrenize ihtiyaç duymaz. Müşteriden kredi kartı şifresini talep eden alışveriş sitelerinden uzak durulması gerekir.

- Alışveriş yapılacak e-ticaret sitesi internetten araştırılmalıdır. E-ticaret sitesi herhangi bir arama motorunda aratılıp, site ile ilgili şikâyetler olup olmadığına bakılmalıdır. Siteden alışveriş yapan bazı kullanıcılar beğendikleri ya da şikâyetçi olduğu ürünler hakkında farklı bir sitede yorum yapmış olabilirler. Bu yorumlar okunmalıdır. Çünkü çoğunluğun ne yönde yorum yaptığı site hakkında kişiye fikir verecektir. Fakat her şikâyet gerçek ya da haklı değildir, ancak bir e-ticaret sitesi son dönemde çok şikâyet aldıysa mağdur olma olasılığı göz ardı edilmemelidir.

- Fiyat karşılaştırma siteleri güvenilir alışveriş yapmanın en uygun araçlarıdır. Fiyat karşılaştırma sitelerinden sadece bir ürünün en ucuz fiyata nerede satıldığını öğrenmekle kalınmaz, aynı zamanda tüketicilerin mağazalar hakkında yaptığı yorumlara da ulaşılabilmek mümkündür. Bunları okumak bilgilendirici olabilir.

- Eğer bir mağazadan ilk defa alışveriş yapılacaksa öncelikle sitelerinde bulunan iletişim ve adres linklerinden bu bilgiler incelenmelidir. Muhatap olunacak şirketin gerçek bir adresi ve telefon numarası bulunup bulunmadığı kontrol edilmelidir. Adres ve telefon numarasını sitesinde paylaşmayan internet sitelerinden uzak durmak kişinin yararına olabilir.

- Kapıda ödeme yöntemi son dönemde çok kullanılıyor; ancak bir internet sitesinde sadece kapıda ödeme seçeneği varsa o sitenin sahte ürün satma veya müşteriyi kandırma olasılığının çok yüksek olduğu unutulmamalıdır.

- Bir ürünün piyasa fiyatının çok altında bedeller ile satılmasından mutlaka şüphe duyulmalıdır. Örneğin 3000 TL'lik bir cep telefonunu 200 TL'ye ya da 400 TL'lik bir ayakkabıyı 49,90 TL'ye satılma olasılığı yoktur. Böyle bir durumda alışveriş mağduriyet sebebi olabilir

- Bir ürün satın alınmaya karar verilmeden önce mutlaka satın alma yapılacak sitenin sosyal medya hesaplarını, yani Facebook, Twitter ve Instagram hesaplarını kontrol etmek faydalı olabilir. Hem son dönemde aldığı herhangi bir şikâyet vs. varsa onu görmek mümkün olur hem de en son paylaşımını ne zaman yaptığı kontrol edilmiş olunur.

- Ödeme kredi kartı ile yapılacaksa 3D Secure yönteminin kullanılması önerilir. Bu şekilde kredi kartının istenmeyen bir şekilde kullanılması engellenmiş olunur. Bu işlem karttan para çekilmeden önce cep telefonuna tekil bir onay şifresi yollanması ile sağlanır. Bu şifre ödeme ekranında girilmezse alışveriş tamamlanmaz.

- Ödeme ekranında http:// yerine https:// yazmasına ve alışveriş yapılan sitenin SSL sertifikası olup olmadığına mutlaka dikkat edilmelidir. Bu sertifika, kredi kartı bilgilerinin şifrelenmesini ve başkaları tarafından kopyalan-

masını engeller. Yani alışveriş yapılan internet sitesi kesinlikle kartın tüm bilgilerini göremez.

- Sanal kart kullanımı günümüzde oldukça yaygınlaşmıştır. Limiti çok yüksek olan ve gerçek hayatta kullanılan fiziksel bir kredi kartını kullanmak yerine, internet bankacılığını kullanarak bir sanal kart oluşturulabilir ve kullanılabilir. Çünkü sanal kartın limiti kişinin kendisi tarafından belirlenmekte ve kişi alışveriş yaptığında limit sıfırlanmış olmaktadır. Bu şekilde dolandırılma riski de azalmış olmaktadır.

- Başta BKM Ekspres olmak üzere birçok ödeme sistemleri var. Bu sistemlerde kredi kartı tanımlanarak kredi kartının ve e-ticaret sitesi ile araya bir kademe daha güvenlik duvarı konulmuş olunur.

- Alışveriş yapılan bilgisayarın ortak bir cihaz olmamasına dikkat edilmelidir. Güvenlik şifresi olmayan bir internet bağlantısından, internet kafe ve toplu taşıma araçları gibi alanlarda alışveriş yapılmamasına özen gösterilmelidir.

- Alışverişten sonra ekrana düşen ve e-posta adresine gelecek olan sipariş numarası mutlaka kaydedilmelidir. Herhangi bir sorun yaşanması durumunda bu numara ile çok daha hızlı işlem yapılmaktadır. Ayrıca sipariş takibini, satın alınan ürünün kargodaki durumunu da bu numara ile takip edebilmek mümkündür.

- Online alışveriş sitelerinin olmazsa olmazı mesafeli satış sözleşmesidir. Bu sözleşmeye dikkat edilmesi gerekmektedir. Müşteri bilgilerinin gizli kalmasına yönelik olan mesafeli satış sözleşmesi yoksa o siteden alışveriş yapılmaması gerekmektedir.

- Alınan ürün kargodan teslim alınmadan kargo görevlisi ile beraber ürün mutlaka kontrol edilmeli ve üründe sorun varsa almayıp geri gönderilmelidir.

- İnternetten alışveriş yapılırken bilindik ve genel kullanıcı memnuniyetini kazanmış e-ticaret şirketleri tercih edilmelidir.

10. Ebeveyn Denetim Araçları

İnternetin öncü rol üstlendiği hızlı teknolojik gelişmeler, bilgisayar/internet okuryazarlığını daha da önemli hale getirmiştir. Çünkü gelinen noktada bireylerin işlerini görmek için bunun zorunluluk olduğunun göz ardı edilmemesi gerekmektedir. Günümüzde bilgisayarlar ve bilgisayar özelliği taşıyan, her an çevrimiçi olmaya olanak sağlayan mobil telefonlar, tabletler gibi akıllı cihazlar çocuklar başta olmak üzere tüm kullanıcılar için eşsiz birer öğrenme aracı olduğu kadar eğlence ve iletişim dünyasına açılan bir kapı görevi görmektedir. Özellikle çocukların bu tür cihazları kullanırken denetimsiz bırakılması şiddet içeren oyunlarla ya da zararlı içeriğe sahip uygunsuz internet sitelerle karşılaşma olasılığını artırmaktadır.

Tüm bunlar dikkate alındığında ebeveyn denetim araçlarının kullanılmasının ne denli önemli olduğu ortaya çıkmaktadır. Bunun için yasakçı bir yaklaşımdan uzak çocukların internet aktivitelerinin takip edilmesi, bu ortamın zararlarından onları koruyabilmek adına önemlidir. Burada amaç çocuğun internete girmesini yasaklamak değil, yaşına uygun olmayan ve psikolojik olarak çocuğu etkileyebilecek zararlı içeriklerden onu korumaktır. Bu şekilde ebeveynler, çocuklarının oynayabileceği oyunları, kullanabilecekleri programları ve ziyaret edebilecekleri internet sitelerini belirleyebilmektedirler. Ayrıca ebeveynler, çocukların bilgisayar kullanım zamanlarını diledikleri gibi atayabildikleri denetimler sayesinde, evde olmasalar bile kontrolü ellerinde bulundurabilmektedirler.

Bilgisayarlarında Windows işletim sistemi kullanan ebeveynler. İşletim sisteminin "Ebeveyn Denetimleri" ile ilgili ayarları işletim sisteminin Denetim Masası'nda yer alan kullanıcı hesapları bölümünü kullanarak zaman sınırlaması, oyun sınırlaması ve uygulama sınırlaması yapabilmektedir. Bunun yanında işletim sisteminden bağımsız filtreleme programları kullanılarak da bunlar gerçekleştirilebilmektedir. Kullanıcının kullanacağı filtreleme programının lisanslı olması son derece önemlidir. Bununla birlikte 2011 yılından beri hizmet vermekte olan Güvenli İnternet Hizmeti de internetteki zararlı içeriklerden koruma sağlayan, aynı zamanda ücretsiz olarak sunulan önemli bir seçenektir.

11. Güvenli İnternet Hizmeti

Güvenli İnternet Hizmeti, İnternet servis sağlayıcıları tarafından 22.11.2011 tarihinden beri bireysel ve kurumsal internet abonelerine ücretsiz olarak sunulan ve internetteki zararlı içeriklerden büyük oranda koruma sağlayan filtreli alternatif bir internet erişim hizmetidir. Bu hizmeti, internet servis sağlayıcıları tarafından sunulan merkezi bir filtreleme sistemi olarak düşünmek mümkündür. Bu hizmeti almak isteyen bireysel veya kurumsal internet abonelerinin bilgisayarlarına herhangi bir program kurmasına gerek yoktur. Bireysel ve kurumsal internet aboneleri Güvenli İnternet Hizmetinin ücretsiz bir tüketici hakkı olduğunu ve bu hakkı istedikleri an kullanabileceklerini unutmamaları gerekir.

İnternet servis sağlayıcıları bu hizmeti talep eden bireysel ve kurumsal internet abonelerine ücretsiz olarak sunmakla yükümlüdürler. Bu hizmet için herhangi bir isim altında abonelerden herhangi bir ücret ta-

lep edilemez. Bu hizmet zorunlu olmayıp hizmetin tercih edilip edilmemesi bireylerin ve kurumların özgür iradelerine bırakılmıştır. Dilediklerinde bu hizmeti talep edebildikleri gibi, diledikleri zaman da bu hizmeti kullanmaktan vazgeçebilmektedirler. Seçmek de seçmemek de abonenin tercihine bırakılmıştır. Bu sebepledir ki bu hizmetin sloganı "**Seçmek Özgürlüktür**" şeklinde belirlenmiştir. Bu hizmet, koruyucu ve önleyici tedbirler kapsamında internetteki zararlı içeriklere sahip sitelerden yüksek oranda koruma sağladığı için bireysel ve kurumsal abonelere önerilmektedir.

11.1. Güvenli internet hizmet profilleri (aile ve çocuk profili)

Güvenli internet hizmeti, Aile ve Çocuk Profili olmak üzere 2 profilden oluşmaktadır. Çocuk Profili; İnternetteki risklerden en yüksek oranda koruma sağlayan profildir. Çocuk Profili ile erişilebilen tüm siteler uzmanların kontrolünden geçmiş belirli kriterlere göre onaylanmış pozitif yani olumlu içeriklere sahip sitelerden oluşmaktadır. Çocuk Profili yabancı kişilerle temas kurulmasının önüne geçmektedir. Çocuk Profilinde sohbet ve sosyal medya siteleri gibi içeriğini herkesin değiştirebileceği siteler bulunmamaktadır. Çocuk Profilinde sabit içerikli oyun oynanabilmekte, çocuklarınızın rahatlıkla ödev yapabileceği yetişkin bir bireyin de haber okuyup bankacılık işlemleri yapabileceği sitelerden oluşan bir profildir.

Çocuk Profilinde; içeriği pozitif yani faydalı olduğu uzmanlarca onaylanmış sitelerden oluşan beyaz bir liste söz konusudur ve çocuk profilinde sadece bu listeye erişim vardır. Bu liste dışındaki siteler filtrelenmiştir. Beyaz kabul edilen bu listeye hemen her gün içeriği pozitif olan binlerce yeni site eklenmekte, var olan diğer sitelerin içeriğinin değişip değişmediği de periyodik olarak kontrol edilmektedir.

Aile Profili; müstehcenlik, şiddet, ırkçılık, kumar, intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama ve Atatürk aleyhine işlenen suçlar gibi yasadışı ve zararlı içerikleri barındıran siteler ile Sağlık Bakanlığı'nın zararlı olduğunu açıkladığı ürünlerin satıldığı siteler ve dolandırıcılık siteleri filtrelenmektedir. Aboneler dilerlerse oyun, sohbet ve sosyal medya sitelerini de bu filtre kapsamına dâhil edebilmektedirler.

11.2. Güvenli internet hizmeti ve arama motorları

Bu hizmetin en önemli özelliklerinden biri; bu hizmeti alan bireysel ve kurumsal internet aboneleri için sıklıkla kullanılan Google, Yandex, Bing gibi arama motorlarının abonenin hiçbir ayarlama yapmasına gerek kalmaksızın güvenli arama modunda

çalışıyor olmasıdır. Abone Güvenli İnternet Hizmetini almaya devam ettiği sürece bu devam eden bir hizmettir. Abone bu hizmetten çıkmadığı sürece arama motorlarındaki güvenli arama seçeneğinin devre dışı bırakılması söz konusu olmamaktadır.

11.3. Güvenli internet hizmetine geçiş ve daha fazlası

Arama motorlarında güvenli arama özelliğinin olması demek, bu ortamlarda gerek metinsel gerekse de görsel aramalarda uygunsuz müstehcen ve pornografik sonuçların filtrelenmesi anlamına gelmektedir. Hemen her arama motoru uygunsuz içerikleri filtreleyen güvenli arama özelliğini bünyesinde barındırmaktadır. Fakat bu özelliğin ayarlanması kullanıcının tercihine bırakılmıştır.

Teknik bilgisi olmayan internet kullanıcılarının arama motorlarındaki güvenli arama özelliğini aktif duruma getirmesi bazen mümkün olmayabilmektedir. Aktif yapılsa bile dijital yerliler olarak adlandırdığımız zamane çocukları ve gençleri bu özelliği kolaylıkla devre dışı bırakabilmektedirler. İşte Güvenli İnternet Hizmetinin farkı burada ortaya çıkmaktadır. Bu hizmete geçen internet abonelerinin fazladan bir işlem yapmasına gerek kalmaksızın güvenli arama özelliği, devre dışı bırakılamayacak şekilde otomatik olarak aktif hale gelmektedir. Abone Güvenli İnternet Hizmetinden ayrılmadığı sürece de bu özellik bu şekilde kalmaktadır.

Aboneler 5 farklı şekilde kolaylıkla Güvenli İnternet Hizmetine geçebildikleri gibi, istedikleri zaman bu hizmeti devre dışı bırakabilmektedirler. Bu yöntemleri aşağıdaki gibi sıralamak mümkündür:

- İnternet Servis Sağlayıcının bayisine başvurarak,
- İnternet Servis Sağlayıcının çağrı merkezine telefon ederek,
- İnternet Servis Sağlayıcının online işlem merkezine müşteri numaranız ve şifresi ile giriş yaparak,
- İnternet Servis Sağlayıcının belirlenen numarasına kısa mesaj (SMS) atarak
- İnternet Servis Sağlayıcının mobil uygulamasını kullanarak,

Bu hizmetin en önemli özelliklerinden bir diğeri de profil kapsamında girilemeyen siteler için ihbar/itiraz mekanizmasının olmasıdır. Örneğin herhangi bir profil kapsamında bir siteye giremeyen abone, bu sitenin bulunulan profilde görüntülenmesini talep edebilmektedir. Bu talep kapsamında ilgili site tekrar değerlendirilmekte ve itiraz haklı bulunulduğunda sitenin kategorisi değiştirilerek uygun profilde görüntülenmesi sağlanmaktadır.

Aboneler güvenli internet hizmetinin daha iyi bir noktaya gelebilmesi için karşılaştıkları zararlı ve uygunsuz içeriğe sahip siteleri

http://www.guvenlinet.org/ihbar adresinden bildirebilirler. Bununla birlikte sadece zararlı ve uygunsuz siteleri değil, içeriği pozitif yani faydalı olan internet sitelerini de değerlendirilmek üzere bildirebilmektedirler. Burada tavsiye edilen site bildirimi yapmadan önce söz konusu sitenin hangi profilde olduğunu http://www.guvenlinet.org/tr/domain_sorgula.html adresinden sorgulatmak ve buna göre bildirimde bulunmaktır. Güvenli İnternet Hizmeti konusunda bilgi edinmek, sıkça sorulan soru ve cevaplarını görmek ve daha fazlası için http://www.guvenlinet.org.tr adresi ziyaret edilebilir.

12. Bölüm Kazanımlar

Günümüzde en önemli kavramlardan biri bilgidir ve bilgi her dönemde değerli olmuştur. İnternetle birlikte bilgiye erişim kolaylaşmıştır. Bilginin korunması ve güvenliği oldukça önemli hale gelmiştir. Bilginin korunması noktasında gösterilecek zafiyet gizli kalması gereken bilginin başkalarının eline geçmesine ve mağduriyetlere sebep olabilir. Kişisel veriler, kişiye özgü ve onun izni dışında kullanılmaması gereken önemli bilgilerdir. Bunların korunması için gerek bireylere gerekse de bu bilgiyi elinde bulunduran otoritelere önemli sorumluluklar düşmektedir. Bilginin ve kişisel verilerin korunmasında bilgisayar ve internet güvenliği son derece önemlidir. Çünkü bilgiler bilgisayarlarda sabit disklerde ve internet ortamında depolanmaktadır. Bu bilgilerin korunması ancak bunlarla ilgili güvenlik önlemlerini almakla mümkündür. Bilgisayarlarda, telefonlarda, bankacılık işlemlerinde, internet ortamındaki e-posta başta olmak üzere kullandığımız tüm hesaplarımızda parola ve şifre güvenliği önemlidir. Kötücül yazılımlar bilgisayar sistemlerine zarar veren ve aynı zamanda parola ve şifreler başta olmak üzere kişisel bilgileri izinsiz ele geçirmeye çalışan yazılımlardır. Bu tür yazılımlarda virüs, casus yazılım ve solucanlar gibi zararlı eklentiler bulunmaktadır ve en önemli hedef kişisel bilgilerin ele geçirilmesidir. Sanal internet ortamında aldatıcı birçok internet sitesi bulunmaktadır, e-posta adreslerine dolandırıcılık amaçlı, aldatıcı sitelere yönlendirme yapan birçok istenmeyen spam e-posta gelmektedir. Modemlerde ve kablosuz ağlardaki güvenlik zafiyetleri internet abonelerinin mağduriyetine neden olabilmektedir. Şifrelenmemiş kablosuz ağlar kötü niyetli kişilerin internete çıkıp suç işleyebildiği ve mağduriyeti kablosuz modeme sahip abonenin yaşadığı durumlar olabilmektedir. İnternet bankacılığı ve internet üzerinden alışveriş kredi kartı güvenliğini, hesap güvenliğini alışveriş güvenliğini önemli ve gerekli kılmaktadır. Bilgisayarda ve internette güvende kalabilmek için güvenlik araçlarını, lisanslı antivirüs uygulamalarını kullanmak gerekmektedir. İnternet ortamındaki zararlı internet sitelerini filtreleyecek filtreleme uygulamalarına ve sistemlerine gereksinim vardır. Güvenli İnternet hizmeti bu gereksinimi önemli ölçüde karşılamaktadır. Bu bölüm sonunda internet kullanıcısı;

- Bilgi güvenliği kavramı hakkında bilgi sahibi olur ve bilgi güvenliği için alacağı tedbirleri bilir.
- Kişisel veri kavramını bilir, bu konudaki haklarının farkına varır, bu ve-

rilerini koruma noktasında yapması gerekenleri öğrenir.

- Bilgisayar ve İnternet güvenliği için alması gereken önlemler hakkında bilgi sahibi olur.
- Parola ve şifre güvenliğinin öneminin farkına varır. Bunları güvenli bir şekilde oluşturabilmek için nelere dikkat etmesi gerektiğini öğrenir.
- Kötücül ve zararlı yazılımlar hakkında bilgi sahibi olur ve bu konuda yapması gerekenleri öğrenir.
- Aldatma amaçlı istenmeyene e-postalar ve bu e-postalar yoluyla yönlendirilmek istenen web sitelerinin farkında varır. Oltalama kavramı hakkında bilgi sahibi olur.
- İnternet bankacılığı ve internet alışverişi nedir bilir ve bunlarla ilgili güvenli işlem yapabilmek için yapması gerekenleri öğrenir.
- Ebeveyn denetim araçlarının önemini kavrar ve bunları nasıl ayarlayabileceğini öğrenir.
- Güvenli İnternet Hizmeti filtreleme sistemi hakkında detaylı bilgi alır ve bu hizmete nasıl geçebileceğini öğrenir.

KAYNAKLAR

İnternette Güvenlik,

URL: http://www.guvenliweb.org.tr, Son Erişim tarihi, 06.06.2018.

Güvenli İnternet Hizmeti,

URL: http://www.guvenlinet.org.tr, Son Erişim tarihi, 06.06.2018.

Bilgimi Koruyorum,

URL: http://www.bilgimikoruyorum.org.tr, Son Erişim tarihi,06.06.2018.

Bilgisayar Güvenliği ve İnternet,

URL: http://bilgitoplumu.gov.tr, Son Erişim tarihi, 06.06.2018.

Eğitim Bilişim Ağı, Güçlü Parola Güçlü İnternet,

URL: www.eba.gov.tr, Son Erişim tarihi,06.06.2018.

Google Güvenlik Merkezi, Şifrelerinizin güvenliğini sağlama,

URL: https://www.google.com/intl/tr_tr/safetycenter/everyone/start/password, Son Erişim tarihi, 06.06.2018.

BÖLÜM 3 İNTERNETTE HAK VE SORUMLULUKLAR

İçindekiler

İletişim ve haberleşme teknolojilerinin geldiği nokta itibariyle günümüzdeki en önemli belki de vazgeçilmez araçlardan biri internettir. İnternet, haberleşmeyi günlük değil anlık ve hatta canlı hale getirmiştir. Gerçek hayattaki haklar ve özgürlükler bir anlamda internet ortamına taşınmıştır. Bu haklar ve özgürlükler beraberinde bireylere birçok kolaylıklar getirmiş olsa da aynı zamanda sorumluluklar da getirmiştir. İnternet ortamı için, "gerçek hayatta suç olan, internet ortamında yapıldığında da suçtur" ilkesi temel bir ilke olarak kabul edilmiştir. Bu ortam bireylere özgürlükler ve temel haklar noktasında her ne kadar birçok olanak tanıyor olsa da sonsuz bir özgürlük sunmamaktadır. Bireylerin özgürlük sınırı, bir başka bireyin özgürlüğünün başladığı yerde bitmektedir. Bu kural gerçek hayatta geçerli olduğu gibi internet ortamında da geçerli olan bir kuraldır.

İnternet, getirdiği birçok özelliği ile birlikte düşünceyi açıklama ve bunu yayma özgürlüğünün en etkili şekilde kullanıldığı haberleşme ve yayıncılık aracıdır. Ayrıca doğası gereği sınırsız özelliği sayesinde dünyanın her yerindeki bilgiye erişme ve tüm dünyaya düşüncelerini aktararak kendini ifade etme olanağı sağlayan bir yapıya sahiptir. Bilgi edinme ve ifade özgürlüğü kapsamında değerlendirilmesi gereken internet yayıncılığı kavramı ile temel hak ve özgürlüklerin birlikte düşünülmesi gerekir. Erişim ve bilgi edinme hakkı, ifade özgürlüğü, özel hayatın gizliliği, kişilik hakları, kişisel verilerin korunması, iletişim mahremiyeti gibi kavramların ele alınıp yorumlanması, hak ve sorumlulukların da temel hak ve özgürlüklerin temel ilkeleri doğrultusunda düzenlenmesi elzemdir.

Bu bölümde; insan hakları ve ifade özgürlüğü anlatılacak, internet başta olmak üzere iletişim konusundaki uluslararası düzenlemeler ve politikalar, internet ortamında temel haklar ve ifade hürriyeti içinde değerlendirilemeyecek olan siber zorbalık, nefret söylemi, kişilik haklarının ihlali, özel hayatın gizliliğinin ihlali, ırkçılık, çocukların cinsel istismarı gibi yasal olmayan içerikle mücadele başlıkları irdelenecektir. İnternetin etik ve ahlaki kullanımı konusunda bilgi verilecektir.

1. İnsan Hakları ve İfade Özgürlüğü

İnsan hakları, tüm insanların din, dil, ırk, ulus, etnik köken ve cinsiyet ayırımı gözetmeksizin doğduğu andan itibaren sahip olduğu ve yararlanabileceği temel hak ve özgürlükleri olarak tanımlanmaktadır. İnsan Hakları Evrensel Beyannamesi'nin ilk maddesinde "Bütün insanlar hür, haysiyet ve haklar bakımından eşit doğarlar…" ve ikinci maddesinde "Herkes, ırk, renk, cinsiyet, dil, din, siyasi veya diğer herhangi bir akide, milli veya içtimai menşe, servet, doğuş veya herhangi bir fark gözetilmeksizin bu haklardan ve bütün hürriyetlerden istifade edebilir" denilmekte ve bu haklar garanti altına alınmaktadır. İnsan haklarının yasal temelini, 10.12.1948 tarihli İnsan Hakları Evrensel Beyannamesi (İHEB) ve 04.11.1950 tarihli Avrupa İnsan Hakları Sözleşmesi (AİHS) oluşturmaktadır.

Türkiye, Avrupa İnsan Hakları Sözleşmesi'ni 1954'te onaylamış ve iç yasal mevzuatın bir parçası haline getirmiştir. Avrupa İnsan Hakları Sözleşmesi temel hak ve öz-

gürlükleri; yaşama hakkı, işkence, insanlık dışı veya küçültücü muamele yasağı, kölelik ve zorla çalıştırma yasağı, kişi özgürlüğü ve güvenliği, hak arama özgürlüğü ve adil yargılanma hakkı, suç ve cezaların kanuniliği, özel hayat, aile hayatı ve haberleşmenin gizliliği, düşünce, din ve vicdan özgürlüğü, ifade özgürlüğü, toplantı, dernek ve sendika kurma özgürlüğü, evlenme ve aile kurma hakkı, şikayet hakkı, ayrım yapma yasağı olarak belirlemiştir. Sonraki süreçte toplum hayatında meydana gelen gelişmeler paralelinde düzenlenen protokollerle bu haklara mülkiyet hakkı, eğitim ve öğrenim hakkı, seçim hakkı, yerleşme ve seyahat özgürlüğü gibi yeni haklar eklenmiştir.

Anayasal demokrasilerin en önemli bileşenlerinden birisi ifade özgürlüğüdür. İfade özgürlüğü bir düşünce, inanç, kanaat, tutum veya duygunun barışçı yoldan açıklanmasının veya dış dünyada ifade edilmesinin serbest olmasıdır. İfade özgürlüğü sözlü ve yazılı anlatım ile olabileceği gibi sanatsal gösterim, kişisel görünüm ve görüntü tercihi, gösteri, yürüyüş, toplantı yapma ve örgütlenme şeklinde de olabilir. İfade özgürlüğü kişinin kendini gerçekleştirmesine, kişisel gelişimine katkı sunan ve İnsan Hakları Evrensel Beyannamesi ile garanti altına alınan bir özgürlüktür. İnsan Hakları Evrensel Beyannamesi'nin 18'inci maddesinde "Her şahsın, fikir, vicdan ve din hürriyetine hakkı vardır; bu hak, din veya kanaat değiştirmek hürriyeti, dinini veya kanaatini tek başına veya topluca, açık olarak veya özel surette, öğretim, tatbikat, ibadet ve ayinlerle izhar etmek hürriyetini içerir." ve 19'uncu maddesinde "Her ferdin fikir ve fikirlerini açıklamak hürriyetine hakkı vardır. Bu hak fikirlerinden ötürü rahatsız edilmemek, memleket sınırları mevzubahis olmaksızın malumat ve fikirleri her vasıta ile aramak, elde etmek veya yaymak hakkını içerir." denilmektedir.

Bununla birlikte Avrupa İnsan Hakları Sözleşmesi'nin 10'uncu maddesinde ve Türkiye Cumhuriyeti Anayasası'nın 26'ıncı maddesinde düzenlenen ifade özgürlüğü ve sınırları AİHS'nin 10'uncu maddesinde;

> *"Herkes görüşlerini açıklama ve anlatım özgürlüğüne sahiptir. Bu hak, kanaat özgürlüğü ile kamu otoritelerinin müdahalesi ve ülke sınırları söz konusu olmaksızın haber veya fikir alma ve verme özgürlüğünü de içerir. Bu madde, devletlerin radyo, televizyon ve sinema işletmelerini bir izin rejimine bağlı tutmalarına engel değildir.*
>
> *Kullanılması görev ve sorumluluk yükleyen bu özgürlükler, demokratik bir toplumda zorunlu tedbirler niteliğinde olarak, ulusal güvenliğin, toprak bütünlüğünün veya kamu emniyetinin korunması, kamu düzenin sağlanması ve suç işlenmesinin önlenmesi, sağlığın veya ahlakın, başkalarının şöhret ve haklarının korunması veya yargı gücünün otorite ve tarafsızlığının sağlanması için yasayla öngörülen bazı biçim koşullarına, sınırlamalara ve yaptırımlara bağlanabilir." şeklinde ifade edilmektedir.*

Avrupa İnsan Hakları Mahkemesine (AİHM) göre de ifade özgürlüğü, toplumun ilerlemesi ve her insanın gelişmesi için gerekli koşullardan biri olan demokratik toplumun asıl temellerinden birini oluşturmaktadır. AİHS'nin 10'uncu maddesinde düzenlenen ifade özgürlüğünün kapsamına

sadece belli kişi ve gruplar değil herkes girer. Bu haktan gerçek ve tüzel kişiler, tüm kamu görevlileri, tutuklular ve hükümlüler ile yabancılar da yararlanır.

İfade özgürlüğü, Anayasa'nın 26'ıncı maddesinde "Düşünceyi açıklama ve yayma hürriyeti" kenar başlığı ile şu şekilde düzenlenmiştir.

> *"Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir.*
>
> *Bu hürriyetlerin kullanılması, millî güvenlik, kamu düzeni, kamu güvenliği, cumhuriyetin temel nitelikleri ve devletin ülkesi ve milleti ile bölünmez bütünlüğünün korunması, suçların önlenmesi, suçluların cezalandırılması, devlet sırrı olarak usulünce belirtilmiş bilgilerin açıklanmaması, başkalarının şöhret veya haklarının, özel ve aile hayatlarının yahut kanunun öngördüğü meslek sırlarının korunması veya yargılama görevinin gereğine uygun olarak yerine getirilmesi amaçlarıyla sınırlanabilir.*
>
> *Haber ve düşünceleri yayma araçlarının kullanılmasına ilişkin düzenleyici hükümler, bunların yayımını engellememek kaydıyla, düşünceyi açıklama ve yayma hürriyetinin sınırlanması sayılmaz. Düşünceyi açıklama ve yayma hürriyetinin kullanılmasında uygulanacak şekil, şart ve usuller kanunla düzenlenir."*

Anayasanın "Düşünce ve kanaat hürriyeti" kenar başlıklı 25'inci maddesi şöyledir:

> "Herkes, düşünce ve kanaat hürriyetine sahiptir. Her ne sebep ve amaçla olursa olsun kimse, düşünce ve kanaatlerini açıklamaya zorlanamaz; düşünce ve kanaatleri sebebiyle kınanamaz ve suçlanamaz."

Anayasanın "Temel hak ve hürriyetlerin sınırlanması" kenar başlıklı 13'üncü maddesi şöyledir:

> "Temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz."

Anayasanın "Milletlerarası antlaşmaları uygun bulma" kenar başlıklı 90'ıncı maddesinin son fıkrası şöyledir:

> "Usulüne göre yürürlüğe konmuş milletler arası antlaşmalar kanun hükmündedir. Bunlar hakkında anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz. Usulüne göre yürürlüğe konulmuş temel hak ve özgürlüğe ilişkin milletler arası antlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletler arası antlaşma esas alınır"

Sonuç olarak, ulusal ve uluslararası tüm bu düzenlemelerden hareketle insan hakları ve ifade özgürlüğünün temel hak ve özgürlükler kapsamında çok önemli bir yere sahip olduğu sabittir. Öyle ki bu hakların sınırlanması, AİHS'nin 10'uncu maddesinin 2'inci fıkrasındaki meşru amaçlara ulaşmak dışında başka sebeplere ya da sözleşmenin başka bir maddesindeki sınırlama sebeplerine dayanamaz. Sıradan sebeplere dayanarak meşru amaçlara ulaşmak için yapılan orantısız müdahaleler sözleşmeye aykırılık teşkil etmektedir.

2. İnternette İnsan Hakları ve İlkeleri

İnternetin çıkış noktası her ne kadar Amerika Birleşik Devletleri gibi görünse de hali hazırda internetin bir sahibi bulunmamaktadır. Hemen her gün büyüyen ve kontrolü zorlaşan bir ağ olan interneti kontrol etmek dünyadaki birçok ülkenin ve politik yapının arzu ettiği bir durumdur. Mevcut durum böyle iken, her devletin kendi milli hukuku ile internet ve sosyal ağ platformlarını düzenlediği görülmektedir. İnternetin düzenlenmesi milli hukuk ile sınırlı gibi gözükse de Avrupa Birliği Parlamentosu, Avrupa Birliği Komisyonu, Birleşmiş Milletler, Avrupa İnsan Hakları Mahkemesi, Avrupa Adalet Divanı, Amerikan Yüksek Mahkemesi veya İnternet Tahsisli Sayılar ve İsimler Kurumu yani diğer ifadeyle Internet Corporation for Assigned Names and Numbers (ICANN) gibi kurumlar interneti ve internetten doğan hakları düzenleme ve birincil merci olma görevini paylaşmakta ve kimi zaman da diğer ülkelere örnek olacak hukuk ve bağlantılı kurallar sistemleri geliştirmektedirler. İşte böyle çok aktörlü bir internet imparatorluğunda bireylerin, internet yönetimi altındaki haklarını ve bu haklara ilişkin yaptırım mekanizmalarını bilmesi daha da önemli hale gelmektedir.

Günümüzde internet sadece bir iletişim aracı olarak değil, aynı zamanda eğlence ve toplum dinamiklerini etkileyen ve devamını sağlayan sosyo-ekonomik bir yatırım aracı haline de gelmiştir. İnternetin yükselişi ile birlikte maliyetlerin diğer sektörlere göre azalması, yatırımcıları bu ortam için daha fazla yatırım yapmaya yöneltmiştir. Yatırımcılar için interneti cazip hale getiren en önemli sebeplerden birisi de internet ile ilgili referans alınabilecek tek ve küresel bir hukuk veya kanunun bulunmamasıdır. Bu durum yatırımcılara bu ortamda daha fazla kabiliyet alanı sağlamış ve üretkenliklerini gösterebilme olanağı sunmuştur.

Milyonlarca üyesi bulunan sosyal platformlarda yapılan kişisel paylaşımların akıbeti, dijital hakların, sorumlulukların ve hürriyetlerin tartışılmasına zemin oluşturmuştur. Bu durum dijital hakların tanımlanmasını ve uygulama alanlarını önemli hale getirmiştir. Twitter, Facebook gibi milyonlarca üyesi bulunan ağlarda ve bunlarla bağlantılı hesaplardaki bazı paylaşımlar, çok hızlı şekilde beğeni ve paylaşımın getirdiği viral bir etkiye sahip olmasından dolayı çok sayıda kullanıcıya ulaşmakta ve bazen bu paylaşımların çıkış noktası dahi tespit edilememektedir. Bunun sonucu olarak bu içeriği sağlayan içerik sağlayıcısının haklarının ve internetteki ifade özgürlüğünün sınırları gibi birçok konu da dijital hak ve hürriyetler kapsamındaki tartışmaya dâhil olmuştur.

Bununla birlikte, son yıllarda hemen hemen her şeyin internet ortamına taşınmasıyla birlikte her bir internet kullanıcısının birden fazla farklı platformlara üyeliği ve platformlarda kullanıcı kimliklerinde bulunan kişisel bilgilerin kimlerle paylaşıldığının bilinmemesi, hatta bazı durumlarda bunu bilme imkânının dahi bulunmaması kullanıcılarda "dijital bir körlük" oluşmasına neden olmuştur. Bir anlamda kullanıcıların hâkim olamadığı, hatta unuttuğu birçok üyelik ve bu üyeliklerde paylaşılan fakat kimlerle paylaşıldığı dahi bilinmeyen kişisel bilgilerin varlığı söz konusudur. Bu bağlamda, kullanıcıların kendi gizlilik ayarları üzerinde kontrol yetkisine sahip olması ciddi bir önem taşımaktadır. Kullanıcılar ancak bu sayede, kimlerle hangi bilgileri, ne zaman ve ne amaçla paylaştıklarını veya bu bilgilerin başkaları tarafından ne şartlar altında paylaşılacağını bilebilecek ve bu konuda bilinçli bir karar verebilecektir.

Mevcut yasal düzenlemelerde dijital haklar ve bu hakların kapsamına ilişkin henüz bir bildirgenin veya kanunun bulunmuyor olmasına karşın ülkeler, iç hukuklarında İnternet İnsan Hakları Bildirgeleri gibi kanun çalışmaları yapmaktadırlar. Diğer taraftan üniversitelerde de bu konuda önemli araştırmalar yürütülmekte ve bu araştırmaların kapsamı ve sayısı her geçen gün artarak devam etmektedir. Hali hazırda bu bildirgelerden en günceli ve en kapsamlısı Birleşmiş Milletler, İnternet Hakları ve İlkeleri Dinamik Koalisyonu tarafından hazırlanan "İnternette İnsan Hakları ve İlkeleri Şartı"dır. Bu şartta belirlenen "10 İnternet İlkesi" ile insan hakları odaklı bir internet ortamının sağlanması ve geliştirilmesi amaçlanmıştır.

İnternetin insan hakları farkındalığı noktasında benzersiz fırsatlar sunduğu, günlük hayatı kolaylaştırdığı ve hayatımızda önemi gittikçe artan bir rol oynadığı vurgulanan bildirgede; özel ve kamu teşebbüsleri de dâhil olmak üzere, tüm aktörlerin internette insan haklarını koruması ve bu haklara saygı göstermesinin büyük önem taşıdığı ifade edilmekte, bunun için de insan haklarının öngördüğü yükümlülüklerin en geniş kapsamda yerine getirilmesi için internetin işleyişi ve gelişiminin garanti altına alabilecek adımlar atılması gerektiğinin altı çizilmektedir. İnsan hakları odaklı internet ortamının gerçekleştirilebilmesi için gereken "On Hak ve İlke" aşağıdaki şekilde belirlenmiştir:

1) Evrensellik ve Eşitlik: Herkes eşit haklarla özgür doğar. Söz konusu haklara sanal ortamda da saygı gösterilmeli ve bu hakların devamı için gerekenler yapılmalıdır.

2) Haklar ve Sosyal Adalet: İnternet insan haklarının teşviki, korunması ve gerçekleştirilmesi ve sosyal adaletin ilerlemesi için bir alandır. Sanal ortamda herkes, diğer bireylerin insani haklarına saygı göstermekle yükümlüdür.

3) Erişebilirlik: Herkes güvenli ve açık internete erişim ve kullanım hakkına sahiptir.

4) İfade ve Örgütlenme: Sansür veya herhangi bir başka müdahale olmadan herkesin internette serbestçe bilgi arama, alma ve bilgi açıklama hakkı vardır. Ayrıca, herkesin internet ortamında ve internet aracılığıyla sosyal, politik, kültürel veya başka nedenler için özgürce bir araya gelme hakkı vardır.

5) Özel Hayatın Gizliliği ve Veri Koruması: Herkes sanal ortamda özel hayat/

mahremiyet hakkına sahiptir. Söz konusu hakka gözetlenmeme, şifreleme ve sanal ortamda anonimlik (bilinmeme durumu) hakkı dâhildir. Her bireyin kendi kişisel verilerini koruma hakkı vardır. Bu haklara veri tutma, işleme, saklama ve veriyi ifşa etme dâhildir.

6) Yaşam, Hürriyet ve Güvenlik: Yaşam, hürriyet ve güvenlik haklarına sanal ortamda saygı duyulmalı, bu haklar korunmalı ve hayata geçirilmelidir. Bu haklar sanal ortamda başkalarının haklarını ihlal etmek için kullanılmamalıdır.

7) Çeşitlilik: İnternette kültürel ve dilbilimsel çeşitlilik teşvik edilmeli ve ifade çoğulluğu için teknik ve politik metotlarda yenilik teşvik edilmelidir.

8) Ağ Eşitliği ve Tarafsızlığı: Herkes internet içeriğine öncelik ayırımı olmadan, ticari, politik veya sair sebeplerden kaynaklanabilecek filtreleme veya trafik kontrolünden bağımsız, evrensel ve açık internet erişimine sahip olmalıdır.

9) Standartlar ve Düzenleme: İnternetin mimarisi, iletişim sistemi, belge ve veri formatları açık standartlar esas alınarak düzenlenmeli ve bütünsel bir ortaklaşa çalışma, katılım ve herkes için eşit fırsat sunması sağlanmalıdır.

10) Yönetim: İnsan hakları ve sosyal adalet, İnternetin işleyişi ve yönetimi için esas alınan yasa ve kurallar temeline göre şekillendirilmelidir. Söz konusu şekillendirme açıklık, aktif katılım ve hesap vermeye dayalı şeffaflık ve çok yönlü bir biçimde yapılmalıdır. İnternette İnsan Hakları ve İnternet İlkeleri Şartı, İnternet Hakları ve İlkeleri Dinamik Koalisyonu tarafından oluşturulmuştur ve Gelişen İletişim Birliği'nin İnternet Hakları Bildirgesi ve diğer yürürlükte olan belgelerden ilham almıştır. İnsan hakları standartları uluslararası hukukta tanımlandığı şekliyle pazarlığa tabi değildir anlayışından hareketle bu şart, bu standartları yeni bir ortam olan İnternet ekseninde yorumlayarak açıklamakta ve insan haklarının hem sanal ortamda hem de günlük hayattaki önemini yeniden vurgulamaktadır. Ayrıca internet çağında hayata geçirilmesi gereken insan hakları konusunda gerekli olan sivil, politik, ekonomik, sosyal ve kültürel kalkınma aracı olarak internetin kullanılmasını desteklemeyi, İnternetin kapasitesini arttırmayı ve geliştirmeyi kapsamakla beraber internet politikası ilkelerini de tanımlamaktadır.

İnternet ortamı için belirlenen taahhütlerin yerine getirilebilmesi için, gerekli olan insan hak ve özgürlüklerinin dijital ortamda nasıl uygulanacağına dair ortak bir anlayış gerekliliğinden hareketle hazırlandığı ifade edilen "İnternette İnsan Hakları ve İlkeleri Şartı", internet ortamındaki ortak standartların belirlenmesi ve uygulanmasını amaçlamaktadır. Şartta bu taahhütler ve gerekçeler aşağıdaki gibi sıralanmaktadır:

- İnternetin insanların birbiriyle iletişim kurduğu ve buluştuğu bir yer, insanların, toplulukların ve kuruluşların temel fayda sağladıkları ve tüm insani ve sosyal alanlarda birçok farklı olay için çabaladıkları ortak alan olması,
- Düşük maliyetli internete erişimin, tüm insan haklarının ve temel hak ve özgürlüklerinin, demokrasinin, kalkınmanın ve sosyal adaletin tam

anlamıyla uygulanması için temel bir ihtiyaç haline gelmiş olması,

- İnternet denetim ve yönetiminin, altyapısından ve protokollerinden uygulamasına ve kullanımlarına kadar, insan haklarının, temel hak ve özgürlüklerin, demokrasinin, kalkınmanın ve sosyal adaletin gerçekleşmesi için doğrudan etkisi olması,
- İnsan haklarının ve temel haklar ve özgürlüklerin tam ve evrensel bir yararlanmanın sağlanmasına, söz konusu bu hakların internet ortamında da etkili olarak uygulanmasına bağlı olması,
- İnternetin, küresel doğası gereği, dünyadaki farklı insanları daha iyi anlama ve kabul etme, yerel ve bölgesel farklılıkları, çeşitli tarihi ve kültürel geçmişi gözetmeksizin daha iyi bir ortak bilgi alanını geliştirmede değerli bir ekonomik hazine olması,
- Evrensel, bölünmez ve birbiriyle ilişkili olan insan haklarının herhangi bir siyasi, ekonomik ve kültürel sistemden daha ağır basıyor olması,
- Kamusal ve özel geçmişinden dolayı internette insan haklarının tam olarak uygulanması ve bunun devamı için kendi üzerlerine düşen yükümlülükleri ve görevleri devlet ve toplumun diğer aktörlerinin yerine getirmesi gerekmesi,

İnternette İnsan Hakları ve İlkeleri Şartı'ndan hareketle internet ortamı için farklı başlıklarda ve bunların alt başlığında haklar sıralanmış, internetteki yükümlülükler ile genel şartlar ortaya konmuştur. İnternette erişim hakkı, ayrımcılığa uğramama hakkı, özgürlük ve kişi güvenliği hakkı, internet yoluyla kendini geliştirme hakkı, bilgi edinme özgürlüğü, internette din ve inanç özgürlüğü, internette örgütlenme özgürlüğü, özel hayatın gizliliğinin korunması hakkı, kişisel verilerin korunması hakkı, unutulma ve lekelenmeme hakkı, çocuk hakları, eğitim, bilgi ve diğer kültürlerle etkileşim hakkı gibi birçok haktan bahsetmek mümkündür.

2.1. İnternete erişim hakkı

Erişim hakkı; tek başına değerlendirildiğinde temel gereksinimlere erişim, sosyal ve sanatsal faaliyetlere erişim, okula erişim, bilgiye erişim gibi birçok hakkı çağrıştırmaktadır. 20. yüzyılın ikinci yarısı ve 21. yüzyılın ilk çeyreğinde yaşanan teknolojik ilerlemeler, interneti hayatımızın vazgeçilmez bir parçası yapmıştır. İnternet, beraberinde internete erişim hakkının da ortaya çıkmasına sebep olmuştur. Erişim hakkı denildiğinde akla ilk "İnternet Erişimi" gelmesi, bu teknolojinin hayatımızla ne kadar çok iç içe girdiğinin açık bir göstergesidir.

İnsanlık tarihine bakıldığında iletişim ve bilgiye erişimin birçok aşamadan geçerek günümüze geldiği görülmektedir. Bilgiye erişim ve iletişim, zamanın şartlarına göre farklılık göstermiştir. Resimlerin, kuşların, yaya ya da atlı ulakların kullanıldığı bir dönemden telsizlerin, telefonların, radyoların, televizyonların, gazetelerin kullanıldığı ve en nihayetinde internetin kullanılmaya başlandığı yüzyıllarca devam eden bir sürecin an itibariyle geldiği zirve noktasında

yaşanılmaktadır. Teknolojik gelişmelerin hızına bakıldığında bu zirvenin ne ilk ne de son zirve olacağını kestirmek zor gözükmektedir.

Bilgi ve iletişim teknolojilerindeki bu gelişmeler, küresel ağlar aracılığıyla sosyal ve iktisadi faaliyetlerin küresel çapta dolaşım kabiliyetinin artmasına neden olmuş, bireylerin bilgiye erişimini ve iletişim olanaklarını zenginleştirmiştir. Bu durum bireylerin yönetimsel kararlara katılımını sağlayan bir süreci başlatmış ve hızlandırmıştır. Bir anlamda bu gelişmeler; bir ülkedeki karar alma süreçlerinde ve alınan kararların uygulanmasında ilgili tüm aktörlerin etkin rol oynaması olarak tanımlanan yönetişim kavramının da ortaya çıkmasını sağlamıştır. Bu paydaşların en önemlisi hiç şüphesiz bireyler yani o ülkenin vatandaşlarıdır.

İnternete erişim hakkının olmaması durumunda bilgi, bireyler için pek fazla bir anlam ifade etmeyebilir. Bilgiyi anlamlı ve değerli kılan, bireylerin bu bilgiye erişebilmesi ve bundan faydalanabilmesidir. İnternet, bilgiye erişimi oldukça hızlandırmış ve kolaylaştırmıştır. Bu durum ister istemez internet erişiminin bir insan hakkı olup olmadığı konusunu tartışmaya açmıştır. Bunun nedeni; internetin benzersiz ve dönüştürücü doğasıyla, bireylere sadece fikir ve ifade özgürlüğünü sağlamakla kalmaması, bununla birlikte toplumun bir bütün olarak gelişmesini sağlaması ve diğer insan haklarını da destekliyor olmasıdır. Öyle ki internete erişim hakkının engellenmesi, bilgiye erişim hakkının engellenmesi şeklinde düşünülmeye ve algılanmaya başlanmıştır. Nitekim Avrupa İnsan Hakları Mahkemesi, Litvanya aleyhine verdiği bir kararda; güvenlik gerekçesiyle de olsa bir mahkûmun, yeterli ve meşru bir gerekçe ortaya konulmadan internet erişiminin engellenmesini, bilgiye erişim hakkının engellenmesi olarak değerlendirmiştir. Kararda ilgili ülkenin AİHS'nin 10'uncu maddesini ihlal ettiği ve mahkûmun belirli bilgilere erişim hakkının engellenmesinin "demokratik bir toplumda gerekli olarak görülemeyeceği" ifade edilmiştir.

İnternet erişimini temel bir insan hakkı olarak değerlendirmekten ziyade, ifade özgürlüğü başta olmak üzere temel bazı hakların etkili bir şekilde kullanılmasına yardımcı bir hak olarak değerlendirmek gerekmektedir. İnternet birçok açıdan önemli bir teknoloji olduğundan hareketle, bu teknolojiyi kullanmak bireyin hakkı olsa da bunu temel bir hak olarak değil, temel hak ve özgürlüklerin kullanılmasında önemli ve etkili bir araç olarak değerlendirmek daha doğru olacaktır. Bununla birlikte, BBC'nin 26 ülkede 27 bin kişiyle yaptığı bir araştırmada, Avrupa'da interneti hak olarak görenlerin oranının en yüksek olduğu ülke Türkiye olduğunu da hatırlatmakta fayda vardır.

İnternet erişiminin temel bir insan hakkı olarak değerlendirilmesi, kısa süreli de olsa bireylerin bu haktan mahrum bırakılmasının insanlık suçu olarak görülmesine neden olacaktır. Hali hazırda gelişmiş ülkelerde bile internet erişimi olmayan bir kesim olduğu düşünüldüğünde, dünyanın hemen hemen birçok ülkesinin insan haklarını ihlal eden ülke konumuna düşmesi olasıdır. Bazıları tarafından internet erişimi temel bir insan hakkı olarak kabul ediliyor olsa da bu hakkın temel bir insan hakkı olup ol-

mayacağını zamana bırakmak daha doğru olacaktır.

İnternete erişim hakkı, bireylerin çevrimdışı (offline) haklarının sanal internet ortamına yansıması olarak da değerlendirilen çevrimiçi (online) hak kavramını ortaya çıkarmıştır. Çevrimiçi haklar, diğer bir ifadeyle "Dijital haklar", bireylerin internet ortamında bilgiye erişebilme, içerik oluşturma ve bu içeriği yayma haklarını ifade etmektedir. Dijital hak kavramının ortaya çıkması bir anlamda artık internetin gerçek hayatla ayrılamayacak şekilde iç içe geçtiğinin bir göstergesidir. Hali hazırda "internet toplumu" diyebileceğimiz ve bugün dünya nüfusunun yarıdan fazlasının bu toplumun üyesi olduğu gerçek bir durum karşısında dijital hakların bilinmesi bireyleri internette daha özgür kılacaktır.

Herkesin interneti kullanma ve internete erişim hakkı vardır. Bu hak, İnternette İnsan Hakları ve İlkeleri Şartı'nda geçen tüm hakların temelini oluşturmaktadır. Günümüzde internet erişimi ve kullanımı, ifade özgürlüğü, eğitim hakkı, barışçıl nitelikli toplanma ve örgütlenme özgürlüğü, ülke yönetiminde yer alma hakkı, çalışma hakkı, dinlenme ve boş zaman hakkı gibi önemli insan haklarının tam olarak uygulanabilmesi için zorunluluk haline gelmiştir. İnternete erişim ve interneti kullanma hakkı insan hakları ile iç içe olduğu için vazgeçilmez bir hak halini almıştır. Kanunlara uyulduğu ve karşı gelinmediği sürece, demokratik bir toplumda ulusal güvenliği, toplum düzenini ve kamu sağlığını tehdit etmediği sürece, diğerlerinin hak ve özgürlüklerini kısıtlamadığı sürece ve bireylere tanınan diğer haklara riayet etmek koşuluyla, herkes internete erişim ve kullanım hakkına sahiptir. İnternete erişim ve kullanım hakkı; hizmet kalitesi, sistem ve yazılım seçme özgürlüğü, dijital ortama dâhil olmanın garanti altına alınması, ağ tarafsızlığı ve eşitliği gibi kavramları da içine almaktadır.

İnternete erişim için hizmet kalitesinin gelişen ve mevcut teknolojinin olanaklarına uygun olması önemlidir. Bireylerin internete erişmek için kullanacakları sistemleri ve yazılımları özgürce seçebilmeleri gerekmektedir. Bunu kolaylaştırmak, bağlantıda kalmayı ve yeniliklerin takibini sağlamak için erişim altyapısının ve protokollerin birlikte çalışabilir olması gerekir. Ayrıca her birey merkezi bir kurum veya kuruluştan izin almadan içerik, uygulama ve hizmet geliştirebilmelidir. Dijital ortama dâhil olan herkesin, çeşitli dijital medya araçlarına, iletişim platformlarına ve bilgi yönetimine erişebilmesi ve bunları etkili olarak kullanabilmesi bu hakkın kullanılabilmesi için önemlidir. Bu amaçla, tesis ve hizmet hususunda şahıs şirketlerine ve diğer kamu teşebbüslerine aktif destek verilmesi, telemerkezler, kütüphaneler, toplum merkezleri, klinikler ve okul gibi alanlarda kamuya açık internet erişim noktaları oluşturulmasına gereksinim duyulmaktadır. Ayrıca mobil medya araçlarıyla internete erişimin desteklenmesi dijital ortama dâhil olmanın garanti altına alınmasına katkı sunacaktır.

Bunlara ek olarak, internetin halka açık küresel bir ortam olduğundan hareketle bu ortamın mimarisinin korunup geliştirilerek özgür, açık ve bilgi değişiminde, iletişim ve kültürde ayrımcı olmayan bir araç haline getirilmesi oldukça önemlidir. Bunun için ekonomik, sosyal, kültürel veya politik se-

beplerden ötürü herhangi bir içeriğe veya gruplara özel imtiyazlar tanınmamalı veya onlara karşı bir engel konulmamalıdır. Bu görüş, internette eşitlik ve çeşitliliği geliştiren pozitif ayrımcılığı engelleyen bir yaklaşım değildir.

2.2. İnternet kullanımı, erişimi ve yönetiminde ayrımcılığa uğramama hakkı

Evrensel İnsan Hakları Beyannamesi'nin (EİHB) 2'inci maddesine göre: "Herkes, ırk, renk, cinsiyet, dil, din, siyasal ya da diğer görüş, ulusal ya da sosyal köken, mülkiyet, doğum ya da başka statüler gibi herhangi bir türde farklılık gözetilmeksizin bu bildiride düzenlenen bütün haklara ve özgürlüklere sahiptir." denilmektedir. Bu maddeden hareketle marjinal (uç) gruplar veya diğer gruplar için erişim eşitliğinin garanti altına alınması, erişimde cinsiyet eşitliğinin sağlanması gerekmektedir.

Erişim eşitliği kapsamında; toplumda yer alan bazı grupların diğer gruplara nazaran internetin etkili kullanılması ve bilgiye ulaşım noktasında daha sınırlı bir internet erişimine, internet erişim araçlarına veya sınırlı olanaklara mecbur bırakılması bu grupların internetin sağladığı insan haklarından mahrum kalmalarına sebebiyet vermektedir. Bu gruplar için erişim imkânlarının artırılması, etkili kullanıma ilişkin çabaların yoğunlaştırılması ve söz konusu eşitsizliklerin farkına varılarak giderilmesi hususunda gayret gösterilmesi gerekmektedir.

İnsan hakları çerçevesinde, herkesin onurlu yaşama, sosyal ve politik hayata katılma ve insan haklarına saygı duyulma gibi hakları vardır. Bu haklara bağlantılı olarak interneti kullanan her bireyin özel ihtiyaçlarının karşılanmasına gereksinim vardır. Bu kapsamda, yaşlıların, gençlerin, etnik veya dil kökenli azınlıkların, yerlilerin, engelli kişilerin ve her türlü cinsel kimlikten insanların bulunduğu söz konusu marjinal grupların ihtiyaçlarına özel ilgi ve özen gösterilmelidir. Öyle ki bütün donanım, kod, uygulama ve içerik, herhangi bir başka adaptasyon veya özel tasarım gerektirmeden, evrensel tasarım prensipleri göz önünde bulundurularak tasarlanmalı ve mümkün olduğu kadar büyük ve geniş ölçekteki kitlelere hitap etmesi gerekir. Bu aynı zamanda birden fazla dil ve metnin kullanılmasının teşvik edilmesini de içermektedir.

İnternete erişim noktasında kadın ve erkek eşitliğine aykırılık olmaması cinsiyet eşitliği açısından son derece önemlidir. Her kadın ve erkek internete erişme, interneti öğrenme, tanımlama, kullanma ve internetin şekillendirilmesinde eşit haklara sahiptir. Cinsiyet eşitliğini sağlamak adına kadınların internetin gelişme gösterdiği tüm alanlara katılımı gerekmektedir.

2.3. İnternette özgürlük ve kişi güvenliği hakkı

Evrensel İnsan Hakları Beyannamesi'nin 3'üncü maddesinde "Herkesin yaşama, hürriyet ve kişi güvenliği hakkı vardır." denilmektedir. Güvenlik konusundaki önlemler uluslararası insan hakları hukuk ve standartlarına uygun ve onlarla uyumlu olmalıdır. Diğer bir ifadeyle kanunla öngörülen istisnai haller dışında eğer alınan güvenlik önlemleri başka bir insan hakkını (mahremiyet hakkı veya ifade özgürlüğü gibi) sınırlıyorsa hukuka uygunsuzluk söz konudur. Eğer bir sınırlama olacaksa bu sınırlama kabul edilebilir gerekçeye dayanan kesinlikte olması ve dar anlamda tanımlanıp yorumlanması gerekmektedir. Yani, yapılan kısıtlamalar uluslararası hukuka uygun olarak tanımlanan asgari meşru neden ve gerekçelerle örtüşmeli ve orantılı olmalıdır. Bununla birlikte bu kısıtlamalar her hakkın uygulanması için gerekli olan ek kıstaslarla da örtüşmelidir. Söz konusu kesin çerçevenin dışına çıkan herhangi bir sınırlandırma olmaması gerekmektedir.

Bu kapsamda internet ortamında tüm suçlara karşı korunma ve internet güvenliğinin sağlanması ön plana çıkmaktadır. Herkesin internet üzerinde ya da internet aracılığıyla taciz, sanal takip, istismar, insan ticareti, kişisel verilerin kötüye kullanılması, özel hayatın gizliliğinin ihlal edilmesi, kişilik haklarının ihlal edilmesi gibi işlenen her çeşit suça karşı korunması gerekir. Buna ek olarak interneti kullanan herkesin güvenli bir bağlantıya sahip olması, bağlantısının güvenli olmasına gereksinim vardır. İnternet güvenliği, virüsler, kötücül yazılımlar, kimlik hırsızlığı gibi internet kaynaklı ve bağlantı güvenliğini tehdit eden risklerden korunmayı kapsamaktadır. İnternet güvenliğindeki eksiklikler, bireylerin haklarının ihlal edilmesine, mağdur edilmesine ve ifade özgürlüğünü tam olarak kullanamamasına yol açmaktadır.

2.4. İnternet yoluyla gelişme hakkı

İnternet bireylerin kendilerini geliştirme noktasında çok iyi bir öğretmen görevi görmektedir. Bilgiye erişimin kolay ve hızlı olması, belirli düzeyde fırsat eşitliğinin sağlanmış olması bireylerin kendilerine önceki yıllara oranla daha hızlı geliştirmelerine olanak sağlamıştır. 1986 yılında Birleşmiş Milletler (BM) Gelişim Hakkı Bildirgesi'nde tanındığı üzere, İnsan Hakları Evrensel Beyannamesi ile tanımlanan tüm insan haklarının tam olarak gerçekleşebilmesi için ekonomik, sosyal, kültürel ve politik gelişime ihtiyaç duyulmaktadır. İnternet, bu gelişimin sağlanması noktasında bireylere çok önemli ve vazgeçilmez bir imkân sunmuştur. Bu noktada, İnsan haklarının tam anlamıyla uygulanması, özellikle yoksulluğun, açlığın ve hastalıkların yok edilmesi ve cinsiyet eşitliğinin desteklenmesi ve kadının güçlenmesi bağlamında internet, büyük hayati öneme sahiptir. Gelişim hakkı da, bireylerin internet ile ilgili tüm haklardan yararlanmasını ve bu hakları kullanmasını öngörmektedir.

İnternet başta olmak üzere bilgi ve iletişim teknolojilerinin, yoksulluğun azaltılması ve insani gelişmenin güçlendirilmesine katkı sunacak şekilde tasarlanması, geliştirilmesi, kullanılması ve uygulanması elzemdir. Ayrıca bu teknolojilerin sürdürülebilir şekilde kullanılması, elektronik atıkların (e-waste) imha edilerek internetin çevreyi korumaya

yönelik kullanılması da çevresel sürdürülebilirlik açısından önem arz etmektedir.

2.5. İnternette ifade ve bilgi edinme özgürlüğü

Evrensel İnsan Hakları Beyannamesi'nin 19'uncu maddesine göre: "Herkesin fikir ve ifade özgürlüğü vardır; bu hak müdahale olmaksızın ifade özgürlüğünü ve herhangi bir sınırlama olmadan medya (mecralar) aracılığıyla fikirlere ait bilgileri araştırmayı, almayı ve açıklamayı içerir." denilmektedir.

Uluslararası Medeni ve Siyasal Haklar Anlaşması (UMSHA)'nda belirtildiği şekliyle ifade özgürlüğü bazı sınırlandırmalara tabi olabilir. Bu sınırlandırmalar, yasalar tarafından tanımlanabilir, başkalarının hak ve itibarlarına saygı duymak ve onları korumak amaçlı olabilir veya ulusal güvenliğin, kamu düzeni ve sağlığının veya ahlakın korunması gibi gerekli olan istisnai hallerde uygulanabilir. İfade özgürlüğünün yasa tarafından öngörülen istisnai haller dışında herhangi bir başka gerekçeyle sınırlandırılmasına izin verilemez.

Demokrasi ve insan gelişimi yanında diğer insan haklarından yararlanmanın sağlanabilmesi için ifade özgürlüğü her toplumda önemli bir yere sahip olmuştur. Bu kapsamda insan haklarını ve insan onurunu rencide etmeyecek medeni eleştiri veya protestolar internet yoluyla da yapılabilmekte ve bu sanal protesto özgürlüğü olarak ifade edilmektedir. Herkesin bu özgürlüğünü belirtilen kıstaslar ölçüsünde kullanabilmesi için herhangi bir engele yani sansürlemeye maruz kalmaması gerekmektedir. İnternette faaliyet gösteren aktörlerin insan haklarını ihlal etmeyen yani bu manada suç teşkil etmeyen içeriklerin çıkartılması için herhangi bir devlet kurumu veya diğer kişiler tarafından içerik kaldırmak, saklamak, engellemek veya internet kullanıcılarının bilgilerini ifşa etmek için baskı altına alınmaması gerekmektedir. Herhangi bir kısıtlama ve müdahale yapılması gerekiyorsa bunun, meşru neden ve gerekçelerle örtüşmesine ve orantılı olmasına dikkat edilmelidir.

Bireylerin internet yoluyla bilgi edinme, bilgi arama, bilgi alma ve fikirlerini açıklama hakları bulunmaktadır. Her bireyin ulusal ve uluslararası hukuk ölçülerine uygun olarak erişilebilir biçimde açıklanan kamusal bilgileri elde etme ve bu bilgileri etkin bir şekilde kullanabilme haklarını internette ifade ve bilgi özgürlüğü kapsamında değerlendirmek gerekir. Bu aynı zamanda basın özgürlüğü ve çoğulculuğa saygı duyulmasını da beraberinde getiren bir durumdur.

Ayrıca her bireyin gerçek ortamda olduğu gibi internet ortamında da başkalarının inanç ve fikirlerine saygı duyması gerekmektedir. Yani bireyin inancından ve fikrinden dolayı nefret söylemine maruz kalmaması inanç ve fikir hürriyeti noktasında son derece önemlidir. Nitekim Uluslararası Medeni ve Siyasal Haklar Sözleşmesi'nde; "Ulusal, ırksal ya da dinsel nefretin ayrımcılık, düşmanlık ya da şiddete kışkırtma şeklini alacak biçimde savunulması yasalarla yasaklanır" denmektedir. Elbette başkalarının insan haklarının ciddi anlamda zarar gördüğü durumlarda söz konusu bu insanların haklarını koruma amaçlı ifade özgürlüğünde bazı özel sınırlandırmaya gidilebilir. Ancak, bu sınırlandırmalar, bireyleri veya toplulukları korumak yerine

soyut veya öznel düşünce veya kavramları korumak için kullanılmamalıdır. Diğer bir ifadeyle bu bağlamdaki sınırlamaların ifade özgürlüğünün sınırlandırılması için gerekli tüm ölçütlerle bağdaşması gerekir.

2.6. İnternette din ve inanç özgürlüğü

Evrensel İnsan Hakları Beyannamesi'nin 18'inci maddesine göre: "Herkes düşünce, vicdan ve din özgürlüğü hakkına sahiptir" Bu hak, dinini ya da inancını değiştirme özgürlüğünü, dinini ya da inancını gerek tek başına gerekse de toplum içinde başkalarıyla birlikte, aleni veyahut özel şekilde öğretme, uygulama, ibadet etme, ya da gereklerini yerine getirme yollarıyla ortaya koyma özgürlüğünü içerir. Dolayısıyla bu kural sadece gerçek hayatta değil internet ortamında da bu hakların özgür bir şekilde kullanılmasını gerektirir. Her iki durumda bu hakkın kullanılmasına yönelik meşru gerekçelere ve hukuk kurallarına dayanmayan sınırlamalar ve engellemeler düşünce, vicdan ve din özgürlüğü hakkına müdahale olarak algılanacaktır.

Burada Avrupa İnsan Hakları Sözleşmesi'nin 9'uncu maddesi "Herkes düşünce, vicdan ve din özgürlüğüne sahiptir; bu hak, din veya inanç değiştirme özgürlüğü ile tek başına veya topluca, kamuya açık veya kapalı ibadet, öğretim, uygulama ve ayin yapmak suretiyle dinini veya inancını açıklama özgürlüğünü de içerir. Din veya inancını açıklama özgürlüğü, sadece yasayla öngörülen ve demokratik bir toplumda kamu güvenliğinin, kamu düzeninin, genel sağlık veya ahlakın ya da başkalarının hak ve özgürlüklerinin korunması için gerekli sınırlamalara tabi tutulabilir" diyerek bu hakkın kullanılamama istisnalarını ve sınırlama gerekçelerini de ortaya koymuştur. Şöyle ki bireyin bu hakkını kamu güvenliği ve düzenini bozmadan, genel sağlık veya ahlak ile başkalarının hak ve özgürlüklerini ihlal etmeyecek şekilde kullanması gerekir. Aksi durumda bunun sınırlanmasına yönelik yaptırım ile karşı karşıya kalınması durumu ortaya çıkacaktır.

2.7. Sanal toplantı (toplanma) ve örgütlenme özgürlüğü

EİHB'nin 20'inci maddesine göre: "Herkesin barışçıl toplanma ve örgütlenme hakkı vardır. Hiç kimse bir örgüte üye olmaya zorlanamaz." denilmektedir. Bunu sadece fiziksel mekânlarda toplanma şeklinde değil, internet ortamındaki toplanma ve örgütlenme şeklinde de düşünmek gerekir. Günümüzde internetteki binlerce blog, sosyal medya grupları göz önüne aldığında bu özgürlüğün kullanılmasını tek bir fiziksel alana hapsetmenin mantıksızlığı görülecektir.

İnternet ortamında toplantı ve örgütlenme özgürlüğünü, bireylerin her nedenle olursa olsun bir grubun, örgütün veya birliğin sayfasına üye olma, ziyaret etme şeklinde düşünmek gerekir. Fakat burada, ziyaret edilen veya üye olunan mecraların kamu güvenliğini ve düzenini bozmayan, genel sağlık ve ahlak ilkelerine riayet eden ve diğer bireylerin hak ve özgürlüklerini ihlal etmeyen yerler olması önem arz etmektedir. Aksi durumda meşru müdahale gerekçelerinin oluşması gibi bir durum ortaya çıkar ki bu durum internet ortamında toplanma ve örgütlenme özgürlüğünün kullanılmasını sekteye uğratır.

2.8. Özel hayatın gizliliğinin korunması hakkı

EİHB'nin 12'inci maddesine göre: "Hiç kimsenin keyfi veya yasal olmayan şekilde mahremiyetine, ailesine, evine veya haberleşmesine müdahale edilemez. Böyle bir müdahale veya saldırıda, herkesin kanuni korunma hakkı vardır." denilmektedir. Bireylerin özel hayatının gizliliği değerlidir ve korunmayı gerektiren en önemli haklar arasında yer alır. Özel hayatın gizliliğinin korunmasına yönelik hukuksak düzenlemeleri, bireylere verilen hizmetlerdeki gizlilik politikaları, ayarları ve standartları, sanal ortamdaki kişiliğin korunması, anonimlik ve şifreleme hakkı, gözetlenmeme ve izlenmeme hakkı, internet ortamında hakarete maruz kalmama hakkı gibi birçok kavramı bu kapsamda ele almak mümkündür.

Devletlerin vatandaşlarının kişisel verilerinin ve özel hayatlarının korunmasına yönelik hukuki düzenlemeler yapma zorunluluğu bulunmaktadır. Bu düzenlemelerin hem uygulamalı olması hem de caydırıcı etkiye sahip yaptırıma bağlı olması son derece önemlidir. Bu konuda yapılacak hukuki düzenlemelerin, uluslararası insan hakları ve tüketicilerin korunması ilke ve standartlarıyla uyumlu ve aynı doğrultuda olması gerekir. Bireylerin özel hayatının gizliliğini sadece bireyler ihlal etmeyebilir. Devletler ve şirketler de bu ihlali gerçekleştirebilir. Bunun için de yapılacak düzenlemelerin şirketlerin ve devletlerin de özel hayatın gizliliği ihlallerine karşı korumayı içerecek ve garanti edecek şekilde olmalıdır.

Devletin veya şirketlerin verdikleri hizmetlerde gizlilik politikalarının ve gizlilik ayarlarının kolay ulaşılabilir olması, bunların kontrol edilmesi ve yönetilmesinin kullanışlı olması, bireyin özel hayatının gizliliğinin ihlali noktasında önem arz eder. Özel hayatın gizliliğinin korunması noktasında bilişim sistemlerindeki gizlilik ve bütünlük standartlarının diğer kişilerin bu sistemlere erişimini önleyecek şekilde olmasına ve bu standartların korunmasına ihtiyaç bulunmaktadır. Bireyin sahip olduğu internet ortamındaki sanal kimliğin yani bilgi iletişim sistemlerinde tanımlanmış bireye ait kimliğin korunması gerekir. Bireyin izni olmadan bireye ait dijital imza, kullanıcı adı, şifre ve parola gibi kullanıcıya özel olan kodların kullanılmaması ve değiştirilmemesi, kişilerin sanal kimliklerine saygı gösterilmesi, kişinin sanal kimliğini kişiye veya başkalarına zarar vermek amaçlı kullanılmaması bireyin özel hayatını ihlal edilmemesi noktasında oldukça önemlidir.

Uluslararası düzenlemeler ve ulusal yasalara aykırı şekilde yapılan gözetleme ve izleme, bireyin özel hayatın gizliliğini ihlaldir. Herkesin keyfi bir gözetlenme veya dinlenme tehlikesi yaşamadan iletişim ve haberleşme özgürlüğü vardır. Eğer herhangi bir gözetim ve izleme olacaksa da gözetimin kabulünü içeren çevrimiçi hizmet erişim sözleşmesinde gözetimin ve izlenmenin içeriği açık bir şekilde belirtilmesi gerekmektedir.

Bireyin gerçek hayatta hakarete maruz kalmama ve rencide edilmeme hakkı internet ortamı için de geçerlidir. Gerçek hayatta yapıldığında suç olan bir şeyin internet ortamında da yapılması halinde suç teşkil edeceğinden hareketle bireyin internet ortamında hakarete maruz kalması gerek özel hayatın gizliliği gerekse kişilik haklarının ihlal kapsamında değerlendirilir. Hiç kimse

internet ortamında bir başkasının onuruna karşı hukuka aykırı saldırılarda bulunamaz. Herkesin bu tür müdahale veya saldırılara karşı hukuk tarafından korunma hakkı vardır. Fakat hakarete maruz kalmama hakkı ifade özgürlüğünü sınırlamak için bir gerekçe olarak kullanılmamalıdır ve olası bir sınırlama izin verilen dar sınırların dışına çıkmamalıdır.

2.9. Dijital verinin koruması hakkı

EİHB'nin 12'inci maddesinde de belirtildiği üzere herkes özel hayatın gizliliği hakkına sahiptir. Bu hakkın önemli bir kısmı kişisel verilerin koruması hakkı ile ilgilidir. Bu hak kişisel verilerin korunarak bireylerin özel hayatının gizliliğinin önlenmesi noktasında devletlere önemli sorumluluklar yüklemektedir. Kişisel verileri toplayan, depolayan ve işleyen kurumlara, kuruluşlara ve yönetimlere caydırıcı yaptırım uygulanabilmesi ve bilgisi toplanan bireylerin haklarının korunması ve teminat altına alınması için uluslararası hukuka uygun olacak şekilde ulusal mevzuatın düzenlenmesine gereksinim bulunmaktadır.

Verilerin toplanmasında veriyi toplayanların yükümlülükleri bulunmaktadır. Bu yükümlülükler, dijital verilerin korunarak bireylerin özel hayatlarının gizliliklerinin ihlal edilmemesini garanti altına almak için önem arz etmektedir. Bunun için verinin toplanması, kullanılması, ifşası ve tutulması, şeffaf gizlilik koruma standartlarına uygun olmalıdır. Bununla birlikte her bireyin de kendisi hakkında toplanan verilerin kullanımını kontrol edebilme hakkına sahip olması gerekmektedir. Kişisel veri talep edenlerin, bireylerden istenilen bilginin amacı, içeriği, kaydedileceği yer, saklanacağı ve kullanılacağı durumlar, süre, kullanım koşulları, geri kazanım ve kişisel bilgilerin düzeltilmesi konusunda bireylerin rızasını ve onayını almaları gerekir. Ayrıca kişilerin, toplanan bu veriye erişebilme, veriyi kurtarabilme ya da veriyi silme hakkına sahip olabilmesi gerekir.

Kişisel verilerin kullanımında asgari standartların olması, kişisel bir veri talep edildiğinde olası en az verinin çok kısa bir süre içerisinde toplanması gerekir. Veriyi toplayanların, topladıkları verinin üçüncü şahısların eline geçmesi, başkaları tarafından suiistimal edilmesi, kaybolması, silinmesi veya çalınması durumunda bunun bilgisini verinin sahibine haber vermesi ve yeniden geçerli bir izin talep etme yükümlülüğü bulunmaktadır. Veriyi tutanların, veri dosyalarında kaydedilmiş bilgilerin kazayla veya yetkisiz erişim yapılması yoluyla kaybedilmesine, izinsiz kullanılmasına, değiştirilmesine veya yayılmasına karşın gerekli güvenlik önlemlerini alması özel hayatın gizliliği ihlalinin önlenmesi açısından gereklidir. Diğer bir husus da verinin korunup korunmadığının denetlenmesi hususudur. Konunun hassasiyetine binaen veri koruma işlemlerinin şeffaf bir şekilde bağımsız kurumlar tarafından izlenmesi ve denetlenmesi suiistimalleri önleme noktasında caydırıcı işlev görecektir.

2.10. Unutulma ve lekelenmeme hakkı

İnternetin yasadışı ve zararlı içeriğine bağlı olarak etik ilkeler dışında sorumsuzca kullanılması, kişilik hakları ve özel hayatın gizliliğine bağlı olarak internette unutulma

hakkı (right to be forgotten) ve dijital itibar (digital reputation) kavramlarını gündeme getirmiştir. Yani unutulma hakkı, bir internet kullanıcısının internette uzun zaman önce yaptığı faaliyetler ile ilgili olarak o kullanıcının oluşturduğu veya o kullanıcıya yönelik oluşturulan içeriğin (metin, resim, video vs.) internet ortamında bir daha geri getirilemeyecek biçimde ortadan kaldırılmasıdır. Bunun daha çok kurumsal bir tüzel kişiliği veya bir markayı hedef alması veya çevrimiçi ortamda zarar verici bir eyleme karışmaksızın pozitif bir algı veya güven yaratılması çabası da dijital itibar olarak adlandırılmaktadır.

2012 yılının başlarında Avrupa Komisyonun adalet ve vatandaşlıktan sorumlu üyesi Viviane Reding'in açıklamalarıyla gündeme gelen unutulma hakkı, 2014 yılında Avrupa Adalet Divanı tarafından verilen bir karar ile tekrar gündemdeki yerini almıştır. Avrupa Birliği'nin en yüksek düzeydeki mahkemesi olan Avrupa Adalet Divanı, 13 Mayıs 2014 tarihli kararında, Google'ın, kullanıcılarına bazı durumlarda kendileri ile ilgili bilgilere yönlendiren linkleri silme hakkı tanıması gerektiğine karar verdi. Mahkeme, Avrupa genelinde tanınmış hale gelen "unutulma hakkı" kapsamında, silmemek için "özel/belirli bir neden" bulunmadıkça, Google gibi bir arama motorunun bir süre sonra kullanıcılar ile ilgili arama sonuçlarının silinmesine izin vermesi gerektiğini belirtti. Bu karar, Avrupa Birliği Adalet Divanı Google/İspanya davasında unutulma hakkı konusunda verdiği karara ilişkin bir süreç olarak ortaya çıkmıştır. Mahkeme kararı daha çok Google İspanya üzerinden gitse de aslında tüm arama motorlarının bu konuda sorumlu oldukları belirtilmektedir. Bu yüzden Google ile birlikte Bing de unutulma hakkı ile ilgili talepleri almaya başlamıştır. Avrupa Birliği Adalet Divanı'nın vermiş olduğu bir karar olmasına rağmen taleplerin, sadece AB vatandaşlarını kapsaması ise ayrı bir sorun teşkil etmektedir. Bununla birlite Google, Türk kullanıcılarına yönelik unutulma hakkı kapsamında olmasa da içerik çıkarma talep hakkı sunmaktadır.

Unutulma hakkı ile ilgili olarak 2015 yılında Türkiye'de de Yargıtay Hukuk Genel Kurulundan bir karar çıkmış bulunmaktadır. Kararda (Karar No: 2015/1679) unutulma hakkı şöyle tanımlanmıştır:

"Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin ve gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geç-

mişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir.

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlamamasına yönelik önlenmeleri alma yükümlülüğü yükler. Bu hakkın; bireylerin fotoğraf, internet günlüğü gibi kendileri hakkındaki içerikleri silmek için üçüncü şahısları zorlamayı içermesinin yanında geçmişteki cezalarına ilişkin bilgilerin veya haklarında olumsuz yorumlara neden olabilecek bilgi ve fotoğraflarının kaldırılmasını isteme hakkını tanıdığı kabul edilmektedir. Diğer taraftan bu hak, bireyin geçmişindeki belirli yönlerinin mümkün olmayacak biçimde hatırlanmaması için önlemler alınmasını gerektirmektedir."

Unutulma hakkı görüldüğü üzere geçmişte yaşanan olumsuz olayların şimdi veya ilerde hatırlanmaması olarak görülmelidir. Bu noktada da kişisel verilerin korunması, kişilik hakları ve özel hayatın gizliliği ile ayrılmaktadır. Yani unutulma hakkı bir kişinin kişilik ve özel haklarına saldırı, siber zorbalık veya bilgi kirliğinden kaynaklanan zedeleyici davranışlardan ziyade gerçekte geçmişte yaşanan olaylardan dolayı kişinin ileride bundan sorumlu tutulmaması gerekliliği ve bu konuda çevrimiçi ortamda kişinin hatırlanmama özgürlüğünün olduğuna yönelik tanınmış bir hak olarak karşımıza çıkmaktadır.

2.11. İnternet ile eğitim, bilgi ve kültüre erişim hakkı

EİHB'nin 26'inci maddesine göre: "Herkesin eğitim hakkı vardır." denilmektedir. Dolayısıyla, her bireyin internet hakkında eğitim almaya ve interneti eğitim amaçlı kullanmaya hakkı vardır. Bireylerin internet ortamındaki yayınlar, araştırmalar, ders kitapları, ders materyalleri ve diğer eğitim araçlarına ulaşabilmeleri internet aracılığıyla eğitimi fırsat eşitliği noktasında önemli hale getirmiştir. İnternette eğitim kapsamında, dijital okuryazarlık eğitiminin temel esaslardan biri haline getirilmesi, kişilerin dijital bilgi ve becerilerinin gelişmesini sağlayarak internette aradıklarını bulmaları ve uygun şekilde kullanmalarına olanak sunacaktır.

EİHB'nin 27'inci maddesinde: "Herkes, topluluğun kültürel yaşamına serbestçe katılma, sanattan yararlanma ve bilimsel ilerlemeleri ve bunun sağladığı olanakları paylaşma hakkında sahiptir." denilmektedir. Bu noktada internet, bireylerin farklı kültürel yaşamlar edinme ve bulunduğu toplum içerisinde de kültürel yaşama katılma, sanatsal faaliyetlerden faydalanma, bilimsel ilerlemeleri takip edebilme ve bunların sağladığı ayrıcalıklar sahip olma imkânına kavuşmuştur. Bireylerin internet üzerinden bu imkânlara kavuşmasının engellenmesi, bilgiye kültüre ulaşmasını orantısız bir şekilde, sınırlayıcı ve kısıtlayıcı müdahalenin olmaması gerekmektedir. Herkesin internet yoluyla bilgiye ve araştırmalara erişim hakkı vardır ve bireyler bu haklarını herhangi bir tacize veya kısıtlamaya maruz kalmadan kamuya açık bilgilere erişebilmesi ve bu bilgileri paylaşabilmesi gerekir.

İnternet, görünüm ve işlevsellik bağlamında gerek metin, gerek görsel gerekse de ses bakımından farklı kültür ve dil çeşitliliğini temsil etmektedir. İnternetteki bu çeşitliliğin desteklenmesi için teknolojik yeniliklere ihtiyaç duyulmaktadır. İnternet üzerinde herkesin kendi anadiliyle bilgi yayma, oluşturma ve bunları kullanabiliyor olması gerekir. Bununla birlikte bireylerin bilgiye erişimde telif ve lisanslama gibi sınırlamalara maruz kalmaması, kamu tarafından desteklenen araştırma ve kültürel çalışmaların herkesin erişimine açık hale getirilmesi, açık kaynaklı yazılımlar ve standartların olması İnternet ile eğitim, bilgi ve kültüre erişim hakkının geniş anlamda kullanılmasına katkı sağlayacaktır.

2.12. Çocuk hakları ve internet

Çocuk Haklar Sözleşmesinin 5'inci maddesine göre "çocuğa tanıdığı haklar doğrultusunda çocuğun yeteneklerinin geliştirilmesi ile uyumlu olarak, çocuğa yol gösterme ve onu yönlendirme konusunda ana–babanın, yerel gelenekler öngörüyorsa uzak aile veya topluluk üyelerinin, yasal vasilerinin veya çocuktan hukuken sorumlu öteki kişilerin sorumluluklarına, haklarına ve ödevlerine saygı gösterirler." denilmektedir.

İnternet söz konusu olduğunda, yukarıdaki ifade çocukların interneti kullanma ve ondan yararlanma özgürlüğünün olması ve internetin getirdiği tehlikelere karşı korunması anlamına gelmektedir. Bahis konusu önceliklerle çocuğun yetenekleri arasında bir denge kurulmalıdır. Devlet, çocuğun yeteneklerinin geliştirilmesine uyumlu bir tarzda olmak kaydıyla, tanımlanan hakların çocuk tarafından kullanılmasında çocuğu uygun şekilde yönlendirmek ve ona rehberlik etmek bakımından ebeveynlerin sorumluluklarına, haklarına ve ödevlerine saygı göstermelidir.

Çocuklar internette yaşlarına uygun içeriklere sahip sitelerden faydalanmalıdır. Çocukların internette medeni, politik, ekonomik, kültürel ve sosyal haklarını kullanma fırsatları olmalıdır. Bu haklar arasında sağlık, eğitim, özel hayatın gizliliği, bilgiye erişim, ifade özgürlüğü ve örgütlenme özgürlüğü de bulunmaktadır. Çocuklar, bu haklarını kullanırken cinsel taciz ve diğer suiistimallerden arınmış güvenli bir çevrede büyümeleri ve gelişmeleri sağlanmalıdır. Çocuk ticareti ve çocuk tacizine ilişkin görseller de dâhil olmak üzere çocuk haklarını ihlal eden internet kullanımlarının engellenmesine ilişkin adımlar atılmalıdır. Kendi fikirlerini ortaya koyan çocuklara, onları etkileyen tüm internet politikaları hakkında söz hakkı tanımak, onların fikirlerinin de duyulmasını sağlayarak çocuğun yüksek menfaatinin korunmasına özen göstermek gerekir.

2.13. İnternet ve engelli hakları

Birleşmiş Milletler Engelli Hakları Sözleşmesi'nin 4'üncü maddesinde de belirtildiği üzere: "Taraf devletler engelliliğe dayalı herhangi bir ayrımcılık yapılmaksızın bütün engellilerin tüm insan hak ve temel özgürlüklerinin tam olarak hayata geçirilmesini sağlama ve hak ve özgürlükleri güçlendirme sorumluluğu altındadır." Bu bağlamda internetin, engellilerin tüm temel insan hak ve özgülüklerinden tam olarak yararlanmasını sağlamak adına önemli bir rol oynadığını söylemek mümkündür. Bunun için en-

gellilerin internet erişim hakkının, engelli olmayan diğer kişilerle eşit şartlarda olmasına özen gösterilmesi gerekir. Onların da internet erişimine ilişkin temel ilkelerin asgari standartlar çerçevesinde geliştirilmesi, yayınlanması ve takibi, engellerle yüzleşen kişilerin erişilebilirlik hususunda eğitilmesi, bilgiye erişmelerinin garanti altına alınması için diğer uygun yardım metotlarının desteklenmesi gerekmektedir. Bu noktada engellilerin interneti etkin ve kullanışlı biçimde kullanması için adımlar atılmalıdır.

2.14. Diğer haklar

Önceki bölümlerde bahsedilen haklar dışında aşağıdaki haklardan da bahsetmek mümkündür:

- İnternet ve çalışma hakkı,
- İnternet aracılığıyla yönetime katılma hakkı,
- İnternetteki e-ticaret hacmi dikkate alındığında internette tüketici hakkı,
- Sağlık ve diğer sosyal hizmetlere ulaşabilme hakkı,
- İnterneti ilgilendiren uyuşmazlıklarda etkin yargı yolundan faydalanma ve adil yargılanma hakkı,
- İnternette toplumsal ve uluslararası düzene sahip olma hakkı,
- İnternetteki ödev ve yükümlükler,

İnternet ve çalışma hakkı kapsamında internet, çalışma hayatına da birçok yenilikler ve hareket getirmiştir. İnternet üzerinde yürütülmekte olan işlerin boyutu dikkate alındığında çalışma hakkının sadece gerçek hayatta kullanılan bir hak olmadığı, internetin de buna dâhil edilmesi gerektiği ortadadır. EİHB'nin 23'üncü maddesinde: "Herkes çalışma hakkına sahiptir." denmektedir. Her bireyin internet üzerinden iş arama, internet üzerinden ve internet araçlarını kullanarak çalışma hakkını kullanmasını da bu kapsamda değerlendirmek gerekir. Günümüzde internet bağlantısı olmayan işyeri ya da işveren yok gibidir. Hatta internet olmadığı durumlarda bazı kurum ve kuruluşlarda iş üretme noktasında aksamalar bile yaşanabilmektedir. Dolayısıyla çalışanların işyerinde internet bağlantısı olması bir hak olmaktan ziyade bir gereklilik haline gelmiştir denilebilir. Bir anlamda bu hakta yaşanabilecek aksaklıklar aslında vatandaşa yönelik verilmesi gereken hizmetlerin de aksamasına sebep olacaktır.

İnternet aracılığıyla yönetime katılma hakkı kapsamında; EİHB'nin 21'inci maddesinde: "Herkes doğrudan ya da serbestçe seçilmiş temsilciler aracılığıyla ülkesinin yönetiminde yer alma hakkında sahiptir." denilerek bireylerin internet ortamında ülke yönetiminde yer alma hakkına atıfta bulunulmuştur. Bu katılım bir anlamda verilmekte olan hizmetlerin kalitesine olumlu yönde etki edecek ve karar vericilerin bireylerin eleştiri ve önerilerini daha fazla dikkate almalarını sağlayacaktır. Bu hakkın tam olarak kullanılabilmesi için, hangi görüş ve düşüncede olursa olsun aşırı uç olmayan fikirlerin ve görüşlerin paylaşılmasına olanak tanıyan elektronik hizmetlere eşit erişim hakkının olması gerekir.

İnternette tüketici hakkı kapsamında; internetteki e-ticaret hacmi dikkate alın-

dığında bireylerin sadece tüketici değil aynı zamanda üretici konumunda olduğu görülmektedir. Dolayısıyla internet ortamında üretici ve tüketicilerin haklarının korunması elzemdir. Herkes internette tüketicinin korunmasına ilişkin kurallara saygı duymalı, söz konusu kuralları korumalı ve üzerine düşen yükümlülükleri yerine getirmelidir. Gerek e-ticarette, gerekse bireylerin oluşturduğu eserlerin korunmasında bunun gerçekleştirilmesi önem arz etmektedir. Eserlerin korunması noktasında EİHB'nin 27'inci maddesinde: "Herkes yaratıcısı olduğu herhangi bir bilimsel, edebi ya da sanatsal üründen doğan manevi ve maddi menfaatlerin korunması hakkında sahiptir." denilerek bu garanti altına alınmıştır. Elbette bunu yaparken telif rejimlerinin toplumun internet üzerinden bilgiye ve kültüre erişimini orantısız bir şekilde sınırlayıcı olmamasına dikkat edilmelidir. Aynı şekilde e-ticarette için de e-ticaret yönetmeliklerinin tüketicilerin elektronik ortamda olmayan işlemlerde korunduğu düzeyde korunmasını sağlayacak şekilde düzenlenmesi gerekmektedir.

Sağlık ve diğer sosyal hizmetlere ulaşabilme hakkı; internetin getirdiği fırsatlar noktasında önemli bir hak olarak karşımıza çıkmaktadır. İnternet üzerinde sağlıkla ilgili bilgilere ve sosyal hizmetlere erişme de bireylerin bir hakkı olarak karşımıza çıkmaktadır. Bireylerin bu haktan tam olarak yararlanabilmesi için herkesin internetten sağlanan sağlık ve sosyal hizmetlere ilişkin içeriklere erişimi olması gerekmektedir. Örneğin e-devlet üzerinden sunulan e-nabız ve benzeri uygulamalar gibi hizmetlere erişim bu hakkın kullanılması noktasında iyi bir örnek olarak değerlendirilebilir. EİHB'nin 25'inci maddesinde söz edildiği şekilde: "Herkes kendisinin ve ailesinin sağlık ve refahının temini için yeterli bir yaşam standardına sahip olma hakkına; işsizlik, hastalık, sakatlık, dulluk ve yaşlılık hallerinde, ya da kendisinin kontrolü dışındaki koşullardan doğan diğer yoksunluk durumlarında sosyal güvence hakkına sahiptir." denilmektedir. Dolayısıyla bireylerin, gerek sağlık gerekse de sağlık dışında kamunun ve özel sektörün sunduğu sosyal hizmetlerden internet yoluyla haberdar olması ve bu hizmetlere hızlı bir şekilde ulaşabilmesinin sağlanması, sosyal bir devletin vatandaşlarına yönelik yerine getirmesi gereken önemli bir hizmet ve sorumluluktur.

İnterneti ilgilendiren uyuşmazlıklarda etkin yargı yolundan yararlanma ve adil yargılanma hakkı bireyler için çok önemli bir hak olarak değerlendirilmektedir. EİHB'nin 8'inci maddesinde söz edildiği şekilde: "Herkesin anayasa ya da yasayla tanınmış temel haklarını ihlal eden eylemlere karşı yetkili ulusal mahkemeler eliyle etkin bir yargı yolundan yararlanma hakkı vardır." denilmektedir. Ayrıca EİHB'nin 10'uncu maddesinde de hükme bağlandığı üzere: "Herkesin, hak ve yükümlülüklerinin belirlenmesinde ve kendisine herhangi bir suç isnadında bağımsız ve yansız bir mahkeme tarafından tam bir eşitlikle, hakça ve kamuya açık olarak yargılanmaya hakkı vardır." denilmektedir. İnternette suç teşkil eden içeriklere yönelik devletler tarafından uygulanan yaptırımlarda, içerik sahiplerinin bağımsız mahkemelerde haklarını arayabilmekte ve yaptırıma yönelik itirazlarını yapabilmektedir. Bu içerikler

sebebiyle suçlanan bireylerin de bu noktada kendilerini savunma hakkı olduklarını ifade etmek gerekir.

Adil yargılanma ve etkin hukuk yollarından yararlanma hakkı, internet ortamında giderek daha çok ihlal edilmektedir. Örneğin, internet servis sağlayıcıları veya arama motorları gibi internette faaliyet gösteren aracılardan barındırdıkları içeriğin hukuka aykırı olup olmadığına dair karar vermeleri veyahut geçerli bir mahkeme kararı olmadan bazı içerikleri tümden kaldırmaları istenebilmektedir. Bununla birlikte uluslararası ve ulusal hukukta suç sayılan bazı içerikler de talep edilmesine rağmen içerik sağlayıcıları tarafından kaldırılmayabilmektedir. Bu durum içerik sağlayıcılarla devletleri bazen karşı karşıya da getirmektedir. Kaldırılmayan içerikler bazı durumlarda kişisel hakların ve özel hayatın gizliliğinin ihlaline kadar gidebilmektedir. Bu nedenle usule ilişkin haklara fiziki hayatta olduğu kadar internet ortamında da saygı gösterilmesinin, korunmasının ve uygulanmasının vurgulanması son derece önemlidir.

İnternette toplumsal ve uluslararası düzene sahip olma hakkı kapsamında anlaşılması gereken, internetin insan haklarına uygun bir şekilde yönetilmesidir. Her ne kadar internetin çıkış noktası ABD olmuş olsa da bu ABD'yi internetin tek sahibi yapmaz. EİHB'nin 28'inci maddesinde belirtildiği üzere: "Herkesin bu Bildirgede ileri sürülen hak ve özgürlüklerin tam olarak gerçekleşebileceği bir toplumsal ve uluslararası düzene sahip olma hakkı vardır." denilerek aslında internet yönetiminin, açıklık, kapsayıcı ve hesap verilebilirlik ekseninde şeffaf ve çok yönlü olarak uygulanması gerektiği anlaşılmalı ve uygulama da bu yönde olmalıdır. Bu sebepledir ki internet ve iletişim sistemleri insan haklarını olabilecek en geniş kapsamda sürdürebilen ve genişletilebilen biçimde yönetilmelidir.

İnternet doğası gereği, toplumsal ve uluslararası bir düzen ekseninde çok dilliliği, çok kültürlülüğü, çoğulculuğu ve farklılığı yani heterojenliği kabul etmektedir. Bu açıdan devlet veya birey olarak herkesin internet yönetimine katılması bir hak olarak görülmeli ve özellikle tüm dezavantajlı grupların küresel, yöresel ve milli eksende karar mekanizmalarına tam ve etkin katılımları garanti altına alınmalıdır.

İnternette hakları olan her bireyin yükümlülükleri de vardır. EİHB'nin 29'uncu maddesinde kabul edildiği üzere: "Herkesin, kişiliğinin özgürce ve tam gelişmesine olanak sağlayan tek ortam olan topluma karşı ödevleri vardır." denilmektedir. Bu kabul aynı şekilde internet ortamı için de geçerlidir. Her bireyin topluma kaşı taşıdığı sorumlulukları internet kullanıcılarına karşı da yerine getirmesi gerekmektedir. Sadece bireylerin değil, internetteki güç odakları konumundaki aktörlerin de aynı tavrı sergilemesi beklenir. Şöyle ki; interneti kontrol eden güç odakları diğer bir ifade ile aktörler yürütmeyi, insan haklarını ihlal etmekten kaçınarak, insan haklarına saygı göstererek, koruyarak ve olabilen en geniş kapsamda insan haklarını dikkate alarak yükümlülüklerini yerine getirmelidir.

Gerek devletler gerekse internet aktörleri tarafından meşru bir gerekçe olmadan, orantılılık ölçüsüne dikkat edilmeden in-

ternete ve dijital medyaya ulaşımın kısıtlanması ve çevrimiçi etkinliklerin ya da elektronik iletişimin izlenmesine yönelik girişimler, kişilerin temel hakları olan ifade ve bilgi alma, örgütlenme, mahremiyet ve özel yaşam özgürlüklerine (ve muhtemelen din ve inanç özgürlüğü ya da adil yargılanma hakkı gibi diğer haklara da) bir müdahale oluşturmaktadır.

3. İletişim Hakkı

İletişim teknolojilerinin gelişmesi sonucu küreselleşen dünyada, interneti sadece ekonomik bir pazar olarak değil, aynı zamanda bireylerin ve grupların siyasal, toplumsal ve kültürel ihtiyaçlarını karşılamak için önemli ve gerekli bir iletişim ve haberleşme aracı olarak görmek ve değerlendirmek gerekir. Düşünce ve ifade özgürlüğü hakkının tam olarak uygulanması iletişim hakkının tam olarak gerçekleştirilmesiyle mümkündür.

İletişim hakkı; tüm insanların hayat standartlarını iyileştirmelerini, her yerde ve her platformda bireysel ya da toplu olarak kendilerini ifade etmelerini sağlayan haktır. Bu hak, bireyin içinde bulunduğu toplumda karar alma süreçlerine tam katılımı, bilgiye erişimi, kendini ifade etme özgürlüğü, kültürel etkileşim, kültürel çeşitlilik gibi birçok unsuru içerisinde barındırmaktadır. İletişimi tek yönlü değil, çift yönlü bir süreç olarak düşünmek gerekir. Bu durum beraberinde kamu veya özel birçok kaynaktan bilgi alma hakkını beraberinde getirmektedir. İletişim hakkı aynı zamanda bireylerin iletişim araçlarına erişim hakkını, bireyin kendi kültürünü yaşama ve bunu ifade etme hakkını, kendi dilini kullanma hakkını, başkalarının kişilik haklarını ve özgürlüğünü ihlal etmeyecek şekilde eleştiri hakkını, kamuda alınacak karar süreçlerine katılım hakkını, bilgiye erişim hakkını kullanabilmesi açısından anlam ifade etmektedir.

3.1. Ulusal ve uluslararası hukukta iletişim hakkı

İletişim hakkı kavramının temel dayanağını İnsan Hakları Evrensel Beyannamesi'nin 19'uncu maddesi oluşturmaktadır. Bu madde "Herkesin düşünce ve anlatım özgürlüğüne hakkı vardır. Bu hak, düşüncelerinden dolayı rahatsız edilmemek, ülke sınırları söz konusu olmaksızın, bilgi ve düşünceleri her yoldan araştırmak, elde etmek ve yaymak hakkını gerekli kılar" hükmünü içermektedir. Özgürlük, eşitlik, dayanışma, dokunulmazlık, kapsayıcılık, çeşitlilik, evrensellik ve katlım gibi ilkeleri dayalı insan haklarının kullanılabilmesi bir hak olan iletişim olanakları ile mümkün olmaktadır. İletişim hakkı; ifade özgürlüğü, bilgiye erişim hakkı, bilgi edinme hakkı, iletişim politikaları ve kültürel çeşitliliğin sağlanması ile ilgili karar alma süreçlerine bireylerin katılımını sağlaması açısından önemli bir haktır. İnternetin hayatımıza girmesiyle birlikte bireylerin kendini ifade edebileceği olanaklar artmış ve belli bir ölçüde fırsat eşitliği sağlanmıştır. Fırsat eşitliğinin tam olarak sağlanabilmesi iletişim hakkının var olması ve bireylerin bu hakkı kullanarak internete erişmeleri ile mümkün olmaktadır.

İletişim hakkının kısıtlanması ya da tamamen ortadan kaldırılması, düşünce ve ifade özgürlüğünün ortadan kaldırılması sonucunu doğurabilir. Bunun için bu yönde yapılacak müdahalelerde; hukuken öngö-

rülmüş olmasına, ulusal güvenlik ve toprak bütünlüğü, kamu güvenliği, kamunun sağlığı ve ahlakı, başkalarının haklarının ve özgürlüklerinin korunması, kamu düzeninin sağlanması ve suç işlenmesinin önlenmesi veya yargı gücünün otorite ve tarafsızlığının sağlanması gibi meşru amaçlardan birinin gerçekleşmesine, müdahalenin demokratik bir toplumda gerekli acil bir sosyal ihtiyaca yanıt verecek geçerli bir sebebe dayanmasına ve orantılılık ölçüsüne dikkat edilmesi gerekmektedir. Orantılılık ölçütünde yapılacak müdahalenin; söz konusu temel hakka mümkün olduğunca az kısıtlama getirmesi, belirlenen meşru amaçları gerçekleştirmek için dikkatli bir şekilde hazırlanmış olması, hakkaniyete aykırı olmaması, temelsiz düşüncelere dayanmaması oldukça önem arz etmektedir.

İletişim ve haberleşmede kitle iletişim araçları, haberleşme, genel kültürü geliştirmek için bilgi edinme, toplumların kültürlerini yeni nesillere aktarmasında, tüketicilere yönelik eşya ve hizmetlerin tanıtılmasında, karşılıklı etkileşim, paylaşım ve toplumsal sorunların çözümü için zemin hazırlamak amacıyla kullanılmaktadır. Bu sebeple, kitle iletişim özgürlüğü her bireyin en temel haklarından biri olarak haber alma, bilgi edinme, basın, radyo, televizyon, sinema ve günümüzde en çok tercih edilen internet ve sosyal medya gibi iletişim araçlarının kullanılmasıyla birlikte elde edilen haklar olarak kabul edilmektedir. İletişim hakkının yani kitle iletişim özgülüğünün gerçekleşebilmesi için haberleşmeye ulaşabilme hakkı, açıklayabilme hakkı ve yayabilme hakkı gibi üç temel unsurun varlığına ihtiyaç vardır. Bireylerin düşüncelerini ifade etmesi temel hak ve özgürlükler arasına girer ve bir bireyin düşüncesini, elde ettiği bilgiyi ya da herhangi haberi toplum ile paylaşabilmesi iletişim hakkı için gerekli bu üç unsurun varlığıyla mümkündür. Kitle iletişimin kamuoyu oluşturulmasındaki etkisinin ve payının ne denli büyük olduğu düşünüldüğünde iletişim hakkının önemi daha iyi anlaşılacaktır. Bu yüzdendir ki iletişim hakkı demokrasinin vazgeçilmezi olarak kabul edilir. Demokrasinin gelişmesi de ancak toplumun kitle iletişim araçları vasıtasıyla yönetime katılarak katkı sunması ve fikirlerini paylaşmasıyla mümkündür.

Anayasa'nın 22'inci maddesinde "Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; **haberleşme engellenemez ve gizliliğine dokunulamaz.** Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar." denilerek bir anlamda haberleşme hürriyeti yani iletişim hakkı koruma altına alınmıştır.

İletişim hakkı ve haberleşme özgürlüğü konusunda Anayasa Mahkemesi'nin verdiği bazı kararlardan hareketle haberleşme özgürlüğünün sınırlanabilir bir hak olduğu ancak sınırlamanın kanuna ve meşru bir amaca dayanması gerektiği vurgulanmıştır.

Uygulamanın aşırı, dolayısıyla orantısız olmaması ve demokratik toplum düzeninde gerekli olma ve ölçülülük ilkesine uygun olması gerektiği ifade edilmiştir. Haberleşme özgürlüğüne getirilen sınırlamaların öncelikle kanunla öngörülmüş olması gerekmektedir.

4. Bilgi Edinme Hakkı

İnternet tabanlı teknolojilerin getirmiş olduğu yenilikler ve dönüşümler bilginin üretilmesi, dağıtılması ve paylaşılması noktasında önemli yapısal ve kültürel değişimler getirmiştir. Bilginin bireylerle yani vatandaşlarla paylaşılması, onların yönetime katılımın sağlanması aşamasında bu bilgilere ulaşılabiliyor olması bilgi edinme hakkını ve bu hakkın kullanılmasını hem önemli hale getirmiş hem de bunun sınırlarını genişletmiştir.

Kısa ve basit ifadeyle bilgi edinme hakkı, toplumu oluşturan bireylerin kamu kurum ve kuruluşlarından görevlerinden dolayı ve görevleriyle ilgili sahip oldukları bilgilere erişim hakkını ifade etmektedir. İdare hukuku çerçevesinde teknik bir tanım yapmak gerekirse, bilgi edinme hakkı, idarenin tek yanlı iradesiyle hukuk düzeninde yapacağı değişiklikler hakkında ilgili bireylerin, işlemin niteliği ve sonuçları hakkında bilgi alabilmesini sağlayan bir özgürlüktür. Bilgi edinme hak ve özgürlüğünün temel amacı, idarenin alacağı kararları hukuka uygun bir şekilde etkileyebilmesi için, kişinin bilgilenmesini sağlamaktır. Bu hak demokratik yönetim ve şeffaflık ilkelerinin kamu yönetiminin olmazsa olmazları olan eşitlik, tarafsızlık ve açıklık ilkelerinin yerleşerek güçlenmesinde önemli bir yere sahiptir.

Bilgi edinme hakkının kullanılmasının getirilerini şu şekilde sıralamak mümkündür:

- Yolsuzlukla mücadelede etkin bir denetim mekanizması görevi görür,
- Devlet ile vatandaşları arasındaki iletişim kanallarının açık tutulmasını sağlar,
- Devlet ile vatandaşlar arasındaki mesafenin azalmasını sağlar ve güveni tesis eder,
- Bireylerin devlet yönetimine yabancılaşmasına engel olur,
- Bireylerin idarenin aldığı kararları denetlemesine olanak sunar,
- Bireylerin karar alma mekanizmalarında etkin rol oynamasına imkân sağlar,
- Karar alma mekanizmasında etkin rol oynama imkânına sahip bireyler nazarında idarenin iş ve eylemlerine meşruiyet kazandırır,

Bilgi edinmeyi açık kaynaklardan ve resmi kaynaklardan bilgi edinme şeklinde birbirinden ayırmak gerekir. Açık kaynaklardan bilgi edinmede internet erişim hakkının, iletişim hakkının olması yeterli iken, resmi kaynaklardan bilgi edinme talepleri bir takım usul ve esaslara tabi olabilmektedir. İnternet ve sosyal medya gibi açık bilgi kaynaklarından bilgi edinmede internet erişim hakkının olması ve meşru gerekçeler ve şartlar dışında erişimin açık tutulması yeterlidir.

Bilgi edinme hakkı, demokratik toplumların önemli gereklerinden biri olarak değerlendirilmekte, temel hak ve özgürlükler

arasında sayılmakta ve ifade özgürlüğü, düşünce özgürlüğü, hak arama talebi gibi kavramlarla ilişkili olarak açıklanmaktadır. Bilgi edinme hakkı veya özgürlüğü aşağıdaki gibi farklı şekillerde de tanımlanabilmektedir;

- Bilgi akışının hâkim olduğu bilgi toplumunda, devletçe tutulan, kayıtlı (kanunda belirtilen istisnalar dışında) her türlü belge, doküman vb. bilginin halka akışının yasal olarak serbest oluşu,
- İdarenin kurduğu ve kurmakta olduğu işlemler ile eylemlere ilişkin kişinin bilgi almasını, belgelere ulaşmasını öngören temel bir insan hakkı,
- Kamunun resmi kuruluşların kararlarından eylemlerinden ve bu eylemlerindeki yöntemlerinden haberdar olması hakkı,
- Bireylerin devletçe oluşturulan veya herhangi bir şekilde tutulan kayıt ve bilgileri devlet içindeki gönüllü ve gönülsüz kaynaklardan öğrenme hakkı,
- İdarenin tek taraflı iradesiyle hukuk düzeninde gerçekleştirdiği değişikliklere ilişkin ilgililerin işlemin niteliği ve neticeleri hakkında bilgi alabilmesini temin eden hak,

Bu tanımlardan hareketle, bilgi edinmenin temel bir insani hak olarak kabul gördüğünü söylemek mümkündür. Bu yaklaşım aslında bilgiye erişimin temel olarak hiçbir ayrım gözetmeden herkese açık olmasından kaynaklanmaktadır ki günümüzde internet bunu oldukça kolaylaştırmıştır. Aslında özellikle siyaset bilime ve kamu yönetimin literatüründe sıklıkla dile getirilen "açıklık, şeffaflık" gibi kavramların temelinde herkese açık olma ve ayrım gözetmeme ilkesi yatmaktadır. Bir başka deyişle bilgi edinme hakkını, diğer hak ve özgürlükler ile birlikte, demokratik toplumlarda şeffaflığın, açıklığın ve bireylerin yönetime katılımının önemli bir kanalı olarak da tanımlamak mümkündür.

Son yüzyılda devlet yönetimlerinde açıklık ve şeffaflık ilkeleri ön plana çıkmıştır. Bu bağlamda günümüz modern toplumları bu ilkenin teminatı olarak bilgi edinme hakkını tüm gerçek ve tüzel kişilere eşitlik ve tarafsızlık ilkelerine uygun olarak kullandırmayı kendilerine görev olarak kabul etmişlerdir. Bu kapsamda dünyanın birçok Ülkesinde olduğu gibi Türkiye'de de bilgi edinme hakkına ilişkin yasal düzenlemeler yapılmıştır. Bu düzenlemeler ile ilgili mevzuat aşağıdaki şekildedir;

- Anayasanın 74'ünci maddesi,
- 4982 sayılı Bilgi edinme Hakkı Kanunu,
- Bilgi Edinme Hakkı Kanunun Uygulanmasına İlişkin Esas ve Usuller Hakkında Yönetmelik
- Bilgi Edinme ve Değerlendirme Kurulunun Çalışma Usul ve Esasları Hakkında Yönetmelik
- Bilgi ve Belgeye Erişim Genel Tebliği
- 4982 sayılı Bilgi Edinme Hakkı Kanunu ve Buna Bağlı Yönetmelik Uyarınca Karşılıklılık İlkesi Kapsamında Bulunan Ülkeler Hakkında Tebliğ

Bilgi edinme hakkı her ne kadar şeffaflık ve açıklık kavramları etrafında şekillenmiş ve kanunda herkes bilgi edinme hakkına sahiptir denilmiş olsa da bazı istisnai durumların bilgi edinme hakkı için göz önünde bulundurulması gerekmektedir. Dünya üzerindeki genel kabule ve konuyla ilgili yasalara bakıldığında sınırlamaların aşağıdaki gibi belli başlı bazı alanlarda yapıldığı görülmektedir;

- Savunma,
- Uluslararası ilişkiler,
- Ulusal ekonomik çıkarlar,
- Yasaların uygulanması ve adalet sisteminin yönetilmesi,
- Kişi güvenliği,
- Kamusal ve ticari çıkarlar,

Devletin resmi bilgi ve belgelerine erişimde genelde içerik ve fiziksel olmak üzere iki tür sınırlama ile karşılaşılmaktadır. Kanunlarda yapılan sınırlamalar da bu doğrultuda gerçekleştirilmiştir. Bu kanun kapsamı dışında kalan durumlar aşağıdaki gibi sıralanabilir:

- Yargı denetimi dışında olan işlemler,
- Devlet sırrına ilişkin bilgi veya belgeler,
- Ülkenin ekonomik çıkarlarına ilişkin bilgi veya belgeler,
- İstihbarata ilişkin bilgi veya belgeler,
- İdari soruşturmaya ilişkin bilgi veya belgeler,
- Adlî soruşturma ve kovuşturmaya ilişkin bilgi veya belgeler,
- Özel hayatın gizliliği,
- Haberleşmenin gizliliği,
- Fikir ve sanat eserleri,

Günümüzde bilgi edinme hakkının en geniş manada kullanıldığı platformların internet ve sosyal medya gibi dünyanın her yerinden erişilebilme olanağı bulunan açık kaynaklar olduğu ortadadır. İnternet ve sosyal medyanın sunduğu çeşitlilik, çift yönlü, etkileşimli ve dinamik yapısı itibariyle bilgi edinme hakkının en etkin ve verimli kullanıldığı ortamlar olduğu gerçeği göz ardı edilmemelidir. Bilgi edinme hakkı ve bu hakkın kullanımı açısından internet ve sosyal medyayı ayrıca incelemekte fayda vardır.

4.1. Dünya ve Türkiye uygulaması

Bilgi edinme hakkına ilişkin ilk yaklaşımın 1707 tarihinde o dönemde İsveç'e bağlı olan Finlandiya'da ortaya konulduğu görülmektedir. 1766'da İsveç'te yürürlüğe giren Basın Özgürlüğü Kanunu ise bilgi edinme konusunda ilk yasal düzenleme olarak dikkat çekmektedir. Söz konusu yasa ile yurttaşların haber alma özgürlüğüne yönelik önemli güvenceler getirilmiş, haberlere erişim konusunda önemli gelişmeler kaydedilmiştir. Şu anda Anayasanın da bir parçası olan Basın Özgürlüğü Kanunu "Tüm İsveç vatandaşlarının resmi belgelere serbest erişim hakkı vardır." der. Kamu görevlileri, açıklanması istenen belge taleplerine derhal cevap vermek zorundadır. Kanunun mevcut hali 1949 yılında yürürlüğe girmiş ve

1976 yılında birkaç değişikliğe uğramıştır. 1789 Fransız İnsan Hakları Bildirgesi'nde vatandaşlara bütçe ile ilgili olarak bilgiye erişim hakkı tanındığını, buna benzer bir hakkın 1795'te Hollanda'da tanındığını ve 1888'de ise Kolombiya'da Siyasi ve Yerel Örgütlenmelerle ilgili kanunda, vatandaşlara başka kanunlarla yasaklanmadığı takdirde hükümetin elinde bulundurduğu bilgiyi talep etme hakkı tanındığı görülmektedir. Ancak, çağdaş anlamda bilgi edinme hakkının ülkelerin hukuk metinlerine girmesi, II. Dünya Savaşı sonrasında yaşanan yönetimin şeffaflaşması ya da yönetimde açıklık ilkesinin bütün dünyada yaygınlaşması ile mümkün olmuştur.

Amerika Birleşik Devletleri'nde 1946'da New Deal atılımı ve reformları döneminde çıkarılan "Administrative Procedure Act/ İdari Usul Kanunu" ile İdarenin karar alma süreç ve mekanizması bir usule bağlanarak, buna ilgililerin de katılımını sağlayan ve olabildiğince yargılama usulüne benzetilen bir şekle dönüştürülmüştür. Ancak, geçen zaman içinde İdari Usul Kanunu o haliyle yeterli görülmemiş ve sistem 1967 yılında çıkarılan "Freedom of Information Act/ Bilgi Edinme Özgürlüğü Kanunu" ile desteklenmiştir. Nihayet, 1974 yılında kabul edilen "Sunshine Act/Günışığı Kanunu" ile kurul halinde ve kolektif bir karar alma mekanizması söz konusu ise, toplantıların herkese açık bir biçimde yapılması sağlanmış ve bütün sisteme de "Goverment in the Sunshine/Günışığında Yönetim" ismi verilmiştir.

Danimarka ve Norveç'te bilgi edinme usulüyle ilgili kanunlar 1970 yılında yayımlanmıştır. Danimarka, 1985 yılında kanunu gözden geçirerek bazı değişiklikler yapmıştır. Fransa'da usul kanunu 1978 yılında yürürlüğe girmiş ve aynı yıl kişilerin özel yaşamına saygıyı kapsayan bir kanun da yürürlüğe konulmuştur. Hollanda'da 1978 yılında yürürlüğe giren bilgi edinme kanunu, 1991 yılında yeniden gözen geçirilmiştir. Kanada'da bilgi edinme ile kişilerin özel hayatına saygıya ilişkin kanunlar 1982 yılında kabul edilmiştir. Avustralya'da ise bilgi edinme ile ilgili kanun 1982 yılında kabul edilmiştir.

1990'ların başında Soğuk Savaş döneminin sona ermesinden sonra Doğu Bloğu'nun baskıcı rejimlerinden kurtulan Merkezi ve Doğu Avrupa ülkelerinin daha özgürlükçü rejimlere geçmeye başlamalarıyla birlikte arka arkaya bilgi edinme kanunlarını çıkardıkları gözlenmiştir. Günümüzde yaklaşık 100'den fazla ülkede bilgi edinme hakkı uygulama alanı bulan bir hak haline gelmiştir.

Türkiye'de ise bilgi edinmeye de referans olan bir düzenleme olarak 1982 Anayasası'nda tanımlanan dilekçe hakkına ilişkin hükümler ile 09.10.2003 tarihli 4982 sayılı Bilgi Edinme Hakkı Kanunu ve 24.01.2004 tarihli 25356 sayılı Resmi Gazete 'de yayınlanarak yürürlüğe giren Dilekçe ve Bilgi Edinme Hakkının Kullanılmasına ilişkin Başbakanlık genelgesi örnek gösterilebilir. 2004 tarihli düzenleme ile vatandaşların yönetimlere dilekçe yoluyla yaptıkları başvurulara ilişkin standartlar yapılandırılmış ve süreç tarif edilmiştir. Söz konusu düzenlemede devlet ile toplum arasındaki iletişimin güçlendirilmesi bakımından bu hakkın kullanımının önemine işaret edilmiş olup intikal eden taleplere azami düzeyde yanıt verilmesi yönündeki gereklilik vatandaş

odaklı yaklaşımın bir boyutu olarak tanımlanmıştır. Ayrıca 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun uyarınca kişiler dilek, istek, şikâyet ve ihbarlarını kurum ve kuruluşlara iletebilmektedirler.

Son dönemde özellikle e-devletin (turkiye.gov.tr) bu konudaki en önemli bileşeni olan CİMER (Cumhurbaşkanlığı İletişim Merkezi – cimer.gov.tr) ve kamu kurum ve kuruluşlarının kendi bilgi edinme kanalları aracılığıyla, elektronik ortamın da desteğiyle etkin biçimde bilgi edinme başvuruları kabul edilmekte ve değerlendirilmektedir. Başvurular bireylerin kendi kimliklerini doğrulamaları şartıyla hem site üzerinden hem de e-devlet üzerinden yapılabilmektedir.

Bilgi Edinme Kanunu ile demokratik ve şeffaf yönetimin gereği olan eşitlik, tarafsızlık ve açıklık ilkelerine uygun olarak kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usuller düzenlenerek, bireylerin bu haklarını ne şekilde kullanacağı ortaya konmuştur. Bilgi edinme hakkı kapsamında bilgi edinme hakkını sadece gerçek kişiler değil, kurum ve kuruluş tüzel kişileri de kullanmaktadır. Kanunda "Herkes bilgi edinme hakkına sahiptir" denilmektedir. Türkiye'de ikamet eden yabancılar ile Türkiye'de faaliyette bulunan yabancı tüzel kişiler, isteyecekleri bilgi kendileriyle veya faaliyet alanlarıyla ilgili olmak kaydıyla ve karşılıklılık ilkesi çerçevesinde, bu Kanun hükümlerinden Türkiye'nin taraf olduğu uluslararası sözleşmelerden doğan hak ve yükümlülükleri saklı kalmak şartıyla yararlanabileceği ifade edilmektedir.

4.2.Birleşmiş Milletler belgelerinde bilgi edinme hakkı

İlk olarak Birleşmiş Milletler (BM) Genel Kurulu'nun 1946 yılında aldığı 59 (1) sayılı Karar'da temel insan haklarından birisi olarak sayılan ve BM'nin değer verdiği bütün hakların mihenk taşı olarak nitelenen bilgi edinme hakkı, yine BM Genel Kurulu'nun 10.12.1948 tarih ve 217 A (III) sayılı kararı ile benimsenerek ilan edilen 'İnsan Hakları Evrensel Bildirgesi'nin 19'uncu maddesinde şöyle yer almıştır:

Madde 19- Herkesin görüş ve anlatım özgürlüğüne hakkı vardır. Bu hak, karışmasız görüş edinme ve herhangi bir yoldan ve hangi ülkede olursa olsun bilgi ve düşünceleri arama, alma ve yayma özgürlüğünü içerir.

Yine 1966 yılında kabul edilen BM Uluslararası Medeni ve Siyasi Haklar Sözleşmesi'nin "İfade Özgürlüğü" başlıklı 19'uncu maddesinde de bilgi edinme hakkı bir temel hak olarak düzenlenmiş ve bunun yanı sıra bilgi edinme hakkının hangi sınırlamalara tabi olabileceği ifade edilmiştir. Madde metni şöyledir:

Madde 19-

- Herkesin, bir müdahale ile karşılaşmaksızın fikirlere sahip olma hakkı vardır,
- Herkes ifade özgürlüğü hakkına sahiptir; bu hak bir kimsenin ülke hudutlarıyla sınırlanmaksızın sözlü, yazılı veya basılı veya sanatsal ürün şeklinde veya kendi tercih ettiği başka bir iletişim vasıtasıyla her türlü bilgi

ve düşünceyi arama, edinme ve ulaştırma özgürlüğünü de içerir,

- Bu maddenin ikinci fıkrasındaki haklar özel bir ödev ve sorumlulukla kullanılır. Bu nedenle bu hak, sadece hukuken öngörülen ve aşağıdaki sebeplerle gerekli olan sınırlamalara tabi tutulabilir,
- Başkalarının haklarına ve itibarına saygı,
- Ulusal güvenliği veya kamu düzenini veya sağlık ve ahlakı koruma,

4.3. Avrupa Konseyi belgelerinde bilgi edinme hakkı

1950 yılında yürürlüğe giren Avrupa İnsan Hakları Sözleşmesi'nin 10'uncu maddesi ifade ve bilgi özgürlüğünü düzenlemekte, ayrıca sınırlandırmanın kriterlerini detaylandırmaktadır. Avrupa Konseyi'nin (AK) 1970'lerden itibaren başlattığı ve bilgi edinme hakkını da içeren çalışmaları, 28.09.1977 tarih ve 275 sayılı Bakanlar Komitesi toplantısında alınan (77) 31 sayılı İdarenin İşlemleri Karşısında Bireyin Korunması Hakkında Karar ile neticelenmiştir. Avrupa Konseyi bu Karar'da üye Devletlere, hukuk kurallarında ve idari işlemlerde "dinlenilme hakkı, bilgi kaynaklarına girişin sağlanması hakkı, hukuki yardım ve temsil ettirme imkânı, idari işlemlerin gerekçeli olması, işleme karşı başvuru yollarının belirtilmesi" ilkelerinden esinlenmeleri tavsiyesinde bulunmuştur.

Bundan sonra Avrupa Konseyi Bakanlar Komitesi, bilgi edinme hakkının üye devletlerce hangi ilkelere göre tanınması gerektiğine ilişkin daha detaylı tavsiye kararları almaya başlamıştır. Bunlardan 25.11.1981 tarihli Kamu Makamlarının Sahip Olduğu Bilgiye Ulaşma Hakkında Tavsiye Kararı, bilgi edinme hakkı ile ilgili bir dizi ilkeyi sıralıyor; bu ilkelerden gerçek ve tüzel kişilerin yararlanabileceğini belirtiyor; bu hakkı kullanabilecek olan gerçek ya da tüzel kişilerin, isteme konu olan bilgi ile doğrudan bir yarar ilişkisinin olmasının zorunlu olmadığını düzenliyor ve nihayet bilgi edinme hakkının sınırlanması için belli kriterler getiriyordu. Avrupa Konseyi Bakanlar Komitesi'nin 29.04.1982 tarihli İfade ve Bilgi Özgürlüğü Bildirisi, düşünce, bilgi ve görüşün araştırılması, edinilmesi, ilgili kaynaklara ulaşılabilmesi hakkı; bu yolla özgür düşünceyi oluşturma hakkı; oluşturulan düşünceyi ya da görüşü ifade etme özgürlüğü; oluşturulan düşünce ve edinilen bilgi ve görüşün yayılması özgürlüğü; bütün bunların koşulları olarak, sansür yasağı ve bu özgürlüğün kullanılmasına keyfi müdahalede bulunulması yahut kısıtlama getirilmesi yasağı ve nihayet bağımsız ve özerk medyanın öneminden bahsetmektedir.

Avrupa Konseyi Bakanlar Komitesi'nin 21.02.2002 tarihli Üye Ülkelerin Resmi Belgelere Erişimi ile İlgili Tavsiyeleri ise çoğulcu ve demokratik bir toplumda saydam yönetimin ve halkı ilgilendiren konulardaki bilgilerin mevcut olmasının önemini göz önüne alarak, eşitlik ilkesi ve açıklık kuralları gereğince resmi belgelere erişimin;

- Halkın, içinde yaşadığı toplumun durumu ve kendilerini yönetenler hakkında, ortak konularda halk tarafından bilgilendirilmiş katılımı teşvik ederek yeterli görüş kazanmasına ve

eleştirel düşünceye sahip olmasına izin vereceği,

- Yönetimlerin yeterliliğinin ve etkinliğinin artmasını teşvik edeceği ve yozlaşma riskini yok ederek bütünlüklerin korunmasına yardım edeceği,
- Yönetimlerin kamu hizmetleri olarak meşruluğunun onaylanmasına ve kamu yetkililerine karşı halkın güveninin güçlenmesine yardım edeceği,

hususlarını dikkate alarak, üye ülke hükümetlerine, kanunlarında ve uygulamalarında rehber olmak üzere bir kısım kurallar önermiştir.

4.4. Avrupa Birliği belgelerinde bilgi edinme hakkı

Avrupa Birliği'nin (AB) hali hazırda bilgi edinme hakkını düzenleyen iki temel belgesi bulunmaktadır. Bunlardan ilki Avrupa Parlamentosu (AP), Konsey ve Komisyon Belgelerine Kamunun Erişimi Hakkında 30.05.2001 Tarihli 1049/2001 numaralı Avrupa Parlamentosu ve Konseyi Tüzüğü olup, 19 maddeden oluşan söz konusu Tüzük ile Avrupa Toplulukları Antlaşmasının 255'inci maddesinde belirtilen Avrupa Parlamentosu, Konsey ve Komisyon belgelerine, kurumsal ve özel çıkar sebeplerine dayanılarak mümkün olan en geniş kapsamlı erişimi sağlamak amacıyla, bilgi edinme hakkının ilke, koşul ve sınırları açıklanarak, bu hakkın mümkün olan en kolay şekilde kullanılmasını sağlayacak kurallar saptanmıştır.

AB'nin ikinci temel belgesi ise 07.01.2002 tarihli Avrupa Birliği Temel Haklar Şartı olup, bilgi edinme hakkı ile ilgili hükümleri İfade ve bilgilenme özgürlüğünü içeren 11'inci madde, iyi yönetilme hakkını içeren 41'inci madde ve Belgelere Erişim hakkını düzenleyen 42'inci madde olarak karşımıza çıkmaktadır.

4.5. Diğer bölgesel anlaşmalarda bilgi edinme hakkı

2000'li yıllardan sonra bilgi edinme hakkının dünyanın diğer bölgelerinde de bölgesel anlaşmalarda yer aldığı görülmektedir. Nitekim Afrika Birliği'nin 2006 yılında yürürlüğe giren Yolsuzluğu Önleme ve Yolsuzlukla Mücadele Sözleşmesi'nin 9'uncu maddesi bilgiye erişim hakkını düzenlemekte, yine Afrika İnsan Hakları Sözleşmesi'nin 9'uncu maddesi de her bireyin bilgi edinme hakkından bahsetmektedir. Diğer taraftan Amerikan Devletleri Örgütü'nün (ADÖ) kabul ettiği İnsan Hakları Sözleşmesi'nin 13'üncü maddesi bilgiyi arama, elde etme ve yayma özgürlüğünü tanımlamaktadır.

5. Avrupa Konseyi Kararları

Avrupa Konseyi 16.04.2014 tarihinde Bakanlar Komitesinin toplantısında CM/Rec(2014)6 sayılı Tavsiye Kararını kabul etmiştir. Tavsiye kararı doğrultusunda CM/Rec(2014)6 sayılı Tavsiye Kararını ek olarak "İnternet Kullanıcıları İçin İnsan Hakları Rehberi" kılavuzu oluşturulmuştur. Bu tavsiye kararının amacı Avrupa Konseyinin tüm üye ülkelerinde, internette insan haklarının ve temel özgürlüklerin kullanılmasını ve korunmasını destekleyip yaygınlaştırmaktır. Bireylerin ve toplulukların

internete erişimi ve interneti en iyi şekilde kullanımı için bu hak ve özgürlükleri internet ortamında kullanmaları konusunda bilgilendirilmeleri ve güçlendirilmeleri gerekliliği olarak belirtilmiştir. Bu yaklaşım, Avrupa konseyi Bakanlar Komitesinin, internete insan odaklı ve insan haklarına dayalı vizyonunu vurguladığı, internet kullanıcılarının, bir internet yönetişim ilkesi olarak, internette hak ve özgürlüklerini kullanma konusunda güçlendirildiği, 2011 yılında yayınlanan **İnternet Yönetişim İlkeleri Deklarasyonunda** da teyit edilmişti.

İnsan hakları ve temel özgürlükler gerek çevrim dışı gerekse internet ortamında geçerli olan çeşitli Avrupa Konseyi belgelerinde teminat altına alınmış olup, bunlar sadece internete özgü hususlar değildir. Özellikle de Avrupa İnsan Hakları Mahkemesinin içtihatlarında yorumlanan insan hakları ve temel özgürlükler Avrupa İnsan Hakları Sözleşmesinde yer almaktadır. Bir dizi Avrupa Konseyi sözleşmesi ve diğer bağlayıcı olmayan araçlar, internet kullanıcıları için ilave açıklamalar ve yönelimler sunmaktadır. Söz konusu tavsiye kararı aşağıdaki maddelerden oluşmaktadır:

1) Avrupa Konseyi üye ülkeleri, yetki alanları içinde bulunan herkesin, Avrupa İnsan Hakları Sözleşmesinde yer alan insan haklarını ve temel özgürlüklerini güvence altına almakla yükümlüdürler. Bu yükümlülük internet kullanımı bağlamında da geçerlidir. Bu bağlamda, ifade özgürlüğü, bilgiye erişim, toplanma özgürlüğü, siber suçlardan korunma, özel hayatın korunması ve kişisel verilerin korunması haklarının savunulmasıyla ilgili diğer Avrupa Konseyi sözleşmeleri ve belgeleri de geçerlidir.

2) Üye devletlerin, insan haklarına saygı gösterme, insan haklarını koruma ve yaygınlaştırma yükümlülüklerine özel şirketlerin denetlenmesi de dâhildir. Evrensel ve bölünemez olan insan hakları ve bununla ilgili standartlar, internet kullanıcıları üzerine herhangi bir özel sektör oyuncusunun yükleyeceği genel şartlar ve kuralların üzerindedir.

3) İnternet'in bir kamu hizmeti değeri vardır. İnsanlar, topluluklar, kamu yetkilileri ve özel kuruluşlar faaliyetleri için internete ihtiyaç duyarlar ve internet hizmetlerinin erişilebilir, ayrım gözetmeksizin ve makul bir ücret karşılığı sağlanabilir, emniyetli, güvenilir ve sürekli olmalıdır. Dahası, hiç kimse, interneti kullanırken insan haklarını ve temel özgürlüklerini kullanma konusunda yasalara aykırı, gereksiz ve orantısız bir müdahaleye maruz bırakılmamalıdır.

4) Hak ve özgürlükleri kısıtlandığında veya bu hak ve özgürlüklere müdahale edildiğinde kullanıcılar insan haklarını "online" (çevrimiçi) olarak yani çevrim içinde anlayıp etkin bir biçimde kullanma konusunda desteklenmelidirler. Bu destek, etkin hukuk yollarına erişim konusunda rehberliği de içermelidir. İnternetin kamuya ilişkin faaliyetlerin icrasında saydamlık ve hesap verebilirlikle ilgili olarak sunduğu fırsatlar göz önüne alınarak, kullanıcılar demokratik yaşama katılmada internetten yararlanma konusunda güçlendirilmelidirler.

5) Mevcut insan haklarının ve temel özgürlüklerin gerek 'offline' (çevrimdışı)

gerekse "online" olarak eşit bir biçimde uygulanmasını sağlamak üzere, Avrupa Konseyi Bakanlar Komitesi, Avrupa Konseyi Kuruluş Belgesinin 15'inci maddesinin b bendi uyarınca:

- Oluşturulan kılavuzun yurttaşlar, kamu yetkilileri ve özel sektör oyuncuları arasında, internet kullanıcılarının insan haklarının savunulması amacıyla aktif bir biçimde yaygınlaştırılmasını ve kullanıcıların insan haklarını ve temel özgürlüklerini internet üzerinden tam olarak kullanmalarını sağlamak üzere, bu Kılavuzun uygulanması için özel önlemler alınmasını tavsiye eder.
- Özellikle de Avrupa İnsan Hakları Mahkemesi'nin ilgili içtihatları ışığında, Avrupa İnsan Hakları Sözleşmesi'ne aykırı olduğu durumlarda, internette hakların ve özgürlüklerin kullanılmasının değerlendirilmesini, düzenli aralıklarla gözden geçirilmesini ve yerine göre, söz konusu hak ve özgürlüklerin önündeki kısıtlamaların kaldırılmasını tavsiye eder. Uygulanacak herhangi bir kısıtlama, yasa ile öngörülmeli, demokratik bir toplumda geçerli bir amaca ulaşılması için gerekli olmalı ve bu geçerli amaçla orantılı olmalıdır.
- Hak ve özgürlükleri kısıtlandığında veya haklarının ihlal edildiğini düşün düklerinde, internet kullanıcılarının etkili yasal çözümlere erişimlerinin temin edilmesini tavsiye eder. Bunun gerçekleştirilmesi için ilgili kurum, kuruluş ve topluluklar arasında işbirliğinin ve koordinasyonun iyileştirilmesi gerekir. Bu ayni zamanda özel sektör oyuncularının ve sivil toplum örgütlerinin olaya dâhil edilmesini ve bunlarla etkili işbirliğini de gerektirir. İlgili ulusal bağlama bağlı olmak üzere, söz konusu işbirliği, veri koruma makamlarınca, ulusal insan hakları kurumlarınca (Ombudsmanlar – Kamu Denetçisi gibi), yargı usulleri ve acil telefon hatları kanalıyla sağlanacak hak arama mekanizmalarını da içerebilir.
- İnternette insan hakları ve temel özgürlüklerin korunmasını etkileyen standartlar ve prosedürlerle ilgili olarak, Avrupa Konseyi sınırlarının ötesindeki diğer Devlet ve Devletler dışındaki aktörlerle koordinasyonun yaygınlaştırılmasını tavsiye eder.
- Özel sektörün kurumsal sosyal sorumluluklarını yerine getirirken, özellikle de saydamlıkları ve hesap verebilirlikleri açısından, Birleşmiş Milletlerin "Koru, Saygı Göster ve Çare Bul" çerçevesinin uygulanmasını sağlayan, 'İş ve İnsan Haklarıyla İlgili Rehberlik İlkeleri'ne uygun olarak, ilgili devlet yetkilileriyle ve sivil toplumla hakiki bir diyaloğa girmesinin teşvik edilmesini tavsiye eder. Özel sektör aynı zamanda kılavuzun yaygınlaştırılmasına katkıda bulunma konusunda da teşvik edilmelidir.
- Sivil toplum örgütlerinin, kılavuzun internet kullanıcıları için etkili bir vasıta olmasını sağlamak üzere yaygınlaştırılması ve uygulanmasını desteklemeleri için teşvik edilmesini tavsiye eder.

5.1. İnternet kullanıcıları için insan hakları rehberi

Hazırlanan bu rehber internet kullanıcısı için, internet kullanırken sahip olduğu insan haklarını, bunların muhtemel kısıtlamalarını ve bu gibi kısıtlamalarla ilgili olarak başvurulabilecek mevcut yasal çözümleri öğrenebileceği bir araçtır. İnsan hakları ve temel özgürlükler internet üzerinde çevrimiçi olarak da, çevrim dışı olarak da eşit bir biçimde geçerlidir. Bu ilke diğer internet kullanıcılarının hak ve özgürlüklerine saygıyı da içerir. Kılavuzda size internet bağlamında, pratikte hak ve özgürlüklerin neler olduğu, bu hak ve özgürlüklere nasıl bel bağlanabileceği ve bunların nasıl kullanılabileceği ve bunun yanı sıra, hukuksal yollara nasıl başvurulabileceğiyle ilgili bilgiler sunulmaktadır.

Bu rehber, insan haklarının korunmasına ilişkin Avrupa İnsan Hakları Sözleşmesi ve diğer Avrupa Konseyi sözleşmeleri ve belgelerine dayalıdır. Avrupa Konseyi'nin tüm üyeleri, imzalayıp kabul ettikleri belgelerde yer alan hak ve özgürlüklere saygı göstermek, onları korumak ve yerine getirmekle görevlidirler. Rehber aynı zamanda bu hak ve özgürlüklerin Avrupa İnsan Hakları Mahkemesi'nce sürekli yorumlanmasından ve Avrupa Konseyi'nin ilgili diğer belgelerinden esinlenmiştir. Rehberde bireylerin dijital hakları 7 başlıkta altında ifade edilmiştir.

- Erişim ve ayrımcılık yapmama,
- İfade ve bilgi özgürlüğü,
- Toplanma, örgütlenme ve katılım özgürlüğü,
- Mahremiyet ve verilerin korunması
- Eğitim ve okur-yazarlık,
- Çocukların ve gençlerin korunması,
- Etkili yasal yollar ve tazminat,

5.1.1. Erişim ve ayrımcılık yapmama

İnternete erişim ve ayrımcılığa maruz kalınmaması için ilgililerin yapması gerekenler 5 başlık altında toplanmıştır:

- İnternete erişim, hak ve özgürlüklerin kullanılmasında ve demokrasiye katılımda önemli bir araçtır. Bu nedenle mahkeme kararı olmaksızın hak ve özgürlüklerin kullanımını ihlal edecek şekilde internet bağlantısı kesilemez. Bazı durumlarda sözleşmelerden kaynaklanan düzenlemeler sonucunda hizmet kesintiye uğrayabilir ancak bu, en son başvurulacak bir tedbir olarak düşünülmelidir.
- Bireylerin internete erişimi makul bir ücret karşılığında olmalı ve herkese hiçbir ayrım gözetilmeksizin sağlanmalıdır. Bireyler kendileri seçtikleri teknolojik cihazları kullanarak internet içeriğine, uygulamalarına ve hizmetlerine mümkün olan en geniş biçimde erişim sağlayabiliyor olmalıdır.
- Kırsal ve coğrafi olarak uzak bölgelerde yaşayan, düşük gelirli ve/veya özel ihtiyaç veya engeller varsa kamu makamlarınca bu bireylerin internete erişimini kolaylaştırmak için makul bir gayret gösterilmeli ve bu konuyla ilgili özel tedbirler alınmalıdır.
- Bireyler kamu yetkilileriyle, internet servis sağlayıcılarıyla ve içerik ve hiz-

met sağlayıcılarla veya diğer gruplarla veya kullanıcı gruplarıyla ilişkilerinde, toplumsal cinsiyet, ırk, renk, dil, din veya inanç, siyasi veya diğer görüş, ulusal veya sosyal köken, ulusal bir azınlıkla bağlantı, mülk, doğum veya etnik köken, yaş veya cinsel yönelim gibi diğer durumlar nedeniyle ayrımcılığa uğramamalıdırlar.

5.1.2. İfade ve bilgi özgürlüğü

Bireyler, herhangi bir müdahaleye maruz kalmadan ve ulusal sınırlar göz önüne alınmaksızın istedikleri ve seçtikleri bilgi ve fikirleri araştırma, alma ve verme hakkına sahiptirler. Bu noktada bireylerin bu haklarını kullanmadaki yaklaşım şekilleri ve devletlerin bireylere yaklaşımları şu şekilde olmalıdır:

Tüm bireyler, internet üzerinden çevrimiçi olarak kendilerini ifade etme ve diğerlerinin bilgi ve görüşlerine erişim özgürlüğüne sahiptirler. Buna, siyasi konuşmalar, dinle ilgili görüşler, olumlu kabul edilen ve incitici bulunmayan görüş ve ifadelerin yanı sıra, diğerlerini rencide edebilecek, şoke edebilecek veya rahatsız edebilecek görüş ve ifadeler de dâhildir. Bireyler bu noktada mahremiyet hakkı dâhil olmak üzere, başkalarının saygınlığına veya haklarına gerekli duyarlılığı göstermelidir.

Yapılacak kısıtlamalar ayrımcılığı, nefret duygularını veya şiddeti tetikleyen ifadeler için uygulanabilir. Söz konusu kısıtlamalar yasalara uygun olmalı, dar kapsamlı tutulmalı ve mahkemelerin gözetiminde uygulanmalıdır. Bireyler, internet ortamında telif hakları dâhil olmak üzere, fikri mülkiyet haklarının korunmasına saygı göstermek şartıyla içerik oluşturmakta, içeriği yeniden kullanıp dağıtmakta serbesttirler.

İfade ve bilgilenme özgürlüğüne saygı göstermek ve bu özgürlükleri korumak kamu yetkililerinin bir görevidir. Bu özgürlüklere getirilecek herhangi bir kısıtlama keyfi olmamalı, Avrupa İnsan Hakları Sözleşmesi'ne uygun olarak, diğer amaçların yanı sıra, ulusal güvenliğin veya kamu düzeninin, kamu sağlığının ve ahlakının korunması gibi geçerli bir amaca yönelik olmalı ve insan hakları yasasıyla uyumlu olmalıdır. Ayrıca, bu kısıtlamalar bu konuda bireye rehberlik edecek ve bireyin hakkını aramasına yardımcı olacak bilgilerle birlikte bireyin bilgisine sunulmalı ve yalnızca geçerli bir amaca ulaşılması için gerekli olandan daha geniş kapsamlı veya daha uzun süreli kısıtlamalar olmamalıdır.

İnternet servis ve içerik sağlayıcısının insan haklarına saygı gösterme ve bireyin taleplerine cevap verecek mekanizmalar sağlama konusunda kurumsal anlamda sorumlulukları vardır. Ancak bireylerin, sosyal ağlar gibi çevrimiçi servis sağlayıcılarının içerikle ilgili politikaları nedeniyle belirli tür içerik ve davranışları kısıtlayabileceklerini bilmeleri gerekir. Bu tür platformlar, söz konusu hizmeti kullanıp kullanmama konusunda bireyleri bilgilendirerek bir şekilde özgürce karar verebilmesi için bireyi muhtemel kısıtlamalardan haberdar etmektedir.

5.1.3. Toplanma, örgütlenme ve katılım özgürlüğü

Gerçek hayatta bireyler nasıl ki toplanma, örgütlenme ve katılım hakkına sahipse aynı şekilde interneti kullanarak diğer bireylerle bir araya gelme ve dernek kurma hakkına da sahiptirler Pratikte bu şu anlamlara gelmektedir:

- Bireyler, kamu yetkililerince resmen tanınmasına veya tanınmamasına gerek kalmaksızın sosyal gruplar ve topluluklar kurma, bunlara katılma, bunları harekete geçirme ve bunlarda yer alma amacıyla herhangi bir web sitesini, uygulamayı veya diğer hizmet oluşumunu seçme özgürlüğüne sahiptirler. Aynı zamanda bireyler işçi sendikası kurma ve bunlara katılma hakkını kullanmak için de interneti kullanabilme hakkına sahiptir. Elbette bu hak kullanılırken, kişisel hakları, kişilerin özel hayatının gizliliğinin ve kamu düzeni ve milli güvenliğin ihlal edilmemesine, gerçek hayatta suç olanın internette de suç olduğu anlayışına dikkat edilmelidir.

- Bireyler, internet üzerinden barışçı bir biçimde protesto eylemi gerçekleştirme hakkına sahiptirler. Ancak, çevrimiçi protesto eylemi tıkanıklıklara, diğer bireylerin hak ve özgürlüklerinin ihlaline, hizmetlerin sekteye uğramasına ve/veya başkalarının malına zarar verilmesine neden olursa, bunun yasal sonuçlarıyla karşılaşabileceği unutulmamalıdır.

- Benzer şekilde bireyler, gerçek hayatta olduğu gibi dilekçeler imzalamak ve internetin nasıl yönetileceğine dair politikaların oluşturulmasına katılmak da dâhil, yerel, ulusal ve küresel kamu politikaları tartışmalarına, yasamayla ilgili inisiyatiflere ve karar verme süreçlerinin kamu tarafından incelenmesine katılmak üzere mevcut çevrimiçi araçları kullanma özgürlüğüne sahiptirler. Bu durum aslında demokrasinin gelişmesine de katkı sunacak ve iyi bir yönetişim örneği olacaktır.

5.1.4. Mahremiyet ve verilerin korunması

Bireyler gerçek hayatta olduğu gibi internette de özel ve aile yaşamı hakkına sahiptirler. Bunun gerçek hayattan ayrı düşünülmemesi gerekir. Çünkü mahremiyetin ihlali ve kişisel verilerin izinsiz kullanımı sadece gerçek hayata ilişkin bir durum olmaktan çıkmıştır. Artık bireylerin, gerçek hayattaki gibi internette de bir kimlikleri, bir mahremiyetleri yani özel hayatları ve kişisel bilgileri mevcuttur. Dolayısıyla bireylerin kişisel verilerinin korunması, yazışmalarının ve iletişiminin gizliliğinin sağlanması da bu kapsamda değerlendirilmesi gereken önemli bir husustur. Bu şu anlamlara gelmektedir:

- Bireyler, interneti kullanırken kişisel verilerinin düzenli aralıklarla işleme tabi tutulduğunu bilmelidir. Bu, internet tarayıcıları, elektronik posta, mesajlar, internet üzerinden sesle iletişim protokolleri, sosyal ağlar, arama motorları ve bulut veri saklama hizmetlerini kullanırken gerçekleşmektedir.

- Kamu makamlarının ve özel şirketlerin, bireylerin kişisel verilerini işleme

tabi tutarken belirli kurallara ve prosedürlere saygı gösterme yükümlülükleri vardır.

- Kişisel veriler, sadece yasalar tarafından öngörüldüğünde veya bireyin rızasıyla işleme tabi tutulmalıdır. Hangi kişisel verilerin işleme tabi tutulduğu ve/veya üçüncü taraflara aktarıldığı, bu işlemin ne zaman, kimin tarafından ve ne amaçla yapıldığı konusunda bireylerin bilgilendirilme hakları bulunmaktadır. Bireylerin genel kişisel verileri üzerinde kontrol yetkisini kullanabilmesi gerekir. Yani bireyler kişisel verilerinin doğruluğunu kontrol edebilmeli, bu verilerde düzeltme yapabilmeli, silinmesini talep edebilmeli, kişisel verilerinin gereğinden uzun bir süre saklanıp saklanmadığını görebilmelidir.
- Bireyler, keyfi olarak genel gözetleme veya dinleme tedbirlerine maruz bırakılmamalıdır. Yasal mevzuatta öngörülen istisnai durumlarda, örneğin bir ceza soruşturması amacıyla kişisel veriler bağlamında bireylerin mahremiyetine müdahale edilebilir. Bu açıdan bireylere ilgili yasal mevzuat veya politikalar ve bu konudaki hakları konusunda erişilebilir, anlaşılabilir ve net bilgiler sağlanmalıdır.
- İş yerinde de bireylerin mahremiyetine saygı gösterilmelidir. Buna bireylerin özel çevrimiçi yazışmalarının ve iletişim mesajlarının mahremiyeti de dâhildir. İşveren, bireyle ilgili olarak gerçekleştirilen herhangi bir gözetleme ve/veya izlemeden bireyi doğrudan haberdar etmelidir.

5.1.5. Eğitim ve okur-yazarlık

Bireyler internette bilgiye erişim hakkı da dâhil olmak üzere eğitim hakkına sahiptirler. İnternet üzerinden elektronik kütüphanelere, veri tabanlarına, açık kaynaklara, uzaktan eğitim programlarına erişebilmek gibi birçok işlem bu kapsamda değerlendirilebilir. İnternette bilgiye erişim hakkı ve okur-yazarlıktan kasıt şudur:

- Bireyler, resmi dillerde, eğitime ve kültürel, bilimsel, akademik ve diğer içeriğe çevrimiçi olarak erişime sahip olmalıdır. Fakat fikri mülkiyet hakkı sahiplerine eserleri karşılığında ödeme yapılabilmesi için bu erişim bazı koşullara tabi olabilir. Bununla birlikte bireyler, gerektiğinde internetteki kamuya açık alanda kamunun oluşturduğu araştırma ve kültür eserlerine serbestçe erişim sağlayabilmelidir.
- Bireyler, internet ve medya okuryazarlığının bir parçası olarak, internetteki hak ve özgürlüklerinizi kullanmak üzere dijital eğitime ve bilgiye erişim sağlayabilmelidir. Dijital eğitim ve bilgiye erişim, çok geniş bir yelpazeyi kapsayan internet araçlarını anlamaya, kullanmaya ve bunları kullanarak çalışmaya yönelik becerileri de içermektedir. Bu sayede bireyler, erişim sağladığı veya erişmek istediği içerikler, uygulamalar ve hizmetlerin doğruluğunu ve güvenilirliğini eleştirel bir biçimde analiz edebilme olanağına kavuşmuş olacaktır.

5.1.6. Çocukların ve gençlerin korunması

Yetişkinler gibi çocuklar veya gençler de bir insan olarak, tüm hak ve özgürlüklere sahiptirler. Bu hakların sadece belli bir hedef kitleye özgü olduğunu düşünmek kabul edilebilir bir durum değildir. Bu haklarla birlikte özellikle de çocukların ve gençlerin yaşlarının küçük olması nedeniyle, interneti kullanma, internete erişme hak ve özgürlüklerini kullanırken başkaları tarafından herhangi bir istismara uğramamaları için özel korumaya ve rehberliğe hakları bulunmaktadır. Çocukların ve gençlerin internette korunmasından anlaşılması gereken şunlardır:

- Çocuk ve genç bireyler, görüşlerin özgürce ifade etme ve toplum yaşamına katılma, sesini duyurma ve onları etkileyen konularda karar verme sürecine katkıda bulunma hakkına sahiptirler. Görüşlerine, ayrımcılık yapılmaksızın, yaşlarına ve olgunluk durumlarına göre gereken ağırlık verilmesi gerekir.

- Onlar, internet ortamında mahremiyetlerini nasıl koruyacakları da dâhil olmak üzere, internetin bilinçli ve güvenli bir biçimde kullanılması konusunda öğretmenlerinden, eğitimcilerden ve ebeveynlerinden veya velilerinden yaşlarına ve eğitim düzeylerine uygun bir dilde bilgi almayı bekleme hakları vardır. Bu bilgileri vermek söz konusu kişilerin sorumluluğundadır.

- Çocukların ve gençlerin, internette oluşturacakları veya diğer internet kullanıcılarının onlarla ilgili olarak oluşturacakları içeriğe dünyanın her tarafından erişilebileceğini ve bunun onların onurlarını, güvenliğin ve özel hayatlarının gizliliğini tehlikeye atabileceğini, şimdi veya hayatlılarının daha sonraki bir evresinde kendilerine veya haklarına bir şekilde zarar verebileceğini bilmeleri gerekmektedir.

- Çocuklar ve gençlere, yasadışı çevrimiçi içerik ve davranışlar (örneğin çevrimiçi taciz) ve ayni zamanda yasa dışı olduğu iddia edilen içeriğin ilgili makamlara bildirilebileceği konusunda açık ve anlaşılır bilgiler verilmesini bekleme hakkına sahiptirler. Bu bilgiler onların yaşlarına ve içinde bulunduğu şartlara göre uyarlanmalıdır. Bu bilgiler, onların özel hayatlarının gizliliğini ihlal etmeden, kimliklerini açıklamadan, özel hayatlarına saygı duyularak tavsiye niteliğinde verilmelidir.

- Çocuklara ve gençlere özellikle de internette cinsel istismar ve tacizle ve diğer siber suçlarla ilgili olarak, fiziksel, zihinsel ve ahlaki sağlıklarına yönelik müdahalelere karşı onlara özel bir korunma sağlanmalıdır. Onlar, özellikle de bu tür tehditlere karşı kendilerini korumak üzere eğitilme hakkına sahiptirler

5.1.7. Etkili yasal yollar ve tazminat

Bireyler, hakları ve temel özgürlükleri kısıtlandığında veya ihlal edildiğinde etkili bir hukuk yoluna başvurma hakkına sahiptirler. Hukuki bir çözüme ulaşmak için yasal işlemlere hemen başlamaya gerek olmasa da yasal çözüm arama yolları mevcut olmalı, bilinir olmalı, erişilebilir olmalı, makul

maliyetli olmalı ve uygun tazmin ve telafiyi sağlayabilmelidir. Etkili hukuksal çözümler doğrudan doğruya internet hizmet sağlayıcılarından, kamu yetkililerinden ve/veya insan hakları kurumlarından sağlanabilir. Söz konusu ihlale bağlı olmak üzere, etkili yasal çözümler arasında soruşturma, açıklama, yanıt, düzeltme, özür dileme, hakların eski haline getirilmesi, internet bağlantısının yeniden sağlanması ve tazminat yer alabilir. Uygulamada bu şu anlama gelmektedir:

- İnternet hizmet sağlayıcısı, çevrimiçi içerik ve servis sağlayıcıları veya diğer şirket ve/veya kamu makamları bireyleri hakları, özgürlükleri ve bunları nasıl elde edeceklerine ilişkin yasal çözümler konusunda bilgilendirmelidir. Bu bilgilendirmeye, bireyin haklarına müdahaleyle ilgili bildirim yapma ve şikâyette bulunma ve haklarının telafisi konusunda bilgiye kolayca erişim de dâhildir.

- Etkili yasal yollarla ilgili ilave bilgiler ve rehberlik kamu makamlarınca, ulusal insan hakları kurumlarınca (Ombudsmanlar gibi), veri koruma makamlarınca, danışma merkezlerince, insan hakları, dijital haklar veya tüketici gibi kuruluşlarca sağlanabilir.

- İlgili makamlar, siber suçlar gibi özellikle de bireylerin dijital kimliklerine, bilgisayarlarına ve bilgisayarlarındaki bilgilere yasa dışı erişim, bunlara müdahale, bunlarda sahtecilik veya bunlarla ilgili diğer dolandırma amaçlı manipülasyon söz konusu olduğunda, bireyleri internette işlenen veya internet kullanılırken işlenen suç faaliyetlerine veya ceza suçlarına karşı, korumakla yükümlüdürler.

- Bireyler, internetle ilgili olarak hak ve özgürlüklerinin belirlenmesinde veya bir ceza suçuyla suçlanmasında bağımsız ve tarafsız bir mahkeme tarafından makul bir süre içinde adil yargılanma hakkına sahiptirler. Tüm iç hukuk yolları tüketildiğinde de Avrupa İnsan Hakları Mahkemesine bireysel başvuru hakkına sahiptirler.

6. 5651 Sayılı Kanun Kapsamında Hak ve Sorumluluklar

Bilişim denildiğinde bunun en önemli bileşeni olan internet akla gelmektedir. Türkiye'de internet konusunda en kapsamlı yasal düzenleme internet kanunu olarak da bilinen 04.05.2007 tarih ve 5651 sayılı **"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**" ile yapılmıştır. Kanunun amacı ve kapsamı; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek olarak ifade edilmektedir. Söz konusu yasayı koruyucu önleyici işlev gören bir yasa olarak değerlendirmekte fayda vardır.

Burada içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı kavramlarını konunun daha iyi anlaşılması

açısından açıklamak gerekir. Erişim Sağlayıcı; kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri, İçerik sağlayıcı; internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri, Toplu Kullanım Sağlayıcı; kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı ifade etmektedir. Ayrıca kurum ifadesiyle kastedilmek istenen Bilgi Teknolojileri ve İletişim Kurumudur.

Bu kapsamda bireyler internet ortamında kendilerine rahatsız eden içeriklerle ilgili şikâyet ve ihbarda bulunabilme hakkına sahip olmuşlardır. Dolayısıyla bireyler hem bu haklarını yerine getirirlerken aslında temiz bir internet ortamının oluşması için de sorumluluklarını yerine getirmektedirler. Kanun, Türk Ceza Kanunu (TCK)'ndaki maddelere atıfta bulunarak bu suçların internet ortamında gerçekleşmesi durumunda yapılacakları düzenlemiş ve bu konuda internet aktörlerine sorumluluklar yüklemiştir. Türkiye'de 5651 sayılı kanun ile ilk defa aşağıdaki başlıklar altında düzenlemeler yapılmıştır:

- İnternet aktörleri olan içerik sağlayıcı, yer ve erişim sağlayıcı, toplu kullanım sağlayıcı tanımı yapılmış ve bu aktörlerin hak ve sorumlulukları belirlenmiştir.
- Yasada suçlar bakımından suçun işlendiği internet sitesi, URL, IP adresine erişimin engellenmesinin hangi usul ve esaslara göre yapılacağı düzenlenmiştir.
- İnternet ortamında yayınlanan içerik nedeniyle haklarının ihlal edildiğini iddia eden kişilere ilişkin; içeriğin yayından çıkarılmasını sağlama ve cevap hakkı uygulamalarına ilişkin usul ve esaslara yer verilmiştir.
- Konusu suç teşkil eden ve/veya küçükler için zararlı içeriklere sahip sitelerle ilgili filtreleme usulü öngörülmüştür.
- Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen katalog suçlara ilişkin şikâyetlerin yapılabileceği İnternet Bilgi İhbar Merkezi (www.ihbarweb.org.tr) kurulmuştur.

6.1. İnternette yasadışı içerikler ve bunlarla mücadele

İnternet ortamında yasadışı içeriklerle ilgili 5651 sayılı yasanın;

- 8'inci maddesinde yer alan katalog suçlar,
- 8/A maddesinde millî güvenlik ve kamu düzeninin korunması,
- 9'uncu maddesinde kişilik haklarının ihlali,
- 9/A maddesinde özel hayatının gizliliğinin ihlali,

durumlarında ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi tedbiri uygulanmaktadır. 8'inci maddedeki katalog suçlar dışındaki maddeler için erişimin engellenmesi kararları erişim sağlayıcılar birliği tarafından yerine getirilir. Bu kararlar erişim sağlayıcıları birliğine gönderilir. Bu kapsamda Birliğe yapılan tebligat erişim

sağlayıcılara yapılmış sayılır. Birliğin mevzuata uygun olmayan kararlara itiraz hakkı vardır.

6.1.2. Katalog suçlar (5651 sayılı kanun madde 8)

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ile düzenlenmiş olan suçlardır. Bu kanun ile internet ortamında işlenen 8 suç için, suçun işlendiği internet sitesi, URL veya IP adresine erişim engelleme kararı verilebilmektedir. Bu suçlar; kanunun 8'inci maddesinde düzenlenmiş olan İntihara Yönlendirme, Çocukların Cinsel İstismarı, Uyuşturucu veya Uyarıcı Madde Kullanılmasını Kolaylaştırma, Sağlık için Tehlikeli Madde Temini, Müstehcenlik, Fuhuş, Kumar Oynanması için Yer ve İmkân Sağlama ve Atatürk Aleyhine İşlenen Suçlardır. Bu suçlarla ilgili ihbarda bulunulacak resmi internet adresi https://www.ihbarweb.org.tr/ adresidir. Bu adresten internet üzerinde işlenen suçun kategorisi seçilerek ve içeriğin yayınlandığı internet adresi belirtilerek ihbarda bulunulabilmektedir.

1) İntihara yönlendirme (TCK Madde 84)

5237 sayılı TCK'nın intihara yönlendirme başlıklı 84'üncü maddesi gereği, internet ortamında yapılan yayınlarda intihara yönlendirme, azmettirme, teşvik etme, başkasının intihar kararını kuvvetlendirme veya intihara herhangi bir şekilde yardım etme fiillerinden birinin veya birkaçının oluştuğu durumlarda internet bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

2) Çocukların cinsel istismarı (TCK Madde 103, birinci fıkra)

5237 sayılı TCK'nın 103'üncü maddesi gereği, internet ortamında yapılan yayınlarda, 18 yaşından küçük bireylere cinsel istismar suçunun işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

3) Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (TCK Madde 190)

5237 sayılı TCK'nın 194'üncü maddesi gereği, internet ortamında yapılan yayınlarda sağlık için tehlikeli madde (alkollü içkiler, tütün, tiner ve sağlık için tehlikeli her türlü madde) temini suçunun işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

4) Sağlık için tehlikeli madde temini (Madde 194)

5237 sayılı TCK'nın 190'ıncı maddesi gereği, internet ortamında yapılan yayınlarda uyuşturucu veya uyarıcı madde kullanımını kolaylaştırma veya özendirme suçlarının işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

5) Müstehcenlik (TCK Madde 226)

5237 sayılı TCK'nın 226'ıncı maddesi gereği, internet ortamında yapılan yayınlarda müstehcenlik suçunun işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

6) Fuhuş (Madde 227)

5237 sayılı TCK'nın 227'inci maddesi gereği, internet ortamında yapılan yayınlarda kişilerin ve özellikle çocukların fuhuşa

teşvik edilmesi, bunun yolunun kolaylaştırılması, buna aracılık edilmesi suçlarından birinin veya birkaçının işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

7) Kumar oynanması için yer ve imkân sağlama (Madde 228)

5237 sayılı TCK'nın 228'inci maddesi gereği, internet ortamında yapılan yayınlarda kumar oynanması için yer ve imkân sağlama suçunun işlendiği durumlarda bilgi ihbar merkezi üzerinden ihbarda bulunulabilmektedir.

8) Atatürk Aleyhine İşlenen Suçlar

İnternet ortamında yapılan yayınlarda, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'a aykırılık bulunduğunu düşünüldüğünde İnternet Bilgi İhbar Merkezi üzerinden ihbarda bulunulabilmektedir.

6.1.3. Erişimin engellenmesi kararı ve yerine getirilmesi

İnternet ortamında yapılan ve içeriği yukarıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişim engelleme karar verilir. Erişimin engellenmesi kararı, soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından verilir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilebilir.

Bu durumda Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Cumhuriyet savcısı tarafından derhal kaldırılır. Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir. Koruma tedbiri olarak verilen erişimin engellenmesine ilişkin karara 4.12.2004 tarih ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz edilebilir.

İçeriği bu katalogda belirtilen suçları oluşturan yayınların içerik veya yer sağlayıcısının yurt dışında bulunması halinde veya içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocukların cinsel istismarı, müstehcenlik ve fuhuş suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Başkan tarafından verilir. Bu karar, erişim sağlayıcısına bildirilerek gereğinin yerine getirilmesi istenir. Burada başkan, Bilgi Teknolojileri ve İletişim Kurumu Başkanıdır.

Erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir. Başkan tarafından verilen erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkan tarafından, Cumhuriyet başsavcılığına suç duyurusunda bulunulur. 5651 sayılı kanunun 8'inci maddesi kapsamı dışında kalan erişim engelleme kararlarının uygulanmak üzere erişim sağlayıcılara bildirilmesi görevi Erişim Sağlayıcıları Birliği'ne aittir. Erişim Sağlayıcıları Birliği ile ilgili detaylı bilgiye https://www.esb.org.tr/ adresinden erişmek mümkündür.

6.1.4. Milli güvenlik ve kamu güvenliğinin ihlali

İnternet ortamında bireylerin yaşam hakkını tehlikeye sokan, can ve mal güvenliğini ortadan kaldıran durumlar çok yoğun olarak yaşanabilmektedir. Özellikle terör ve terörist faaliyetlerin internet ortamında milli güvenlik ve kamu düzenini tehlikeye sokacak boyutlara ulaştığı görülebilmektedir. Bunu engellemek amacıyla yasa koyucu 5651 sayılı kanunun 8/A maddesi kapsamında düzenleme yapmıştır. Bu kapsamda; internette milli ve manevi değerlere saldırı ile sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak yapılan hakaret ve saldırıların yer aldığı internet siteleri ile karşılaşılması durumunda Emniyet Genel Müdürlüğü İhbar Hattı https://www.egm.gov.tr/sayfalar/ihbar.aspx adresi üzerinden ihbarda bulunabileceği gibi en yakın kolluk birimine ya da savcılığa da durum yazılı veya sözlü olarak iletilebilir.

Bu düzenlemeye göre; yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde, Başbakanlık veya millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması ile ilgili bakanlıkların talebi üzerine Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı tarafından internet ortamında yer alan yayınla ilgili olarak içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilebilir. Karar, Başkan tarafından derhâl erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilir. İçerik çıkartılması ve/veya erişimin engellenmesi kararının gereği, derhâl ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilir.

Başbakanlık veya ilgili Bakanlıkların talebi üzerine Başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararı, Başkan tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi hâlde, karar kendiliğinden kalkar. Bu madde kapsamında verilen erişimin engellenmesi kararları, ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda, internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilir.

Bu madde kapsamındaki suça konu internet içeriklerini oluşturan ve yayanlar hakkında Başkan tarafından, Cumhuriyet Başsavcılığına suç duyurusunda bulunulur. Bu suçların faillerine ulaşmak için gerekli olan bilgiler içerik, yer ve erişim sağlayıcılar tarafından hâkim kararı üzerine adli mercilere verilir. Bu bilgileri vermeyen içerik, yer ve erişim sağlayıcıların sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç bin günden on bin güne kadar adli para cezası ile cezalandırılır. Bu madde uyarınca verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereğini yerine getirmeyen erişim sağlayıcılar ile ilgili içerik ve yer sağlayıcılara Başkan tarafından elli bin Türk lirasından beş yüz bin Türk lirasına kadar idari para cezası verilir.

6.1.5. Kişilik haklarının ihlali

Bireylerin bilgiye her an ulaşabildiği, anlık bilgi paylaşımlarında bulunabildiği internet ortamı ve özellikle sosyal medya platformları günümüzün sosyal, kültürel ve iktisadi gelişmelerinde yönlendirici özelliğe sahip önemli bir aktör haline gelmiş bulunmaktadır. Bu ortamdaki anlık paylaşımlar dikkate alındığında oldukça fazla etkileşimin olduğu görülmektedir. Elbette internet; internetin, bilgiye kısa sürede ulaşmada, toplumda ve dünyada olan olayları, gündemi takip etmede çok önemli fayda sağladığı tartışmasız bir gerçektir. Ancak internette başta bireyin kişilik hakları olmak üzere, kişi hak ve hürriyetlerine süreklilik taşıyacak şekilde müdahalenin olduğu, bunun tahammül edilemez boyutlara ulaştığı da bir gerçektir.

Başta sosyal medya platformları başta olmak üzere internetin farklı platformlarında bireylerin kişilik haklarını ihlal eden paylaşım ve yorumlara oldukça fazla rastlanmaktadır. Yalan haberden, hakarete, itibar suikastına, iftiraya varan içerikler üretilmekte ve bu ortamlarda sorumsuz bir şekilde ve sonucunun nereye varacağına bakılmadan paylaşılmaktadır. Kişilik hakkı ihlali yapanlar bazen farklı ve sahte kimlikler arkasına gizlenerek bunu yaparken bazen de gerçek kimlikleriyle bunu gerçekleştirmektedirler. Suçun işlendiği ortamın internet olması suçun mahiyetini asla değiştirmez.

Böyle bir durumda en önemli şey, kişilik hakları ihlal edilen bireyin hakkını nerede, nasıl ve hangi kanun kapsamında arayacağını bilmesidir. Böyle bir durumda birey kişilik haklarının ihlal edildiği yayına erişim engelleme talebinde bulunabileceği gibi mevcut mevzuat kapsamında kişilik haklarını ihlal eden kişilerin tespit edilmesi amacıyla suç duyurusunda bulunabilmekte ve bunlar hakkında dava açabilmektedir. Gerçek hayatta veya internet ortamında olsun fark etmez hakaret eden kişinin TCK'nın 125'inci maddesine göre 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılması söz konusu olabilmektedir.

Bununla birlikte kişilik hakkı ihlal edilen bireylerin bunu yapanlar hakkında medeni kanunun 49'uncu maddesine göre manevi tazminat davası açma hakları bulunmaktadır. Medeni Kanunun 49'uncu maddesi; "şahsiyet hakkı hukuka aykırı bir şekilde tecavüze uğrayan kişi, uğradığı manevi zarara karşılık manevi tazminat namıyla bir miktar para ödenmesini dava edebilir. Hâkim, manevi tazminatın miktarını tayin ederken, tarafların sıfatını, işgal ettikleri makamı ve diğer sosyal ve ekonomik durumlarını da dikkate alır." denilmektedir.

İnternet ortamında kişilik hakları ihlali gerçekleşmesi durumunda bireyin, 5651 sayılı '**İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun**'un 9'uncu maddesine göre ihlalin yapıldığı sitedeki içeriğin çıkartılmasını isteme veya bu isteğin karşılanmaması durumunda da hakkın ihlal edildiği internet adresine erişimin engellemesin talep etme hakkı bulunmaktadır.

İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe eri-

şimin engellenmesini de isteyebilir. Bu talebin içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılması gerekmektedir. İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilmektedir.

Hâkim tarafından erişimin engellenmesi kararları esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilmekte olup hâkim eğer URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirirse, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir. Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Erişim Sağlayıcılar Birliği'ne gönderilir. Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilmesi gerekir. Eğer benzer ihlal başka internet adreslerinde de vuku bulursa mevcut erişim engelleme kararı bu siteler için de uygulanır. Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır.

İnternet ortamında Kişilik Haklarının İhlali hususunda başvuru yapmak isteyen kişiler, başvuru örneklerine http://internet.btk.gov.tr adresinden ulaşabileceği gibi **Mahkeme başvuru örneği** ve **İçerik sağlayıcı başvuru örneği** için ekteki şablon belgelerden faydalanarak başvuru belgelerini oluşturabilirler.

6.1.6. Özel hayatın gizliliğinin ihlali

Bir diğer önemli husus, internet ortamında bireylerin özel hayatlarının gizliliğinin ihlal edilerek mağdur edilmesidir. Ne yazık ki günümüzde insanların haberi olmadan uygunsuz görüntülerinin çekilerek internet ortamında paylaşılması durumu oldukça sık rastlanan bir durumdur. Bu tür ihlaller, intiharlara kadar gidebilecek geri dönüşü olmayan çok olumsuz sonuçlara sebep olabilmektedir. Böyle bir durumda bu suçu işleyenlerin tespit edilmesi amacıyla savcılığa suç duyurusunda bulunulması, suça konu olan görüntülerin paylaşıldığı internet sitelerine erişimin engellenmesi seçeneklerinin değerlendirilmesi gerekmektedir.

Bu kapsamda 5651 saylı yasanın 9/A maddesine göre; internet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilmektedir. Doğrudan başvuru için BTK'nın https://www.ihbarweb.org.tr/ohg/ adresi kullanılabilmektedir.

Hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz. BTK başkanı, kendisine gelen bu talebi uygulanmak üzere derhâl

Erişim Sağlayıcılar Birliğe'ne bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. Erişimin, engellenmesi tedbiriözel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olan (URL şeklinde) içeriğe yapılır.

Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar.

İnternet ortamında özel hayatın gizliliğinin ihlali hususunda başvuru yapmak isteyen kişiler, başvuru örneklerine http://internet.btk.gov.tr adresinden ulaşabileceği gibi BTK'nın https://www.ihbarweb.org.tr/ohg/ adresinden doğrudan başvurabilmektedirler. Bununla birlikte eklerde yer alan Mahkeme başvuru örneği ve Kurum başvuru örneği kullanılabilir.

6.2. İnternet kullanıcı farkındalığı ve internet yardım

Bilgi Teknolojileri ve İletişim Kurumu tarafından sunulan İnternet Yardım Merkezi Portali'nde, kullanıcıların interneti bilinçli ve güvenli kullanımı kapsamında aşağıdaki konularda yaşadıkları problemlere yönelik çözüm önerileri bulunmaktadır. Bununla birlikte; kullanıcılar portaldeki mevcut içeriklerde bulamadığı hususlarda yardım formu aracılığıyla bilgi talebinde bulunabilmektedir.

1) İnternette Yasadışı İçerikler

2) İnternet ve Mahremiyet

3) İnternet ve Bilgi Güvenliği

4) Sosyal Ağ Platformları

5) Online Oyunlar

6) Siber Zorbalık

7) İnternet ve Sağlık

8) Güvenli İnternet Hizmeti

Ayrıca internet kullanıcıları, internetin bilinçli ve güvenli kullanımı ile birlikte internet ortamı için çeşitli bilgilerin yer aldığı; Güvenli Web (http://www.guvenliweb.org.tr/) ve http://internet.btk.gov.tr/ portallerinden destek alabilmektedir.

Sonuç ve Değerlendirme

İnternet, sosyal medya başta olmak üzere diğer tüm platformlarıyla birlikte bireylerin iletişim hakkını kullanarak bilgi edindiği ve ifade özgürlüğünü kullandığı güçlü ve etkili bir iletişim platformudur. Evet, internet bir özgürlük alanıdır, lakin sonsuz bir özgürlük alanı değildir. Bu ortamı kullanan diğer bireylerin özgürlük alanlarını ihlal edildiği an bu ortamdaki özgürlüğün de bittiği andır. Hemen herkesin bildiği ve ifade ettiği bir kural vardır. Bu da "Gerçek hayatta suç olan şey, internet ortamında da suçtur" kuralıdır. İnternette haklarını ve sorumluluklarını bilen bilinçli internet kullanıcısı;

- İnternet ortamında nasıl hareket etmesi gerektiğini bilen,
- Karşılaştığı olumsuz durumlarda nasıl davranması gerektiğini bilen,
- Mağduriyet yaşadığında hakkını doğru yerde arayan,
- İnternetteki doğru veya yalan bilgiyi ayırt edebilen,
- Aldatılması ve aldanması zor olan,
- Fikir ve görüşleriyle yönetime katılan,
- Bilgi ve iletişim kaynaklarını kullanırken eleştirebilen,
- Eleştirirken diğerlerinin hak ve hukukuna saygı gösteren,
- Etik davranan ve çevrimiçi davranışlarının etik sonuçlarını bilen,
- Teknolojiyi kişilere ve sistemlere zarar verecek şekilde kötüye kullanmayan,
- Başkalarıyla iletişim kurarken, işbirliği yaparken doğru ve ahlaki davranışı teşvik eden,
- İnterneti bilinçli ve güvenli kullanan ve bilinçli ve güvenli kullanmayı teşvik eden,
- Yasadığı içerik indirmekten, paylaşmaktan ve saklamaktan kaçınan,
- Başkalarına zorbalık yapmayan, onları taciz etmeyen, kabalıkta bulunmayan,
- Fikir ve sanat eserleri ile telif hakları ve lisanslama konusunda titiz davranan,
- Paylaşmadan önce düşünen ve paylaşması gerekiyorsa paylaşan kişidir.

İnternetin sunduğu fırsatlardan faydalanmak bir haktır ve bu hakkı her birey meşru sınırlar içerisinde özgürce kullanabilir. Bu hak bireylere;

- Bir başkasının kişilik haklarını ihlal etme hakkı vermez,
- Bir başkasına hakaret etme, taciz etme ve zorbalıkta bulunma hakkını vermez,
- Bir başkasının özel hayatının gizliliğini ihlal etme hakkı vermez,
- Bir başkasını dolandırma, aldatma ve mağdur etme hakkı vermez,
- Çocukları istismar etme hakkı vermez
- Başkalarının can ve mal güvenliğini ihlal etme hakkı vermez,
- Millî güvenlik ve kamu düzenini bozacak faaliyetlerde bulunma hakkı vermez,
- Bir başkasını itibarsızlaştırma, onur ve haysiyetini lekeleme hakkı vermez
- Bilgisayar sistemlerine siber saldırıda bulunma ve bunlar bozma hakkı vermez,
- Başkasının sağlığını tehlikeye düşürme hakkı vermez,
- Yalan haberleri, zararlı ve uygunsuz içerikleri yayma hakkı vermez,
- Başkalarının hesaplarını ele geçirme hakkı vermez,

Kısaca, karşı tarafa maddi ve manevi olarak zarar verme hakkını asla vermez. Bu açıdan bireylerin internetteki haklarını ve sorumluluklarını bilmeleri ve internet ortamında

bu bilinçle hareket etmeleri ham mağduriyet yaşamamaları hem de bilerek ya da bilmeyerek başkalarının mağduriyetine sebep olmamaları açısından oldukça önemlidir.

Bu nedenle bireylerin, internetin getirdiği fırsatları ve riskleri azami ölçüde bilmeleri bilinçli, güvenli ve haklarının ve sorumluluklarının farkında olmalarını sağlayacaktır. Bu da toplumda bilinçli internet kullanım kültürünün oluşmasına ve artmasına katı sağlayacaktır.

7. Bölüm Kazanımları

İletişim bireyler için önemli bir haktır. Günümüzde iletişimde en önemli araç internettir. İnternet bireylerin haklarını kullandığı bir özgürlük alanıdır, lakin sonsuz bir özgürlük alanı değildir. Başkalarının haklarının ihlal edildiği noktada bu özgürlük alanı biter ve yapılan işlemle ilgili cezai sorumluluk başlar. İnternet ortamında "Gerçek hayatta suç olan şey, internet ortamında da suçtur" kuralı geçerlidir. Burada işlenen suçlar gerçek hayatta olduğu gibi cezai yaptırıma tabidir. İnternet bireyin başka bir bireye maddi ve manevi olarak zarar verme hakkını asla vermez. Bireylerin internetteki haklarını ve sorumluluklarını bilmeleri ve bu ortamda bu sorumluluk ve bilinçle hareket etmeleri önemlidir. İnternetin getirdiği fırsatları bilmek ve risklerin farkında olmak, bireylerin internetten maksimum fayda sağlamalarına ve zararın da minimum düzeyde kalmasına katkı sunar. Bilinçli internet için hak ve sorumlulukların farkında olmak, sorumlu davranış sergilemek, iyi bir medya okur-yazarı olmak bilinçli internet kullanım kültürünün oluşmasına ve artmasına katkı sağlayacaktır. Bu bölüm sonunda bireyler aşağıdaki kazanımları elde edeceklerdir;

- İnternet ortamındaki hak ve sorumluluklarının farkına varır.
- İnternette hak ve sorumluluklar konusunda uluslararası uygulamalar hakkında bilgi sahibi olur.
- İletişim hakkı ve uluslararası hukuktaki yeri hakkında bilgi sahibi olur.
- İnternette insan hakları ve ilkeleri hakkında bilgi sahibi olur.
- Karşılaştığı olumsuzluklarda nasıl davranması gerektiğini bilir.
- İnternette çocuk hakları hakkında bilgi sahibi olur.
- İnternette unutulma ve lekelenmeme hakkında bilgi edinir.
- İnterneti yoluyla yapabileceği meşru haklarını bilir.
- Bilinçlendirme ve yardım hatları hakkında bilgi sahibi olur.
- 5651 sayılı kanun ve uygulamaları hakkında bilgi sahibi olur.
- İnternetin kötü amaçlı kullanımın yaptırımlara tabi olduğunu bilir.
- Özel hayatı ve kişilik hakkı ihlal edildiğinde hakkını nasıl arayacağını öğrenir.

KAYNAKLAR

YÜKSEK, M. (2006). Avrupa İnsan Hakları Sözleşmesinde İfade Özgürlüğünün Sınırları. 116. TAAD, Yıl:7, Sayı:25.

URL:http://www.taa.gov.tr/indir/avrupa-insan-haklari-sozlesmesinde-ifade-ozgurlugunun-sinirlari-bWFrYWxlfDViNDUyLTkwMjc4LWNlMDIyLWEyODQyLnBkZnw5NTQ, Son Erişim tarihi, 17.07.2018.

ERDOĞAN M. (2001). "Demokratik Toplumda İfade Özgürlüğü: Özgürlükçü Bir Perspektif", Liberal Düşünce, Sayı: 24, Ankara, ss. 8-13.

URL:https://ozgurtoplumundegerleri.com/res/Mustafa_Erdogan_Demokratik_Toplumda_Ifade_Ozgurlugu_Ozgurlukcu_Bir_Perspektif.pdf , Son Erişim tarihi, 16.07.2018.

ARAS Ü. Y. (2010)., İnsan Hakları temelinde özel hayat Hakkının Ulusal ve Uluslararası Alanda Uygulamaları, Yüksek Lisans Tezi.

URL: http://libris.bahcesehir.edu.tr/dosyalar/Tez/083923C1.pdf , Son Erişim tarihi, 16.07.2018.

İnsan Hakları Evrensel Beyannamesi

URL: https://www.unicef.org/turkey/pdf/_gi17.pdf , Son Erişim tarihi, 16.04 2018.

Ersan ŞEN, İnternet Hukuku ve Kişilik Haklarının Korunması

URL: http://web.e-baro.web.tr/uploads/50/dergi/sayi1/12.pdf , Son Erişim tarihi, 16.07.2018.

AİHM: Mahkûmlara internet erişimi engeli hak ihlali,

URL: http://www.bbc.com/turkce/haberler-dunya-38655007, Son Erişim tarihi, 16.07.2018.

FENDOĞLU H. T. (2016). Avrupa İnsan Hakları Mahkemesi Kararlarında İfade Özgürlüğü, TAAD, Yıl:7, Sayı:25, Şubat 2016

URL:http://www.taa.gov.tr/indir/avrupa-insan-haklari-mahkemesi-kararlarinda-ifade-ozgurlugu-bWFrYWxlfGQzZWM2LTk0ZmQ0LTFjYWJjLTNhOTBiLnBkZnw5NTA, Son Erişim tarihi, 16.07.2018.

İnternette İnsan Hakları ve İlkeleri Şartı

URL: https://iprgezgini.org/2016/03/09/internette-insan-haklari-ve-ilkeleri-sarti/, Son Erişim tarihi, 16.07.2018.

Edip Emil ÖYMEN, İnternete erişim insan hakkı mıdır?

URL: https://www.dunya.com/kose-yazisi/internete-erisim-insan-hakki-midir/29094, Son Erişim tarihi, 16.07.2018.

Kullanıcı Hakları Bildirgesi

URL:https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/sunumlar/alternatif_bilisim_kullanici-haklari_bildirgesi.pdf , Son Erişim tarihi, 16.07.2018.

İnternette İnsan Hakları ve İlkeleri Şartı

URL:http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_Booklet_Turkish_final.pdf , Son Erişim tarihi, 16.07.2018.

IGF&UN, Internet Rights & Principles Coalition, İnternette İnsan Hakları ve İlkeleri Şartı,

URL: http://www.resmigazete.gov.tr/eskiler/2015/12/20151203-14.pdf, Son Erişim tarihi, 16.07.2018.

Ümit Arklan, Halkla İlişkiler ve Bilgi Edinme Hakkı, İstanbul, Literatürk Academia, 2009, URL: http://literaturkacademia.com/urun/halkla-iliskiler-ve-bilgi-edinme-hakki/, Son Erişim tarihi, 16.07.2018.

Dilekçe ve Bilgi Edinme Hakkının Kullanılması, Başbakanlık Genelgesi, 2014/12,

URL:http://www.resmigazete.gov.tr/eskiler/2004/01/20040124.htm#4, Son Erişim tarihi, 16.07.2018.

Bilgi Edinme Hakkı Kanunu. (24 Ekim 2003). T.C. Resmi Gazete, 25269

URL:http://www.resmigazete.gov.tr/eskiler/2003/10/20031024.htm#1, Son Erişim tarihi, 16.07.2018.

Kadir Canöz, Kamuda Halkla İlişkilerin Yeni Yüzü: Bilgi Edinme Yasası, Selçuk İletişim Dergisi: 5, Sayı: 3, 2008

URL:http://josc.selcuk.edu.tr/article/download/1075000166/1075000161, Son Erişim tarihi, 16.07.2018.

25 soruda bilgi edinme hakkı, T.C. Başbakanlık Bilgi Edinme Değerlendirme Kurulu,

URL: http://www.bedk.gov.tr/Yayinlar/BEH/BilgiEdinmeHakkiNedir.html, Son Erişim tarihi, 16.07.2018.

Çelik, A. ve Tonta, Y. (1996). Düşünce özgürlüğü, bilgi edinme özgürlüğü ve bilgi hizmetleri.

Bilgi edinme özgürlüğü içinde (ss.1-13). Ankara: Türk Kütüphaneciler Derneği.

URL:http://yunus.hacettepe.edu.tr/~tonta/yayinlar/beozgur.html, Son Erişim tarihi, 16.07.2018.

Bilgi Edinme Hakkı Kanunu. (24 Ekim 2003). T.C. Resmi Gazete, 25269.

URL:http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.5.4982&MevzuatIliski=0, Erişim: 16.07.2018

American Conventıon On Human Rights

URL:https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm, Son Erişim tarihi, 16.07.2018.

Amerikan İnsan Hakları Sözleşmesi

URL:https://burakgemalmaz.files.wordpress.com/2015/05/02.pdf, Son Erişim tarihi, 16.07.2018.

Afrika İnsan ve Halkların Hakları Şartı,

URL:https://burakgemalmaz.files.wordpress.com/2015/05/01-1981-june-27-af-ihhc59f.pdf, Son Erişim tarihi, 16.07.2018.

Afrikalı İnsan ve Halkların Hakları Şartı,

URL:http://www.canaktan.org/hukuk/insan_haklari/yirminci-yuzyilda/afrikali_insan.htm, Son Erişim tarihi, 16.07.2018.

American Conventıon On Human Rights,

URL:http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf, Son Erişim tarihi, 16.07.2018.

İnternet Kullanıcıları İçin İnsan Hakları Rehberi, Tavsiye Kararı CM/Rec(2014)6 ve açıklayıcı memorandum,

URL:https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2017/12/13/coe_guide_hr_internet_users_TR.pdf, Son Erişim tarihi, 16.07.2018.

Avrupa Konseyi Statüsü,

URL: http://uhdigm.adalet.gov.tr/sozlesmeler/coktaraflisoz/ak/turkce/001_tur.pdf, Son Erişim tarihi, 16.07.2018.

AB Konseyi, Guide to Human Rights for Internet Users,

URL: https://rm.coe.int/168008c37f, Son Erişim tarihi, 16.07.2018.

AB Konseyi, İnternet ve daha geniş dijital dünyada hukukun üstünlüğü, Özet ve Avrupa Konseyi İnsan Hakları Komiserinin tavsiyeleri, Tematik Belge,

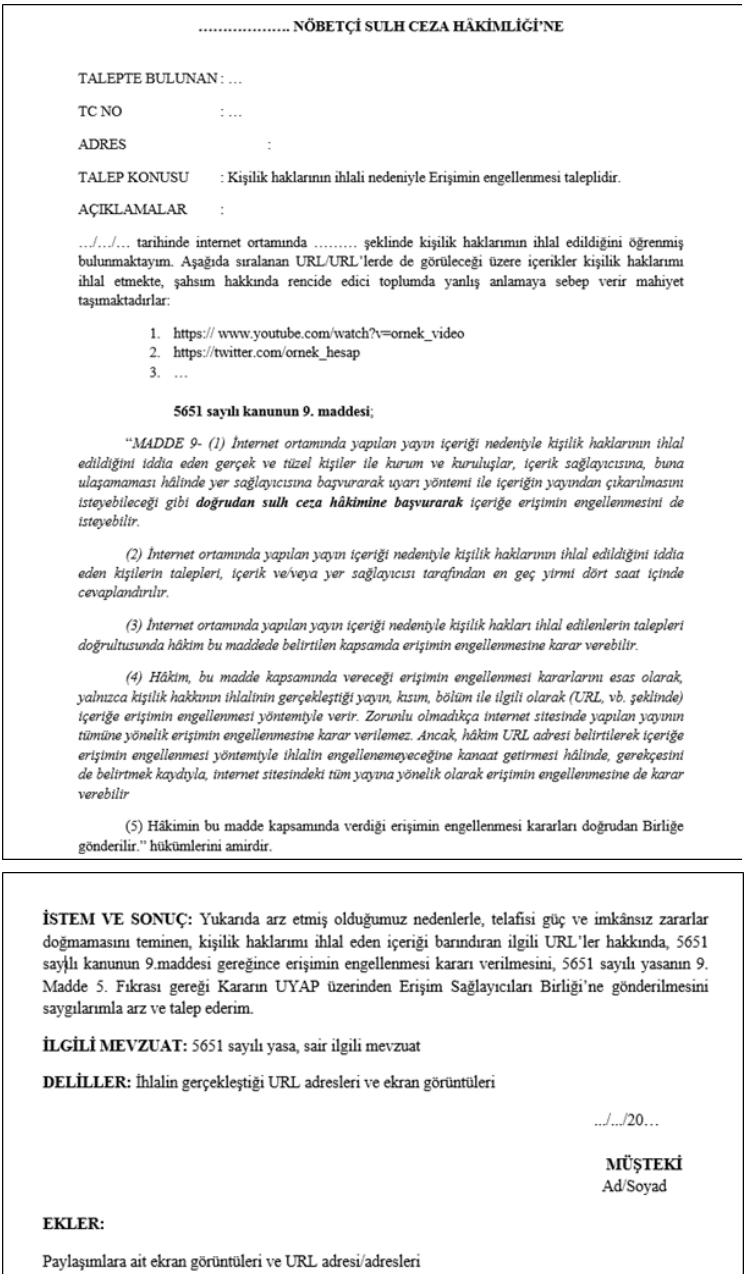
URL: https://rm.coe.int/internet-ve-daha-genis-dijital-dunyada-hukukun-ustunlugu-avrupa-konsey/16806daa33, Son Erişim tarihi, 16.07.2018.

BBC, Internet access is 'a fundamental right',

URL: http://news.bbc.co.uk/2/hi/8548190.stm, Son Erişim tarihi, 16.07.2018.

EKLER

Burada eklerde şekil olarak verilen örnek şablonların Word haline http://internet.btk.gov.tr adresinden erişmek mümkündür. İlgili şablon belge doğrudan bu adresten indirilerek gerekli düzenlemeler yapıldıktan sonra ilgili yerlere başvuru yapılabilir.



…… NÖBETÇİ SULH CEZA HÂKİMLİĞİ'NE

TALEPTE BULUNAN : …

TC NO : …

ADRES :

TALEP KONUSU : Kişilik haklarının ihlali nedeniyle Erişimin engellenmesi taleplidir.

AÇIKLAMALAR :

…/…/… tarihinde internet ortamında …… şeklinde kişilik haklarımın ihlal edildiğini öğrenmiş bulunmaktayım. Aşağıda sıralanan URL/URL'lerde de görüleceği üzere içerikler kişilik haklarımı ihlal etmekte, şahsım hakkında rencide edici toplumda yanlış anlamaya sebep verir mahiyet taşımaktadırlar:

1. https:// www.youtube.com/watch?v=ornek_video
2. https://twitter.com/ornek_hesap
3. …

5651 sayılı kanunun 9. maddesi;

*"MADDE 9- (1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi **doğrudan sulh ceza hâkimine başvurarak** içeriğe erişimin engellenmesini de isteyebilir.*

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir." hükümlerini amirdir.

İSTEM VE SONUÇ: Yukarıda arz etmiş olduğumuz nedenlerle, telafisi güç ve imkânsız zararlar doğmamasını teminen, kişilik haklarımı ihlal eden içeriği barındıran ilgili URL'ler hakkında, 5651 sayÿlı kanunun 9.maddesi gereğince erişimin engellenmesi kararı verilmesini, 5651 sayılı yasanın 9. Madde 5. Fıkrası gereği Kararın UYAP üzerinden Erişim Sağlayıcıları Birliği'ne gönderilmesini saygılarımla arz ve talep ederim.

İLGİLİ MEVZUAT: 5651 sayılı yasa, sair ilgili mevzuat

DELİLLER: İhlalin gerçekleştiği URL adresleri ve ekran görüntüleri

…/…/20…

MÜŞTEKİ
Ad/Soyad

EKLER:

Paylaşımlara ait ekran görüntüleri ve URL adresi/adresleri

Şekil 1: İnternet Ortamında Kişilik Haklarının İhlali Mahkeme başvuru örneği

Sayın Yetkili;

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9. Maddesi 1. Fıkrasına göre" İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına ,buna ulaşamaması halinde yer sağlayıcısına başvurarak uyarı yöntemiyle içeriğin çıkartılmasını isteyebilirler...."

İnternet sitenizde yer alan ve aşağıda URL olarak uzantısı verilmiş bulunan içerikte, kişilik haklarım ihlal edilmiştir. Yukarıda anılan yasa hükmü gereğince içeriğin çıkartılması ile, aynı yasanın 2. Fıkrası gereğince talebime verilecek cevabın 24 saat içerisinde aşağıda bildirmiş olduğum adrese gönderilmesini saygıyla talep ederim...../...../.....

URL ADRESİ:

.....

CEVABIN GÖNDERİLECEĞİ MAİL ADRESİ

(Eğer maille cevap isteniyorsa)

.....

CEVABIN GÖNDERİLECEĞİ FİZİKİ ADRES

(Eğer ev-işyeri adresi verilmek isteniyorsa)

Ad-Soyad

TC No

Adres

Şekil 2: İnternet Ortamında Kişilik Haklarının İhlali İçerik sağlayıcı başvuru örneği

..... NÖBETÇİ SULH CEZA HÂKİMLİĞİ'NE

TALEPTE BULUNAN : ...

TC NO : ...

ADRES :

TALEP KONUSU : Özel Hayatın Gizliliğinin ihlali nedeniyle Erişimin engellenmesi/ içeriğin çıkarılması taleplidir.

AÇIKLAMALAR :

.../.../... tarihinde internet ortamında ..... şeklinde özel hayatımın ihlal edildiğini öğrenmiş bulunmaktayım. Aşağıda sıralanan URL/URL'lerde de görüleceği üzere içerikler özel hayatımı ihlal etmekte, bu sebeple ağır mağduriyet yaşamaktayım.

1. https:// www.youtube.com/watch?v=ornek_video
2. https://twitter.com/ornek_hesap
3. ...
4. ...

5651 Sayılı yasanın 9/A maddesi "özel hayatın gizliliği Nedeniyle içeriğe Erişimin Engellenmesi" başlığı altında:

"MADDE 9/A- (Ek: 6/2/2014-6518/94 md.)

(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. (1)

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. (1)

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar. (1)

(6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. (1)

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. **(Mülga cümle: 26/2/2014-6527/18 md.)** (1)

(9) **(Ek: 26/2/2014-6527/18 md.)** Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, (...) (1) yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar." Şeklinde olup, iş bu başvuru doğrudan hâkimliğinize yapılmıştır.

İSTEM VE SONUÇ: Yukarıda arz etmiş olduğumuz nedenlerle, telafisi güç ve imkânsız zararlar doğmamasını teminen, özel hayatımı ihlal eden içeriği barındıran ilgili URL/URL'ler hakkında, erişimin engellenmesi kararı verilmesini, 5651 sayılı yasanın 9/A Madde 5.Fıkrası gereği Kararın Bilgi Teknolojileri ve İletişim Kurumu'na gönderilmesini saygılarımla arz ve talep ederim.

İLGİLİ MEVZUAT: 5651 sayılı yasa, sair ilgili mevzuat

DELİLLER: İhlalin gerçekleştiği URL adresleri ve ekran görüntüleri

../.../20..

MÜŞTEKİ
Ad/Soyad

EKLER:

Paylaşımlara ait ekran görüntüleri ve URL adresi/adresleri

Şekil 3: İnternet Ortamında Özel Hayatın Gizliliğinin İhlali Mahkeme Başvuru Örneği

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU'NA

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla işlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A maddesi:

"(1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. (1)

(2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi (URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz.

(3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. (1)

(4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır.

(5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar. (1)

(6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. (1)

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

....." Şeklinde olup, Aşağıda belirttiğim URL adresi/adreslerinde özel hayatımın gizliliğine ilişkin ihlal gerçekleşmektedir. İhale konu içeriklerde şahsımın özel hayatına ait ..... şeklinde yayın yapılmaktadır.

Kurumumuza başvuru yaptıktan sonra 24 saat içerisinde Hâkimliğe Başvuracağım.

Kurumunuz tarafından gerekli incelemenin yapılarak erişimin engellenmesi talebinin uygulanması için Erişim sağlayıcıları Birliği'ne gönderilmesini saygı ile talep ederim.

URL Adresleri: .....

Adres:

Ad-Soyad
TC Kimlik No

EK: Nüfus Cüzdanı örneği

Şekil 4: İnternet Ortamında Özel Hayatın Gizliliğinin İhlali Kurum Başvuru Örneği

BÖLÜM 4 İNTERNET VE SAĞLIK

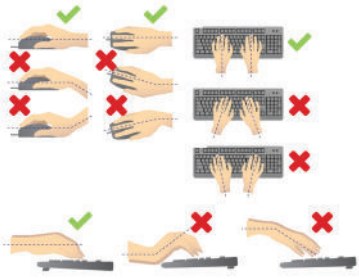
İçindekiler

1. Fiziksel Sağlık Sorunları

Günümüzde hayatın bir parçası haline gelen internete sadece bilgisayarlardan değil cep telefonlarından ve tabletlerden de erişilebilmektedir. İstenilen her yerde ve her zaman ulaşabilme kolaylığı internet başında geçirilen sürenin artmasına neden olmaktadır. Özellikle çocuk ve gençler bu kadar kolay erişebildikleri internet karşısında zaman sınırlandırması yapmakta zorlanmaktadır. Uzun süreler ekran başında vakit geçirmek kas iskelet sistemi hastalıkları, göz sorunları, uyku bozuklukları, obezite ve baş ağrısı gibi pek çok sağlık sorununa neden olmaktadır.

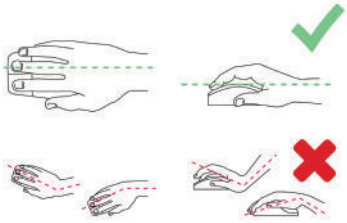
(resimler yeniden çiziliyor)

1.1 Kas iskelet sistemi hastalıkları



Kas iskelet sistemi hastalıkları uzun süreli bilgisayar kullanımı sonucunda en sık rastlanılan fiziksel sağlık sorunlarının başında gelmektedir. Ekran karşısında geçirilen sürenin artması, el bileği, dirsek, omuz, boyun ve sırtın yanlış pozisyonda tutulması, yanlış oturma pozisyonu, mouse ve klavye kullanırken sık tekrarlanan hareketler, uzun süre hareketsiz oturma ve kullanılan cihazların çocukların kullanımı için uygun olmaması gibi sebeplere bağlı olarak ortaya çıkabilmektedir. Bu hastalıklar arasında;

- Boyunda kas ağrısı ve kasılmalar (gergin boyun sendromu)
- Boyun fıtığı

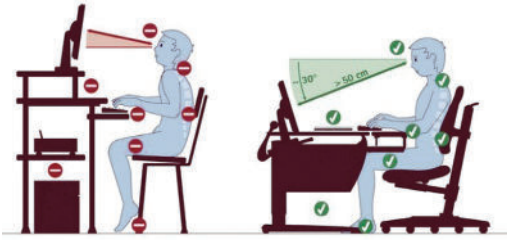


- El bileğinde sinir sıkışması (karpal tünel sendromu),
- El ve bilek çevresinde ağrı (tendinit),
- Başparmak ve el bileğinde tendon iltihaplanması,
- Omuz ve dirsekte tendon iltihaplanması,
- Sırt ve kürek kemiği çevresindeki kas gruplarında ağrı (miyofasiyel ağrı sendromu),
- Duruş problemleri(omurgada eğrilik ve kamburluk),
- Hareket yetersizliğiyle ilişkili olarak kemik gelişiminin olumsuz etkilenmesi sayılabilir.

Yukarıda sayılan rahatsızlıklar yaşam kalitesini düşüren ve tedavide gecikilmesi durumunda önemli sonuçlar doğuran ağrılı süreçlerdir. Belirtileri arasında; kol ve parmaklarda uyuşma ve karıncalanma hissi, bilek, boyun, omuz, sırt ya da belde ağrı ve hareket kısıtlılığı sıklıkla görülmektedir.

Bu rahatsızlıkların önlenmesi için dikkat edilmesi gerekenler şu şekilde sayılabilir;

- Otururken vücut doğru pozisyonda olmalıdır.
- Sandalye, masa ve bilgisayar malzemelerinin ergonomisi vücudunuza uygun olmalıdır.



- Mouse tutarken ve klavye kullanırken eller ve bilek doğru pozisyonda tutulmalıdır.
- Uzun süreli hareketsiz oturmak yerine egzersiz ve dinlenme süreleri belirlenmelidir.

1.2. Göz sorunları (ekrana bakma sendromu)

Bilgisayar kullanırken gözler pek çok sebebe bağlı olarak olumsuz etkilenebilir. Ekranın parlaklığı/özelliği, ekrana olan mesafe, ortamın aydınlığı, daha önceden kişide var olan kırma kusuru için gözlük kullanılıp kullanılmaması bu etmenler arasında sayılabilir.

Ekrana bakma sendromu, belirli bir noktaya uzun süre bakma sonucunda oluşan ve gözlerde yanma, kızarma, kaşınma, göz kuruluğu, bulanık görme ve baş ağrısı gibi şikâyetlerle seyreden bir göz sorunudur. Gün içerisinde farklı yönlere ve uzaklıklara bakıldığında gözün hareket etmesini sağlayan 6 farklı kasın da çalışması sağlandığından göz yorulmaz. Ancak uzun süre sabit bir noktaya bakmak gözü yorar.

Her gün yaklaşık olarak 2 saatini ekran karşısında geçiren bir kişi ekrana bakma sendromu açısından risk altındadır. Günde 6 saatten fazla ekran karşısında zaman geçirenlerin %75'inde gözlerde yorgunluk, yanma, batma, kızarma, baş ağrısı gibi göz problemlerinden kaynaklı sorunlar yaşanmaktadır.

Ekrana uzun süre ve dikkatle bakarken göz kırpma sayısı da azalır. Normal bir durumda dakikada 12-16 kez göz kırpılırken, ekran karşısında bu sayı 5-6 defaya kadar düşebilir. Bu durum da yine göz kuruluğuna neden olmaktadır.

Göz sağlığını korumak için dikkat edilmesi gerekenleri şu şekilde sıralayabiliriz;

- Ekran karşısında daha fazla gözleri kırpmaya çalışmalı ve belli aralıklarla gözler dinlendirilmelidir,
- Bilgisayar ekranının yüksekliği göz seviyesini aşmayacak şekilde ayarlanmalı ve gözlerden 35-40 cm uzaklıkta olmalıdır,
- Ortam sık sık havalandırılmalıdır,
- Çok aydınlık ya da çok karanlık ortamlarda bilgisayarla çalışılmamalıdır,
- Monitörün parlaklık ve çözünürlük seviyeleri gözü yormayacak şekilde ayarlanmalıdır.

1.3. Yeme problemleri ve obezite

Günümüzde obezite, özellikle ergen ve gençler arasında hızla artmaktadır. Hipertansiyon, diyabet, insülin direnci (hiperinsülinemi), koroner kalp hastalığı, bazı kanser türleri, uyku apnesi gibi pek çok hastalıkla ilişkilendirilen ve yaşam kalitesini olumsuz etkileyen obezitenin en önemli risk faktörleri arasında fiziksel aktivite azlığı ve düzensiz beslenme ilk sırayı almaktadır. Vücuda alınan enerjinin harcanan enerjiden fazla olması ile ortaya çıkan obezitenin önüne geçmek için mümkün olduğunca sağlıklı beslenmeli ve günlük hayatta fiziksel aktivite oranı artırılmalıdır.

Televizyon, bilgisayar ya da tablet karşısında fazla zaman geçirmek, uzun süre hareketsiz kalmak anlamına gelmektedir. Bu da obezite riskini artırmaktadır. Uzun süreli ekran karşısında oturmak bazı insanlarda sürekli bir şeyler atıştırmak ihtiyacı hissettirirken bazılarında da yemeyi unutturabilmektedir. Sürekli bir şeyler atıştırmak obezite riskini artırırken yemenin unutulması da kilo kaybına neden olabilmektedir.

Yapılan araştırmalar da, ekran karşısında vakit geçirme süresi arttıkça obezite görülme sıklığında da anlamlı düzeyde bir artış olduğu görülmektedir.

1.4 Uykusuzluk problemi

Uyku, zihinsel ve fiziksel performansı her gün yenileyerek canlı tutabilmek ve beden sağlığını koruyabilmek için önemli olan aktif bir süreçtir. Genetik olarak kodlanmış uyku süresi kişiden kişiye ve yaşa göre değişkenlik göstermekle birlikte ortalama 7-11 saat arasında seyredebilmektedir.

İnternet, sosyal ağlar, online oyunlar ve cep telefonu gibi uyaranlarla zaman geçirmek uykuya geçiş süresini uzatabilir. Yapılan çalışmalarda, odasında bilgisayar, tablet cep telefonu, televizyon gibi teknolojik cihazlar bulunan çocuk ve gençlerin daha fazla uyku problemi yaşadığı saptanmıştır.

Uyku düzeninde bozulma, yaşam aktivitelerini olumsuz etkilerken çeşitli hastalıklara da sebebiyet verebilir. Yetersiz uyku; fiziksel ve bilişsel yorgunluk, sinirlilik, dikkatsizlik, unutkanlık, baş ağrısı gibi durumlara yol açar. Çocuklarda davranış problemlerine neden olabilir. Uzun süreli uykusuzluğun, bağışıklık sistemini bozduğu, hipertansiyon, kanser, diyabet, kalp-damar hastalıkları ile bilinç bozukluklarına yol açtığı bilinmektedir.

İyi bir uyku düzenine sahip olmak için; yatmadan 1 saat önce bilgisayar, cep telefonu, televizyon gibi uyaranlardan uzak durmak,

yoğun hareketli faaliyetlerden, kafeinli ve bol kalorili içecek ve yiyeceklerden kaçınmak ve aynı saatte yatıp aynı saatte uyanmak gerekmektedir.

1.5. Elektromanyetik kirlilik ve sağlığa etkileri

Elektromanyetik kirlilik; yüksek gerilim hatları, baz istasyonları, evlerde ve ofislerde kullandığımız her türlü elektrikle çalışan araçlar, akım taşıyan kablolar, saç kurutma makinesi, televizyon, bilgisayar, cep telefonu ve benzeri cihazların oluşturduğu elektromanyetik alanların kontrolsüz kullanımı sonucunda meydana gelmektedir. Şehirleşme ile elektromanyetik kirlilik arasında doğrusal bir orantı mevcuttur.

Kablosuz ağların yaydığı radyo frekans, radyasyon ve çok düşük frekanslı manyetik alanlar, yasal güvenlik sınırlarında olmalarına rağmen Dünya Sağlık Örgütü tarafından muhtemel kanserojen etkileri olabileceği değerlendirilen maddelerin sınıflandırıldığı 2B grubuna alınmıştır.

Elektromanyetik alanlarla uzun süreli etkileşim kısa vadede stres, baş ağrısı, yorgunluk, sersemlik gibi sorunlara neden olurken; uzun vadede beyin ve sinir sistemlerinde tümörlere, hafıza sorunlarına ve kalıcı işitme kayıpları gibi ciddi sorunlara neden olabilmektedir. Son dönemlerde yapılan çalışmalar, elektromanyetik alan etkileşimi ile özellikle kanser, üreme sağlığı, sinir dokusu bozulması ile seyreden hastalıklar ve kalp hastalılarını ilişkilendirmektedir.

Çocuklar yetişkinlere oranla daha fazla risk altındadır. Yapılan çalışmalar 5-10 yaşlarındaki çocukların beyinlerinin yetişkinlere göre mikrodalgaları daha fazla soğurduğunu ve ışınların ise çocuk beyninde daha derinlere ulaşabildiğini saptamıştır. Bu durum özellikle çocukları daha fazla korumak gerektiği sonucunu ortaya koymaktadır.

Elektromanyetik alanlara maruziyeti en aza indirmek için;

- Evde ya da ofiste elektrikli cihazlar çalışırken yakınında bulunmamak,
- Kullanılmayan elektrikli aletleri ya kapatmak ya da fişini çekmek,
- Yatak odalarında televizyon, radyo, cep telefonu, bilgisayar gibi cihazları bulundurmamak,
- Cep telefonlarını kısa sürelerle ve mümkünse kulaklık takarak kullanmak ve özellikle kalp üstü, bel ve göğüs hizasında taşımamak,
- Evlerde mümkün olduğunca kablosuz ağları kullanmamak ya da gerekmediğinde kapatmak,
- Diz üstü bilgisayarları kullanırken vücudumuzdan uzakta tutmak,
- Uzun süreli bilgisayar kullanmamaya dikkat etmek gerekmektedir.

2. İnternetin Psikolojik Etkileri

İnternetin aşırı ve yanlış kullanımının psikolojik sağlık üzerinde bir takım etkileri mevcuttur. Bunlardan bazıları;

- Anksiyete (kaygı) bozukluğu
- Depresyon
- İntihar düşünceleri
- Dürtüsel internet kullanımı
- Hiperaktivite - Dikkat eksikliği bozukluğu

Kaygı hayatın bir parçasıdır. Herkes günlük yaşamında çeşitli sebeplere bağlı olarak kaygı duyabilir. Sağlık, aile vb. konular ile ilgili sorunlar gibi birçok konu insanı kaygılandırabilir. Bu tarz kaygılar baş edilebilir düzeydedir. Anksiyete bozukluğu olan kişiler ise sürekli ve aşırı bir endişe durumu içinde olmaktadırlar. Anksiyete durumu günlük yaşamlarının olumsuz etkilenmesine ve günlük etkinliklerini sürdürmelerine engel olmaktadır. Kişilerde meydana gelen anksiyete (kaygı) bozukluğu, öfke ve şiddet davranışı sergilemelerine de yol açabilmektedir. Bunun bir sebebi de şiddet içerikli siteler olabilmektedir. Şiddeti elde edilen bir başarı gibi yansıtan oyunlar, kişileri bu tarz davranışlara daha çok itebilmektedir. Bireylerin iç dünyasında bastırdığı duygular, şiddet içerikli sitelerin veya oyunların varlığı ile su yüzüne çıkabilir ve kişilerin yaşamlarına yansıyabilir.

Bireyler internet ve sosyal paylaşım siteleri aracılığıyla belli gruplar içinde yer almakta ve farklı insanlarla iletişim kurabilmektedirler. İnternet, günlük hayatta iletişim problemi yaşayan insanlara kolaylık sağlamaktadır. Bir yandan da bireylerin sosyal fobi geliştirerek, kendilerini sosyal ortamdan geri çekmelerine ve sosyal ortama girdiklerinde kendilerini nasıl ifade edeceklerini bilemeyip kaygı yaşamalarına sebep olabilmektedir. İnternet başında geçirilen zamanın artması ile bireyler sosyal çevresi ile olan etkileşimini azaltarak kendilerini toplumdan soyutlayabilmektedir. Bu durum, kişiler arası iletişimlerinin zayıflamasına, kendilerini yalnız hissetmelerine, içe kapanmalarına, depresyon, çöküntü ve yalnızlık duyguları yaşamalarına sebep olacaktır. İnsanlarla kurduğu iletişimi sürekli olarak internet ortamından sağlayan birey gitgide yalnızlaşacak ve kendini sürekli bir endişe haline sürükleyecektir. Ayrıca, internetin sağladığı kolay ulaşılabilirlik ve bazı özendirici içeriklerin varlığının, gerçeği kavrama yetisi yetersiz olan bireyleri farklı davranış ve düşüncelere itebileceği, hatta intihar düşüncelerine dahi sürükleyebileceği düşünülmektedir.

İnternet bağımlılığı; depresyon, öfke ve özgüven eksikliğinden kaynaklı da ortaya çıkabilmektedir. Sosyal becerileri konusunda kendisini yetersiz hisseden, fiziksel görünüşünden rahatsız olan, kişiler arası ilişkilerde kendine güvenmeyen bireyler sanal ortamda kendilerini daha rahat hissedebilmekte ve sanal ilişkileri, gerçek ilişkilere tercih edebilmektedirler. Sürekli bu ihtiyaçlarını sanal ortamdan gideren bireyler zamanla internet ortamına daha da sıkı bağlanarak bir bağımlılık geliştirebilmektedirler. Ayrıca, yapılan bir araştırmada, Dikkat eksikliği, hiperaktivite bozukluğu, depresyon ve sosyal fobi semptomları olan bireylerin, internet bağımlılığına daha yatkın oldukları

tespit edilmiştir. DEHB tanısına sahip bireyler, kolay sıkılan bir yapıya sahiptirler ve yaptıkları iş sonrası hemen haz alma duygusu ile hareket etmektedirler. Herhangi bir iş üzerinde uzun süre odaklanmakta sıkıntı yaşarlar, sonuca çabuk ulaşmak isterler ve hızlı hareket ederler. Bu özelliklerinden dolayı DEHB tanısı almış bireyler internetin hızı ve uyarıcı etkisinden dolayı kolaylıkla bağımlılık geliştirebilmektedirler. Yine yapılan bir araştırmaya göre, internet bağımlılığının beynin duygu işleme, karar verme, dikkat ve dürtü kontrolünden sorumlu bölgesinde yapısal ve işlevsel değişimlere yol açtığı da bulunmuştur.

2.1 Sağlıksız internet kullanımının insan hayatına etkileri

İnterneti sağlıklı kullanmada başarı sağlayan bireyler internetin sunduğu birçok fırsattan faydalanabilirken bazı bireyler ise patolojik internet kullanımı göstermiş oldukları için bazı problemlerle karşılaşabilmektedirler.

Bağımlılık, bireyin bağımlı olduğu şeye ulaşamaması ve ulaşamaması halinde yoksunluk hissetmesi ve ihtiyaç duyma halinin giderek artması durumudur. Madde veya alkol gibi bağımlılıklar ile birlikte, kumar ve teknoloji bağımlılığında da yakın semptomlar ile karşılaşılabilmektedir.

İnternet bağımlısı olan bireylerin bağımlı olmayan bireylere oranla daha çok takıntı, depresyon gibi psikiyatrik ve psikososyal sorunlarla karşı karşıya kaldığı görülmektedir. İnternet başında geçirilen uzun sürelerin ve bireylerin gerçek hayatta kurdukları iletişimden çok internet ortamında kurdukları sanal ilişkiler üzerine yoğunlaşması durumuyla bireyler gerçek hayatta yalnızlaşabilmektedirler. Bu durum bireylerin aile, okul, iş ve sosyal çevrelerinde birçok sorunla karşılaşmalarına neden olmaktadır. Ayrıca, depresyon, yalnızlık ve kaygı bozukluğu gibi sıkıntılar da meydana getirebilmektedir.

2.2 Kişilik özelliklerinin problemli internet kullanımı üzerindeki rolü

Kişilik özelliklerinin bireylerin mutluluğu ve yaşamsal alandaki memnuniyet duyguları ile yakından ilişkili olduğu düşünülmektedir. Yapılan çalışmalar sonucu, kişilik özelliklerinin problemli internet kullanımına etki ettiği ve bu etkiyle de bireylerin yaşamsal memnuniyetlerinin azaldığı görülmüştür. Problemli internet kullanımının belirleyicisi olarak; duygusal tutarsızlık, dışa dönüklük, yalan söyleme gibi kişilik boyutları etkili görülmüştür. Duygusal tutarsızlık yaşayan bireyler interneti hem eğlence hem de iletişim amaçlı kullanmakta, dışa dönük bireylerin ise interneti iletişim amaçlı kullanmakta oldukları, sosyal iletişim kurma amacıyla internete daha az gereksinim duydukları belirlenmiştir. Bazı

bireylerin, internet ortamında kimliklerini gizleyebilme şansları olması bakımından kendilerini ifade etmelerinin gerçek hayata kıyasla daha kolay olduğu ve daha rahat sosyalleşebildiği gerekçesiyle interneti tercih ettikleri görülmektedir. Ayrıca, sosyal çevrelerinde çekingen olan bireylerin problemli internet kullanımına daha yatkın oldukları da araştırmalarda elde edilen bulgular arasındadır.

2.3. Sağlıklı internet kullanımı

İnternet, bilinçli ve güvenli kullanıldığı takdirde bireylere birçok fırsat tanımaktadır. İnternetin bilinçli ve sağlıklı kullanılması için de birtakım konulara dikkat etmek gerekmektedir. İnternetin bireyler adına psikolojik bir tehdit haline gelmemesi için gerçek hayatta kurulan iletişimle internette kurulan iletişimin ayırt edilmesi gerekmektedir. Bilişsel ve davranışsal bir rahatsızlık olmaksızın uygun bir zaman içerisinde belli bir amaç için kullanılması önemlidir fakat internetin, amaç ne olursa olsun kimlik kaynağı olarak kullanılmaması da önemli bir konudur. İnternet ile ilgili bilişler depresyon, yalnızlık gibi sorunların nedeni değil bu psikososyal sorunların bir sonucudur.

3. İnternet Bağımlılığı

İnternetin çok fazla kullanılması internet bağımlılığı, bilgisayar bağımlılığı, ya da patolojik internet kullanımı terimleriyle ifade edilirken, alan içinde yapılan akademik araştırmaların artmasıyla beraber problemli internet kullanımı tanımlaması da kullanılmaya başlanmıştır.

3.1. İnternet bağımlılığının gelişmesi

Günümüzde internet kullanımı, toplumsal ve bireysel yaşamın en önemli iletişim yollarından birisidir. İnternet bağımlılığının tanım ve tanı kriterleri konusunda henüz bir uzlaşmışlık yoktur. 1990'lı yıllarda literatüre girmeye başlamıştır. İnternet, insanların birçok ihtiyacını karşılarken bir yandan da bazı özellikleri sebebiyle olumsuz olarak adlandırabileceğimiz bir bağımlılığın oluşmasına sebep olabilmektedir. İnternet kullanım süresinin son zamanlarda artması ve bireyden bireye farklılık gösteren internet kullanım alışkanlıklarının insanlar üzerinde ne gibi etkilere sebep olduğu da çeşitli araştırmalarla sorgulanmıştır. Araştırmalar sonucunda; bazı bireylerin internet kullanımında kendilerini sınırlayabildikleri, bazı bireylerin ise kendilerine herhangi bir sınırlama getiremedikleri için okul, iş, sosyal hayatlarında birtakım problemlerle karşılaştıkları bilgisi elde edilmiştir.

İlk kez psikiyatrist Ivan Goldberg tarafından kullanılan bir terim olan "internet bağımlılığı" kişisel yaşamda bireylerin aşırı internet kullanımının olumsuz etkilerini tanımlamak için tasarlanmıştır.

İnternet bağımlılığı hakkında yapılan araştırmalara göre tanımlanmış bazı belirtiler aşağıdaki gibidir;

- Tolerans belirtileri: Sürekli bir şekilde artan çevrimiçi zaman geçirme ihtiyacı,
- Geri çekilme belirtileri: (Withdrawal Syndrome): İnternet kullanımının so-

nuçlarını endişe içinde karşılama, internet hakkında takıntılı düşüncelere kapılmak,

- Planlanan zamandan daha fazla süre internette kalmak,
- İnternet kullanımını azaltmak için sürekli bir istek duymak,
- İnternette yapılan faaliyetlere fazla zaman harcamak,
- İnternet yüzünden sosyal ve mesleki faaliyetleri beklemeye almak veya bırakmak.
- İnternet kullanımına bağlı fiziksel veya psikososyal problemler yaşanmasına rağmen interneti aşırı kullanmaya devam etmek.

Tartışmalara sebep olan "İnternet bağımlılığı" terimi ilk kez Kimberly S.Young tarafından Amerikan Psikoloji Derneği'nin 1996'da gerçekleştirilen yıllık toplantısında tanımlanmıştır.

Young, internet bağımlılığı tanımını yaparken "patolojik kumar oynama" kriterlerini temel almıştır. Amerikan Psikiyatri Birliği'nin 1994 yılında yayınlanmış olan, DSM IV (Diagnostic and Statistical Manual of Mental Disorders) Mental Bozuklukların Tanımsal ve Sayısal El Kitabı listesinden yararlanmıştır. 8 maddeden 5 tanesinin yaşanması halinde kişi bağımlı olarak tanımlanabilmektedir.

Bu kriterler aşağıdaki gibidir:

1. İnternet ile ilgili aşırı zihinsel uğraş,
2. İnternette geçirilen zamanda artışa ihtiyaç duyma,
3. İnternet kullanımını azaltmaya veya bırakmaya yönelik başarısız girişimlerde bulunma,
4. İnternet kullanımının azaltılması durumunda yoksunluk belirtileri (huzursuzluk, öfke vb.),
5. Günlük aktiviteleri planlama ile ilgili sorunlar,
6. Aşırı internet kullanımı sebebiyle okul, iş ve sosyal çevre ile ilgili problemler,
7. İnternette kalma süresi ile ilgili aileye, arkadaşa veya terapiste yalan söylemek, dürüst olmayan davranışlar sergilemek,
8. İnternete bağlı olduğu süre içerisinde duygulanımda değişikliğin olması, internetin olumsuz duygulardan (huzursuzluk, suçluluk, kaygı) kaçmak için kullanılması.

İnternet kullanımında işle ilgili olmayan ve 6 aylık periyotta, yukarıda belirtilen 8 maddeden, 5 veya daha fazlasına "evet" cevabı veren kişiler "bağımlı" olarak nitelendirilmektedir.

3.2 İnternet bağımlılığının alt yapıları

İnternet bağımlılığının birçok davranışı kapsamasından yola çıkarak Young, internet bağımlılığını beş alt yapıya ayırmıştır.

1. Siber-cinsel bağımlılık: Genellikle bireyler cinsel içerikli sitelerde gezinme, pornografik içerikli videoları izleme veya indirme gibi davranışlar gösterirler.

2. Siber-ilişki bağımlılık: Bu tarz bağımlılığa sahip bireyler, internet üzerinde kendilerine farklı bir kişilik oluşturup, interneti çevrimiçi arkadaşlıklar kurmak için kullanırlar. Kendilerine sanal bir dünya yaratırlar.

3. Net bağımlılığı: İnternet aracılığıyla yapılan çevrimiçi alışveriş, kumar vb. davranışlar olarak belirtilebilir.

4. Bilgi aşırı yüklemesi: Birey, bilgi araştırma amacıyla kullandığı internette aşırı ve gereksiz derecede vakit geçirebilir, uzun süre internete bağlı kalabilir.

5. Bilgisayar bağımlılığı: İnternet bağımlısı birey, çevrimiçi veya çevrimiçi olmayan oyunlara bağımlı olabilmektedir.

Bağımlı olan bireylerde, internete giremediklerinde madde bağımlılarında gözlemlenen sinirlilik ve huzursuzluk gibi belirtilerin görüldüğü de yapılan çalışmalarla belirlenmiştir.

3.3. Giderek artan internet kullanımı bağımlılık olarak değerlendirilebilir mi?

İnternet bağımlılığının DSM-V el kitabı içine dâhil edilmemesi (DSM-V), genel anlamda "altta yatan bozukluklara ait "yeni bir ortama uyum sağlayan psikososyal problemler" olarak değerlendirildiğini göstermektedir. DSM, Amerikan Psikiyatri Birliği tarafından hazırlanmaktadır ve Ruhsal Bozuklukların Tanısal ve İstatiksel El Kitabıdır. (Diagnostic and Statistical Manual of Mental Disorders).

Ruhsal Bozuklukların Tanısal ve İstatiksel El Kitabı dördüncü baskısı içerisinde psikolog ve psikiyatristlerin çalışmalarında internete olan düşkünlüğün (addiction) "problematik bir davranış" olarak değerlendirilmemesi sebebiyle Young, yaptığı çalışmayı 'patolojik kumar oynama' davranışı üzerine kurmuştur. Bu çalışmanın internetin henüz ilk aşamalarında olduğu bir dönemde gerçekleştirilmesi ve araştırmanın yapıldığı tarihte internet kullanıcı sayısının ABD'de 56 milyon olması, bugün bu orana bakıldığında ise sayının 290 milyona yakın olduğu yapılan araştırmalarda elde edilen bulgulardır.

İnternet Bağımlılığının Gelişmesinde Psikolojik Kaynaklı Nedenler

- Bireyin dürtülerini kontrol etmekte güçlük çekmesi,
- İçe kapanıklık,
- Toplum tarafından beğenilmeme korkusu,
- Karamsar düşünce yapısı,
- Özgüven eksikliği,
- Hayata karşı olumsuz bakış açısı,
- Bireyin sosyal ilişki kurmada güçlük çekmesi,

- Bireyin kendini yeteri kadar tanıması,
- Bireyin dışlanma korkusu yaşaması ve çevreden gelen her isteği kabul etmesi,
- Gerçek hayatta elde edemediği başarıyı sanal ortamda elde etmeye çalışması gibi nedenler internet bağımlılığının gelişmesinde büyük rol oynamaktadır.

4. İnternet Bağımlılığı ve Çocuklar

Çocukların internet kullanımı ve günlük hayatta yapmış oldukları diğer etkinlikler arasında sağlıklı, iyi bir denge kurabilmelerine yardımcı olabilmek önemli ve dikkat edilmesi gereken bir konudur.

4.1. Çocuklar ve gençlerin internet bağımlısı olmasında etkileyici faktörler nelerdir?

- Sosyal destek eksikliği
- Aile içi problemler
- Özgüven eksikliği
- Yalnızlık duygusu
- İçe ve dışa dönüklük

İnternet bağımlılığı konusunda yapılan araştırmalarda, bağımlılığı etkileyen serotonin ve dopaminden yetersiz sayıda bulunabileceği de ileri sürülmüştür. Serotonin, insanda mutluluk, canlılık ve zindelik hissi verir ve eksikliği sıkılgan, depresif, yorgun bir ruh haline sebep olmaktadır. Dopamin ise, keyifli ve hayata daha bağlı yaşamayı sağlamaktadır. Aşırı internet kullanımının bireylerin psikolojik durumunu değiştirdiği ve aşırı mutluluk hissi oluşturmasına yardımcı olduğu belirlenmiştir.

Yalnızlık ve yetersizlik duygusu taşıyan, sosyal ortamda kendini rahat ifade edemeyen, fiziksel görünüşünden rahatsız ve özgüven eksikliği olan gençlerin de internet başında daha fazla zaman harcadıkları ve kişilerle iletişimlerini internet ortamından sağlamalarının da bağımlılık geliştirmelerinde büyük etken olduğu araştırmalarla belirtilmiştir. Ailesi ile iletişimi kötü olan gençler de internet ve sosyal paylaşım sitelerinde daha çok zaman geçirmektedirler.

Ayrıca, sosyal fobi, depresyon, hiperaktivite bozukluğu ile ailede bağımlılığa karşı yatkınlık söz konusu ise çocuk ve gençlerin bağımlılık geliştirmeye daha yatkın oldukları yapılan çalışmalarca belirlenmiştir.

Çocukların ve gençlerin internet kullanımına yönelik bağımlılık geliştirmemeleri ve interneti kullanırken sergiledikleri tutumlarını tespit etmek ve ebeveynlerin çocuklarının internet kullanımına yönelik bilinç düzeylerinin arttırılmasını sağlamak için aşağıdaki sorulara dikkat etmek gerekmektedir;

- Çocuklar gün içerisinde ne kadar süreyi internet başında geçirmektedir?
- Çocukların internete erişim araçları nelerdir?
- Çocukların internette tercih etmiş oldukları içerikler nelerdir?
- Çocuklarının internet kullanımı ebeveynler tarafından denetliyor mu?

- Ebeveynlerin çocukların internet kullanımına yönelik aldığı önlemler nelerdir?
- İnternetin çocuklar üzerindeki etkileri nelerdir?

4.2. Çocuklar ve gençlerde internet bağımlılığı belirtileri

İnternet kullanımı günlük hayatı etkileyecek duruma gelmiş ve kişinin sorumluluklarını yerine getirmesinde engel oluşturmaya başlamış ise bağımlılıktan söz edilebilir. İnternet bağımlılığı belirtileri kişiden kişiye göre değişiklik gösterebilmektedir. İnternet kullanımı konusunda kişi fazla vakit geçirdiğini kabul etmiyor ve inkâr ediyorsa, aile ve arkadaş ortamından kendini soyutlar duruma gelmişse, internet başında geçirdiği vakti kontrol edemiyorsa ve günlük işlerini yerine getirememesi gibi bir durum söz konusu ise kişide internet bağımlılığının belirtilerinden söz edilebilir.

4.3. İnternette gerçek dünyayla uyuşmayan karakterlerin çocukların psikolojisi üzerindeki etkisi

İnternet'te yer alan gerçekten uzak karakterler ve olaylar çocuklar için bir rol model olarak sunulmaktadır. Bu karakterlerin ve olayların çocuklarda ve gençlerde yarattığı cazibe onları daha da çekmektedir. Çocuklar ve gençler, gerçeklik algılarını etkileyen, keyif aldıkları bir durumun kendilerinde oluşturduğu etkiden kaynaklı verilenleri daha çabuk öğrenip kabullenebilmektedirler.

Çocuklar, yetişkin bireylere göre gerçek ve kurgu arasındaki farkları kavramakta zorlanmakta veya kimi zaman ayırt edememekte ve izledikleri çizgi film veya oynadıkları oyundan etkilenebilmekte ve gerçek hayata taşıma eğilimi gösterebilmektedir.

Çocuklar okul öncesi dönemde, yanlış davrandıkları için ceza alması gereken kahramanların, cezalandırılmadıklarını gördüklerinde bu tür kahramanların davranışlarını model alabilirler.

Şiddet içerikli görüntüleri taklit edebilir ve bunun sonucunda çevresine karşı saldırgan davranışlarda bulunabilirler. Çoğu kez hayran oldukları kahraman ya da karakterler, büyüyünce olmak istedikleri kişi olabilmektedir.

Çocukların karşılaştıkları görüntülerin onlarda şiddete eğilim, kaygı ve yalnız kalmak istememe gibi duygusal sıkıntılara yol açmasını önleyebilmek adına;

- Çocuklarla birlikte oyun karakterleri üzerine detaylı konuşulup, onların sadece çizgi filmler ya da hikâyelerdeki kahramanlar oldukları açıklanmalı,
- Çocuklarda yanlış algıya sebep olabileceği düşünülen içeriklerde müdahalede bulunulmalı ve ne anlatılmak istendiğine dair çocuğa açıklamalarda bulunulmalı,
- Çocuğu olumsuz etkileyeceği düşünülen karakterlerin varlığı biliniyor ise önceden tespit edilmeli ve aile tarafından kontrolü sağlanmalıdır.

4.4. Dijital oyunlar ve çocuklar üzerindeki psikolojik etkileri

Çocuklar ve gençlerin son yıllarda daha da sıklaşarak dışarda arkadaşları ile sosyalleşerek oynadıkları oyunların yerini evde bilgisayar başında oynadıkları sanal oyunlar almıştır. Bu dijital oyunların kullanımının giderek artması ve denetimsiz bir şekilde kullanımı "dijital oyun bağımlılığı" tanımını da ortaya çıkarmıştır. Amerikan Psikiyatri Birliği bu bozukluğun el kitabına eklenmesi için klinik tanıyı destekleyen ve ruhsal bir hastalık olduğunu tanımlayan daha fazla araştırmanın yapılmasını önermiştir. Dijital oyun bağımlılığının, beraberinde getirmiş olduğu sıkıntılar, ailelerin bu konuda kendilerini çaresiz hissetmeleri ve yapılan araştırmaların sonuçlarına göre diğer bağımlılık türleri ile benzerliklerinin ortaya konulmuş olması sebebiyle önem gerektiren bir konu olduğunu kanıtlanmaktadır.

Yakın zamanda Dünya Sağlık Örgütü (DSÖ), 'Bilgisayar Oyunu Bağımlılığı'nın ruhsal sağlık kategorisinde yer alması için birtakım çalışmalar yapmıştır. Çalışmalar sonrası, Hastalıkların Uluslararası Sınıflandırılması (ICD) tanı kılavuzunun 11'inci versiyonunun listesine hastalık olarak alınmıştır. Hastalık "Oyun rahatsızlığı" olarak isimlendirilmiştir ve böylelikle bilgisayar oyunları bağımlılığı ruhsal sağlık problemi kategorisine geçmiştir. Dünya Sağlık Örgütü, oyun rahatsızlığını, kişinin günlük aktivitelerini oluşturmada sıkıntı yaratan ve devamlı tekrar eden ciddi bir bağımlılık ve şiddetli bir davranış modeli olarak açıklamıştır.

Oyun bağımlılığı, oyun oynama süresini kontrol edememe, günlük yapılacak etkinliklere karşı ilgi kaybı, yarattığı olumsuz durumlara rağmen karşı koyulamaz şekilde oyuna devam etme isteği ve oyun oynamadığı zaman yoksunluk hissetme gibi belirtiler gösteren bir dürtü kontrol bozukluğu olarak tanımlanmaktadır. Oyunların olumlu ya da olumsuz etkilerini belirleyen temel faktör oyunların içerikleridir.

4.5. Dijital oyunların olumlu etkileri

Dijital oyunların aşırı şekilde oynanmadığı ve sosyal yaşamda herhangi bir değişikliğe neden olmadığı takdirde olumlu etkilerinin olduğu da kabul edilmektedir. Dijital oyunların denetimli bir şekilde oynanması, çocuk ve gençlerin gelişimlerine önemli katkı sağladığını da göstermektedir.

Olumlu etkileri aşağıdaki gibidir;

- Görsel-dikkat becerilerini geliştirir.
- Eğitsel içerikli oyunlar ders başarısını arttırır.
- Problem çözme becerisi kazandırır.
- Oyunlar çocukların daha hızlı ve doğru kararlar almalarını gerektirir ve bu sebeple karar verme becerilerine katkı sağlar.
- Çocuğa başarı duygusu kazandırır ve öz güvenini artırır.
- Öğrenilen bir davranışı farklı problemlere farklı ortamlarda farklı şekillerde uygulayabilme imkânı sağlar.
- Çocuk günlük yaşamında ve eğitimi sırasında öğrendiği pek çok kavramı bilgisayar oyunlarıyla pekiştirebilir.
- Motivasyon ve serbest zaman aracı olarak kullanılabilir.
- Psikoterapi tedavisi gören bazı hastalarda motor becerilerini geliştirmeleri için kullanılmaktadır.

4.6. Dijital oyunların olumsuz etkileri

Dijital oyunların çok fazla ele alınmasına neden olan konu çocuklar üzerindeki olumsuz etkileri ile çocuklar ve aileler için getirdiği risklerdir. Özellikle küçük yaştaki çocuklar için yemek yedirmede bir araç olarak bile kullanılabilmektedir. Ailelerin bilinçsiz hareket etmesi farklı sonuçlara yol açabilmektedir. Bu tarz yaklaşım ve davranışlar çocuklarda dijital oyun bağımlılığına zemin oluşturabilmektedir. Dijital oyunların bazı olumsuz etkileri aşağıdaki gibidir;

- Aile içi iletişimi azaltması,
- Kurgu ile gerçeklik arasındaki farkı ayırt etmede güçlük,
- Bazı şiddet içerikli oyunların saldırgan duygu, düşünce ve davranışların gelişmesine sebep olması,
- Ders çalışma, yapması gereken işleri yapma konusunda ayırdıkları zamanlarını azaltması sebebiyle kişisel başarıyı olumsuz etkilemesi,
- Anti sosyal davranışlar gösterme,
- Gerçek duygulardan uzaklaşma,
- Dikkat bozukluğu gibi problemlere sebep olması,
- Dil gelişimini olumsuz etkilemesi,
- Çocukların çevrimiçi tehditlere maruz kalabilmesi,
- İçine kapanma, sosyal aktivitelere ve dış dünyaya ilginin azalması,

4.7. Aileler ne yapabilir?

Dijital oyunların çocukların hayatında bağımlılık düzeyine ulaşmaması için; ailelerin çocukları ile yeteri kadar ve kaliteli vakit geçirmesi, aile içinde çocukların fikirlerine, duygularına önem vererek çocukların özgüvenini artırıcı önlemler alması çok önemlidir. Çocukların oynadıkları oyunların içeriğini araştırarak şiddet içerikli oyunlar yerine eğitsel oyunlar oynamaları yönünde bir bilinç aşılayıp yönlendirme yapabilirler. Oyunlarını arkadaşlarıyla birlikte oynamaları için yönlendirebilirler. Böylelikle, arkadaşları ile iletişiminin gerçek hayatta devam etmesi ve bu durumun çocuğun sosyal iletişiminin korunması yönünden de fayda sağlayacağı düşünülmektedir. Ebeveynler, çocukların iç dünyasına daha çok yönelmeli, anlamaya çalışmalı, kafalarında herhangi kalıcı bir soruna yer vermeden, çocukların farkındalıklarını arttırmaları gerekmektedir. Bunların yanında, ebeveynlerin internet kullanımı konusunda çocuklarına uygun rol model olmaları gerekmektedir. Çocuklar, anne-babalarının, interneti ne sıklıkla ve nasıl kullandıklarını gözlemleyecek onları model alacaklardır. Çocukların, ebeveynlerinin kendilerine öğrettikleri ve uygulanmasını bekledikleri şekilde interneti kullandıklarını görmeleri çocuklar için olumlu bir pekiştireç sağlayacaktır. Elinden telefon düşmeyen ve sürekli internette gezinen bir ebeveynin çocuğundan aksini beklemesi uygun olmayacaktır. Ebeveynlere büyük görev düşmektedir. Aynı zamanda ebeveynlerin oyunu oynayan çocuğa süre kısıtlaması getirerek, oyun sürelerini kontrol altına alması oyunların bağımlılık yapıcı etkisini de azaltacaktır. Oyun esnasında çocuklara eşlik etmek ve çocukları yönlendirmek oyundan gelebilecek riskleri de minimize edecektir.

5. İnternet Bağımlılığında Siber Zorbalık ve Psikolojik Etkileri

İlk defa 2000 yılında ABD'de "Cyberbullying" terimi kullanılmış ve dilimize "Siber Zorbalık" olarak çevrilmiştir.

Siber zorbalık, kasıtlı bir şekilde karşıdaki kişiye zarar verici, küçük düşürücü, düşmanca davranışları içermektedir.

5.1. Siber zorbalığın nedenleri

Bir kişinin daha önceden siber zorbalık ile karşılaşmış ve bu durumdan zarar görmüş olması, özgüven eksikliği, düşük benlik algısı, sosyal kaygı, yaşadığı aile içi huzursuzluklar, kişinin, kendi davranışlarının ne gibi sonuçlara yol açabileceğini görememesi gibi davranışlar siber zorbalığa neden olan durumlardır.

5.2. Siber zorbalığa maruz kalan kişilerde gözlemlenen psikolojik etkiler

Sanal zorbalık olaylarına maruz kalanlar bu olaylardan dolayı farklı duygular yaşamaktadırlar. Çocuk ve ergenlerin siber zorbalığa maruz kalmaları halinde yetişkinlere göre daha fazla hasar gördükleri gözlemlenmiştir. Yapılan çeşitli çalışmalar doğrultusunda, siber zorbalığa maruz kalan kişiler; üzgün, utanmış ve incinmiş hissettiklerini ifade etmişler ve bu durumların kişilerde; öfke, kızgınlık, üzüntü, içe kapanma, gerginlik gibi sorunları ortaya çıkardığı görülmüştür. Ülkemizde görülmemekle birlikte yurtdışında siber zorbalığa maruz kalanlarda intihar vakalarına rastlanmaktadır.

5.3. Siber zorbalığa karşı alınabilecek tedbirler nelerdir?

Ebeveynlerin çoğu günümüzde iletişim araçlarına uzak kalmakta, teknolojik gelişmeleri yakından takip etmemektedir. Bu durum çocukları ile olan iletişimlerini etkilemekte ve çocuklarının siber zorbalıkla karşılaşma ihtimallerini gözden kaçırmalarına, fark edememelerine sebep olabilmektedir. Ebeveynlerin çocukları ile iyi bir iletişim geliştirmesi, teknoloji ve internet konularında kendilerini geliştirmeleri önem taşımaktadır. Ebeveynlerin iletişim araçlarını iyi tanıması, internetin bilinçli ve güvenli kullanımına yönelik yeterli bilgi düzeyine sahip olmaları, çocuklarının gelişim düzeylerine uygun şekilde interneti nasıl kullanacakları konusunda çocuklarını eğitebilmelerine ve yardımcı olabilmelerine olanak sağlayacaktır. Okul psikolog ve psikolojik danışmanları siber zorbalık ile ilgili farkındalık ve önleme konularında eğitim programları oluşturmalı, okul ve aile arasında işbirliği sağlamalıdır. Ebeveynler internet kullanımı ile ilgili sınırlamalar getirmeli ve denetimini mutlaka yapmalıdır. Ebeveynlerin üzerine düşen en büyük görev çocukları ile açık ve iyi bir iletişimde olmaktır. Yapılan araştırmalara göre, ailesi ile iletişimi kuvvetli olan bireyler siber zorbalık ile daha az karşılaşmakta ve siber zorbalığa daha az maruz kalmaktadır.

6. İnternet Bağımlılığı Tedavi Yaklaşımları

İnternet bağımlılığı hakkında yapılan araştırmalar sonucu, internet bağımlılığının bilişsel-davranışçı yaklaşım ile tedavi edilebileceği sonuçlarına ulaşılmıştır. Bilişsel-davranışçı terapi yöntemi ile devam eden tedavi sürecinde bireyin kişilik yapısı göz önünde bulundurularak teşhisi yapılmalı ve tedavi aşamasına geçilmelidir.

6.1. Farmakoterapi

Farmakoterapi, rahatsızlıklarda ilaç tedavisinin kullanılmasıdır. Öncelikle altta yatan başka bir psikiyatrik rahatsızlığın olup olmadığına bakılmalıdır. İnternet bağımlılığı pek çok psikiyatrik bozukluk ile aynı anda görülebilmektedir. Bu nedenle, öncelikle eğer altta yatan başka bir bozukluk varsa bu bozuklukların tedavi edilmesi patolojik internet kullanımını azaltabilmektedir. Farmakoterapi, psiko-

terapi ile tedavide bazen tek başına bazen de kombine olarak kullanılabilmektedir. İnternet bağımlılığı şikâyetleri ile başvuran bir kişinin hikâyesi geçirilmiş hipomani ve mani açısından dikkatle kontrol edilmeli, detaylı incelenmelidir. Mani, anormal olarak yükselmiş duygu durumudur. Hipomani ise kişinin psikolojik ve bedensel olarak normal seyrin üzerinde bir canlılık sergilediği, ancak mani kadar şiddetli olmadığı bir ruh halidir.

6.2 Bilişsel davranışçı yaklaşım

Bilişsel-davranışçı yaklaşım, kişinin kendisi ve çevresi ile ilgili olumsuz ve otomatik gelişen sağlıksız düşünce biçimlerinin yerine alternatif sağlıklı ve gerçekçi düşünceler geliştirmesini sağlayan yaklaşımları içermektedir. Bilişsel-davranışçı yaklaşıma göre, düşüncelerimiz duygularımızı belirlemektedir, herhangi bir bireyin hissettiği duyguya ancak onun düşünceleri yoluyla ulaşılabilir. Bireyin hatalı inançlarını düzeltebilmesine yardımcı olarak alternatif düşünce ve davranış geliştirmesine katkı sağlanabilir. Uygun olmayan reaksiyonları azaltılabilir veya engellenebilir. Bilişsel-davranışçı yaklaşıma göre sağlıklı internet kullanımı; "kişinin kendi koşulları içerisinde, belli bir amaç doğrultusunda, sanal-gerçek iletişimin farkında olarak ve kendi kimliğini gizlemeden interneti kullanabilmek" şeklindedir. Bilişsel-davranışçı yaklaşımın, internet bağımlılığının tedavisinde oldukça etkin ve olumlu etkisinin olduğu belirtilmektedir.

Bilişsel modele göre A noktasında yaşanan bir olaya C noktasında verilen duygusal yanıt, B noktasında A noktası ile ilgili düşünülen ve yapılan yoruma bağlıdır. Bireyin A noktasındaki olaya B noktasında geliştirdiği yorum C noktasında değişik duygulara kapılmasına sebep olacaktır. Örneğin; bir arkadaşımızın selam vermeden yanımızdan geçmesi ve bu durumun bizde yaratacağı duygu, o esnada duruma karşı yapacağımız yoruma bağlıdır. Arkadaşımızın yanımızdan geçerken selam vermemesinin birçok sebebi olabilir. Fakat bu durumu yorumlama biçimiz öfke, üzüntü vb. farklı duyguları yaşamamıza neden olacaktır. Dalgın olup görmemiş olabileceğini düşünürsek arkadaşımıza karşı daha empatik yaklaşabiliriz, göstermiş olduğu davranışın kasıtlı olduğunu düşündüğümüz takdirde ise öfke ya da üzüntü duyabiliriz. Verilen örnekte olduğu gibi internet bağımlılığının oluşma sürecinde de çeşitli otomatik düşünce ve inançların etkisi göz ardı edilemez. Otomatik düşünceler ortama ve duruma göre değişiklik gösteren zihinsel işlemlerdir. Otomatik düşüncelerin oluşturduğu inançların ve duyguların azaltılması öncelikli hedeftir.

İnternet bağımlılığının tedavisinde internet kullanımının yasaklanması etkili bir yöntem değildir. İnternet yaşamımızın her alanında var olan, çeşitli ihtiyaçlarımıza cevap veren iletişim ağıdır ve bu sebeple internet bağımlılığının tedavisinde kontrollü internet kullanımı sağlamak en uygun yöntem olarak görülmektedir.

İnternet bağımlılığının bilişsel-davranışçı tedavisinde kullanılan tedavi hedefleri şu şekildedir;

Var olan problemin kabulü: Aşırı internet kullanımı gösteren bireyin internet kullanımı nedeniyle günlük hayatında yapmasına engel olan faaliyetlerin kendisi tarafından fark edilmesi sağlanır. Bu faaliyetlerin neler olduğu, yaşamında ne gibi sorunlara sebep olabileceği, yapması gereken işleri tekrardan yapabilmesi halinde hayatında ne gibi olumlu değişmelerin olabileceği konuları ayrıntılı bir şekilde ele alınır. Sıkıntı yaratan aşırı internet kullanımı davranışını kendine itiraf edemeyen bireyin, farkındalık oluşturulduktan sonra bu sorunu kendisinin görüp, kabul etmesi sağlanır. Bilişsel yeniden yapılandırma yöntemi bu duruma katkı sağlar.

Davranış analizi: Bireyi internetin aşırı kullanımına iten durumlar, düşünceler ve bireyde oluşturduğu duygular belirlenir. Gün içinde internette geçirdiği vakit ve internette geçirdiği sürelerde ne gibi aktiviteler yaptığı ve hangi sitelerde gezindiği belirlenerek analiz edilmektedir.

Zaman yönetimini sağlamak: İnternetin planlı kullanılması, şuan kullanmış olduğu saatlerden farklı şekilde interneti kullanması, internette geçirilen vaktin sınırlandırılması, internet dışı çeşitli aktivitelerin planının oluşturulması gibi zamanın yönetimi tekniği kullanılmaktadır.

Sosyal aktiviteler oluşturmak: Aşırı ve problemli internet kullanımına yönelik psikolojik ve sosyal desteklerin oluşturulması, aşırı internet kullanımından kaynaklı bireyde oluşan yalnızlık psikolojisi ile yüzleşmesinin sağlanması ve problem çözme becerilerinin geliştirilmesi amaçlanmaktadır.

Tekrarlama olasılığının önlenmesi: Problemli internet kullanım davranışının tekrardan başlayıp devam etmesine sebep olabilecek durumların belirlenip önleyici politikaların geliştirilmesi, bu gibi durumlarda bireye yeni alternatif davranışların kazandırılması amaçlanmaktadır.

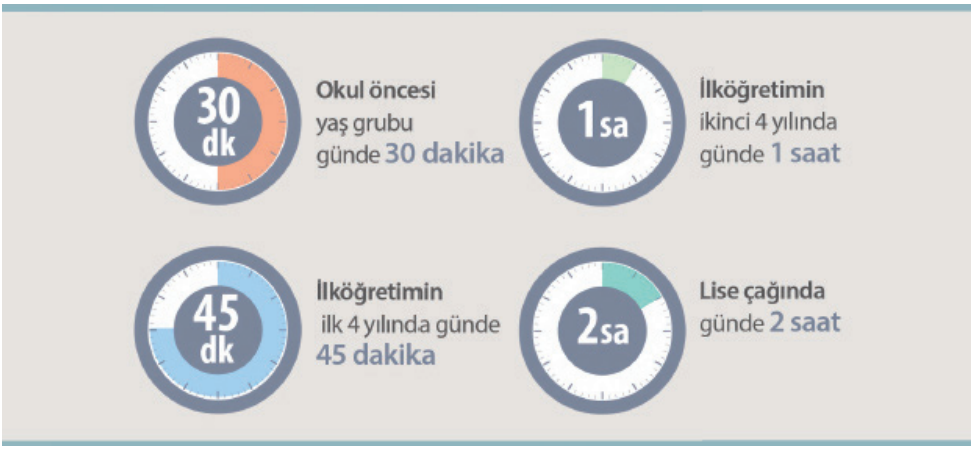
7. İnternet Bağımlılığı Konusunda Öneriler

İnternet önlenemez bir biçimde kimi zaman hayatımızın odak noktasında yer almaktadır. İnternet kullanımının ergenler, yetişkinler ve çocuklar tarafından farklı ihtiyaçlar doğrultusunda kullanıldığı görülmektedir. Yapılan bir araştırmanın sonucuna göre, ergenler içinde bulundukları gelişimsel dönemin etkisiyle kendilerine bir hedef belirleyememekte, günlük yaşamda birçok konuda karmaşa yaşamakta ve bu sıkıntılı durumlardan kurtulmak için de internet kullanımına daha çok başvurmaktadırlar. Bu sebeple internetin ergenler için sosyal destek ve kimlik arayışında bir kaynak aracı olarak görülmemesi ve kullanılmasını önlemek önemlidir. Problemli internet kullanımının meydana gelmesi, doğru yönlendirme yoluyla önlenebilir. İnternet, bilinçli, güvenli ve etkin kullanımı halinde bireyin ufkunu açan, başarısına katkı sağlayan aynı zaman-

da çocukların gelişimini de desteklemeye yardımcı etkili bir faktördür. Önemli nokta; risk ihtimallerini belirlemek, önlemini alabilmektir. Bireyin internet kullanımını kısıtlaması ya da kullanımından tamamen kendini mahrum bırakması bir çözüm yolu olmamakla birlikte, bireyin kendini kontrol etme ve sorumluluk bilincini kazanması temel amaç olmalıdır. Bireylerin psikolojik ihtiyaçlarının, yaşam doyumlarının karşılanıyor olması ve statüsünün başarılı olması halinde problemli internet kullanımının azaldığı, kimlik statüsünün karmaşık olması halinde ise problemli internet kullanımının artış göstermesi durumu da yapılan araştırmalar sonucu elde edilen sonuçlar arasındadır.

7.1. Çocuklarda ve ergenlerde internet bağımlılığını önlemek için ebeveynlerin sorumlulukları

- Çocuklarda internet bağımlılığını önlemek için;
- Ebeveynlerin uygun rol modeli olması,
- İnternetteki video veya benzeri içeriklerin ev ortamında çocuğu oyalamak için kullanılmaması,
- İnternette geçirilen sürenin kontrolünün ebeveyn tarafından sağlanması,
- Çocuğun gelişimine, hayal gücüne katkı sağlayacak faaliyetlerin ebeveynlerle birlikte yapılması,
- İnternet dışında da bilgi edinebilecekleri kaynakların var olduğunu bilmeleri ve kitap, kütüphane gibi kaynaklardan da fayda sağlayabilecekleri yönünde bilinçlendirilmeleri,
- 2 yaşından küçük çocukların internet, TV ya da bilgisayar ile karşılaştırılmaması,
- Çocuğun internet başında geçirdiği sürenin gereğinden fazla uzamasını önlemek amacıyla, yararlanılacak sitelerin ebeveyn ile birlikte belirlenmesi ve denetiminin sağlanmasının bağımlılığı önlemede faydalı olacağı düşünülmektedir.
- İnternet kullanımı, çocuk ve ergenlerde bağımlılığı önlemek adına; okul öncesi yaş grubunda günde 30 dakika, ilköğretimin ikinci 4 yılında 1 saat, ilköğretimin ilk 4 yılında günde 45 dakika, lise çağında ise günde 2 saat önerilmektedir(Şekil 1).



Şekil 1 - Çocuk ve Ergenlerde Bağımlılığı Önleme

8. Bölüm Kazanımları

İnternet günümüzde insanlar için vazgeçilmez bir iletişim kanalı olmakla beraber, istenilen her yerde ve her zaman ulaşabilme kolaylığı internet başında geçirilen sürenin artmasına neden olmaktadır. Ekran başında geçirilen uzun süreli vakitler ise birtakım psikolojik ve fiziksel sorunları da beraberinde getirebilmektedir. İnternet doğru ve etkin bir şekilde kullanıldığı zaman birçok fayda sağlayabilirken yanlış ve bilinçsiz kullanımı da beraberinde kötü sonuçlar doğurabilmektedir. Bu bölümde internetin fiziksel sağlık ve psikolojik sağlığa etkisi, internet ortamında siber zorbalık ve psikolojik etkileri, internet bağımlılığı ve belirtileri, dijital oyunlar ve çocuklar üzerindeki etkileri, internet bağımlılığı tedavi yaklaşımları gibi konulardan bahsedilerek özetlenmeye çalışılmıştır. İnternetten doğru ve etkin bir şekilde fayda sağlayabilmek için dikkat edilmesi gereken faktörler üzerinde durulmuştur.

KAYNAKLAR

Amerikan Psikiyatri Birliği. Mental Bozuklukların Tanısal ve Sayımsal El Kitabı, dördüncü baskı (DSM IV) (Çev. Ed: E. Köroğlu) Hekimler Yayın Birliği, Ankara,1995

Akbulut, Y. (2013). Çocuk ve ergenlerde bilgisayar ve internet kullanımının gelişimsel sonuçları. Trakya Üniversitesi Eğitim Fakültesi Dergisi, 3(2).

Arısoy, Ö. (2009). İnternet Bağımlılığı ve Tedavisi. Psikiyatride Güncel Yaklaşımlar, 1,55-67.

Aydeniz, A., & GÜRSOY, S. (2008). Upper extremity musculoskeletal disorders among computer users. Turkish Journal of Medical Sciences, 38(3), 235-238.

Bilgisayar Oyunu Bağımlılığı Resmen Ruhsal Hastalık,

URL:https://www.e-psikiyatri.com/bilgisayar-oyunu-bagimliligi-resmen-ruhsal-hastalik-64653, Son Erişim tarihi, 03.07.2018.

Bülbül, S., Kurt, G., Ünlü, E., & Kırlı, E. (2010). Adolesanlarda uyku sorunları ve etkileyen faktörler. Çocuk Sağlığı ve Hastalıkları Dergisi, 53, 204-210.

Ceyhan, A., (2014). Ergenlerin İnternet Ve Problemli İnternet Kullanım Davranışlarının Bazı Psiko-Sosyal Özellikler Açısından İncelenmesi, Doktora Tezi, Eskişehir Anadolu Üniversitesi

Çerezci O, Kartal Z, Pala K, Türkkan A, Elektromanyetik Alan ve Sağlık Etkileri, Bursa 2012

Güvenli Web, Bilgi Teknolojileri ve İletişim Kurumu,

URL: http://www.guvenliweb.org.tr/, Son Erişim tarihi, 16.07.2018.

Güvenli Web, Bilgi Teknolojileri ve İletişim Kurumu,

URL:http://www.guvenliweb.org.tr/blog-detay/dijital-oyunlarin-cocuklar-ve-gencler-uzerindeki-etkileri, Son Erişim tarihi, 18.06.2018.

Hakala, P. T., Rimpelä, A. H., Saarni, L. A., & Salminen, J. J. (2006). Frequent computer-related activities increase the risk of neck–shoulder and low back pain in adolescents. The European Journal of Public Health, 16(5), 536-541.

İnandı T ve Akyol İ. Bilgisayar Kullanımı İle İlgili Sağlık Sorunları, Sted, Mart 2001,

URL: http://www.ttb.org.tr/STED/sted0301/3.html, Son Erişim tarihi, 16.07.2018.

Jensen, C., Finsen, L., Søgaard, K., & Christensen, H. (2002). Musculoskeletal symptoms and duration of computer and mouse use. International journal of industrial ergonomics, 30(4-5), 265-275.

Muslu, G. K., & Bolışık, B. (2009). Çocuk ve Gençlerde İnternet Kullanımı. TAF Preventive Medicine Bulletin, 8(5).

Özcanlı Atik D, Erdoğan Zeydan Z, Albayrak Çoşar A, Uyku Sorunları Hipertansiyona Neden Olur mu?

Türk Kardiyoloji Dern. Kardiyovasküler Hemşirelik Dergisi,

URL: http://www.journalagent.com/kvhd/pdfs/KVHD_1_3_2_8.pdf, Son Erişim tarihi, 16.07.2018.

Savaşhan, Ç., Erdal, M., Sarı, O., & Aydoğan, Ü. (2015). İlkokul çağındaki çocuklarda obezite görülme sıklığı ve risk faktörleri. Türkiye Aile Hekimliği Dergisi, 19(1), 14-21.

URL:http://www.turkailehekderg.org/makaleler/arastirma/ilkokul-cagindaki-cocuklarda-obezite-gorulme-sikligi-ve-risk-faktorleri/, Son Erişim tarihi, 16.07.2018.

ŞENORMANCI, Ö., Konkan, R., & Sungur, M. Z. (2010). İnternet bağımlılığı ve bilişsel davranışçı terapisi. Psychiatry, 11, 261-268.

Tarhan,N., Nurmedov, S. (2014). Bağımlılık (5.Baskı). İstanbul:Timaş.

Teknoloji Bağımlılığı,

URL: http://yesilay.org.tr/tr/bagimlilik/teknoloji-bagimliligi, Son Erişim tarihi, 10.05.2018.

Young, K. S. (1998). Internet addiction: The emergence of a new clinical disorder. Cyberpsychology & behavior, 1(3), 237-244.

What Is Cyberbullying,

URL: https://www.stopbullying.gov/cyberbullying/what-is-it/index.html, Son Erişim tarihi, 20.04.2018.

BÖLÜM 5 SOSYAL MEDYA

İçindekiler

1. Sosyal Medya Nedir?

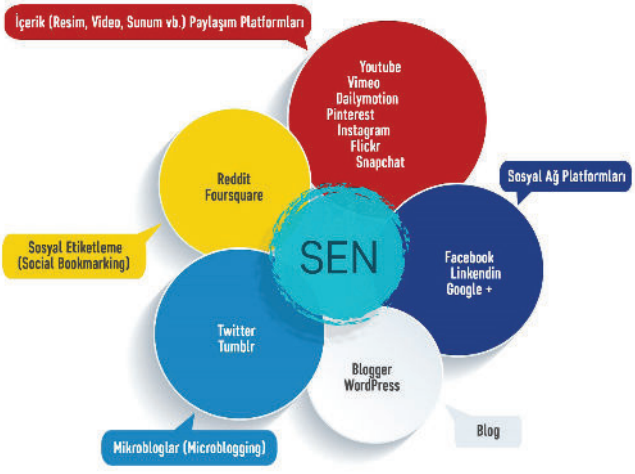
Sosyal medya platformları, İnternet kullanıcılarının mesajlaşma, diğer kullanıcılar ile iletişim, resim, video, haber, ses, yorum vb. içerik paylaşımı yapabildiği; paylaşılan içeriğin hem izlenebildiği hem de hızlı bir şekilde içeriğe cevap verilebilen veya yorum yapılabilen internet üzerinden hizmet veren platformlardır.

İnternet ortamında web siteleri ve akıllı telefon uygulamaları üzerinden hizmet veren sosyal medya, insanların arkadaşlarıyla veya diğer kişilerle iletişim kurmalarına, devlet kurumlarının ve sivil toplum kuruluşlarının hizmetlerini ve yeniliklerini vatandaşlara ve internet kullanıcılarına aktarmalarına ve ticari işletmelerin de ürün ve markalarının tanıtımını yapmalarına imkan sunmaktadır. Sosyal medya platformları, internet kullanıcıları, devlet kurumları, sivil toplum kuruluşları (STK) ve ticari işletmeler tarafından yaygın şekilde kullanılmaktadır.

Sosyal medya, geleneksel medya ile aynı şekilde haberleri takip etmek ve paylaşmak, okuyucu veya izleyicilerle iletişim kurmak gibi imkanlar sunmaktadır. Ancak geleneksel medyanın aksine sosyal medya tüm bunları internet ortamında canlı olarak ve interaktif şekilde küresel veya bölgesel sosyal ağlar üzerinden gerçekleştirmektedir.

Günümüzde yaygın kullanıma sahip Sosyal Medya Platformları genel hatlarıyla aşağıdaki şekilde gruplandırılabilir:

- **Sosyal Ağ Platformları:** Facebook, Linkedin, Google+
- **İçerik (Resim, Video, Sunum vb.) Paylaşım Platformları:** Youtube, Vimeo, Dailymotion, Pinterest, Instagram, Flickr, Snapchat
- **Blog:** Blogger, WordPress
- **Mikrobloglar (Microblogging):** Twitter, Tumblr



Şekil 1 - Sosyal Medya Çeşitleri

- **Sosyal Etiketleme (Social Bookmarking):** Reddit, Foursquare

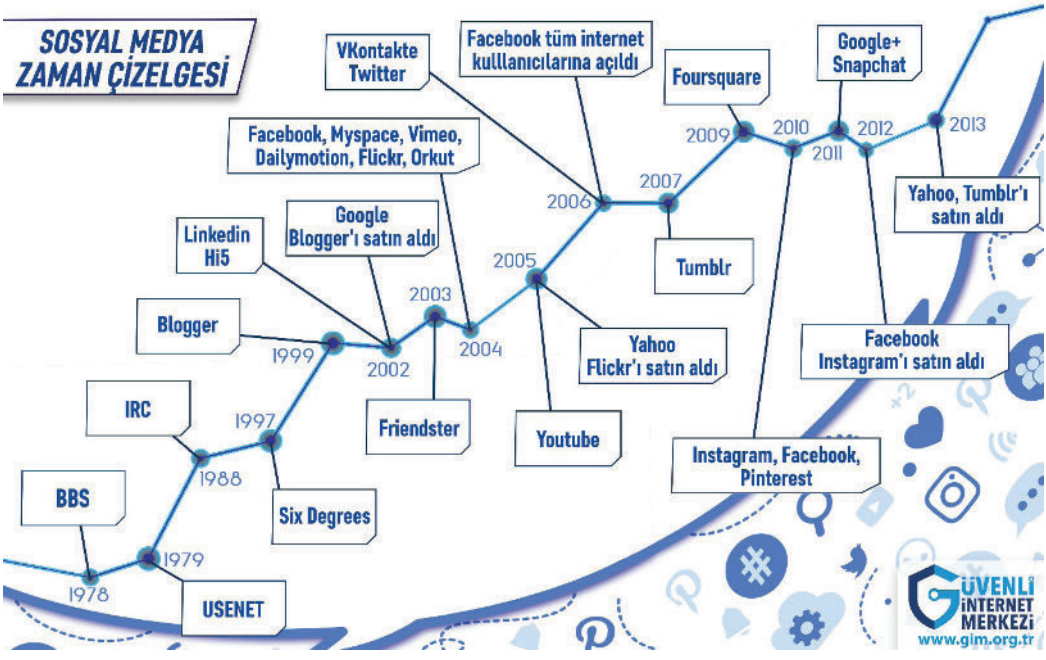
Sosyal ağlar, kullanıcıların kendilerine ait bir profil ve arkadaşları ve takipçilerinden oluşan bir ağ oluşturabildikleri internet topluluklarıdır. Kullanıcılar sosyal ağ platformundaki diğer kişiler ile iletişim ağ platformu bulunmakta olup küresel ölçekte en popüler olanlarına Facebook, Twitter ve Tumblr örnek verilebilir. Twitter ve Tumblr, microblogging siteleri olarak da bilinmektedir.

Blog (Web Log – Web Kayıt, ifadesinin kısaltması) siteleri, bir blogger'ın (blog sahibi ve içerik oluşturan kişi), blog'un konusuyla ilgili düzenli olarak resimler, videolar, haberler, yazılar veya diğer web sitelerinin bağlantısını paylaştığı çevrimiçi iletişim platformlarıdır. Bloglar genellikle dergilere benzetilmektedir çünkü çoğu blog sitesinde, blog sahibinin kişisel anlatımı ve bakış açısıyla oluşturulmuş içerikler bulunmaktadır. Diğer sosyal medya ortamlarında olduğu gibi Blog'larda da okuyucular bloggerlar ile blog'a yazdıkları yorumlar aracılığıyla iletişim kurabilirler. Ayrıca yeni içerik oluştuğunda haberdar olmak için blog'a üye olabilirler. Popüler blog platformlarına; WordPress ve Blogger örnek verilebilir.

Akıllı telefonların yaygınlaşması ile beraber resim ve video paylaşım sitelerinin popülerliği de hızlı bir şekilde artmıştır. Resim ve video paylaşım web siteleri, kullanıcıların yüklediği videoları ve resimleri barındırmaktadır. Günümüzde en popüler video paylaşım sitesi olan YouTube, kullanıcının oluşturduğu hesabından video paylaşmasına olanak sağlamakta olup, videoları izlemek için bir kullanıcı hesabına gerek yoktur. Vimeo da video yüklemek ve paylaşmak için kullanılan diğer bir platformdur. Popüler resim paylaşım siteleri olan Flickr, Instagram ve Pinterest her biri ayrı ilgi alanlarında resim paylaşılmasına olanak sağlamaktadır. Aynı zamanda bazı resim paylaşım siteleri video paylaşılmasına da imkan vermektedir.

2. Sosyal Medya'nın Kısa Tarihçesi

Sosyal Medyanın nasıl tanımlandığına bağlı olarak başlangıcı ve gelişimi de değişiklik gösterebilmektedir. Örneğin posta hizmetlerini kullanarak mektup ile yapılan iletişimi de sosyal medya başlangıcı olarak kabul eden bir görüş olsa bile büyük çoğunluk sosyal medyayı internet aracılığıyla küresel ölçekte yapılan kişiler arasındaki bilgi paylaşımı ve iletişimi olarak kabul etmektedir. Bu kapsamda sosyal medya tarihindeki kilometre taşı olarak nitelendirilebilecek gelişmeler bu bölümde özetlenmiştir.



Şekil 2 - Sosyal Medyanın Tarihi

Tam anlamıyla sosyal medya olarak tanımlanamasa da sosyal medyanın ilk türlerinden biri 1970'lerin sonundaki duyuru tahtası sistemidir (BBS - Bulletin Board Systems). Bu sistemde; kullanıcıların kişisel bilgisayarlarında barındırılan hizmete aynı anda sadece bir kullanıcı bağlanabiliyordu. BBS kullanıcıların oturum açarak birbirlerine mesaj bırakabildiği, okuyabildiği ve dosya transferi yapabildiği ilk web sitesi türüdür ve 1990'ların sonuna kadar kullanılmıştır.

1979 yılında hizmete verilen Usenet, haber gruplarında yazı ve haber paylaşımına imkan verdi. Usenet sistemi RSS besleme okuyucuların (RSS Feed Reader) öncüsüdür.

1988 yılında internet kullanıcıları İnternet Aktarmalı Sohbet (IRC - Internet Relay Chat) ile tanıştı. IRC, sohbet ve dosya paylaşımı amacıyla kullanılıyordu ve günümüz modern anlık mesajlaşma uygulamalarının öncüsüydü.

1996 yılında masaüstü bilgisayarlara kurulabilen ilk anlık mesajlaşma programı olarak bilinen ICQ ve ondan kısa zaman sonra ise sosyal medya tarihinde önemli bir yere sahip olan AOL (America Online) anlık mesajlaşma sitesi hizmete açılmıştır.

Çoğunlukla üzerinde hem fikir olunan ilk sosyal medya sitesi

Six Degrees'dir. 1997 ve 2001 yılları arasında hizmet veren Six Degrees web sitesi ismini "Ayrımın Altı Derecesi Teorisinden" (six degrees of separation theory) almıştır. En popüler olduğu dönemde yaklaşık bir milyon üyeye sahip olmuştur. Six Degrees, kullanıcıların profil oluşturabilmesi, arkadaşlık daveti gönderebilmesi, gruplar oluşturabilmesi, diğer kullanıcıları arayabilmesi ve diğer kullanıcıların profillerini inceleyebilmesi özellikleriyle ilk sosyal medya sitesi olarak tanımlanmaktadır.

1999 yılında internet kullanıcıları kendi blogları üzerinden yazılarını ve paylaşımlarını yapabileceği Blogger ile tanıştı.

2000 yılı itibariyle tüm dünyada 100 milyona yakın insanın internet erişimi bulunmakta olup, daha fazla insan anlık mesajlaşma uygulamalarında arkadaşlarıyla konuşmak veya ilgilendikleri konularda tartışmak amacıyla vakit geçirmeye başlamıştır.

2002 yılında kurulan Friendster, modern sosyal medyanın ilk örneği kabul edilebilir. Çoğunluğu Asya kıtasından 100 milyonun üzerinde üyeye ulaşan Friendstar'ın temel amacı kullanıcılarının gerçek hayat yerine internet ortamında yeni insanlarla tanışabilmesine ortam yaratmaktı.

2003 yılında hizmete verilen LinkedIn, iş dünyasındaki çalışanların ve firmaların birbirlerine ulaşabildikleri, personel veya iş arama imkanı sunan ve bu şekilde iş dünyasındaki çalışanların sosyalleşmesine ve birbirleriyle bağlantı kurmasına olanak sağlayan bir platform olarak günümüzde de hizmet vermeye devam etmektedir. LinkedIn, belirli bir konuya özel bir sosyal medya sitesi olması sebebiyle sosyal medya platformlarının ilklerinden birisidir.

2003 yılında yayına verilen diğer bir sosyal medya platformu Hi5'dır. Günümüzde çoğunluğu Afrika, Asya ve Latin Amerika kıtalarından 1 milyonun üzerinde üyesi ile hizmet vermeye devam etmektedir.

2004 yılında Mark Zuckerberg günümüzün en popüler sosyal medya platformu olan Facebook'u yarattı. Aslında Zuckerberg Facebook'u Harvard Üniversitesi öğrencileri için geliştirdi ancak daha sonra potansiyelini gördükten sonra 2006 yılında tüm dünyanın kullanımına açtı.

2004 yılında yayına alınan MySpace ise genel amaçlı bir sosyal medya sitesi olarak hizmet vermiştir. MySpace web sitesi kullanıcı profili oluşturma, video, müzik yükleme ve diğer kullanıcılar ile sohbet edebilme özellikleri ile döneminin popüler bir uygulamasıydı. Myspace kullanıcı profili tabanlı bir web sitesi olmasıyla Facebook gibi platformlara ilham veren öncü bir web sitesiydi.

2005 yılında YouTube web sitesi yayına alındı. Günümüzün en popüler video paylaşım sitesi olan YouTube yayına alındığı yıllarda da döneminin en kapsamlı ve büyük video paylaşım sitesiydi.

2006 yılında ise, Twitter hizmet vermeye başladı.

İnternet hızının artması, yazılım araçlarındaki gelişmeler, daha güçlü ve hızlı bilgisayarlar ve elbette akıllı telefonların gelişimi ve teknolojik cihazlara ve internete erişimdeki maliyetlerin ucuzlaması sosyal medya kullanımındaki hızlı büyümeyi destekleyen faktörlerdir.

Akıllı telefon ve tablet teknolojisinin gelişimine bağlı olarak sosyal medya da değişiklik göstermiştir. Bir masaya bağlı kalarak masaüstü bilgisayarlar kullanmak yerine elimize aldığınız mobil cihazımız ile herhangi bir zaman ve mekanda işlevsel şekilde sosyal medyaya erişim imkanı oluştu. Bu gelişime bağlı olarak 2010 yılında resim ve video paylaşım uygulamaları Snapchat ve Instagram uygulamaları hizmet vermeye başladı.

Mobil uygulamaların gelişimi sosyal medyayı da etkilemiş ve tüm özellikleri barındıran genel amaçlı sosyal medya ile birlikte; tüm kullanıcılara açık resim paylaşımı (Instagram) ve belirlenen kullanıcılara açık resim paylaşımı (Snapchat) gibi sadece belirli tür etkileşim için özelleştirilmiş uygulamalar ortaya çıkmıştır. Günümüzde İnternet kullanıcıları bu çeşitli sosyal medya platformlarını birlikte kullanarak daha geniş bir dijital ortamın parçası haline gelmektedir.

3. Popüler Sosyal Medya Platformları

Sosyal medya platformları hızla yaygınlaşmakta ve daha geniş kitlelere ulaşmaktadır. Sosyal medya kullanıcıları da mevcut küresel popüler platformları kullanmakla beraber belirli ülkeler veya bölgelerdeki kullanıcıların ihtiyaçları ve beklentileri doğrultusunda geliştirilmiş bölgesel sosyal medya platformlarını da kullanabilmektedir. Bu bölümde bazı popüler küresel ve bölgesel sosyal medya platformları hakkında bilgiler verilmiştir.

3.1. Popüler küresel sosyal medya araçları ve platformları

Günümüzde resim ve video paylaşım sitelerinden, blog sitelerine ve insanların birbirleriyle iletişim kurmasına olanak sağlayan sosyal ağlara kadar çok çeşitli sosyal medya platformu bulunmakta olup, sürekli olarak yeni platformlar da ortaya çıkmaktadır.

3.1.1. Facebook

Facebook[1], Harvard Üniversitesi'nde okuyan Mark Zuckerberg tarafından 2004 yılında ABD'de kurulan ve günümüzde küresel olarak en çok kullanılan sosyal ağ platformudur. Hem web sitesi hem de mobil uygulamaları üzerinden hizmet veren Facebook ile internet kullanıcıları, kurumlar, ticari işletmeler kendilerine ait profiller veya gruplar oluşturarak resim ve video paylaşabilir, etkinlikler, haberler, bilgiler gibi içerikler paylaşabilir ve diğer profillerdeki içeriklere yorum yapabilir veya beğenebilirler.

1 https://tr-tr.facebook.com/

3.1.2. LinkedIn

LinkedIn[2], 2002 yılında ABD'de kurulmuş ve 2003 yılında hizmete açılmıştır. LinkedIn, iş dünyasındaki kişilerin, firmaların, kurumların diğer kişilerle iletişim kurmasını ve bilgi alışverişi yapmasını amaçlayan profesyonel amaçlı bir sosyal ağ platformudur. LinkedIn belirli bir konuya özel bir sosyal medya sitesi olarak tanımlanmaktadır.

3.1.3. Google+

Google+[3], Google firmasının sahibi olduğu, 2011 yılında hizmete girmiş ve Google'ın sunduğu diğer hizmetlerin birleşiminden oluşan bir sosyal ağ platformudur. Hem web sitesi hem de mobil uygulamaları üzerinden hizmet veren Google+ ile fotoğraf, video eklenip paylaşılabilmekte, çoklu video görüşmesi yapılabilmekte (Google Hangouts), başka kullanıcılar takip edilebilmektedir. Kullanıcılar Google+'ta Google'ın Maps, Gmail, Blogger, arama motoru gibi diğer servislerini de entegre şekilde kullanabilmekte ve bu hizmetlerdeki içeriklerini takipçileri ile paylaşabilmektedir. Google+ hizmetine, Gmail hesabı ile üye olunabilmektedir.

3.1.4. Twitter

Twitter[4], 2006 yılında hizmete açılan bir sosyal ağ ve mikroblog platformudur. Twitter'da internet kullanıcıları profil oluşturabilir, takipçi kazanabilir veya başkalarını takip edebilirler. Twitter mesajları Tweet olarak isimlendirilmektedir ve 280 karakter ile sınırlıdır. Kullanıcılar, Tweet'lerle metin, bağlantı, resim benzeri içerik paylaşabilir, başka bir Tweet'i yineleyebilir (Retweet), Tweet'e cevap verebilir ve Tweet'i favorilerine ekleyebilirler.

3.1.5. Tumblr

Tumblr[5], 2007 yılında ABD'de kurulan bir sosyal ağ ve mikroblog platformudur. Hem web sitesi hem de mobil uygulamaları üzerinden ücretsiz olarak hizmet veren Tumblr'da; kullanıcılar oluşturdukları kendilerine ait blog sitelerinde, metin, fotoğraf, bağlantı, ses ve video ve ilgi alanlarıyla alakalı yazılarını paylaşabilmekte, diğer blog kullanıcıları ile sohbet edebilmekte, diğer blogları takip edebilmekte ve içeriklere yorum yapabilmektedir.

3.1.6. YouTube

YouTube[6], 2005 yılında PayPal firması eski çalışanları tarafından ABD'de kurulmuş dünyanın en yaygın ve popüler video paylaşım ve barındırma platformudur. 2006 yılında Google tarafından satın alınan YouTube'de, içerikler kullanıcılar tarafından oluşturulmaktadır. Ücretsiz şekilde üye olabilen kullanıcılar video yükleyebilmekte iken; üye olmadan videoları izlemek mümkündür. Hem web sitesi hem de mobil uygulamaları üzerinden hizmet veren YouTube'ye üye olan kullanıcılar izledikleri videoları değerlendirebilmekte ve aynı zamanda izlenen videolar hakkında yorum yazabilmektedir.

3.1.7. Vimeo

Vimeo[7], 2004 yılında bir grup film yapımcısı tarafından ABD'de kurulan bir video

2 https://tr.linkedin.com/
3. https://plus.google.com/
4 https://twitter.com/
5 https://www.tumblr.com/
6. https://www.youtube.com/
7. https://vimeo.com

paylaşım ve barındırma platformudur. Vimeo ismi hem İngilizce "movie" kelimesinin anagramıdır hem de İngilizce video ve me kelimeleri kullanılarak türetilmiştir. Vimeo'da ücretsiz şekilde belirli boyutlara kadar video yüklenebilmekte ve daha çok kullanım alanı, hızlı yükleme, yüksek video kalitesi gibi özellikleri kullanabilmek için ücretli sürümü satın alınabilmektedir.

3.1.8. Dailymotion

Dailymotion[8], 2004 yılında Fransa'da kurulan ücretsiz bir video paylaşım ve barındırma platformudur. Ücretsiz şekilde üye olabilen kullanıcılar video yükleyebilmekte iken üye olmadan videoları izlemek mümkündür.

3.1.9. Pinterest

Pinterest[9], 2010 yılında ABD'de kurulmuş; video ve fotoğraf paylaşımına imkân veren ücretsiz bir sosyal paylaşım platformudur. Pinterest ismi İngilizce "pin (iğneleme)" ve "interest (ilgi)" kelimelerinden türetilmiştir. Kullanıcılar ilgi alanlarına giren video ve resimleri bir ilan panosuna benzer şekilde oluşturdukları Pinterest panolarında paylaşabilmekte ve farklı kategorilerde listeleyebilmektedir. Pinterest paylaşımları görsel ağırlıklıdır. Kullanıcılar diğer kullanıcıları takip edebilmekte ve paylaşılan resimlere ve videolara yorum yapabilmektedir.

3.1.10. Instagram

Instagram[10], 2010 yılında ABD'de kurulmuş ücretsiz bir video ve fotoğraf paylaşım platformudur. Instagram'ın kurucu ortaklarından olan Kevin Systrom, daha önce Google'da Gmail ve Google Okuyucu (Google Reader) ürünleri üzerinde çalışmıştır. Instagram, 2012 yılında Facebook tarafından satın alınmıştır. Mobil cihazlardaki uygulaması üzerinden hizmet veren Instagram ile kullanıcılar telefonları ile çektikleri veya telefonlarına yükledikleri resimlere çeşitli görsel efektler uygulayabilmekte ve bunları Twitter, Facebook, Foursquare, Tumblr gibi sosyal medya mecralarından yayınlayabilmektedir.

3.1.11. Flickr

Flickr[11], 2004 yılında hizmete verilen ücretsiz bir resim ve video paylaşım ve barındırma platformudur. Flickr, 2005 yılında Yahoo firması tarafından satın alınmıştır. Hem web sitesi hem de mobil uygulamaları üzerinden hizmet veren Flickr'da ücretsiz üyelerin yükleyeceği içeriğin boyutu sınırlı olup ücretli üyelik ile sınırsız yükleme hakkı satın alınabilmektedir.

3.1.12. Snapchat

Snapchat[12], 2011 yılında hizmete alınan ve akıllı telefonlarda kullanılabilen kamera tabanlı ücretsiz bir sosyal ağ platformudur. Snapchat, kullanıcıların oluşturdukları kişi listesindekilere çektikleri fotoğrafları ve videoları gönderebildiği, gönderdiği dosyaların üzerine notlar ekleyebildiği ve hepsinden önemlisi gönderdiği dosyaların karşı tarafta ne kadar süre görüntülenebileceğini belirleyebildiği bir anlık mesajlaşma uygulaması olarak hizmet vermektedir.

8. http://www.dailymotion.com/tr
9. https://tr.pinterest.com
10. https://www.instagram.com
11. https://www.flickr.com
12. https://www.snapchat.com/

3.1.13. Reddit

Reddit[13], sosyal haberlerin paylaşıldığı ve tartışıldığı bir sosyal medya platformudur. Yeni mezun iki üniversite arkadaşı tarafından 2005 yılında ABD'de kurulmuştur. Reddit ismi, İngilizce "Read It" kelimelerinin birleşiminden oluşmaktadır. Kullanıcılar; yazı, haber, resim, video benzeri içeriklerin bulunduğu bağlantıları paylaşmakta ve diğer kullanıcılar da listelenen bu içerikleri oylayarak yayınlandığı sıralamayı yukarı veya aşağı doğru değiştirebilmektedir. Ayrıca; spor, eğlence, politika, haber benzeri ve şehir, ülke özelindeki listeler de takip edilebilmektedir. Reddit platformundaki içerikleri tüm kullanıcılar okuyabilirken sadece üye olan kullanıcılar yazabilmektedir. Üyelik ücretsizdir.

3.1.14. Foursquare

Foursquare[14], 2009 yılında ABD'de kurulmuş konum tabanlı bir mobil sosyal ağ platformudur. Foursquare, mobil cihazlar üzerindeki GPS teknolojisini kullanarak kullanıcıların bulunduğu konumlarda etraflarında olan mekanları (alışveriş, eğlence, yemek, okul, hastane vb.) görebilmesini ve inceleyebilmesini sağlamaktadır. Mobil cihazlardaki uygulaması üzerinden hizmet veren Foursquare'de kullanıcılar bulundukları mekanlarla ilgili tavsiyede bulunabiliyor, diğer tavsiyeleri okuyabiliyor, mekanlara puan verebiliyor ve aradığı mekan kriterine göre önerileri de görebiliyor. Ayrıca kullanıcılar ayarlar bölümünden Foursquare hesaplarını Twitter ve Facebook hesaplarına bağlayabilmekte ve aktivitelerini bu platformlarda da yayınlayabilmektedir.

13. https://www.reddit.com/
14. https://tr.foursquare.com

3.1.15. Blogger

1999 yılında yayına alınan Blogger[15] hizmeti, 2003 yılında Google firması tarafından satın alınmıştır. Google firması tarafından ücretsiz olarak sunulan Blogger, internetteki ilk blog platformu olup halen en popülerlerinden birisidir. İnternet kullanıcıları Blogger ile ücretsiz olarak istedikleri tema seçeneklerini kullanarak blog tasarımında bir web sitesi sahibi olabilmekte;k moda, sağlık, spor, siyaset, günlük yaşam benzeri kendi seçtikleri alanlarda kendilerini ifade edebilmekte ve kendi bireysel tercihleri doğrultusunda paylaşımlar yapabilmektedir.

3.2. Bölgesel sosyal medya araçları ve platformları

İnternetin küresel ölçekteki sosyal medya platformlarının yanında, belirli bölgelerin ve ülkelerin kullanıcı beklentileri ve ihtiyaçları doğrultusunda geliştirilmiş sosyal medya platformları da bulunmaktadır.

İnternet kullanıcılarının profil oluşturabildikleri ve arkadaşlarıyla iletişim kurabildikleri bir sosyal ağ platformu olan Rusya menşeili Odnoklassniki , 2006 yılında hizmete alınmıştır ve Facebook'un bir alternatifi olarak hizmet vermektedir.

15. https://www.blogger.com

Ayrıca 2006 yılında hizmete alınan sosyal medya platformu VKontakte de, Orta Asya ve Doğu Avrupa bölgelerindeki Rusça konuşan internet kullanıcıları arasında oldukça popülerdir. VKontakte platformunda, internet kullanıcıları Facebook'a benzer şekilde profil oluşturabilmekte, diğer kullanıcılar ile iletişim kurabilmekte, video ve resim paylaşabilmektedir.

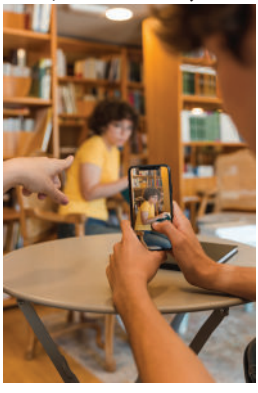
Latin Amerika'da Facebook ve Twitter en çok kullanılan sosyal medya platformları olmakla birlikte, belirli ülkelerde popüler olan birkaç bölgesel platform da mevcuttur. Twoo da (eski ismi Sonico'dur) , Latin Amerika bölgesindeki kullanıcılar tarafından tercih edilen bir sosyal medya platformudur. 2004 yılında Google firması bünyesinde kurulan Orkut platformu ise, başta Brezilya olmak üzere Latin Amerika bölgesinde oldukça popüler olan bir sosyal medya platformudur.

4. Sosyal Medyanın Birey ve Toplum Üzerindeki Etkileri

Sosyal medya günümüzde çok yoğun bir şekilde kullanılmaktadır. İletişim, paylaşım, bilgiye ulaşma, eğlenme, oyun ve e-ticarete kadar çok çeşitli amaçlar için kullanılan sosyal medyanın temel dinamiğini, yapılan "paylaşımlar" oluşturmaktadır. Paylaşım burada önemli bir kelime olarak karşımıza çıkmaktadır. Gerçek hayattaki "paylaşmanın" karşılığı olamayan bu faaliyetler aslında görünmenin bir karşılığıdır. Göründükçe yani paylaştıkça var olunan sosyal paylaşım platformları, bağımlılık, zamanın bilinçsiz kullanılması, sanal zorbalık, tüketim ve yaşam alışkanlıklarının sorgulanması ve Türkçe'nin giderek bozulması gibi bir takım riskler taşımaktadır.

Sosyal medya ile fazlaca iç içe olma durumu, bireysellik, sosyal normlara uyum, ahlaki tavır ve tutum, tüketim alışkanlıkları, sorumluluk duygusu gibi birçok açıdan bireyi yakından ilgilendirmektedir. Vaktinin tamamını sosyal medyada geçiren bir birey, sorumluluk duygusunu zedelemiş ve günlük hayatın akışında yapması gereken diğer bütün işlerini ihmal etmiştir. Sosyal paylaşım platformları zamanla bireylerde; bağımlılık, şiddet eğilimi, bencillik, narsisizm, amaçsızlık, sosyal hayattan kopukluk gibi olumsuz durumlar oluşturabilmektedir. Özellikle sosyal medya ile yaygınlaşan ve "moda" olan çeşitli oyunlar ve akımlar çocukların ve gençlerin önce psikolojilerini sonra da hayatlarını olumsuz yönde etkileyebilmektedir. Bunun en yakın örneği dünyada yüzden fazla kişinin hayatını kaybetmesine sebep olan Mavi Balina'dır.

Bir taraftan bu çağa, yani İnternet çağına özgü yeni nesil hastalıklar türerken, bir taraftan da çocuklara bedensel ve ruhsal olarak ciddi zarar veren durumlar yaşanabilmektedir. Bilgi ve iletişim teknolojilerinin büyük bir hızla ilerlemesi bireyleri teknolojiye mecbur kılarken bireylere düşen teknolojiyi, bilgi ve iletişim kaynaklarını doğru ve bilinçli bir şekilde kullanmak ve bunu yeni nesillere aktarmak olmalıdır. Ge-



lecek kuşakların teknoloji bağımlısı, doğaya, kendine ve gerçek hayata uzak, tüketim ve haz odaklı, kuralsız bir kuşak olmaması için, toplum olarak önlemler alınmalı; teknoloji ve internetin doğru kullanımı noktasında genç nesillere yol gösterici olunmalıdır. En önemlisi de sevgi, saygı, sorumluluk ve bilinç gibi erdemlerin, bilgiden ve teknolojiden çok daha önemli olduğu yeni kuşaklara anlatılmalıdır.

Sosyal medyanın aşırı kullanımı özellikle genç nesli gerçek hayattan izole edip yalnızlaştırırken, vaktin kontrolsüzce geçirilmesine de sebep olmaktadır.

Duygu ve düşünceleri ifade etmenin en kolay yolu olarak kabul edilmesi, gerçek hayatta kurulamayan ilişkilerin daha rahat kurulabilmesine imkân sağlaması, eğlenmek, sosyalleşmek ve özellikle harcanabilir gelir düzeyinin azlığı sebebiyle internete mecbur kalma gibi faktörler bugün insanları günümüzün kitle iletişim medyasından biri olan sosyal medyaya bağımlı kılmaktadır. Sosyal medya, sıradan insanlara bilgiyi paylaşma ve organize etme olanağı sağlamıştır.

Yapılan araştırmalarda, internetten alışverişi tercih eden bireylerin, markaların internet reklamlarına yoğun bir ilgi gösterdikleri ve bu tavrı sosyal medya üzerinden devam ettirdikleri görülmüştür. Bu noktada sosyal medya kullanırken kişisel bilgileri koruma açısından dikkatli ve bilinçli olunmadığı takdirde çeşitli dolandırıcılık olaylarının yaşanması ihtimali akıllarda tutulmalıdır.

4.1. Siber zorbalık

Siber zorbalık; elektronik ortamda bir birey veya grubun, başkalarına yönelik kasıtlı, tekrarlayan; aşağılama, iftira, dedikodu, nefret, taciz, tehdit, utandırma, dışlama, küçük düşürme, müstehcen içerikler yollama yoluyla, psikolojik ve sosyal yönden rahatsız edici, olumsuz davranışlarda bulunma eylemlerini ifade etmektedir.

Siber zorbalık çok çeşitli biçimlerde ortaya çıksa da ergenler arasında yaşanan siber zorbalığın genellikle sosyal paylaşım platformları üzerinden yapıldığı görülmektedir.

Bir öğrencinin fotoğrafından sadece yüzünü kesip başka bir pornografik fotoğrafa yapıştırmak, bireye ait özel bilgileri çalmak ve bunları sosyal paylaşım sitelerinde yayınlamak sanal zorbalığın örneklerindendir. Sosyal medya ortamlarında, birey (kurban) hakkında karalayıcı, hakaret eden ve aşağılayıcı içeriklerin servis edilmesi, kameralı cep telefonları aracılığıyla kurbanların görüntülerinin çekilmesi, çirkin, şişko, aptal, tembel gibi lakaplar ile yorumlarda bulunulması sosyal medyada yaşanan siber zorbalığın türleridir. Bu yollarla siber zorbalar, kurbanlarını utandırmak, aşağılamak, dışlamak, itibarsızlaştırmak ve yalnızlaştırmaya çalışırlar.

4.2. Türkçe'nin doğru kullanımı

Dijitalleşme süreci, her alanda olduğu gibi iletişim ve dil alanında da toplumu hızla dönüştürmektedir. İnternette ve özellikle sosyal medyada iletişim faaliyetlerinin giderek yaygınlaşması, kullanıcılar arasında yeni bir dilin oluşmasına sebep olmuştur. Söyleşi Dili veya Sanalca olarak adlandırılan bu yeni dil Türkçe'yi farklı boyutlarda ve çeşitli yönlerden etkilemektedir.

Özellikle sosyal medyada, gençler arasında giderek yaygınlaşan bu dilin oluşmasına etki eden faktörlerden bazıları; internetin giderek yaygınlaşması, iletişim hızı ve hızlı yazma kaygısı, yabancı dillerin etkisi, konuşma dili, bilgisayar ve internetin getirdiği yeni ifadeler-semboller ve bu sembollerin kullanım pratikleri, söyleşi jargonu, eğitimdeki eksiklikler olarak sayılabilir.

Sosyal medyanın olmazsa olmazı haline gelen bu sanal dil, imla kurallarının ve noktalama işaretlerinin olmadığı, kelimelerin eksik, yanlış, argo ve basit bir şekilde kullanılmasıyla oluşmaktadır. Özellikle dijital yerliler için Türkçe'nin doğru kullanılmasının önündeki en büyük engellerden biridir. Teknoloji ile iç içe büyümüş bu neslin kullandığı kelimelerden bazı örnekler aşağıdaki gibidir:

Merhaba: mrb, Selam: slm, Olmaz: Olmas, Teşekkürler: tşk, Ne yapıyorsun: Napion, Canım: Cnm, N'aber: Nbr, Söyleyeceğim: Sölücem, İyiyim: iiiii, Tamam: Ok, Zaman: Zmn, Allah Razı Olsun: ARO

Kelimeler, duyguları ve düşünceleri ifade etmek için kullanılır. Eksik ve yanlış kullanılan kelimeler, bireylerin düşünce ve zihin dünyasında da eksikliklere ve yanlış anlaşılmalara sebebiyet verir. Anlamları tam karşılamayan, derinlikten yoksun ve yamalı bir iletişim dili, zamanla edebiyata, kültür ve sanata, eğitime, sosyolojiye ve psikolojiye varana dek pek çok alana yansıyacak ve topluma zarar verecektir.

Teknoloji hiçbir mecrada ve hiç kimseyi belli bir dil kalıbına sokmamalıdır. Bizler kendimizi, hayatımızı ve eşyayı kelimelerle anlamlandırırız. Dil kültürdür, dil bir medeniyeti oluşturan ve devam etmesini sağlayan en önemli unsurlardan biridir. Dili oluşturan kelimeler, her nerede kullanılırsa kullanılsın kısaltmadan, değiştirmeden ve doğru bir şekilde kullanılmalıdır.

"Merhaba" demek yerine "mrb" demek, dil suikastı yapmak olur. Gerçek hayatta kullanılmayan anlamsız ve yapay bir dil internet ortamlarında da kullanılmamalıdır.

4.3. Sosyal medya ve kişisel veriler

Sosyal medya, kullanıcıların yaptığı paylaşımlar, yorumlar ve medya içerikleri ile varlıklarını sürdürmektedirler. Kullanıcılar sosyal medyada, düşüncelerinden, duygu durumlarına, ilgi alanlarından, kişisel eğilimlerine kadar nerdeyse her bilgiyi paylaşmaktadırlar. Yapılan bu paylaşımlar kişiler hakkında önemli ve detaylı bilgiler içermektedir.

Sosyal medyanın bu şekilde kullanımı beraberinde bir takım riskleri ve tehlikeli durumları da beraberinde getirmektedir. Fotoğraf, video, yer ve konum bilgisi ve her türden kişisel verinin paylaşıldığı sosyal medya platformlarını bilinçli ve güvenli kullanmanın önemi burada bir kez daha anlaşılmaktadır.

Sosyal medyadaki güvenlik açıklıklarının temel nedeni mahremiyetin korunamaması ve kullanıcıların kişisel bilgilerini paylaşarak kendilerini bu ortamda hedef haline getirmeleridir. Ayrıca sosyal medyada hızlı bir şekilde yayılmaya devam eden, sayısız güvenlik açığı içeren 3. Parti uygulamaların kullanılmasına izin verilmesi kişisel bilgilerin kötü niyetli kişilerin eline geçmesine de neden olabilmektedir. Gerek sosyal medyadaki uygulamaların gerekse kaynağı belli olmayan internet ortamından indirilen uygulamaların, gereğinden fazla kişisel veri talep ettiği bilinmekte, bu uygulamalara karşı da dikkatli olunması gerekmektedir.

Sosyal medya ile birlikte kullanılan uygulamalar konusunda güvenlik bilinci arttıkça alınacak güvenlik önlemleri de artmaktadır. İnternet kullanıcılarının, kişisel verilerini korumak için kullandıkları sosyal medya platformlarında aşağıdaki hususlara özen göstermesi faydalı olacaktır:

- Kullandığınız sosyal medya platformlarının kullanım politikası ve gizlilik sözleşmelerini okuyun.
- Sosyal medyada gizlilik ve güvenlik ayarlarınızı gözden geçirin.
- Sosyal medyadaki hesaplarınıza olan erişimi tanıdığınız ve güvendiğiniz kişilerle sınırlayın.
- Özel ve kişisel bilgilerinizi asla paylaşmayın.
- Doğum tarihiniz, doğduğunuz yer, telefon numaranız gibi kişisel bilgilerinizden oluşan kolay tahmin edilebilir şifreler yerine en az 8 karakterden oluşan, hem küçük hem büyük karakterler içeren tahmin edilmesi zor güçlü şifreler belirleyin.
- Sosyal medya platformlarına akıllı telefonunuzdan erişiyorsanız, telefonunuzun ayarlar bölümünden uygulamalarınıza verdiğiniz erişim izinlerini kontrol edin, gereksiz veya riskli olduğunu bulduğunuz izinleri kaldırın.

- Sosyal medya platformları üzerinden yaptığınız paylaşımların, milyonlarca kişiye erişebileceğini unutmayın ve paylaşımlarınızı bu bilinç ile yapın.
- İnternete erişim hakkınızı kullanırken, başkalarının haklarını gözetme sorumluluğunuzu unutmayın.

Kullanılan uygulamaların güvenlik, erişilebilirlik ve gizlilik politikalarını sürekli gözden geçirerek verilen izinleri sorgulayın.

4.4. Ebeveynlere tavsiyeler

Ebeveynler çocukları ile güven temelli, güçlü ilişkiler tesis etmelidir. Ebeveynler durumu yok saymayan, abartısız ve makul yaklaşımlarla konuya eğilmelidir. Ebeveynler çocukları ile sosyal medya, dijital güvenlik ve internette karşılaşabilecekleri dijital tehlikeler hakkındaki güncel olayları konuşmalı ve bilgilendirmelidir. Sanal ortamda, gizli ve daha çok psikolojik taktiklerle yaşanması sebebiyle elektronik zorbalığın farkında olunmalı ve bu gizli tehlike ebeveynler ve eğitimciler tarafından ciddiyetle takip edilmelidir.

5. Sosyal Medyanın Etik Boyutu

Etik ile ahlak kavramı çoğu zaman birbirine karıştırılır. Etik, doğru ve yanlış eylemin teorisi, ahlak ise onun pratiği gibi düşünülebilir. Bireylerin sosyal medya üzerinden gerçekleştirdikleri bütün etkileşimlerde tıpkı gerçek hayatta olduğu gibi dürüstlük, nezaket, kişi haklarına saygı ve duygudaşlık gibi erdemlere uyması beklenmektedir.

Sosyal medya platformlarına etik ve ahlaki değerlere uygun kullanmak için asgari olarak aşağıda sıralanan hususlara dikkat edilmesi gerekmektedir.

» İnternetin erişim, iletişim ve içerik olanaklarından olabildiğince faydalanınız. İnternet teknolojilerinin getirmiş olduğu fırsatları kaçırmayınız.

» İnternette kendinizi doğru bir şekilde ifade ediniz. İfade özgürlüğü hakkınızı kullanınız; yalnız bu hakkı kullanırken başkalarının haklarını çiğnemeyiniz.

» Başkalarını incitici ve rahatsız edici davranışlardan sakınınız. Zorba olmayınız, zorbalığa müsaade etmeyiniz.

» Başkalarının haklarına saygılı olunuz. Kimsenin kişiliğini ve itibarını zedeleyici davranışlarda bulunmayınız.

» Başkalarının internette sergilediği hoşunuza gitmeyen davranışlara karşı hoşgörülü olunuz, gerekirse ilgili kişiyi onu küçük düşürmeden ve özel bir iletişim kanalı ile uyarınız.

» İnternette ve özellikle sosyal medyada başkalarına karşı her zaman kibar bir dil kullanınız ve saygılı davranınız.

» Fikri mülkiyet haklarının internette de korunmasına özen gösteriniz.

» Gerçek hayatta suç olan her şey internette de suçtur.

» Gerçek hayatta başkalarına karşı söyleyemeyeceğiniz veya söylenmesi uy-

gun olmayan sözleri, internette de söylemeyiniz.

» Gerçek hayattaki sorumluluk bilincinizi internette de sürdürünüz.

» Gerçek hayatta size karşı yapılması hoşunuza gitmeyen davranış ve hareketleri siz de başkalarına yapmayınız.

» İnternette paylaştığınız bilgilerin kolay kolay geri alınmayacağını ve ardınızda silinmez izler bırakabileceğini unutmayınız.

» İnternette, sonradan pişman olabileceğiniz ve sizi etkileyebilecek paylaşımlar yapmayınız.

» İnternetin fiziksel ve ruhsal sağlığınızı bozmasına müsaade etmeyiniz, zamanınızı boşa harcamayınız. İnterneti doğru zaman, yer ve miktarda kullanmaya özen gösteriniz.

» İnternette güvenilir, doğru ve başkalarına fayda sağlayacak içerik ve bilgiler üretmeye gayret gösteriniz.

» İnternette bilgi sahibi olduğunuz konularla ilgili paylaşımcı olunuz. Başkaları ile bilgi alışverişi yapınız

» İnternette okuduğunuz her bilginin kaynağını araştırınız; sörf yapmayınız dibe dalınız.

» Doğruluğundan emin olmadığınız hiçbir bilgiyi internette paylaşmayınız. Gerekirse farklı kaynaklardan araştırarak teyit ediniz, eleştirel olunuz.

» Öncellikle kendinizi eğitiniz, interneti kullanımını öğreniniz. Bilinçli ve iyi birer dijital vatandaş olmaya özen gösteriniz.

» İnternet ortamında hak ve sorumluluklarınızı biliniz, internet ve bilişim ile ilgili yasal düzenlemeler hakkında bilgi edininiz.

6. Sosyal Medya Ne Kadar Güvenli?

Günümüz bilgi teknolojileri çağının en büyük sosyalleşme aracı sosyal medya platformlarıdır. Sosyal medya platformları artık internet teknolojilerini kullanan çoğu birey tarafından kullanılmaktadır. İnternet kullanıcıları sosyal medya ve sosyal medyanın sunduğu hizmetleri günlük hayatlarının bir parçası olarak benimsemesinden dolayı sosyal medya, kullanıcılar için farklı güvenlik ve gizlilik tehlikeleri de oluşturabilmektedir. Sosyal medya sahte hesaplar, üçüncü parti uygulamalar, oltalama yoluyla yönlendirmeler, yanlı/yalan haberler ile birlikte çeşitli iletişim riskleri gibi birtakım internet risklerine daha da kapı aralamıştır.

Sosyal medya kullanıcıları maalesef bu platformlarda çok fazla bilinçli değillerdir.

Yalan haberlere çok çabuk kanıp bunu rahatlıkla paylaşıp daha da yayılmasına sebep olabilmektedirler. Veya hangi ünlüye benziyorsun? Profiline en uygun meslek hangisi? gibi oltalama içeren üçüncü parti uygulamalar ile kişisel bilgi güvenliklerine ciddi zararlar verebilmektedirler.

Üçüncü partiler telefonları dinlemeden kamera ve rehberlere erişime kadar birçok zararlı faaliyet ile kişinin özeline rahatlıkla erişebilmektedir. Çevrimiçi topluluğun önemli bir bölümünün bu tarz uygulamaları kullanması, bu uygulamalar ile ilgili güvenliymiş imajı verse de durum tam tersidir.

Sosyal medyada kullanıcıların farkında olmadığı diğer önemli bir risk ise büyük veri ve bu verinin getirdiği veri madenciliği riskidir. Maalesef kullanıcılar bu noktada da oldukça bilinçsiz durumdadır. Günümüz iletişim teknolojilerinin geldiği nokta ile kullanıcılar farkında olmadan paylaşmadığını zannettiği birçok bilgiyi sosyal medya da rahatlıkla paylaşabilmektedir. Örneğin atılan tweet'ler ile konumunuzu belirtmeseniz bile konumunuz tespit edilebilmektedir. Zevkleriniz, tercihleriniz veya beğenilerinizin analizi ile internet kullanıcılarının aklına gelmeyen birçok bilgi elde edilebilmektedir. Kullandığınız dil üslubu hangi siyasi partiye yakın olduğunuzu ortaya çıkarabiliyor. Meta veri analizleri ile paylaştığınız resim ve videoların nerede çekildiği çok rahatlıkla tespit edilebiliyor. Yine sosyal medya eklentileri kullanıcı tercihleri ve internete gezinme davranışları ile ilgili bilgiler sunabilmektedir.

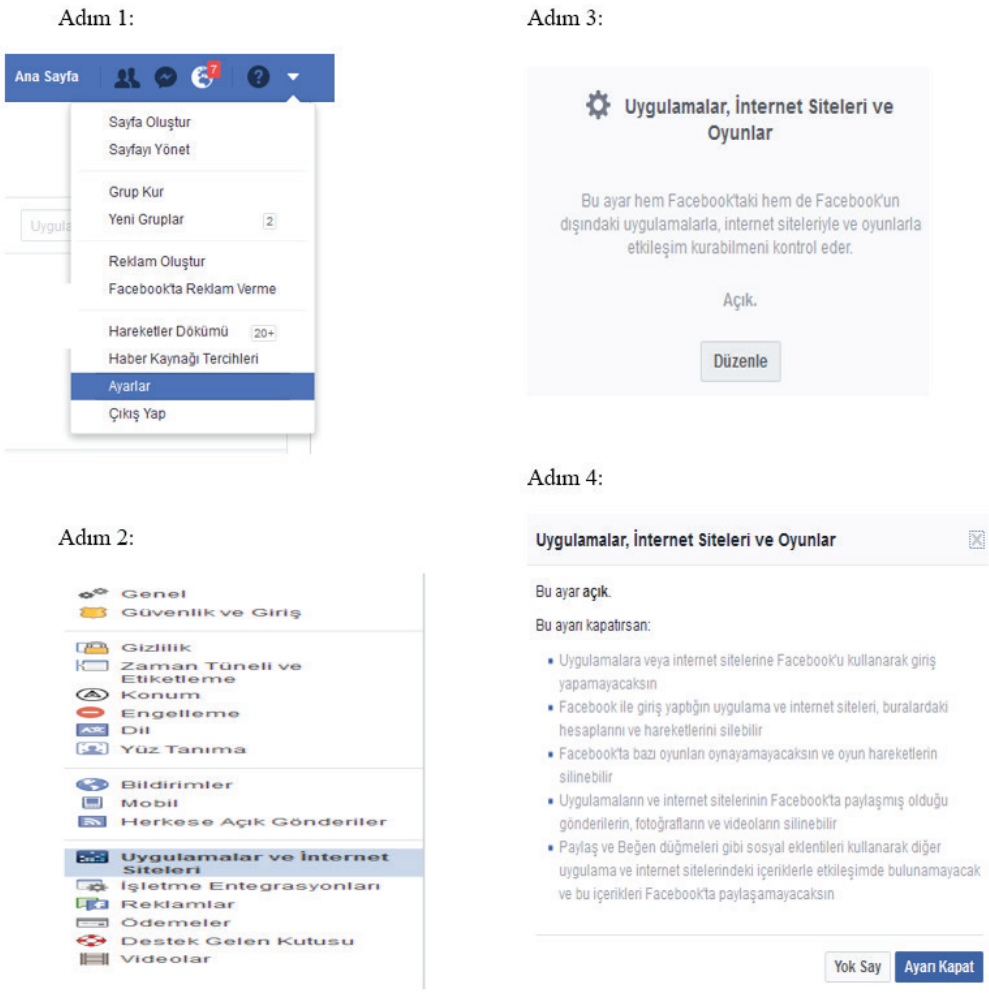
Sosyal medyada diğer önemli risk grubu ise mobil uygulamalardır. Mobil uygulamaların sahip olduğu yetkilendirmeler ile rehberinizden SMS'lerinize; konum bilginizden internet trafik bilginize kadar geniş bir yelpazede bilgileriniz çok rahatlıkla erişim izinleri ile alınabilmektedir. Sosyal medya platformlarının mobil uygulamaları da bunu yapabilmekle birlikte birçok uygulamada benzer problemler göze çarpmaktadır.

Sosyal medyada üzerinde durulması gereken diğer önemli bir konu başlığı "ortak arkadaşlar" problemidir. Maalesef bugün Facebook başta olmak üzere arkadaşlık üzerine kurulmuş sosyal medya platformlarında sahte veya ele geçirilmiş hesaplar, oltalama amacı güden paylaşımlar veya 3. parti uygulamalar "ortak arkadaşlar" özelliği çok sayıda kişiye kısa bir sürede ulaşarak siber suçlara kapı aralayabilmektedir.

7. Sosyal Medyayı Ne Kadar Güvenli Hale Getirebiliriz?

Sosyal medyayı güvenli hale getirmek büyük olasılıkla kullanıcıların elindedir. "Ortak arkadaşlar" gibi kullanıcıların kısıtlayamadığı bazı özellikler hariç kullanıcıların yapacağı gizlilik ve güvenlik ayarları ile birlikte en önemli konu bilinçlenmedir.

Kullanıcılar bilinçlenmediği sürece ne kadar teknik önlem alırsa alsın birtakım risk ve tehlikelerin odağında olacaktır. Örneğin bugünün ebeveynleri çocuklarına ait birçok içerik ve görseli sosyal medyada rahatlıkla masumane bir şekilde paylaşmaktadır. Paylaştıkları içerikler yukarıda sayılan riskler



Şekil 3 – Facebook 3. Parti Uygulama İzinlerini Kapatma Süreci

de gözetildiği zaman ne gibi problemlere yol açabileceğini kestirmek zordur. Ayrıca bugünün risklerinden çocuk istismarı başta olmak üzere bu büyük verinin o çocuk üstünde yıllar sonra ortaya çıkarabileceği bilgi kirliliğini hesap etmek çok zordur. Bununla birlikte özel yaşantımız, ev veya işyerimize ait görseller, özel zevk ve tercihlerimiz, sorun ve problemlerimiz, düşünce yapımız gibi kişiye özel kalması gereken bilgiler ile kişisel verilerimiz (gerçek doğum tarihi, adres, cep telefonu, dayı ve teyze ilgilerinden yola çıkacak kızlık soyadı vs.) internet ve sosyal medyada paylaşılmamalı ve bu konudaki etkileşimlerden (beğeni, yorum, paylaşım, eklenti, uygulama vs.) uzak durulmalıdır.

Sosyal medyada en önemli güvenlik aracı paylaşımlarımızı kontrol etmektedir. Neyi ne amaçla paylaştığımızı iyi bilmemiz gerekmektedir. Bununla birlikte de sizler için 10 temel önlem belirledik. Bu önlemleri sıralamak gerekirse;

1. Üçüncü parti uygulamalara hesap erişim izinleri tamamen kapatılmalıdır. Örneğin Facebook için aşağıdaki şekilde yer alan süreçleri izleyebilirsiniz veya https://www.facebook.com/settings/?tab=applications adresine gidebilirsiniz. Benzer şekilde Twitter için https://twitter.com/settings/connections; Google için https://security.google.com/settings/security/permissions?pli=1 Instagram için https://instagram.com/accounts/manage_access; Linkedin için https://www.linkedin.com/secure/settings?goback=.aas&userAgree= adresine giderek benzer işlemleri tamamlayabilirsiniz.

2. Şifre güvenliği ile birlikte farklı sosyal medya hesaplarında farklı şifreler kullanımına özen gösterilmeli. Ayrıca hesabınıza erişim sağlamaya çalışan saldırganlar için şüpheli durumlarda bildirim alınması ile birlikte sosyal medya platformları ile bu gibi durumlar için bizimle irtibat kurabilmeleri için doğru bir e-posta adresi ve cep telefonu numarası paylaşmaya özen göstermeliyiz. İki adımlı doğrulma da diğer bir güvenlik tedbiridir.

3. Bilgi gizliği ve güvenliğine dikkat edilmelidir. Örneğin Facebook'ta "Paylaştıklarımı kimler görebilir?" "Benimle kimler iletişim kurabilir?" "Aramada beni kimler bulabilir?" "Zaman tünelimdeki şeyleri kimler görebilir?" İnsanların eklediği etiketleri ve etiketleme önerilerini nasıl yönetebilirim?" gibi ayarlamalar yapılmalıdır (Yukarıdaki şekilde yer alan Adım 2'de yer alan Gizlilik, Zaman tüneli ve etiketleme ayarları). Benzer şekilde Twitter'da "Tweet gizliliği" "Tweet konumu" "Fotoğraf etiketleme" "Keşfedilebilirlik" "Kişiselleştirme" ve "Sponsorlu içerik" gibi ayarlar yapılmalıdır (Profil görseline tıkla – Ayarlar ve gizlilik - Gizlilik ve güvenlik).

4. Mobil sosyal ağlardan mobil rehber bilgilerinizi kaldırabilirsiniz. Bunun için örneğin Facebook için https://www.facebook.com/contact_importer/remove_uploads.php adresine giderek tüm kişileri silebilirsiniz ama bu kalıcı bir yol değildir. Kalıcı hale getirmek için;

Android için Facebook:

1. ☰ simgesine dokunun.
2. Ayarlar ve Gizlilik'ten Uygulama Ayarları'na dokunun.
3. Sürekli Kişi Yüklemesi'ne dokunarak ayarı kapatın.

iPhone veya iPad için Facebook:

1. ☰ simgesine dokunun.
2. Ayarlar > Hesap Ayarları > Genel'e dokunun.

3. Kişileri yükle'ye dokunarak ayarı kapatın.

Benzer süreci Twitter için Profil görseline tıkla – Ayarlar ve gizlilik – Arkadaşlarını Bul - Dilediğin zaman adres defterinden yüklediğin kişileri yönetebilirsin basamaklarını kullanarak yapabilirsiniz.

5. Ağınızdaki arkadaşlarınızdan gelen alışılmış olağan görünümün dışında gelen mesajlar asla açılmamalı. Çünkü bu tip mesajlar arkadaşlardan geliyor gibi gözükse de, aslında onların hesaplarını ele geçiren saldırganlar veya saldırıya uğramış hesaplardan size ulaşıyor olabilir.

6. Gelişmiş oltalama saldırılarına dikkat edilmelidir. Geleneksel sosyal mühendislik ve oltalama saldırıları basit spam, kısaltılmış URL'ler veya zararlı reklam ağları ile yapılabilmekteyken kullanıcıların daha da bilinçlenmesi ile zararlı yöntemler de gelişti. Örneğin; CSRF (Cross-Site Request Forgery) saldırıları sahte istekler ile gerçekleştirilerek kullanıcının gözünden kaçabilir. Veya XSS (Cross Site Scripting) Exploitleri genelde siteler ile uygulamaların kod yapılarının suistimali yoluyla yapılır. Bunun için sosyal medyahesapları ile birlikte tarayıcı güvenliği ve gizliliği de ön plana çıkmaktadır.

7. Sosyal medya eklentileri ve mobil uygulamaların hangi erişim izinleri istedikleri iyi analiz edilmelidir. Bir tuşa basıp geçilmemelidir.

8. İnternet güvenliği adımları sosyal medyadaki güvenlik için de geçerlidir. İnternet güvenlik yazılımları kullanılmalı, halka açık internet ağlarından hesap girişleri gerçekleştirilmemeli, tarayıcı ve virüs yazılımlarınız güncel tutulmalıdır.

9. Sosyal medyada gizlilik ve güvenliğinizi kontrol eden önemli araçlar da vardır. Minor Monitor, Anti forced like, Secretbook ve Trend Micro Sosyal Ağ Koruması gibi programları deneyebilirsiniz.

10. Sadece ihtiyaç olduğu zaman değil risklerden korunmak için de ara ara sosyal medya platformlarının yardım merkezini ziyaret edip bilgi alınız ve herhangi bir olumsuzluğu bu platformlara anında rapor ediniz.

Facebook için: https://www.facebook.com/help/

Twitter için: https://help.twitter.com/tr

Instagram için: https://help.instagram.com/

Linkedin için: https://www.linkedin.com/help/linkedin?lang=tr

Google için: https://support.google.com/?hl=tr

8. Sosyal Medya Platformları İhbar Süreçleri

Sosyal medya platformlarının kullanımı genişledikçe sosyal medya platformlarının ihbar ve raporlama süreçleri de gelişmektedir. Sosyal medya araçları genellikle yurtdışı kaynaklı platformlar oldukları için sosyal medya ile ilgili şikâyet ve itirazların genellikle bu platformlara yapılması süreci ve alınacak sonuçları da hızlandırmaktadır.

Sosyal medya platformları kullanıcılar tarafından sıklıkla kullanılmasına rağmen maalesef sadece ihtiyaç halinde bu platformların güvenlik ve yardım merkezleri kullanılmaktadır. Mesela Facebook'un hem de Türkçe hem Emniyet Merkezi hem de Zorbalığı Önleme Merkezi bulunmaktadır.

Facebook Güvenlik Merkezi, gençler, aileler ve öğretmenler için çeşitli tavsiyelerde bulunmaktadır: https://www.facebook.com/safety

Zorbalık Önleme Merkezi'nin de tavsiyeleri ve kaynakları vardır: https://www.facebook.com/safety/bullying

Bunumla birlikte Facebook Yardım Merkezi'ni kullanarak Facebook ile ilgili bir konuda yardım alabilirsiniz:

https://www.facebook.com/help/

Facebook'ta şikâyet etmek istediğiniz bir profil için:

1 Şikâyet etmek istediğiniz profile gidin

2. Kapak fotoğrafının sağ altındaki ••• simgesine tıklayın ve **Bu gönderi ile ilgili görüşlerini bildir**i seçin

3. Profildeki zararlı içerik kategorisini seçip gönderi tuşlayın.

Profil dışında diğer tüm genel şikâyetler için şu linki kullanabilirsiniz:

https://www.facebook.com/help/report-links

Bununla birlikte sizler için sıklıkla kullanılan tüm sosyal medya platformlarının güvenlik araçları ve raporlama seçeneklerini Güvenli Web sitesinde Sosyal Medya Rehberi adı altında toplamaya çalıştık. Ayrıca Youtube ve Twitter için içerik şikâyet sürecini aşağıdaki bağlantıda yer alan videolardan izleyebilirsiniz:

Youtube için;
http://www.guvenliweb.org.tr/galeri-detay/youtube-icerik-sikayet-sureci

Twitter için;
http://www.guvenliweb.org.tr/galeri-detay/twitterda-icerik-sikayet-sureci

Kaynak: http://www.guvenliweb.org.tr/sosyal-medya-rehberi

9. Bölüm Kazanımları

Bu bölümde öncelikle, sosyal medya deyince akla ne geliyor, sosyal medya platformları neler ve sosyal medyanın kısa tarihçesi gibi konulardan bahsedilerek internet kullanımımızda en önemli yeri tutan sosyal medya ve bileşenlerine kısa bir bakış yapılmıştır. Popüler sosyal medya araçlarından bahsedildikten sora sosyal medyanın birey ve toplum üzerindeki etkileri analiz edilmiştir. Bu etkiler ve sosyal medya platform-

larında sıklıkla karşılaşılan olumsuzluklardan bahsedildikten sonra ebeveynlere konu ile ilgili çeşitli tavsiyelerde bulunulmuştur.

İlerleyen bölümlerde, sosyal medyanın etik boyutu incelenmiştir. Sosyal medya kullanımına bağlı etkileşim ve sosyalleşme kanallarında hangi etik değerlere bağlı kalınması gerektiği özetlenmiştir. Daha sonra sosyal medyanın ne kadar güvenli olduğu ve kullanıcılar tarafından ne kadar güvenli hale getirilebileceği örneklerle birlikte incelenmiştir. En son bölümde de birçok internet kullanıcısının sosyal medya platformlarında gizlilik ve güvenlik ihlalleri başta olmak üzere karşılaştıkları risklere ilişkin ihbar süreçlerini nasıl yönetmeleri gerektiği yine örneklerle sunularak internet kullanıcılarının farkındalıklarının artırılması hedeflenmiştir.

KAYNAKLAR:

AKSÜT, Mehmet - Zekeriya Batur – Tülin Avşar (2006), "Sanalca, Sanal Odalarda (İnternet) İletişim ve Türkçe", Akademik Bilişim Konferansında Sunulmuş Bildiri, Pamukkale Üniversitesi, Denizli.

Boyd,M.D. ve Ellison,B.N., (2007). Social Network Sites: Definition, History, and Scholarship, Michigan State University, Department of Telecommunication, Information Studies, and Media

ÇAKIR, Hamza – Hakan Topçu (2005), "Bir İletişim Dili Olarak İnternet", Sosyal Bilimler Enstitüsü Dergisi, S. 19, s. 71–96.

Facebook'ta Yapılan Siber Saldırılar ve Korunmanın Yolları,

URL: https://www.sibergah.com/genel/sosyal-medya-guvenligi/facebook-ta-yapilan-siber-saldirilar-ve-korunmanin-yollari/, Son Erişim tarihi, 29.05.2018.

Güvenli Web, Bilgi Teknolojileri ve İletişim Kurumu,

URL: http://www.guvenliweb.org.tr/blog-detay/kusak-farki-ve-sifir-kusagi-tehlikesi, Son Erişim tarihi, 08.08.2018.

Güvenli Web, Bilgi Teknolojileri ve İletişim Kurumu,

URL: http://www.guvenliweb.org.tr/dokuman-detay/siber-zorbalik, Son Erişim tarihi, 09.08.2018.

Güvenli Web, Bilgi Teknolojileri ve İletişim Kurumu,

URL: http://www.guvenliweb.org.tr/dokuman-detay/internet-etigi, Son Erişim tarihi, 09.08.2018.

Social Networking: A Guide to Strengthening Civil Society Through Social Media, URL: https://www.usaid.gov/SMGuide4CSO, Son Erişim tarihi, 15.08.2018.

Sosyal Ağların Tehditlerini Önlemeye Yardımcı Araçlar

URL: https://www.sibergah.com/genel/sosyal-medya-guvenligi/sosyal-aglarin-tehditlerini-onlemeye-yardimci-araclar/, Son Erişim tarihi, 29.05.2018.

The History of Social Media: Social Networking Evolution!,

URL: http://historycooperative.org/the-history-of-social-media/, Son Erişim tarihi, 17.06.2018.

The history of social networking,

URL:https://www.digitaltrends.com/features/the-history-of-social-networking/, Son Erişim tarihi, 17.06.2018.

The History of Social Media,

URL: https://www.future-marketing.co.uk/the-history-of-social-media/, Son Erişim tarihi, 17.06.2018.

YAMAN, Havva – Yavuz Erdoğan (2007), "İnternet Kullanımının Türkçe'ye Etkileri: Nitel Bir Araştırma", Journal of Language and Linguistic Studies, Vol. 3, No. 2, s. 237-249.

Çocuklar, İnternetteki Güvenliğiniz İçin 5 Altın Kuralı Takip Edin

Tanışma

Unutma, onlarla uzun süredir sohbet ediyor olsan bile internetteki arkadaşların halen birer yabancıdır.Tanımadığın insanların niyetini bilemezsin ve zarar görebilirsin. İnternetten kimseyle asla tanışma ve görüşme, tanımadığın kişilerin arkadaşlık tekliflerini kabul etme.

Ailene Anlat

Eğer internette bir kişi veya bir şey seni rahatsız ediyor veya üzüyorsa ailene anlat. İnternette yaşadığın tüm olumsuzlukları ailene çekinmeden anlatmalısın.

Kabul etme

Tanımadığın ve güvenmediğin insanlardan gelen e-posta, mesaj, resim veya dosyaları kabul etme ve açma çünkü virüsler veya hoşuna gitmeyen mesajlar içeriyor olabilir.

İnanma

İnternette konuştuğun kişiler, kim oldukları hakkında sana yalan söylüyor olabilirler, herkese inanma. İnternette sohbet etmek istiyorsan, bunu yalnızca gerçek hayattaki arkadaşların veya ailenle yapmak en iyisidir

Paylaşma

İnternette kişisel bilgilerini vermemeye dikkat et. Bulunduğun yeri, telefonunu, şifreni asla kimseyle paylaşma ve güvende kal.

www.gim.org.tr | www.guvenliweb.org.tr

GÜVENLİ İNTERNET MERKEZİ | GÜVENLİ WEB

İNTERNETTE ÖNCE DÜŞÜN SONRA PAYLAŞ!!!

GÜVENLİ İNTERNET MERKEZİ

Paylaştığımız bilgilerin doğruluğundan emin olmalıyız.

Faydalı ve gerekli bilgiler içeriyor mu kontrol etmeliyiz.

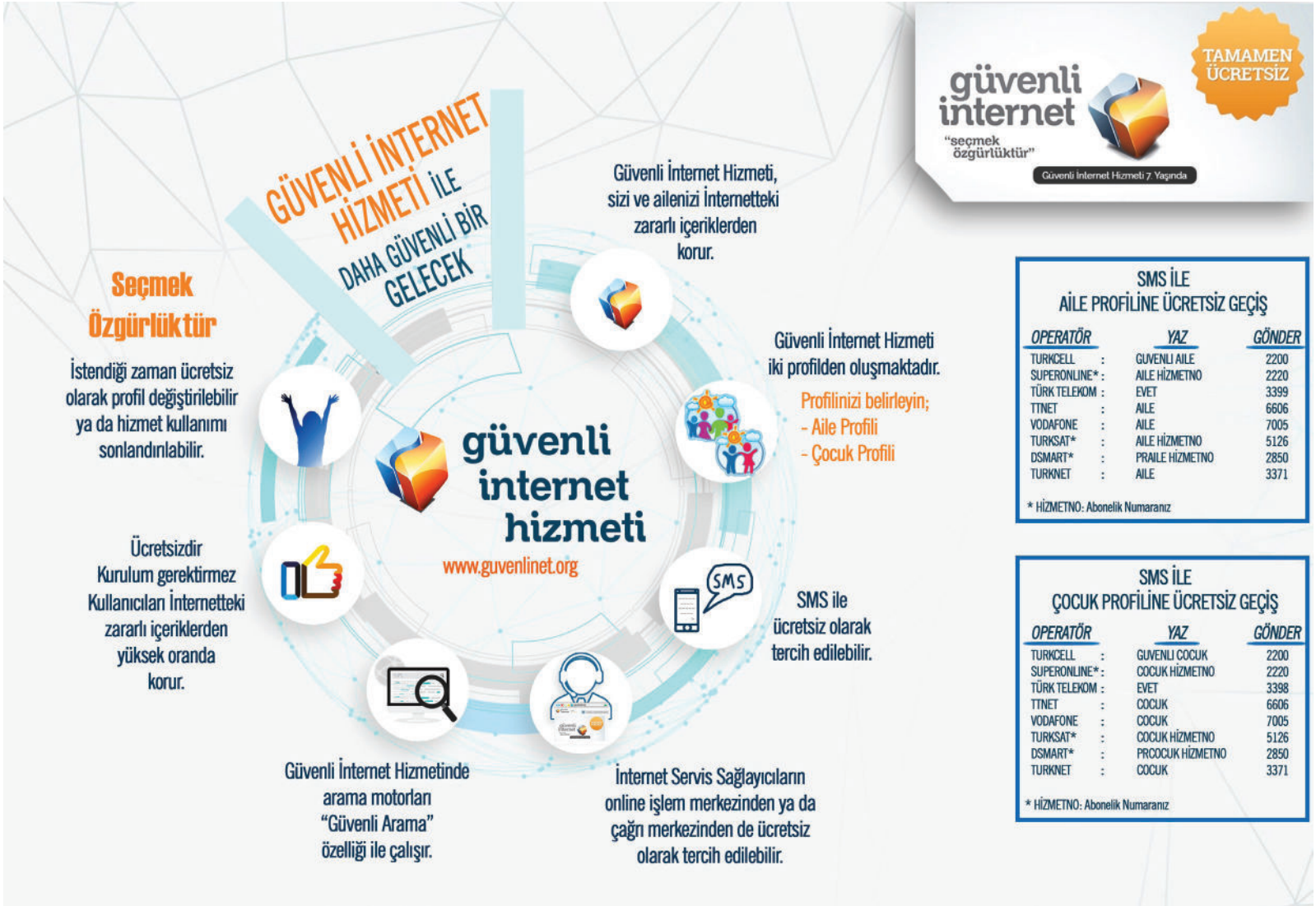
Kimlik bilgileri, telefon numarası gibi özel bilgiler içermemesine dikkat etmeliyiz.

Arkadaşlarımızı, ailemizi üzecek, incitecek paylaşımları yapmamalıyız.

Türkçe'yi düzgün kullanmaya, argo kelimeler ve kaba bir dil kullanmamaya özen göstermeliyiz.

www.guvenliweb.org.tr

www.gim.org.tr



SMS İLE AİLE PROFİLİNE ÜCRETSİZ GEÇİŞ

OPERATÖR		YAZ	GÖNDER
TURKCELL	:	GUVENLI AILE	2200
SUPERONLINE*	:	AILE HİZMETNO	2220
TÜRK TELEKOM	:	EVET	3399
TTNET	:	AILE	6606
VODAFONE	:	AILE	7005
TURKSAT*	:	AILE HİZMETNO	5126
DSMART*	:	PRAILE HİZMETNO	2850
TURKNET	:	AILE	3371

* HİZMETNO: Abonelik Numaranız

SMS İLE ÇOCUK PROFİLİNE ÜCRETSİZ GEÇİŞ

OPERATÖR		YAZ	GÖNDER
TURKCELL	:	GUVENLI COCUK	2200
SUPERONLINE*	:	COCUK HİZMETNO	2220
TÜRK TELEKOM	:	EVET	3398
TTNET	:	COCUK	6606
VODAFONE	:	COCUK	7005
TURKSAT*	:	COCUK HİZMETNO	5126
DSMART*	:	PRCOCUK HİZMETNO	2850
TURKNET	:	COCUK	3371

* HİZMETNO: Abonelik Numaranız

Dostça şakalar eğlencelidir, ancak şaka sınırları aştığında zorbalığa dönüşür...

GÜVENLİ İNTERNET MERKEZİ
www.gim.org.tr

ŞAKA MI?

- ✓ **Konuşmadan önce düşünün, başkası size aynı şeyleri söylese komik olur mu?**
- ✓ **Arkadaşınız yaptığınız şakalardan hoşlanmıyorsa; Durun ve Devam Etmeyin!**
- ✓ **Yaptığınız şakalar arkadaşınızı kırıyor ve incitiyorsa şaka değildir!**
- ✓ **Şaka ile zorbalık arasında ince bir çizgi vardır, çizgiyi aşmayın...**

Dostluklarınızı kötü şakalarla kaybetmeyin.

ZORBALIK MI?

Sosyal Medya Kullanımı
Yaş Sınırları

GÜVENLİ İNTERNET MERKEZİ
www.gim.org.tr

Google+
Facebook
Reddit
Twitter
Instagram
Tumblr
Pinterest
Vimeo
Skype
Foursquare
MySpace
Snapchat

13

Linked In

16

Badoo
Tinder

18

Youtube*
Flickr*
WeChat*

18

*13-18 yaş arası ebeveyn denetiminde.

Çocuklar ve Gençler İNTERNET Kullanım "TAKTİK"lerimizi Belirledik
Artık İnterneti Daha Güvenli Kullanabiliriz...

GÜVENLİ İNTERNET MERKEZİ
www.gim.org.tr

T — TANIŞMA
İnternet üzerinden kimseyle asla tanışma. Tanımadığın kişilerin arkadaşlık tekliflerini kabul etme.

A — AİLENE ANLAT
İnternette bir kişi veya herhangi bir durum seni rahatsız ediyor veya üzüyorsa ailene anlat. İnternette yaşadığın tüm olumsuzlukları ailene çekinmeden anlatmalısın.

K — KABUL ETME
Tanımadığın ve güvenmediğin insanlardan gelen e-posta, mesaj, resim veya dosyaları kabul etme ve açma. Bu mesajlar virüs veya hoşuna gitmeyen mesajlar içeriyor olabilir.

T — TÜRKÇEYİ DÜZGÜN VE DOĞRU KULLAN
Güzel Türkçemizi koru, düzgün ve doğru kullan. Anlamsız kısaltmalar, yabancı kelimeler, bozuk cümleler kullanma. İnan ki Türkçeyi doğru kullandıkça kendine olan saygın artacak.

İ — İNANMA
İnternette konuştuğun kişiler, kim oldukları hakkında sana yalan söylüyor olabilirler. Herkese inanma.

K — KİŞİSEL BİLGİLERİNİ PAYLAŞMA
İnternette kişisel bilgilerini paylaşırken çok dikkatli ol. Bulunduğun yer, telefon numaran, şifren gibi kişisel bilgilerini, kimseyle paylaşma ve güvenli kal.

YALAN HABER NASIL TESPİT EDİLİR?

DOĞRULAYIN!

Bir haberin doğruluğundan emin olmak için, aynı habere güvenilir başka kaynaklardan da ulaşabilmelisiniz. Haberi, güvenilir farklı kaynaklardan teyit edin.

KAYNAK GÜVENİLİR Mİ?

Haberin kaynağı ne, kaynağı kim?
İletişim bilgileri ve "Hakkında" bilgisi olmayan kaynaklara güvenmeyin.

ELEŞTİREL VE ŞÜPHECİ OLUN!

Şüpheci olun ve eleştirel bir bakış açısı edinin.
Öncelikle sorgulayın çünkü ulaşılan her bilgi doğru değildir.

HEMEN İNANMAYIN!

İnternette ve sosyal medyada gördüğünüze ve duyduğunuza hemen inanmayın.
Haber hakkında arka plan bilgileri edinin, gerekirse resmi ve birincil kaynaklarla iletişime geçin.

TARİHİ İNCELEYİN

Yalan haberlerdeki tarih ve saatler değiştirilmiş veya tutarsız olabilir.
Tarihe, yere ve görsellere dikkat edin.

EMİN OLMADAN PAYLAŞMAYIN!

Bazı haberler yönlendirme, yanıltma ve provokasyon amacı taşıyor olabilir.
Doğruluğundan ve ne amaçla dolaşımda olduğundan emin olmadan paylaşmayın!

İDDİALI BAŞLIKLARA DİKKAT!

Olağan dışı iddialar, ilgi çekmek için abartılmış başlıklar ve
çok fazla kullanılan noktalama işaretleri, genellikle asılsız haberlere aittir.

URL / ADRES GERÇEK Mİ?

Sahte haber siteleri genellikle güvenilir haber kaynaklarına çok benzeyen
taklit bir adres (URL) kullanırlar. İnternet adreslerine dikkat edin.

GÖRSELLERİ DOĞRULAYIN

Sahte haberler montajlanmış, garip görüntüler veya videolar içeriyor olabilir.
Görselleri doğrulamak için arama motorlarında ararak fotoğrafın
ne zamana ait olduğunu, ne zaman yayınlandığını görebilirsiniz.

PARODİ VEYA REKLAM MI?

Bazı web siteleri parodi, reklam veya sahte haber yapıp yayma amacıyla kuruluyor.
Haberlere bunun bilincinde olarak yaklaşın.

GÜVENLİ İNTERNET MERKEZİ

ağ'a takılmayalım

İnternet ortamı, sosyal ağlar, bizim ve çocuklarımızın iletişim araçlarından biridir. Dikkat edilmesi gereken okul adı, ev adresi, telefon numarası gibi kişisel bilgilerin paylaşılmasının yaratacağı riskleri bilmektir.

Sosyal ağlarda karşımızdaki kişinin gerçekte kim olduğunu ve niyetinin ne olduğunu bilemeyiz. Bu kişiler dolandırıcılık, hırsızlık veya istismar amacıyla bilgilerimizin peşinde olabilirler.

Bilinçli kullanıcı olarak İnternetin bizim ve çocuklarımız için güvenli hale gelmesine katkıda bulunalım.

bağlantıyı koparmayalım

Çocuklarımızın zarar görmemesi için İnternetin bilinçli kullanılması çok önemlidir. Unutmayalım ki çocuklarımız İnternet ortamında da hata yapabilir. Çocuklarımızla sürekli iletişim içerisinde bulunmak ve anlayışlı olmak

Güvenlik yazılımları ve aile denetim araçlarıyla bir yandan İnternetteki tehlikelerden korunurken, diğer yandan bize sunulan geniş imkanlardan faydalanabiliriz.

İNTERNET aile REHBERİ

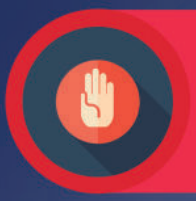
Güvenli Web
www.guvenliweb.org.tr

Güvenli Çocuk
www.guvenlicocuk.org.tr

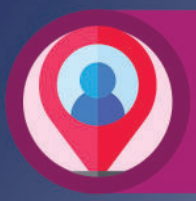
www.internetbk.org.tr


güvenli internet
www.guvenlinet.org.tr
güçlü bir şifre belirle!
sosyal ağlarda çocuklarınla arkadaş ol!
bilinçli ol, keyfini sür!
çocukların oyunlarının içeriğini ve harcadığı zamanı kontrol et!
herkesin kullanımına açık internet ağlarında alışveriş ve bankacılık işlemlerini yapma!
ihbar web
www.ihbarweb.org.tr
olumsuz içeriklerle karşılaştığında Hakkını ara!
Çocukların yaşına uygun ve güvenli olan internet sitelerini belirle!
Not: sık kullanılanlara ekleyebilirsin.

Güçlü bir şifre belirleyin



Gizlilik ayarlarınızı mutlaka yapın



Özel bilgilerinizi koruyun

Sorgulayan bir kullanıcı olun

Paylaşmadan önce bir daha düşünün

Bilinçli kullanıcı olun, İnternetin keyfini sürün

www.gim.org.tr
www.guvenliweb.org.tr
www.guvenlicocuk.org.tr
www.guvenlinet.org.tr
www.ihbarweb.org.tr

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

GÜVENLİ İNTERNET MERKEZİ