Siber Suçların Hukuksal Yönleri ve Psikolojik Dinamikleri

The Legal Aspects and Psychological Dynamics of Cybercrimes

Erdinç ÖZTÜRK[a],
Afranur ATEŞ[b],
Barışhan ERDOĞAN[c]

[a]İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, Sosyal Bilimler ABD, İstanbul, TÜRKİYE
[b]İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, İstanbul, TÜRKİYE
[c]İstanbul Arel Üniversitesi Fen-Edebiyat Fakültesi, Psikoloji Bölümü, İstanbul, TÜRKİYE

Yazışma Adresi/*Correspondence:*
Erdinç ÖZTÜRK
İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, Sosyal Bilimler ABD, İstanbul, TÜRKİYE
erdincerdinc@hotmail.com

ÖZET İnternetin hayatımızın tamamına yayılmasıyla birlikte suçların da siber alanda yeni biçimlere bürünerek küresel bir hâl aldığını söylemek mümkündür. İnternetin coğrafî sınırlardan muaf doğası içinde doğan bu yeni suçlar ve alışılageldik suçların biçim değiştirmesiyle oluşan yeni suç tipleri siber suçlar olarak tanımlanmaktadır. Tıpkı geleneksel suçlarda olduğu gibi siber suçlar da detaylı bir psikososyolegal değerlendirme gerektirmektedir. Değişmekte olan sosyokültürel dinamikler sözü edilen suçların gelişmesine uygun zemini oluşturmaktadır. Bu suçların psikolojik dinamikleri fail ve mağdur tipolojilerinin belirlenmesinde, dolayısıyla önleyici çalışmaların geliştirilip sürdürülebilmesinde önem kazanmaktadır. Hukuk sistemleri içindeki yasal düzenlemeler de mağdur haklarını koruma altına alabilmek, faillerin gereken yaptırımlarla karşılaşmasını sağlamak ve suçun gerçekleşmesini önlemek noktalarında hayatî bir rol oynamaktadır. Bu çalışmanın amacı, modern dünyada karşımıza çıkan bir kavram olarak siber suçların Türk Ceza Kanunu'nda tanımlandıkları biçimleriyle ve siber psikoloji, kriminal psikoloji ve adli psikoloji literatürlerinde ele alındıkları hâliyle incelenmesidir. Bu noktada kuramsal bilgiler ve mevcut uygulamalar tartışılacak; olası önleme politikaları gözden geçirilecektir.

Anahtar Kelimeler: Ceza psikolojisi; bilişim; siber psikoloji

ABSTRACT It is possible to state that certain types of crime have taken a global form along with the expansion of the Internet in our lives. These new types of crime that were born in geographically unlimited nature of the Internet, as well as those that were generated via reformation of usual (or offline) crimes, are described as cybercrimes. Quite similar to traditional crimes, cybercrimes also require a comprehensive psycho-socio-legal evaluation. The everchanging sociocultural dynamics contribute to the formation of the suitable ground for the aforementioned crimes. The psychological dynamics of these crimes are important for determining victim and perpetrator typologies, thus enabling the development and sustainability of prevention programs. Legislative regulations in legal systems play a vital role in taking the rights of victims under preservation, guaranteeing perpetrators to face required sanctions and preventing crime. The aim of this study is to scrutinize the cybercrimes as a notion observed in modern world in the light of their described forms in Turkish Penal Code and in the literatures of cyber, criminal and forensic psychology. At this point, theoretical knowledge and existing applications will be discussed, along with the examination of prevention policies.

Keywords: Criminal psychology, informatics; cyberpsychology

Günümüzde teknolojik gelişmeler ışığında fizikselliğin olmadığı ve sınırların neredeyse tamamen ortadan kalktığı yeni bir "yer" olarak siber alandan bahsetmek mümkündür.[1] Cep telefonları, bilgisayarlar ve tabletler gibi cihazlarla her bireyin bu siber alanda en az bir temsili ya da kimliği bulunmaktadır. Kişilerarası iletişim, alışveriş, eğitim-öğretim faaliyetleri ve eğlence sektörü günümüzde büyük ölçüde bu siber alanda, bütün fiziksellik ve sınırlardan uzak, her bireyin evinin içine hatta odasına kadar girmiş bir şekilde sürdürülmektedir. Günümüzde artık bireyler bu siber alandaki temsil ve kimlikleri ile gerçek yani aktüel alandaki temsil ve kimliklerini entegre etmek zorundadırlar. Bu entegrasyon süreci ise çoğu zaman fonksiyonel bir şekilde yürütülememektedir. Postmodern toplumlarda bu fonksiyonelliği kazanmak adına ruhsal yapı-

KAYNAK GÖSTERMEK İÇİN:
Öztürk E, Ateş A, Erdoğan B. Siber suçların hukuksal yönleri ve psikolojik dinamikleri. Öztürk E, editör. Siber Psikoloji. 1. Baskı. Ankara: Türkiye Klinikleri; 2020. p.48-55.

lanmada dissosiyasyon süreci devreye girmektedir. Bilinç kesintisi, amnezi, dalgınlık ve affektif mobilite ile karakterize olan dissosiyatif eksenli yaşantılar siber alanda bireylerin siber mağduriyetine yol açabilmekte ve onları suçun tanığı ya da mağduru yapabilmektedir. Siber alandaki optimal mesafenin yani sınırların belirsiz doğası ve dissosiyojen ruhsal zemin, bireylerin suça yönelmesini kolaylaştırabilmektedir. Gündelik ve toplumsal yaşamın bütün bileşenleriyle siber alanda temsil edildiği düşünülürse elbette suç faktörünün de yepyeni tezahürlerle karşımıza çıkacağını öngörmekteyiz. Bu çalışmanın amacı, siber suçların hukuksal ve psikolojik dinamiklerinin incelenmesidir. Diğer bir ifadeyle teknolojik gelişmeler ışığında değişen ya da oluşan suçları psikolegal faktörleriyle birlikte incelemek, Türk Ceza Kanunu'nda tanımlanan siber suçları (bilişim suçlarını) ele almak ve bu görece yeni alana multidisipliner bir katkı sağlamaktır.

SİBER SUÇLARIN HUKUKSAL YÖNLERİ

Siber suçların hukuksal yönleri, bireyin siber alanda içerisinde olduğu dissosiyojen ve mobil affektif bir zeminde çok eksenli olarak ayrıntılı bir şekilde değerlendirilmelidir. Bu kapsamda öncelikle Türk Hukuku kapsamında Türk Ceza Kanunu'nda "bilişim alanında suçlar" başlığı altında düzenlenen suç tiplerinden "bilişim sistemine girme", "sistemi engelleme, bozma, verileri yok etme veya değiştirme" ve "banka veya kredi kartlarının kötüye kullanılması" suçları inceleme konusu yapılarak ceza kanunu düzenlemesinde dikkati çeken noktalara değinilecektir. Daha sonrasında mukayeseli hukuk çerçevesinde siber suçlara hukuki perspektiften genel bir bakış sunulacaktır. 5237 sayılı Türk Ceza Kanunu'nda bölüm başlığının "bilişim alanında suçlar" şeklinde düzenlenmesi nedeniyle kanunun diliyle paralellik sağlanması amacıyla çalışmanın ilerleyen bölümlerinde siber suç kavramı yerine "bilişim alanında suçlar" kavramı kullanılacaktır.

Bilişim alanında suçlar mevzuatımızda ilk defa 1991 yılında 765 sayılı TCK'ya eklenen düzenlemeler ile cezai müeyyideye bağlanmıştır. 5237 sayılı yeni Türk Ceza Kanunu'nda ise klasik suç tiplerinde bilişim suçlarıyla ilgili yapılan düzenlemelerin yanı sıra, bilişim alanında suçlar ikinci kitap üçüncü kısım onuncu bölümde ayrı bir başlık altında da düzenlenmiştir.[2,3]

Türk Ceza Kanunu'nda bilişim suçları ikili sınıflandırmaya tabi tutulmuştur. Buna göre doğrudan bilişim suçları olarak Türk Ceza Kanunu'nun onuncu bölümünde bilişim sistemine karşı suçlar başlığı altında özel suç tipleri düzenlenmiştir. Aynı zamanda ceza kanununda yer alan klasik suç tiplerinin bazılarına bilişim sistemi kullanılarak işlenmesine yönelik yeni fiiller eklenerek dolaylı bilişim suçları düzenlemesine gidilmiştir. Dolaylı bilişim suçları, bilişim sistemi kullanılmasıyla işlenebilecek suç tipleridir. Dolaylı bilişim suçlarına TCK 142/2-e bendindeki hırsızlık suçunun bilişim sistemi kullanılarak işlenmesi nitelikli hali örnek gösterilebilir.[3-5]

TCK MADDE 243: BİLİŞİM SİSTEMİNE GİRME SUÇU

Türk Ceza Kanunu'nun 243. maddesi "bilişim sistemine girme" başlığı altında bir suç düzenlemesi getirmiştir. Bu madde ile kanuni ifadesiyle "bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek" cezai yaptırım altına alınmaktadır. İlgili düzenleme ile bilişim sistemindeki verilerin ele geçirilmesi şart olarak aranmamakta, sisteme haksız olarak girmek veya orada kalmaya devam etmek suçun oluşmasına neden olmaktadır.

Bilişim sistemine girme suçu bilişim sistemine ulaşmayı sağlayan aracın parçalarına somut olarak yapılacak müdahaleleri kapsamamaktadır. İlgili düzenlemede "bilişim sistemine girmek" ifadesiyle bilişim sisteminin tamamına ya da bir kısmının oluşturduğu dijital platforma erişim kast edilmektedir. Suçun kanuni ifadesinde, failin davranışlarıyla mağdura zarar vermek istemesi gibi bir psikolojik etken amaç olarak aranmamaktadır; dolayısıyla fiilin manevi unsurunun oluşabilmesi için genel kast yeterlidir. Söz konusu maddede fiilin hukuka aykırı olarak gerçekleşmesi aranmaktadır. Buna göre mağdurun geçerli rızası gibi hukuka uygunluk sebeplerinden birinin bulunması halinde fiil suç teşkil etmeyecektir. Bu noktada dikkat edilmesi gereken mağdurun rızası bulunsa bile sisteme girildikten sonra rızanın kalkması durumunda sistemde kalınmaya devam edilmesi halinde fiilin suç teşkil edeceğidir.[6,7]

Belirtmek gerekir ki inceleme konusu Türk Ceza Kanunu'nun 243. maddesinin düzenlemesi 24.03.2016 tarihli ve 6698 sayılı Kanunun 30. maddesiyle değişikliğe uğramıştır. Zira maddenin değişiklik öncesi eski halinde "bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girmek ve orada kalmaya devam etmek fiili yaptırım altına alınmaktaydı. Bu durumda yalnızca hukuka aykırı olarak bilişim sistemine girmiş olmak suçun oluşması için yeterli olmamakta; bir süre sistemde kalmaya devam etmiş olma şartı aranmaktaydı.[8,9] Bahsi geçen değişiklik sonrası maddede yaptırıma bağlanan fiil "bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek" şeklinde düzenlenmiştir. Bu haliyle düzenlemenin, Türkiye tarafından 10.11.2010 tarihinde Strazburg'da imzalanan "Sanal Ortamda İşlenen Suçlar Sözleşmesi"nin (doktrinde kullanılan adıyla Avrupa Siber Suç Sözleşmesi) "Yasadışı

Erişim" kenar başlıklı 2. maddesinin gereklerini yerine getirilmeye hizmet ettiği söylenebilir. Zira sözleşmenin bahsi geçen 2. maddesinde bilişim sistemine hukuka aykırı erişimin suç teşkil edeceği düzenlenirken sistemde kalmaya devam etme şartı aranmamıştır.[7] İlgili sözleşme 22.04.2014 tarihli ve 6533 sayılı yasa ile TBMM tarafından onaylanmış, ilişik çekinceler ve beyanlar ile birlikte onaylanmasına dair karar 09.08.2014 tarihinde Resmi Gazete'de yayınlanmıştır. Söz konusu sözleşmenin 2. maddesi taraf devletlerin yasadışı erişimin kendi iç hukuklarında bir suç olarak tanımlaması için gerekli olabilecek tedbirleri kabul ettiğini belirtmektedir.[10] Yukarıda bahsi geçen TCK'daki bilişim sistemine girme suçu, belirtilen uluslararası sözleşmenin Türk iç hukukuna aktarılmasının bir parçası olarak düşünülebilir.

TCK MADDE 244: SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME

Türk Ceza Kanunu'nun 244. maddesi aslında üç farklı suç tipini düzenlemektedir. "Bilişim sistemini engelleme ve bozma", "bilişim sisteminde bulunan verilere zarar verme" ve "bilişim sistemi kullanarak haksız menfaat sağlama" davranışları aynı maddenin değişik fıkralarında farklı suç tipleri olarak yaptırım altına alınmıştır. Bahsi geçen madde yukarıda zikredilen Avrupa Siber Suç Sözleşmesi'nin 4, 5 ve 8. maddelerinin iç hukuktaki görünümü niteliğindedir. Nitekim ilgili sözleşmenin 4. maddesi taraflardan her birinin, bilgisayar verilerine haksız yere zarar verilmesi, silinmesi, değiştirilmesi vb. maddede belirtilen fiillerin kasten gerçekleştirildiği durumları kendi iç hukukunda suç olarak tanımlanması için gerekli tedbirleri alması gerektiğini belirtmektedir. Sözleşmenin "sisteme müdahale" başlıklı 5. maddesinde de sözleşmeye taraf ülkelerden her birinin, bilgisayar verilerine zarar verilmesi, değiştirilmesi gibi fiillerle, haksız yere bir bilgisayar sistemin işleyişinin kasıtlı olarak engellendiği durumları, kendi iç hukukunda bir suç olarak tanımlanması için gerekli tedbirleri almayı kabul ettiğini ifade etmektedir. Benzer şekilde ilgili sözleşmenin 8. maddesi de sözleşmeye taraf devletlerin, maddede belirtilen fiillerin kasten ve haksız yere gerçekleştirilerek bir kimsenin mal kaybına sebep olunduğu durumların kendi iç hukukunda suç olarak tanımlanması için gerekli tedbirleri alacağını belirtmektedir.[10]

Söz konusu maddenin birinci fıkrasındaki suç tipinin maddi unsuru "bilişim sisteminin işleyişini engellemek veya bozmaktır." Bu suç tipi seçimlik hareketli suç olarak düzenlenmiştir. Engelleme veya bozma fiillerinden birinin işlenmesi suçun gerçekleşmesi için yeterlidir. İki seçimlik hareketin gerçekleştiği durumda ise tek bir suç oluşacaktır. Bahsi geçen "bilişim sistemini engelleme" ile kast edilen sistemin işleyişinde geçici olarak kesinti meydana getirmektir. Bilişim sisteminin işleyişini bozma ise sistemden yararlanmanın kalıcı şekilde engellenmesi anlamına gelmektedir. Bu noktada ikili bir ayrıma gitmek gerekmektedir. Zira bilişim sisteminin işleyişinin bir bütün olarak sisteme karşı işlenen fiillerle bozulması mümkün olduğu gibi sistemin verilerine yapılacak müdahalelerle de sistemin işleyişinin bozulması mümkündür. Sistemin verilerine yönelen fiilin sistemin işleyişini engellemesi veya bozması durumu 244. maddenin birinci fıkrasına; sistemin işleyişini engellememesi veya bozmaması durumu ise 244. maddenin ikinci fıkrasına karşılık gelmektedir.[8]

244. maddenin ikinci fıkrasında bilişim sistemindeki verilere zarar verme suçu düzenlenmektedir. İlgili fıkrada "sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi"nin cezalandırılacağı belirtilerek seçimlik hareketli bir suç düzenlemesine yer verilmiştir.[1] Söz konusu düzenleme, yukarıda zikredilen Avrupa Siber Suç Sözleşmesi'nin 4. maddesindeki verilere müdahale fiillerinin iç hukuktaki yansımasıdır.[8]

Türk Ceza Kanunu'nun sistematiğinde 244. maddenin ilk iki fıkrasında belirtilen fiillerin *"*banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali" üçüncü fıkrada cezayı arttırıcı nitelikli hal olarak düzenlenmiştir. Maddenin son fıkrasında ise ilk iki fıkrada düzenlenen fiillerin gerçekleştirilmesiyle "kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması" hali ayrı bir suç olarak düzenlenmiştir. Fıkrada, belirtilen fiillerin başka bir suç oluşturmaması halinde bu düzenlemenin uygulanacağı ifade edilmiştir. Başka bir deyişle 244. maddenin dördüncü fıkrası tamamlayıcı bir kural olarak düzenlenmiştir.[8]

TCK MADDE 245: BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI

İlgili suçla korunmak istenen hukuki değer madde gerekçesinde banka veya kredi kartlarının hukuka aykırı kullanılmasıyla bankaların veya kredi kartı sahiplerinin zarara sokulmasının önüne geçilmesi olarak belirtilmiştir. Bu çerçevede maddenin ilk fıkrasında başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlama suçu; ikinci fıkrasında başkalarına ait banka hesapları ile ilişkilendirerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçu; üçüncü fıkrasında ise sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla hukuka aykırı yarar sağlama suçu cezai müeyyideye bağlanmıştır.[7]

Birinci fıkradaki suçun maddi unsuru açısından dikkati çeken husus düzenlemede "başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse" ifadesinin yer almasıdır. Buna göre failin kartı ne şekilde ele geçirdiği önemli değildir. Önemli olan maddede belirtildiği üzere failin "kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlama" eylemini gerçekleştirmesidir.[7]

İkinci fıkrada ise suçun maddi unsuru seçimlik olarak düzenlemiştir. Seçimlik hareketler sahte banka veya kredi kartını üretmek, satmak, devretmek, satın almak veya kabul etmek olarak ifade edilmiştir. Maddede düzenlenen suçun oluşması için bu eylemlerin başkasına ait banka hesabı ile ilişkilendirilerek işlenmesi gerekmektedir.[8] Suçun düzenlemesinde dikkati çeken bir başka husus seçimlik hareketler sonucu sahte kart ile yarar sağlanması şartının aranmamasıdır. Suçun meydana gelmesi için yarar elde edilmesi şeklinde bir netice aranmadığı için seçimlik hareketler ile oluşturulan fiiller tehlike suçu olarak düzenlenmiştir.[7]

İnceleme konusu düzenlenmenin üçüncü fıkrasında ise "sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi" hakkında yaptırım düzenlenmiştir. Suçun oluşum şeklinde ilk olarak sahte oluşturulmuş ya da üzerinde değişiklik yapılarak sahte hale getirilmiş bir kartın bulunması gerekmektedir. İkinci olarak failin bahsedilen niteliklerdeki kartı kullanarak kendisine veya başkasına yarar sağlaması aranmaktadır.[9]

MUKAYESELİ CEZA HUKUKU'NDA BİLİŞİM SUÇLARI

Alman Ceza Kanunu'nda bilişim suçları Türk Ceza Kanunu'nda olduğu gibi bağımsız bir bölüm olarak düzenlenmemiş; farklı bölümlerde çeşitli hükümler altında ele alınmıştır.[2] Türk ceza mevzuatında 243. maddede düzenlenen suç tipinin Alman Ceza Kanunu'nda doğrudan karşılığı bulunmamakla birlikte, 202a ve 202b maddelerinin mevzuatımızdaki düzenlemeyle benzerlik gösterdiği söylenebilir. 202a maddesi bilişim sistemi içindeki verilere yönelik yetkisiz olarak gerçekleştirilen eylemlere müeyyide getirirken; 202b maddesi verilerin yetkisiz olarak ağda ele geçirilmesine yönelik düzenlemeleri içermektedir. Alman Ceza Kanunu'nun 202a maddesinin TCK madde 243'den önemli bir farkı bilişim sistemine yetkisiz girme davranışının değil; verilere yetkisiz olarak ulaşım veya erişim imkânını sağlama davranışının düzenleniyor olmasıdır. Alman Hukukunda 2007 yılında bilgisayar suçlarıyla mücadele kapsamında düzenlenen "41. Ceza Hukuku Değişiklik Kanunu" ile 202a maddesinde yapılan değişikliğin ardından sistemdeki verilere erişilmese dahi bu amaçla sisteme girmek fiili hükmün yasakladığı davranış çerçevesinde değerlendirilecektir.[2]

Türk Ceza Kanunu'nda 244. maddede düzenlenen bilişim sistemindeki verilere zarar verme suçuna benzer düzenlemeler Alman Ceza Kanunu'nda 303a maddesinde yer almaktadır. "Verilerin değiştirilmesi" kenar başlıklı 303a maddesine göre "hukuka aykırı olarak verileri silen, gizleyen, kullanılmaz hale getiren veya değiştiren kişi" iki yıla kadar hapis veya para cezası ile cezalandırılmaktadır. Alman Ceza Kanunu'nda 303a maddesi verilerin değiştirilmesini; 303b maddesi ise bilgisayar sabotajını düzenlemektedir. "Bilgisayar sabotajı" kenar başlığı ile düzenlenen 303b maddesinde bilgisayar sistemine zarar verilmesine yönelik fiillere yaptırım getirilmektedir.[2,8]

Türk Ceza Kanunu'nun 244. maddesine benzer bir hüküm Macar Ceza Kanunu'nda 300c maddesinde yer almaktadır. Buna göre söz konusu düzenlemede "kendisine yasadışı bir kazanç sağlamak veya zarar vermek kastı ile programları değiştirerek, silerek, yanlış veya eksik bilgi girerek veya diğer hukuka aykırı yollarla elektronik veri işleminin sonuçlarına müdahale eden kişi" üç yıla kadar hapis cezası ile cezalandırılmaktadır.[8]

Bilişim sistemini engelleme veya bozma fiilini yaptırıma bağlayan Türk Ceza Kanunu'nun 244. maddesine benzer norma sahip bir diğer mukayeseli hukuk metni ise Fransız Ceza Kanunu'nun 323-2. maddesinde yer almaktadır. Paris İstinaf Mahkemesi Ceza Dairesi'nin bir kararında ana bilgisayara otomatik mesajlar göndererek ana belleği yavaşlatma fiilinin bu madde kapsamında incelendiği belirtilmektedir.[9]

Alman Ceza Kanunu'nda "dolandırıcılık ve güveni kötüye kullanma" bölümünde düzenlenen 266b maddesinde; "para ve kıymetli damgalarda sahtecilik" bölümünde düzenlenen 152a maddesi ve 152b maddelerinde Türk Ceza Kanunu'nda 245. maddede düzenlenen banka veya kredi kartlarının kötüye kullanılması suçuna paralel düzenlemeler yer almaktadır. Bu noktada Alman Ceza Kanunu'nda bilişim suçları düzenlemelerinde tercih edilen kanun sistematiği gereği suçların farklı bölüm ve hükümlerde düzenlenmiş olması dikkati çekmektedir.[2]

SİBER SUÇLARIN PSİKOLOJİK DİNAMİKLERİ

Siber suçların, adli ve kriminal psikolojide bu özel suç tipine getirilen kuramsal açıklamalar çerçevesinde ayrıntılı olarak değerlendirilmesi gerekmektedir. Bireyler aktüel

alana kıyasla siber alanda, daha değişken ve daha mobil bir ruhsal doğada olup daha hızlı karar vermek durumundadır. Bu daha hızlı karar verme durumu onları dijital iletişimde hatalı ve yanlış davranışlara kolaylıkla itebilmektedir. Hatta bu yanlış davranışlar bireyin çoğu zaman suç eksenine geçiş yapabilmesine küçümsenemeyecek bir oranda neden olmaktadır. Bu kapsamda siber suçların psikolojik dinamikleri, klinik psikolojinin temel yaklaşımları ve kuramları ekseninde öncelikle değerlendirildikten sonra adli ve siber psikolojinin temel yaklaşım ve kuramlarıyla desteklenmelidir. Diğer bir ifadeyle siber suçların psikolojik dinamikleri klinik psikoloji disiplini olmadan sadece adli ve siber psikoloji disiplinleriyle izah edilemez. Daha geniş bir kapsamda siber suçların hem hukuksal boyutunun hem de adli ve siber psikolojik boyutlarının değerlendirilmesinde klinik psikoloji eğitimine sahip olan uzmanlardan destek ve görüş alınması son derece önemlidir. Ayrıca siber suçların psikolojik dinamikleri ile kriminal dinamikleri bir bütün olarak değerlendirilmelidir.[11-13]

Günümüzde ulusal ve uluslararası akademik platformda siber suçlar alanındaki hukukçuların, klinik ve adli/kriminal psikologların multidisipliner bir çerçevede daha kapsamlı ve boylamsal çalışmalar yapması bu alanın daha geniş bilimsel bir perspektifte algılanmasını kolaylaştıracaktır**.** Türk Ceza Hukuku'ndan ayrı olarak kriminal psikoloji literatüründe siber suçları farklı sınıflandırmalar altında incelemek mümkündür. Bunlardan ilki siber suçların mal varlığına ve kişilere karşı işlenen suçlar olarak ele alınmasıdır. Benzer şekilde siber suçları kriminal psikoloji literatüründe "internete özgü suçlar", "internet üzerinde de işlenebilir suçlar" ve "salt siber alan suçları" olarak üç farklı başlık altında toplayan araştırmacılar da vardır.[14,15] Tıpkı geleneksel ya da "çevrimdışı" suçlar gibi siber suçları da şiddet, yöntem ve motivasyonları bakımından incelemek mümkündür. Bu bileşenlerin yanı sıra adli ve kriminal psikoloji alanları, siber suçların mağdur, fail ve tanıklar üzerindeki etkileri, risk grupları ve suçlu profilleme çalışmaları ile de yakından ilgilenmektedir.[16]

Bilişim sistemine girme davranışının, siber psikoloji literatüründe sıklıkla sözü geçen "hackleme" eylemine karşılık geldiği söylenebilir. Bir başkasının bilişim sistemine izinsiz olarak giren ve sistem içerisinde kalan, yani "hackleme" eylemini gerçekleştiren kişiye de bu bağlamda "hacker" adı verilmektedir. Bilişim sisteminin işleyişini engellemek veya bozmak temelinde şekillenen davranış ise, siber psikoloji literatüründe "crackleme" kavramıyla karşılanmaktadır. Benzer şekilde bu hareketi gerçekleştiren kimseye de "cracker" denmektedir. Kimi araştırmacılar bu iki fiili gerçekleştirenler arasındaki ayrıma dikkat çekerken, kimi araştırmacılar da tanımlı her iki hareketi işleyenler için "hacker" kavramını kullanmayı tercih etmektedir.[15] Bu suçlar, kriminal psikoloji literatüründe internete özgü suçlar olarak karşımıza çıkmaktadır.[15] Siber alanda gerçekleştirilen davranışların ardındaki motivasyonu anlamak, bu alanda güvenliğin sağlanması ve sürdürülmesi noktasında büyük önem arz etmektedir.

Kriminal psikoloji literatüründe hackerların motivasyonları pek çok araştırmacı tarafından çalışılmıştır. Taylor, bağımlılık hissi, merak dürtüsü, güç duygusunun verdiği haz ve siyasi eylemler gibi motivasyonlar önermişken Kilger, Arkin ve Stutzman para, ego, eğlence, statü ve sosyal grup aidiyeti gibi faktörlerin altını çizmektedir.[17,18] Hackleme ve hackerlar konusunda çalışmalar yapan bir diğer araştırmacı olan Lafrance, yukarıda sözü edilen motivasyonlara intikam arzusu ve bilişim sistemindeki belli bir dosya ya da belgeye duyulan kişisel ilgiyi eklemiştir.[19] Schneier'e göre hackleme davranışının altında yatan diğer önemli motivasyonlara heyecan arayışı, saygınlık ve tanınırlığı da eklemek gerekmektedir.[20] Fötinger ve Ziegler hacker motivasyonlarına getirdikleri kuramsal açıklamalarının merkezine failin derinde yatan aşağılık duygusunu yerleştirmiştir. Buna göre hacklemenin sonucunda elde edilen güç, hackerın özgüven kazanmasına yol açmaktadır.[21] Hackleme davranışı faillerine dair profilleme çalışmaları yapılmasının gerekli olduğunu dile getiren ilk araştırmacı Donato olmuştur.[22] Literatürde hackerların genellikle tek başına hareket eden, eğitim seviyesi yüksek genç erkekler olduğu pek çok araştırmacı tarafından dile getirilmiştir.[23-25] Woo, hackerlarda daha yüksek narsisizm ve saldırganlık skorları bulgulamıştır.[26]

Banka veya kredi kartlarının kötüye kullanılması davranışı, kriminal/siber psikoloji literatüründe geniş bir spektrum hâlinde ele alınmaktadır. Bu bağlamda, bu davranışı kriminal/siber psikoloji literatüründe kimlik hırsızlığı ve sahtecilik başlığı altında incelemek mümkündür. Banka veya kredi kartlarının kötüye kullanılmasının yanı sıra çok sık karşımıza çıkan bir kimlik hırsızlığı ve sahtecilik yöntemi sahte sosyal medya hesaplarıyla çevrimiçi arkadaşlık sitelerindeki sahte hesaplardır.[27] Bu sahte hesaplarda kişiler kendilerini başkaları gibi tanıtarak bir başkasının hesap detayları ve şifreler gibi özel bilgilerine ulaşmayı, kredi kartı ya da diğer alışveriş kanallarıyla ilgili bilgilerini ele geçirmeyi amaçlamakta veya ikinci kişilerden doğrudan para talep etmekte; bunu da sıklıkla tuzak e-postalar göndererek (phishing) gerçekleştirmektedir. Kimlik hırsızlığı ve sahteciliğini, kriminal/siber psikoloji literatüründe internet üzerinde de işlenebilen suçlar başlığı altında ele almak mümkündür. Literatürde kimlik hırsızlığı ve sahte-

ciliğe maruz kalmış kimselerde gözlenen tablolar arasında utanç duygusu ve depresyona eşlik eden travma sonrası stres bozukluğu, somatik semptomlar ve reviktimizasyon gösterilmektedir.[28-30]

İnternetin günlük yaşam ile profesyonel hayatın merkezine yerleşmesiyle birlikte, Türk Ceza Kanunu'ndaki tanımlamalardan ayrı olarak, pek çok farklı suç tipinin doğuşu, pek çok farklı suç tipinin de geleneksel (çevrimdışı) yöntemlerin yanı sıra çevrimiçi yöntemlerle de işlenebilir biçimlerinin ortaya çıkması kolaylaşmıştır. Çevrimiçi çocuk istismarı, siber zorbalık ve siber stalking (ısrarlı takip) bu şekilde ortaya çıkmış ya da biçim değiştirmiş suçlar arasında sayılabilir.

Siber alanın tanıdığı anonimiteyle yetişkinlerin cinsel haz amacıyla çocuklara ve ergenlere ulaşmasının daha kolay hâle geldiğini söylemek mümkündür. Yar'a göre çevrimiçi çocuk istismarının (i) iletişimin sadece siber alanla sınırlı kaldığı, fail ve çocuğun cinsel içerikli yazışmalar ya da konuşmalar yaptığı, çoğunlukla her iki taraf için de mastürbasyonun eşlik ettiği "sanal istismar" ve (ii) çevrimiçi iletişimin sonunda yüz yüze bir buluşmaya ve fiziksel temasa evrildiği istismar olmak üzere iki biçimi vardır.[31] Geleneksel istismar vakalarından ayrı olmak üzere çevrimiçi istismar vakalarında kurbanların küçük çocuklar değil, çoğunlukla ergenlerden oluştuğu ve mağdur konumundaki ergenlerin faili tanıma olasılıklarının daha düşük olduğu bulgulanmıştır.[15] Daha küçük yaşlardaki çocuklar internette daha kısıtlı sayıda, daha yoğun ebeveyn gözetimi altında vakit geçirdiklerinden çevrimiçi cinsel istismarın daha ziyade hebefilik bir örüntüde seyrettiğini dile getirmek mümkündür. Lanning, çevrimiçi hebefillerin motivasyonları arasında dürtüsellik, öfke, merak ve güç arzusu gibi faktörlerin altını çizmiştir.[32] Wolak, Finkelhor, Mitchell ve Ybarra ise çevrimiçi hebefillerin dürtüsel ya da sadist olmadıklarını; aksine kurbanlarıyla buluşmadan önce ilişki kurabilecek ve onları buluşmaya ikna edebilecek kadar sabırlı ve planlı olduklarını ifade etmektedir.[33] Çevrimiçi cinsel istismarın risk grupları arasında sıklıkla adı geçenler sorunlu aile yaşamları olan, fiziksel olarak çekici ve düşük özgüvenli ergenlerdir.[34] Çoğu çevrimiçi cinsel istismar vakasında kurbanın kız çocukları olduğu, eğer erkek çocukları mağdursa failin genellikle erkek olduğu; cinsiyet fark etmeksizin kurbanların büyük çoğunluğunun ise on dört yaşından büyük olduğu bulunmuştur.[35]

Çevrimiçi çocuk istismarı konusunda internetle ilişkili cinsel suçlar bakımından en önemli noktalardan biri çocuk pornografisidir. Çocuk pornografisi yeni bir mesele olmamakla birlikte bilgisayar kameraları ve akıllı telefonlar gibi kayıt cihazlarının yanı sıra söz konusu görüntülerin yayılabileceği paylaşım siteleri gibi kanalların da sayı ve kullanım sıklığının artmasıyla erişimi daha kolay bir hâl almıştır. Yapılan araştırmalar çevrimiçi çocuk pornografisi kullanıcılarının çoğunlukla hiç evlenmemiş, internet bağımlılığı belirtileri göstermesi muhtemel, eğitimli kimseler olduklarını göstermektedir.[36-38] Cinsel içerikli görüntülerin İnternet'te ne kadar yayıldığını kestirmek ve olası bütün kopyaları yok etmek çok da olası olmadığı için çevrimiçi istismar mağdurlarının psikolojik dinamiklerinin, geleneksel istismar mağdurlarında gözlenen dinamiklerden farklılaştığı düşünülmektedir. Aktüel alanda yaşanan istismardan farklı olarak siber alandaki istismarın kurbanları genellikle küçük çocuklar değil ergenler olmaktadır. Geleneksel istismar durumunda bu çocuklar en sık kendi evleri gibi özel alanlarda ve tanıdıkları ya da güvendikleri kimseler tarafından istismar edilmekteyken çevrimiçi istismar kurbanı ergenlerin yalnızca %14 gibi bir oranı daha önceden tanıdıkları kimseler tarafından istismara uğramakta, siberalanın yer, zaman ve sınırlardan muaf doğası itibariyle bu istismar biçimi de hayatlarının bütününe yayılmaktadır. Ergenlerin yoğun sosyal medya kullanımı istismarcılar için bu yaş grubunu daha ulaşılabilir kılmaktadır. Siberalanın görece anonim yapısı, ergenlerin özel bilgi ve görüntülerini istismarcılarla paylaşma ihtimalini artırmakta, bu yaş grubunu daha ulaşılabilir kılmaktadır. Literatürde her iki istismar türünün sonucu olarak da mağdurlarda depresyon, madde kötüye kullanımı ve travma sonrası stres bozukluğu başta olmak üzere yaşamın ilerleyen yıllarına kadar devam eden olumsuz etkiler gözlendiği ifade edilmektedir.[15]

Siber zorbalık ve siber stalking, internet ve özellikle de sosyal medyanın yaygınlaşmasıyla farklı bir biçim alan diğer olgulardır. Daha önceden de bilinen bir kavram olan akran zorbalığı, teknolojideki güncel gelişmelerle birlikte biçim değiştirerek siber zorbalık hâlini almış ve bu iletişim araçlarını çok yoğun olarak kullanan bir popülasyon olarak ergenlerle okul çağı çocuklarını tehdit eder olmuştur. Hem siber zorbalık hem de siber zorbalık mağduriyetinin anksiyete, depresyon, somatizasyon, olumsuz benlik algısı ve internet bağımlılığı gibi faktörlerle yüksek bir korelasyon içerisinde olduğu bulunmuştur. Siber zorbalık ve mağduriyeti açısından sözü geçen bu faktörlerin hem birer belirti hem de birer yordayıcı olduğunu söylemek mümkündür.[39] Israrlı takibin güncel bir türü olarak karşımıza çıkan siber stalking failleri çoğunlukla erkeklerden, mağdurları ise büyük oranda kadınlardan oluşmaktadır.[40] Tıpkı siber zorbalık gibi siber stalking mağdurlarında da depresyon, psikosomatik rahatsızlıklar, uyku bozuklukları ve panik atakları görülme sıklığı artmaktadır.[41]

Sonuç olarak daha önce ifade ettiğimiz üzere siber suçların, adli ve kriminal psikolojide bu özel suç tipine getirilen kuramsal açıklamalar çerçevesinde ayrıntılı olarak değerlendirilmesi gerekmektedir. Bireyler aktüel alana kıyasla siber alanda, daha değişken ve daha mobil bir ruhsal doğada olup daha hızlı karar vermek durumundadır. Bu daha hızlı karar verme durumu onları dijital iletişimde hatalı ve yanlış davranışlara kolaylıkla itebilmektedir. Hatta bu yanlış davranışlar bireyin çoğu zaman suç eksenine geçiş yapabilmesine küçümsenemeyecek bir oranda neden olmaktadır. Bu kapsamda siber suçların psikolojik dinamikleri, klinik psikolojinin temel yaklaşımları ve kuramları ekseninde öncelikle değerlendirildikten sonra adli ve siber psikolojinin temel yaklaşım ve kuramlarıyla desteklenmelidir. Diğer bir ifadeyle siber suçların psikolojik dinamikleri klinik psikoloji disiplini olmadan sadece adli ve siber psikoloji disiplinleriyle izah edilemez. Daha geniş bir kapsamda siber suçların hem hukuksal boyutunun hem de adli ve siber psikolojik boyutlarının değerlendirilmesinde klinik psikoloji eğitimine sahip olan uzmanlardan destek ve görüş alınması son derece önemlidir. Ayrıca siber suçların psikolojik dinamikleri ile kriminal dinamikleri bir bütün olarak değerlendirilmelidir.

Yasal düzenlemeler ve hukuk sistemleri ise toplumun içinde bulunduğu sosyokültürel durum ve teknolojik gelişmelere bağlı olarak değişmek ve gelişmek durumundadır. Günümüzde pek çok suç tipinin siber alanda bir karşılık bulabilecek şekilde işlenebilir olduğundan bahsetmek mümkündür. Dahası siber alan bu süreçte hem faile hem de mağdura anonimlik katmakta ve bu iki unsurun bir araya gelmesini kolaylaştırmaktadır. Teknolojinin ilerlemesi ile çeşitlenen, bilişim alanında hukuka aykırılık teşkil edecek her bir eylemin Türk Ceza Kanunu'nda karşılık bulabilmesi için küreselleşen iletişim ağlarında yaşanan güncel ihlallere yönelik suç tipi düzenlemelerinde gerekli revizyonlar yapılmalıdır.

Siber alanda kendilerine yeni birer tezahür bulan bu suçların yanı sıra internetin gelişimi siber stalking, hackleme, crackleme, kimlik hırsızlığı gibi yepyeni kavramları da hayatımıza katmıştır. Hem yeni yasal düzenlemeler hem de önleme programları açısından bu konularda çok daha fazla araştırmaya ihtiyaç duyulmaktadır. Özellikle siber zorbalık konusunda psikoloji, sosyoloji ve hukuk alanlarının multidisipliner çalışmalarının sayısının artması aktüel hayatın her alanında yaşanabilme ihtimali olan bu durumun daha iyi anlaşılmasını sağlayacaktır. Fail ve mağdur tipolojilerine ilişkin araştırmaların önleyici programlar geliştirilmesi ve siber alanda işlenen suçlar ile mücadele noktasında oluşan farkındalığın artırılmasına katkı sağlayacağı düşünülmektedir.

KAYNAKLAR

1. Gürkaynak M, Adem Aİ. "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler." Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi.2011;(16)2:263-79.
2. Erdağ Aİ. Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda).Gazi University Journal of Law. 2010;14(2):275-303.
3. Eker ÖU. "Türk Ceza Hukuku'nda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu. Journal of Union of Turkish Bar Asssociation. 2006;(62):101-31.
4. Altunok E, Vural AF. Bilişim Suçları. Journal of Denetişim. 2011;(8):74-84.
5. Turan M, Külcü Ö. Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi. The Journal of Turkish Librarianship. 2014; 28(1):18-46.
6. Erdoğan Y. Bilişim Sistemine Girme ve Kalma Suçu. Dokuz Eylül University Faculty of Law Rewiev. 2010;12(Özel Sayı):1363-433.
7. Parlar A. Türk Ceza Hukukunda Bilişim Suçları.1. Baskı. Ankara: Bilge Yayınevi; 2011.p.16-54.
8. Artuk ME, Gökcen A, Yenidünya AC. Ceza Hukuku Özel Hükümler.14. Baskı. Ankara: Adalet Yayınevi; 2014. p.744-76.
9. Tezcan D, Erdem MR, Önok RM. Teorik ve Pratik Ceza Özel Hukuku.11.Baskı. Ankara: Seçkin Yayıncılık; 2014. p.841-57.
10. Resmi Gazete (09.08.2014/29083) Sanal Ortamda İşlenen Suçlar Sözleşmesi; 2014.
11. Öztük E. Travma ve Dissosiyasyon. 1. Baskı. İstanbul: Nobel Tıp Kitabevleri; 2017. p. 1-101.
12. Öztürk E, Çalıcı C. Modern Toplumda Kimlik, "Siber Dissosiyasyon" ve "Siber Alter": Teorik ve Klinik Bir Yaklaşım. Öztürk E, editör. Ruhsal Travma ve Dissosiyasyon. Ankara: Türkiye Klinikleri; 2018. p.39-47.
13. Öztürk E. Travma Merkezli Alyans Model Terapi: Dissosiyatif Kimlik Bozukluğunun Psikoterapisi. Öztürk E, editör. Ruhsal Travma ve Dissosiyasyon. Ankara: Türkiye Klinikleri; 2018. p.31-8.
14. Power A. The online public or cybercitizen. SCRIPTed. 2010;7:185.
15. Kirwan G, Power A. The psychology of cyber crime. Pennsylvania: IGI Global Press. Crossref; 2011.
16. Welsh BC, Farrington DP. Surveillance for crime prevention in public space: Results and policy choices in Britain and America. Criminology & Public Policy. 2004;3(3):497-526.
17. Taylor P. Hackers. London: Routledge; 1999.
18. Kilger M, Arkin O, Stutzman J. Profiling. In: The Honeynet Project, ed. Boston, MA: Addison-Wesley Professional. 2004; p.505-56.
19. Lafrance Y. Psychology: A precious security tool. SANS GSEC Certification, Practical Assignment; 2004.
20. Schneier B. We are all security consumers. IEEE Security & Privacy. 2003;1:104.
21. Fötinger CS, Ziegler W. Understanding a hacker's mind–A psychological insight into the hijacking of identities. Danube-University Krems, Austria: RSA Security; 2004.
22. Donato L. An introduction to how criminal profiling could be used as a support for computer hacking investigations. Journal of Digital Forensic Practice. 2009;2(4):183-95.

23. Bissett A, Shipton, G. An investigation into gender differences in the ethical attitudes of IT professionals. ETHICOMP99, Rome; 1999.
24. Levy S. Hackers: Heroes of the computer revolution(Vol. 14). Garden City, NY: Anchor Press/Doubleday; 1984.
25. Turgeman-Goldschmidt O. Identity construction among hackers. Cyber criminology: Exploring internet crimes and criminal Behavior. 2011.p.31-51.
26. Woo HJ. The hacker mentality: Exploring the relationship between psychological variables and hacking Activities; 2003 (Doktora tezi, uga).
27. Whitty MT, Buchanan T. The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking. 2012;15(3):181-3.
28. Carey L. Can PTSD affect victims of identity theft: Psychologists say yes. Associated Content. Retrieved on November, 21, 2009.
29. Sharp T, Shreve-Neiger A, Fremouw W, Kane J, Hutton S. Exploring the psychological and somatic impact of identity theft. Journal of Forensic Science. 2003;49(1):1-6.
30. Grubb A, Harrower J. Attribution of blame in cases of rape: An analysis of participant gender, type of rape and perceived similarity to the victim. Aggression and violent Behavior. 2008;13(5):396-405.
31. Yar M. Cybercrime and Society. London: Sage; 2006.
32. Lanning KV. Child molesters: A behavioral analysis for law-enforcement officers investigating the sexual exploitation of children by acquaintance molesters. National Center for Missing & Exploited Children; 2001.
33. Wolak J, Finkelhor D, Mitchell KJ, Ybarra ML. Online "predators" and their victims: myths, realities, and implications for prevention and treatment. American Psychologist. 2008;63(2), 111.
34. Elliott M, Browne K, Kilcoyne J. Child sexual abuse prevention: What offenders tell us. Child abuse & Neglect. 1995;19(5):579-94.
35. Wolak J, Mitchell KJ, Finkelhor D. Online Victimization of Youth: Five Years Later. 2006.
36. Siegfried KC, Lovely RW, Rogers MK. Self-reported online child pornography behaviour: A psychological analysis. International Journal of Cyber Criminology. 2008;2(1):286-97.
37. Blundell B, Sherry M, Burke A, & Sowerbutts S. Child pornography and the internet: Accessibility and policing. Australian Police Journal. 2002;56(1):59-65.
38. Burke A, Sowerbutts S, Blundell B, Sherry M. Child pornography and the Internet: Policing and treatment issues. Psychiatry, Psychology and Law. 2002;9(1):79-84.
39. Ildırım E, Çalıcı C, Erdoğan B. Psychological correlates of cyberbullying and cyber-victimization. The International Journal of Human and Behavioral Science. 2017;3(2):7-21.
40. Pittaro ML. Cyber stalking: An analysis of online harassment and intimidation. International Journal of Cyber Criminology. 2007;1(2):180-97.
41. İnce B., Ildırım E. (2017). Israrlı Takibin Yeni Hali: Siber Stalking. 14. Adli Bilimler Kongresi. 2017. (Özet Bildiri/Poster). (Yayın No: 3568812).