PROF. DR. HÜLYA ÇALIŞKAN | GÜLDEN BAYRAK | İLKER BAYRAK | PROF. DR. BUKET AKKOYUNLU

DİJİTAL HAKLAR KILAVUZU

DİJİTAL GÜVENLİK ÖNERİLERİ

Avrupa Birliği sivil düşün

"Bu çalışma Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla Prof. Dr. Hülya Çalışkan'a aittir ve AB'nin görüşlerini yansıtmamaktadır."

PROF. DR. HÜLYA ÇALIŞKAN | GÜLDEN BAYRAK | İLKER BAYRAK | PROF. DR. BUKET AKKOYUNLU

DİJİTAL HAKLAR KILAVUZU

DİJİTAL GÜVENLİK ÖNERİLERİ

Avrupa Birliği sivil düşün

"Bu çalışma Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla Prof. Dr. Hülya Çalışkan'a aittir ve AB'nin görüşlerini yansıtmamaktadır."

Bu çalışma: Avrupa Birliği Sivil Düşün Programı tarafından desteklenen "SilverSAFE: Empowering Seniors with Secure Digital Access / SilverSAFE: İleri Yaşlılara Güvenli Dijital Erişim Sağlamak"çalışması kapsamında hazırlanmıştır.

Çalışmamız kapsamında yetişkin eğitimi yapan öğreticiler, halk eğitim merkezi öğreticileri, ileri yetişkinler (yaşlılar) ve hayat boyu öğrenme programları hazırlayanların, öğretmen ve öğrencilerin yararlanması hedeflenmiş, bu hedef kitleye yönelik dijital haklar ve siber güvenlik konusunda yapılandırılmış içerikler hazırlanmıştır. Büyükçekmece İlçe Milli Eğitim Müdürlüğü işbirliği ile 27 Kasım 2024'te Büyükçekmece'de Dijital Haklar Paneli gerçekleştirilmiştir.

ISBN: 978-625-99749-5-8

Çalışmanın Koordinatörü:

Prof. Dr. Hülya Çalışkan

Yayını Hazırlayanlar:

Prof. Dr. Hülya Çalışkan / İstanbul Üniversitesi Cerrahpaşa Öğretim Üyesi
Gülden Bayrak / Büyükçekmece MEM Proje Koordinatörü
İlker Bayrak / Büyükçekmece MEM Proje Koordinatörü
Prof. Dr. Buket Akkoyunlu / Çankaya Üniversitesi Öğretim Üyesi

Araştırmacılar:

Doç. Dr.Özgür Yılmaz / İstanbul Üniversitesi Cerrahpaşa Öğretim Üyesi
Dr. Öğretim Üyesi Ahmet Ağır / İstanbul Üniversitesi Cerrahpaşa Öğretim Üyesi

Grafik Tasarım:

Burçak Karahacıoğlu

Yayınevi:

İstanbul STEAM Bilim Teknoloji Eğitim Kültür Sanat Derneği Yayınları
Sertifika Numarası:72283
Adres: Kamiloba Mahallesi, Mustafa Kemal Atatürk Caddesi, Şemsa No:13/C-29
Büyükçekmece / İstanbul
Telefon: 0 535 286 70 46 | isteamder.com | isteamder@gmail.com

Baskı:

Dermen Bilişim Anonim Şirketi
Adres: Mecidiyeköy Mahallesi Şehit Er Cihan Namlı Cad. Adalet Apt. No:8/A Şişli / İstanbul
Sertifika Numarası: 75629

Basım Tarihi:

Kasım, 2024

Avrupa Birliği sivil düşün

"Bu çalışma Avrupa Birliği Sivil Düşün Programı kapsamında Avrupa Birliği desteği ile hazırlanmıştır. İçeriğin sorumluluğu tamamıyla Prof. Dr. Hülya Çalışkan'a aittir ve AB'nin görüşlerini yansıtmamaktadır."

İÇİNDEKİLER

DİJİTAL HAKLARIMIZ

Gülden Bayrak
Büyükçekmece İlçe Milli Eğitim Müdürlüğü
Proje Koordinatörü
buyukcekmeceprojeler@gmail.com

Günümüzün dijitalleşen dünyasında, dijital haklar çevrimdışı sahip olduğumuz temel insan haklarının, teknoloji ve internetin etkisiyle yeniden şekillenmiş halidir. İfade özgürlüğü, mahremiyet ve bilgiye erişim gibi temel haklarımız, dijital ortamda da geçerlidir ve hayatımızın her alanını etkileyen bu teknolojik dönüşümle birlikte daha da kritik bir hale gelmiştir. Sosyal medyada düşüncelerimizi paylaşmak, kişisel verilerimizi korumak ya da çevrimiçi bilgiye ulaşmak gibi günlük dijital deneyimlerimiz dijital haklarımızın kapsamına girer.

Dijital hakların önemini kavrarken, internet aracıları olarak adlandırılan sosyal medya platformları, arama motorları ve internet servis sağlayıcıları gibi aktörlerin rollerini de anlamak gereklidir. Bu platformlar, dijital haklarımızı ya koruyabilir ya da zayıflatabilir. İçerik denetimi, veri kullanımı ve gözetim politikaları, çevrimiçi ifade özgürlüğü ve diğer dijital haklarımız üzerinde büyük etkiler yaratabilir.

Çevrimiçi ifade özgürlüğü, sınırları aşan doğasıyla büyük bir güce sahiptir. Geleneksel medyanın yerel sınırlamalarına karşın, internet üzerinden fikirler anında küresel çapta yayılabilir. Ancak bu özgürlükle birlikte, yeni hukuki ve etik sorular da gündeme gelmiştir. Bu yeni dijital dünyadaki haklarımızı korumak ve savunmak büyük önem taşır. Dijital hakların korunması, internetin özgür ifade, mahremiyet ve bilgiye erişim haklarımızın sürdürülebilir bir biçimde var olduğu bir alan olmasını sağlar. Dijital çağ, yeni zorluklar

getirirken, bu zorluklara karşı yenilikçi çözümler üretmek ve insan haklarını korumak için fırsatlar da sunmaktadır.

Dijital haklar, dijital dünyada da geçerli olan temel insan haklarımızı savunmak demektir. Teknoloji, iletişim, toplumsal katılım ve insan etkileşimlerini yeniden şekillendirirken, dijital hakların korunması, insan haklarımızın dijital ortamda da sürdürülmesini sağlar. Mahremiyetin korunmasından ifade özgürlüğüne kadar, dijital hakların savunulması, internetin insan gelişimi ve güçlenmesi için bir alan olarak kalmasının anahtarıdır.

Dijital İnsan Hakları Kavramı Nedir?

Dijital teknolojiler, insan haklarını savunma ve kullanma konusunda yeni olanaklar sunarken, aynı zamanda bu hakları bastırma ve ihlal etme amacıyla da kullanılabilir. Mevcut insan hakları sözleşmeleri, dijital öncesi bir dönemde imzalanmıştır. Günümüzde çevrimiçi ihlaller, çevrimdışı suistimallere yol açabileceğinden, internetin denetimsiz bir alan olmaması gerekmektedir. İnsan hakları, çevrimiçi ve çevrimdışı olarak varlığını sürdürmeli ve tam olarak haklara saygı gösterilmelidir.

Teknoloji ürünlerinin, politikalarının ve hizmet koşullarının insan hakları ilkeleriyle uyumlu olmasını sağlamak için etkin bir dikkat gösterilmesi gerekmektedir. Dijital çağda insan hakları standartlarının nasıl uygulanacağına dair daha fazla rehberlik geliştirilmesine ihtiyaç vardır. Ayrıca, sürekli gelişen dijital teknolojilerin yaratabileceği olası koruma boşluklarını ele almak da önemlidir. Birleşmiş Milletler insan hakları mekanizmaları, genel internet kesintilerini ve hizmetlerin engellenmesini uluslararası insan hakları hukukuna aykırı olarak değerlendirmektedir. Yanlış bilgilendirmeyi ve özellikle zararlı içerikleri kontrol etmek için, hükümetler, sanayi ve sivil toplum arasında uluslararası insan hakları hukuku çerçevesinde danışmalarla uygun yollar bulunmalıdır.

Özellikle, teknolojilerin insan haklarını ihlal etme, eşitsizlikleri derinleştirme ve ayrımcılığı artırma potansiyeli olan alanlara dikkat edilmesi gerekmektedir.

En temel dijital haklarımız:

- ***İnternete Erişim Hakkı:*** İnternete herkesin erişebilmesi, bilgiye ve dijital kaynaklara ulaşımda eşitlik sağlar.

- ***İfade Özgürlüğü:*** Dijital platformlarda görüş ve düşüncelerimizi, başkalarının özgürlük alanına, haklarına, mahremiyetine zarar vermeden özgürce ifade edebilme hakkı.
- ***Mahremiyet Hakkı:*** Çevrimiçi ortamda kişisel verilerimizin korunması, izinsiz takip ve gözetimden korunma hakkı.
- ***Bilgiye Erişim Hakkı:*** İnternet üzerinden doğru, güvenilir ve tarafsız bilgiye ulaşma hakkı.
- ***Anonimlik Hakkı:*** Dijital ortamda kimliğimizi gizli tutma ve anonim olarak iletişim kurabilme hakkı.
- ***Kişisel Verilerin Korunması:*** Kişisel bilgilerimizin izinsiz kullanılmasına ve paylaşılmasına karşı korunma hakkı.
- ***Siber Güvenlik Hakkı:*** Çevrimiçi ortamda güvenli bir şekilde faaliyet gösterebilme, siber saldırılardan korunma hakkı.
- ***Dijital Katılım Hakkı:*** Dijital teknolojiler ve hizmetlere erişimde eşit fırsatlara sahip olma, dijital dünyaya katılabilme hakkı.
- ***Dijital Okuryazarlık Hakkı:*** Teknolojiyi kullanmayı öğrenme ve dijital dünyadaki gelişmeleri takip etme hakkı.

Dijital hak kavramı, özellikle pandemi dönemindeki hızlı dijitalleşme süreciyle birlikte daha fazla tartışılmaya başlanmıştır. Dijital araçlar, gelişmiş akıllı telefon uygulamaları ve yapay zekâ alanındaki hızlı ve çarpıcı gelişmeler, dijital hakların güncel tutulmasını gerektirmekte ve bu hakların korunmasına yönelik etkili yol haritalarının oluşturulması ihtiyacını ortaya koymaktadır.

Birleşmiş Milletler Genel Sekreterliği, Dijital İşbirliği Yol Haritası Raporuna göre (Haziran 2020) COVID-19 pandemisiyle mücadele sürecinde, dijital teknolojilerin tehditlerle başa çıkma ve insanları bağlı tutmadaki rolü önemli ölçüde öne çıkmıştır. Süper bilgisayarlar, tedavi ve aşı geliştirme konusunda ilaç bileşenlerini analiz ederken; e-ticaret platformları temel ev ihtiyaçları ve tıbbi malzemeleri önceliklendirmiş, video konferans araçları ise eğitim ve ekonomik faaliyetlerin devam etmesini sağlamıştır.

Ancak, pandemi sürecinde dijital teknolojilerin getirdiği zorluklar da artmıştır. Doğru bilgiye erişim salgınla mücadelede kritik öneme sahipken, bazı sosyal medya platformları tehlikeli yanlış bilgilere ve ayrımcılığın, yabancı düşmanlığının yayılmasına yol açmıştır.

Dijital teknoloji boşlukta var olmaz; olumlu değişim yaratma potansiyeli-

ne sahip olsa da mevcut eşitsizlikleri derinleştirebilir. 2019'da, gelişmiş ülkelerdeki bireylerin %87'si internet kullanırken, en az gelişmiş ülkelerde bu oran sadece %19'du. İnternet erişimi arttıkça, yeni güvenlik açıkları ortaya çıkmaktadır. Tahminlere göre, 2024 yılı sonuna kadar dünya çapındaki veri ihlallerinin potansiyel maliyeti 5 trilyon doları aşabilir.

Ayrıca, dijital teknolojilerin çevre üzerindeki etkileri de önemlidir. Bilgi ve iletişim teknolojilerine (ICT) dayalı operasyonların, küresel elektrik talebinin %20'sine kadar çıkması beklenmektedir. Ancak, teknolojinin çevreyi koruma ve sürdürülebilirliği ilerletme konusunda sunduğu fırsatlar da vardır. Doğru şekilde kullanıldığında, dijital devrim iklim değişikliğiyle mücadelede ve küresel sürdürülebilirlikte önemli bir rol oynayabilir. Aslında dijital haklar diğer pek çok insan hakkıyla doğrudan ya da dolaylı olarak ilgilidir. Bu nedenle belki de ilk olarak ele alınması gereken hak "İnternete Erişim Hakkı" olmalıdır.

İnternete Erişim Hakkı:

Günümüz dijital çağında anlamlı katılım, yüksek hızlı geniş bant internet bağlantısını gerektirmektedir. Ülkeler, dünya nüfusunun %93'ünün mobil geniş bant veya internet hizmetlerine fiziksel olarak erişim sağladığını bildirmektedir. Ancak, dünya nüfusunun yalnızca %53,6'sı interneti kullanmaktadır ve yaklaşık 3,6 milyar kişi internet erişiminden yoksundur. En az gelişmiş ülkelerde ise bu oran sadece %19'dur. Dijital uçurumu derinleştiren birçok engel bulunmaktadır. İlk olarak, geleneksel geniş bant bağlantılarının kurulumu maliyetlidir ve ülkeler, gereken fiber optik kabloları finanse etme konusunda zorluklarla karşılaşmaktadır. İkinci olarak, piyasa dinamikleri genellikle elverişli değildir. En az gelişmiş ülkelerdeki düşük alım gücü, bağlantı sağlayıcıları için sınırlayıcı bir faktördür. Kablosuz teknolojilerin geniş bant kapsama alanını daha hızlı ve daha ucuz bir şekilde yaymak için yardımcı olabileceği düşünülse de, şirketlerin bunu teşvik edecek bir motivasyonu yoktur. Son olarak, dijital becerilerin eksikliği de dijital araçların benimsenmesini kısıtlayabilmektedir.

Dijital Kapsayıcılık:

Dijital teknolojilere erişim, görünürde mevcut olsa bile eşit değildir. Rapor (Birleşmiş Milletler Genel Sekreterliği, Dijital İşbirliği Yol Haritası Raporu) en çok ihtiyaç duyanların genellikle bu erişimi en az karşılayabilenler olduğunu belirtmektedir. Dijital bölünmeler, mevcut sosyal, kültürel ve ekonomik eşitsizlikleri yansıtarak artırmaktadır. Küresel internet kullanımında cinsiyet farkı, bu eşitsizliğin çarpıcı bir örneğidir; birçok ülkede erkekler kadınlardan daha fazla internet kullanmaktadır. Dijital araçlar milyonlarca insan için hayati öneme sahip olmuştur. Gelişmekte olan ülkelerin ekonomik destek çabalarında dijital araçların kullanılmasının, kapsayıcı bir dijital altyapı inşa edilmesine katkı sağlayacağı belirtilmektedir. Üye Devletler ve paydaşlar, cinsiyet eşitliği için teknoloji ve inovasyon konularında çok paydaşlı eylem koalisyonu gibi girişimlerde bulunmaktadır. Ancak, küresel çabaların daha iyi koordine edilmesi ve ölçeklendirilmesi gerekmektedir. Dijital kapsayıcılığı ölçmek için bir dizi metriğin geliştirilmesi, kanıta dayalı politika oluşturma açısından önemlidir. Bu metriklerin, dijital okuryazarlığın ve erişimin ne anlama geldiğini tanımlarken herkesin ICT aracılığıyla güçlendirilme fırsatına eşit olarak sahip olması gerektiği temel ilkesine dayanması önemlidir. Erişim, yalnızca fiziksel erişim ve beceri geliştirme ile değil, aynı zamanda engelli bireylerin ihtiyaçlarını da göz önünde bulunduran bir tasarım ile sağlanmalıdır. Ayrıca, göçmenler ve acil durumlar veya çatışma bölgeleriyle karşılaşan kişiler gibi hareket halindeki toplulukların durumuna daha fazla dikkat edilmesi gerekmektedir. Bu en savunmasız gruplar, dijital iş birliği tartışmalarında genellikle yer almamakta ve bağlantı sağlama konusunda ek zorluklarla karşılaşmaktadırlar.

Erişim ve erişimde kapsayıcılık için dijital kapasite geliştirme ihtiyacı son derece büyüktür. Dijitalleşmenin farklı boyutlarında gerçek ve sürdürülebilir bir ilerleme kaydetmek, özellikle gelişmekte olan ülkelerde, daha çok beceri geliştirme çalışmalarına ve etkili eğitim süreçlerine ihtiyaç duymaktadır.

İnternet, bilgi paylaşımı, eğitim, ifade, harekete geçme ve katılım için güvenli bir alan sağlamalıdır. Şifrelemenin gerekliliğini ele alırken, yasal uygulama hedeflerini zayıflatmadan, insan haklarına dayalı yasalar ve yaklaşımlar ile yasadışı ve zararlı çevrimiçi içeriklere karşı çözümler geliştirmek mümkündür.

Kişisel Verilerin Korunması Hakkı ve Mahremiyet:

Kişisel verilerin korunması, bireylerin özel bilgilerinin güvenliğini sağlamaya yönelik önlemler ve yasaların bütünüdür. Hızla gelişen dijital teknolojiler, veri ihlalleri ve siber saldırılarla birlikte, kişisel verilerin korunmasını zorunlu hale getirmiştir. 2019 yılında 7,000'den fazla veri ihlali kaydedilmiş ve 15 milyardan fazla kayıt ifşa edilmiştir. Bu bağlamda, uluslararası standartlarla uyumlu etkili kişisel veri koruma yasaları ve uygulamaları gerekmektedir. Veri koruma otoritelerinin bağımsız ve iyi kaynaklarla desteklenmesi, özel şirketler ve hükümetler tarafından verilerin kötüye kullanılmasını önlemek için önemlidir. Özel sektör aktörleri için dijital alanda mahremiyet hakkını korumak ve bu konuda net adımlar atmak temel bir gerekliliktir.

Mevcut sosyal medya platformlarının finansman modeli, ticari amaçlarla kişisel verilerin toplanmasını teşvik etmektedir. Bu modelin değiştirilmesi, veri koruma haklarını güçlendirmek ve bireylerin gizliliğini sağlamak açısından önem taşımaktadır. Kişisel verilerin korunması, bireylerin haklarını ve özgürlüklerini güvence altına almak için kritik bir unsur olup, bu alanda etkin ve katılımcı politikaların geliştirilmesi gerekmektedir.

Dijital mahremiyetin korunmasında şu unsurlar önemlidir:

- ***Veri Toplama ve Kullanım Şeffaflığı:*** Şirketlerin, kullanıcıların verilerini nasıl topladıkları ve kullandıkları konusunda şeffaf olmaları gerekmektedir.
- ***Kullanıcı Kontrolü:*** Bireylerin, hangi verilerin toplandığı ve nasıl kullanıldığı üzerinde kontrol sahibi olmaları önemlidir. Bu, kullanıcılara veri erişimi ve silme hakları verilmesiyle sağlanabilir.
- ***Güvenlik Önlemleri:*** Verilerin korunması için güçlü güvenlik protokollerinin uygulanması, şifreleme ve veri koruma araçlarının kullanılması gereklidir.
- ***Yasal Düzenlemeler:*** Ulusal ve uluslararası düzeyde dijital mahremiyeti korumaya yönelik yasaların geliştirilmesi ve uygulanması kritik öneme sahiptir. Örneğin, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR), kullanıcıların mahremiyet haklarını korumaya yönelik önemli bir adımdır.

Siber Güvenlik Hakkı:

Siber güvenlik, bilgisayar sistemlerinin, ağların, programların ve verilerin siber tehditlere karşı korunmasını sağlayan uygulama, süreç ve teknolojilerin toplamıdır. Dijital dünyanın hızla büyümesi ve internetin yaygınlaşmasıyla, siber güvenlik önemi daha da artmıştır. Siber saldırılar, veri ihlalleri, fidye yazılımları ve diğer zararlı faaliyetler, bireyler, şirketler ve devletler için ciddi tehditler oluşturur.

Temel Bileşenler:

- ***Ağ Güvenliği:*** Bilgisayar ağlarının izinsiz erişimlere ve saldırılara karşı korunması. Güvenlik duvarları, antivirüs yazılımları ve izleme araçları bu alanda kullanılır.
- ***Uygulama Güvenliği:*** Yazılımların ve uygulamaların güvenli bir şekilde geliştirilmesi, dağıtılması ve sürdürülmesi. Güvenlik açıklarının tespit edilmesi ve kapatılması önemlidir.
- ***Veri Güvenliği:*** Kişisel ve kurumsal verilerin korunması. Şifreleme, erişim kontrolleri ve veri kaybı önleme yöntemleri kullanılır.
- ***Son Kullanıcı Güvenliği:*** Bireylerin siber tehditlere karşı bilinçlendirilmesi ve eğitilmesi. Phishing saldırıları gibi sosyal mühendislik tekniklerine karşı farkındalık yaratılması önemlidir.
- ***Mobil Güvenlik:*** Mobil cihazların güvenliğini sağlamak için özel önlemler. Mobil uygulamaların güvenliğinin sağlanması ve cihazların koruma altına alınması gereklidir.
- ***Bulut Güvenliği:*** Bulut hizmetlerinin güvenliği, verilerin bulut ortamlarında güvenli bir şekilde saklanması ve işlenmesi için önlemlerin alınması.

Tehditler:

- ***Kötü Amaçlı Yazılımlar:*** Virüsler, solucanlar, trojanlar ve fidye yazılımları gibi zararlı yazılımlar.
- ***Phishing:*** Kullanıcıları kişisel bilgilerini vermeye ikna eden sahte e-postalar ve web siteleri.

- ***DDoS Saldırıları:*** Hedef sistemleri aşırı yükleyerek erişilemez hale getiren saldırılar.
- ***Veri İhlalleri:*** Yetkisiz kişiler tarafından veri tabanlarına erişim sağlanarak bilgilerin çalınması.

Önlemler:

- ***Güçlü Parolalar:*** Zayıf parolalardan kaçınılmalı, karmaşık ve güçlü parolalar kullanılmalıdır.
- ***Düzenli Güncellemeler:*** Yazılım ve sistem güncellemeleri zamanında yapılmalı, güvenlik açıkları kapatılmalıdır.
- ***Antivirüs Yazılımları:*** Güncel antivirüs yazılımları kullanılarak sistemler korunmalıdır.
- ***Eğitim ve Farkındalık:*** Kullanıcılar, siber tehditler ve korunma yöntemleri hakkında eğitilmelidir.
- ***Veri Yedekleme:*** Önemli verilerin düzenli olarak yedeklenmesi, kayıpların önlenmesi açısından kritik öneme sahiptir.

DİJİTAL VATANDAŞLIK & DİJİTAL EBEVEYNLİK

Prof. Dr. Hülya Çalışkan
İstanbul Üniversitesi-Cerrahpaşa
Hasan Âli Yücel Eğitim Fakültesi
caliskan@iuc.edu.tr

Dijital Vatandaşlık

Dijital vatandaşlık kavramı literatüre daha tam olarak yerleşemese de konu ile paralel olarak çevrimiçi teknolojilerin güvenli ve doğru kullanımı hususunda özellikle çocukların ve yaşlıların korunumuna ilişkin çeşitli uluslararası kuruluşlar tarafından tavsiye kararları yayımlanmakta ve bu konuda çeşitli stratejiler oluşturulmaktadır. OECD (Ekonomik Kalkınma ve İş birliği Örgütü), CoE (Avrupa Konseyi), ITU (Uluslararası Telekomünikasyon Birliği) ve Avrupa Birliği Komisyonu gibi birçok uluslararası önemli kuruluş konu ile ilgili birçok girişimde bulunmakta ve ülkelere çeşitli tavsiyeler sunmaktadırlar. Bunlardan en önemlisi ve günceli, aralarında Microsoft, Samsung, Apple, Facebook ve Vodafone gibi önemli şirketlerin bulunduğu, sektöründe lider 28 şirketin Avrupa Birliği Komisyonu önderliğinde toplanarak hazırladıkları ve 2011 yılı sonunda mutabık kaldıkları bir eylem planı olmuştur (DigitalAgenda, 2011).

Dijital vatandaş olmak, internetle bağlanılan dijital ortamda, saygılı ve sağlıklı iletişimi, mahremiyete saygı göstermeyi, yorumlarda açık fikirli olmayı, sorumluluk içinde üretmeyi ve paylaşmayı ve yapıcı geribildirim vermeyi gerektirir. Dijital vatandaşlık, dijital ortamlarımızda güvenli ve sorumlu bir şekilde gezinme ve bu

alanlarda aktif ve saygılı bir şekilde yer alma bilgisiyle birlikte, aslında bir ülke vatandaşlığından çok da farklı değildir; sadece teknolojinin katkısıyla vatandaşlık görevleri daha kısa zamanda ve kolay gerçekleştirilmeye başlamıştır. Önceden sıraya girilerek ya da bir aracı ile yapılan birçok iş; Vergi ödemeleri, bankacılık işlemleri, haberleşme, iletişim, yatırım, randevu alma gibi işlemler şimdi akıllı cep telefonları ve bilgisayarlar üzerinden dijital olarak yapılmaktadır.

Bir vatandaşlık numaramız vardır ve bir de şifremiz. Bu durum artık dijital bir hayata başladığımızı göstermektedir. Bu hayatın sorumluluklarını bilmeli ve sahip olduğumuz hakları da öğrenmeliyiz.

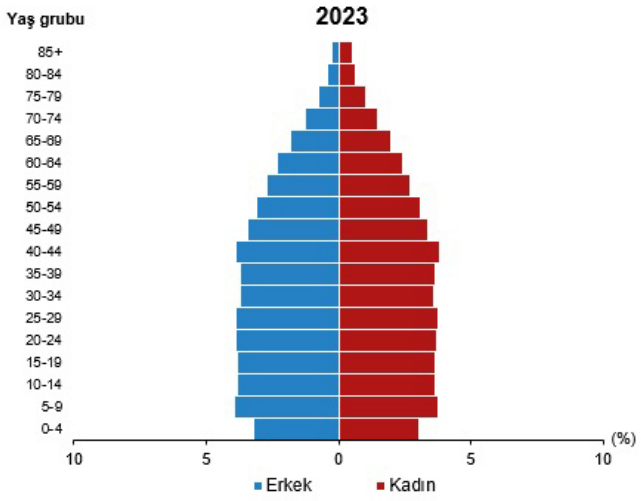
Dijital vatandaşlığın, 1-dijital erişim, 2-dijital ticaret, 3-dijital iletişim, 4-dijital okuryazarlık, 5-dijital etik, 6-dijital hukuk, 7-dijital haklar ve sorumluluklar, 8-dijital sağlık ve 9- dijital güvenlik olmak üzere dokuz ögesi bulunmaktadır (Ribble, 2015)

Ülkemizde dijital vatandaş olanlar genelde teknolojinin içinde bulunan ve dijital dünyada dolaşmayı ögrenebilenlerdir. Bu kesimin Dijital vatandaşlığın öğelerinden haberdar olduklarını varsayarsak, Dijital vatandaş olmayı öğrenmeye çalışanların, genellikle çocuklar ve 65 yaş üzerindeki vatandaşlar olduğunu kabul edebiliriz.

Dijital vatandaş olabilmenin kapsamı okuma yazma oranı ile oldukça bağlantılıdır, bu nedenle ülkemizde, çocuk, yaşlı ve okuma yazma oranlarının son durumuna bakacak olursak, dijital vatandaşlıkta ne kadar ilerleyebileceğimizi de anlayabiliriz.

Türkiye İstatistik Kurumunun (TÜİK) 2024 yayınlarına göre 2023 yılı 65 yaş üstü oranı %10,2 olarak verilmiştir. Yaşlı nüfusun %64 ü, 65-74 yaş grubu %28,1 i 75-84 yaş grubu ve %7,9'u 85 ve daha yaşlı grubu, %0,1 i de 100 yaş ve üzerini oluşturmaktadır.

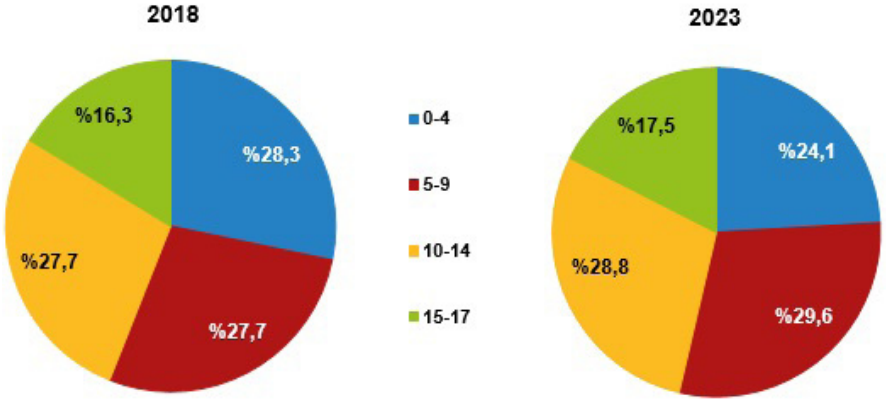
Türkiye'de Çocuk nüfusun 2023 yılında %24,1'inin 0-4 yaş grubunda, %29,6'sının 5-9 yaş grubunda, %28,8'inin 10-14 yaş grubunda ve %17,5'inin 15-17 yaş grubunda yer aldığı görülmüştür (TÜİK2, 2024).



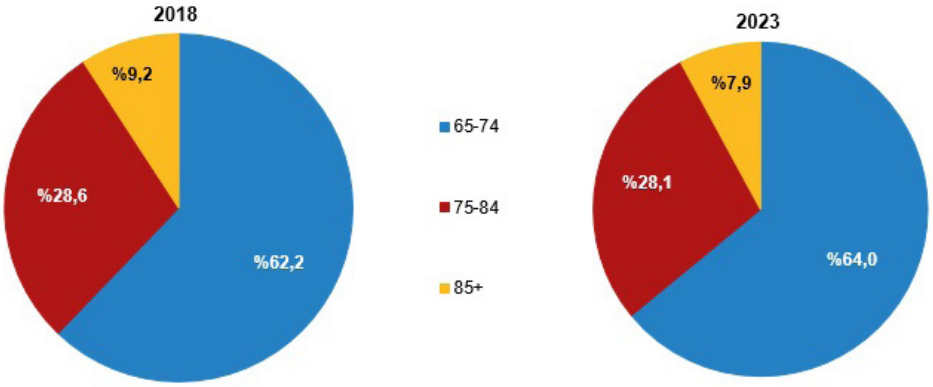
Şekil1: 2023 yılında kadın erkek sayısı ve yaşlara göre gösterimi

Şekil 2: 65 Yaş Üstü Vatandaşların Eğitim Durumu Dağılımı

Bu görüntüye göre Dijital vatandaşlıktan bahsedildiği dönemlerden günümüze doğru geldiğimizde eğitim oranlarında hemen her grupta yaklaşık %3-4 oranında değişimler olduğu görülmektedir. Bu oranların yetersiz olduğu açıktır.



Şekil 3: 0-17 Yaş Arası Çocuk Vatandaş İstatistiği



Şekil 4: 65-85+ Yaş Arası Vatandaş İstatistiği

Bu grafikte de çocuk nüfus oranının 5 yılda ortalama aynı kaldığı veya %1 oranında değiştiğini, 65 yaş üstünün ise, 5 yılda %2 oranında arttığını söyleyebiliriz. Ayrıntılı istatistiklerde yaşlı oranı artmakta ve Türkiye yaşlanmaktadır sonucu çıkmaktadır.

Yine Dijital vatandaşlık paralelinde, 2023'te TÜİK 'in internet kullanımı oranlarına bakacak olursak; (TÜİK3, 2024)

- ***İnternete erişim imkânı olan hane oranı 2023'te %95,5***
- ***E-devlet hizmetlerini kullanan bireylerin oranı %73,9 olarak gerçekleşmiştir.***

İnternet üzerinden mal veya hizmet satın alma ya da sipariş verme oranı %49,5 oranında görünmektedir. Bireylerin %84,9'u WhatsApp kullanabilmektedir.

Son 3 ayda İnternet kullanan bireylerin kişisel verilere erişimi yönetmek amacıyla en fazla kullandıkları yöntem %41,8 ile web sitelerinin kişisel verilerin güvenliğini sağlama konusunda sahip olduğu özellikleri kontrol etmek olmuştur. Bunu %36,2 ile kişisel verileri reklam amaçlı olarak paylaşımına izin vermeme ve %31,1 ile kişisel verileri vermeden önce web sitesinin veya uygulamaların gizlilik politikasını okuma takip etti.

İnternet kullanan 65-74 yaşındaki Bireylerin Oranı 2023 Yılında Yüzde 40,7 olmuştur. İnternet kullanımında yaşlı erkeklerin oranı 2023 yılında %49,8 iken yaşlı kadınların oranı %32,7 olmuştur.

Sonuçta İnternete erişim kolaylığı görülürken, %41,8 civarında güvenli internet kullanımı yapıldığı anlaşılmaktadır. Tüm bu veriler Türkiye'de Dijital vatandaşlığın yapısı hakkında bilgi almamızı sağlayabilir. Ülkemizde henüz dijital vatandaşlığın yüksek seviyelerde olmadığını hatta yarıdan az olduğunu söyleyebiliriz. Sorumlu birimlerin bu konu üzerinde yoğunlaşması gerekmektedir. Dijital vatandaşlık dünyaya açılan kapı olan internet ile donatılmış olduğundan bir bakıma dünya vatandaşlığı ile de adlandırılabilir. Bu açıdan bakıldığında, çok daha fazla dikkat edilmesi gereken konunun, güvenlik ve etik değerlere saygı olduğu açıktır.

Bu durumda özet olarak dijital vatandaş olmak için şunları söyleyebiliriz; (mediasmarts.ca, 2024)

Dijital vatandaş olmak, dijital toplulukların sağlığına ve refahına katkıda bulunmakla ilgili çalışmayı gerektirir. Çevrimiçi ortamda olumlu bir kültüre nasıl katkıda bulunuruz; Bunun için çalışmalarımızı 4 bölümde toplayabiliriz;

- **Dört kategori:**
  1. ***Empati ve Topluluk***
  2. ***Pozitif Teknoloji Kullanımı***
  3. ***Bilgi Paylaşımı***
  4. ***Etik ve Gizlilik***

1. Empati ve topluluk oluşturma:

- *Ekranın arkasında gerçek bir insan olduğunu kendime hatırlatıyorum.*
- *Siber zorbalığa uğrayan birini görürsem yardım etmek için ulaşırım.*
- *Öfkelendiğimde herhangi bir şey yapmadan önce ara veriyorum.*
- *Çevrimiçi olarak tanıdığım biriyle bir anlaşmazlığa düşersem, bunu şahsen konuşurum.*
- *Nefret ve önyargıyı çevrimiçi gördüğümde onlara karşı koyuyorum.*
- *Nefret ve tacizi çevrimiçi gördüğümde bildiriyorum.*
- *Nefreti desteklediklerini gördüğümde platformlara ve reklam verenlere şikâyette bulunuyorum.*
- *Çevrimiçi topluluklarımın değerlerini şekillendirmek için konuşuyorum.*

2. Pozitif teknoloji kullanımı:

- *Arkadaşlarımla ve ailemle bağlantı kurmak için dijital araçları kullanıyorum.*
- *Toplumumda aktif bir vatandaş olmak için dijital araçları kullanıyorum.*
- *Dijital medya kullanımımın farkındayım ve dijital cihazları belirli zamanlarda belirli amaçlar için araç olarak kullanıyorum.*

3. Bilgi paylaşımı:

- *Bilgi paylaşmadan önce güvenilir kaynakları kontrol ediyorum.*
- *Faydalı ve güvenilir olduğunu bildiğim bilgileri paylaşıyorum.*
- *Yanlış bilgiye karşı çıkıyorum.*
- *İnternette bir bilgi gördüğümde şunu soruyorum:*
  - ***Bu konuda ne biliyorum?***
  - ***Neden inanmak veya çürütmek istiyorum?***
  - ***Fikrimi değiştirmemi sağlayacak şey ne?***

4. Etik ve Gizlilik:

- *Gizliliğimi yönetmek için araçları, ayarları ve tercihleri kullanıyorum.*
- *Çevrimiçi bir şeyler paylaştığımda diğer insanların mahremiyetine saygı duyuyorum.*
- *Müzik, oyun ve video gibi içeriklere etik bir şekilde nasıl erişeceğimi biliyorum.*
- *Adil Kullanım haklarımı ve kamuya açık alan ve Creative Commons TR medyasını nasıl kullanacağımı biliyorum.*
- *Bir vatandaş, tüketici ve insan olarak haklarımı ve bunları çevrimiçi olarak nasıl savunacağımı biliyorum.*

Dijital Ebeveynlik

Dijital vatandaş olmayı bildikten sonra, dijital ebeveynlik konusuna girebiliriz; Ebeveynlik, anne baba olarak kısa tanımı yapılsa bile, çocuğun yetiştirilmesinden birinci derecede sorumlu kişiler olarak da tanımlanabilir. Ebeveynlik çocuklarımıza örnek olmayı gerektiren bir sorumluluk göreviyle başlamaktadır. Çocuklar daima büyüklerini taklit ederek eğitim alırlar, büyüklerinin örnek olarak davranamadığı konular için de öğretim kaynaklarına başvurulur ve kitaplar, okul ve öğretmenler devreye girer.

Çocukların birincil eğitim kaynakları aile ve ebeveyn iken, öğretim kaynakları da okul ve öğretmenlerdir. Çocuklar ve gençler günümüzde bir üçüncü kaynağı da kullanarak tek başlarına öğrenme ve eğitim alabilmeye başlamışlardır. Dijital çağın getirilerinden olan akıllı telefon, bilgisayar ve medya alanları, çocuklarımızın kişisel gelişimi veya bozunumu için son derece önemli kaynakları oluşturmaktadır. Bu nedenle dijital vatandaş olan yetişkin bireyler aynı zamanda dijital ebeveynlik de yapmak zorundadırlar.

Çocukların sosyal, duygusal, psikolojik, zihinsel ve fiziksel gelişimlerini pek çok açıdan etkileyebilecek olan bu konuda ebeveynlerin çocukların dijital dünyasında iyi birer rehber olabilmesi ve teknolojinin doğru kullanım tarzlarını çocuklarına aşılayabilmeleri için sahip olmaları gereken özellikler "dijital ebeveynlik" kavramını doğurmuştur (TYC, 2019).

Çocuk asla dijital ortamda yalnız bırakılmamalı ve değişimi izlenmelidir.

Günümüzde özellikle çocukların oyalanması sebebiyle kontrolsüz olarak ellerine verilen bir medya aracı, onların işitsel, görsel ve bedensel eğitim araçları olabilmektedir. Bu sebeple, dijital ebeveyn olan bireyler, çocukların yaşlarına göre davranışlarını düzenlemelidirler, bu, anne baba tarafından yapılabileceği gibi, çocukla ilgilenen her birey tarafından da dikkat edilmesi gereken bir durumdur.

Bazı yapılabilir davranışları sayacak olursak; *(İSTEAMDER, 2020)*

5-7 yaş arasındaki çocuklar için yapılabilecekler;

- *Yanında olma ve katılma,*
- *Güvenlik yazılımı kullanma,*
- *Kişisel bilgilerin korunmasını anlatma,*
- *Kontrol etme,*
- *Süre sınırı getirme ve kararlı olma gibi davranışlar sergilenebilir.*

8-11 yaş grubundaki çocuklar için;

- *Sosyal medya kullanımı ve süresi konusunda anlaşma yapma,*
- *Güvenlik yazılımı kullanma,*
- *Dijital dünyada saygılı olmanın ve etik davranışların öğretilmesi,*
- *Tehlikelere karşı duyarlı olma gibi işlemlerin yapılması beklenebilir.*

12-14 yaş grubundaki çocuklar için;

- *Kimlerle görüştüklerini ve neler yaptıklarını anlatmasını sağlama,*
- *Yönlendirme ve denetleme,*
- *Güvenlik yazılımı kullanma,*
- *Dijital dünya sorumluluğu edindirme,*
- *Size danışmasını sağlama,*
- *Kişisel bilginin önemini hatırlatma,*

- *Mobil kullanım için kurallar koyma,*
- *Sözleşme imzalama gibi ciddiye alınma işaretleri sunma,*

15 yaş ve üzeri gruptaki bireyler için;

- *Kontrolden çok, yönlendirici olma,*
- *İnternetin yasal ve etik kullanımı hakkında açıklamalar yapma,*
- *Yer ve konum bildiriminin tehlikelerini açıklama ve dijital ayak izinin önemini vurgulama gibi işlemler yapılabilir.*

Ebeveynler, çocuğu topluma yararlı olabilecek niteliklerle donatmak için gerekli olan bilgileri onlara kazandırmalıdırlar. Bunun için de önce kendine saygı öğretilmelidir. Bu da ebeveynin çocuğa saygı konusunda örnek olmasını gerektirir.

Toplum içerisinde nasıl davranacağını ve kendisine nasıl davranılması gerektiğini bilen canlıların haklarını koruyabilecek vatandaşlar yetiştirmek her ebeveynin görevi olmalıdır.

7'DEN 70'E DİJİTAL GÜVENLİK VE GÜVENLİ İNTERNET KULLANIMI

İlker Bayrak
Büyükçekmece İlçe Milli Eğitim Müdürlüğü
Proje Koordinatörü
ilkerhocaturkce@gmail.com

Dijital güvenlik, her yaştan birey için giderek daha önemli hale gelen bir konudur.

İnternetin sağladığı olanaklardan faydalanırken, güvenli bir şekilde hareket etmek herkesin sorumluluğundadır ve yaş gruplarına göre dikkat edilmesi gereken konular farklı nitelikler taşıyabilir.

Çocuklar:

- ***Gizlilik Eğitimi:*** Bu yaş grubunda ilk olarak çocuklara kişisel bilgilerini paylaşmamaları gerektiği öğretilmelidir. Adres, telefon numarası ve okul bilgileri gibi veriler gizli tutulmalı, fotoğraf ve video paylaşımı konusunda gerekli bilgilendirmeler yapılmalıdır. Yüz bulanıklaştıma, fotoğraf yerine avatar kullanma, yakın çekim fotoğraf ve video kesinlikle paylaşmama gibi konularda çocuklara gerekli bilgilendirme ve yönlendirmeler yapılmalıdır.
- ***İnternet Güvenliği:*** Çocuklar, güvenli web siteleri ve uygulamalar hakkında bilgilendirilmelidir. Tanımadıkları kişilerle iletişim kurmamaları gerektiği vurgulanmalıdır.
- ***Ebeveyn Denetimi:*** Ebeveynlerin, çocuklarının internet kullanımını izlemesi ve belirli zaman dilimle-

rinde kısıtlamalar getirmesi önemlidir. Çocukların internete erişebildiği cihazlara ebeveyn denetim programları kurulmalıdır. Ebeveyn Denetimleri sayesinde çocukların internet erişimlerine sınır koyulabilir, hangi oyunları oynayıp, hangi programları çalıştırabilecekleri belirlenebilir, oturum açma saatlerine karar verilebilir. Ebeveyn Denetimlerinde bir Web sayfasına veya oyuna erişim engellendiğinde, programın veya Web sayfasının engellendiğini bildiren bir uyarı görüntülenir. Ebeveynler kendi hesap bilgilerini girerek bu bağlantılara ya da programlara izin verebilir ya da neden uygun olmadığı konusunda çocuklarını bilgilendirebilirler.

Gençler:

- ***Sosyal Medya Bilinci:*** Gençler, paylaşımlarının çevrimiçi kalıcı olduğunu anlamalıdır. Sosyal medya hesaplarını gizli tutarak tanımadıkları kişilerden gelen takip isteklerini geri çevirmeli ve hesaplarına tam koruma sağlamayı ebeveyn ve öğretmenleri aracılığıyla öğrenmeliler.
- ***Siber Zorbalık:*** Siber zorbalık hakkında bilgi edinmeli ve karşılaştıklarında nasıl davranmaları gerektiğini öğrenmelidirler.
- ***Güçlü Şifre Kullanımı***: Güçlü ve karmaşık şifreler oluşturma alışkanlığı kazanmalıdırlar. Aynı şifreyi farklı hesaplarda kullanmamalıdırlar.

Tehlikeli olabilecek her tür online oyunla ilgili de bilgilendirilmelidirler.

Yetişkinler:

- ***Güvenlik Yazılımları:*** Antivirüs programları ve güvenlik duvarları kullanarak cihazlarını korumalıdırlar. Yazılımları güncel tutmak önemlidir.
- ***Phishing (Aldatıcı E-postalar):*** Dolandırıcılık amacıyla gönderilen e-postalara karşı dikkatli olmalı ve tanımadıkları bağlantılara tıklamamalıdırlar.
- ***Veri Paylaşımı:*** Kişisel bilgiler paylaşmadan önce dikkatli olunmalı, e-devlet, internet bankacılığı gibi platformlara giriş yaparken site uzantıları ve güvenli olup olmadığı kontrol edilmeli, yapılacak işlerin tamamlanmasının ardından güvenli çıkış yapılması önemlidir.

Yaşlılar (60 yaş ve üzeri):

- ***Eğitim ve Bilinçlendirme:*** Dijital okuryazarlık kurslarına katılmaları teşvik edilmelidir. İnternetin temel işleyişi hakkında bilgi sahibi olmaları önemlidir.

- ***Güvenli Alışveriş:*** Çevrimiçi alışveriş yaparken güvenilir siteleri tercih etmeleri gerektiği öğretilmelidir. Kredi kartı bilgilerini güvende tutma bilinci kazandırılmalıdır. Sanal kart kullanımı teşvik edilebilir.
- ***Destek ve Yardım:*** Yakınlarından veya güvenilir kişilerden yardım alarak dijital dünyada daha güvende hissetmeleri sağlanmalıdır.

Genel Öneriler:

- ***Farkındalık ve Bilinç:*** Herkes, dijital güvenlik ve mahremiyet konularında bilinçlenmeli ve sürekli kendini geliştirmelidir.
- ***Güvenli İnternet Ortamı:*** İnternetin sunduğu olanaklardan faydalanırken, güvenli bir ortamda kalmak için gerekli önlemler alınmalıdır.

Avrupa Dijital Haklar ve İlkeler Bildirgesi:

7'den 70'e Bir Yol Haritası

Avrupa Dijital Haklar ve İlkeler Bildirgesi, Avrupa değerleri ile şekillenen bir dijital geçişi teşvik etmektedir. Avrupa Birliği (AB), dijital geçişin sunduğu fırsatlardan herkesin yararlanabilmesi için bireyleri güçlendirmeyi hedeflemektedir. Bu amaçla, AB değerlerini yansıtan ve insan merkezli, güvenli ve sürdürülebilir bir dijital dönüşüm vizyonunu destekleyen dijital haklar ve ilkeler benimsenmiştir.

Bildirge, Avrupa Komisyonu, Avrupa Parlamentosu ve Konseyi başkanları tarafından imzalanmış olup, AB ve Üye Devletlerin bu hakları ve ilkeleri teşvik etme konusundaki yüksek siyasi taahhütlerini göstermektedir. Bildirge, AB Temel Haklar Şartı'na dayanmaktadır ve dijital dönüşümdeki ifade özgürlüğü, veri koruma ve mahremiyet gibi önemli hakları hatırlatmaktadır. Dijital haklar ve ilkeler, AB mevzuatı ve politikalarıyla desteklenerek vatandaşlar için somut hale gelmektedir.

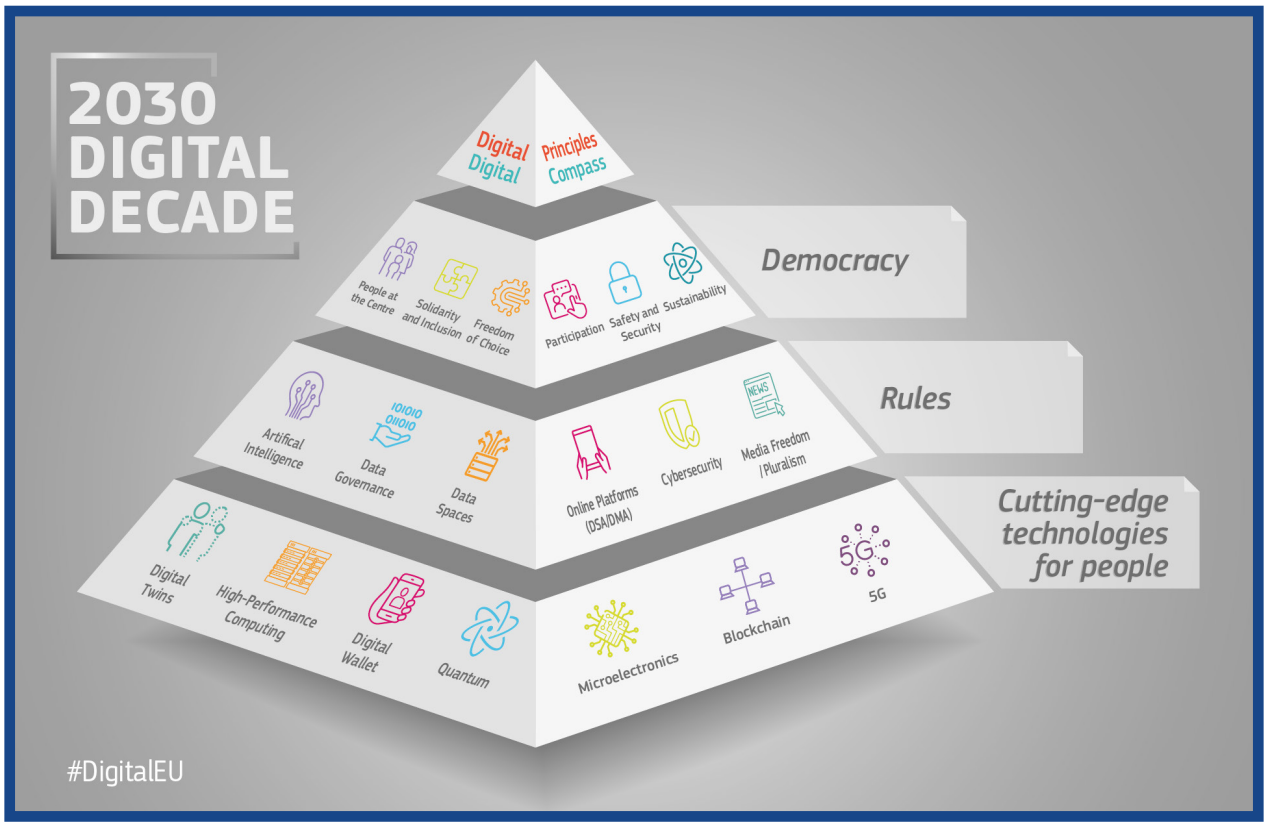
Bildirge ile AB ve Üye Devletler, insan merkezli bir dijital dönüşüm vizyonunu hem ulusal düzeyde hem de uluslararası alanda teşvik etme taahhüdünde bulunmaktadır. Komisyon, dijital hakların ve ilkelerin AB genelinde uygulanmasını izlemektedir.

Temel İlkeler:

1. ***İnsanların Merkezde Olması:*** Teknoloji, tüm vatandaşların yararına hizmet etmeli ve onların haklarını ihlal etmemelidir.
2. ***Dayanışma ve Kapsayıcılık:*** Herkesin uygun fiyatlı, yüksek hızlı dijital bağlantıya erişimi olmalı ve dijital teknolojilerin faydalarından yararlanabilmesi için gerekli eğitim ve becerileri edinmesi sağlanmalıdır.

3. ***Tercih Özgürlüğü:*** Bireyler, çevrimiçi olarak bilinçli seçimler yapma hakkına sahip olmalıdır. Yapay zekâ sistemleri, insanın refahını artırmayı hedefleyen araçlar olmalıdır.
4. ***Dijital Kamu Alanında Katılım:*** Herkes güvenilir, çeşitli ve çok dilli bir çevrimiçi ortama erişebilmelidir. Bu, demokratik katılımı teşvik etmektedir.
5. ***Güvenlik ve Emniyet:*** Tüm bireyler, güvenli ve mahremiyeti koruyan dijital teknolojilere erişim sağlamalıdır. Özellikle çocuklar ve gençler, çevrimiçi ortamda güvenli seçimler yapabilmeli ve yaratıcılıklarını ifade edebilmelidir.
6. ***Sürdürülebilirlik:*** Dijital ve yeşil geçişler birbirine bağlıdır. Dijital ürünler ve hizmetler, çevre dostu bir şekilde tasarlanmalı, üretilmeli ve elden çıkarılmalıdır.

Avrupa Dijital Haklar ve İlkeler Bildirgesi, vatandaşlara AB dijital yasaları ve politikaları arasında bir köprü sunmakta, AB'nin dijital dönüşüm yolundaki yönünü göstermektedir. Komisyon, dijital hakların uygulanmasını izleyerek her yıl raporlar yayınlamakta ve Üye Devletlerin en iyi uygulamalarını teşvik etmektedir. Bildirge, AB'nin uluslararası ilişkilerini de yönlendirerek, insan haklarını merkez alan küresel bir dijital dönüşümü şekillendirmeye yardımcı olmaktadır.



SİBER ZORBALIK: EKRANIN ARKASINA SAKLANMAK

Prof. Dr. Buket Akkoyunlu
Çankaya Üniversitesi
Eğitim Teknolojisi ABD.
buket@cankaya.edu.tr

Giriş

Siber zorbalık, dijital dünyada giderek artan bir tehlike haline gelmiştir. Ancak çevrimiçi ortamda nasıl güvende kalabiliriz? Siber zorbalık, dijital dünyada artan bir tehlike olarak karşımıza çıkmakta, "Ekranın Arkasına Saklanmak" ifadesi ise, zorbalık yapan bireylerin çevrimiçi platformlar aracılığıyla kimliklerini gizleyerek veya fiziksel mesafe sağladıkları bir alan yaratmalarına işaret etmektedir (Peebles, 2014). Siber zorbalık, bir kişinin başka bir kişiyi internet, sosyal medya, mesajlaşma platformları veya diğer dijital ortamlarda tehdit etmesi, aşağılaması, utandırması ya da taciz etmesi anlamına gelir. Bu zorbalık türünde fail, genellikle "ekranın arkasına saklanarak" kimliğini gizleyebilir ya da kendini daha güçlü ve güvende hissedebilir. Bu "ekranın arkasına saklanma" durumu, zorbalık yapan bireyin kendisini fiziksel bir karşılaşma tehdidinden uzak hissetmesine, dolayısıyla davranışlarında daha pervasız olmasına neden olmaktadır. Siber zorbalığın mağdurlar üzerinde ciddi etkileri vardır. Mağdurlar üzerinde psikolojik açıdan anksiyete, depresyon, özgüven kaybı ve özsaygı düşüşüne neden olurken; sosyal alanda ise izolasyon, arkadaşlık ilişkilerinin zedelenmesi ve çevrim içi ortamlardan uzaklaşma gibi sonuçlar doğurur. Bu etkiler, mağdurların uzun vadede yaşam kalitesini düşürebilir ve zihinsel sağlığını olumsuz etkileye-

bilir. Siber zorbalıkla mücadele, hem mağdurların kendilerini koruyabilmesi hem de toplumsal farkındalık yaratılması açısından büyük önem taşır. Bu nedenle, dijital ortamlarda zorbalıkla başa çıkmak daha karmaşık hale gelir. Sonuç olarak, siber zorbalık, dijital çağın bir gerçeği haline gelmiştir. Bu sorunla başa çıkmak için bireysel farkındalığın artırılması, hukuki düzenlemelerin güçlendirilmesi ve teknoloji şirketlerinin bu konuda daha fazla sorumluluk alması gerekmektedir. Siber zorbalıkla mücadelede toplumun her kesimi aktif bir rol üstlenmelidir.

Bu bölüm siber zorbalığın tanımı, yaygınlığı, etkileri, risk ve koruyucu faktörleri hakkında kapsamlı bir bakış açısı sunmayı amaçlamakta, siber zorbalıkla mücadele yolları tartışılmaktadır.

Siber Zorbalık Nedir?

İnternetin yaygın olarak benimsenmesi, insanların sosyalleşmesi, iletişim kurması, öğrenmesi ve boş zamanlarını en iyi şekilde değerlendirmesi için pratik yollar sunmuş, aynı zamanda yeni tehlikeleri de beraberinde getirmiştir. Hem dünyada hem de ülkemizde siber zorbalık giderek yaygınlaşırken, aynı zamanda önemli bir sosyal sorun haline dönüşmektedir (Donat Bağcıoğlu, 2022; Peebles, 2014). Literatürde "siber zorbalık," "siber suç," "çevrimiçi taciz," "elektronik saldırganlık," "elektronik mağduriyet" veya "internet tacizi" gibi terimler de siber zorbalık kavramı ile birbirinin yerine kullanılmaktadır (Elsaesser ve diğerleri 2017; Kim ve diğerleri 2017; Selkie ve diğerleri 2016; Kowalski ve diğerleri, 2008; Vandebosch ve Van Cleemput, 2008).

Hinduja ve Patchin'e (2017) göre, siber zorbalık, bilgisayarlar, cep telefonları veya diğer elektronik cihazlar kullanılarak gerçekleştirilen kasıtlı, tekrarlayıcı ve zarar verici eylemleri kapsar olarak tanımlanırken; Akdeniz ve Doğan'a göre (2024), dijital ortamlar aracılığıyla bir kişiye karşı kasıtlı olarak gerçekleştirilen zarar verici davranışlar olarak tanımlanır. Alternatif bir tanıma göre, siber zorbalık, elektronik veya dijital medya aracılığıyla bireylere veya gruplara düşmanlık veya saldırganlık içeren mesajların tekrar tekrar iletilmesini içeren ve rahatsızlık veya zarar verme amacı taşıyan davranışları kapsar (Englander ve diğerleri 2017). Siber zorbalık, Smith ve arkadaşları tarafından (2008) bir grup veya birey tarafından, elektronik iletişim biçimleri kullanılarak, bir mağdura karşı tekrarlayan ve zamanla devam eden, mağdurun kolayca kendini savunamayacağı şekilde gerçekleştirilen saldırgan ve kasıtlı bir eylem olarak rapor

edilmektedir. Bu tanım, fiziksel ortamlarda gerçekleşen geleneksel zorbalıktan farklı olarak, coğrafi sınırlamaların ötesine geçer ve mağdura sürekli olarak ulaşabilir (Erdur Baker ve Kavşut, 2007).

Geleneksel zorbalık, bir kişinin fiziksel, sözel veya sosyal olarak diğer bir kişiye yönelik yaptığı aşağılayıcı veya zarar verici eylemleri içerir. Genellikle yüz yüze gerçekleşir ve mağdura doğrudan etki eder. Okulda, iş yerinde veya toplum içinde görülebilir. Bu zorbalık türü, mağdura duygusal, fiziksel veya sosyal zarar verme amacı taşır. Fiziksel veya sözlü taciz, sosyal dışlama ya da dedikodu yoluyla yapılır. Dijital ortamda gerçekleşen siber zorbalık, fiziksel ortamdan bağımsızdır; internetin olduğu her yerde yapılabilir. Geleneksel zorbalık belirli zamanlarda ve mekânlarda gerçekleşir, bir öğrenci yalnızca okuldayken zorbalığa maruz kalabilir. Siber zorbalık ise 7/24 devam edebilir. İnternet bağlantısı olan her yerden mağdura ulaşılabilir (Hay, Meldrum ve Mann, 2010).

Siber zorbalık ile geleneksel zorbalık arasındaki farklar ortam, anonimlik, erişim süresi, yayılma hızı ve kalıcı etki özellikleri açısından Tablo 1'de özetlenmiştir.

Özellik	Siber Zorbalık	Geleneksel Zorbalık
Ortam	Dijital ortam (sosyal medya, e-posta vb.)	Fiziksel ortam (okul, iş yeri, sokak gibi yüz yüze alanlar.)
Anonimlik	Zorbayı tanımak zor olabilir, anonim olarak yapılabilir.	Zorbanın kimliği genellikle bilinir.
Erişim Süresi	7/24 erişim, sürekli tehdit.	Genellikle belirli yer ve saatlerde gerçekleşir.
Yayılma Hızı	İnternet üzerinden hızlıca geniş kitlelere yayılabilir.	Zorbalık, belirli bir grupla sınırlıdır.
Kalıcı Etki	Dijital içerikler uzun süre internet üzerinde kalabilir.	Olaylar genellikle yüz yüze anlık gerçekleşir, kalıcı etkisi sınırlıdır.

Tablo 1: Siber zorbalık ile geleneksel zorbalık arasındaki farklar

Mesajlar, paylaşımlar, yorumlar veya e-postalar gibi yazılı kanıtlar kolayca belgelenebilir. Bu dijital izler, hukuki süreçlerde delil olarak kullanılabilir. Ancak bu durum mağdur için tekrar tekrar travmatik bir etki yaratabilir, çünkü zorbalık içeriği tekrar tekrar görüntülenebilir (Cosma ve diğerleri; 2020; Sticca ve Perren, 2013).

Dijital Dünyada Anonimlik

Dijital dünyada anonimlik, siber zorbalığın en belirgin özelliklerinden biridir. Bu, kişilere zorbalık yaparken kimliklerini gizleyebilme ve fark edilmeden zarar verme imkânı sunar. Bu anonimlik unsuru, siber zorbalık yapan kişiye yüz yüze zorbalıkta sahip olmayacağı bir güç verir ve bu güç, kimi zaman daha acımasız ve tehlikeli zorbalık eylemlerine yol açabilir. Dijital platformlarda sahte hesap açmak kolaydır ve bu da zorbanın farklı isimler altında aynı kişiyi tekrar tekrar hedef almasını sağlar. Bu, mağdurun üzerindeki psikolojik baskıyı artırır çünkü mağdur, karşısında kaç farklı zorba olduğunu veya zorbanın kim olduğunu bilemez. İnternet ortamında, özellikle kişinin anonim olduğuna dair hissettiği sahte güven duygusunun arkasına sığınarak, başka kullanıcılara serbestçe hakarete varan ifadeler kullanması ve sosyal medya hesaplarından siber zorbalığın giderek yaygınlaşarak, önemli bir sosyal soruna dönüştüğü görülmektedir (Maviş, 2021; Erdur Baker ve Kavşut, 2007).

Siber zorbalığın anonim olması, mağdurlar üzerinde derin ve yıkıcı etkiler yaratabilir. Mağdur, zorbanın kimliğini bilmediği için zorbalık her an devam edebilir gibi hisseder. Anonim zorbalık, mağduru sürekli tetikte olmaya zorlar, bu da günlük yaşamında bile güvensizlik hissetmesine yol açar. Anonim bir saldırganla karşı karşıya olan mağdur, kim tarafından veya neden hedef alındığını bilemediği için kendini savunmakta zorlanır. Bu belirsizlik, mağdurun sürekli stres içinde yaşamasına ve günlük hayatında konsantre olamamasına sebep olabileceği gibi, zorbanın kimliğini bilmediği için çevresindeki insanlara güvenmekte zorlanabilir (Maviş, 2021; Bingöl ve Tanrıkulu, 2014).

Anonimliğin sağladığı güç, zorbanın kendini gizleyerek daha acımasız davranmasına yol açarken, mağdur üzerinde de kalıcı olumsuz etkiler yaratır. Bir başka deyişle. siber zorbalığın anonimlik boyutu, zorbalık yapan kişiye yüz yüze zorbalıkta sahip olamayacağı bir güç sağlar.

Siber Zorbalıkta Güç

Siber zorbalıkta güç, zorbanın dijital ortamda sağladığı avantajları kullanarak mağduru baskı altına alması, korkutması ya da psikolojik olarak etkilemesi anlamına gelir. Siber zorbalık yapan kişiler, dijital ortamın sağladığı bazı özelliklerle kendilerini güçlü hisseder ve mağduru daha kolay kontrol altına alabilirler. Bu güç, fiziksel zor-

balıktan farklı olarak anonimlik, geniş kitlelere ulaşma ve sürekli erişim gibi dijital avantajlarla desteklenir.

Anonim bir zorba, mağdura sürekli mesaj atarak veya tehditlerde bulunarak kendini güçlü hisseder, çünkü kimliğini saklayarak kendini savunmasız bırakmaz. Zorba, dijital dünyada 7/24 erişim imkânına sahiptir, bu da mağduru her an hedef alabileceği anlamına gelir. Mağdurun çevrimdışı olduğu bir ortam olmadığı için zorbalık sürekli hale gelebilir ve zorbanın mağdur üzerinde kurduğu baskı daha güçlü bir hale gelir (Akgül, 2020; Bingöl ve Tanrıkulu, 2014; Erdur Baker ve Kavşut, 2007). Zorbanın sahip olduğu güç, mağduru sürekli stres, korku ve güvensizlik içinde bırakır. Zorbanın psikolojik baskısı nedeniyle mağdur, sosyal çevresinden uzaklaşabilir, özgüven kaybı yaşayabilir ve hatta depresyon gibi psikolojik sorunlarla karşı karşıya kalabilir. Sürekli tehdit veya alaycı mesajlar, mağdurun kendine olan saygısını azaltırken dijital dünyadan da uzaklaşmasına yol açabilir. Özetle, siber zorbalıkta güç, dijital dünyanın sunduğu olanaklardan yararlanılarak mağdur üzerinde baskı kurma ve psikolojik etki yaratma becerisi olarak öne çıkar. Bu güç, mağdur üzerinde kalıcı olumsuz etkiler bırakabilir ve zorbalıkla mücadeleyi daha zor hale getirir (Maviş, 2021; Akgül, 2020).

Siber Zorbalıkta Niyet

Siber zorbalıkta niyet de zorbalığın temel bir unsurudur ve zorbalığı yapan kişinin kasıtlı olarak karşı tarafa zarar verme amacını ifade eder. Dijital ortamda gerçekleştirilen bu tür zorbalıklarda zorbanın asıl amacı, mağdura psikolojik olarak zarar vermek, onu küçük düşürmek ya da korkutmak olabilir. Niyet, siber zorbalık vakalarının ciddi sonuçlar doğurmasına katkıda bulunur, çünkü zorba bilinçli bir şekilde mağdurun duygusal sağlığını hedef alır (Akgül, 2020; Bingöl ve Tanrıkulu, 2014).

Zorba, mağdura kasıtlı olarak duygusal, sosyal veya psikolojik zarar vermek ister. Bu, mağduru aşağılamak, utandırmak veya toplumdan dışlanmasına yol açmak gibi çeşitli niyetler içerir. Bu tür bir kasıt, zorbalığın etkisini daha yıkıcı hale getirir. Zorba, mağduru tehdit ederek veya rahatsız edici mesajlarla sürekli baskı altında tutarak kendini güçlü hissetmek ister. Bu güç gösterisi, zorbanın niyetinin mağduru kontrol etmek ya da sindirmek olduğunu gösterir. Siber zorbalık bazen kişisel bir durumdan veya anlaşmazlıktan kaynaklanan intikam niyetiyle yapılabilir. Örneğin, arkadaşlar arasında yaşanan bir tartışma sonrasında bir kişi, diğerine siber zorbalık yaparak öç

almak isteyebilir. Bazı zorbalık vakalarında zorbanın niyeti sadece eğlenmek ya da dikkat çekmektir. Ancak bu tür davranışlar da mağdurlar üzerinde ciddi psikolojik baskılar yaratır. Eğlence amacıyla yapılan zorbalık, genellikle mağduru alay konusu yapma veya küçük düşürme içerir. Siber zorbalık, mağdurun itibarını zedelemek amacıyla da yapılabilir. Sosyal medya hesaplarından yanlış veya iftira niteliğinde bilgiler paylaşarak mağdurun toplumdaki saygınlığını sarsmak, zorbanın niyetinin bir parçası olabilir (Maviş, 2021; Akgül, 2020; Erdur Baker ve Kavşut, 2007).

Siber Zorbalığın Farklı Türleri

Siber zorbalık, farklı tutum ve davranış biçimleriyle karşımıza çıkabilir. Bu tür zorbalıklar bazen teknik bilgi gerektiren uzmanlarca gerçekleştirilirken bazen de bilgiye dayalı olarak ortaya çıkmaktadır. Siber zorbalık birçok şekilde olabilir ve genellikle insanlara isim takmak, onları lanetlemek, onlar hakkında yalanlar yaymak veya onları incitmeye veya zorbalık etmeye çalışmak olarak yorumlanabilecek başka herhangi bir davranış gibi görünür (Maviş, 2021; Dilmaç, 2020; Hinduja ve Patchin 2017).

Siber zorbalık türleri aşağıda sıralanmıştır.

- **Öfkelendirme:** Bu tür, genellikle çoklu bireyler arasında hakaret ve küfre varan argo dil kullanımıyla görülür. Sanal sohbet platformları, çevrimiçi oyunlar ve tartışma içerikli bloglar gibi halka açık dijital ortamlarda karşılaşılan bu tür zorbalık, daha sonra tehditlerin öfkeye dönüşmesiyle devam edebilir.
- **Sanal Taciz:** Kişiye yönelik tekrar eden tehdit, hakaret ve saldırganlık içeren mesajların sürekli olarak gönderilmesi şeklinde gerçekleşir. İnternet tabanlı mesajlaşma uygulamaları, e-posta ve anlık mesajlar aracılığıyla yazılı olarak yapılır ve sıklıkla çoklu saldırılar ile tehdit içerikleri içerir. Bu tür zorbalıkta, mağdur çevrimiçi olduğu anda rahatsız edici mesajlarla karşılaşır.
- **İftira ve Karalama:** Hedef kişiyi itibarsızlaştırmak amacıyla doğru olmayan dedikodular yayılır. Bu, mağdurun saygınlığını zedelemek için halka açık platformlarda herkesin görebileceği şekilde yapılan manipülatif paylaşımlar içerir.
- **Taklit ve İfşa Etme:** Zorba, başkasıymış gibi davranarak kurbanı aşağılayıcı içerikleri paylaşır. Sosyal medya hesaplarına veya iletişim kanallarına ait şifrelerin başkalarıyla paylaşılması sonucu kurban adına alaycı veya mahrem içerikler ifşa edilir. Bu tür zorbalıkta, mağdur el-

lerindeki içeriklerle tehdit edilerek istenmeyen bir eyleme zorlanabilir.

- **Dışlama:** Çoğunlukla çevrimiçi oyunlar, tartışma blogları veya mesaj gruplarında yaşanan anlaşmazlıklar sonucu kişiyi gruptan atma veya engelleme şeklinde ortaya çıkar.
- ***Rahatsız Etme:*** Tehdit edici veya aşağılayıcı mesajların sürekli gönderilmesi yoluyla mağdurun korkutulması, alaya alınması ve küçük düşürülmesi amaçlanır.

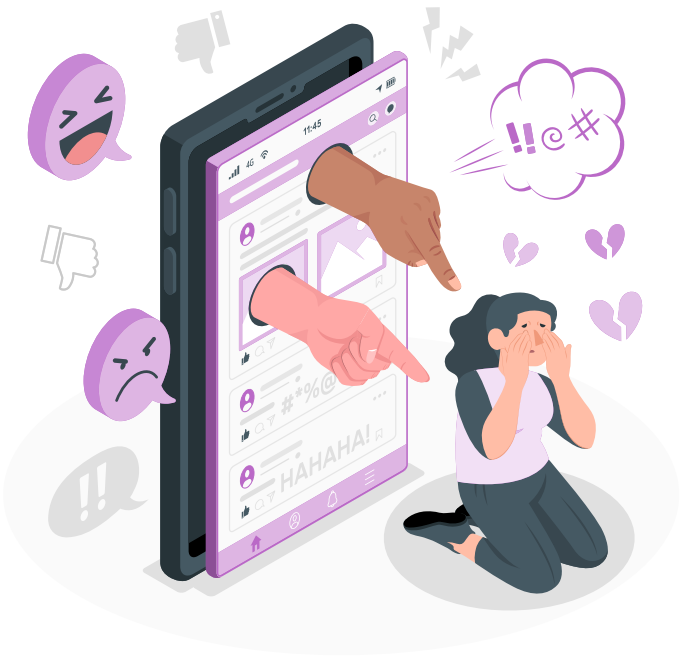
Bu zorbalık biçimleri, dijital dünyada mağdurlar üzerinde ciddi olumsuz etkiler yaratır ve çoğu zaman sürekli bir psikolojik baskıya yol açar (Baştürk ve Sayımer, 2017; Betts, 2015; Kowalski ve diğerleri 2008).

Tablo 2'de Siber zorbalık türleri örneklerle özetlenmiştir.

Siber Zorbalık Türü	Açıklama	Örnek
Öfkelendirme	Hakaret ve küfür içeren argo dil kullanımı. Halka açık platformlarda başlayıp tehditlerle devam edebilir.	Bir öğrenci, çevrimiçi oyun sırasında diğer oyunculara hakaret eder ve kışkırtıcı söylemlerle tartışmayı alevlendirir. İlerleyen süreçte doğrudan tehditler savurur.
Sanal Taciz	Tekrarlanan tehdit ve hakaret mesajları gönderilmesi. Çoklu saldırılar ve tehditler içerir.	Bir kişi, eski partnerine sosyal medya ve mesajlar aracılığıyla sürekli tehdit ve hakaret mesajları gönderir. Mağdur, her çevrimiçi olduğunda rahatsız edici mesajlarla karşılaşır.
İftira ve Karalama	Mağdur hakkında yanlış dedikodular yayarak itibarını zedeleme. Halka açık platformlarda paylaşılır.	Bir sosyal medya hesabı, bir öğrenci hakkında yalan yanlış bilgiler paylaşıp itibarını zedeler. Bu içerikler, okul arkadaşları tarafından görülebilir ve mağdurun sosyal çevresini etkileyebilir.
Taklit ve İfşa	Başka bir kişiymiş gibi davranarak mağduru küçük düşürücü içerikler paylaşma ve tehdit yoluyla eyleme zorlama.	Bir zorba, mağdurun sosyal medya hesabına erişerek alaycı ve küçük düşürücü içerikler paylaşır. Mağdur, bu içeriklerin kaldırılması karşılığında istenmeyen bir eyleme zorlanır.
Dışlama	Çevrimiçi oyunlar veya gruplardan dışlama veya engelleme şeklinde ortaya çıkar.	Bir grup öğrenci, bir arkadaşını çevrimiçi sohbet grubundan çıkarır ve onu oyunlara veya grup sohbetlerine dahil etmez, dışlayarak mağduriyet yaratır.
Rahatsız Etme	Mağduru korkutmak ve aşağılamak amacıyla tehdit edici mesajların sürekli gönderilmesi.	Bir kullanıcı, başka bir kullanıcıya sürekli tehdit veya aşağılayıcı mesajlar gönderir, mağduru korkutur ve kendini kötü hissetmesine neden olur.

Tablo 2: Örneklerle siber zorbalık türleri

Siber zorbalığın mağdurlar üzerinde ciddi etkileri vardır. Mağdurların, bilişsel, duygusal, sosyal ve akademik gelişimleri üzerindeki olumsuz etkileri, hem kısa hem de uzun vadede gözlemlenmiştir (Kowalski ve diğerleri 2008). Anksiyete, depresyon ve özgüven kaybı gibi duygusal zorluklara yol açabilir. Özellikle gençler, sosyal medya aracılığıyla zorbalıkla karşı karşıya kaldıklarında, çevrimiçi dünyadan kopmaları zor olabilir. Bu nedenle, dijital ortamlarda zorbalıkla başa çıkmak daha karmaşık hale gelir.



Siber Zorbalığın Psikolojik ve Sosyal Etkileri

Siber zorbalık, mağdurlar üzerinde hem psikolojik hem de sosyal alanda ciddi ve uzun süreli etkiler yaratabilir. Dijital ortamda gerçekleşen zorbalık, mağdurların özgüvenini zedeleyebilir, sosyal ilişkilerini etkileyebilir ve duygusal olarak yıpratıcı olabilir. Bu etkiler, zorbalığın süresi ve yoğunluğuna bağlı olarak değişiklik gösterebilir.

Siber zorbalığın psikolojik etkilerini anksiyete ve stres, depresyon, özgüven kaybı, öz saygı düşüşü ve kendine zarar verme eğilimleri olarak sıralayabiliriz.

Anksiyete ve stres, siber zorbalık mağdurları sürekli olarak çevrimiçi ortamda tehdit edici veya aşağılayıcı içeriklerle karşılaştıkları için kaygı ve stres yaşayabilirler. Bu tür saldırılar, kişinin günlük hayatını ve sağlığını etkileyebilir, uyku problemleri ve gerginlik gibi belirtiler ortaya çıkabilir. Depresyon, sürekli olarak dijital zorbalığa maruz kalan bireyler, zamanla değersizlik ve çaresizlik hissi yaşayabilirler. Sosyal çevrelerinden dışlandıklarını veya küçük düşürüldüklerini hissettiklerinde depresyon riski artar. Bu durum, kişinin kendine olan güvenini azaltır ve kendini sosyal çevresinden uzaklaştırabilir.

Özgüven kaybı, siber zorbalık, özellikle gençlerde özgüven kaybına yol açabilir. Zorbalık içerikli mesajlar veya hakaretler, mağdurun kendine olan güvenini sarsar ve kendini değersiz hissetmesine neden olabilir. Mağdur, başkalarının kendisi hakkında kötü

düşündüğünü düşünebilir ve bu durum sosyal ilişkilerini etkileyebilir. Siber zorbalığa maruz kalan bireyler, kendilerini toplumda değersiz hissedebilirler. Zorbalığın yoğunluğuna bağlı olarak birey, kendi kimliği ve kişiliği hakkında olumsuz düşünceler geliştirebilir, kendisini toplumdan soyutlama eğilimi gösterebilir. Kendine zarar verme eğilimleri, siber zorbalık, mağdurlar üzerinde derin psikolojik yaralar açabilir.

Uzun süreli zorbalığa maruz kalan bazı bireyler, kendine zarar verme düşüncelerine ya da davranışlarına yönelebilir. Özellikle genç yaş gruplarında bu durum ciddi bir risk oluşturur.

Siber zorbalığın sosyal etkilerini sosyal izolasyon, arkadaşlık ilişkilerinin zedelenmesi, akademik ve iş performansının düşmesi, çevrimiçi ortamlardan uzaklaşma ve toplumsal güven kaybı olarak sıralayabiliriz.

Sosyal izolasyon, siber zorbalık mağdurları, zorbalığın etkisinden kurtulmak için sosyal medya platformlarından ve çevrim içi topluluklardan uzaklaşmayı tercih edebilirler. Bu durum, sosyal çevrelerinden izole olmalarına ve kendilerini yalnız hissetmelerine neden olabilir. Arkadaşlık ilişkilerinin zedelenmesi, siber zorbalığa maruz kalan bireyler, kendilerini sosyal çevrelerinde güvende hissetmeyebilir ve bu nedenle arkadaşlık ilişkilerini sınırlandırabilir. Zorbalığın arkadaş çevresinden gelmesi durumunda, mağdurun ilişkileri zedelenebilir ve kişi, yalnızlaşabilir. Akademik ve iş performansının düşmesi, okulda veya iş yerinde siber zorbalığa maruz kalan bireylerin motivasyonları düşebilir. Dikkat dağınıklığı ve stres nedeniyle akademik veya iş performansları olumsuz etkilenebilir. Mağdurlar, zorbalık nedeniyle iş yerinde veya okulda verimsiz hale gelebilir. Çevrimiçi ortamlardan uzaklaşma, siber zorbalık mağdurları, çevrim içi ortamlardan kaçınarak zorbalıkla başa çıkmaya çalışabilir. Sosyal medya platformlarından, forumlardan veya çevrim içi oyunlardan uzak durmak, mağdurların kendilerini dijital dünyadan soyutlamalarına neden olabilir. Toplumsal güven kaybı, siber zorbalık, mağdurun toplumdaki insanlara olan güvenini sarsabilir (Donat Bağcıoğlu, 2022).

Özellikle zorbanın anonim olması durumunda, mağdur kime güveneceğini bilemez hale gelir ve toplumdaki insanlara karşı mesafeli bir tutum geliştirebilir.

Tablo 3'de siber zorbalığın psikolojik ve sosyal etkilerini örneklerle açıklanmıştır.

Etkiler	Açıklama	Örnek
Anksiyete ve Stres	Sürekli tehdit veya hakaret mesajları nedeniyle sürekli gerginlik ve endişe durumu.	Bir öğrenci, sosyal medyada sürekli alay edildiği için okula gitmek istemez, sürekli stres yaşar.
Depresyon	Değersizlik ve çaresizlik hisleri nedeniyle duygu durum bozuklukları.	Bir genç, sürekli aşağılayıcı mesajlar aldığı için kendini değersiz hisseder ve içine kapanır.
Özgüven Kaybı	Kendine olan güvenin zedelenmesi ve kendini değersiz hissetme durumu.	Zorbalıkla hedef alınan bir kişi, sosyal medyada alay edildiği için özgüvenini kaybeder ve fotoğraf paylaşmaktan çekinir.
Özsaygı Düşüşü	Kendisini toplumda yetersiz ve değersiz hissetme.	Bir birey, hakkındaki yalan içeriklerden dolayı toplum içinde kendisini değersiz hissetmeye başlar.
Kendine Zarar Verme	Uzun süreli zorbalık nedeniyle psikolojik olarak yıpranma ve kendine zarar verme eğilimleri.	Akranları tarafından sosyal medyada sürekli tehdit edilen bir genç, depresyon nedeniyle kendine zarar verme eğilimi gösterir.
Sosyal İzolasyon	Sosyal çevreden uzaklaşma ve yalnızlaşma eğilimi.	Mağdur, sürekli çevrim içi alay konusu olduğu için sosyal medyayı bırakır ve arkadaşlarıyla görüşmemeye başlar.
Arkadaşlık İlişkilerinde Bozulma	Zorbalık nedeniyle arkadaş çevresine olan güvenin azalması.	Bir grup sohbetinde zorbalığa uğrayan birey, arkadaş grubuna güvenini yitirir ve kendini geri çeker.
Akademik ve İş Performansı Düşüşü	Zorbalık nedeniyle konsantrasyon kaybı ve verimsizlik.	Sosyal medyada sürekli eleştirilen bir öğrenci, derslerine odaklanmakta zorlanır ve notları düşer.
Çevrim İçi Ortamlardan Uzaklaşma	Dijital dünyadan ve sosyal medyadan kaçınma isteği.	Mağdur, sürekli rahatsız edici mesajlar aldığı için sosyal medya hesaplarını kapatır.
Toplumsal Güven Kaybı	Toplumdaki insanlara olan güvenin azalması ve mesafeli davranma.	Zorbanın kimliğinin bilinmemesi nedeniyle mağdur, çevresindeki insanlara şüpheyle yaklaşır ve sosyal ortamlarda kendini geri çeker.

Tablo 3. Örneklerle siber zorbalığın psikolojik ve sosyal etkileri

Siber Zorbalıkla Mücadele Yolları

Siber zorbalıkla mücadele etmek için birçok farklı yöntem vardır. Bunlar, eğitim ve farkındalık, hukuki adımlar, çevrimiçi platformların zorbalığa karşı aldığı önlemler ve bireylerin kendilerini korumak için geliştirebilecekleri stratejiler olarak dört ana başlık altında incelenebilir. ***Bunlar kısaca aşağıda açıklanmıştır.***

- **Eğitim ve Farkındalık**

Eğitim ve farkındalık çalışmaları, siber zorbalıkla mücadelede en etkili yollardan biridir. Okullarda, ailelerde ve toplumun farklı kesimlerinde bilinç artırıcı etkinlikler düzenlenerek çocukların, gençlerin ve ebeveynlerin siber zorbalığı tanımaları, olası etkilerini anlamaları ve kendilerini koruma yollarını öğrenmeleri sağlanabilir. Öğrencilere yönelik siber güvenlik ve zorbalık konularında özel eğitim programları düzenlenmelidir. Bu programlar, siber zorbalığın ne olduğunu, hangi davranışların zorbalık sayıldığını ve karşılaşıldığında ne yapılması gerektiğini öğretir. Okullarda psikolojik danışmanlık birimleri, siber zorbalığa uğrayan öğrencilere destek sunar. Öğrenciler, zorbalık vakalarında danışmanlardan yardım alabilir ve duygusal olarak desteklenebilir. Öğretmenler ve okul yöneticileri de siber zorbalık hakkında bilinçlendirilmelidir. Bu, zorbalığın belirtilerini tanımalarına ve öğrencilere destek olabilmelerine olanak tanır. Öğretmenler, öğrenciler arasında zorbalık olaylarına karşı daha hassas hale gelir.

Televizyon, radyo ve sosyal medya üzerinden yürütülen kampanyalar, geniş kitlelere ulaşarak siber zorbalık hakkında toplumsal bilinç oluşturur. Bu kampanyalar, siber zorbalığın zararları, mağdurların korunması ve zorbalıkla nasıl başa çıkılacağı hakkında bilgi verebilir. Belediyeler, sivil toplum kuruluşları ve diğer yerel örgütler, toplum genelinde farkındalığı artırmaya yönelik seminerler ve çalıştaylar düzenleyebilir. Bu etkinlikler, her yaştan bireyin siber zorbalığı tanımasını ve kendini koruma yollarını öğrenmesini sağlar.

Öğrencilere, dijital vatandaşlık kapsamında çevrimiçi ortamlarda etik davranış, saygı ve empati gibi konular öğretilmelidir. Bu dersler, siber zorbalığın zararlarını anlamalarına ve dijital dünyada sorumluluk sahibi olmalarına katkı sağlar. Ailelerin çocuklarıyla birlikte katılabileceği dijital etik eğitimleri veya seminerler, siber zorbalık konusunda ailelerin bilinçli hale gelmesine yardımcı olur. Bu etkinlikler, aile içi güvenli internet kullanımı hakkında bilgilendirir (Ayas ve Horzum, 2023).

- **Hukuki Adımlar**

Siber zorbalığı önlemek amacıyla birçok ülkede çeşitli yasal düzenlemeler ve hukuki yaptırımlar uygulanmaktadır. Bu yasalar, siber zorbalığın mağdurları koruma altına almasını, zorbalık yapanların cezalandırılmasını ve internet ortamında güvenli bir alan oluşturulmasını hedefler.

Siber zorbalık ve ilgili suçlar için kanuni düzenlemeler tehdit ve taciz yasaları, itibar zedelenmesi ve iftira yasaları, veri koruma ve gizlilik yasaları başlıkları altında ele alınmaktadır. Bu yasalarla çeşitli hukuki yaptırımlar ve cezalar belirlenmiştir. Örneğin, Siber zorbalık içerikli tehdit, taciz veya iftira gibi suçlar için zorbalık yapan kişilere para cezası veya hapis cezası uygulanabilir. Zorbalık içeren paylaşımların veya hesapların sosyal medya ve diğer dijital platformlardan kaldırılması kararı alınabilir. Bu tür içerikler yasal olarak yayından kaldırılır ve mağdurun korunması sağlanır. Mağdurlar, siber zorbalık nedeniyle uğradıkları psikolojik veya maddi zararlardan ötürü zorbalık yapan kişilere karşı tazminat davası açabilirler. Bu davalar, mağdurlara zararlarının telafi edilmesini sağlar.

Türkiye'de siber zorbalıkla mücadele amacıyla çeşitli kanuni düzenlemeler ve hukuki yaptırımlar bulunmaktadır. Türk Ceza Kanunu (TCK) ve diğer yasal düzenlemeler, siber zorbalık kapsamındaki eylemleri suç sayarak mağdurları koruma altına almayı hedefler. Türk Ceza Kanunu, siber zorbalık kapsamına giren pek çok eylemi suç olarak tanımlar ve cezai yaptırımlar öngörür (Meray, 2024; Maviş, 2021; Öztürk, Ateş ve Erdoğan, 2020). Türkiye'de siber zorbalıkla mücadele amacıyla kullanılan başlıca yasal düzenlemeleri ve her birinin kapsamı Tablo 4'de özetlenmiştir.

Yasa / Düzenleme	Madde	Kapsam	Yaptırım
Türk Ceza Kanunu (TCK)	106 - Tehdit	Tehdit içerikli mesaj ve paylaşımlar.	Hapis cezası.
	125 - Hakaret	Sosyal medya veya dijital ortamlarda hakaret içeren paylaşımlar.	Para cezası veya hapis cezası (Mağdur şikayetiyle soruşturulur).
	134 - Özel Hayatın Gizliliği İhlali	Mağdurun özel bilgilerini izinsiz ifşa etme veya yayma.	Hapis cezası.
	135-140 - Kişisel Verilerin Korunması	Mağdurun kişisel verilerini izinsiz paylaşma.	Hapis ve para cezası.
	267 - İftira	Dijital ortamda asılsız suçlamalar ve yalan bilgiler yayma.	Hapis cezası.
5651 Sayılı İnternet Kanunu	Tüm maddeler	Dijital ortamlarda zorbalık içeren içeriklerin kaldırılması.	İçeriğin kaldırılması, erişim engelleme.
	İçerik Sağlayıcı Sorumluluğu	Zorbalık içeren içeriklerin kaldırılmasına olanak tanır.	Para ve erişim engeli cezası.
Kişisel Verileri Koruma Kanunu (KVKK)	Tüm maddeler	Kişisel bilgilerin izinsiz kullanılması ve yayılması.	İdari para cezası ve diğer yaptırımlar.
Çocuk Hakları ve Koruma Yasaları	Çocuk Hakları Sözleşmesi	Çocukların siber zorbalıktan korunması.	Güvenlik tedbirleri ve koruyucu önlemler.
Mahkemeler ve Hukuki Süreç	Şikayet ve Dava Hakkı	Mağdurun zorbalığa karşı dava açma hakkı.	Tazminat ve diğer hukuki yaptırımlar.

Tablo 4. Türkiye'de siber zorbalıkla ilgili başlıca yasal düzenlemeler

Türk Ceza Kanunu'nda tehdit, hakaret, özel hayatın gizliliği ihlali, iftira gibi eylemler suç olarak değerlendirilir ve çeşitli yaptırımları vardır. 5651 sayılı yasa, dijital ortamda yapılan yayınların düzenlenmesi ve suç içeren içeriklerin engellenmesi için önemli bir düzenlemedir. Siber zorbalıkla mücadelede bu yasa kapsamındaki maddeler etkili bir şekilde kullanılmaktadır (Meray, 2024).

Bu yasa, internet siteleri, sosyal medya platformları ve diğer dijital içerik sağlayıcılarına, zorbalık içeren içeriklerin kaldırılması ve zorbalık yapan kullanıcıların engellenmesi gibi yükümlülükler getirirmiştir (Maviş, 2021; Dülger, 2020). Kişisel Verileri Koruma Kanunu, kişisel bilgilerin hukuka aykırı olarak işlenmesini, ifşa edilmesini veya paylaşılmasını yasaklayarak, mağdurun kişisel bilgileri izinsiz şekilde paylaşıldığında, KVKK ihlali gerçekleşir. KVKK, mağdurların bu tür durumlarda Kişisel Verileri Koruma Kurumu'na şikâyette bulunmasını sağlar, veri ihlali yapan kişiler hakkında yasal işlem yapılabilir.

Çocukları korumak için de, özellikle siber zorbalıkla mücadele kapsamında çeşitli düzenlemeler yapılmıştır. Türkiye, Çocuk Hakları Sözleşmesi'ni kabul ettiğinden, çocukların siber zorbalık gibi dijital tehditlerden korunması için yasal güvenceler sağlar. Siber zorbalığa maruz kalan kişiler, şikâyetlerini polise veya savcılığa bildirerek hukuki süreç başlatabilirler. Mağdurun sunduğu deliller doğrultusunda soruşturma başlatılır ve zorba hakkında işlem yapılır. Mağdurlar, uğradıkları maddi ve manevi zararlar için zorbalık yapan kişilere karşı tazminat davası açabilirler.

Türkiye'de siber zorbalıkla mücadele kapsamında Türk Ceza Kanunu, 5651 Sayılı Kanun ve KVKK gibi yasal düzenlemeler mevcuttur. Tehdit, hakaret, iftira ve kişisel verilerin ihlali gibi suçlar için hem hapis hem de para cezaları öngörülmektedir (Meray, 2024). Çocukları koruma yasaları, erişim engelleme ve dijital güvenlik programları gibi önlemlerle siber zorbalıkla daha etkin mücadele edilebilmesi amaçlanmaktadır. Bu düzenlemeler, mağdurlara koruma sağlarken, zorbalık yapan kişilere karşı caydırıcı bir etki oluşturur (Maviş, 2021; Dülger, 2020).

Çevrimiçi Platformların Zorbalığa Karşı Aldığı Önlemler

Çevrimiçi platformlar, siber zorbalığı önlemek ve kullanıcıları korumak için çeşitli önlemler geliştirmiştir. Bu önlemler, kullanıcıların güvenli bir dijital deneyim yaşamalarını sağlamak ve zorbalığı caydırmak amacıyla uygulanmaktadır. Bunlar, kötüye kullanım bildirimi, gizlilik ve güvenlik ayarları, topluluk kuralları ve içerik politikaları, yapay zekâ destekli içerik denetim, eğitim ve farkındalık programları, rehberlik ve destek hizmetleri, kanun ve kolluk kuvvetleri ile işbirliği olarak sınıflandırılabilir.

Tablo 5 çevrimiçi platformların siber zorbalıkla mücadelede hangi önlem-

leri aldığını ve her bir önlemin nasıl işlediğini özetlemektedir.

Sosyal medya platformları, kullanıcıların zararlı içerikleri veya zorbalık yapan profilleri bildirmesine olanak tanır. Bu raporlama sistemi, zorbalık içeren içeriklerin platform tarafından incelenmesini sağlar. Bildirilen zorbalık içerikli paylaşımlar incelendikten sonra, platform kurallarına aykırı bulunursa kaldırılır. Bu, zorbalığın etkisini sınırlamak ve mağduru korumak için yapılan önemli bir adımdır. Platformlar, kullanıcıların gizlilik ayarlarını yapılandırarak kişisel bilgilerini koruma altına almalarını sağlar. Kullanıcılar, yalnızca güvenilir kişilerin içeriklerine ulaşabilmesi için hesaplarını gizli tutabilirler.

Çoğu platform, kullanıcılarına zorbalık ve taciz içeren davranışların kabul edilemez olduğunu belirten topluluk kurallarını sunmaktadır. Bu kurallara uymayan içerikler platformdan kaldırılır ve kullanıcılar cezalandırılır.

Platformlar, yapay zekâ algoritmalarını kullanarak zorbalık veya taciz içeren mesajları otomatik olarak tespit edebilir. Örneğin, tehdit içeren anahtar kelimeler veya nefret söylemleri içeren içerikler, yayınlanmadan önce incelenir. Yapay zekâ, zorbalık içeriklerini filtreleyerek mağdurların bu içeriklerle karşılaşmasını önler. Algoritmalar, yorumları veya mesajları inceleyerek zorbalık içeriklerinin yayınlanmasını engelleyebilir.

Çoğu sosyal medya platformu, zorbalık ve güvenli internet kullanımı konusunda kullanıcılarına eğitim içerikleri sunarak, kullanıcıların zorbalıkla karşılaştıklarında nasıl tepki vermeleri gerektiği ve nasıl korunabilecekleri konusunda bilgilendirir. Bazı platformlar, zorbalığa maruz kalan kullanıcılar için rehberlik ve psikolojik destek kaynakları sunar. Mağdurlar, dijital zorbalıkla başa çıkabilmek için bu rehberlerden yararlanabilir. Ayrıca, özellikle çocuk kullanıcılar için sunulan özel güvenlik ayarları, zorbalığa karşı koruyucu önlemler sağlar.

Çevrimiçi platformlar, ciddi siber zorbalık vakalarında emniyet güçleri ve adli makamlarla işbirliği yapabilir. Suç teşkil eden durumlarda, yetkililere IP adresi ve diğer kullanıcı bilgileri sağlanarak hukuki işlemler başlatılabilir.

Bu önlemler, çevrimiçi platformların zorbalıkla mücadele konusunda sorumluluklarını yerine getirmelerine ve kullanıcıları güvenli bir ortamda korumalarına yardımcı olur. Platformların siber zorbalıkla mücadelede daha etkin olması, zorbalığı caydırıcı etkiler yaratır ve dijital ortamda sağlıklı iletişimi destekler.

Önlem	Açıklama	Detaylar / Örnekler
Raporlama ve Şikayet Seçenekleri	Zorbalık içeren içerik veya profiller kullanıcılar tarafından platforma bildirilebilir.	Zararlı içeriklerin kaldırılması için kullanıcılar, zorbalık yapan hesapları veya paylaşımları rapor eder.
Gizlilik ve Güvenlik Ayarları	Kullanıcıların hesap gizliliğini ve erişim ayarlarını kontrol etmelerini sağlar.	Hesap gizliliği ayarları, kişisel bilgilerin yabancılara karşı korunmasına yardımcı olur.
Engelleme ve Sessize Alma	Zorbalık yapan kişilerin erişimini engelleyerek veya sessize alarak zorbalık içeriklerini gizler.	Mağdur, zorbalık yapan kişilerin mesajlarını veya paylaşımlarını görmezden gelebilir.
Topluluk Kuralları ve İçerik Politikaları	Zorbalık ve taciz içeren içeriklerin kabul edilemez olduğunu belirleyen kurallar oluşturur.	Platform kurallarına aykırı davranışlarda bulunan kullanıcılar uyarı, engel veya hesap kapatma cezası alır.
Yapay Zeka Destekli İçerik Denetimi	Zorbalık içeren içerikleri otomatik olarak tespit eden algoritmalar kullanır.	Tehdit içeren anahtar kelimeleri tespit eden yapay zeka, saldırgan içerikleri engelleyebilir.
Zorbalık İçeriklerinin Filtrelenmesi	Yapay zeka, mağdurların zorbalık içerikleriyle karşılaşmasını engeller.	Örneğin, bazı kelimeler veya ifadeler içerik paylaşılmadan önce filtrelenir.
Eğitim ve Farkındalık Programları	Kullanıcıların siber zorbalıkla başa çıkabilmeleri için bilgilendirici içerikler sunar.	Siber zorbalık, güvenli internet kullanımı ve zorbalıkla mücadele için rehberler ve farkındalık kampanyaları sunar.
Rehberlik ve Destek Hizmetleri	Zorbalığa uğrayan kullanıcılar için rehberlik ve psikolojik destek sağlar.	Mağdurlar için erişilebilir psikolojik destek ve rehberlik hizmetleri sunulur.
Özel Güvenlik Ayarları ve Çocuk Koruma Modları	Çocuk kullanıcılar için güvenli mod ve ebeveyn kontrol ayarları sunar.	Çocuk kullanıcılar, yaşlarına uygun olmayan içeriklerden korunur ve ebeveynler tarafından denetlenebilir.
Kanun ve Kolluk Kuvvetleri ile İşbirliği	Ciddi zorbalık vakalarında yetkililere bilgi sağlayarak yasal sürece destek olur.	Suç teşkil eden zorbalık durumlarında IP adresi gibi bilgiler adli makamlara iletilir.
Zorbalık Olaylarında Acil Müdahale	Mağdurları korumak amacıyla hızla erişim engeli veya içerik kaldırma işlemi yapar.	Tehdit içeren içerikler, mağdurun güvenliğini sağlamak için hızlı bir şekilde kaldırılır.

Tablo 5. Çevrimiçi platformların siber zorbalığa karşı aldığı önlemler

Siber Zorbalık Karşısında Ailelerin Rolü

Siber zorbalık karşısında ailelerin rolü, çocukları ve gençleri korumak, onları bilinçlendirmek ve destek olmaktır. Aileler, çocuklarının dijital ortamda karşılaşabileceği tehditleri anlamalarına yardımcı olabilir, güvenli internet kullanımı alışkanlıkları kazanmalarını sağlayabilir ve zorbalık durumunda çocuklarını destekleyerek psikolojik olarak rahatlatabilirler. Aileler, çocuklarına siber zorbalığın ne olduğunu, nasıl ortaya çıktığını ve hangi tür davranışların zorbalık sayıldığını anlatmalıdır. Bu, çocukların zorbalık karşısında daha bilinçli olmalarını sağlar.

Aileler, çocuklara çevrimiçi güvenlik önlemlerini öğretmelidir. Örneğin, güçlü parolalar kullanma, kişisel bilgileri paylaşmama ve tanımadıkları kişilerden gelen mesajlara dikkat etme gibi konularda çocuklar bilgilendirilmelidir. Ancak bu şekilde bir farkındalık yaratılabilir.

Çocuklar, çevrimiçi ortamda zorbalıkla karşılaştıklarında, ailelerine rahatça açılabilecekleri bir iletişim ortamı bulmalıdır. Aileler, çocuklarını suçlamadan veya yargılamadan dinleyerek onları desteklediklerini hissettirmelidir. Çocuklar, dijital ortamlarda karşılaştıkları sorunları onlarla paylaşarak rehberlik alabilmelidir. Aileler, çocuklarının çevrimiçi ortamda yaşadığı sorunlara duyarlı olmalı ve zorbalık durumunda nasıl hareket edecekleri konusunda yol göstermelidir, başka bir deyişle açık ve destekleyici iletim bu aşamada çok önemlidir. Çocukların zorbalık karşısında yalnız olmadıklarını hissetmeleri önemlidir. Aileler, çocuklarına zorbalığın onların suçu olmadığını, bu durumu aşmak için yanlarında olduklarını hissettirmelidir.

Eğer siber zorbalık, çocuğun psikolojisini derinden etkiliyorsa, ebeveynler profesyonel psikolojik destek almayı düşünmelidir. Bir terapist veya psikolojik danışman, çocukların bu süreci sağlıklı bir şekilde atlatmalarına yardımcı olabilir. Bunların yanı sıra, aileler, çocuklarının internet kullanımını güvenli hale getirmek için ebeveyn kontrol yazılımları kullanabilir. Bu yazılımlar, çocukların hangi içeriklere eriştiğini denetlemeye ve güvensiz platformlardan uzak tutmaya yardımcı olur. Eğer, çocuk siber zorbalığa maruz kalıyorsa, aileler bu durumu çevrimiçi platformlara rapor edebilir veya gerektiğinde hukuki süreç başlatabilir. Aileler, zorbalığın ciddi sonuçları olabileceğini ve gerektiğinde polise veya diğer yetkililere başvurabileceklerini bilmelidir.

Aileler, çocuklarına siber zorbalık karşısında nasıl davranacaklarını öğretirken aynı zamanda onları koruma ve destekleme görevi üstlenir. Bu süreçte çocuklar için güvenli bir dijital ortam yaratmak, onları bilinçlendirmek ve gerektiğinde profesyonel yardım sağlamak önemlidir. Aileler, çocuklarının dijital dünyada güvenli ve sağlıklı bir deneyim yaşaması için kilit bir role sahiptir ve zorbalığın zararlarını azaltmada büyük katkı sağlar.

Siber zorbalık, güç ve kontrol ihtiyacı, anonimlik, empati eksikliği ve kıskançlık gibi birçok faktörün etkisiyle ortaya çıkabilir. Dijital dünyada sağlanan kimlik gizleme imkanı ve sorumluluktan kaçabilme, zorbalığın daha kolay yapılabilmesini sağlar. Siber zorbalık davranışları genellikle kişinin dijital ortamda sağladığı anonimlik, güç gösterisi yapma isteği, sosyal onay arayışı veya kendini üstün hissetme gibi motivasyonlardan kaynaklanır. Bu nedenlerle, hem bireysel hem de toplumsal farkındalık ve bilinçlendirme çalışmaları, siber zorbalıkla mücadelede önemli bir rol oynar.

Dijital Güvenliği Tehdit Eden Kötü Alışkanlıklar ve KorunmaÖnerileri

İyi siber güvenlik alışkanlıklarının benimsenmemesi, bireyleri siber saldırılara ve veri ihlallerine karşı savunmasız hale getirir. Ne yazık ki, dijital dünyada kendimizi korumanın yollarını bilmeliyiz (Bilgiç ve Seferoğlu, 2020; Dowdell, 2010). En kötü siber güvenlik alışkanlıkları ve bunların yaratabileceği riskler:

1. Zayıf ve Kolay Tahmin Edilebilir Şifreler Kullanmak

- ***Riskler:*** "123456", "password" gibi kolay tahmin edilebilen şifreler, saldırganların hızlıca hesaplara erişimini sağlar. Zayıf şifre kullanımı, hassas verilerinize ve hesaplarınıza erişim riskini artırır.
- ***Çözüm:*** Güçlü, karmaşık ve uzun şifreler (büyük-küçük harf, sayı ve özel karakterler içeren) kullanmak, hesap güvenliğini artırır.

2. Aynı Şifreyi Birçok Platformda Kullanmak

- ***Riskler:*** Bir hesap şifresi ele geçirildiğinde diğer tüm hesaplar da tehlikeye girer. Bir platformdan sızdırılan şifreler, diğer hesaplarda da kullanılabilir.
- ***Çözüm:*** Her platform için farklı ve güçlü şifreler oluşturmak. Şifre yöneticileri, güçlü ve benzersiz şifreler kullanmayı kolaylaştırır.

3. Şifreleri Kağıda Yazmak veya Dijital Notlarda Saklamak

- ***Riskler:*** Şifrelerin açık bir şekilde yazılması veya dijital notlarda saklanması, başkaları tarafından kolayca bulunmalarına yol açar. Bu, veri güvenliğini zedeler.
- ***Çözüm:*** Şifre yöneticisi kullanarak şifreleri güvenli bir şekilde saklamak. Şifreleri yalnızca güvenilir ortamlarda tutmak.

4. Çok Faktörlü Kimlik Doğrulamayı (MFA) Kullanmayı İhmal Etmek

- ***Riskler:*** Tek faktörlü kimlik doğrulama (yalnızca şifre), hesapların daha kolay ele geçirilmesine neden olur. Hesaplar, ek bir güvenlik katmanı olmadan korumasız kalır.
- ***Çözüm:*** Mümkün olan her platformda iki veya çok faktörlü kimlik doğrulama (MFA) kullanmak, hesap güvenliğini artırır.

5. Güncellemeleri İhmal Etmek

- ***Riskler:*** Yazılım, işletim sistemi ve uygulamaların güncel tutulmaması, bilinen güvenlik açıklarından yararlanılarak saldırıya uğrama riskini artırır.
- ***Çözüm:*** Cihaz ve uygulamaların otomatik güncellemelerini açmak veya düzenli olarak güncellemeleri kontrol etmek, güvenlik açıklarını kapatır.

6. Halka Açık Wi-Fi Ağlarında Korumasız Bağlantı Kullanmak

- ***Riskler:*** Korunmayan ağlarda, saldırganlar cihazlara kolayca erişebilir ve veri çalabilir. Bu, kişisel bilgilerin veya finansal verilerin ele geçirilmesine yol açabilir.
- ***Çözüm:*** Halka açık Wi-Fi ağlarını kullanırken VPN (sanal özel ağ) kullanmak, veri güvenliğini artırır. Ayrıca, halka açık ağlarda hassas işlemlerden kaçınmak da önemlidir.

7. Güvenilmeyen E-postalar ve Bağlantılara Tıklamak

- ***Riskler:*** Kimlik avı (phishing) e-postaları veya kötü niyetli bağlantılar,

zararlı yazılımların indirilmesine ve kişisel bilgilerin çalınmasına yol açar.

- ***Çözüm:*** Bilinmeyen veya şüpheli e-postalara ve bağlantılara tıklamaktan kaçınmak. E-postaları açmadan önce gönderenin kimliğinden emin olmak.

8. Antivirüs veya Güvenlik Yazılımı Kullanmamak

- ***Riskler:*** Cihazlarda güvenlik yazılımı olmaması, virüs ve kötü amaçlı yazılımların kolayca bulaşmasına neden olur. Bilgisayar korsanları cihazları ele geçirebilir veya verilere zarar verebilir.

- ***Çözüm:*** Güvenilir bir antivirüs yazılımı kullanmak, düzenli tarama yapmak ve güvenlik duvarını açık tutmak, cihaz güvenliğini sağlar.

9. Bilgisayar ve Cihazları Kilitlemeyi İhmal Etmek

- ***Riskler:*** Cihazların kilitlenmemesi, özellikle halka açık alanlarda veya iş yerlerinde kişisel veya hassas verilere yetkisiz erişime yol açar.

- ***Çözüm:*** Bilgisayarları, telefonları ve diğer cihazları kullanmadığınız zaman kilitlemek veya otomatik kilit ayarlarını kullanmak, güvenliği artırır.

10. Veri Yedeklemeyi İhmal Etmek

- ***Riskler:*** Cihazlar saldırıya uğradığında veya veriler kaybolduğunda, yedekleme yapılmamışsa verilerin geri alınması mümkün olmayabilir. Bu, hem bireysel hem de iş verileri için ciddi sonuçlar doğurur.

- ***Çözüm:*** Önemli verileri düzenli olarak yedeklemek ve bu yedekleri güvenli bir konumda saklamak, veri kaybını önlemeye yardımcı olur.

11. İki Aşamalı Onay Gerekmeden Çevrim İçi Alışveriş Yapmak

- ***Riskler:*** Güvensiz veya doğrulanmamış sitelerden alışveriş yapmak, kredi kartı bilgilerinizin çalınmasına veya dolandırıcılığa neden olabilir.

- ***Çözüm:*** Bilinen, güvenli sitelerden alışveriş yapmak ve iki aşamalı doğrulama (örneğin, SMS kodu ile onay) kullanmak.

Bu kötü alışkanlıklardan kaçınarak ve güvenlik önlemlerine dikkat ederek, çevrim içi dünyada güvenliğinizi artırabilirsiniz. Güçlü şifreler kullanmak, yazılım güncellemelerini takip etmek, çok faktörlü kimlik doğrulama ve güvenilir güvenlik yazılımlarından yararlanmak, dijital güvenlik risklerini en aza indirir.

Sonuç:
Güvenli Ve Saygılı Bir Dijital Ortam Yaratmak

Siber zorbalık, dijital ortamın sunduğu anonimlik, güç gösterisi isteği, sosyal onay arayışı, empati eksikliği ve kıskançlık gibi çeşitli nedenlerle ortaya çıkan ciddi bir sorundur.

Çevrim içi ortamda kimliğini gizleyebilme imkanı, zorbalığın yaygınlaşmasına ve mağdurlar üzerinde derin psikolojik ve sosyal etkiler bırakmasına yol açmaktadır.

Siber zorbalık, özellikle çocuklar ve gençler arasında duygusal yaralanmalara, özgüven kaybına ve sosyal izolasyona neden olabilecek sonuçlar doğurur.

Güvenli ve saygılı bir dijital ortam yaratmak, siber zorbalığın etkilerini azaltmak ve insanların çevrim içi alanlarda kendilerini güvende hissetmelerini sağlamak için önemlidir. Siber zorbalık, dijital dünya üzerinde kontrolsüzce yayılarak bireylerin psikolojik ve sosyal sağlığını tehdit eder hale gelmiştir. Bu nedenle, dijital platformların güvenli bir ortam sunabilmesi ve kullanıcıların birbirlerine saygı gösterdiği bir kültür oluşturulması, siber zorbalıkla mücadelede önemli bir hedeftir.

Hem bireylerin hem de toplumun bilinçli hareket etmesiyle, dijital dünyada saygı ve güven temelinde bir kültür inşa edilebilir.

İnternette bulduğum her bilgiye hemen inanmam.
Şüpheciyimdir! Mutlaka kontrol ederim.

Kişisel bilgilerimi internette paylaşmam.
Adresimi, telefon numaramı hiçbir yerde bulamazsın.

Bilgisayarımı korurum.
Emin olmadığım programları bilgisayarıma indirmem.

Parolalarımı güçlü ve karmaşık tutarım.
Kolay tahmin edilen parolalar kullanmam.

Gerçek hayatta olduğu gibi, internet ortamında da insan haklarına saygılı davranırım. Kimseye zarar verecek ifadeler kullanmam ve kaynağı bilinmeyen, doğruluğundan emin olmadığım bilgileri paylaşmam.

DİJİTAL HAKLAR KILAVUZU

DİJİTAL GÜVENLİK ÖNERİLERİ

İki aşamalı kimlik doğrulama kullanırım.
Hesaplarım için ekstra güvenlik sağlarım.

Sosyal medya ayarlarımı kontrol ederim.
Gizlilik ayarlarımı sık sık güncellerim.

Tanımadığım bağlantılara tıklamam.
Bilinmeyen e-postalardaki bağlantılardan kaçınırım.

Güvenilir kaynaklardan bilgi alırım.
Bilgiye ulaşırken güvenilir siteleri tercih ederim.

Çocuklarımı dijital güvenlik konusunda eğitirim.

Ailemle dijital güvenlik hakkında konuşurum.

DİJİTAL HAKLAR KILAVUZU

DİJİTAL GÜVENLİK ÖNERİLERİ

KAYNAKÇA:

1. *International Telecommunications Union (ITU), Measuring Digital Development. Facts and figures 2019 (Geneva, 2019).*
2. *Juniper Research, "Business losses to cybercrime data breaches to exceed $5 trillion by 2024", 27 August 2019.*
3. *Nicola Jones, "How to stop data centers from gobbling up the world's elec tricity", Nature, vol. 561, No. 7722 (September 2018).*
4. *United Nations. (2020). Report of the Secretary-General: Roadmap for Digital Cooperation. June 2020.*
5. *European Commission. (n.d.). Digital principles. Retrieved October 23, 2024, from https://digital-strategy.ec.europa.eu/en/policies/digital-principlestab_2*
6. *Creative Commons TR 2024, https://creativecommons.org.tr/*
7. *DigitalAgenda 2011, Digital Agenda: Coalition of top tech & media companies to make internet better place for our kids. Europa Press*
8. *Mediasmarts.ca 2024; https://ghostarchive.org/archive/bUDjg*
9. *Ribble, M. (2015), Okullarda Dijital Vatandaşlık: Tüm Öğrencilerin Bilmesi Gereken Dokuz Unsur (3. baskı). Washington DC: Uluslararası Eğitim Teknolojileri Derneği.*
10. *TÜİK1,2024; 2023 yaşlı istatistikleri, https://data.tuik.gov.tr/Bulten/Index?p=Istatistiklerle-Yaslilar-2023*
11. *TÜİK2, 2024; 2023 çocuk istatistikleri, https://data.tuik.gov.tr/Bulten/Index?p=Istatistiklerle-Cocuk-2023*
12. *TÜİK3, 2024; 2023 Hane halkı bilişim teknolojileri kullanım Araştırması, https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2023-49407*
13. *İSTEAMDER, 2020 ; https://buyukcekmece.meb.gov.tr/meb_iys_dosyalar/2020_03/08175827_TEKNO_TOPLUM_2._SAYI.pdf*
14. *TYC, 2019 ; Türkiye Yeşilay Cemiyeti https://yesilaymarket.com/Data/EditorFiles/DijitalEbeveynlik.pdf*
15. *Akdeniz, B. & Doğan, A. (2024). Cyberbullying: Definition, prevalence, effects, risk and protective factors. 16 (3), 425 -438.*
16. *Akgül, G. (2020). Siber zorbalığın nedenleri üzerine kuramsal açıklamalar. Gelisim ve Psikoloji Dergisi. 1, (2) 9-16.*
17. *Ayas T. & Horzum, M. B. (2023). Cyberbullying and victimization status of secondary school students: change in 10 years. Online Journal of Technology Addiction & Cyberbullying, 10(2), 63 – 84.*
18. *Baştürk Akça, E. & Sayımer, İ. (2017) Siber zorbalık kavramı, türleri ve ilişkili olduğu faktörler: mevcut araştırmalar üzerinden bir değerlendirme. Baştürk Akça E, Sayımer İ (2017) Siber zorbalık kavramı, türleri ve ilişkili olduğu faktörler: mevcut araştırmalar üzerinden bir değerlendirme. AJIT-e: Bilişim Teknolojileri Online Dergisi, 8(30):7-19., 8(30):7-19.*
19. *Betts, L. R. (2015). Cyber bullying behaviours. Encyclopedia of Information Science and Technology, 6727–6735.*
20. *Bilgiç, H. G. & Seferoğlu, S. S. (2020). Z kuşağinin sosyal ağlarda karşı karşıya olduğu tehlikeler ve onlari bu tehlikelerden korumaya yönelik öneriler. Gençlik ve Dijital Çağ. https://yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_Genclik-2020_Bilgic-Seferoglu_SosyalAg-Tehlike_53-68.pdf*
21. *Bingöl, N. & Tanrıkulu, T. (2014). Siber zorba ve mağdur olma ile algılanan sosyal destek düzeyi arasındaki ilişkinin incelenmesi. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, 43, 261-277.*
22. *Cosma A., Walsh SD., Chester KL., Callaghan M., Molcho M., & Craig W et.al. (2020) Bullying victimization: Time trends and the overlap between traditinal and cyberbullying across countries in Europe and North America. Int J Public Health, 65:75–85.*
23. *Dilmaç, J. A. (2020). Dijital ortamda sapkınlık: siber zorbalık, Turkish Studies - Social, 15(3), 1087- 1099. https://dx.doi21.org/10.29228/TurkishStudies.39895*
24. *Donat Bağcıoğlu, S. (2022). 21. yüzyılda çocukları ve gençleri bekleyen siber riskler. Psikiyatride Güncel Yaklaşımlar-Current Approaches in Psychiatry. 14(1):29-37.*
25. *Dowdell, E. B. (2010). Risky internet behaviors: A case study of online and offline stalking. The Journal of School Nursing Vol. 26, (2010): 436-442.*
26. *Dülger, M. V. (2020). Bilişim Suçları ve İnternet İletişim Hukuku, (8. Baskı), Ankara: Seçkin Yayınları.*
27. *Englander E, Donnerstein E, Kowalski R, Lin CA & Parti K (2017). Defining cyberbullying. Pediatrics, 140:148-151.*
28. *Elsaesser C, Russell B, Ohannessian CM & Patton D (2017). Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. Aggress Violent Behav, 35:62-72.*
29. *Erdur-Baker, Ö. & Kavşut, F. (2007). Akran zorbalığının yeni yüzü: Siber zorbalık. Eurasian Journal of Educational Research, 27, 31-42.*
30. *Hay, C; Meldrum, R & Mann, K. (2010). Traditional bullying, cyber bullying, and deviance: A general strain theory approachi Journal of Contemporary Criminal Justice. 26 (2), 130-147.*
31. *Hinduja S & Patchin JW (2017). Cultivating youth resilience to prevent bullying and cyberbullying victimization. Child Abuse Negl, 73:51-62.*
32. *Horzum, M. B. & Ayas, T. (2011). Ortaöğretim öğrencilerinin sanal zorba ve mağdur olma düzeylerinin okul türü ve cinsiyet açisindan incelenmesi. Journal of Educational Sciences & Practices, 10(20).*
33. *Kowalski, R. M., Limber, S., & Agaston, P. (2008). Cyber bullying: Bullying in the digital age (first edition). Malden, MA: Blackwell Publishing.*
34. *Kim J, Song H & Jennings WG (2017). A distinct form of deviance or a variation of bullying? Examining the developmental pathways and motives of cyberbullying compared with traditional bullying in South Korea. Crime Delinq, 63:1600-1625.*
35. *Maviş, V. (2021). Ceza hukuku boyutuyla siber zorbalık. Selçuk Üniversitesi Hukuk Fakültesi Dergisi. 29, (3), 2455 – 2500.*
36. *Meray, M. S. (2024). Ceza hukukunda siber zorbalık. Karatekin Hukuk Dergisi. 2(2). 77 – 105.*
37. *Öztürk E, Ateş A. & Erdoğan B. (2020). Siber suçların hukuksal yönleri ve psikolojik dinamikleri. Öztürk E, editör. Siber Psikoloji. 1. Baskı. Ankara: Türkiye Klinikleri; 48-55.*
38. *Peebles, E. (2014). Cyberbullying: Hiding behind the screen. Paediatr Child Health (Oxford), 19:527–528.*
39. *Selkie EM, Fales JL & Moreno MA (2016). Cyberbullying prevalence among US middle and high school–aged adolescents: A systematic review and quality assessment. J Adolesc Health, 58:125-133.*
40. *Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact insecondary school pupils. Journal of Child Psychology and Psychiatry, 49, 376–385.*
41. *Sticca F. & Perren S. (2013). Is cyberbullying worse than traditional bullying? Examining the differential roles of medium, publicity, and anonymity for the perceived severity of bullying. Journal of Youth and Adolescence, 42, 739-750.*
42. *Vandebosch H.& Van Cleemput K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. Cyberpsychology & Behavior, 11, 499-503.*

ISBN: 978-625-99749-5-8

"Bandrol Uygulamasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 5. maddesinin ikinci fıkrası çerçevesinde bandrol taşıması zorunlu değildir."