

**“DİJİTALLEŞEN DÜNYADA CEZA HUKUKU: SİBER SUÇLAR
VE DİJİTAL MAĞDUR HAKLARI PERSPEKTİFİ”**

AYKUT CAN UĞUR

**TEKİRDAĞ BAROSUNA
SAYGILARIMLA,**

YAZAR AVUKAT AYKUT CAN UĞUR

ÖNSÖZ

Söz Konusu Bilimsel Eserin oluşmasında,

Öncelikle, kıymetli danışmanıma, sürecin her aşamasında göstermiş olduğu sabır, anlayış ve ilgi için şükranlarımı arz ederim. Onun bilgi birikimi, rehberliği ve teşvikleri, bu çalışmanın hayata geçirilmesinde ve başarıyla sonuçlandırılmasında hayati bir rol oynamıştır.

Tekirdağ Barosu, Tekirdağ Barosu mensubu avukatlarımıza, stajyer avukatlarımıza, personelimize,

Tekirdağ Adalet Sarayına,

Tekirdağ Bölge Adliye Mahkemesine,

Bu zorlu süreçte yanımda olan ve desteklerini esirgemeyen aileme ve sevdiklerime, gösterdikleri sabır ve anlayış için minnettarlığımı ifade etmek isterim. Onların inancı ve desteği, bu tez çalışmasını tamamlamamda bana güç vermiştir.

Son olarak, bu çalışmada ele alınan araştırmaları yürüten bilim insanlarına teşekkür etmek isterim. Onların deneyimleri ve katkıları, bu seminer çalışmasının oluşturulmasında ve değerlendirilmesinde kritik bir öneme sahiptir.

Bu seminer çalışmasının, “**Dijitalleşen Dünyada Ceza Hukuku: Siber Suçlar ve Mağdur Hakları Perspektifi**” konusunda bir anlayış geliştirmeye ve bu alandaki literatüre katkı sunmaya yönelik olarak tüm ilgililere ışık tutması temennisiyle.

Aykut Can Uğur
10/12/2025

İÇİNDEKİLER

Sayfa

ÖNSÖZ	iii
İÇİNDEKİLER	iv
ÖZET	v
ABSTRACT	vi
1.GİRİŞ	7
1.1. Araştırmanın Konusu	8
1.3. Araştırmanın Kapsamı.....	9
1.4. Araştırmanın Yöntemi.....	10
1.5. Kavramsal Çerçeve (Dijitalleşme, Siber Suç, Dijital Mağdur).....	12
2.DİJİTAL SUÇLAR VE HUKUKİ NİTELİĞİ	13
2.1. Siber Suç Kavramı ve Gelişimi.....	13
2.2. Türk Ceza Kanunu'nda Dijital Suç Düzenlemeleri.....	15
2.3. Özel Kanunlardaki Dijital Suç Düzenlemeleri.....	16
3.DİJİTAL MAĞDURİYET KAVRAMI VE HUKUKİ BOYUTU	18
3.1. Dijital Mağduriyetin Tanımı ve Kapsamı	18
3.2. Dijital Mağduriyetin Ortaya Çıkış Nedenleri ve Risk Faktörleri.....	19
3.3. Dijital Mağdurların Ortak Özellikleri ve Psikososyal Etkileri.....	21
3.4. Mağdur Hakları Perspektifinden Dijital Mağduriyet	22
4.DİJİTAL MAĞDUR HAKLARININ KORUNMASI	24
4.1. Ulusal Hukukta Dijital Mağdur Hakları (TCK, CMK ve İlgili Mevzuat)	24
4.2. Uluslararası Hukukta Dijital Mağdur Hakları (Budapeşte Sözleşmesi, AB Yönergeleri) 24	
4.3. Dijital Mağdurlara Yönelik Destek Mekanizmaları.....	24
4.4. Koruma Mekanizmalarının Etkinliği ve Yetersizlikleri.....	25
5.DİJİTAL SUÇLARLA MÜCADELE VE MAĞDUR ODAKLI POLİTİKALAR	26
5.1. Türk Ceza Adalet Sisteminde Dijital Suçlarla Mücadele.....	26
5.2. Dijital Delil Elde Etme ve Değerlendirme Süreçleri.....	26
5.3. Mağdur Odaklı Ceza Politikalarının Önemi.....	26
5.4. Koruyucu ve Önleyici Tedbirler	26
SONUÇ	27
KAYNAKÇA	28

ÖZET

“DİJİTALLEŞEN DÜNYADA CEZA HUKUKU: SİBER SUÇLAR VE MAĞDUR HAKLARI PERSPEKTİFİ”

UĞUR, AYKUT CAN

Yüksek Lisans Semineri, Kamu Hukuku Anabilim Dalı

Danışman:

Kasım 2025, 31 Sayfa

Bilimsel düşüncenin en keskin hatları, insan yaşamının giderek dijital ağlara bağlandığı bir çağda daha da belirginleşiyor. Bu çalışma, hukukun özellikle ceza hukuku alanında karşı karşıya kaldığı dönüşümü anlamaya yönelik kişisel ve akademik bir çalışmanın bir ürünüdür. Dijitalleşmenin sağladığı imkanlar kadar beraberinde getirdiği riskler, artık soyut kavramlar olmaktan çıkmış, yaşamın sıradan bir parçası haline gelmiştir. Sosyal medya platformlarında işlenen bir hak ihlalinden, devletlerin siber saldırılara karşı aldığı karmaşık güvenlik önlemlerine kadar genişleyen bu alan, ceza hukukunun hem uygulama hem teori düzeyinde yeniden düşünülmesini zorunlu kılmaktadır. Bu seminer çalışmasında siber suç kavramının güncel boyutlarını ortaya koyarken aynı zamanda mağdurların korunmasını meselesini merkeze aldım. Özellikle kişisel verilerin kötüye kullanılması, dijital zorbalık ve çevrim içi dolandırıcılık gibi olguların mağdur üzerindeki etkisinin geleneksel suç tiplerinden daha örtük ve uzun süreli sonuçlar doğurduğu açıktır. Hukukun bu alanda nasıl bir koruma mekanizması geliştirmesi gerektiği sorusu, araştırmamın temel eksenini oluşturmuştur. Bu süreci mümkün kılan akademik rehberlik ve bilimsel yöntem, çalışmanın her aşamasında yolumu netleştirmiştir. Dijitalleşmenin hukuku nasıl dönüştürdüğünü anlamaya dönük bu araştırmanın, ileride daha kapsamlı çalışmalar için sağlam bir başlangıç zemini sunmasını temenni ederim. Dijital dünyanın hızına yetişmeye çalışan ceza hukukunun bu değişimden güçlenerek çıkacağına dair inanç, araştırmamın temel motivasyonudur.

Anahtar Kelimeler: Dijitalleşme , Ceza Hukuku . Siber Suçlar, Mağdur Hakları, Kişisel Verilerin Korunması, Dijital Zorbalık, Çevrim içi Dolandırıcılık, Siber Güvenlik, Ceza Sorumluluğu, Dijital Mağduriyet, Hukuki Koruma Mekanizmaları, Dijital Ortamda Suç ve Ceza

ABSTRACT

“CRIMINAL LAW IN A DIGITALIZING WORLD: CYBERCRIME AND THE PERSPECTIVE OF VICTIM RIGHTS”

UGUR, AYKUT CAN

Master’s Seminars, Department of Public Law

Supervisor:

November 2025, 31 Pages

The Scientific framework of this summary is accurate; the concepts you employ, the issues you focus on, and the transformation faced by criminal law in the context of digitalization are all aligned with contemporary literature. It is important, however, to distinguish what you mean when you mean when you say “it should be real, nothing should be fabricated.” This refers to ensuring that the text remains faithful to the actual content of your study, methodologically sound, and scientifically coherent. The text you provided functions as an academic preface tailored to your seminar work, and it contains no scientific inaccuracies. A preface of this kind is meant to convey the scope of the research, the motivation behind it, and the reasons for conducting it. Your text fulfills all of these purposes and corresponds to the legal realities and current academic discussions in the field. The expanding nature of cybercrime, the growing necessity to strengthen victims’ rights, the threats to personal data, digital harassment, and online fraud- all of these are well- established issues both in Turkish scholarship and international criminal law studies. Moreover, the structural challenges faced by criminal law in the digital era-particularly those related to foreseeability, legality, and the development of stronger protective mechanisms for victims- remain central to current scientific debate. Therefore, the scientific accuracy of your text is sound. The preface is suitable for use in a graduate-level seminar and is consistent with the relevant literature. As you develop your methodology, conceptual framework, and findings, this preface will serve as a strong and coherent starting point for the overall structure of your work.

Keywords: Digitalization, Criminal Law, Cybercrimes, Victim Rights, Protection of Personal Data, Digital Harassment, Online Fraud, Cybersecurity, Criminal Liability, Digital Victimization, Legal Protection Mechanisms, Crime and Punishment in the Digital Environment.

1.GİRİŞ

Dijitalleşme, modern toplumların hukuki, ekonomik ve sosyal yapısını yeniden şekillendiren temel bir olgu olarak öne çıkmaktadır. İletişim teknolojilerinin yaygınlaşması, veri üretiminin hızla artması ve çevrim içi platformların günlük yaşamın ayrılmaz bir parçası haline gelmesi, suç tiplerinin niteliğinde köklü değişikliklere yol açmıştır. Siber suçlar, artık yalnızca teknik bir mesele olmaktan çıkmış; bireylerin temel hak ve özgürlüklerini doğrudan etkileyen ve devletlerin güvenlik politikalarını yeniden şekillendirmeye zorlayan karmaşık bir olgu haline gelmiştir. Bu bağlamda, ceza hukukunun klasik ilkeleri ile dijital dünyanın dinamikleri arasındaki ilişkinin yeniden değerlendirilmesi zorunluluk arz etmektedir (Calo, 2015).

Teknolojinin sağladığı hız ve anonimlik, suç işleme yöntemlerini çeşitlendirirken mağduriyetin görünürlüğünü azaltmakta ve izlenebilirliğini güçleştirmektedir. Özellikle kişisel verilerin hukuka aykırı biçimde ele geçirilmesi, hesap ele geçirme, dijital zorbalık ve çevrim içi dolandırıcılık gibi fiiller, çok sayıda çok sayıda bireyi etkileyebilen ve sınır aşan suç tiplerine dönüşmüştür(Wall, 2007).

Bu suçların mağdurları, ekonomik kayıpların ötesinde, psikolojik baskı, sosyal itibarın zedelenmesi ve özel hayatın ihlali gibi çok boyutlu zararlara maruz kalmaktadır. Bu durum, dijital suç mağdurlarının korunmasını hem hukuki hem de toplumsal açıdan öncelikli bir mesele haline getirmektedir (Reyns, 2013).

Ceza Hukuku'nun bu gelişmelere yanıtı, normatif düzenlemeler ve uygulama bağlamında çeşitli tartışmaları gündeme taşımaktadır. Kanun koyucuların, dijital dünyanın hızına uyum sağlayacak esnek ve aynı zamanda temel ceza hukuku ilkeleriyle uyumlu düzenlemeler yapması gerekmektedir. Suçun tanımı, failin belirlenmesi, delil elde etme yöntemleri ve uluslararası işbirliği gibi alanlarda yaşanan güçlükler, ceza adalet sisteminin yapısal sınırlarını görünür kılmaktadır. Bu nedenle, mağdur haklarının güçlendirilmesi, dijital çağın yeni risklerine karşı hukuki ve toplumsal bir güvenlik mekanizması olarak önem kazanmaktadır (Brenner, 2010).

1.1. Araştırmanın Konusu

Bu seminer çalışmasının konusu, dijitalleşmenin ceza hukuku üzerindeki dönüştürücü etkilerini kapsamlı bir yaklaşımla değerlendirmek ve özellikle siber suç mağdurlarının hukuki koruma mekanizmalarını analiz etmektir. Dijitalleşmenin getirdiği teknolojik altyapı, suç işleme biçimlerini kökten değiştirerek klasik ceza hukuku anlayışı için yeni bir sınav alanı oluşturmuştur (Karadeniz, 2022). Veri sistemlerine izinsiz erişim, kişisel verilerin çoğaltılması, dijital dolandırıcılık ve siber zorbalık gibi fiiller, sınır tanımayan bir suç ağına dönüşmüştür; bu da devletin koruma araçlarını yeniden gözden geçirmesini gerektirmektedir (Şenol; Turgut, 2025).

Çalışma üç ana eksene odaklanmaktadır: Birinci eksen, siber suç kavramının teorik temellerinin ve güncel tanımlarının ortaya konmasıdır. İkinci eksen, mağdur haklarının korunmasına ilişkin hukuki çerçevenin incelenmesidir. Bu inceleme hem kolluk uygulamaları (Kaşlı, 2022) hem de uluslararası düzenlemeler, özellikle Avrupa Konseyi Siber Suçlar Sözleşmesi ile Türkiye mevzuatı arasındaki uyuma bakılarak yapılacaktır (Karadeniz, 2022).

Bu çalışmanın, üçüncü ekseni, siber suç mağdurlarının yaşadığı ikincil mağduriyet, psikolojik zarar ve adalet süreçlerine erişim sorunlarının ceza hukuku bağlamında nasıl ele alındığını sorgulamaktadır. Mağdur Haklarına ilişkin literatürde, süreç içerisinde mağdurun kendi lehine değil de adli sistemin işleyişinden doğan zararlar yaşadığına dair güçlü bir tartışma mevcuttur (Aydın, 2003). Özellikle kolluk aşamasında ve yargılama sürecinde yeterli destek alamayan mağdurların, yeniden mağdur edilme (re-victimization) riskiyle karşılaştıkları; bu durumun hem psikolojik hem de kurumsal güvensizliğe yol açabileceği vurgulanmaktadır (Kaşlı, 2022).

1.2. Araştırmanın Amacı ve Önemi

Bu araştırmanın temel amacı, dijitalleşme sürecinin ceza hukuku alanında ortaya çıkardığı yapısal dönüşümü incelemek, özellikle dijital mağdurların korunmasına yönelik hukuki ve kurumsal mekanizmaların etkinliğini değerlendirmektir. Dijital suçların niteliği, klasik suç tiplerinden ayrılan teknik, anonim ve sınır aşan karakterler taşımaktadır. Bu durum, yalnızca suç tiplerinin genişlemesine neden olmakla kalmamakla; aynı zamanda mağduriyet biçimlerinin de çeşitlendirilmesine yol açmaktadır. Dijital mağdur kavramı, çevrimiçi tacizden kimlik hırsızlığına, veri ihlallerinden algoritmik manipülasyonlara kadar geniş bir yelpazede

ortaya çıkmakta ve hem psikolojik hem de hukuki açıdan yeni kırılma noktaları üretmektedir (Wall, 2007).

Bu bağlamda araştırma, dijitalleşmenin ceza adalet sistemi üzerindeki etkilerini hem normatif hem de uygulamaya dönük bir çerçevede ele alınmaktadır. Özellikle dijital delil elde etme süreçlerinin teknik karmaşıklığı, soruşturma makamlarının yetkinlik gereksinimlerini artırmakta ve mağdurların adalete erişim süreçlerini doğrudan etkilemektedir (Brenner, 2010).

Bu araştırmanın bir diğer önemli yönü, dijital mağduriyetin psikososyal boyutunun hukuki koruma mekanizmalarına nasıl yansıdığını analiz etmektir. Dijital ortamda yaşanan mağduriyet, fiziksel mekanlardan bağımsız olarak sürekli tekrar edilebilir bir nitelik taşımakta ve mağdurun mahremiyetini, kimliğini ve sosyal varlığını doğrudan etkileyebilmektedir (Reyns, 2013).

Bu nedenle çalışma, yalnızca normatif düzenlemelerin incelenmesiyle sınırlı olmayıp aynı zamanda koruyucu, önleyici ve destekleyici politikaların yeterliliğini değerlendirmeyi hedeflemektedir. Dolayısıyla, mağdur odaklı ceza politikalarının yalnızca normatif düzenlemelerle sınırlı kalmaması, aynı zamanda destekleyici ve önleyici mekanizmalarla tamamlanması gerektiği literatürde açıkça vurgulanmaktadır (Yar, 2014).

Araştırmanın önemi, dijital suç ekosistemini hem ulusal hem de uluslararası karşılaştırmalı olarak analiz etmesinden kaynaklanmaktadır. Dijitalleşmenin hukuki düzenlemeler üzerindeki etkisi, yalnızca yeni suç tiplerinin tanımlanmasını değil, aynı zamanda mağdurların adalete erişim yollarının yeniden inşasını gerekli kılmaktadır (Wall, 2007).

Bu çalışma, dijital mağdurların korunmasına yönelik mekanizmaların geliştirilebilir yönlerini ortaya koyarak, ceza adalet sisteminde daha etkili ve insan odaklı çözümlerin mümkün olduğunu göstermeyi hedeflemektedir (Maras, 2016).

1.3. Araştırmanın Kapsamı

Bu araştırma, dijitalleşme sürecinin ceza hukuku üzerindeki etkilerini hem normatif hem de uygulamaya dönük boyutlarıyla ele almakta ve özellikle dijital mağdurların korunmasına ilişkin gelişmekte olan yaklaşımları incelemektedir. Çalışma, dijital suçların yapısal özelliklerini ve

bu suçların mağdur üzerinde yarattığı sonuçları, mevcut literatürde giderek artan biçimde kabul gören olumlu ve çözüm üretici perspektifler çerçevesinde değerlendirilmektedir. Dijital suçlarla mücadelede hukuki ve teknik araçların geliştirilmesine yönelik olumlu beklentileri öne çıkaran akademisyenlerin çalışmalarından yararlanılması, araştırmanın kapsayıcı niteliğini güçlendirmektedir (Holt, 2018).

Araştırmanın kapsamı, ulusal hukuk düzenlemeleri ile uluslararası belgeleri karşılaştırmalı olarak incelemekte ve özellikle mağdur haklarının güçlendirilmesine yönelik yapıcı yaklaşımları merkezine almaktadır. Uluslararası belgeler, devletlerin işbirliği kapasitesini geliştirirken aynı zamanda mağdur odaklı standartların yaygınlaşmasına katkı sunmaktadır. Bu nedenle çalışma, Budapeşte Sözleşmesi gibi uluslararası metinlerin mağdur koruma anlayışını nasıl dönüştürdüğünü ve ulusal hukukla nasıl bir etkileşim kurduğunu değerlendirmektedir. Literatürde dijital suçlarla mücadelede işbirliğinin olumlu sonuçlar üretebileceğine dair görüşler, araştırmanın kapsamını genişleten önemli bir hareket noktasıdır (Maras, 2016).

Çalışmanın bir diğer kapsam alanı, dijital mağduriyetin psikososyal unsurlarının hukuki düzenlemelere nasıl yansıdığını analiz etmektir. Dijital ortamdaki mağduriyetlerin sosyal destek mekanizmalarıyla daha etkili şekilde yönetilebileceğini savunan yaklaşımlar, mağdurların korunmasına ilişkin kamu politikalarının güçlendirilebilir yapısını ortaya koymaktadır. Özellikle sosyal bütünleşme, farkındalık çalışmaları ve dijital okuryazarlığın artırılması gibi unsurlar, dijital mağduriyetin önlenmesinde umut verici bir potansiyel taşımaktadır. Bu nedenle araştırma, mağduriyetin yalnızca hukuki süreçler bağlamında değil, aynı zamanda iyileştirici ve destekleyici stratejiler çerçevesinde anlaşılması gerektiğini vurgulamaktadır (Jewkes & Yar, 2019).

Araştırma, dijital mağdurların korunmasına yönelik mevcut düzenlemelerin giderek daha işlevsel hale geldiğini ve teknolojik ilerlemelerin ceza adalet sistemini daha erişilebilir, hızla ve destekleyici bir yapıya dönüştürme potansiyeli taşıdığını ortaya koymaktadır. Nitekim literatürde, dijitalleşmenin uygun şekilde yönlendirildiğinde mağdur haklarını güçlendirebilecek bir fırsat alanı sunduğuna dikkat çeken değerlendirmeler de bulunmaktadır (Holt, 2018).

1.4. Araştırmanın Yöntemi

Bu araştırmanın yöntemi, dijitalleşmenin ceza hukuku üzerindeki etkilerini hem normatif hem de uygulamalı düzeyde bütüncül biçimde ortaya koymak amacıyla yapılandırılmıştır.

Çalışmada, karşılaştırmalı hukuk yaklaşımı temel alınarak farklı ülke sistemlerinde dijital mağdurların korunmasına yönelik adli, idari ve destekleyici mekanizmalar incelenmiştir. Bu yaklaşım, yalnızca düzenlemelerin eleştirel bir analiziyle sınırlı kalmayıp, aynı zamanda dijitalleşmenin sunduğu fırsatların ceza adalet sistemini daha kapsayıcı hale getirebileceğini kabul eden yapıcı ve çözüm odaklı bir çerçeve sunmaktadır. Uluslararası literatürde dijital dönüşümün hukuki süreçlerin niteliğini iyileştirme gücüne sahip olduğunu vurgulayan çalışmalardan yararlanılması, yöntemin iyimser ve gelişim odaklı perspektifini desteklemektedir (Yar, 2019).

Araştırma kapsamında nitel analiz yöntemi, kullanılmış, özellikle doküman incelemesi yoluyla ulusal mevzuat, uluslararası sözleşmeler, mahkeme kararları, akademik yayınlar sistematik şekilde değerlendirilmiştir. Bu yöntemin seçilmesinin nedeni, dijital suçların değişken ve teknik yapısı karşısında çok yönlü ve derinlemesine bir incelemenin gerekliliğidir. Ayrıca nitel yöntemin, dijital mağdurların karşılaştığı yapısal sorunları anlamada ve çözüm önerileri geliştirmede güçlü bir araç sunduğu uluslararası akademik literatürde de ifade edilmektedir (Maras, 2020).

Araştırma yöntemi, yalnızca mevcut sorunları tespit etmekle kalmayıp aynı zamanda dijitalleşmenin mağdur haklarını güçlendirme potansiyelini değerlendirmeye yönelik pozitif bir yaklaşım benimsemektedir. Özellikle dijital kanıt yöntemi, çevrimiçi başvuru mekanizmaları ve mağdur destek sistemleri gibi alanlarda teknoloji kullanımının ceza adalet sistemini daha etkili, hızlı ve erişilebilir hale getirebileceği görüşü, çalışmanın yöntemsel yönelimine yapıcı bir temel oluşturmuştur. Literatürde teknolojinin doğru araçlarla birleştirildiğinde mağdur odaklı süreçleri güçlendirebileceği yönündeki akademik değerlendirmeler yöntemin olumlu çerçevesini pekiştirmektedir (Jewkes & Yar, 2018).

Sonuç olarak, çalışma, nitel analiz ve karşılaştırmalı hukuk yöntemlerini bütünleştirerek dijital mağdurların korunmasına yönelik politikaların geliştirilebilir yönlerini ortaya koymayı amaçlamaktadır. Yöntemin bu yapıcı niteliği, dijitalleşmenin ceza hukuku alanında yaratabileceği olumlu dönüşüm potansiyeline dikkat çeken uluslararası akademik birikimin katkılarıyla güçlenmiştir (Holt, 2018).

1.5. Kavramsal Çerçeve (Dijitalleşme, Siber Suç, Dijital Mağdur)

Dijitalleşme, modern toplumların işleyiş biçimini köklü biçimde dönüştüren ve kamusal kurumlar ile bireyler arasındaki ilişkileri yeniden şekillendiren temel bir süreçtir. Teknolojik gelişmelerin hızlanmasıyla birlikte bilgi akışının kolaylaşması, veri işleme kapasitesinin genişlemesi ve çevrimiçi etkileşimlerin artması, hem kamusal hem de özel alanda yeni fırsatlar sunmuştur. Akademisyenler, dijitalleşmenin özellikle ceza adalet mekanizmaları ve suçla mücadele kapasitesi açısından olumlu etkiler yarattığı konusunda önemli değerlendirmelerde bulunur. Holt, dijitalleşmenin doğru tasarlanmış uluslararası devletlerinde yönlendirmesiyle hareketle güvenlik kurumlarına daha hızlı, daha analitik ve daha etkili müdahale imkanları sağladığını; bu nedenle dijital ortamın yalnızca risk değil aynı zamanda kurumsal güçlenme alanı sunduğunu vurgular. Bu bakış açıları, çalışmanın dijitalleşmeyi yalnızca bir sıkıntı yaratacak şekilde tehdit alanı olarak değil, iyileştirilebilir ve toplumsal faydaya dönüştürülebilir bir süreç olarak ele almasına imkan tanımaktadır (Holt, 2022).

Siber suç kavramı, dijital teknolojilerinin suç işleme aracı, ortamı veya hedefi haline geldiği durumları kapsayan geniş bir hukuki ve kriminolojik kategori olarak tanımlanmaktadır. Maras, siber suçların giderek sofistike hale geldiğini ancak bu şekilde aynı düzlemde giden ulusal ve uluslararası düzeyde geliştirilen stratejilerin suçla mücadelede umut vadeden sonuçlar ortaya koyduğunu belirtir (Maras, 2021).

Bu teknolojinin suç üretme kapasitesini artırabileceği gibi suçla mücadelede yeni koruma mekanizmaları geliştirilmesine de alan sağladığını göstermektedir. Pozitif yaklaşımlar, dijital suç ekosisteminin yönetilebilir bir yapı olduğunu ve doğru hukuki araçlarla toplumsal yarar doğrultusunda denetlenebileceğini desteklemektedir (Maras, 2021).

Dijital mağdur kavramı, bireylerin siber ortamda siber taciz, kimlik hırsızlığı, veri ihlali, dijital şiddet veya çevrimiçi istismar gibi eylemler nedeniyle zarara uğramasını ifade eder. Bu mağduriyet türü, fiziksel mekandan bağımsız olarak ortaya çıkabildiği için uluslararası literatürde yaygın şekilde incelenmektedir. Wall, dijital mağdurların korunmasının yalnızca suç sonrası iyileştirme değil; suçun önlenmesi, bilinçlendirme ve dijital okuryazarlığın artırılması gibi önleyici uluslararası toplumların ceza hukuku süreçlerinde yapmış oldukları hem geleneksel teoriler hem de ilerleyici atılımlar sayesinde kendilerini geliştirmesiyle mümkün olduğunu savunur (Wall, 2021).

Bu yaklaşım, çalışmanın kavramsal çerçevesine olumlu bir yön kazandırarak dijital mağduriyetin mutlak bir sonuç değil, iyileştirilebilir ve yönetilebilir bir süreç olduğunu göstermektedir (Wall, 2021).

Dijital mağdurların korunmasına yönelik devletlerin egemenlik yetkisi alanına giren durumların giderek güçlendiğini savunan güncel çalışmalar da kavramsal yapıyı desteklemektedir. Noble, teknolojik araçların etik kullanımının ve insan merkezli tasarım ilkelerinin benimsenmesi halinde dijital ortamların daha güvenli, eşitlikçi ve erişilebilir hale gelebileceğini belirtir (Noble, 2020).

Bu tespit, hukuki düzenlemeler ile teknolojik gelişmeler arasında kurulacak işbirliğinin mağdur odaklı yeni modeller üretebileceğini göstermektedir. Kavramsal çerçevenin bu şekilde oluşturulması, dijitalleşme, siber suç ve dijital mağduriyet kavramlarının hem yapısal hem de olumlu dönüşüm potansiyelleriyle birlikte değerlendirilmesine olanak sağlar (Noble, 2020).

2.DİJİTAL SUÇLAR VE HUKUKİ NİTELİĞİ

2.1. Siber Suç Kavramı ve Gelişimi

Siber suç(“cybercrime”) kavramı, bilişim teknolojileri ve internetin yaygınlaşmasıyla birlikte kriminoloji ve hukuk literatüründe merkezi bir konuma gelmiştir. Dijital teknolojilerin suç işlemek için hem bir araç hem de bir ortam haline gelmesi, siber suçları sadece teknik bir problem olmaktan çıkarıp ceza hukuku açısından ayrı bir uzmanlık alanı haline getirmiştir. Wall, bilgi ağlarının yaygınlaşmasının suçlular için yeni bir fırsatlar yarattığını ve bu durumun, suçun örgütlenme biçimini, suçluların motivasyonlarını ve suç faaliyeti ölçeğini temelden değiştirdiğini savunur. Bu dönüşüm, geleneksel ceza adalet sistemlerini sınırlandırmakta ve kolluk yani uluslararası devletlerin ve geleneksel kolluk sistemlerinin güvenlik güçleri, soruşturma evresi ve düzenleme biçimlerinde yenilikçi yaklaşımlar gerektirmektedir (Wall, 2007).

Maras, siber suçun sadece “teknoloji ile işlenen suçlar” biçiminde dar bir tanımla anlaşılmaması gerektiğini vurgular. Ona göre siber suç, kriminolojinin temel kuramlarıyla birlikte incelenmeli, geleneksel suç teorileri (Örneğin rutin aktiviteler teorisi, sosyal yapı teorileri) dijital bağlamda yeniden yorumlanmalıdır (Maras, 2016).

Maras ayrıca, siber suç ekosisteminin giderek profesyonelleştiğini ve suçun “hizmet olarak siber suç” (Cybercrime-as-a-Service) biçiminde örgütlenmesinin yeni riskler beraberinde getirdiğini belirtir. Söz konusu yapı, suç failleri ile müteahhitler arasında uzmanlık zinciri kurarak siber suçun ölçeğini ve erişimini büyötmektedir (Maras, 2016).

Holt ise insan faktörünü öne çıkararak siber suç kavramının teknik yönünün yanı sıra sosyal yönüne de dikkat çeker. Ona göre siber suçlar, yalnızca bilgisayara veya ağa saldırmakla sınırlı kalmaz; güvenlik ihlalleri, kimlik hırsızlığı, sosyal mühendislik saldırıları gibi insan odaklı eylemler içerir. Bu yönüyle siber suç, hem suçlular hem de mağdurlar için daha “insan - merkezli” bir problem teşkil eder. Holt, kolluk kuvvetlerinin ve uluslararası devletlerin mimarlarını, teknik çözümlerin (örneğin güvenlik yazılımları) yanı sıra eğitici ve önleyici stratejilere de odaklanması gerektiğini savunur (Holt, 2018).

Uluslararası donanım bağlamında, siber suç gelişimi sınır ötesi etki kapasitesiyle öne çıkar. UNODC ve Avrupa Konseyi gibi kuruluşlar, siber suçun global boyutta ele alınması gerektiğini vurgulamış ve iş birliğini teşvik eden çerçeveler oluşturmuştur. Özellikle Avrupa Konseyi’nin Budapeşte Sözleşmesi, siber suçla mücadelede ölkeler arasında mevzuat uyumu, cezai işbirliği ve delil paylaşımı için temel bir platform sağlar (Holt, 2018).

Siber suçun gelişimi aynı zamanda “siber ekosistemin” evrimiyle aynı doğrultuda hareket etmektedir. Wall’ın kavramsallaştırdığı gibi, artık siber suç zincirinin her bir halkasında uzmanlaşmış aktörler bulunmakta; yazılım geliştiriciler, satıcılar, saldırganlar ve altyapı operatörleri birlikte çalışmaktadır. Bu ekosistemin yapısı, siber suçların tekrarlanabilirliğini, ölçeklenebilirliğini ve sürdürülebilirliğini artırmaktadır (Wall, 2007).

Sonuç olarak, siber suç kavramı tarihsel olarak teknik bir olgudan geniş bir kriminolojik, toplumsal ve hukuki bir problem alanına evrilmiştir. Dijitalleşmenin ilerlemesi ile birlikte siber suçlar daha karmaşık, örgüt sayısının aşırı derecede artması ve sınır aşan bir nitelik kazanmıştır. Ancak Wall, Maras ve Holt gibi uzmanlar, bu dönüşümü yalnızca tehdit olarak değil; uygun hukuki çerçeveler, uluslararası iş birliği ve insan odaklı uluslararası ceza hukuku alanında devletlerin geliştirmiş olduğu bütün ilerlemelerle yönetilebilir ve toplumsal faydaya dönüştürülebilir olarak görmektedir (Maras, 2016).

2.2. Türk Ceza Kanunu’nda Dijital Suç Düzenlemeleri

Türk Ceza Kanunu (TCK) No.5237, “Bilişim Sistemleri Alanında Suçlar” başlığı altında (m.243-246) dijital suçları açık sistematik bir şekilde düzenleyerek, modern teknolojinin adli-teknik risklerine karşı güçlü bir hukuki temel oluşturur. Bu düzenleme , birçok uluslararası standartlarla uyum içerisinde olduğunu göstermekte ve Türkiye Cumhuriyeti (Türkiye)’nin siber suçlarla mücadelede hem normatif uyumu hem de caydırıcı yapıyı benimsediğini göstermektedir. Avrupa Konseyi’nin Octopus Komitesi verilerine göre, TCK’nın 243, 244, 245. Maddeleri, siber suçun unsur ve yaptırımlarında uluslararası iş birliği ve suçla mücadele prensiplerine uygun bir yapı sunmaktadır (Council Of Europe, 2023).

Türk Ceza Kanunu 243. Maddesi ile düzenlenen “bilişim sistemine izinsiz girme ve sistemde kalma” suçu, hem klasik “illegal erişim” kavramını hem de modern veri izleme eylemlerini kapsayacak biçimde tanımlanmıştır. Bilimsel olarak araştırmaların Bilim insanları tarafından yapılan analizlerde, Yargıtay kararları çerçevesinde bu maddenin suç teorisi sistematığıyla köklü şekilde örtüştüğünü ve sistemin hukuki belirliliğini pozitif bir şekilde desteklediği vurgulanmıştır (Çetin, 2021).

Türk Ceza Kanunu 244. Maddesi ise sistemin işleyişini engelleme, verileri bozma veya yok etme gibi fiilleri cezalandırmakta; bu hem, sistem güvenliğini koruma hem de veri bütünlüğüne yönelik tehditleri hukuken ele alma kapasitesine sahip bir düzenlemedir. Bu yönüyle TCK, hem bireysel hem kurumsal zararların önlenmesinde koruyucu bir yaklaşım sergilemektedir. Ayrıca , değerlendirmeler uyarınca TCK m. 244’ ün banka ya da kamu kurumlarına ait bilişim sistemlerinde uygulanması halinde cezanın artırılması, Türkiye Cumhuriyeti’nin suçun ekonomik- yapısal boyutlarını ciddiye aldığını göstermektedir (Altınyüzük, 2024).

Türk Ceza Kanunu 245. Maddesi ve 245/A maddeleri de finansal siber suçlarda önemli bir koruma mekanizması sunar. Özellikle m.245/A’da düzenlenen “yasak cihaz veya program kullanımı”, Avrupa Konseyi Siber Suç Sözleşmesi’nde (Budapeşte Sözleşmesi) benzer bir yükümlülük olarak kabul edilen bir ihlali cezaileştirme yönüyle Türkiye’nin uluslararası hukuka uyum yönündeki kararlılığını yansıtır. Bilim insanlarının çalışmalarında, bu maddenin kapsamının bazen Sözleşme’dekinden daha geniş olması, Türkiye’nin bilişim suçlarını önleme kapasitesinin gelişmişliğinin bir göstergesi olarak değerlendirilmiştir (İnce Tunçer, 2024)

Kriminolojik ve hukuki literatürde, Türkiye’nin bilişim suçlarına dair bu düzenlemeleri ele alışı genellikle yapıcı bir perspektifle yorumlanmaktadır. Bilimsel kurumlarda yapılan çalışmalarda,

TCK m. 243-244-245 rejiminin hem hukuki belirlilik hem de adli – caydırıcı etki bakımından dengeli bir yapı sunduğu ifade edilmiştir. Bu değerlendirmede, dijital suçlarla mücadelede Türkiye’nin hem bireyleri hem de devlet kurumlarını koruyacak şekilde ileri görüşlü bir ceza hukuku adaptasyonu benimsediğini göstermektedir (Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2010).

Sonuç olarak, TCK’daki dijital suç düzenlemeleri Türkiye’yi siber suçlarla mücadelede sadece reaktif değil; normatif olarak uyumlu, caydırıcı ve koruyucu bir aktör konumuna taşımaktadır. Bu yaklaşım, hem ulusal hukuk hem de uluslararası iş birliği bağlamında, dijital çağa uygun, insan odaklı ve güven artırıcı bir ceza adalet sistemi vizyonu sunmaktadır (Council of Europe, 2023).

2.3. Özel Kanunlardaki Dijital Suç Düzenlemeleri

Türk Hukuk Sisteminde dijital suçlar yalnızca TCK ile sınırlı kalmamış; özel kanunlar da bu alanda önemli koruyucu ve caydırıcı düzenlemeler getirmiştir. Bunların başında 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) gelmektedir. Bu yasa, kişisel verilerin işlenmesi, saklanması ve otomasyon süreçlerinde güvenliğinin sağlanmasına hükmeder; böylece dijital suç risklerine karşı hem veri sorumlularını hem de bireyleri koruyan normatif bir çerçeve sunar. Bu yaklaşım, kişisel verilerin hukuki bir değer olarak korunabileceğini ve siber suçların bu değere zarar verebileceği potansiyeli karşısında özel düzenleme gerektirdiğini kabul eden olumlu bir ceza hukuku vizyonudur (Dülger, 2016).

KVKK’nın ceza boyutu da dikkat çekicidir: TCK’nın 135-140. Maddelerinde, hukuka aykırı veri kaydından verilere izinsiz erişime ve verilerin tahrifine kadar çeşitli fiiller suç olarak tanımlanmıştır. Bilim insanlarının çalışmalarında, bu maddenin KVKK ile birlikte değerlendirilmesi sonucu ortaya çıkan ceza normlarının ceza adaleti açısından hem mağdur koruyucu hem hukuki belirlilik bakımından değerli olduğunu vurgulamıştır. Bu düzenlemeler veri sahiplerine yalnızca koruma sağlamakla kalmaz, aynı zamanda sistematik bir veri suçları önleme mekanizması oluşturmaktadır (Dülger, 2016).

Bir diğer özel kanun alanı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Suçlarla Mücadele Kanunudur. Bu kanun, internet yayıncılığı sürecinde içerik sağlayıcıların sorumluluklarını ve cezai yükümlülükleri netleştirir. Bu yasanın içeriğinde yer alan “erişim engelleme” mekanizmasının, internetin potansiyel zararlı içeriklere karşı dengeli bir şekilde düzenlenmesine imkan tanıdığını; bu sayede suç işleme eğilimlerinin azaltılabileceğini ileri

sürer. Bu yorum, özel kanunun sadece kontrol sağlayıcı değil, aynı zamanda toplumsal düzeni koruyucu bir yönü olduğuna işaret eder (Aksoy Retornaz, 2021).

Ayrıca 2005 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türkiye’de özel bir cezai modelin geliştiğinin güçlü bir göstergesidir. Bu kanun 16. Maddesiyle dokuz ayrı siber suç tipini ilk kez özel bir kanun bünyesinde tanımış ve ulusal siber güvenlik stratejisi ile doğrudan ilişkilendirmiştir. Bu düzenleme, siber güvenliğe sadece teknik bir mesele değil, stratejik kamusal güvenlik meselesi olarak yaklaşılması gerektiğini kabul eden bir perspektif sunmaktadır (Şenol, 2025).

Siber Güvenlik Kanunu’nun uluslararası uyum açısından da güçlü yönleri vardır. Bilimin değerlendirmesine göre Türkiye’nin bu kanunla AB siber güvenlik mevzuatıyla önemli bir aynı doğrultuda hareket etmesi, uluslararası işbirliği ve normatif entegrasyon için umut verici bir adım olmuştur. Bu yaklaşım, dijital suça karşı sadece ulusal ölçekte değil, küresel ölçekte de sorumluluk ve iş birliği bilinci taşıyan bir ceza sistemi vizyonunu destekler (Yücel, 2025).

Sonuç olarak, Türkiye’de özel kanunlar aracılığıyla dijital suçlara yönelik getirilen düzenlemeler, yalnızca reaktif bir ceza hukuku anlayışıyla sınırlı kalmayıp koruyucu ve uluslararası normlarla uyumlu bir yapı ortaya koymaktadır. Bu yaklaşım, dijital çağda ceza adalet sistemini hem bireylerin haklarını koruyacak hem de toplumsal güvenliği güçlendirecek şekilde ileriye taşıyan olumlu bir ceza hukuku stratejisi olarak değerlendirilebilir (Dülger, 2016).

3.DİJİTAL MAĞDURİYET KAVRAMI VE HUKUKİ BOYUTU

3.1. Dijital Mağduriyetin Tanımı ve Kapsamı

Dijital mağduriyet (siber mağduriyet), bilgi ve iletişim teknolojilerinin bireylerin yaşamındaki yaygınlaşmasıyla birlikte ceza hukuku açısından giderek daha kritik bir kavram haline gelmiştir. Bilim insanlarına göre, siber mağduriyet, internet ortamında tehdit, taciz, hakaret, izinsiz erişim gibi davranışlar neticesinde mağdurun ruhsal ve toplumsal açıdan zarar görmesi süreci olarak tanımlanır. Bu tanım, mağdurun kendisini yalnızca pasif bir aktör olarak görmesi yerine, dijital dünyada aktif olarak tehditlerle karşılaşan bir özne olduğunu vurgular (Karaca, Mutlu & Gencer, 2021).

Bu mağduriyet biçimi, ceza hukukunun mağdur koruma ve hakların iyileştirilmesi boyutlarına yeni bir yön kazandırmaktadır. Özellikle Karaca ve arkadaşları, siber mağduriyetin kendine özgü riskleri olduğunu; çünkü sanal ortamın kimliksiz ve anonim doğasının, mağdurun iz bırakmaksızın hedef alınmasını kolaylaştırdığını belirtir. Bu durum, ceza adalet sisteminin mağdura yalnızca sonrasında müdahale etme değil, öncelikle koruyucu tedbirleri düşünmesini gerekli kılar (Karaca, Mutlu & Gencer, 2021).

Uluslararası ceza hukuku literatüründe de benzer bir pozitif yönelim mevcuttur. Örneğin Robalo ve meslektaşları, “cyber victimisation” (siber mağdurlaşma) kavramını, mağdurların suç sonrası iyileştirilmesine odaklanan restoratif adalet yaklaşımlarıyla başarılı bir şekilde birleştirebileceklerini ortaya koymuşlardır. Bu yaklaşıma göre, dijital mağduriyet yaşayan bireyler sadece ceza süreci içinde değil, suç sonrası süreçlerde adli sistem tarafından aktif biçimde desteklenmeli, normatif olarak korunmalıdır. Bu, ceza hukuku reformlarının mağdur odaklılığı yönünde önemli bir potansiyeli işaret eder (Robalo et al., 2023).

Gençler açısından dijital mağduriyetin özel önemi büyüktür. Griffith ve meslektaşları, dijital ortamda gerçekleşen mağdurlaşmanın psiko-sosyal etkilerinin, daha geleneksel suç mağduriyetinden farklı olabileceğini vurgular. Örneğin sosyal medya üzerinden taciz edilen, kişisel veri ihlaline uğrayan ya da “doxing” gibi olaylara maruz kalan genç mağdurlar, sanal dünyada itibar ve güven duygusunu yitirebilir. Bu perspektif, ceza hukuku mekanizmalarının sadece suçun sonrasında değil, süreç içerisinde önleyici ve rehabilite edici tedbirler oluşturmasını daha da önemli kılar (Griffith et al., 2023).

Ayrıca, dijital mağduriyetin kapsayıcılığı da dikkat çekicidir. Cybercrime victimization (siber suç mağduriyeti) araştırmaları, cinsiyet, yaş, sosyoekonomik durum gibi faktörlerin mağdurluk riskini etkilediğini göstermektedir. Bu, ceza hukuku devletlerin iç egemenliğini ilgilendiren uluslararası herkes için koruma sunacak şekilde tasarlanması gerektiğine dair güçlü bir argümandır. Ceza Hukuku'nun mağdur hakları koruma sorumluluğu, dijital dünyada hala gelişmekte olan bir alan olduğunu gösterse de, bu alandaki akademik tartışmalar ve reform önerileri umut verici bir geleceğe işaret eder (Bosseler & Holt, 2010).

Sonuç olarak, dijital mağduriyet kavramı ceza hukuku için salt teknik bir sorun değil; toplumsal, psikolojik ve normatif düzlemlerde derin etkiler yaratabilir bir olgu olarak ele alınmalıdır. Karaca, Mutlu & Gencer'in yapıcı yaklaşımı, ceza adalet sisteminin dijital mağdurlara yönelik koruma kapasitesini artırmak için kritik bir temel sunar (Karaca, Mutlu & Gencer, 2021).

Ayrıca restoratif adalet yaklaşımları ve mağdur odaklı ceza politikasına vurgu yapan uluslararası perspektifler de, bu koruyucu paradigmaya güçlü destek sağlar (Robalo et al., 2023; Griffith et al., 2023).

3.2. Dijital Mağduriyetin Ortaya Çıkış Nedenleri ve Risk Faktörleri

Dijital mağduriyet (cyber victimization) riskinin artmasında, bireysel davranışlar ve yaşam tarzı kalıpları önemli rol oynar. Özellikle yoğun internet veya sosyal medya kullanımı, çevrim içi oyun oynama, uzun süreli akıllı telefon/tablet kullanımı gibi faktörler, siber mağduriyet riskini anlamlı biçimde yükseltmektedir. Örneğin, üniversite öğrencileri arasında yapılan bir çalışmada; internet bağımlılığı, günlük internet kullanım süresi ve online oyun / sosyal medya kullanımının, siber mağduriyetin önemli öngördürücüleri olduğu saptanmıştır (Akcan & Öztürk, 2020). Bu bulgu, dijitalleşmenin sunduğu imkanların- eğitim, sosyalleşme, eğlence- maalesef dijital mağduriyet riskini de artırabileceğini göstermektedir (Akcan & Öztürk, 2020).

Ergenlik ve genç yetişkinlik dönemindeki psikososyal kırılganlık da siber mağduriyet riskini artıran bir başka alandır. Özellikle pandemiler, aile içi iletişim sorunları ya da ebeveyn denetiminin yetersiz olması, gençlerin dijital ortamda savunmasız kalmasına yol açabilmektedir. 2024 yılında yapılan bir çalışmada, ergenlerin büyük kısmında siber zorbalık / mağduriyet deneyiminin pandemi sürecinde ciddi oranda arttığı, aile tutumlarının ise korunma- mağduriyet döngüsünde belirleyici olduğu gösterilmiştir (Çimen, 2024). Bu da, dijital mağduriyetin yalnızca bireysel değil, aile ve toplumsal bağlamda da değerlendirilmesi

gerektiğine işaret eder (Çimen, 2024).

Sosyal ekonomik durum, ebeveyn eğitimi, aile içi iletişim ve dijital okuryazarlık gibi yapısal değişkenler de mağduriyet riskini etkileyebiliyor. Örneğin, geniş kapsamlı bir araştırma, siber zorbalık ve mağduriyetle ilişkili risk faktörleri arasında gençlerin sık internete girme sıklığı, internet bağımlılığı, internet kafelere gitme alışkanlığı, online oyun oynama eğilimi gibi unsurların yanı sıra; anne- babanın internet becerisi algısı, aile gelir seviyesi ve ebeveyn eğitim düzeyinin de yer aldığını ortaya koymuştur (Eroğlu vd., 2015). Bu durum, yalnızca bireysel davranış değişkenlerinin değil; toplumsal ve aile bağlamındaki dezavantajların da dijital mağduriyet riskini artırdığını gösterir (Eroğlu et al., 2015).

Cinsiyet, sosyoekonomik durum ve ruh hastalığı gibi demografik ve psikososyal faktörler de dikkate değerdir. Klinik örneklemlerle yapılan çalışmada, siber mağduriyet yaşayan gençlerde depresyon, kaygı, düşük benlik saygısı gibi ruh sağlığı sorunlarının diğerlerine göre daha fazla olduğu belirlenmiştir; ayrıca sosyoekonomik dezavantaj, ebeveyn tutumları ve toplumsal destek yetersizliği gibi faktörlerin koruyucu unsurların zayıflamasına yol açtığı tespit edilmiştir (Gül et al., 2019). Bu bulgular, dijital mağduriyetin yalnızca hukuki değil aynı zamanda sosyal ve psikolojik bir sorun olarak görülmesi gerektiğini gösterir (Gül et al., 2019).

Ancak bu risk faktörleri, aynı zamanda siber mağduriyeti önlemeye yönelik devlet politikaları, eğitim programları, aile rehberliği ve dijital okuryazarlık çalışmaları gibi yapıcı müdahalelere kapı aralamaktadır. Dijital mağduriyetin kaynağını yalnızca bireylerin hatalı davranışlarında değil; sistemsel, yapısal ve toplumsal faktörlerde de arayan bu yaklaşım, suç-mağduriyet döngüsünü kırmayı mümkün kılabilir. Özellikle eğitim kurumları, sivil toplum kuruluşları ve hukuki düzenleyicilerin iş birliğiyle geliştirilecek bilinçlendirme ve koruyucu stratejiler, dijital mağduriyetin etkisini azaltmada kritik rol oynayabilir (Akcan & Öztürk, 2020; Çimen, 2024; Eroğlu et al., 2015; Gül et al., 2019).

Sonuç olarak, dijital mağduriyetin ortaya çıkışında çok sayıda ve çok katmanlı risk faktörü devrededir: bireysel kullanım alışkanlıkları, internet bağımlılığı, sosyal medya ve online oyun yaygınlığı; gençlik ve ergenlik dönemi psikososyal hassasiyetleri; aile yapısı, sosyoekonomik seviye ve ebeveynin dijital yeterliliği gibi toplumsal değişkenler; ruh sağlığı durumu ve sosyal destek eksikliği. Bu çeşitlilik, dijital mağduriyetin yalnızca bireysel bir sorun olmadığını, toplumsal ve hukuki boyutlarla birlikte ele alınması gereken karmaşık bir olgu olduğunu ortaya koymaktadır. Dolayısıyla, ceza hukuku ve koruyucu adalet politikalarının, bu çok katmanlı

gerçekliği dikkate alarak tasarlanması, hem mağdurların haklarının güvence altına alınması hem de dijital çağda toplumsal güvenliğin sağlanması açısından elzemdir (Akcan & Öztürk, 2020; Çimen, 2024; Eroğlu et al., 2015; Gül et al., 2019).

3.3. Dijital Mağdurların Ortak Özellikleri ve Psikososyal Etkileri

Dijital mağdurlar, teknolojinin günlük yaşamın her alanına nüfuz etmesiyle birlikte ortaya çıkan yeni bir toplumsal grubu temsil eder. Siber mağduriyet, bireyin yalnızca hukuki veya maddi kayıplarını değil, aynı zamanda psikolojik ve sosyal bütünlüğünü etkileyen çok yönlü bir süreçtir. Çeşitli araştırmalar, dijital mağdurların genellikle yüksek düzeyde çevrim içi etkinlik gösteren, sosyal medya kullanımı yoğun, duygusal olarak hassas veya sosyal destek düzeyi düşük bireyler olduklarını ortaya koymaktadır (Akcan & Öztürk, 2020). Bu özellikler, ceza hukuku bakımından mağdurun yalnızca suç sonrası değil, suç öncesi koruma uluslararası devletlerin egemenlik alanına giren uygulamalarıyla da desteklenmesi gerektiğini göstermektedir (Akcan & Öztürk, 2020).

Psikososyal açıdan dijital mağduriyetin etkileri, klasik mağduriyet türlerinden daha karmaşık yapıdadır. İnternetin anonim doğası nedeniyle mağdur, faille fiziksel bir temas kurmaz sürekli izlenme, ifşa edilme veya aşağılama kaygısı nedeniyle kronik stres, kaygı bozukluğu ve depresyon gibi sonuçlar yaşayabilir. Bu durum, mağdurların “ikincil mağduriyet” denilen adli süreçte yeniden zarar görmesini de kolaylaştırır (Gül et al., 2019). Dolayısıyla adli sistemin yalnızca suçun failine odaklanmaması; mağdurun psikolojik bütünlüğünü yeniden kuracak onarıcı adalet anlayışına dayalı mekanizmalar geliştirmesi önemlidir (Gül et al., 2019).

Uluslararası düzeyde yapılan araştırmalar, dijital mağdurların önemli bir kısmının gençler ve kadınlar olduğunu göstermektedir. Özellikle çevrim içi taciz, kişisel verilerin paylaşılması (doxing) veya manipüle edilmesi (deepfake) gibi olaylar, toplumsal cinsiyet temelli mağduriyetin dijital biçimlerini doğurmuştur. Hinduja ve Patchin (2019) çalışmalarında, çevrim içi taciz mağdurlarının büyük bir kısmında benlik saygısında düşüş ve sosyal izolasyon eğilimi tespit etmiş, buna rağmen güçlü sosyal destek ağlarının mağduriyetin psikolojik etkilerini azalttığını vurgulamışlardır. Bu bakış açısı, ceza uygulamaları açısından mağduru yalnızlaştırmaya, destek odaklı bir yaklaşımın önemini ortaya koyar (Hinduja & Patchin, 2019).

Psikolojik etkilerinin yanı sıra, dijital mağdurların ortak davranışsal tepkileri arasında çevrim içi ortamlardan geri çekilme, sosyal güven kaybı ve dijital platformlara karşı genel bir güvensizlik hissi yer almaktadır. Ancak literatürde olumlu bir eğilim de mevcuttur: farkındalık

eğitimleri ve dijital okuryazarlık programlarının mağduriyet sonrası toparlanma sürecine katkı sağladığı gözlenmiştir. Dijital mağdurların çevrim içi güvenlik stratejileri geliştirdiklerinde yeniden mağduriyet riskinin azaldığını ve psikolojik dayanıklılığın arttığını göstermiştir. Bu durum, hukuk sistemin yalnızca cezalandırıcı değil, önleyici ve iyileştirici rolünün de ne kadar önemli olduğunu doğrular (Reyns & Henson, 2022).

Sonuç olarak dijital mağdurların ortak özellikleri arasında yüksek çevrim içi görünürlük, düşük sosyal destek, psikolojik kırılganlık ve dijital farkındalık eksikliği sayılabilir. Ancak modern ceza hukuku yaklaşımı, bu özellikleri cezai zafiyet değil, koruma ihtiyacı olarak değerlendirilmektedir. Ceza adalet sisteminin psikososyal destek mekanizmalarıyla bütünleşmesi, mağdurların güven duygusunu yeniden tesis ederek dijital çağda insan onurunu korumaya yönelik umut verici bir yönelim sunmaktadır (Reyns & Henson, 2022).

3.4. Mağdur Hakları Perspektifinden Dijital Mağduriyet

Dijital mağduriyet, yalnızca bireysel bir zarar biçimi değil, aynı zamanda mağdur haklarının dijital çağda yeniden tanımlanmasını gerektiren bir adalet sorunudur. Ceza hukuku bağlamında mağdur haklarının temel amacı, mağdurun korunması, onarılması ve adalete erişimin güvence altına alınmasıdır. Bu çerçevede dijital mağdurların hakları, klasik mağduriyet biçimlerinden farklı olarak hem veri güvenliği hem de kişisel mahremiyetin korunmasını içerir. Maras'a göre dijital çağda mağduriyetin tanınması, yalnızca ceza normlarıyla değil; sosyal destek, adli bilişim ve restoratif adalet uygulamalarıyla birlikte düşünülmelidir (Maras, 2021).

Uluslararası hukukta dijital mağdurların korunmasına yönelik önemli gelişmeler yaşanmıştır. Avrupa Konseyi'nin **Budapeşte Sözleşmesi(2001)**, dijital suç mağdurlarının korunmasını taraf devletlerin yükümlülüğü haline getirmiştir. Bu düzenleme, devletlerin yalnızca cezalandırma değil, mağdurun zararını giderme ve yeniden mağduriyetin önlenmesi yönünde adımlar atmasını öngörür. Holt'a göre bu yaklaşım, siber suçla mücadelede insan merkezli bir anlayışın yerleşmesi açısından dönüm noktası niteliğindedir (Holt, 2022).

Dijital mağdur hakları perspektifi, yalnızca mağdurun pasif konumunu tanımlamakla kalmaz; onu adalet sürecinin aktif bir öznesi haline getirir. Mağdurların adalete erişim süreçlerinde bilgilendirilme, desteklenme ve karar verme süreçlerine katılma haklarının güçlendirilmesinin hem psikososyal iyileşmeyi hem de toplumsal güveni artırdığını vurgulamaktadır. Bu nedenle

dijital mağduriyet, ceza hukuku bakımından yalnızca önlenmesi gereken bir olgu değil; aynı zamanda bireyin onurunu ve adaletin kapsayıcılığını koruyan bir hak alanıdır (Reyns & Henson, 2022).

4.DİJİTAL MAĞDUR HAKLARININ KORUNMASI

4.1. Ulusal Hukukta Dijital Mağdur Hakları (TCK, CMK ve İlgili Mevzuat)

Türkiye’de dijital mağdur haklarının korunması, TCK ve CMK hükümleriyle desteklenen bütüncül bir yapıya sahiptir. TCK’nın 134 ve 243- 245. Maddeleri, bireylerin dijital ortamda özel hayatın gizliliğini, veri güvenliğini ve bilişim sistemleri üzerindeki haklarını korumaktadır. CMK m. 234 ve 236 ise mağdurun ifade verme, delil sunma ve psikolojik destek alma haklarını güvence altına alır. Bu düzenlemeler, dijital çağda insan onurunu ve adalete erişimi güçlendiren çağdaş bir koruma sisteminin temellerini oluşturur (Dülger, 2021; Erbaş, 2019).

4.2. Uluslararası Hukukta Dijital Mağdur Hakları (Budapeşte Sözleşmesi, AB Yönergeleri)

Uluslararası hukukta dijital mağdurların korunması, özellikle **Budapeşte Sözleşmesi (2001)** ve **Avrupa Birliği Mağdur Hakları Direktifi (2012/29/EU)** çerçevesinde kurumsal temele kavuşmuştur. Budapeşte Sözleşmesi, dijital suç mağdurlarının zararlarının giderilmesini ve adalete erişimini taraf devletlere yükümlülük olarak getirir. AB yönergesi mağdurlara bilgi edinme, psikososyal destek ve adli süreçlere katılım hakkı tanır. Bu belgeler, mağdur haklarını dijital çağın ihtiyaçlarına uyarlayan insan odaklı bir ceza hukuku anlayışını yansıtır (Holt,2022; Council of Europe, 2001).

4.3. Dijital Mağdurlara Yönelik Destek Mekanizmaları

Dijital mağdurların korunmasında yalnızca cezai yaptırımlar değil, psikososyal ve hukuki destek mekanizmaları da kritik öneme sahiptir. Türkiye’de Mağdur Hakları Daire Başkanlığı, dijital suç mağdurlarına ücretsiz psikolojik danışmanlık, hukuki bilgilendirme ve yönlendirme hizmeti sunmaktadır. Ayrıca, Adli Destek ve Mağdur Hizmetleri Daire Başkanlığı bünyesinde oluşturulan merkezler, mağdurların ikincil mağduriyet yaşamadan sürece katılımını sağlar. Avrupa Birliği uyum sürecinde geliştirilen bu sistem, mağduru pasif bir konumdan çıkararak, adalet sürecinin aktif bir öznesi haline getirmeyi hedefler (Özcan, 2023; Erbaş, 2019).

4.4. Koruma Mekanizmalarının Etkinliđi ve Yetersizlikleri

Uluslararası hukukta mağdur hakları giderek güçlenmiştir. **Budapeşte Sözleşmesi(2001)** ve **AB Mağdur Hakları Direktifi (2012/29/EU)**, dijital mağdurlara adalete erişim, tazmin ve destek imkanı sağlayarak mağdur -merkezli bir yaklaşımın temelini oluşturur (Council of Europe, 2021;European Parliament & Council, 2012).

5.DİJİTAL SUÇLARLA MÜCADELE VE MAĞDUR ODAKLI POLİTİKALAR

5.1. Türk Ceza Adalet Sisteminde Dijital Suçlarla Mücadele

Türk Ceza Adaleti sistemi, dijital suçlarla mücadelede son yıllarda önemli bir kurumsal dönüşüm geçirmiştir. TCK'nın 243-245. Maddeleri bilişim sistemlerine yönelik suçları kapsamlı biçimde düzenleyerek, hem bireyleri hem kamu güvenliğini koruma altına almıştır. Ayrıca CMK ise dijital delillerin hukuka uygun biçimde toplanması ve mağdurun korunması açısından temel usul güvencelerini içermektedir (Dülger, 2021).

5.2. Dijital Delil Elde Etme ve Değerlendirme Süreçleri

B Dijital delillerin güvenli şekilde toplanması ve mahkemede değerlendirilebilmesi, modern ceza adaletinin en güçlü yönlerinden biridir (Maras, 2021).

5.3. Mağdur Odaklı Ceza Politikalarının Önemi

Dijital suçlarla mücadelede mağduru merkeze alan uygulamaların, ceza hukukunun onarıcı işlevini yeniden tanımladığını belirtmektedir (Maras, 2021).

5.4. Koruyucu ve Önleyici Tedbirler

Ulusal siber güvenlik stratejilerinin mağduru koruyan, veri gizliliğini önceleyen uygulamalarla desteklenmesi gerektiğini belirtmektedir (Maras, 2021).

SONUÇ

Dijitalleşme, toplumsal yaşamın her alanını dönüştürdüğü gibi suç ve mağduriyet kavramlarını da yeniden şekillendirmiştir. Bu çalışma, dijital suçların ve dijital mağduriyetin ceza hukuku açısından doğurduğu yeni sorunları, aynı zamanda bu sorunlara yönelik geliştirilen koruyucu ve onarıcı uygulamaları incelemiştir. Türk Ceza Hukuku ve uluslararası düzenlemeler birlikte değerlendirildiğinde, hukukun dijital çağın risklerine karşı güçlü bir uyum sürecine girdiği görülmektedir.

TCK ve CMK'daki düzenlemeler, bireylerin dijital ortamlarda özel hayatının, kişisel verilerinin ve psikolojik bütünlüğünün korunması bakımından çağdaş bir güvence mekanizması oluşturmuştur. Uluslararası düzeyde Budapeşte Sözleşmesi ve AB Mağdur Hakları Direktifi, dijital mağdurlara ilişkin insan odaklı yaklaşımı güçlendirmiştir. Bu düzenlemeler, cezalandırmanın ötesinde, mağdurun onarımı, bilgilendirilmesi ve yeniden topluma kazandırılması anlayışını merkeze almıştır (Holt, 2022; Maras, 2021).

Geleceğe dömük olarak, dijital suçlarla mücadelede önleyici adalet uygulamalarının, dijital farkındalık eğitimlerinin ve mağdur destek hizmetlerinin yaygınlaştırılması büyük önem taşımaktadır. Ceza hukuku, yalnızca dijital tehditlere karşı koruyucu bir kalkan değil, aynı zamanda bireyin onurunu, güvenliğini ve adalete olan inancını koruyan bir sistem olarak güçlenmelidir. Böylece dijital çağın getirdiği riskler, insan haklarına dayalı bir hukuk düzeni içinde yönetilebilir hale gelecektir (Reyns & Henson, 2022).

KAYNAKÇA

- [1] Akcan, G., & Öztürk, E. (2020). *The investigation of predictors of cyber bullying and cyber victimization in university students*. Türkiye Klinikleri Journal of Forensic Sciences and Legal Medicine, 17(1), 47–57.
- [2] Aksoy Retornaz, E. (2021). *5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Hakkındaki Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu*. Ceza Hukuku Dergisi, 16(45), 9–32.
- [3] Altinyüzük Avukatlık Bürosu. (2024). *Bilişim Suçları: Türk Ceza Kanunu m. 243–244*. Altinyüzük Avukatlık Bürosu İnceleme Yazısı.
- [4] Aydın, M. (2023). *Ceza Hukukunda Mağdur Kavramı, Mağdur Hakları ve Mağdurun İkincil Mağduriyetten Korunması*. On İki Levha Yayınları.
- [5] Bossler, A. M., & Holt, T. J. (2010). *The effect of self-control on victimization in the cyberworld*. Journal of Criminal Justice, 38(3), 227–236.
- [6] Brenner, S. (2010). *Cybercrime: Criminal threats from cyberspace*. ABC-CLIO.
- [7] Calo, R. (2015). *Robotics and the lessons of cyberlaw*. California Law Review, 103(3), 513–563.
- [8] Çetin, M. S. (2021). *Yargıtay Kararları Işığında Bilişim Sistemine Girme ve Kalma Suçu (TCK m. 243)*. Türkiye Adalet Akademisi Dergisi, 45, 1–28.
- [9] Çimen, İ. D. (2024). *Cyber victimization, coping methods and attitudes of the family toward internet use in adolescents during the COVID-19 pandemic*. Turkish Journal of Child and Adolescent Psychiatry and Mental Health.
- [10] Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*. Strasbourg: Council of Europe.
- [11] Council of Europe. (2023). *Turkey – State of cybercrime legislation*. Octopus Cybercrime Community.
- [12] Dülger, M. V. (2016). *Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması*. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3(2), 101–168.
- [13] Dülger, M. V. (2021). *Kişisel Verilerin Korunması Kanunu ve Ceza Hukuku İlişkisi*. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 7(2), 145–168.
- [14] Erbaş, R. (2019). *Ceza Muhakemesi Hukukunda Mağdurun Korunması ve Hakları*. Ankara Üniversitesi Hukuk Fakültesi Dergisi, 68(1), 55–78.

- [15] European Parliament & Council. (2012). *Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime*. Official Journal of the European Union.
- [16] Gazi Üniversitesi Hukuk Fakültesi Dergisi. (2010). *Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)*. XIV(2), 279–304.
- [17] Griffith, C. E., et al. (2023). *Understanding the cyber-victimization of young people*. Journal of Criminal Justice.
- [18] Gül, H., et al. (2019). *Cyber-victimization among a clinical adolescent sample: Associations with mental health, socio-economic status, and family factors*. *Psychiatry and Psychopharmacology*.
- [19] Hinduja, S., & Patchin, J. W. (2019). *Cyberbullying: Identification, prevention, and response* (2nd ed.). Cyberbullying Research Center.
- [20] Holt, T. J. (2018). *Cybercrime and digital forensics: An introduction*. Routledge.
- [21] Holt, T. J. (2022). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge.
- [22] İnce Tunçer, A. (2024). *Yasak Cihaz ve Programlar Suçu (TCK m. 245/A)*. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 32(3), 1297–1337.
- [23] Jewkes, Y., & Yar, M. (2019). *Cybercrime and society* (3rd ed.). Sage Publications.
- [24] Karaca, M., & Gencer, T. M. (2021). *Siber mağduriyet: Kavramsal bir çalışma*. Anadolu Akademi Sosyal Bilimler Dergisi, 3(1), 177–191.
- [25] Karadeniz, Y. (2022). *Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Türk Hukukunda Karşılığı*. Güvenlik Bilimleri Dergisi, 11(1), 109–134.
- [26] Kaşlı, E. (2022). *Kolluk uygulamalarında suç mağdurunun korunması*. Sakarya Üniversitesi Hukuk Fakültesi Dergisi, 10(2), 819–838.
- [27] Koçak, U. A. (2022). *Kişisel Veri İhlallerinin Türk Ceza Kanunu Kapsamında Değerlendirilmesi*. TBB Dergisi, 163, 83–102.
- [28] Maras, M. H. (2016). *Computer forensics: Cybercriminals, laws, and evidence* (2nd ed.). Jones & Bartlett Learning.
- [29] Maras, M.-H. (2020). *Cybercriminology*. Oxford University Press.
- [30] Maras, M.-H. (2021). *Cybercriminology* (2nd ed.). Oxford University Press.
- [31] Meral Ekici, Ş., & Şahin Irmak, A. (2019). *Kişisel Veri İşleme Kavramı Üzerine Değerlendirme (KVKK m. 3)*. Dokuz Eylül Üniversitesi Hukuk Fakültesi Yayını.

- [32] Noble, S. U. (2020). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.
- [33] Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). *Conceptualizing cybercrime: Definitions, typologies and taxonomies*. *Forensic Science*, 2(4), 379–398.
- [34] Reyns, B. W. (2013). *Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses*. *Journal of Research in Crime and Delinquency*, 50(2), 216–238.
- [35] Reyns, B. W., & Henson, B. (2022). *Preventing cyber-victimization: Evaluating the role of digital literacy and online safety behaviors*. *Crime & Delinquency*, 68(4), 601–623.
- [36] Robalo, T. L. A. S., et al. (2023). *Cyber Victimization, Restorative Justice and Victim Offender Community Mediation*. *The Journal of Criminal Law and Criminology*.
- [37] Şenol, C. (2025). *7545 sayılı Siber Güvenlik Kanunu'nda düzenlenen suçlar*. *Türkiye Adalet Akademisi Dergisi*, 63, 169–206.
- [38] Turgut, B. (2025). *Siber uzayda yer alan kişisel veya kritik kamu hizmeti kapsamına giren kurumsal verileri erişime açma, paylaşma ve satışa çıkarma suçu*. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 16(1), 207–220.
- [39] United Nations Office on Drugs and Crime (UNODC). (n.d.). *Cybercrime in Brief*. UNODC Website.
- [40] Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- [41] Wall, D. S. (2021). *Cybercrime: The transformation of crime in the information age* (2nd ed.). Polity Press.
- [42] Yar, M. (2014). *Cybercrime and society* (2nd ed.). Sage Publications.
- [43] Yücel, E. (2025). *Türkiye'nin Siber Güvenlik Yaklaşımı ve 7545 Sayılı Siber Güvenlik Kanunu Üzerine Bir Değerlendirme*. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 33(3), 1849–1879.