SİBER SUÇLAR, SOSYAL MEDYA VE SİBER ETİK

Gönül CENGİZ
Gaziantep Üniversitesi, Türkiye
gonulcengiz88@gmail.com
https://orcid.org/0000-0001-6685-5376

Atıf	Cengiz, G. (2021). SİBER SUÇLAR, SOSYAL MEDYA VE SİBER ETİK. İletişim Çalışmaları Dergisi, 7 (3), 407-424.

Geliş tarihi / Received: 15.05.2021

Kabul tarihi / Accepted: 05.07.2021

DOI: *10.17932/IAU.ICD.2015.006/icd_v07i3001*

ÖZ

1990'ların ortalarından beri internet, dünya çapında insanların bir yaşam gerçeği hâline gelmiştir. Bu durum beraberinde siber dünyadaki kullanıcılar için yeni risklerin oluşmasına neden olmuştur. İnternetin hızlı yayılımı suç unsurlarını yeniden şekillendirmiş ve onları elektronik ortama taşıyarak yeni boyut kazandırmıştır. Bu bağlamda çalışmanın amacı, siber suç kavramını açıklamak, sosyal medyadaki suçların tanımlarını yapmak ve siber dünyadaki etik durumlarını incelemektir. Aynı zamanda çalışmanın amacının daha iyi anlaşılması için dijital suçlar sınıflandırılarak belirli gruplara bölünmüştür.

Çalışmamızın problemi, sosyal medyanın içinde bulunduğu siber dünyadaki endişeye neden olan dijital suçlara ve bu suçlarda ihlal edilen etik konusuna odaklanmıştır. Aynı zamanda sosyal medyanın çevrim içi suçları yeniden nasıl şekillendirdiği de araştırma problemi kapsamına girmektedir. Çalışmada dijital toplum, denetim, gözetim ve dijital kültür gibi başlıklara da yer verilerek siber dünyadaki suçları önlemek için kullanılan kontrol mekanizmalarına da değinilmiştir.

Çalışmada geniş veri hazinesine sahip dijital dünyada sosyal medya kullanıcılarının sayısının gün geçtikçe arttığı bu durumda siber etik kurallarının yetersiz kaldığı ve siber suçlara dair yeni hukuki düzenlemelerin yapılması sonucuna varılmıştır.

Anahtar Kelimeler: *Siber Suçlar, Sosyal Medya, Siber Etik.*

CYBERCRIME, SOCIAL MEDIA AND CYBER ETHICS

ABSTRACT

Since the mid-1990s, the internet has become a reality of life for people around the world. This situation has created new risks for users in the cyber world. The rapid spread of the Internet has reshaped the criminal elements and brought them to a new dimension by moving them to the electronic environment. In this context, the aim of the study is to explain the concept of cybercrime, to define the crimes in social media and to examine their ethical situation in the cyber world. At the same time, digital crimes are classified and divided into specific groups in order to better understand the purpose of the study.

The problem of our study is focused on digital crimes that cause anxiety in the cyber world of social media and the ethics violated in these crimes. It is also within the scope of the research problem how social media reshapes online crimes. In the study, the control mechanisms used to prevent crimes in the cyber world are also mentioned, including titles such as digital society, control, surveillance and digital culture.

In the study, it was concluded that the number of social media users in the digital world, which has a large data treasure, is increasing day by day, and that the rules of cyber ethics are insufficient and new legal regulations regarding cybercrimes are made.

Keywords: *Cybercrime, Social Media, Cyber Ethics.*

GİRİŞ

İnsanın bulunduğu tüm alanlarında bilgi ve iletişim teknolojisi sistemlerinin kullanımı bilinmekte ve yaygın olarak kabul görmektedir. Öte yandan, bilgi sistemleri daha çeşitli insan faaliyetlerini mümkün kılmaktadır. Örneğin, günlük faaliyetlerin hızını artırmakta, insanların yeni ve genellikle daha faydalı ilişkiler geliştirmesine ve sürdürmesine olanak tanımakta, kuruluşların yapısını etkilemekte, satın alınan ürünlerin türünü değiştirmekte ve işin doğasını etkilemektedir. Bu anlamda enformasyon ve bilgi, hayati ekonomik kaynaklar hâline gelmektedir. Bu durumun sonucu olarak da yeni fırsatlarla birlikte, bilgi sistemlerinden sürekli yararlanma ihtiyacı yeni tehditleri de beraberinde getirmektedir. Zwass'a (URL-1) göre, yoğun endüstri inovasyonu ve akademik araştırmalar, tehditleri kontrol altına almayı hedeflerken sürekli olarak yeni fırsatlar geliştirmektedir. Bu bağlamda sıklıkla rastlanan sorunlardan biri siber saldırılardır. Siber saldırılar genellikle "bilgisayar korsanlarının bir bilgisayar

ağına veya sistemine zarar verme veya yok etme girişimi" olarak tanımlanır (Oxford Dictionary, 2018).

Dijitalleşen toplumsal boyutla beraber geleneksel suçlar da dijital ortama taşınarak siber suç başlığı altında değerlendirilmektedir. Siber suçlar, bilgisayar korsanlığı, virüs ve diğer istismar türlerinde sürekli artışla birlikte artık büyük bir uluslararası sorun olarak kabul edilmektedir. Siber suçlarla ilgili terminoloji kabul edilse de gerçekte ne anlama geldiği yeterince anlaşılmadığı için etik sorunları da beraberinde getirmektedir. Ağ bağlantılı bilgisayar sistemleri daha geniş coğrafyalara yayıldıkça, dünyadaki suç ve taciz olayları da artmaktadır.

Bilişimin ortaya çıktığı ilk dönemlerde, geleneksel suçlardan olan dolandırıcılık ve hırsızlık siber görünüm kazanmıştı. Kurt'un da (2005: 157) belirttiği üzere, toplum tarafından duyulan ilk siber suç, 18 Ekim 1966 tarihinde *Minneapolis Tribune* dergisinde yayınlanan "Bilgisayar uzmanı, banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile insanlara duyurulmuştur.

Kriminolojik açıdan siber suçların failleri geleneksel suçlulara nazaran ya bulunamamaktadır ya da bulunma olasılıkları çok düşüktür. Yakalanma risklerinin az olduğunu bilen siber suçlular caydırıcı cezalardan da çekinmemekteler. Bu bağlamda siber suçluların genel özelliklerinden bahseden Yılmaz ve Güllüpınar'a (2020) göre;

Hackerların yaş ortalamasının 14 - 21 yaş arasında olduğu ve genel itibariyle bilişim suçu faillerinin yaş ortalamalarının düşük olduğu bilindiğinden, yine yaşlılara göre caydırıcılıktan etkilenmeleri oranı düşüktür. Ayrıca, faillerin büyük çoğunluğunun erkek olmasından dolayı da kadınlara göre caydırmaya yönelik faktörlerden etkilenmeleri düşüktür. Sosyoekonomik durumları genelde geleneksel suçlardaki gibi düşük değildir. Bu özellikleriyle caydırılma oranları yüksektirler. Genel itibariyle bilişim suçu failleri özellikleri caydırıcı etkinin çok fazla etkili olmadığı bir profil çizmektedir.

Teknolojik gelişmelerle birlikte ortaya çıkan sosyal medya kavramı hızla toplumun tüm kesimlerine yayılmakta ve bu durum tüketim kültüründe önem kazanmaktadır. Tek taraflı düşünceyi dayatan sosyal medyanın tüketim kültürüne hizmet etme işlevselliği, gözetim kavramına dayalı panoptikon yaklaşımıyla örtüşmektedir. Demir'in (2017: 57) de belirtiiği gibi panopticon, insan zihni üzerinde bir güç olarak görülürken, teknolojinin gelişmesiyle birlikte insan davranışlarını kontrol altında tutmuş ve toplumsal kontrole karşı olmayan bireylerin oluşmasını hedeflemiştir. Bu anlamda dijital gözetim ile bireylerin kişisel bilgileri kayıt altına alınmakta ve bireyler bu bilgilerin gönüllü dağıtıcısı olmaktadır. Böylece, dijital gözetimle beraber dijitalleşen toplumda işlenen suçlar da dijitalleşmekte ve sosyal medya bu suçların önemli zemini olarak görülmektedir (İsmayilzada, Topçu, 2019: 188).

SİBER SUÇ

Suç ve suçluluk kavramları tarih boyunca bireyle ilişkilendirmiştir. Farklı ülkeler, kültürlerine ve kapsamlarına bağlı olarak suçla mücadele etmek için farklı stratejiler benimsemiştir. Suç oranı yüksek olan ülkeler gelişimleri bağlamında zorlanmaktadırlar. Çünkü bu durum negatif sosyal ve ekonomik sonuç doğurmaktadır. Suç kavramına Freud bağlamında bakarsak, saldırgan veya yıkıcı insan eylemlerinin hem 'doğal' (id) hem de 'kültürel' (ben ve üst ben) gerekçeleri veya nedenleri vardır.

1990'ların ortalarından bu yana internet, dünya çapında, özellikle de sanayileşmiş Batı dünyasında yaşayanlar için yaşamın vazgeçilmez parçası hâline gelmiştir. Webster'in (2003) de belirttiği gibi, internet, aynı zamanda "küçülen" dünyamızda yaşamla bağlantılı yeni fırsatlar ve zorluklar yaratan küreselleşme sürecinin bir parçası olarak da görülmektedir. Bu durum, kontrolü zor olan siber dünyada tehlikeleri de beraberinde getirmektedir. İnternetin suç ortamı bağlamında düşünülmesinde kitle iletişim araçlarının önemli payı vardır (Yar, 2006: 4). Siber suçlardan bahsederken yerel suç durumları ile beraber bazen diğer ülkeleri de ilgilendiren sınır ötesi suçlara da rastlanmaktadır. Örneğin, insan ticareti, kaçakçılık, terörizm gibi evrensel sorunlar çatısı altında araştırılan suç türleri gösterilebilir.

Siber suç kavramı ile ilgili sınırları çizilmiş net bir tanım olmasa da birçok araştırmacı tarafından genel olarak birbirine yakın tanımlamalar yapılmıştır. Örneğin, Thomas ve Loader (2000: 3), siber suçu, "yasa dışı veya belirli taraflarca yasa dışı kabul edilen ve küresel elektronik ağlar aracılığıyla yürütülebilen bilgisayar aracılı faaliyetler" olarak kavramsallaştırır. Thomas ve Loader'in tanımı aynı zamanda suç (kanunen açıkça yasaklanmış ve dolayısıyla yasa dışı eylemler) ve sapkınlık (gayri resmi sosyal normları ve kuralları ihlal eden, dolayısıyla istenmeyen veya sakıncalı kabul edilen eylemler) arasındaki ayrıma da dikkat çekmektedir.

Siber suçlarla ilgili karşılaşılan sorunların başında faillerin bulunmasındaki zorluklar gelmektedir. İnternet ortamı sosyal kimliği manipüle ederek siber etkileşimleri arttırmakta ve bireylere kendilerini yeniden keşfetme imkânı sağlayarak onları 'gerçek dünyadaki' kimliklerinden uzak olan yeni sanal kişilere dönüştürmektedir (Poster, 1990). Bu durum kriminolojik açıdan, suçlunun bulunmasını da zorlaştırmaktadır.

SİBER SUÇ KATEGORİLERİ

En temel düzeyde, dijital (siber) suçlar basitçe bilgisayar kullanımını içeren suç türleri olarak yorumlanabilir. Parker (1998) ve Furnell (2002), bilgisayar ve siber suç kavramlarını birbirinden ayırmakta ve aşağıdaki tanımları sunmaktadır:

1. ‘Bilgisayar destekli suçlar’ (internet’ten önce gelen, ancak siber alanda yeni bir hayat süren suçlar, ör. dolandırıcılık, hırsızlık, kara para aklama, cinsel taciz, nefret söylemi, pornografi), failin bilgisayar teknolojisi hakkında özel bilgileri kullandığı bir suçtur.

2. ‘Bilgisayar odaklı suçlar’ veya ‘siber suçlar’ (internetin kurulmasıyla birlikte ortaya çıkan ve ondan ayrı var olamayan suçlar, örneğin, bilgisayar korsanlığı, viral saldırılar, web sitesi tahrifatı), failin özel siber alan bilgisini kullandığı suçtur.

Bu sınıflandırmaya göre, siber suçların alt bölümlere ayrılmasındaki önemi, teknolojinin, yani internetin suç bağlamında olası (internetsiz de başka yollarla yapılabilir) veya gerekli (İnternet olmadan böyle bir suç olamaz) bir rol oynayıp oynamadığına bağlıdır. Bu anlamda Wall (2001: 3-4), siber suçları dört kategoriye ayırmaktadır:

1. Siber izinsiz giriş - diğer insanların sınırlarını aşmak (özel alana girmek) veya hasara neden olmak. Örneğin, bilgisayar korsanlığı, virüsler.

2. Siber aldatma ve hırsızlık (para, mal). Örneğin, kredi kartı dolandırıcılığı, fikri mülkiyet ihlalleri.

3. ‘Cinsel açıdan ifade edici materyalin’ çevrim içi ticaretine atıfta bulunan ve cinsel sapkın ve fetiş alt kültürleri, seks işçiliği, seks kaçakçılığı ve seks turizminin yanı sıra çocuklara yönelik cinsel istismar materyallerini içeren siber porno ve müstehcenlik;

4. Bireylerin başkalarına zarar verebileceği çeşitli yollara atıfta bulunan siber şiddet: Bu tür zararlar arasında siber taciz, siber zorbalık ve olası terör eylemlerini destekleyen iletişimler (örneğin, ‘bomba konuşması’ veya patlayıcı ve diğer silahların yapımı için talimatların dolaşımı dâhil) yer alır.

Bu yasal kategorilerden ilk ikisi ‘mülke karşı suçları’, üçüncüsü 'ahlaka karşı suçları' ve dördüncüsü 'kişiye karşı işlenen suçları' kapsamaktadır. Aynı zamanda ilk kategori ‘bilgisayar odaklı’ eylemleri (yani makineye yönelik) temsil ederken, son üç kategori ‘bilgisayar destekli’ eylemler olarak tanımlanır (Smith, Grabosky, Urbas, 2004).

Siber suç kavramı ile ilgili bir diğer tanımlamayı Holt ve Bossler (2014) yaparken özellikle marjinalleştirilmiş ve azınlık topluluklara yönelik şiddet biçimleriyle ilgilenen siber suç türlerinin eksikliğinden söz etmektedirler.

Dijital suçların alt türlerini Furnell (2002) aşağıdaki tabloda daha detaylı tanımlanmıştır.

Tablo 1. Dijital Suç Türleri

Suç	**Tanımı**
Dolandırıcılık	Özel kazanç veya fayda için girişi yetkisiz bir şekilde değiştirmek; bilgisayar çıktılarını yok etmek / bastırmak / kötüye kullanmak; bilgisayarlı verilerin değiştirilmesi; programların değiştirilmesi veya kötüye kullanılması
Hırsızlık	Veri ve yazılım hırsızlığı. E-hırsızlığı önlemek için, çoğu büyük banka müşterilerinin çevrim içi yapabileceklerini sınırlamaktadır.
Lisanssız yazılım kullanımı	Yasa dışı yazılım kopyalarını kullanmak
Siber Terörizm	Terör eylemlerinin sanal ortamlarda teşviki
Özel iş	Özel kazanç veya menfaat için kuruluşun bilgi işlem olanaklarının izinsiz kullanımı
Kişisel verilerin kötüye kullanılması	Bilgisayar kayıtlarında resmi olmayan 'gezinme' ve veri koruma mevzuatının ihlalleri
Hacklemek	Genellikle iletişim olanaklarını kullanarak bir bilgisayar sistemine kasıtlı olarak yetkisiz erişim elde etmek.
Sabotaj	İşleme döngüsüne veya ekipmana kasıtlı zarar vererek bilgisayar sürecine müdahale etmek
Pornografik materyal tanıtmak	İnternetten indirerek pornografik materyallerin tanıtılması
Casusluk	Failler diğer şahıslara (suçlular) satmak amacıyla gizli bilgileri elde etmek için çevrim içi sistemlere veya kişisel bilgisayarlara saldırır.

Virüs	Bir bilgisayar sürecini bozmak amacıyla bir program dağıtma
Çevrim içi hizmet reddi	Çevrim içi hizmet reddi, çevrim içi bilgisayar sistemlerine zarar vermek veya bunları kapatmak için e-posta engellemelerinin, bilgisayar virüslerinin veya diğer tekniklerin kullanılmasıdır.

Kaynak: Furnell (2002)

DİJİTAL TOPLUM VE DİJİTAL GÖZETİM

Teknolojiyi toplumda ayrı bir alanda konumlandırmak yerine, 'dijital toplum', bu tür teknolojileri daha büyük sosyal varlığın (suç eylemi, mağduriyet ve adalet) yerleşik bir parçası olarak tanıyan ve dijital teknolojileri günlük yaşam pratiği olarak kabul eden bir kavramdır (Lupton, 2014). Chayko (2018) ise 'süper bağlantılı' (superconnected) kavramı ile önceki dönemlerden farklı olarak yeni 'tekno-sosyal yaşam' biçimleriyle karakterize edilen dijital topluma yönelik bir tanımla yapmıştır. Süper bağlantılı (superconnected) kavramı, demokrasilerin işleyişini tehdit eden 'sahte haberler' ve çevrim içi 'önemli siyasilere ait özel odalardan', dijital olarak aracılık edilen kumar ve tüketim biçimlerine nüfuz eden yeni bağımlılık biçimlerine kadar, dijital toplumu oluşturan konulara kapsamlı bir genel bakış sunar. Chayko (2018), bu kavramın kapsama alanının kamu yetkililerinin işini kolaylaştırdığını söylerken, diğer taraftan sürekli yenilenen dijital uygulamalarla da bu kavramın kuvvetlendiğini ve denetiminin zorlaştığını iddia etmektedir.

Demokratik ülkelerde devlet kurumları vatandaşlarla dijital teknolojiler aracılığıyla daha önce ulaşılamayan yollarla iletişim kurmaktadır. Goldsmith'e (2015) göre sosyal medyanın polis ve mahkemeler tarafından kullanılması adalet sistemine erişimi ve katılımı teşvik etse de, mahkeme sistemi geleneksel adalet sürecini olumsuz etkilemektir. Dijital toplum aynı zamanda suçla ilgili 'gayri resmi' adalet uygulamalarını ve toplumsal tepkileri de teşvik etmektedir.

Post-endüstriyel dijital toplum, yoğun bir sanallaştırma ile karakterize edilir. Çünkü çevre aslında gerçekçi özelliğini kaybederek insanlar için sanal hâle gelir. Bu tür sanallaştırmanın basit bir örneği, dijital toplumun üyesi / vatandaşı olan insanların davranış kalıplarıyla ilgilidir. Yani kişilerin çeşitli faaliyetlerindeki başarıları, insanların gerçekteki eylemlerinden ziyade, bir bilgisayar arayüzü aracılığıyla olaylara yeterli ve etkili bir şekilde tepki verme yeteneğine bağlıdır (Levin, 2014: 15).

Teknolojinin gelişmesiyle birlikte dijital toplumdaki denetlenenlerin sayısı giderek artmakta ve bireylerin özel bilgileri hem devlet hem de devlet dışı

organlar tarafından kayıt altına alınmaktadır. Parmak izi okumalarından çipli veya biyometrik kartlara kadar birçok teknoloji, insanların her anının kayıt altına almasını ve gözetlemesini sağlamaktadır. Bu durum beraberinde dijital okuryazarlık mevusunu da gündeme getirmektedir. Santos and Serpa'nın (2018) tanımına göre, "dijital okuryazarlık, bireylerin dijital kaynakları tanımlamak, erişmek, yönetmek, entegre etmek, değerlendirmek, analiz etmek ve sentezlemek, yeni bilgiler oluşturmak, medya ifadeleri oluşturmak ve başkalarıyla iletişim kurmak için dijital araçları ve olanakları uygun şekilde kullanma farkındalığı, tutumu ve yeteneğidir". Sosyal medya kullanıcılarının dijital okuryazarlık seviyelerindeki artışlar dijital toplumu olumlu yönde etkilemektedir.

Dijital kültür etkileşimi artırmakla beraber dijital katılımı da hızlandırmaktadır. Prins (2011), dijital katılımın kendi kendine yardım ve kendi kendine aktivizm için yeni uygulamaları nasıl kolaylaştırdığı, mağdurların refahına ve mahremiyetine yönelik artan tehdit potansiyelini dijital suç bağlamında araştıran 'e-kurban bilimi' (e-victimology) alt türüne dikkat çekmektedir.

Dijitalleşme, toplumlarda gözetimi de kolaylaştırmaktadır. Çetin ve Asıl'a (2017) göre dijital gözetim, kişisel bilgilerin teknolojik yollarla toplanmasıdır. Dijital teknolojiler, devlet onaylı gözetimin gerçekleşmesi için fırsatları arttırmaktadır. Bu durum adalet sistemlerindeki güç temsilcilerinin giderek daha fazla izlendiği, belgelendiği, eylemleri ve davranışları için sorumlu tutulduğu dijital bir yolla karşı gözetlemeleri de yaygınlaştırmaktadır (Bradshaw, 2013).

Lyon'a (2007: 14) göre günümüzde gözetim, hükümet yetkililerini, şirketleri ve bireyleri etkilemek, yönetmek, korumak veya yönlendirmek için kişisel ayrıntılara odaklanan sistematik ve rutin bir teknik olarak ortaya çıkmıştır.

Gözetim kavramına sosyal medya perspektifinden bakınca bu medyanın sosyal protesto hareketleri, siyasi aktivistler tarafından bilgi yayma ve sosyal koordinasyon aracı olarak kullanılması, sadece baskıcı devletler tarafından yoğun çevrim içi gözetleme ile sonuçlanmamış, aynı zamanda sosyal medyanın kullanımının toptan yasaklanmasına (Çin, İran, Kuzey Kore gibi) da neden olmuştur.

Dijital gözetimin bir diğer bouyutu da mahremiyetin ifşasıdır. Her kesimin rahatlıkla erişebileceği sosyal medya araçları ile kişilerin mahremiyetinin herkes tarafından izlenmesi söz konusu ve bu durum her zaman güvenli olmamaktadır. Dolayısıyla güvenli olmayan bir gözetim, kişisel verilerin çalınması, özel hayatın izinsiz ifşası gibi siber suçların işlenmesine yol açmaktadır.

SOSYAL MEDYA VE SUÇ

Sosyal medya, insanların kültürel, ekonomik ve sosyal hayatını etkilemekte ve hayatın vazgeçilmez bir parçası hâline gelmektedir. Soomro ve Hussain'e (2019:

15) göre, sosyal medya platformlarının popülaritesi, 2019 yılında 2,22 milyar olan kullanıcı kitlesinin 2021'de 3,02 milyara ulaşması beklenen kullanıcı kitlesi ile ölçülmektedir. Bu bağlamda sosyal medya, geniş kullanıcı sayısı ile büyük sosyal veri üretmektedir. Kolay ulaşılan veriler güvenlik açığı zorluğunu da beraberinde getirmektedir. Sosyal medya özellikle siber taciz ve siber kimlik hırsızlığı gibi suçlar için potansiyel hedef hâline gelmektedir. Sosyal ağlara kaydolurken kullanıcının doğum tarihi, doğum yeri, ev adresi, medeni durumu ve aile üyelerinin isimleri gibi 'özel bilgilerinin' yasa dışı kullanımını gerektiren kimlik hırsızlığıyla ilgili özel riskler ortaya çıkmaktadır (Smith, 2010: 277). Bu tür bilgiler, finansal hizmet sağlayıcıları (bankacılık, krediler ve kredi kartları gibi) tarafından kimliği doğrulamak için sıklıkla kullanılmakta ve bu tür ayrıntıların sosyal medya aracılığıyla paylaşılması, dolandırıcılık için zengin veri kaynağı sunmaktadır. Bu anlamda Facebook ve Twitter gibi sosyal medya kullanıcılarının, kullanıcı olmayanlara göre kimlik hırsızlığının kurbanı olma olasılıkları daha yüksektir ve aynı zamanda mağdur olma riskinin, bireylerin aktif kullanıcı olma süresi uzadıkça arttığı da görülmektedir (Yar, 2012: 214). Sosyal medya aracılığıyla açıklanan bilgiler, geleneksel çevrimdışı suçların işlenmesini kolaylaştırmak için de kullanılabilir. Örneğin, seyahat planlarını paylaşan (tatile gitmek gibi) veya gerçek zamanlı konumlarını etiketleyen (Foursquare gibi konuma dayalı hizmetlerden sosyal medya güncellemeleri yoluyla) kullanıcılar gerçek dünyada hırsızlar için fırsatlar sunabilmekteler.

Sosyal medya sadece bir iletişim aracı değil, aynı zamanda bu ortamdaki etki-tepki süresinin hızlı olmasından dolayı suç dünyası için de önemli araç hâline gelmiştir. Diğer taraftan, sosyal medya, kolluk kuvvetlerinin suçu önlemesi için de başvurulan araçtır.

Facebook, Twitter ve YouTube gibi sosyal medya sitelerinin milyonlarca aktif kullanıcısı vardır ve bu web sitelerini kullanarak insanlar birbirleriyle anında iletişim sağlamaktırlar. Ulusal Beyaz Yaka Suçları Merkezi'nin "Sosyal Medyanın Suçlu Kullanımı" raporuna göre sosyal medya bağlamında altı suç türünden söz edilebilir (NW3C, 2013):

1) Sosyal ağ üzerinden hırsızlık,

2) Sosyal sahtekârlık ve kimlik avı,

3) Kötü Amaçlı Yazılım,

4) Kimlik hırsızlığı,

5) Siber taciz,

6) Siber yer tespiti.

Sosyal ağlar üzerinden hırsızlık

Suçlular potansiyel hırsızlık hedefleri için sosyal medyaya yönelmektedir. Sosyal medya kullanıcıları genellikle yenilen akşam yemeği veya gidilen tatil yerleri gibi kişisel aktivitelerini takipçileri ile paylaşmaktadırlar. Bu paylaşımlar hırsızları hareket geçirmekte ve hedeflerine yönelmeyi kolaylaştırmaktır.

Sosyal sahtekârlık ve kimlik avı

Sosyal ağ kullanıcıları arkadaşlarından acil mali yardım talep eden mesajlar alabilmektedir. Sosyal medya hesabının çalınması sonucu şüpheli olan kişiler o hesapta var olan tüm arkadaşlara maddi anlamda mesaj atarak yardım istemektedir. Bu bağlamda bilgisayar güvenlik firması Trend Micro, doğası gereği kolay olduğu için Facebook'u 'dolandırıcılık mayın tarlası' olarak adlandırmaktadır (Soomro, Hussain, 2019: 10).

Kötü amaçlı yazılım

Soomro ve Hussain'e (2019: 11) göre, sosyal medya, virüsleri ve kötü amaçlı yazılımları yaymak için harika bir platform olarak görülmektedir. Reklam yazılımı, kötü amaçlı yazılım ve virüs geliştiriciler, sosyal medya sitelerinde verilen bağlantılarda, eklerde ve mesajlarda 'yıkıcı' programlarını gizlemektedir. Kullanıcıların bilmeden tıkladığı her link siber hırsızlar için önemli av olarak görülmektedir.

Kimlik hırsızlığı

Araştırmacılar, kimlik hırsızlığını, bir suç faaliyeti nedeniyle bireyin kişisel bilgilerini alma girişimi olarak tanımlamaktadır (Dadkhah, Lagzian, Borchardt, 2018: 288). Araştırma, kimlik hırsızlığını mağdurun kişisel bilgilerinin herhangi bir yasal yetki olmaksızın kasıtlı olarak cezai amaçla kullanılması olarak algılar.

Siber taciz

Sosyal medyayı kullanarak mağduru taciz etmek ve duygusal kaygı duygularına neden olabilecek gizli takip siber taciz olarak tanımlanmaktadır (NW3C, 2015). Moore'ya (2018) göre, çoğunlukla 18-29 yaş arası kadınlar siber taciz mağdurudur.

Siber Yer Tespiti

Ulusal Beyaz Yaka Suçları Merkezi'nin Sosyal Medyanın Suçlu Kullanımı Raporu (2013), siber yer tespitini, çevrim içi kaynaklarda bulunan çeşitli verileri kullanarak gerçek dünya konumunu üretmek için kullanılan bir süreç olarak açıklamaktadır. Sosyal medyanın son yıllarda öne çıkan özelliklerden biri de coğrafi konum etiketlemeleridir. Mobil uygulamaların yaygın kullanımı konum etiketleme durumunu da kolaylaştırmaktadır (Saariluoma, Sacha, 2014).

Kurbanın konumunu kolayca takip etmek işlenecek suç sürecini de hızlandırmaktadır.

Sosyal medyadaki suçlardan bahsederken bu mecralarda işlenen suçların önlenmesinin ve anında müdahale edilmesinin zor olduğu bilinmektedir. Hâl böyle olunca insan davranışlarından bahseden etik kavramına başvurulmaktadır. Sosyal medyadaki etik konusu son dönem dijitalleşen toplum tartışmalarının başında gelmektedir. Her yaştan, her kesimden, her sınıftan insanların rahatça eriştiği bir sosyal ağ olarak en çok görülen etik ihlallerden biri hakarettir. Örneğin, Facebook gibi hem fotoğraf hem video hem de yazı paylaşımı yapılan sosyal medya ortamında kullanıcılar yapılan yorumlar nedeniyle birbirlerine hakaretler etmekte ve hatta bazı durumlarda bir taraf diğer tarafı ölümle tehdit etmektedir. Bu durumun yaşanmasının önemli sebepleri arasında sanal kimliklere sahip kullanıcıların ekranların arkasına saklanarak güvenliklerinin tehlikede olmadıklarını düşünmeleridir. Mavnacıoğlu'na (2009: 71) göre, sosyal medya, kullanıcı odaklı olduğu için bazı etik dışı sorunlar hukuki boyutlara taşınmamaktadır. Etik dışı davranışlar, ticari konularda, telif hakları ve kişilik haklarına saldırı durumlarında hukuki boyuta taşınmaktadır (akt. Öztürk, 2015: 306).

Sosyal medya bağlamında etik sorunların nedenlerini Binark ve Bayraktutan'dan (2013: 113-115) aktaran Öztürk'e (2015: 305) göre;

- Politik nedenler: Bu nedenlerin kaynağı olarak iktidar/güç mücadelesine dikkat çekilmektedir. Sahip oldukları iktidarı/gücü kaybetmemek için çıkarları doğrultusunda sosyal medyaya sansür veya denetim uygulayanlar ve bu yolla kontrolü sağlamayı düşünenler etik ihlallerin yaşanmasına yol açmaktadırlar.

- Ekonomik nedenler: Yeni medya teknolojilerinin yönetimine sahip kapitalist girişimciler sosyal medyadaki etik ihlallerin ekonomik nedenlerini oluşturmaktadır. Kullanıcıların yoğun reklam içeriklerine maruz kalması, haber/reklam ayrımının ortadan kalkması gibi unsurlar etik ihlallere sebebiyet vermektedir.

- Kültürel nedenler: Kişilik haklarının ihlali, mahremiyete müdahale vb. pek çok konuda bilinç ve eğitim eksikliği de etik ihlallerin kültürel nedenleri arasındadır.

SİBER HUKUK VE SİBER ETİK

Siber hukuk, dijital dünyayı (bilgisayar, bilgisayar ağları, yazılım, veri depolama cihazları, internet, cep telefonları, otomatik vezne makinelerinin kullanımı, giriş verilerini ve çıktı sonuçlarını işleyebilen diğer elektronik cihazlar) yöneten kanundur (Shakeel, Tanha, Broujerdi, 2011: 146).

Bazı ülkeler ilgili konuları mevcut yasalar aracılığıyla ele almış olsa da, siber etik üzerinde mutabık kalınmış bir uluslararası anlaşma yoktur (Mbinjama-Gamatham, Olivier, 2014: 35-36). Siber hukuk, siber suç ve siber güvenliği de kapsamı altına almaktadır. Redford ve Jefferson (2011: 35-36), günümüzün gelişmekte olan teknolojileriyle başa çıkmak için siber konuları içeren yasaların olması gerektiğini belirtmektedir: "Dijital dünyada gelişen teknolojinin ele alınması, bu tür teknolojiyi kontrol eden ve korumayı amaçladığı teknolojiye fayda sağlayan yeni yasalarla hızlanmalıdır".

Yılmaz ve Güllüpınara'a (2020: 5375-5376) göre:

Siber suçlar konusunda şu ana kadar yapılan en etkin hukuki düzenlemenin, Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suçlar Sözleşmesi olduğu söylenebilir. Hazırlanan sözleşmenin hedefi "ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi" ve uluslararası işbirliğinin geliştirilmesidir. Türkiye, Avrupa Konseyi Siber Suçlar Sözleşmesine 10 Kasım 2010 tarihinde imza koyarak taraf olduğu hâlde, Sözleşmeyi iç hukukun parçası hâline getirecek işlemleri tamamlayıp, Sözleşmeyi iç hukuka aktaramamıştır. 22 Nisan 2014 tarihinde mecliste yürürlüğe girmiştir, ancak sözleşmenin iç hukuka entegrasyonunda ve uygulanmasında sıkıntılar devam etmektedir.

Siber araştırmacıların bir kısmı dijital yasaların düzenlenmesinin zor ve kısıtlayıcı olacağından, aynı zamanda bu durumun iletişim ve medya endüstrilerinde bilgiyle ilgili yaratıcılığı engelleyeceğinden endişe duymaktadırlar (Boyle, 1996). O yüzden Mbinjama-Gamatham ve Olivier (2020: 111), siber yasalardan daha çok siber etik konusu üzerine yoğunlaşmanın önemi belirtmektedir.

Siber etiği tanımlamadan önce etik kavramına bakmakta fayda vardır. Mahmutoğlu'na (2019: 226) göre, etik insan eylemlerinin bilinç düzeyi ile ilgilenmekte, bir tutum ve davranışı ortaya çıkaran iradeyi irdelemektedir. Aynı zamanda etik tamamen insana ve topluma ilişkin bir kavram olduğundan dolayı, bütün sosyal kurumlarla yakın ilişki veya iletişim kurmak durumundadır (Mahmutoğlu, 2019: 248)

Etik kavramı evrensel değerlere atfen kullanılır; dürüstlük, yardımseverlik, doğruluk, adalet, sadakat, yalan söylememek, hırsızlık yapmamak vb. Etiğin amacı bireye toplum içerisinde diğerleriyle birlikte yaşarken iyi temellendirilmiş ahlaki kararları kendi başına verebilecek durumda olmayı ve kendi başına var olabilmeyi öğretmektir (URL-2).

Siber etik, dijital teknolojilerin kullanıcı davranışını, bu teknolojilerin nasıl programlandığını, bireyleri ve toplumu nasıl etkilediğini kapsayan siber dünya

ile ilgili kavramdır (Otto, Ukpere, 2012). Ki'ye ve Ahn'a (2006) göre, siber etik, siber dünyada ahlakı ve ahlaksızlığı öngören, ifade özgürlüğünün, fikri mülkiyetin ve mahremiyetin korunmasını ifade eden bir standartlar sistemidir.

Sosyal medyadaki aktiviteleri siber etik bağlamında ele alırsak, insanlar bu sosyal ağlar aracılığıyla seslerini duyurmaktadır. Ülke gündemindeki durumlara itiraz etmek, desteklemek, birbiriyle ile topluluk içinde etkileşimde bulunmak sosyal mecralar ile yapılan aktivitelerden bazılarıdır. Fakat sanal dünyanın vermiş olduğu rahatlıkla beraber kullanıcılar çoğu zaman etik ihlaller yapmakta ve hukuksal olarak birçok sınırları da aşmaktalar.

DİJİTALLEŞEN KÜLTÜRDE ETİK

Modern toplumlar 'teknokratik' bir kültürde yaşamakta ve teknokratik, kelimenin tam manasıyla 'teknolojinin kuralı' anlamına gelmektedir (Castells, 2010).

Siber dünyada çok uzun geçirilen zamanı göz önünde bulundurduğumuzda sadizm ve mazoşizm davranış bozukluklarına da sıklıkla rastlandığını söyleyebiliriz. Siber dünyadaki olaylar, diğer kişilerin gizlilik haklarının 'sahte porno' olarak adlandırılan bir tür suiistimalini içerir. Aktörlerin ve diğer 'ünlülerin' yüzlerinin pornografik film oyuncularının vücutlarına 'kopyalanması've internette yayınlanması ile bu tür porno klipler dolaşıma sokularak taciz gibi suçların ortaya çıkmasına sebebiyet vermektedir (URL-3). Siber dünyada bu tür etik açıdan kınanan (ve çoğu zaman suç teşkil eden) eylemleri gerçekleştirenler her zaman bireysel değildir. Örneğin, Avrupa Birliği'nin Rekabetten Sorumlu Komisyon Üyesi Margrethe Vestager tarafından Google'a uygulanan büyük para cezasını (4,3 milyar Euro) anlatan raporda (BBC News 2018), büyük teknoloji şirketlerinin "verileri kötüye kullanma ve vatandaş haklarına saygı göstermeme" konusunda dizginleme ihtiyacının arttığını belirtmektedir (Mbinjama-Gamatham, Olivier, 2020: 108). Aynı zamanda raporda, bir arama motoru olarak hâkimiyetini yasadışı pekiştirdiği için Google'a verilen para cezasına ek olarak, sosyal medya şirketlerinin aşağıdaki önemli etik ihlalleri de listelenmektedir:

- Facebook, siyasi danışmanlık şirketi Cambridge Analytica'nın 87 milyon Facebook kullanıcısının bilgilerine ulaşmasına izin verdiği için özür dilemek zorunda kalmıştır.

- Twitter, Facebook ve YouTube gibi önde gelen sosyal platformların, Rusya ve diğerleri tarafından Batı'daki seçmenleri manipüle etmek amacıyla kullanılması yönünde kanıtlar mevcuttur.

İnternetin olumsuz yönünü doğrulayan başka bir rapora (Al Jazeera, 2019) göre, World Wide Web'in tasarımcısı Tim Berners-Lee, icadının 30. yıl dönümü

vesilesiyle benzer endişeleri dile getirmiştir (Mbinjama-Gamatham, Olivier, 2020: 108).

Birçok olumsuzlukları ile beraber dijital etik bağlamında siber dünyada önemli adımlar da atılmaktadır. Bu anlamda sosyal medya düzenlemesi, pornografiye erişim için yaş sınırlaması, dijital telif hakkı yasası, 'unutulma hakkı' (internetteki güncel olmayan bilgilerin kaldırılması) gibi interneti kullanma biçimindeki değişikliklerin yaşanması olumlu göstergeler olarak kabul edilmektedir (URL-3).

Mbinjama-Gamatham ve Olivier (2020: 109), dijital etik konusunun geliştirilmesi yönünde iki önemli hususta bahsetmektedir:

1. Her kültürde, özellikle çocuklara ve gençlere etik veya ahlaki sorumluluk duygusu aşılamayı amaçlayan 'eğitim'

2. Hukuk aracılığıyla suç davranışını ele almayı amaçlayan 'mevzuat'

Böylece, internet kullanımı söz konusu olduğunda etik ve ahlaki kod biçimi üstlenebilecek yaklaşım için eğitimin ve mevzuatın birbirini tamamlaması önemlidir.

SONUÇ

Günümüz teknolojisi, kişilerin özel hayatlarının izlenmesine ve gözlemlenmesine odaklanmakla beraber sadece iktidarları değil, gözetime yönelik bireyleri de yönlendirmektedir. Yeni dönemin önemli bağımlılıkları arasında yer alan sosyal medya kültürü, dijital ortamda denetimi hep açık tutmaktadır. Diğer taraftan, sosyal medyada dolaşan insanlar paylaşımları sonucu takipçileri ile iletişime geçerek bu mecraya interaktif bir özellik katmaktadır. Bu durum insanların düşüncelerini istedikleri şekilde ifade edebilecekleri gerçekçi bir ortam olmanın yanı sıra, aynı zamanda söylediklerinin sorumluluğunu alamayacakları kadar sanal ortama sahiptir. Bir diğer taraftan, insanlar kendilerini "yaşayan, gelişen, etkileşime giren, bağımsız varlıklar olarak değil, bilgiden oluşan bir dünyada ağ bağlantılı ajanlar olarak" algılamaktalar.

Çalışmadaki değerlendirmelerden elde edilen sonuca göre sosyal medya araçları gelişip çoğaldıkça siber suç oranları da artmaya devam etmektedir. Bu durum sosyal medya üzerindeki denetimi zorlaştırmakta ve beraberinde siber dünyadaki etik ihlallere zemin hazırlamaktadır. Sosyal medya ile beraber artan görünürlük ve erişilebilirlik aynı anda kullanıcıları yeni bir dizi suç tehdidine karşı savunmasız hâle getirerek suç mağduriyeti için imkânlar yaratmaktadır. Sosyal medya kullanıcılarının yaş itibariyle çocuk kullanıcıları suç mağduriyetine karşı savunmasız kalmaktadır. Aynı zamanda kullanıcıların sosyal medya ortamlarında aşırı paylaşımlar yapması, özel hayatlarının her detayını takipçilerine göstermeleri, kişisel bilgilerinin çekinmeden ortaya konulması,

gittiği yerleri, tatilleri ve beraber zaman geçirdikleri kişileri etiketlemesi güvenlik sorunlarını da beraberinde getirmektedir. Bu durumda sosyal medya hem geleneksel suçlar hem de siber suçlar için ortam hazırlamaktadır.

Siber suçların olumsuz etkilerinin hafifletilmesi ve kontrol altına alınması için doğalarını ve dinamiklerini anlamak çok önemlidir. Bu bağlamda dijital teknolojiler geliştikçe sosyal medya platformları da genişlemekte ve bu durum tehlikeleri de beraberinde büyütmektedir. Fakat dijital okuyazarlık bilincine sahip kullancılar, çevrim içi arkadaşlık isteği kararlarında karşılıklı etkileşimin yanı sıra, çevrim içi mağduriyet şansını azaltan uygulamalar ve ayarlar uygulamaktalar.

Dijital dünyayı kapsayan yasal düzenlemeler her geçen gün geliştirilse de siber alandaki hızlı değişimler bu yasal düzenlemeleri yetersiz kılmaktadır. Dolayısıyla internetin kendine özgü niteliklerinden dolayı gerçek dünyadaki yasal düzenlemeler pek işe yaramamaktadır. Bunun nedeni ise gerçek dünyadaki hukuki sınırlar yasayı uygulayan ülkelerin bağımsızlık sınırlarıyken; sanal dünyanın ait olduğu böyle bir sınırdan söz etmek güçtür (Batır, 2005: 158).

Bu durumlarda sosyal medya kullanıcılarının kültürel ve sosyal bilinçlilik düzeylerine göre farklılık gösteren etik değerleri devreye girmekte ve 'yazılı' olmayan düzenlemelerle öz denetim sağlanmaktadır. Fakat internete erişimin artık kolay olduğu dünyada etik kurallarla oluşturulacak kendini denetim mekanizması için de bu kuralları topluma hatırlatacak sosyal medya konulu eğitimlere ihtiyaç duyulmaktadır.

Tüm bunların sonucu olarak ister sosyal medya kullanıcılarının paylaştıkları bilgilerin, isterse de internet ortamında paylaşılan diğer bilgilerin gizli olmadığını dikkate alarak dijital dünyada sorumluluk bilincinde olmakta fayda vardır.

KAYNAKÇA

Batır, K. (2005). İnternet ve Hukuk. Binark, M. ve Kılıçbay, B. (Ed.) *İnternet, Toplum, Kültür* (ss.156-176). Ankara: Epos Yayınları.

Binark, M. & Bayraktutan, G. (2013). *Ayın Karanlık Yüzü: Yeni Medya ve Etik*. Kalkedon Yayınları.

Boyle, J. (1996). *Shamans, Software And Spleens: Law And The Construction Of The Information Society*. Cambridge, MA: Harvard University Press.

Bradshaw, EA. (2013). This is What A Police State Looks Like: Sousveillance, Direct Action And The Anti-Corporate Globalization Movement. *Critical Criminology.* 21(4): 447-461. doi: 10.1007/s10612-013-9205-4.

Castells, M. (2010). *The Rise Of The Network Society*. Oxford: Blackwell.

Chayko, M. (2018). *Superconnected*. Londra: SAGE Publications.

Çetin, M. & Asıl, S. (2017). Günümüz Toplumunda Gözetim Olgusu. *Üçüncü Sektör Sosyal Ekonomi.* 52 (1):180-205. ISSN: 2148-1237 / 2587-0114.

Dadkhah, M., Lagzian, M. & Borchardt, G. (2018). Identity Theft in The Academic World Leads To Junk. *Science and Engineering Ethics.* 24 (1): 287–290. doi: 10.1007/s11948-016-9867-x.

Furnell, S. (2002). *Cybercrime: Vandalizing The Information Society*. London: Addison-Wesley.

Goldsmith, A. (2015). Disgracebook Policing: Social Media And The Rise Of Police Indiscretion. *Policing and Society.* 25(3): 249-267. doi: 10.1080/10439463.2013.864653.

Holt, TJ. & Bossler A. (2014). An Assessment Of The Current State Of Cybercrime Scholarship. *Deviant Behavior.* 35(1): 20-40. doi: 10.1080/01639625.2013.822209.

İsmayilzada, L. & Topçu, O. (2019). New Privacy Concept in Social Media in Digital Surveillance Society. Communication and Technology Congress – CTC 2019.

Ki, H. & Ahn, S. (2006). A Study On The Methodology Of Information Ethics Education in Youth. *International Journal of Computer Science and Network Security*. 6 (6): 91-100.

Kurt, L. (2005). *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması*. Seçkin Yayınları.

Levin, İ. (2014). Cultural Trends in A Digital Society. Proceedings of TMCE 2014.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lupton, D. (2014). *Digital Sociology*. London: Routledge.

Mahmutoğlu, A. (2019). Etik ve Ahlâk; Benzerlikler, Farklılıklar ve İlişkiler. *Türk İdare Dergisi.* s.226-250.

Mavnacıoğlu, K. (2009). İnternette Kullanıcıların Oluşturduğu ve Dağıttığı İçeriklerin Etik Açıdan İncelenmesi: Sosyal Medya Örnekleri. Fırat Üniversitesi İletişim Fakültesi Medya ve Etik Semp, 07-09 Ekim 2009, Elazığ.

Mbinjama-Gamatham, A. & Olivier, B. (2020). Dark Technology, Aggressiveness And The Question Of Cyber-Ethics. *Acta Academica.* 52(1), 99-120. doi: 10.18820/24150479/aa52i1/1.

Moore, A.A. (2018). *Cyberstalking and Women: Facts and Statistics*. thoughtco.com.

NW3C. (2013). *Criminal Use of Social Media.*

NW3C. (2015). *Cyberstalking (March).*

Otto, G. & Ukpere, W. I. (2012). National Security and Development in Nigeria. *African Journal of Business Management*. 6 (23): 6765-6770.

Öztürk, Ş. (2015). Sosyal Medyada Etik Sorunlar. *Selçuk İletişim.* 9 (1): 287-311

Parker, D.B. (1998). *Fighting Computer Crime: A New Framework For Protecting Information*. John Wiley & Sons, Inc. New York, NY, United States.

Poster, M. (1990). *The Mode of Information: Post-Structuralism and Social Contexts*. Cambridge: Polity.

Prins, C. (2011). Digital Tools: Risks And Opportunities For Victims: Explorations in E-Victimology. In Letschert R and Van Dijk J (Ed.) *The New Faces of Victimhood. Globalization, Transnational Crimes and Victim Rights*. ss. 215-230. Netherlands: Springer.

Redford, M. & Jefferson, T. (2011). *U.S. And EU Legislation On Cybercrime.* Proceedings of the 2011 European Intelligence and Security Informatics Conference. IEEE Conference Publications. doi: 10.1109/EISIC.2011.38.

Saariluoma, P. & Sacha, H. (2014). *How Cyber Breeds Crime And Criminals*, The Society of Digital Information and Wireless Communications (SDIWC).

Sa, M. & Serpa, S. (2018). Transversal Competences: Their Importance And Learning Processes by Higher Education Students. *Education Sciences*. 8(3): 126. https://doi.org/10.3390/educsci8030126

Shakeel, I., Tanha, A. D. & Broujerdi, H. G. (2011). A Framework For Digital Law Enforcement İn Maldives. Proceedings of the Second International Conference on Computer Research and Development. IEEE Conference Publications. doi: 10.1109/ICCRD.2010.93.

Smith, R., Grabosky, P. & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge, England: Cambridge University Press.

Smith, R. (2010). Identity Theft And Fraud. In Y. Jewkes & M. (Ed.), *Handbook of Internet Crime* (ss. 273–301). Cullompton: Willan.

Soomro, T. R. & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Sciendo*. 24 (1): 9–17, doi: 10.2478/acss-2019-0002.

Thomas, D. & Loader, B. (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age.* London: Routledge.

Yar, M. (2006). *Cybercrime and Society*. Sage Publications.

Yar, M. (2012). *E*-Crime 2.0: The Criminological Landscape Of New Social Media. *Information & Communications Technology Law*, 21 (3): 207-219. doi: 10.1080/13600834.2012.744224.

Yılmaz, F. & Güllüpınar, F. (2020). Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi. *OPUS–Uluslararası Toplum Araştırmaları Dergisi*. 15(10. Yıl Özel Sayısı): 5371-5409. doi: 10.26466/opus.688815.

Wall, D. (2001). Cybercrimes and the Internet. in D. Wall (Ed.), *Crime and the Internet*. London: Routledge.

Webster, F. (2003). *Theories of the Information Society*. London: Routledge.

ELEKTRONİK KAYNAKLAR

URL-1 https://www.academia.edu/6475117/Etik_Kavram%C4%B1_Anlam%C4%B1_Amac%C4%B1_Etik_T%C3%BCrleri (Erişim Tarihi: 31.03.2021)

URL-2 https://www.britannica.com/topic/information-system (Erişim Tarihi: 30.03.2021)

URL-3 https://uk.news.yahoo.com/fourbig-changes-coming-internet-year-porn-privacy-111404413.html (Erişim Tarihi: 30.03.2021)