

Siber Zorbalığa Karşı Gençlik İttifakı



Dijital Güvenlik ve Farkındalık El Kitabı

"Avrupa Dayanışma Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Burada yer alan içerik yazarların görüşlerini yansıtmaktadır ve bu görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz."



**Avrupa Birliği tarafından
finanse edilmektedir**



2024-3-TR01-ESC30-SOL-000284071



**Avrupa Birliđi tarafından
finanse edilmektedir**

ESC-30

Avrupa Dayanışma Programı Dayanışma Programı

Siber Zorbalığa Karşı Gençlik İttifakı

Dijital Güvenlik ve Farkındalık El Kitabı

SAKARYA ÜNİVERSİTESİ

Yazarlar

- Kayra Kaan KABAKÇIOĞLU
- Gülbin ABATAY
- Samet AYAN
- Yaren ŞÜKRE
- Ömer Faruk ACAR

Katkıda Bulunanlar

- Dilanur ŞAHİN
- Sudem ÇAĞ
- Bengüsu ÖZER
- Dilay Gülru ÖZAK
- Yusuf Ziya AĞCAKAYA

Proje Koordinatörü

- Yusuf Buğra KILIÇ

Proje Koçu

- Öğr.Gör.Dr. Sadık DEMİRBAĞ



**Avrupa Birliği tarafından
finanse edilmektedir**



2024-3-TR01-ESC30-SOL-000284071



**Avrupa Birliđi tarafından
finanse edilmektedir**

İÇİNDEKİLER

1. Dijital Dünyada Karşılaşılan Riskler ve Tehditler.....	10
1.1 Dijital Çağın Hastalığı: Yeni Nesil Bağımlılıklar.....	11
1.2 Dijital Bağımlılık Nedir?.....	12
1.3 Dijital Çağın Getirdiği Kaygı Bozuklukları: Fobi, Nomofobi, Netlessfobi.....	12
1.4 Dijital Oyun Bağımlılığı Nedir?.....	13
1.4.1 Dijital Oyun Bağımlılığın Cinsiyet Boyutu.....	13
2.Dijital Haklar ve Korunma Mekanizmaları.....	15
2.1 Avrupa Birliği Gözünden: Dijital Haklarımız.....	15
2.2 Siber Zorbalığa Karşı Nasıl Korunabiliriz?.....	19
3.Siber Zorbalık Nedir?.....	23
3.1 Bilişim Suçu.....	24
3.2 Siber Suçlar.....	25
3.3 Siber Zorbalık Nedir?.....	26
3.4 Türkiye’de Siber Zorbalık.....	26
3.5 Türkiye ve Avrupa Birliği Politikaları.....	27
3.5.1 Türkiye’de Siber Güvenlik Politikaları.....	28



**Avrupa Birliği tarafından
finanse edilmektedir**

3.5.2 Türkiye’de Siber Güvenlik Kanunu.....	30
3.6 Avrupa Birliği Politikaları.....	34
3.6.1 AB Siber Güvenlik Stratejisi.....	34
3.6.2 ENISA (Avrupa Birliği Siber Güvenlik Ajansı).....	35
3.6.3 NIS ve NIS2 Direktifi.....	35
3.6.4 Avrupa Siber Güvenlik Yasası.....	36
3.7 Siber Dayanıklılık Yasası.....	37
3.8 CE Nedir ?.....	38
4.Siber Zorbalığın Toplumsal Etkileri.....	39
4.1 Eskilerden Bir Araştırma.....	39
4.2 Amerika’da Güncel Durum.....	40
4.3 Farklı Bir Ülkeden Benzer Sonuçlar.....	41
4.4 Yereldeki Genel Durum.....	42
4.5 Nişantaşı Üniversitesinden Güncel Bir Araştırma.....	42
5.Siber Zorbalıkla Mücadelede Politika Önerileri.....	45
5.1 Empati.....	47



**Avrupa Birliği tarafından
finanse edilmektedir**

5.2 Öfke Kontrolü.....	48
5.3 Değerler Eğitimi.....	48
5.4 Siber Zorbalık Müdahale Programları.....	49
5.5 Medya Kullanımı Eğitimi.....	49
5.6 Aile İçi Müdahaleler.....	50
5.7 Devletlerin Yaptırımları.....	50
5.8 Avrupa Geneline Politik Olarak Siber Zorbalık Olayları.....	51
6.Kadınlar İçin Dijital Güvenlik.....	53
6.1 Dijital Şiddet ve Türkiye’de Durum.....	53
6.2 Avrupa’da Durum ve Hukuki Düzenlemeler.....	54
6.3 Dijital Güvenlik Önerileri ve Farkındalık Çalışmaları.....	54
6.4 Sonuç ve Çağrı.....	54



**Avrupa Birliği tarafından
finanse edilmektedir**

ÖNSÖZ

Avrupa Dayanışma Programı kapsamında desteklenen *Siber Zorbalığa Karşı Gençlik İttifakı* projesi, Sakarya Üniversitesi öğrencilerinin koordinasyonunda hayata geçirilmiştir.

Projenin temel amacı, gençler arasında dijital güvenlik ve siber zorbalık konularında farkındalık yaratmak, güvenli ve sorumlu dijital davranışları teşvik etmek ve her türlü dijital şiddet ile siber suça karşı durabilecek aktif bir gençlik ağı oluşturmaktır. Bu girişim, özellikle 18–30 yaş arası gençlerin siber zorbalığı tanıyabilmesini, önleyebilmesini ve etkili şekilde karşılık verilmesini sağlamayı hedeflemektedir.

Bu el kitabı, dijital haklar, kişisel verilerin korunması, politika geliştirme, çevrimiçi güvenlik ve kadınlara duyarlı dijital güvenlik yaklaşımlarını içeren konularda açık ve uygulanabilir bilgiler sunmaktadır. Ayrıca gençlerin güvenli dijital davranışları etkileşimli olarak öğrenmesini desteklemek amacıyla mini bir dijital uygulama da geliştirilmiştir.

Proje; yazılım mühendisliği, bilgisayar mühendisliği, coğrafya, iktisat, sosyoloji ve matematik gibi farklı disiplinlerden gençlerin işbirliği ile geliştirilmiştir. Avrupa Birliği'nin, Avrupa Birliği Siber Güvenlik Ajansı'nın ve Türkiye'deki siber suç sosyolojisine dair güncel araştırmaların iyi uygulamaları da bu kitapçığın içerisine entegre edilmiştir.

Proje çıktıları; atölyeler, kamu spotları, farkındalık çalışmaları ve sosyal medya kampanyaları yoluyla kamuoyuyla paylaşılmaktadır. Ayrıca proje kapsamında Sakarya Üniversitesi, Düzce Üniversitesi, Kocaeli Üniversitesi, Uludağ



**Avrupa Birliği tarafından
finanse edilmektedir**

Üniversitesi, Marmara Üniversitesi ve İstanbul Teknik Üniversitesi'ndeki gençlere yönelik farkındalık etkinlikleri düzenlenecektir. Bu proje, gelecekte gençler tarafından yürütülecek benzer girişimlere örnek olacak sürdürülebilir bir model olarak tasarlanmıştır.



**Avrupa Birliği tarafından
finanse edilmektedir**

1. Dijital Dünyada Karşılaşılan Riskler ve Tehditler

Hayatımızın her alanına girmiş olan dijital uygulamalar, sağladıkları faydaların yanında riskler de içermektedir. Bu nedenle, dijital riskleri bilmek ve dijital risklere karşı önlemler almak büyük önem arz etmektedir. Günlük yaşantımızın bir parçası haline gelen internet; bilgiye ulaşma, bilgiyi kullanma ve iletişim kurmak gibi birçok faydası ile çağımızın en büyük icadı olarak karşımıza çıkmaktadır. Neredeyse sonsuz bilgiye erişimi sağlayan internet, aynı zamanda dünyanın herhangi bir yeri ile görüntülü, sesli ya da yazılı iletişim kurmaya olanak tanımaktadır.

Dijital dünya, yaşamı kolaylaştıran çözümler sunarken, aynı zamanda ciddi tehditler ve riskleri de beraberinde getirmektedir. Teknolojinin hızla gelişmesiyle birlikte bireyler, şirketler ve hükümetler, dijital güvenliklerini sağlama konusunda önemli zorluklarla karşı karşıya kalmaktadır.

İnsanoğlu, bulunduğu mekâna göre değişen riskler ve yaşantısına zarar veren etkenlerle karşı karşıya kalabilmektedir. Gerçek dünyada karşılaşılan risk ve zararların daha fazlayla kullanıcılar, yukarıda belirtilen hususlarla internet ortamında da karşılaşabilmektedir. Bu risk ve zararlar şöyle özetlenebilir:

- Yanlış ve/veya zararlı bilgiye erişim, bireylerin yanlış yönlendirilmesine, bilgi kirliliğine ve çeşitli toplumsal zararlara yol açabilir,
- Siber zorbalık, bireylerin psikolojik olarak zarar görmesine, özgüven kaybına ve sosyal izolasyona neden olabilir,
- Sanal dolandırıcılık, maddi kayıplara, kişisel bilgilerin ele geçirilmesine ve güvenlik zafiyetine sebep olabilir,
- Kişisel bilgilerin paylaşımı ve kimlik hırsızlığı, bireylerin mahremiyetinin ihlal edilmesine ve kimliklerinin kötüye kullanılmasına yol açabilir,
- Zararlı yazılımlar, cihazların bozulmasına, veri kaybına ve kişisel bilgilerin çalınmasına sebep olabilir,



**Avrupa Birliği tarafından
finanse edilmektedir**

- Oltalama, kullanıcıların şahsi veya finansal bilgilerinin dolandırıcılar tarafından ele geçirilmesine neden olabilir,
- Pornografi, çocuk istismarı ve fuhuş gibi içeriklere maruz kalmak, psikolojik ve toplumsal zararlara sebep olabilir,
- Yasadışı kumar siteleri, maddi kayıplara, bağımlılığa ve hukuki sorunlara yol açabilir,
- İnternet bağımlılığı, bireylerin sosyal hayatında, akademik ve mesleki performansında olumsuz etkilere ve psikolojik sorunlara neden olabilir,
- İnternetin başında aşırı zaman geçirmek, fiziksel sağlık sorunlarına (göz yorgunluğu, duruş bozukluğu, obezite vb.) yol açabilir,
- Güvenliği doğrulanmamış hesaplarla kurulan iletişim çeşitli tehlikelere (kişisel veri sızdırma, dolandırıcılık, istismar vb.) yol açabilir
- Şiddet, nefret ve ırkçılık içerikli faaliyetler, bireylerin ve toplumun huzurunu bozabilir; psikolojik ve toplumsal zararlara neden olabilir,
- Silah ve madde kullanımıyla ilgili içeriklere erişim, bireylerin yasa dışı faaliyetlere yönelmesine ve fiziksel/psikolojik zararlar yaşamasına sebep olabilir,
- Telif hakları ihlali, hukuki sorunlara, maddi kayıplara ve içerik üreticilerinin haklarının zarar görmesine yol açabilir,

1.1 Dijital Çağın Hastalığı: Yeni Nesil Bağımlılıklar

Dijitalleşme, fiziksel dünyanın internet ortamına taşınması ve günlük yaşamın birçok alanında dijital teknolojilerin etkin şekilde kullanılmaya başlanmasıyla ortaya çıkmıştır. Küreselleşmenin önemli bir basamağı olan dijital iletişim araçları, bilgiye erişimi kolaylaştırmış, sosyal etkileşimi hızlandırmış ve iş yapış şekillerinde köklü değişikliklere neden olmuştur.

Günümüzde, akıllı telefonlar, bilgisayarlar, tabletler ve diğer dijital cihazların aşırı ve kontrolsüz kullanımı sonucu dijital bağımlılık görülebilmektedir. Dijital bağımlılık; yalnızca mobil ağların değil, sosyal medya platformlarının, çevrimiçi



**Avrupa Birliği tarafından
finanse edilmektedir**

oyunların, dijital içeriklerin ve genel olarak internetin yoğun şekilde kullanılmasıyla ortaya çıkan bir sağlık sorunudur. Teknolojinin sunduğu imkanlar hayatı kolaylaştırırken, aşırı ve bilinçsiz kullanımı bireylerin psikolojik, sosyal ve fiziksel sağlıklarını olumsuz etkileyebilmektedir.

1.2 Dijital Bağımlılık Nedir?

Bağımlılık; bir nesneye, davranışa veya maddeye karşı duyulan isteğin kişinin yaşamını olumsuz etkilediğini bilmesine rağmen bu isteği kontrol edememesi durumudur. Dijital bağımlılık ise; akıllı telefonlar, bilgisayarlar, tabletler, televizyonlar, oyun konsolları ve benzeri dijital teknolojilere aşırı ve kontrolsüz şekilde bağlanma sonucu ortaya çıkan davranışsal bir bozukluktur.

Bireyleri dijital bağımlı hale getiren etkenler zaman içinde çeşitlenmiştir. Günümüzde teknolojinin hızla gelişmesi, internet ve dijital ortamların yaygınlaşması, sosyal medya, çevrimiçi oyunlar, dijital içerik tüketimi ve televizyon izleme gibi faktörler dijital bağımlılığa neden olabilmektedir. Dijitale bağımlı birey, yüz yüze iletişim yerine sıklıkla dijital ortamda etkileşimi tercih eder ve dijital cihazlardan uzak kaldığında huzursuzluk, yalnızlık veya eksiklik hissedebilir.

1.3 Dijital Çağın Getirdiği Kaygı Bozuklukları: Fobi, Nomofobi, Netlessfobi

Psikolojide bir tür anksiyete bozukluğu olarak tanımlanan fobi; kişinin belirli bir nesne, durum veya olgu karşısında kendini tehlikede hissederek, aşırı ve mantıksız bir korku geliştirmesidir. Fobik bir nesne veya durumla karşılaşan birey, abartılı ve irrasyonel tepkiler verebilir; bu da kişinin günlük yaşamını olumsuz etkileyen bir duygu durum bozukluğuna yol açar. Fobiler, bireyin bilişsel ve davranışsal tepkileri incelenerek, uygun terapilerle tedavi edilebilen bir rahatsızlıktır.

Nomofobi, bireyin cep telefonundan uzak kalma veya telefonuna erişememe korkusu olarak tanımlanır. Cep telefonu kullanımı sırasında beyinde dopamin salgısının artması, kişide telefona karşı bağımlılık duygusunun gelişmesine neden olabilir. Dijital dünyayla kurulan iletişimin kontrolsüz ve aşırı hâle gelmesi, nomofobinin ortaya çıkmasına yol açan önemli etkenlerdendir. Bu bağımlılık



**Avrupa Birliği tarafından
finanse edilmektedir**

duygusu, kişinin sosyal ilişkilerini ve günlük yaşamını olumsuz etkileyebilir; etkileri travmatik boyutlara ulaştığında ise depresyona kadar ilerleyebilen ciddi psikolojik sorunlara sebep olabilir.

Netlessfobi, aşırı internet kullanımına bağlı olarak kişinin internetsiz bir ortamda kalmaktan yoğun şekilde endişe duyması durumudur. Netlessfobik bireyler, dijital dünyayla bağlantılarını kaybedecekleri ortamlardan kaçınır ve bu nedenle sosyal yaşamdan uzaklaşabilirler. Sürekli olarak dijital platformlarda aktif olma isteği, zamanla bağımlılık gelişmesine yol açar, bireyde davranışsal ve duygusal değişiklikler görülebilir. Global bir sorun hâline gelen netlessfobi, bireylerin hem psikolojik hem de fizyolojik açıdan olumsuz etkilenmesine neden olabilmektedir.

1.4 Dijital Oyun Bağımlılığı Nedir?

Dijital oyun bağımlılığı, çevrimiçi veya dijital oyunların aşırı ve kontrolsüz şekilde oynanması sonucunda bireyde duygusal ve davranışsal bozuklukların ortaya çıkması şeklinde tanımlanır. Oyun oynarken yaşanan etkileşim ve sosyalleşme duygusu, bazı bireylerde bağımlılık gelişmesine neden olabilir. Bu bağımlılık nedeniyle kişinin davranışlarını kontrol edememesi, hem kendisi hem de çevresi için çeşitli tehditler oluşturabilir.

Bağımlılığa yol açan faktörlerin belirlenmesi ve önleyici tedbirlerin alınması, dijital oyun bağımlılığı riskini azaltmada önemli bir rol oynar. Dijital oyun bağımlılığı, zihinsel fonksiyonlarda bozulmalara ve ciddi sağlık sorunlarına yol açabilir. Kontrollü ve dengeli şekilde oyun oynamak; odaklanma ve konsantrasyon gibi zihinsel becerileri geliştirilirken, aşırıya kaçılması durumunda birey, yaşına bakmaksızın bağımlı hâle gelebilir.

1.4.1 Dijital Oyun Bağımlılığın Cinsiyet Boyutu

Dijital oyunlar, içerik ve tema bakımından çoğu zaman toplumsal cinsiyet kalıplarına göre ayrılmaktadır. Savaş ve şiddet içeren oyunlara erkek bireylerin yönelimi daha fazla olurken, giydirme ve makyaj gibi oyunlara ise kadın bireylerin ilgisi daha yüksek olabilmektedir. Toplumda varlığını sürdüren cinsiyete dayalı ayrımcılık, dijital platformlarda da kendini göstermektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Popüler kültürde gözlenen bu algı, cinsiyet faktörleri üzerinden özgüven problemlerinin oluşmasına zemin hazırlamaktadır. Örneğin, dijital oyunlarda erkek karakterler çoğunlukla daha güçlü ve dominant şekilde lanse edilirken, kadın karakterler ise daha pasif veya farklı rollerde sunulabilmektedir. Dijital oyunlarda oluşturulan sanal kimlikler, özellikle gelişim çağındaki bireylerin gerçek kimliğine de etki edebilmektedir.

Sonuç olarak, dijital oyunlarda cinsiyete dayalı içerik ve karakter ayrımları, bireylerin kendilik algısı ve toplumsal rol anlayışı üzerinde kalıcı etkiler bırakabilmektedir. Özellikle çocuklar ve gençler, oyunlardaki cinsiyet temsilleriyle özdeşleşerek, toplumsal cinsiyet normlarını içselleştirebilir veya bu normlara karşı farklı tutumlar geliştirebilirler. Bu nedenle, dijital oyunların tasarımında daha kapsayıcı ve eşitlikçi yaklaşımların benimsenmesi, bireylerin sağlıklı bir kimlik gelişimi açısından büyük önem taşımaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

2.Dijital Haklar ve Korunma Mekanizmaları

Dijitalleşmenin hızla yaygınlaştığı günümüzde, bireylerin sanal ortamda karşılaştıkları riskler ve hak ihlalleri de giderek artmaktadır. Bu durum, dijital hakların tanınması ve korunması konusunun önemini ön plana çıkarmaktadır. Dijital haklar, bireylerin internet ve teknolojik araçlar üzerinden kişisel verilerini, mahremiyetini ve ifade özgürlüğünü koruma amacıyla oluşturulan hukuki ve etik düzenlemeleri kapsamaktadır. Dijital ortamda güvenliğin sağlanabilmesi ve bireylerin haklarının etkin şekilde korunabilmesi için ulusal ve uluslararası düzeyde çeşitli mekanizmalar geliştirilmiştir.

2.1 Avrupa Birliği Gözünden: Dijital Haklarımız

Siber Zorbalıkla mücadelede resmi hak ve hukukları bilmek kilit rol taşımaktadır. Bu kapsamda, dijital hak ve hukuklar da büyük önem taşımaktadır. İnsan hakları kavramı, modern toplumlarda giderek daha fazla önem kazanmakta ve farklı eğitim düzeylerinde yaygın olarak ele alınmaktadır. İnsan hakları, herhangi bir ayırım gözetmeksizin, tüm insanların doğuştan sahip olduğu ve evrensel kabul edilen temel hak ve özgürlükler bütünüdür. İnsan haklarının temel amacı, tüm bireylerin onurunu ve özgürlüğünü korumak, kişilerin güvenlik, eşitlik, adalet ve refahını sağlamak, ayrımcılığa karşı koruma sağlamak ve toplum içinde barışçıl bir yaşamı garanti altına almaktır.[\[1\]](#)

İnsan hakları kavramı, modern toplumlarda çeşitli eğitim, medya ve sivil toplum faaliyetleri sayesinde giderek daha fazla önem kazanmaktadır. Yapılan araştırmalar, bireylerin hak arama konusunda bilinç düzeylerinin arttığını göstermektedir. Ancak dijital haklar alanında farkındalık düzeyi geleneksel insan haklarına kıyasla daha düşük olabilmektedir. Özellikle siber zorbalık vakalarında, mağdurların dijital ortamdaki haklarını yeterince bilmemeleri, hukuki süreçleri başlatmada tereddüt yaşamalarına yol açmaktadır.

Bu durumun sebebi Vatandaşlık ve Dijital Vatandaşlık kavramları incelendiğinde ortaya çıkmaktadır. Vatandaşlık, bir devlet ve birey arasındaki karşılıklı hak, görev



**Avrupa Birliği tarafından
finanse edilmektedir**

ve sorumluluk ilişkilerini belirleyen kavram olarak kabul edilmektedir. Kısaca tanımlamak gerekirse, kişi ile devleti birbirine bağlayan kavramdır. Vatandaşlık kavramı bağlamında kişi vergi vermek, kurallara uymak ve devleti için üretmek gibi görevlerini yerine getirirken devlet de bu görevlerin karşılığında kişinin insan haklarını koruyacağını güvence altına almaktadır.

Dijital dünyada devletleşme gibi bir yapının olmaması kötü niyetli kişileri dijital suçlara iterken iyi niyetli kişilerin ise bu suçlara karşı yapabilecekleri bir şey olmadığı izlenimi yaratmıştır. Bu sorunu düzeltmek için farklı kurum kuruluş ve kişiler birçok farklı çalışma gerçekleştirmiştir. Eğitimde Teknoloji alanında uzman isimlerden biri olan Mike Ribble 2011 yılında Dijital Vatandaşlık kavramını 9 boyutta incelemiş, bu 9 boyutu Dijital Erişim, Dijital Ticaret, Dijital İletişim, Dijital Okuryazarlık, Dijital Etik, Dijital Hukuk, Dijital Haklar ve Sorumluluklar, Dijital Sağlık ve Dijital Güvenlik olarak belirlemiştir. 2021 yılında ISTE(Uluslararası Eğitimde Teknoloji Topluluğu), Dijital Vatandaşlık kavramının önemini vurgulamış ve bir “internette yapılamaması gerekenler listesi” olmaktan çok daha fazlası olduğunu belirtmiştir. [2]

Günümüzde teknolojinin ve dijital çağın artmasıyla Dijital Vatandaşlık, Dijital Hak ve Sorumluluklar kavramları Avrupa Birliği’nin de gündemine alınmış, bu bağlamda farklı çalışmalar hazırlanmaktadır. Türkiye-AB Mali İşbirliği IPA-II süreci kapsamında devam etmekte olan projeler sürecinde Avrupa Polis Teşkilatı Veri Koruma Fonksiyonu Başkanı Daniel Drewer tarafından “Dijital Çağda Temel Hakları Korumak İçin Uluslararası Kurallar” adında bir sunum hazırlanmıştır.

Sunumda dijital çağda temel insan haklarının korunmasına yönelik olarak Birleşmiş Milletler, Avrupa Konseyi ve Avrupa Birliği’nin bu alanda yaptığı çalışmalar listelenmiş; belirlenen kurallar, kararlar ve sözleşmeler aktarılmıştır. [3]

Avrupa Birliği’nin alanla ilgili yaptığı çalışmalardan bir tanesi de “Dijital Haklar ve İlkeler Hakkında Avrupa Bildirgesi”dir. Bildirge, 6 ana tematik başlığa ayrılmıştır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Bu başlıklar genellikle şu şekilde sıralanmaktadır:

1)İnsanları Dijital Dönüşümün Merkezine Koymak: Bildirgede, teknolojinin Avrupa Birliği çatısı altında yaşayan tüm insanlara hizmet etmesi ve fayda sağlaması temel amaç olarak belirlenmiştir. Bu doğrultuda, teknolojinin bireyleri güçlendirmesi, temel haklarını ve güvenliğini koruması gerekmektedir. Bildirgeye göre, dijital dönüşüm sürecinde teknoloji insanların haklarına ve güvenliğine zarar vermemeli; insan odaklı bir yaklaşım benimsenmelidir.

2)Dayanışma ve Kapsayıcılık: Bu başlık kapsamında, insanların uygun maliyetli ve yüksek hızdaki internete erişime sahip olması temel bir hak olarak kabul edilmektedir. Dijital teknolojilerden faydalanabileceği kadar gerekli olan eğitim ve beceriyi alması gerekmektedir. Toplumda önemli bir rol oynayan kamuya açık dijital hizmetlere erişim de herkes için sağlanmaktadır.

3)Seçim Özgürlüğü: Bu başlığa göre herkesin çevrimiçi ortamda özgürce kendi seçimlerini yapabilmesi gerekmektedir. İnsanların çevrimiçi ortamda kendi istedikleri sistem ve hizmetleri kullanabilmesi gerektiğinin altı çizilmiş, yapay zeka araçlarına da özel bir vurgu yapılmıştır. Yapay zeka araçlarının insanlara hizmet etmesi gereken bir araç olduğu ve kullanımlarındaki nihai amacın refah seviyesini artırmak olduğu da belirtilmiştir.

4)Dijital Halka Açık Alanlara Katılım Sağlamak: Bu maddede, herkesin güvenilir, çeşitli ve çok dilli bir çevrimiçi ortama erişim sağlayabilmesi, kullandıkları servislerin de kimin olduğunu ve kim tarafından yönetildiklerini bilmeleri gerektiği yazılmıştır. Böylece insanların bilgi kirliliğinden uzak tutulması amaçlanmaktadır. Bu hakkı güvenli şekilde kullanmak bireylerin kendi sorumluluğundadır. Kullanılan servisin yönetici kişi veya kurumu bilmek, servisle ilgili herhangi bir sorun veya ihtiyaç durumunda doğru ve hızlı bir şekilde çözüm üretebilmek açısından büyük önem taşımaktadır.

5)Güvenlik, Emniyet ve Güçlendirme: Dijital teknolojiler, ürünler ve hizmetlerin güvenliğinin ve gizliliğinin korunması hedeflenmektedir. Avrupa Birliği



**Avrupa Birliği tarafından
finanse edilmektedir**

vatandaşları, iş yerlerini ve halka açık servisleri siber suçlara karşı koruması gerekmektedir. Avrupa Birliği yasalarına göre, bireylerin kişisel ve toplumsal verilerin işlenmesi ve kullanımı üzerinde etkin kontrol hakkına sahip olması gerekmektedir. Dijital ortamda kullanıcı verilerinin kontrolünün yalnızca ilgili kullanıcıda olması zorunludur.

6)Sürdürülebilirlik. Dijital dönüşüm, çevre ve iklim üzerindeki etkilerin en aza indirilmesi ve dijital teknolojilerin sürdürülebilirliği, kaynak verimliliğini, döngüsel ekonomiyi ve enerji verimliliğini teşvik edecek biçimde tasarlanmalıdır. Dijitalleşme ile toplumların daha sürdürülebilir olmaları amaçlanmaktadır.

Bu bildirgeden yapılan çıkarımları özetlemek gerekirse:

- Teknoloji insanlara fayda sağlamak amacıyla geliştirilmelidir.
- Uygun maliyetli ve yüksek hızlı internete erişim her vatandaşın hakkıdır.
- Dijital servis veya ürünlerin kullanımındaki seçim özgürlüğü bireye aittir.
- Kullanılan dijital ürünün sahibini ve yöneticisini bilmek temel haklardan biridir.
- Kişisel ve toplumsal verilerin efektif kontrolü, bireyin elinde olmalıdır.[\[2\]](#)

Bunlardan hareketle, ülkemizdeki KVKK(Kişisel Verilerin Korunması Kanunu)'ya da dikkat çekmek büyük önem arz etmektedir. Avrupa Bildirgesi'nin son maddesinde de belirtildiği üzere, bir kişinin bütün verileri o kişinin kontrolünde olmak zorundadır. Bireyler izinsiz olarak kendisine ait olmayan verileri kullanamaz veya paylaşamaz.

Gerçek hayatta bir kişinin ürettiği resim veya fotoğraf, ilgili kişinin izni olmaksızın başkaları tarafından ticari amaçlarla kullanılamaz veya satılamaz. Benzer şekilde, dijital ortamda bireylerin ürettiği içeriklerin izinsiz olarak üçüncü kişiler tarafından kullanılması ve ekonomik kazanç sağlanması hukuken yasaktır. Telif hakkı ve fikri



**Avrupa Birliği tarafından
finanse edilmektedir**

mülkiyet kuralları kapsamında, her türlü özgün eser sahibinin izni olmadan ticari faaliyete konu edilemez.

2.2 Siber Zorbalığa Karşı Nasıl Korunabiliriz?

Dijital haklarının bilincinde olan bireylerin, siber zorbalığa karşı korunabilmeleri için bazı temel adımlara ve ilkelere dikkat etmeleri gerekmektedir. Bu önlemler, genellikle aile üyeleri, arkadaşlar veya eğitimciler tarafından sıkça dile getirilen ve bilinen, ancak çoğu zaman uygulamada göz ardı edilen hususlardır.

Emniyet Genel Müdürlüğü tarafından yayımlanan ve siber zorbalıktan korunma konusunda altı maddelik öneriler içeren makale, bu alanda önemli bir rehber niteliği taşımaktadır.[\[4\]](#) Söz konusu çalışmada sunulan maddeler, siber zorbalığa karşı alınabilecek önlemleri detaylı bir biçimde açıklamaktadır. Bu maddeleri incelemek gerekirse;

1) Tanımadığınız kişilerden gelen arkadaşlık, takip ya da mesaj isteklerine cevap vermeyin.

Her ne kadar basit bir önlem gibi görünse de, siber zorbalık vakalarının çoğunun temelinde bu madde yer almaktadır. Sosyal medya hesaplarında tanımadık kişilerden gelen takip veya arkadaşlık isteklerini kabul etmek, bireylerin özel yaşamlarına dair bilgileri kontrolsüz şekilde paylaşımlarına yol açabilir. Dijital ortamdaki anonimlik, mesajlaşma süreçlerinde ek bir risk unsuru oluşturur; karşıdaki kişinin kimliğini doğrulamanın güç olması, kötü niyetli kişileri yanıltıcı bilgi vermeye ve kimliklerini gizlemeye teşvik edebilmektedir.

2) Siber zorbaya karşılık vermeyin ve misilleme yapmayın.

Zorbalık yapan kişilerin en belirgin ortak özelliklerinden biri, karşılarındaki bireyin moralini bozarak bundan eğlence elde etmeyi amaçlamaktır. Gerçek hayatta olduğu gibi siber zorbalıkta da, zorbalık yapan kişilere doğrudan karşılık vermemek ve onları görmezden gelmek önerilmektedir. Bu yaklaşım, zorbaların eğlence



**Avrupa Birliği tarafından
finanse edilmektedir**

kaynaklarının kesilmesine ve çoğu durumda hedef aldıkları kişiyi rahatsız etmeyi bırakmalarına yol açabilmektedir.

3)Siber zorbayı ilgili sosyal medya platformuna şikayet edin ve engelleyin.

Bu madde, önceki maddenin üzerine uygulanmalıdır. Siber zorba biriyle karşılaşan kişi, zorbaya cevap yazmak yerine kendisini şikayet etmeli ve engellemelidir. Günümüzde popüler olarak kullanılan bütün sosyal medya platformlarında şikayet etme ve engelleme özellikleri bulunmaktadır. Bu özellikleri kullanmak ise kişinin kendi ellerindedir. Bir siber zorba engellendiğinde, zorbanın o kişiye tekrar ulaşabilmesi için yeni bir hesap açmaktan başka şansı bulunmamaktadır. Çoğu siber zorba kendilerine hızlıca dalga geçip eğlenebilecekleri kurbanlar aradığından dolayı bu uzun ve yorucu işlemi yapmaktansa başka bir kişiye mesaj atmayı tercih edeceklerdir.

4) Çocuklar, siber zorbalığa maruz kalırsanız bu durumu ailenizle paylaşın.

Her ne kadar bu madde özellikle çocuklara yönelik olarak ifade edilmiş olsa da, aslında tüm yaş grupları için geçerlidir. Siber zorbalığa maruz kalan bireylerin, yaşadıkları durumu ailelerine, ya da güven duydukları bir öğretmen veya arkadaşlarına anlatmaları önemlidir. Bu şekilde, hem bireyin yaşadığı olumsuz deneyim konusunda psikolojik destek alması sağlanmakta, hem de olaydan haberdar olan kişiler ilerleyen süreçte benzer bir durumla karşılaşıldığında daha etkili ve ciddi önlemler alınmasına yardımcı olabilmektedir.

5) Mağduriyet yaşanan durumlara ait delilleri saklayın.

Zorbalık başlangıçta engellenemediği ve olaylar büyüdüğü takdirde, mağdurların duruma daha ciddi şekilde yaklaşmaları gerekmektedir. Kişisel hakların yasal olarak korunabilmesi için somut delillerin sunulması önem taşır. Bu nedenle, siber zorba ile yapılan mesajlaşmalar silinmemeli; sistem üzerinde silinme ihtimali varsa, ekran görüntüsü alınarak güvenli bir yerde muhafaza edilmelidir. Ayrıca, sadece mesajlar değil, zorbalığı yapan kişinin profil bilgileri de delil olarak



**Avrupa Birliği tarafından
finanse edilmektedir**

saklanmalıdır. Bu uygulama, zorba hakkında yasal işlem yapılmasını kolaylaştıracak ve sürecin daha hızlı ilerlemesine katkı sağlayacaktır.

6) 18 yaşından küçükseniz anne veya babanızla; büyükseniz şahsen Cumhuriyet Savcılığına, polise veya jandarmaya başvurun.

Gerçek yaşamda bireyler, herhangi bir olumsuz olayla karşılaştıklarında Cumhuriyet Savcılığına, polis veya jandarma birimlerine başvurarak haklarını arayabilmektedirler. Dijital haklarının farkında olan ve gerekli delilleri elinde bulunduran bireyler de benzer şekilde, dijital ortamda maruz kaldıkları ihlallerin çözümü için bu resmi mercilere başvurabilmektedir. Siber zorbalığın önemli etkilerinden biri ise, mağdurların kendilerini yalnız hissetmeleri ve destek alabilecekleri kimsenin olmadığı düşüncesine kapılmalarıdır.

Bu durum, temelde psikolojik bir olgu olmakla birlikte, dijital haklar da tıpkı gerçek hayattaki haklar gibi yasal düzenlemelerle güvence altına alınmıştır. Bireylerin yapması gereken, en kısa sürede doğru mercilere başvurarak haklarını arama konusunda gerekli adımları atmaktır. Cumhuriyet Savcılığı, polis ve jandarma birimleri, gerçek hayatta olduğu gibi dijital suçlar konusunda da giderek daha fazla deneyim kazanmaktadır. Bu tür vakalarda başvurulacak ilk resmi makamlar bu kurumlardır.[\[3\]](#)

Emniyet Genel Müdürlüğü tarafından önerilen altı maddeye ek olarak, UNICEF Türkiye tarafından da siber zorbalıkla mücadeleye yönelik bir web sayfası hazırlanmıştır. Bu platformda vurgulanan temel yaklaşım, siber zorbalığa karşı mücadelenin ilk ve en önemli aktörünün, bizzat zorbalığa maruz kalan kişinin kendisi olduğudur. Zorbalığa uğrayan bireylerin, kullandıkları dijital platformlarda ilgili profilleri bildirmeleri, çevrelerindeki kişileri olası zorbalık riskine karşı bilgilendirmeleri ve yaşadıkları durumu kamuoyuyla paylaşarak seslerini duyurmaları, etkili bir mücadele stratejisi olarak öne çıkmaktadır.

Siber zorbalıktan korunmaya yönelik ne kadar önlem alınırsa alınsın, nihai sorumluluk bireyin kendisindedir. Çoğu siber zorbalık vakası, henüz başlamadan



**Avrupa Birliği tarafından
finanse edilmektedir**

önce alınacak basit önlemlerle engellenebilir. Ancak siber zorbalık gerçekleştiğinde, bireylerin gerekli tedbirleri uygulayarak ilgili resmi mercilere başvurmaları gerekmektedir. Siber zorbalıktan korunmanın en etkili yolu ise, bireyin dijital ortamlardaki davranışlarını bilinçli bir şekilde yönetmesidir. [4]



**Avrupa Birliği tarafından
finanse edilmektedir**

3.Siber Zorbalık Nedir?

Siber güvenlik, dijital sistemleri tehditlerden korumaya yönelik yürütülen çeşitli önlemleri kapsamaktadır. Bu kapsamda, bilgi ve verilerin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması, olası saldırıların ve olayların önceden tespit edilerek gerekli müdahalelerin yapılması ve sistemlerin eski haline döndürülmesi hedeflenmektedir.(Ulaştırma ve Altyapı Bakanlığı, 2020).

Siber güvenlik, bireylerden büyük ölçekli şirketlere ve devlet kurumlarına kadar geniş bir kesimi etkileyen kritik bir konu haline gelmiştir. Dijital teknolojilerin hızla gelişmesi, ekonomik faaliyetlerin ve toplumsal etkileşimlerin büyük ölçüde çevrimiçi platformlara taşınmasına yol açmıştır. Ancak bu dönüşüm, bilgi güvenliği, veri gizliliği ve siber saldırılar gibi yeni tehditleri de beraberinde getirmiştir. (Ulaştırma ve Altyapı Bakanlığı,2020:10).

Siber ortamdaki kurum, kuruluş ve kullanıcıların varlıklarının korunması devletlerin ve kurumların en önemli önceliklerinden biridir. Siber saldırıların maliyetleri gerek kamu gerekse özel sektör kuruluşları için çok ciddi boyutlara ulaşabilmektedir. 2024 yılında siber suçların küresel maliyetinin yıllık 9,5 trilyon Amerikan dolarına ulaşacağı öngörülmektedir. Siber güvenlik konusu değerlendirildiğinde sadece teknolojik tedbirlerin yeterli olmadığı, siber güvenliğin teknik bir konu olmanın ötesinde bir anlam taşıdığı, ulusal ve uluslararası güvenlik stratejilerinin bir parçası haline geldiği görülmektedir (Ulaştırma ve Altyapı Bakanlığı, 2024).



**Avrupa Birliği tarafından
finanse edilmektedir**

Ekonomik açıdan bakıldığında, siber güvenlik ihlalleri şirketler için büyük mali kayıplara yol açabilmekte, finansal piyasaları etkileyebilmekte ve küresel ticarete belirsizliklere neden olabilmektedir. Özellikle e-ticaret, bankacılık ve sigortacılık gibi sektörlerde güvenlik açıkları, müşteri güvenini zedeleyerek ekonomik büyümeyi olumsuz etkileyebilir. Öte yandan, gelişmiş güvenlik önlemlerine yapılan yatırımlar, dijital ekonominin sürdürülebilirliğini destekleyerek uzun vadeli ekonomik istikrarı sağlayabilir.

Toplumsal açıdan değerlendirildiğinde, bireylerin kişisel verilerinin korunması, kimlik hırsızlığı ve siber zorbalık gibi konular giderek daha fazla önem kazanmaktadır. Bilgi güvenliğinin sağlanamaması, bireylerin dijital dünyaya olan güvenini sarsarak teknoloji kullanımını olumsuz etkileyebilir. Aynı zamanda devletlerin ulusal güvenlik politikaları da siber tehditlere karşı güçlü önlemler geliştirmeyi zorunlu kılmaktadır

3.1 Bilişim Suçu

Bilişim suçları 5237 sayılı Türk Ceza Kanunu'nda ikinci kitabının üçüncü kısmının onuncu bölümünde "Bilişim Alanında Suçlar" başlığı altında düzenlenmiştir. Bilişim suçları bilginin elektronik ortamda aktarılması sırasında işlenen suçlardır. Bunlar (Yeldan, 2023: 37);

- Bilişim Sistemine Girme (TCK m. 243),
- Sistemi Engelleme, Bozma Verileri Yok Etme veya Değiştirme (TCK m. 244),
- Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK m. 245),



**Avrupa Birliği tarafından
finanse edilmektedir**

- Yasak Cihaz veya Program Kullanma (TCK m. 245/A),
- Tüzel Kişiler Hakkında Güvenlik Tedbirlerinin Uygulanması (TCK m.246)

5237 sayılı Türk Ceza Kanunda (142/2-e), dolandırıcılık (158/1-f), kumar oynanması için yer ve imkân sağlama (228/3), cinsel taciz (105/2-d), özel hayatın gizliliği ihlal (134/1-2. Cümle) suçlarının düzenlendiği maddelerde bu suçların bilişim sistemlerinin kullanılması suretiyle işlenmesi suçun daha ağır cezayı gerektiren nitelikli halleri olarak düzenlenmiştir. Diğer suçlarının çoğunda ise böyle bir düzenleme bulunmaktadır. 5237 sayılı Türk Ceza Kanununda düzenleme yapılırken “bilgisayar suçu”, “siber suç”, “dijital suç”, “elektronik suç”, “sanal suç”, “internet suçu” gibi kavramlar yerine bilişim alanında suçlar kavramının kullanılması öğretide de son derecede yerinde bulunmuş; bilgisayar suçları kavramının daha dar kapsamlı olduğu, siber suç kavramının ise bilişim sistem ağları (özellikle internet) vasıtasıyla gerçekleştirilen eylemler için kullanıldığı, bilişim suçlarının daha üst bir kavram olduğu ifade edilmiştir (Yeldan, 2023: 38).

3.2 Siber Suçlar

Siber Suç, bir bilişim sisteminin güvenliğini ve/veya buna bağlı verileri ve/veya kullanıcılarını hedef alan ve bilişim sistemi kullanılarak işlenen suçlardır. Siber Suçu diğer suçlardan ayıran özelliği bir bilişim sistemi olmadan işlenememesidir. Bu suç türü bilgisayar ve internete özgü suçlar olarak da adlandırılabilir. (Emniyet Genel Müdürlüğü, 2025).

Günümüz dünyasına baktığımız zaman dijitalleşmenin hızla yayılması, bireyler ve kurumlar için büyük kolaylıklar sağlarken aynı zamanda yeni sorunları da



**Avrupa Birliği tarafından
finanse edilmektedir**

beraberinde getirmiştir. Bu sorunlardan biri de siber suçlardır. İnternetin yaygınlaşmasıyla birlikte, kişisel veriler, finansal güvenlik gibi alanlarda önemli riskler ortaya çıkmıştır.

Siber suçları, bireyler ve kurumların sanal ortamdaki varlıklarına zarar veren yasa dışı faaliyetleri içermektedir. Bunlara örnek olarak; kart hırsızlığı, kimlik hırsızlığı, kişisel verilerin pazarlanması, fidye yazılımlar, sanal dolandırıcılık örnek olarak verilebilir. Günümüzde siber suçlar büyük ekonomik ve toplumsal kayıplara neden olmaktadır.

3.3 Siber Zorbalık Nedir?

“Siber” kelimesi İngilizce “Cyber” kelimesinden uyarlanıp kullanılmaya başlayan bir kelime olup “Bilgisayar ağlarına ait olan”, İnternete ait olan”, “Sanal Gerçeklik” anlamlarına gelmektedir. İngilizcedeki siber bullying ifadesi Türkçemizde sanal zorbalık anlamına gelmektedir. Bu tür eylemler çevrimiçi zorbalık, e-mobbing, cyber mobbing şekillerinde ifade edilmektedir (Yeldan, 2023: 29).

3.4 Türkiye’de Siber Zorbalık

2023 yılında dünya genelinde 5 milyarın üzerinde kullanıcının olduğu görülmektedir. Araştırmalara göre; Türkiye’de internet kullanıcılarının günlük ortalama 7,5 saat internette zaman geçirmekte ve bunun yaklaşık 3 saatini sosyal medya üzerinde harcamaktadır (Ulaştırma ve Altyapı Bakanlığı, 2024:6).



**Avrupa Birliği tarafından
finanse edilmektedir**

Türkiye çapında siber zorbalığın yaygınlığı ve farkındalığı ilişkin araştırmada, Türkiye genelinde ortaokul öğrencilerinin yaklaşık %12'sinin sözlü siber zorbalığa, %10,5'inin ise sözlü olarak siber zorbalık yaptıkları görülmektedir. Siber zorba ve kurban olma oranlarının en yüksek olduğu il İstanbul. İstanbul'da siber mağdur/kurban olma oranı %20'ye yaklaşırken, siber zorba olma oranı ise %15'in üzerine çıkmaktadır. (Baştürk,2020:41).

Okul ortamında siber zorbalıkla mücadele edecek adımların atılması günümüzde temel bir ihtiyaç haline gelmiştir. Okullarda zorbalıkla mücadele programlarının geliştirilmesi, bu programın okul ortamında ders formatında uygulanmasının öğrenciler açısından faydalı olacağı ifade edilmektedir. Dersler kapsamında öğrencilere, sınıf arkadaşları arasında siber zorbalığa maruz kalan ya da olumsuz içeriklere hedef olan bireyleri nasıl tanıyabilecekleri öğretilmelidir. Ayrıca öğrenciler, siber zorbalığa kayıtsız kalmamaları gerektiği konusunda bilinçlendirilmelidir. Tanık oldukları durumları güvenilir yetişkinlere aktarmaları ve zorbalığa karşı tutum sergilemeleri gerektiği vurgulanmalıdır. Aksi halde, siber zorbalığın önce okul ortamında ardından toplumsal düzeyde yaygınlaşmasının önüne geçilemeyeceği belirtilmektedir (Akca ve ark., 2014:19).

3.5 Türkiye ve Avrupa Birliği Politikaları

Türk Dil Kurumu'na göre politika, “Devletin etkinliklerini amaç, yöntem ve içerik olarak düzenleme ve gerçekleştirme esaslarının bütünü” anlamına gelir (TDK, 2022).



**Avrupa Birliği tarafından
finanse edilmektedir**

Siber güvenlik politikasında geçen "politika" kelimesi, bir kurum ya da bir devletin siber güvenliğini, siber verilerini korumak amacıyla benimsediği kurallar, ilkeler, stratejiler ve yönergeler bütünü anlamına gelir. Siber güvenlik politikası: “Sistemlerimizi, verilerimizi ve kullanıcılarımızı dijital tehditlere karşı nasıl koruyacağız?” sorusuna verilen kapsamlı cevaptır.

3.5.1 Türkiye’de Siber Güvenlik Politikaları

Son yıllarda teknolojinin gelişmesiyle ülkemizde siber güvenlik stratejileri bir gereklilik değil zorunluluk olduğu ortaya çıkmıştır özellikle Türk şirketleri ile kamu kurumlarında görevli yetkililerin sıkça siber casusluk faaliyetlerinin hedefi hâline gelmesi, bu alandaki güvenlik açıklarını açıkça gözler önüne sermektedir. Bu durum, siber güvenlik alanına yönelik yatırımların artırılmasını hem ulusal güvenlik hem de ekonomik istikrar açısından zorunlu kılmaktadır.

Siber güvenlik, günümüzde toplumdan ekonomiye, uluslararası ilişkilerden eğitime kadar her alanda vazgeçilmez bir ihtiyaç haline gelmiştir. Türkiye, stratejik konumu, güçlü devlet yapısı ve teknolojik gelişmeleriyle siber tehditler için cazip bir hedef haline gelmiştir. Ancak ülkemiz, siber güvenliği güçlendirmek amacıyla yerli ve milli teknolojilere yatırım yapmış, nitelikli insan kaynağını geliştirerek bu alandaki kapasitesini artırmıştır. Erken dönemde alınan tedbirler ve oluşturulan ulusal siber güvenlik yapısı sayesinde Türkiye, siber güvenlik alanında öne çıkan ülkeler arasında yer almakta ve dijital çağın getirdiği risklere karşı ulusal çıkarlarını korumaya yönelik adımlar atmaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Pandemi süreciyle birlikte daha önce tanımlanmış bilgi güvenliği ve siber güvenlik kavramları yeni bir boyut kazanmış, artan dijitalleşme bu alanda güncel yaklaşımları zorunlu kılmıştır. Özellikle iş sürekliliğinin korunması, ekonomik sistemin işleyişi ve arz-talep dengesinin sağlanması için yaygınlaşan uzaktan çalışma modeli, siber tehditlerin hedefi haline gelmiştir.

Birçok kurum, yeterli dijital altyapıya ve bilgi güvenliği önlemlerine sahip olmadan, hızla uzaktan çalışma düzenine geçmek zorunda kalmıştır. Bu durum, siber saldırılar açısından ciddi bir risk yaratmış ve kurumsal bilgi güvenliği konusunda var olan açıkları daha görünür kılmıştır. Pandemi, dijital dönüşümün kaçınılmazlığını ortaya koyarken, aynı zamanda siber güvenliğin iş sürekliliği için ne denli kritik olduğunu da gözler önüne sermiştir (Yıldırım, 2024:28).

Türkiye’de siber güvenliğe yönelik kurumsal yapılanma üç ana başlık altında şekillenmiştir. İlk grupta, doğrudan siber suçlarla mücadele eden ve bu alanda faaliyet yürüten kamu kurumları yer almaktadır. Bu yapılar, dijital ortamda işlenen suçlara karşı hukuki ve teknik önlemleri uygulamakla görevlidir. İkinci grubu ise kritik altyapıların korunması, kamu kurumlarının dijital güvenliğinin sağlanması ve Türkiye’nin genel siber güvenlik kapasitesinin artırılmasına odaklanan kurumlar oluşturmaktadır. Bu kuruluşlar daha çok stratejik güvenlik planlamaları ve kamu siber savunma sistemleri üzerine çalışmaktadır. Üçüncü yapıda ise, devlet destekli fakat özel girişim niteliği taşıyan kuruluşlar bulunmaktadır. Bu kurumlar, siber güvenlik ekosistemini destekleyici projeler ve iş birlikleriyle sektöre katkı sunmaktadır. Tüm bu yapılanmaların koordinasyonunu sağlayan ve Türkiye'nin



**Avrupa Birliği tarafından
finanse edilmektedir**

ulusal siber güvenlik politikalarını belirleyip yönlendiren en üst düzey organ ise Siber Güvenlik Kurulu'dur. (Yıldırım, 2024:29).

Siber Güvenlik Kurulu'nun görevleri kısaca şunlardır (BTK, 2017);

- Ülke genelinde siber güvenliğin sağlanmasına yönelik politika, strateji ve eylem planlarını onaylamak, bu belgelerin etkili bir biçimde hayata geçirilmesi için gerekli kararları almak,
- Ulusal ölçekte korunması gereken kritik altyapıların belirlenmesine yönelik sunulan önerileri değerlendirmek ve karara bağlamak,
- Mevzuat kapsamında siber güvenlikle ilgili yükümlülüklerin tamamından ya da bir kısmından muaf tutulacak kurum ve kuruluşları belirlemek,
- Yasa ile kendisine verilen diğer görevleri yerine getirmek.

3.5.2 Türkiye'de Siber Güvenlik Kanunu

- Teknolojinin gelişmesiyle artan siber tehditler, ülkeleri ulusal güvenlik stratejileri geliştirmeye yöneltmiştir. Türkiye'de de bu kapsamda strateji belgeleri hazırlanmış, kurumlar kurulmuş ve yasal düzenlemeler yapılmıştır. Son olarak Siber Güvenlik Kanunu Teklifi, 10 Ocak 2025'te TBMM'ye sunulmuş ve 12 Mart 2025'te kabul edilerek yasalaşmıştır.
- Kanunun temel amacı siber tehditlerle mücadelede daha kapsamlı bir hukuki zemin oluşturmak. Siber Güvenlik Kanunun öne çıkan iki maddesi şöyledir (Türkiye Cumhuriyeti, 2025) ;
- **MADDE 1-(1) Bu Kanunun amacı,** Türkiye Cumhuriyeti'nin siber uzaydaki milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan



**Avrupa Birliği tarafından
finanse edilmektedir**

yöneltilen mevcut ve muhtemel tehditlerin tespit ve bertaraf edilmesi, siber olayların muhtemel etkilerini azaltmaya yönelik esasların belirlenmesi, kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşların siber saldırılara karşı korunmasına yönelik gerekli düzenlemelerin yapılması, ülkenin siber güvenliğini güçlendirmek için strateji ve politikaların belirlenmesi ile Siber Güvenlik Kurulunun kurulmasına ilişkin esasları düzenlemektir.

• **MADDE 4- (1) Siber güvenliğin sağlanmasında temel ilkeler şunlardır;**

- a) Siber güvenlik milli güvenliğin ayrılmaz bir parçasıdır.
- b) Kritik altyapı ve bilişim sistemlerinin korunması ile güvenli bir siber uzay oluşturulması temel hedeftir.
- c) Siber güvenlikle ilgili çalışmalar kurumsallık, süreklilik ve sürdürülebilirlik temelli yürütülür.
- d) Siber güvenlik tedbirlerinin, hizmet ve ürünlerin tüm yaşam döngüsü boyunca uygulanması esastır.
- e) Siber güvenliğin sağlanmasına yönelik çalışmalarda öncelikle yerli ve milli ürünler tercih edilir.
- f) Siber güvenlik politika ve stratejilerinin yürütülmesi ile siber saldırıların önlenmesi veya etkisinin azaltılmasına yönelik gerekli tedbirlerin alınmasından tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler sorumludur.
- g) Siber güvenlik süreçlerinin yürütülmesinde hesap verebilirlik esastır.
- h) Siber güvenlik politika ve strateji geliştirme çalışmaları sürekli gelişim yaklaşımı ile yürütülür.



**Avrupa Birliği tarafından
finanse edilmektedir**

- i) Siber güvenlik alanında nitelikli insan kaynağı kabiliyet ve kapasitesinin artırılmasına yönelik çalışmalar teşvik edilir.
- j) Siber güvenlik kültürünün toplum geneline yaygınlaştırılması hedeflenir.
- k) Hukukun üstünlüğü, temel insan hak ve hürriyetleri ile mahremiyetin korunması ilkeleri temel esas kabul edilir

Bu bağlamda, 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, dijital tehditlerin artış gösterdiği günümüz koşullarında Türkiye'nin siber alandaki direncini artırmayı amaçlamaktadır. Kanun, yalnızca teknik tedbirleri değil, aynı zamanda kurumsal kapasitenin geliştirilmesini, yerli teknolojilerin önceliklendirilmesini, bireylerin hak ve özgürlüklerinin korunmasını ve toplumun genelinde siber farkındalık düzeyinin yükseltilmesini hedeflemektedir.

Bu düzenlemeler, siber güvenliğin artık yalnızca teknik bir konu olmaktan çıkıp; ulusal güvenlik, toplumsal bilinçlenme ve hukuk devleti ilkeleriyle doğrudan ilişkili çok boyutlu bir alan haline geldiğini göstermektedir. Kamu ve özel sektör aktörleri ile bireylerin ortak sorumluluğu vurgulanmakta; sürdürülebilirlik ve hesap verebilirlik esas alınarak uzun vadeli bir bakış açısı benimsenmektedir.

Sonuç olarak, siber güvenlik politikaları sadece dijital sistemlerin korunmasıyla sınırlı kalmamakta; bireysel özgürlükler, mahremiyet hakkı ve hukukun üstünlüğü gibi temel değerlerin güvence altına alınmasına da katkı sunmaktadır. Bu yönüyle siber güvenlik, toplumsal kalkınma ve dijital egemenliğin sağlanması açısından stratejik bir öneme sahiptir.

2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı



**Avrupa Birliği tarafından
finanse edilmektedir**

Siber tehditlere karşı etkili mücadele ve caydırıcılık için geliştirilmiştir. Stratejide; güvenliğin tasarım aşamasından itibaren dikkate alınması, siber hijyenin yaygınlaştırılması, proaktif savunma, katmanlı altyapılar ve ileri teknolojilerin kullanımı öne çıkmaktadır. Kamu, özel sektör, akademi ve sivil toplum iş birliğiyle yürütülen çalışmalar sayesinde ulusal ve uluslararası düzeyde güçlü bir siber güvenlik sistemi hedeflenmekte; ayrıca Türkiye'nin bu alanda 7/24 etkin mücadele ile uluslararası liderliğinin pekiştirilmesi amaçlanmaktadır (Ulaştırma ve Altyapı Bakanlığı,2024).

“İnsan”, “Savunma”, “Caydırıcılık” ve “İş Birliği” temalarındaki unsurlardan yola çıkılarak hazırlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028), stratejik siber güvenlik yaklaşımının somut kazanımlara dönüştürülmesine yönelik bir yapıda planlanmıştır (Ulaştırma ve Altyapı Bakanlığı,2024:20);

- 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planının stratejik amaçları şunlardır:
 - a) Siber Dayanıklılık
 - b) Proaktif Siber Savunma ve Caydırıcılık
 - c) İnsan Odaklı Siber Güvenlik Yaklaşımı
 - d) Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı
 - e) Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler
 - f) Uluslararası Alanda Türkiye Markası



**Avrupa Birliği tarafından
finanse edilmektedir**

3.6 Avrupa Birliđi Politikaları

Dijital dönüşümün hız kazanmasıyla birlikte Avrupa Birliđi (AB), siber tehditlere karşı ortak bir mücadele zemini oluşturma gerekliliđi duymuştur. Üye devletlerin farklı dijital kapasiteleri ve güvenlik yaklaşımlarına rağmen AB, dijital tek pazar vizyonu doğrultusunda bütünleşik bir siber güvenlik politikası geliştirmeye odaklanmıştır. Bu kapsamda, AB'nin siber güvenlik politikaları, yalnızca teknik güvenlik önlemlerini değil, aynı zamanda hukuki düzenlemeleri, kurumsal yapılanmayı, uluslararası işbirliğini ve stratejik sertifikasyon mekanizmalarını da kapsayacak şekilde çok boyutlu bir yapıya sahiptir (European Commission, 2025).

3.6.1 AB Siber Güvenlik Stratejisi

- Avrupa Birliđi, dijital dönüşümle artan siber tehditlere karşı ortak bir mücadele ihtiyacı duymuştur. Farklı dijital kapasitelere sahip üye devletlere rağmen, dijital tek pazar vizyonu doğrultusunda bütünleşik bir siber güvenlik politikası geliştirmiştir. AB'nin politikaları yalnızca teknik önlemlerle sınırlı olmayıp; hukuki düzenlemeler, kurumsal yapı, uluslararası iş birliđi ve sertifikasyon mekanizmaları gibi çok boyutlu unsurları da kapsamaktadır.
- Yeni strateji, Avrupa'daki insanların güvenliđi ve temel hakları için risklerin olduđu yerlerde güçlü güvenlik önlemleriyle küresel ve açık bir İnternet sağlamayı amaçlıyor. Önceki stratejiler kapsamında elde edilen ilerlemeyi takiben, üç temel aracın konuşlandırılması için somut öneriler içeriyor. Bu üç araç düzenleyici, yatırım ve politika girişimleridir. Bunlar AB eyleminin üç alanını ele alacak (European Commission, 2025):



**Avrupa Birliđi tarafından
finanse edilmektedir**

- 1) Dayanıklılık, teknolojik egemenlik ve liderlik,
- 2) Önleme, caydırma ve yanıt verme konusunda operasyonel kapasite,
- 3) Küresel ve açık bir siber alanı ilerletmek için iş birliği

3.6.2 ENISA (Avrupa Birliği Siber Güvenlik Ajansı)

Avrupa'nın gelişmiş bir kaynak ve önleme kapasitesine sahip olmadığı sürece siber güvenlik olaylarına karşı korunmasız kalacağı ifade edilmektedir (Avrupa Komisyonu, akt. Eren,2017). Bu ifadeyi Kopenhag Ekolünün güvenlikleştirme yaklaşımı üzerinden okursak, strateji belgesinin burada tehdidinin yaşamsallığı ve ona karşı yeterli önlemlerin geliştirilmemesi durumunda geç olacağı (korunmasız kalınacağı) söylemini kullandığı, böylelikle meseleye hem aciliyet hem de öncelik affettiği söylenebilir. Bu yüzden komisyon ağ ve bilgi güvenliği (NIS) siyasetini geliştirmiştir. Bunu sağlamak için de 2004 yılında Avrupa Birliği Ağ ve Bilgi Güvenliği Kurumu (ENISA) kurulmuştur ve Avrupa Parlamentosu ve Avrupa Konseyi tarafından güncellenerek şimdiki halini almıştır (Eren,2017:77-78).

ENISA, AB'ni siber güvenliğinin sağlanması konusunda koordinasyonu sağlamak ve Avrupa genelinde üst düzey ağ ve bilgi güvenliğinin sağlanmasını amaçlamaktadır (ENISA 2015, akt. Eren,2017).

3.6.3 NIS ve NIS2 Direktifi

AB'nin siber güvenliğe yönelik ilk kapsamlı yasal düzenlemesi, 2016 yılında yürürlüğe giren NIS Direktifi (Network and Information Security Directive)'dir.



**Avrupa Birliği tarafından
finanse edilmektedir**

NIS, AB genelindeki siber güvenlik mevzuatının ilk parçasıdır. AB'nin kritik altyapısı genelinde standart bir ağ ve bilgi sistemi güvenliği düzeyine ulaşmayı amaçlamaktadır (IT Governance USA, 2025). Bu düzenleme ile sağlık, ulaşım, enerji ve bankacılık gibi kritik sektörlerde faaliyet gösteren firmalara siber güvenlik tedbirleri alma ve güvenlik olaylarını bildirme zorunluluğu getirilmiştir. Ancak NIS Direktifi'nin uygulamada bazı eksiklikleri olması nedeniyle, 2023 yılında NIS2 Direktifi yayımlanarak kapsam genişletilmiş, yaptırımlar güçlendirilmiş ve denetim mekanizmaları sıkılaştırılmıştır.

3.6.4 Avrupa Siber Güvenlik Yasası

Avrupa Birliği düzeyinde siber güvenlik konusu ele alındığında, bu alana yönelik bütünsel bir yaklaşımın bulunduğu ancak ortak bir tanım üzerinde uzlaşmaya varılamadığı görülmektedir. 7 Şubat 2013 tarihinde Avrupa Komisyonu tarafından yayımlanan ve Birlik içinde siber güvenlik politikalarının temelini oluşturması beklenen “Siber Güvenlik Strateji Belgesi”, net ve kapsamlı bir siber güvenlik tanımı sunmamaktadır. Bu eksiklik, 2017 yılında strateji belgesinin güncellenmiş versiyonunda da giderilmemiştir. Aynı şekilde, 11 Mart 2019’da Avrupa Parlamentosu tarafından kabul edilen ve 27 Haziran 2019’da yürürlüğe giren “Siber Güvenlik Yasası”nda da siber güvenliğe dair açık bir tanıma yer verilmemiştir. Bu durum, Avrupa Birliği'nin konuya stratejik yaklaşımı olmasına rağmen, kavramsal düzeyde ortak bir çerçevede buluşulamamış olduğunu ortaya koymaktadır. (Altın, 2023:6).



**Avrupa Birliği tarafından
finanse edilmektedir**

2019 yılında yürürlüğe giren Siber Güvenlik Yasası, Avrupa Birliği bünyesindeki siber güvenlik yapısını daha etkili ve kurumsal bir çerçeveye oturtmak amacıyla hazırlanmıştır. Bu yasal düzenleme ile birlikte ENISA'nın görev alanı genişletilmiş; özellikle siber tehdit ve saldırılara karşı üye devletlere destek sağlama konusunda yetkileri güçlendirilmiştir. Ajansın, bilimsel ve teknik açıdan nitelikli öneriler sunabilen, bağımsız ve uzmanlaşmış bir yapı hâline gelmesi hedeflenmiştir. Ayrıca, ENISA'nın yalnızca politika geliştirme sürecinde değil, aynı zamanda uygulama aşamasında da aktif bir danışmanlık rolü üstlenmesi amaçlanmıştır. Yasa, üye ülkelerin sınır aşan siber olaylara karşı daha hızlı ve etkili biçimde müdahale edebilmesi için Birliğin genel siber güvenlik kapasitesinin artırılmasını da öncelikli hedeflerden biri olarak belirlemiştir.

3.7 Siber Dayanıklılık Yasası

Siber Dayanıklılık Yasası 20 Kasım 2024 tarihli Avrupa Birliği (AB) Resmî Gazetesi'nde yayımlanarak 10 Aralık 2024 tarihi itibarıyla yürürlüğe girmiştir. Yasanın temel amacı, dijital ürünlerin piyasaya sürülmeden önce güvenlik testlerine tabi tutulmasını ve tüm yaşam döngüleri boyunca siber tehditlere karşı korunmalarını öngörmektedir. Bu yasa ile dijital cihaz üreticileri, yazılım geliştiriciler ve dağıtımıcılar ciddi yükümlülükler altına alınmakta ve “güvenlik tasarımı başlar” ilkesi benimsenmektedir.

Siber Dayanıklılık Yasası (CRA), dijital bileşenli yazılım veya donanım ürünleri satın alan tüketicileri ve işletmeleri korumayı amaçlamaktadır. Siber Dayanıklılık Yasası, birçok ürünlerdeki yetersiz siber güvenlik seviyesini ve ürünler ve yazılımlar



**Avrupa Birliği tarafından
finanse edilmektedir**

için zamanında güvenlik güncellemelerinin eksikliğini ele almaktadır. Ayrıca, tüketicilerin ve işletmelerin hangi ürünlerin siber güvenli olduğunu belirlemeye ve bunları güvenli bir şekilde kurmaya çalışırken şu anda karşılaştıkları zorlukları da ele almaktadır. Yeni gereksinimler, dijital öğeler içeren ürünleri seçerken ve kullanırken siber güvenliği hesaba katmayı kolaylaştıracaktır. Uygun siber güvenlik özelliklerine sahip donanım ve yazılım ürünlerini belirlemek daha basit olacaktır (European Commission, 2025). Bu yasada dikkat çeken bir diğer önemli madde, ürünlerin Avrupa pazarında satılabilmesi için CE işareti taşıma zorunluluğudur. Bu işaret, ilgili ürünün belirlenen siber güvenlik standartlarına uygun olduğunu göstermektedir.

3.8 CE Nedir ?

"CE" İşareti, ürünün ilgili teknik düzenlemesine uygun olduğunu ve ürünlerin amacına uygun kullanılması halinde insan can ve mal güvenliği, bitki ve hayvan varlığı ile çevreye zarar vermeyeceğini gösteren bir işarettir (T.C. Ticaret Bakanlığı, 2025).



**Avrupa Birliği tarafından
finanse edilmektedir**

4.Siber Zorbalığın Toplumsal Etkileri

Madde bağımlılığı konusunun ele alınmasında, bireyleri bu tür maddelerden uzak tutabilmek amacıyla, söz konusu maddelerin kişiler üzerindeki olumsuz etkilerinin de detaylı şekilde incelenmesi önemlidir. Benzer biçimde, siber zorbalık kavramının ne olduğu ve bu olguya karşı nasıl korunulabileceğinin öğrenilmesi kadar, siber zorbalığın toplum üzerindeki etkilerinin anlaşılması da büyük önem taşımaktadır. Özellikle gençler arasında siber zorbalık vakalarının artış göstermesiyle birlikte, dünya genelinde birçok kişi ve kurum siber zorbalığın toplumsal etkileri üzerine bilimsel araştırmalar yürütmeye başlamıştır. Bu bölümde, söz konusu araştırmalar ve elde edilen bulgular ayrıntılı olarak ele alınacaktır.

4.1 Eskilerden Bir Araştırma

Siber zorbalık üzerine yapılan araştırmalar günümüzde artış göstermekle birlikte, bu alandaki ilk çalışmaların geçmiş yıllar öncesine dayandığı görülmektedir. Örneğin, 2014 yılında Pennsylvania State Üniversitesi Behrend Koleji Klinik Psikoloji Bölümünde öğretim üyeliği yapan araştırmacı Prof. Dr. Charisse L. Nixon tarafından gerçekleştirilen bir araştırmada, Amerika Birleşik Devletleri'ndeki gençlerin %95'inin internete bağlı olduğu tespit edilmiştir.

Bu çalışmada elde edilen bulgulara göre, siber zorbalığa maruz kalan gençlerin depresyona daha yatkın oldukları ve bu gençlerin %93'ünün üzüntü, umutsuzluk ve güçsüzlük duyguları yaşadıkları rapor edilmiştir. Ayrıca, utanç, kırılma ve kendini suçlama gibi olumsuz duyguların arttığı, siber zorbalık mağdurlarının kendilerini yalnız ve yardım alamayacak durumda hissettikleri ifade edilmiştir.

Bu tür duygusal etkiler sonucunda bireylerin ailelerinden ve arkadaşlarından uzaklaşarak içe kapanma eğilimi gösterdikleri belirtilmiştir. Söz konusu çalışmada, özellikle siber zorbalık ile intihar arasındaki ilişkiye dikkat çekilmiştir. Ortaokul, lise ve üniversite öğrencileri üzerinde yürütülen araştırmalarda, siber zorbalıkla



**Avrupa Birliği tarafından
finanse edilmektedir**

ilişkilendirilen öğrencilerin, yaşlılarına kıyasla intihara daha fazla eğilimli oldukları tespit edilmiştir. Burada, “ilişkilendirilen” ifadesinin hem siber zorbalık mağdurlarını hem de zorbalık yapanları kapsadığı vurgulanmaktadır. Araştırma bulgularına göre, siber zorbalık yapan bireylerin intihar girişiminde bulunma oranı kendi yaşlılarına göre 1,5 kat daha yüksekken; siber zorbalık mağdurlarında bu oran 1,9 kat (neredeyse iki kat) daha fazladır.[\[1\]](#)

4.2 Amerika’da Güncel Durum

31 Mayıs 2025 tarihinde The Washington Post’ta yayınlanan bir makale, siber zorbalığın günümüzdeki durumu hakkında önemli bulgular sunmaktadır. Söz konusu makalede aktarılan araştırma, ülke çapında temsili bir örneklem oluşturan 13-17 yaş arası çocuklar üzerinde yürütülmüştür. Araştırma sonuçlarına göre, bu yaş grubundaki bireylerin %53.9’u daha önce siber zorbalığa maruz kaldıklarını belirtmiştir. Elde edilen verilere dayanarak, günümüzde 13-17 yaş arası çocukların yarısından fazlasının siber zorbalık deneyimi yaşadığı ifade edilebilmektedir.

Araştırmada, siber zorbalık olarak tanımlanan davranışların niteliği de katılımcılardan açıklamaları istenerek detaylandırılmıştır. Çocuklar, kendileri hakkında yayılan asılsız bilgiler ve söylentilerin yanı sıra, kasıtlı olarak bazı arkadaş gruplarından dışlanma durumlarını siber zorbalık kapsamında değerlendirmişlerdir. Bulgulara göre, kız çocuklarının erkek çocuklara kıyasla daha fazla travmatik deneyim yaşadıkları; ayrıca, daha küçük yaştaki çocukların, yaşı büyük çocuklara göre siber zorbalık karşısında daha yoğun travma belirtileri gösterdikleri tespit edilmiştir.[\[2\]](#)

Araştırma bulgularına göre, siber zorbalığa maruz kalan çocuklarda travma sonrası stres bozukluğunun (TSSB) tetiklenebildiği uzmanlar tarafından gözlemlenmiştir. Ayrıca, siber zorbalığın “Olumsuz Çocukluk Deneyimleri” (OÇD) kategorisinde değerlendirilmesi önerilmiştir. Olumsuz Çocukluk Deneyimleri, bireylerin ilerleyen yaşamlarında ruhsal sağlık sorunlarıyla karşılaşma riskini artıran çeşitli çocukluk dönemi deneyimlerini kapsayan bir sınıflandırmadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

“Olumsuz Çocukluk Deneyimleri” kapsamında değerlendirilen başlıca durumlar arasında aile içi şiddet ve/veya istismar, aile bireylerinden birinin intihar etmesi ya da intihar girişiminde bulunması ve aile üyelerinden birinin uyuşturucu madde bağımlısı olması yer almaktadır. Yaklaşık üç ay önce gerçekleştirilen bir araştırmanın sonuçlarına göre, uzmanlar siber zorbalığın da bu tür travmatik deneyimler arasında sınıflandırılması gerektiğini savunmaktadır.[3]

4.3 Farklı Bir Ülkeden Benzer Sonuçlar

Siber zorbalıkla ilgili araştırmalar yalnızca Amerika Birleşik Devletleri’nde değil, dünya genelinde de gerçekleştirilmektedir. 14 Ocak 2023 tarihinde Suudi Arabistan Jazan Üniversitesi Tıp Fakültesi Pediatri Anabilim Dalı’nda görev yapan Yardımcı Doçent Gassem Gohal ve çalışma ekibi tarafından yürütülen bir araştırmada, 12-18 yaş aralığındaki 355 öğrenciye çeşitli sorular yöneltilmiştir.

Araştırma sonuçlarına göre, katılımcıların yaklaşık %20’si günlük 12 saatten fazla süreyle internet kullandıklarını ifade etmiştir. Siber zorbalığa maruz kalanların oranı ise %42.8 olarak tespit edilmiştir. Benzer yaş grubunda Amerika Birleşik Devletleri’nde yapılan araştırmada bu oran %53.9 olarak belirlenmiştir. Amerika’daki araştırmanın, Suudi Arabistan’daki çalışmadan iki yıl sonra gerçekleştirilmiş olması, Suudi Arabistan’daki siber zorbalık oranının da zaman içinde artış göstermesinin muhtemel olduğunu göstermektedir.

Siber zorbalığa maruz kalan katılımcıların %26.3’ü, bu durumun akademik başarılarında düşüşe neden olduğunu ifade etmiştir. Katılımcıların %20’si okulu bırakmayı düşündüklerini belirtirken, %21.1’i ise siber zorbalık nedeniyle kendilerine zarar verme düşüncesine sahip olduklarını bildirmiştir. Bölümün başında ele alınan, Charisse L. Nixon’ın 11 yıl önce gerçekleştirdiği araştırmada da siber zorbalığın intihar teşebbüslerini artırabileceği ihtimaline dikkat çekilmişti. Suudi Arabistan’da yapılan güncel araştırmada elde edilen bulguların, bu ihtimali desteklediği görülmektedir.[4]



**Avrupa Birliği tarafından
finanse edilmektedir**

4.4 Yereldeki Genel Durum

Siber zorbalıkla ilgili araştırmalar, yurtdışında olduğu kadar ülkemizde de giderek önem kazanmaktadır. Queen's University Belfast'ta görev yapan Kıdemli Öğretim Üyesi Dr. Gizem Melek ve Yaşar Üniversitesi İletişim Fakültesi'nden Doçent Dr. Dilek Melike Uluçay, 2017 yılında bu konuya ilişkin kapsamlı bir makale yayımlamışlardır. Söz konusu makalede, Türkiye'deki okullarda gerçekleştirilen çeşitli siber zorbalık araştırmaları derlenmiş ve böylelikle sonraki yıllarda bu alanda çalışma yapmak isteyen araştırmacılar için önemli bir kaynak ve ilham kaynağı oluşturulmuştur.

Makalede ele alınan çalışmalardan biri, Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi'nde görev yapan Öğretim Üyesi Adem Peker tarafından 2013 yılında gerçekleştirilmiştir. Bu çalışmada, ülkemizdeki ortaokul öğrencilerinin %65'inin siber zorbalığa maruz kaldığı tespit edilmiştir. Charisse L. Nixon'ın Amerika Birleşik Devletleri'nde yürüttüğü araştırmadan bir yıl önce gerçekleştirilen bu çalışma, Türkiye'deki siber zorbalık oranının yarıdan fazla ve oldukça yüksek seviyede olduğunu göstermektedir.

Adem Peker ve çalışma arkadaşlarının 2015 yılında gerçekleştirdiği araştırmada, siber zorbalığa maruz kalan çocukların öfke problemleri yaşadıkları ve ciddi şekilde üzüntü duydukları tespit edilmiştir. Söz konusu makalede derlenen diğer araştırmalarda da, Charisse L. Nixon'ın çalışmasında olduğu gibi, siber zorbalık mağdurlarının depresyona sürüklendiği ve bu sorunlarla çoğunlukla tek başlarına başa çıkmaya çalıştıkları belirtilmiştir. Ayrıca, Gasseem Gohal'in araştırmasında olduğu gibi, siber zorbalığın mağdurların akademik başarılarını olumsuz etkilediği; üst düzey vakalarda ise, Nixon'ın da vurguladığı gibi, mağdurların intihar eğilimi gösterebildiği ortaya konmuştur.[\[5\]](#)

4.5 Nişantaşı Üniversitesinden Güncel Bir Araştırma

İstanbul Nişantaşı Üniversitesi Yeni Medya ve İletişim Bölümü'nden Dr. Öğr. Üyesi Hakan Tan ile Halkla İlişkiler ve Reklamcılık Bölümü'nden Dr. Öğr. Üyesi



**Avrupa Birliği tarafından
finanse edilmektedir**

Yelda Şenkal tarafından Aralık 2024'te gerçekleştirilen bir araştırmada, 362 üniversite öğrencisi ile görüşülmüştür. Araştırma bulgularına göre, katılımcıların %66.9'u (242 öğrenci) çevrelerinde siber zorbalığa maruz kalan bir bireyin olduğunu belirtirken, %32.9'u (119 öğrenci) ise doğrudan kendisinin siber zorbalığa maruz kaldığını ifade etmiştir.

Araştırma bulgularına göre, siber zorbalığın etkileri arasında anksiyete ve depresyon, akademik performansta düşüş, çevresindeki olaylara ve kişilere olan ilginin azalması, konsantrasyon bozukluğu gibi çeşitli psikolojik ve davranışsal sorunlar yer almaktadır. Alanda yapılan ve bu bölümde ele alınan diğer araştırmalarla karşılaştırıldığında, benzer sonuçların elde edildiği gözlemlenmiştir.[\[6\]](#)

İncelediğimiz makalelere dayanarak, Siber Zorbalığa maruz kalanlarda görülen etkilere dair şöyle bir liste hazırlanabilmektedir:

Anksiyete ve Depresyon: Siber zorbalık mağdurlarında yoğun kaygı, umutsuzluk ve depresyon belirtileri sıklıkla gözlemlenmektedir.

Travma Sonrası Stres Bozukluğu (TSSB): Bazı vakalarda travma sonrası stres bozukluğu gelişebilmektedir.

Öfke Problemleri ve Duygusal İstikrarsızlık: Mağdurlar, öfke kontrolünde güçlükler ve duygusal dalgalanmalar yaşayabilmektedir.

Akademik Başarıda Düşüş: Okul başarısında belirgin bir azalma, derslere ilgi kaybı ve konsantrasyon bozukluğu rapor edilmektedir.

Sosyal İzolasyon ve Yalnızlık: Mağdurlar, ailelerinden ve arkadaşlarından uzaklaşma eğilimi göstermekte ve kendilerini yalnız hissetmektedir.

Kendine Zarar Verme ve İntihar Eğilimi: Özellikle şiddetli vakalarda, kendine zarar verme düşüncesi ve intihar eğilimi ortaya çıkabilmektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Utanç, Kırılma ve Kendini Suçlama: Mağdurlar sıkça utanç, kendini suçlama ve özgüven kaybı gibi duygular yaşamaktadır.

Çevresine İlgil Azalması: Çevresindeki olaylara ve kişilere karşı ilgi kaybı gözlemlenmektedir.

Olumsuz Çocukluk Deneyimleri: Siber zorbalık, ilerleyen yıllarda ruhsal sağlık sorunlarına yol açabilecek olumsuz çocukluk deneyimleri arasında değerlendirilmektedir.

Listeden de anlaşılacağı üzere, siber zorbalık vakalarının toplum üzerinde ciddi ve kalıcı etkileri bulunmaktadır. Özellikle çocuklar ve gençler üzerinde, stres ve akademik performansta düşüşle başlayıp depresyon ve intihar eğilimine kadar ilerleyebilen kalıcı psikolojik hasarlara yol açabilmektedir. Bu nedenle, siber zorbalıkla mücadelede en etkili yöntemlerden biri, bireylerin hem kendilerini hem de çevrelerindeki bu konuda bilgilendirmeleri ve farkındalık geliştirmeleridir. Ayrıca, siber zorbalığa maruz kalma şüphesi bulunan kişilere destek olmak ve onların yanında yer almak, bu süreçte önemli bir koruyucu faktör olarak öne çıkmaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

5.Siber Zorbalıkla Mücadelede Politika Önerileri

Siber zorbalık günümüzde birçok ülkede var olan ve toplumdaki tüm yaş gruplarını ilgilendiren şiddet içerikli davranışları olarak tanımlanabilir. Bu türdeki zorbalığın bireyler üzerinde çeşitli fiziksel ve psikolojik rahatsızlıklara yol açtığı yapılan araştırmalarda gözlemlenmektedir. Bu sebeple, toplumsal yaşam içerisinde var olan bu sorun ile başa çıkmaya yönelik çeşitli adımların atılması gerekmektedir.

Siber zorbalar, eylemlerini genellikle internet ortamında çeşitli yöntemlerle gerçekleştirmektedirler. Bu yöntemler arasında, bir kişiyi bilerek bir gruptan dışlamak, sosyal medya ve elektronik posta hesaplarını ele geçirmek, başkalarına ait elektronik hesaplar üzerinden uygunsuz iletiler göndermek, cep telefonu aracılığıyla rahatsız edici davranışlarda bulunmak, bir kişiye ait fotoğraf veya özel bilgileri izinsiz olarak paylaşmak gibi uygulamalar bulunmaktadır.

Siber zorbalıkla etkin bir şekilde mücadele edilebilmesi için öncelikle ailelerin bilinçlendirilmesi ve çocuklar üzerinde sağlıklı bir kontrol mekanizmasının kurulması gerekmektedir. Özellikle “öfke kontrolü” konusunda ailelerin çocuklarına rehberlik etmesi önem taşımaktadır. Elde edilen veriler, ailelerin eğitim düzeyinin çocukların siber zorbalığa ilişkin tutumlarını anlamada belirleyici bir faktör olduğunu göstermektedir. Ayrıca bulgular, siber zorbalık failleri ve mağdurları arasında cinsiyet farkının dikkat çekici olduğunu; erkeklerin kadınlara kıyasla hem siber zorbalık yapma hem de maruz kalma oranlarının daha yüksek olduğunu ortaya koymaktadır.



**Avrupa Birliği tarafından
finanse edilmektedir**

Tablo 14: Annenin Eğitim Durumuna Göre Siber Zorbalık ve Siber Mağduriyet Puanları Farkı için Yapılan Tek Yönlü Varyans Analizi

		KT	sd	KO	F	P
Siber Zorbalık Puanı	Gruplar Arası	208,264	5	41,653	4,231	,001
	Gruplariçi	42160,806	4283	9,844		
	Toplam	42369,070	4288			
Siber Mağdur Puanı	Gruplar Arası	84,406	5	16,881	1,442	,206
	Gruplariçi	50170,288	4285	11,708		
	Toplam	50254,694	4290			

- ✓ Tabloda görüldüğü üzere, öğrencilerin annelerinin eğitim durumuna göre siber zorbalık puanları arasında istatistiksel olarak anlamlı bir fark bulunurken, siber mağduriyet puanları arasında anlamlı bir fark tespit edilmemiştir [sırasıyla, $F(5, 4283)=4.231$, $p=.001$; $F(5, 4285)=1.442$, $p=.206$]. Gruplar arasındaki farkın hangi eğitim düzeylerinden kaynaklandığını belirlemek amacıyla Scheffe çoklu karşılaştırma testi uygulanmıştır.

	Cinsiyet	N	$\bar{X}$	SS	SH
Siber Zorbalık Puanı	Kız	2225	17,5591	2,08244	,04415
	Erkek	2064	18,1206	3,96219	,08721
Siber Mağdur Puanı	Kız	2226	24,3756	3,28264	,06958
	Erkek	2065	24,6416	3,56303	,07841

- ✓ Cinsiyete göre yapılan analizler sonucunda, hem siber zorbalık puanları hem de siber mağduriyet puanları açısından kızlar ve erkekler arasında, her iki testte de kızlar lehine istatistiksel olarak anlamlı bir fark bulunmuştur [sırasıyla, $t(4287) = -5.868$, $p = .000$; $t(4289) = -2.546$, $p = .011$]. Bulgular, kızların erkeklere kıyasla hem daha az siber zorbalık yaptıklarını hem de daha az siber mağduriyet yaşadıklarını göstermektedir.



**Avrupa Birliği tarafından
finanse edilmektedir**

Tablo 15: Annenin Eğitim Durumuna Göre Siber Zorbalık ve Siber Mağduriyet Puanları Ortalaması, Standart Sapması ve Standart Hatası

		N	$\bar{X}$	SS	SH
Siber Zorbalık Puanı	Okur-Yazar	493	17,8966	3,28080	,14776
	Değil				
	Okur-Yazar	589	17,9898	4,07622	,16796
	İlköğretim	1853	17,6158	2,17491	,05052
	Lise	900	18,0000	3,72288	,12410
	Üniversite	288	17,8264	2,93443	,17291
	Master/Doktora	166	18,5241	4,54166	,35250
	Toplam	4289	17,8293	3,14338	,04800
Siber Mağdur Puanı	Okur-Yazar	493	24,3753	3,32934	,14995
	Değil				
	Okur-Yazar	589	24,2326	3,03358	,12500
	İlköğretim	1855	24,5315	3,76679	,08746
	Lise	900	24,5756	2,99050	,09968
	Üniversite	288	24,6875	3,22656	,19013
	Master/Doktora	166	24,8253	3,45704	,26832
	Toplam	4291	24,5036	3,42263	,05225

- ✓ Tabloda görüldüğü üzere, annesi yüksek lisans veya doktora düzeyinde eğitilmiş olan çocuklar, annesi yalnızca ilköğretim mezunu olan çocuklara kıyasla anlamlı derecede daha fazla siber zorbalık davranışında bulunmaktadır.

5.1 Empati

Siber zorbalığın önlenmesinde en önemli unsurlardan biri empati gelişimidir. Bir bireyin karşısındaki kişiye zarar verme olasılığını azaltmak, empati becerilerinin artırılması ile mümkündür. Bu nedenle, bireylerin empati yönünü geliştirmeye yönelik yöntemlerin uygulanması, siber zorbalıkla mücadelede temel bir yaklaşım olarak değerlendirilmektedir. ;

- Durum Çalışmaları (bakanlık veya devlet tarafından)
- Gazete Makaleleri
- Siber Mağdurların Durumunu Yansıtan Kamu Spotları
- Siber Zorba Mağdurlarıyla İlgili film/video çekilip devlet kanallarında gösterilmesi
- Devlet Tiyatrolarında aktörlerin Siber Zorbalıkla ilgili oyun canlandırması
- Kendini koruma, Empati gibi kazanımlar sağlayacak dersler konulması



**Avrupa Birliği tarafından
finanse edilmektedir**

- Media Heroes Projesi gibi projeler çoğaltılmalıdır

Empati eğitiminin geliştirilmesi amacıyla Avrupa’da yürütülen “Media Heroes Projesi” örnek olarak ele alınabilir. Bu proje kapsamında, 722 lise öğrencisine empati kurma yeteneğini artırmaya yönelik, çevrimiçi ortamda kendini koruma ve sosyal becerilerin geliştirilmesi konularında yardımcı olmayı amaçlayan 15 seanslık bir ders programı uygulanmıştır. Program, ön test ve son test aşamalarını da içerecek şekilde yapılandırılmıştır.

5.2 Öfke Kontrolü

Zorba davranışların temelinde çoğunlukla bireye duyulan öfke yatmaktadır. Bu nedenle, bireylere öfke kontrolü becerisi kazandırılması, siber zorbalık vakalarının azalmasına önemli ölçüde katkı sağlayacaktır. Bireylerin öfke kontrolünü yönetebilmesi için aşağıdaki yöntemlerin geliştirilmesi önerilmektedir;

- Okul müfredatlarına öfke yönetimi ve duygusal zeka derslerinin eklenmesi
- Bireylerin sosyal medya sorumluluklarını kazanabilmesi adına dijital vatandaşlık eğitimi verilmesi
- Psikolog ve psikiyatrilere aracılığıyla öfke kontrolü atölye çalışmalarının yapılması

5.3 Değerler Eğitimi

Siber zorbalığın önlenmesine yönelik çeşitli araştırmacılar tarafından önerilen stratejilerden biri değerler eğitimidir. Bu yaklaşım kapsamında sorumluluk, barışçıl olma, hoşgörü olma ve saygı gibi temel insani değerlerin farkındalığını kazandırmaya odaklanılmaktadır. Bireylerde bu değerlerin geliştirilmesi, siber zorbalık davranışlarının önlenmesinde önemli bir rol oynamaktadır.

- Siber zorbalık mağduru bireylere yönelik insani değerlerin kazandırılmasını hedefleyen psiko-eğitim programlarının düzenlenmesi önemlidir.
- Gençlerin sorumluluk duygusu, hoşgörü ve benzeri değerleri geliştirmelerine yönelik atölye çalışmaları yapılmalıdır.



**Avrupa Birliği tarafından
finanse edilmektedir**

- Ayrıca, bu kapsamda belirtilen konuları içeren Erasmus+ gönüllülük projelerinin düzenlenmesi ve teşvik edilmesi, uluslararası deneyim ve farkındalığın artırılmasına katkı sağlayacaktır.
- Her bireyin siber güvenlik farkındalığı kazanması için temel düzeyde bilgi edinmesi ve dijital ortamda sorumluluk sahibi olması hedeflenmeli; bu doğrultuda uygun metot ve eğitim programları geliştirilmelidir.

5.4 Siber Zorbalık Müdahale Programları

Akranlar arasında şiddet içermeyen ilişkilerin geliştirilmesi ve olumlu bir sınıf ortamının oluşturulması, siber zorbalıkla mücadelede etkili yöntemler arasında yer almaktadır. Ulusal düzeyde bu tür stratejilerin uygulanması, öğrencilerin sosyal becerilerini geliştirmeye, empati kurma yeteneklerini artırmaya ve güvenli bir eğitim ortamı sağlamaya katkı sunacaktır. Bu amaçla, okullarda şiddetsiz iletişim, grup çalışmaları ve pozitif davranış kazandırmaya yönelik faaliyetler yaygınlaştırılabilir.

Siber zorbalıkla mücadelede, belediyeler ve sivil toplum kuruluşlarının (STK) gençlik merkezleriyle iş birliği içinde çalışması önem taşımaktadır. Ayrıca, Milli Eğitim Bakanlığı, adalet sistemi ve sosyal medya platformları arasında etkin bir iş birliği kurulmalıdır. Siber mağdurların zorbalık vakalarını güvenli ve anonim bir şekilde bildirebilecekleri bir programın geliştirilmesi gerekmektedir. Bu tür bildirimlerde, okullarda veya gençlik merkezlerinde görev yapan uzmanların sürece dahil edilmesi sağlanabilir. Siber güvenlik konusunda farkındalık kampanyalarının düzenlenmesi, mesleki eğitim programlarının hazırlanması ve uluslararası forumlara katılımın teşvik edilmesi büyük önem taşımaktadır. Ayrıca, siber güvenlik alanında kamu ve özel sektör işbirliğinin geliştirilmesi gerekmektedir.

5.5 Medya Kullanımı Eğitimi

Bilindiği üzere, siber zorbalık; internet ve cep telefonu aracılığıyla, resim, video ve ses gibi medya türlerinin kötü amaçlarla kullanılması yoluyla gerçekleştirilen bir eylemdir. Bu nedenle, medya kullanımına ilişkin eğitimlerin siber zorbalığı



**Avrupa Birliği tarafından
finanse edilmektedir**

önlemede etkili olabileceği düşünülmektedir. Özellikle öğrencilere, medyayı doğru ve güvenli bir şekilde nasıl kullanabilecekleri, medyanın kötü amaçlarla kullanılması halinde karşılaşılabilecek olumsuz sonuçlar hakkında bilgilendirme ve eğitim verilmesi önem taşımaktadır. Ayrıca, okullarda internetin ve yasal kullanmanın önemiyle ilgili konferanslar düzenlenmeli; telefonların ekran süresi kısıtlamalarının uygulanması ve bu alışkanlığın kazandırılması teşvik edilmelidir.

5.6 Aile İçi Müdahaleler

Bireyin eğitimi aile ortamında başlar; bu nedenle siber zorbalıkla mücadelede en temel ve en önemli unsur ailedir. Araştırmalar, bireylerin aile içi ilişkilerinin siber zorbalık üzerinde etkili olabileceğini göstermektedir. Dolayısıyla, siber zorbalığı önleme konusunda aile içi bazı müdahalelerin gerekliliğinden söz edilebilir. Bu kapsamda yapılabilecekler şunlardır:

- Milli Eğitim Bakanlığı ve ilgili kurumlar tarafından, ebeveynlerin çocuklarıyla olan duygusal etkileşimlerini güçlendirmeye yönelik eğitim programları düzenlenmesi,
- Ailelere aktif müdahale ile sınırlayıcı müdahale arasındaki farkın anlatılması, kazanımların vurgulanması ve ailelerin aktif müdahaleye yönlendirilmesi için içerikler üretilmesi (aktif müdahalenin, sınırlayıcı müdahaleye kıyasla siber zorbalıkla mücadelede daha etkili olduğu belirtilmiştir. Bu bağlamda, ailelerin çocuklarıyla riskli internet kullanımının sonuçları ve korunma yolları hakkında tartışmalar yürütmeleri önerilmektedir,
- Çocukların internet kullanımını ebeveynler tarafından takip edebilmesine imkân tanıyan uygulamaların geliştirilmesi.

5.7 Devletlerin Yaptırımları

Siber zorbalığın önlenmesinde en etkili ve caydırıcı unsurlardan biri hukuk sistemidir. Devletin yalnızca cezalandırıcı değil, aynı zamanda düzeltici ve önleyici



**Avrupa Birliği tarafından
finanse edilmektedir**

bir yaklaşım benimsemesi gerekmektedir. Ulusal düzeyde devletler tarafından alınabilecek başlıca önlemler şunlardır

- **Yasal Düzenlemeler:** Siber zorbalık vakalarını açıkça tanımlayan ve cezai yaptırımları içeren özel yasaların hazırlanması ve uygulanması.
- **Erişilebilir Bildirim Mekanizmaları:** Mağdurların siber zorbalık vakalarını kolaylıkla ve güvenli bir şekilde bildirebileceği anonim ve erişilebilir platformların oluşturulması.
- **Önleyici ve Eğitimsel Programlar:** Okullarda ve toplumda, siber zorbalık ve dijital güvenlik konusunda farkındalık artırıcı ve eğitici programların yaygınlaştırılması.
- **Düzeltilici Adımlar:** Mağdurlara psikolojik ve sosyal destek sağlanması; zorba davranışlarda bulunanlara yönelik rehabilitasyon ve davranış değiştirme programlarının geliştirilmesi.
- **Kolluk Birimlerinin Eğitimi:** Polis ve ilgili kolluk kuvvetlerinin siber suçlar konusunda uzmanlaşması ve etkin müdahale edebilmesi için eğitim verilmesi.
- **Sosyal Medya Platformlarıyla İş Birliği:** Sosyal medya ve dijital platformlarla iş birliği yapılarak, siber zorbalık içeriklerinin hızlıca tespit edilmesi ve kaldırılması için ortak prosedürlerin geliştirilmesi.
- **Veri Koruma ve Gizlilik:** Mağdurların kişisel bilgilerinin korunmasına yönelik yasal ve teknik önlemlerin alınması.
- **Uluslararası İş Birliği:** Sınır ötesi siber zorbalık vakalarında diğer ülkelerle iş birliği yapılması ve uluslararası standartların takip edilmesi.

5.8 Avrupa Genelinde Politik Olarak Siber Zorbalık Olayları

⇒ Slovakya’da 2023 seçimlerinden hemen önce, “medya sessizliği” döneminde yayılan yapay zekâ ile üretilmiş bir derin ses (deepfake audio) kaydı, muhalefet lideri Michal Šimečka ile bir gazetecinin sandık manipülasyonu planladığı



**Avrupa Birliği tarafından
finanse edilmektedir**

izlenimini oluřturmuřtur. Kayıt, hızla doęrulanamadığı için kamuoyu üzerinde etkili olmuř ve Avrupa’da seçim sürecine etki eden ilk büyük derin ses vakalarından biri olarak kayda gemiřtir.

- ⇒ Finlandiya’da 2019–2021 döneminde, hükümet üyelerine ve özellikle kadın bakanlara yönelik eřgüdümlü çevrimii taciz ve cinsiyeti saldırılar ayrıntılı biçimde belgelenmiřtir. NATO StratCom COE tarafından hazırlanan rapor, bu saldırıların örgütlü ve kalıcı bir kampanya nitelięi tařıdığını ortaya koymuřtur. Akademik literatürde ise, dönemin bařbakanı Sanna Marin’e yönelik çevrimii kadın düşmanlığını inceleyen çeřitli alıřmalar yayımlanmıřtır.
- ⇒ Birleşik Krallık’ta 2024–2025 döneminde, kadın milletvekillerinin çevrimii nefret, tehdit ve tacize maruz kalma oranlarının arttığı tespit edilmiřtir. Bu durum, düzenleyici kurum Ofcom’un nitel arařtırmaları ile Avam Kamarası’nın güvenlik raporlarında gündeme getirilmiřtir. Ayrıca, medya haberlerinde seçim adaylarının karřılařtığı dijital istismar ve dezenformasyon vakalarına da dikkat çekilmiřtir.
- ⇒ Baltık ülkeleri olan Litvanya, Letonya ve Estonya, yıllardır özellikle Rusya baęlantılı aęlar tarafından yürütölen trol fabrikaları, dezenformasyon ve çevrimii taciz kampanyaları ile karřı karřıya kalmaktadır. Bu saldırıların hem hükümet kurumlarını hem de kamuoyunu hedef aldığı görölmektedir. Bölgeye özgü olarak, sivil diren ve medya okuryazarlığı programları geliştirilmiř ve uygulanmaktadır.
- ⇒ Avrupa Birlięi Dıř Eylem Servisi’nin 2025 tehdit raporunda, seçimlerin organize bilgi saldırılarının öncelikli hedefi olduęu belirtilmiřtir. Raporda, özellikle Rusya kaynaklı aęların siyasi kurumları ve seçmenleri hedef alan kampanyalarının belgelerle ortaya konduęu ifade edilmektedir. EDMO’nun 2024 Avrupa Parlamentosu seçimleri için hazırladığı ön risk deęerlendirmesi ise, ülke bazında özgül anlatılar üzerinden yürütölen koordineli kampanyalara dikkat çekmektedir.



**Avrupa Birlięi tarafından
finanse edilmektedir**

6. Kadınlar İçin Dijital Güvenlik

Dijitalleşme, günümüz yaşamının ayrılmaz bir parçası haline gelmiştir; ancak bu durum, özellikle kadınlar açısından çeşitli riskleri de beraberinde getirmektedir. Literatürde, kadınların çevrim içi taciz, dijital şiddet, kimlik avı, izinsiz görsel paylaşımı ve hesap ele geçirme gibi tehditlerle erkeklere kıyasla daha sık karşılaştığı belirtilmektedir (UN Women, 2023; Yılmaz & Demir, 2024). Bu tehditler yalnızca bireysel düzeyde psikolojik baskı ve utanç yaratmakla kalmayıp, aynı zamanda sosyal izolasyon ve fiziksel güvenlik kaygılarına da yol açabilmektedir.

6.1 Dijital Şiddet ve Türkiye’de Durum

Dünya genelinde kadınların yaklaşık %73’ü internet üzerinden tacize uğradığını bildirmektedir ve çevrimiçi vakit geçiren kadınların %85’i dijital şiddete tanık olmaktadır (UN Women, 2023). Türkiye özelinde ise her beş kişiden biri dijital şiddete maruz kalmakta; kadınların %51’i yazılı, sesli veya görüntülü taciz mesajları almakta, %46’sı ise ısrarlı takip ile karşı karşıya kalmaktadır (Ekmek ve Gül, 2022). Bu şiddet eylemleri çoğunlukla Instagram (%53), Facebook (%35) ve Twitter (%19) üzerinden gerçekleşmekte olup, failer genellikle tanımadıkları kişiler, troller veya eski partnerler, akrabalar ve arkadaşlar olmaktadır (Ekmek ve Gül, 2022). Dijital şiddetin türleri arasında taciz mesajları, hakaret veya tehdit içerikli yorumlar, özel içeriklerin rızasız paylaşılması, şantaj ve hesaplara izinsiz erişim gibi eylemler öne çıkmaktadır (UN Women, 2023; Yılmaz & Demir, 2024).



**Avrupa Birliği tarafından
finanse edilmektedir**

6.2 Avrupa’da Durum ve Hukuki Düzenlemeler

Avrupa’da dijital şiddet kadınları ve cinsiyet çeşitliliğine sahip bireyleri hedef alan küresel bir sorun olarak ele alınmaktadır. Avrupa Birliği Dijital Hizmetler Yasası (DSA, 2022) platformlara taciz ve şiddet içeriklerini kaldırma yükümlülüğü getirmekte, İsveç ve Danimarka intikam pornosu paylaşımını doğrudan suç kabul ederek cezai yaptırımlar uygulamakta, İngiltere Online Safety Act ile zararlı içeriklerin engellenmesini zorunlu kılmakta ve Fransa, dijital şiddetle mücadele için özel savcılık birimleri kurmaktadır. Ayrıca AB fonları, kadınlara yönelik dijital güvenlik eğitimlerini desteklemektedir.

6.3 Dijital Güvenlik Önerileri ve Farkındalık Çalışmaları

Kadınların dijital dünyada daha güvenli olabilmesi için güçlü şifre kullanımı, iki adımlı doğrulama, bilinmeyen linklere dikkat, konum bilgisini paylaşmama ve gizlilik ayarlarının düzenli olarak gözden geçirilmesi gibi teknik önlemler kritik öneme sahiptir. Bunun yanında toplumsal farkındalık çalışmaları da hayati bir rol oynamaktadır: okullarda ve işyerlerinde dijital güvenlik eğitimleri verilmesi, medya kampanyalarıyla siber şiddetin görünür kılınması, erkeklere yönelik eğitim programları, psikolojik destek hatlarının yaygınlaştırılması ve şirket politikalarında sıfır tolerans yaklaşımı uygulanması önerilmektedir.

6.4 Sonuç ve Çağrı

Kadınlar dijital dünyada cinsiyete dayalı özel tehditlerle karşı karşıyadır ve mevcut yasal altyapı, sosyal destek ağları ve teknolojik araçlar bu tehditlere karşı çoğu



**Avrupa Birliği tarafından
finanse edilmektedir**

zaman yetersiz kalmaktadır. Dijital güvenlik yalnızca teknik bir konu değil; aynı zamanda sosyal, psikolojik ve kültürel bir meseledir. Kadınların dijital alanlarda özgürce var olabilmesi için kadınlara özgü dijital güvenlik politikaları geliştirilmesi, toplumsal farkındalığın artırılması, teknoloji firmalarının sorumluluk üstlenmesi ve kadınlar arası dayanışmanın dijital alana taşınması gerekmektedir. Gerçek güvenlik, dijitalde başlar ve dijital güvenlik, kadınların eşit şekilde güvende hissettiği bir dünya ile mümkündür.



**Avrupa Birliği tarafından
finanse edilmektedir**

KAYNAKÇA

Arxiv.org. (2023). Cybersecurity practices across genders. arXiv.

Brookings Institution. (2023, November 20). AI poses disproportionate risks to women. <https://www.brookings.edu>

CIGI Online. (2024). The dialogue around digital security must account for gendered risks. Centre for International Governance Innovation.

Ekmek ve Gül. (2022). Kadınlar ve çevrimiçi şiddet: Türkiye’de dijital taciz raporu. Ekmek ve Gül Yayınları.

Human Rights Watch. (2021, July 1). Online gender-based violence is a nightmare without borders. Human Rights Watch. <https://www.hrw.org>

Karakuş, M. (2024). Dijital şiddet ve sosyal medya üzerine bibliyometrik bir araştırma. TRT Akademi, 9.

Law Journals (India). (2023). Cyber security concerns for women in the digital era. Law Journals (India).

Manşet International UK. (2023). Toxic Twitter – Women’s experiences of online abuse. Amnesty International UK.

Othman, A. (2025, May 20). AI-generated content and deepfakes: Risks, impacts, and governance challenges. ResearchGate.

Reuters. (2025). Tech firms are failing women entrepreneurs: Here's how to make them feel safer online. Reuters. <https://www.reuters.com>

ResearchGate. (2024). Women and online harassment: A global perspective.

Sarışın, M. (2022). Toplumsal cinsiyete dayalı şiddetin yeni yüzü: Dijital şiddet. KADEM Kadın Araştırmaları Dergisi, 8(2), 257–285.

Sarıçam, E., & Sinsoysal, B. (2024). Dijital şiddetin kadınların kariyer gelişimleri üzerine etkisi. Akra Kültür Sanat ve Edebiyat Dergisi, 12, 7–32.



**Avrupa Birliği tarafından
finanse edilmektedir**

UN Women. (2023). Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women: FAQs. United Nations Entity for Gender Equality and the Empowerment of Women.

UN Women Asia-Pacific. (2024). Online protection and digital security for women. <https://asiapacific.unwomen.org>

United Nations Population Fund (UNFPA) Türkiye. (2021). Turkey digital violence research 2021. UNFPA Turkey.

Yılmaz, A., & Demir, B. (2024). Kadınlara yönelik dijital şiddet ve hukuki önlemler. İstanbul Üniversitesi Hukuk Fakültesi Dergisi, 35(2), 45–67.

Yılmaz, N., & Demir, A. (2024). Kadınlara yönelik dijital şiddet ve sosyal medya. Dergipark.



**Avrupa Birliği tarafından
finanse edilmektedir**



2024-3-TR01-ESC30-SOL-000284071



**Avrupa Birliği tarafından
finanse edilmektedir**

Siber Zorbalığa Karşı Gençlik İttifakı



"Avrupa Dayanışma Programı kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Burada yer alan içerik yazarların görüşlerini yansıtmaktadır ve bu görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz."



**Avrupa Birliği tarafından
finanse edilmektedir**