UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE

Gercke, M. (2012) Understanding Cybercrimes: Phenomena, Challenges and Legal Response. ITU:International Telecommunication Union. pp.280

Ayşe Yaşar ÜMÜTLÜ*

Orcid ID: https://orcid.org/0000-0001-9500-5338

Eserin yazarı Prof. Dr. Marco Gercke, uluslararası bir uzman olarak, hükümetlere ve uluslararası kuruluşlara, Siber Suçlar, Siber Güvenlik, Bilişim ve İletişim Teknolojileri ile ilgili hukuk dallarında danışmanlık yapmaktadır. İnternet suçlarının hukuki yönleriyle ilgilenen bağımsız bir küresel düşünce kuruluşu olan Siber Suç Araştırma Enstitüsü'nün direktörüdür. Siber suç odaklı ceza hukuku alanında doktora derecesine sahip olup, birkaç yıldır Köln Üniversitesi'nde Siber Suçlar, Uluslararası Ceza Hukuku ve Avrupa Ceza Hukuku ile ilgili hukuk dersleri vermektedir. Araştırmalarının odak noktası, siber suçlarla ilgili hukukun uluslararası yönleridir. Bu bağlamda, Avrupa Konseyi, Avrupa Birliği, BM ve Uluslararası Telekomünikasyon Birliği gibi birçok uluslararası kuruluşta uzman olarak görevlerde bulunmaktadır. Gercke, Siber Suçlar mevzuatının hazırlanması konusunda birçok ülkeyle çalışmalar yapmıştır. Araştırmasının temel unsurları, siber suçlara karşı mücadele ile ilgili zorluklar ve medeni hukuk sistemlerinde yasal müdahalenin geliştirilmesinde karşılaştırmalı hukuk konularıdır. En son araştırmaları ise, Teröristlerin İnternet Kullanımına Hukuki Müdahale, Kimlik Hırsızlığı, Kimlik Hırsızlığı ile Mücadelede İç İş birliği, Kara Para Aklama ve Terörün Finansmanı faaliyetlerini içeren hususlarda İnternet teknolojisi ve İnternet Servis Sağlayıcılarının sorumluluğu gibi konuları kapsamaktadır. Makale ve kitaplara ek olarak, Avrupa Konseyi ve Uluslararası Telekomünikasyon Birliği için karşılaştırmalı hukuk analizi de dahil olmak üzere birçok çalışması var. Siber suçlarla ilgili en son eseri tüm BM dillerine çevrildi. Gercke, ITU Üst Düzey Uzmanı olarak 2008 Octopus Konferansı'nda kabul edilen siber suçlara karşı kolluk kuvvetleri ve internet hizmet sağlayıcıları arasındaki iş birliğine yönelik kılavuzların hazırlanmasını desteklemek için Avrupa Konseyi tarafından

* Dr. Ögr. Gör. Necmettin Erbakan Üniversitesi, ayumutlu.ajanda@gmail.com .

kurulan çalışma grubunun eş başkanıydı. Ayrıca Alman Barosu üyesi ve Alman Hukuk ve Bilişim Derneği Ceza Hukuku Departmanı Sekreteridir.[21]

Eserin **giriş** kısmında, yazar, eserin yazılış amacını, gelişmekte olan ülkelerde artan siber tehditlerin ulusal ve uluslararası sonuçlarını daha iyi anlamalarına yardımcı olmak, bununla birlikte mevcut ulusal, bölgesel ve uluslararası araçların gerekliliklerini değerlendirmek ve ülkelere sağlam bir yasal temel oluşturmalarında yardımcı olmayı sağlamak biçiminde belirlediğini görüyoruz. (tanıtım, iii) Eserde kullanılan üslup hukuki terimler içerse de oldukça açık anlaşılabilir nitelikte ve akıcı bir düzeydedir. Her bölüm sıra dışı bir metotla, yoğun bir referans bibliyografyasından o bölüm için seçilenlerin tanıtılması ile başlıyor.

Eser, altı ana bölümden oluşuyor. **Birinci bölümde** yazar, siber suç olgusuna genel bir bakış sunuyor. Teknolojik altyapı ve hizmetler konusunda gelişmelerin öncelikle gelmiş ülkelerin talepleri için tasarlansa da gelişmekte olan ülkelerde de yayıldığını belirtiyor. Bunun en temel nedeninin de e-devlet, e-ticaret, e-eğitim, e-sağlık ve e-çevre gibi uygulamaların kalkınmanın aracı olarak görülmesinden kaynaklandığını vurguluyor. Kalkınma hedeflerine ulaşılmasını, yoksulluğun azaltılmasını, sağlık ve çevre koşullarının iyileştirilmesini kolaylaştırabilir nitelikte görülen bu uygulamaları talep etmelerinin nedenini bu şekilde belirliyor. (s.1) Avantajlar ve riskleri de ele aldığı bu bölümde, teknolojik uygulamaların günlük yaşamın birçok yönüne dahil edilmesi, modern bilgi toplumu kavramının gelişmesine yol açması bakımından büyük fırsatlar sunduğunu vurguluyor. Özellikle bilgiye sınırsız erişim ve hızlı bilgi akışının demokrasiyi destekleyecek bir araç olarak önemini kabul ediyor. Doğu Avrupa ve Kuzey Afrika'daki bu yöndeki gelişmeleri örnek olarak veriyor. Teknik gelişmeler olarak çevrimiçi bankacılık ve alışveriş, mobil veri hizmetlerinin kullanımı gibi uygulamaların günlük yaşamı kolaylaştırmasına yönelik örneklerle görüşünü destekliyor. Fakat öte yandan, bilgi toplumunun büyümesine oldukça ciddi tehditlerin de eşlik ettiğini belirtiyor. Mevcut altyapı ve benzeri sistemlerden, örneğin su ve elektrik temini gibi temel hizmetler artık bilişim teknolojilerine dayandığını hatırlatıyor. Arabalar, trafik kontrolü, asansörler, klima ve telefonlar da bu teknolojilerin sorunsuz çalışmasına bağlı olması ve bunlarda olabilecek arızlar ya da bunlara yapılabilecek saldırıların, tehditlerden biri olduğunu anlıyoruz.

[21] https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Aug-SSC-EGOV/Bio_Marco_Gercke.pdf

Dolayısıyla topluma yeni ve kritik şekillerde zarar verme potansiyeline sahip olduklarını ortaya koyuyor. Bunun yanında, çevrimiçi dolandırıcılık ve bilgisayar korsanlığı saldırıları gibi siber suçların neden olduğu mali zararın çok büyük olduğunu anlatıyor. (s.2) Bu konuda önemli birkaç örnek olarak 2003 yılında, kötü amaçlı yazılımlar 17 milyar ABD doları'na varan zararlara neden olduğunu, bazı tahminlere göre ise, siber suçlardan elde edilen gelir 2007'de 100 milyar ABD dolarını aşarak ilk kez yasadışı uyuşturucu ticaretini geride bıraktığını iddia ediyor. Ayrıca işletmelerin yüzde 60'ının, Amerika Birleşik Devletlerinden kaynaklanan siber suçların kendilerine fiziksel suçtan daha maliyetli olduğuna inandığını iddia ediyor. "Siber güvenlik ve siber suçlar", konusu bu bölümdeki alt başlıklar arasında yer alıyor. Siber suçları caydırmak, ulusal bir siber güvenlik ve kritik bilgilerin altyapısı koruması stratejisinin neden ayrılmaz bir bileşeni olduğunu açıklıyor. Özellikle, ulusal kritik altyapıları etkilemeye yönelik faaliyetler ve suç amaçlı veya diğer amaçlar için bilişim teknolojilerinin kötüye kullanımına karşı uygun bir mevzuatın kabul edilmesinin gerekçeleri ile ilgili hususları içeriyor. Yazar siber güvenlik konularının, ulusal düzeyde, hükümet yetkilileri, özel sektör ve vatandaşlar koordineli hareket etmesini gerektiren ortak bir sorumluluk gerektirdiğinin altını çiziyor. Olayların önlenmesi, müdahalesi ve bu yöndeki çalışmaların iyileştirilmesi konularında birlikteliğin önemini vurguluyor. Bölgesel ve uluslararası düzeyde de iş birliği ve koordinasyon gerektirdiğine dikkat çekiyor. Bu bağlamda Küresel Siber Güvenlik Gündemi'nin beş çalışma alanı üzerine kurulu yedi ana stratejik hedefinden bahsediyor. Bunlar 1) Yasal önlemler; 2) Teknik ve prosedürel önlemler; 3) Organizasyon yapıları; 4) Kapasite geliştirme ve 5) Uluslararası iş birliği olarak belirlenmiş. Bunların genel olarak nasıl şekillendiğini açıklıyor. (s.3) Yine bu bölümde, siber suçların genellikle uluslararası bir boyutu olduğunu örneklerle açıklanıyor. Mesela, yasa dışı içeriğe sahip e-postaların, göndericiden alıcıya aktarım sırasında genellikle birkaç ülkeden geçer veya yasa dışı içerik ülke dışında depolanması şeklinde gerçekleşmesi gibi. Bu nedenle de siber suç soruşturmalarında, ilgili ülkeler arasında yakın iş birliğinin önemini açıklıyor. Fakat mevcut karşılıklı adli yardım anlaşmaların resmi, karmaşık ve çoğunlukla da zaman kaybettiren prosedürlere dayandığını ve buna ek olarak genellikle bilgisayara özgü soruşturmaları kapsamadığını anlatıyor. Bu nedenle de olaylara hızlı müdahale için prosedürlerin yanı sıra uygun prosedürlerin oluşturulmasında uluslararası iş birliğinin neden hayati önem taşıdığını vurguluyor. (ss:2-4) Bu konuda yazarın belirlediği, önemli bir sorun var. Küresel standartların uyumlaştırılmasının ulusal ceza hukukunun gelişimi üzerindeki etkisi meselesi. Çünkü yazarın bu bölümde verdiği bilgilere göre, yasadışı içerik açısından, internet kullanıcıları dünyanın her yanından bilgilere erişebilir ve bu sayede yurtdışında yasal olarak

mevcut olan, kendi ülkelerinde yasa dışı olabilecek bilgilere erişmelerini de sağlıyor. Böylece teknik standardizasyondan kaynaklanan gelişmeler, teknoloji ve hizmetlerin küreselleşmesinin çok ötesine geçmekte ve ulusal kanunların uyumlaştırılmasında sorunlara yol açabilmektedir. Üstelik, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin Birinci Protokolü (Siber Suçlar Sözleşmesi) üzerindeki müzakerelerin ulusal hukuk ilkelerinin, teknik gelişmelerden çok daha yavaş değiştiğini ortaya koyduğunu öğreniyoruz. Gelişmekte olan ülkeler için bu nedenle siber güvenliği ve uygun siber suç mevzuatını teşvik etmek için teknik önlemlerin geliştirilmesi hem gelişmiş ülkeler hem de gelişmekte olan ülkeler için son derece önemli olduğunu belirtiyor. Üstelik bilgisayar ağlarına güvenlik önlemleri ve koruma önlemleri almanın maliyetleriyle karşılaştırıldığında, en baştan alınan önlemlerin daha ucuz olacağına dair de uyarı da bulunuyor. Bu nedenle de yazar, gelişmekte olan ülkelerin siber suçla mücadele stratejilerini en başından itibaren uluslararası standartlarla uyumlu hale getirmeleri gerektiğini ısrarla belirtiyor.

İkinci Bölümde, suçların nasıl işlendiğine ilişkin açıklamalar ve bilgisayar korsanlığı, kimlik hırsızlığı ve hizmet reddi saldırıları gibi en yaygın siber suç suçlarının açıklamaları yer alıyor. Siber suçların soruşturulması ve kovuşturulmasıyla ilgili zorluklara genel bir bakış açısı ortaya koyuyor. Eserde ifade edilen şekliyle, Birleşmiş Milletler Suçun Önlenmesi ve Suçluların Tedavisi Kongresinde ve bir çalıştayda iki tanım geliştirildiğini öğreniyoruz. Buna göre "Dar anlamda siber suç (bilgisayar suçu), güvenliği hedef alan elektronik operasyonlar aracılığıyla yönlendirilen her türlü yasa dışı davranışı kapsıyor; bilgisayar sistemleri ve bunlar tarafından işlenen veriler gibi. Daha geniş anlamda siber suçlar (bilgisayarla ilgili suçlar), bir bilgisayar sistemi veya ağı aracılığıyla veya bunlarla ilgili olarak işlenen her türlü yasa dışı davranışı, bir bilgisayar sistemi veya ağı aracılığıyla yasa dışı bulundurma ve bilgi sunma veya dağıtma gibi suçları kapsıyor." (s.11) Eserde yapılan diğer siber suç tanımlarından yaygın olanları ve onlarla ilgili hukukta oluşabilecek problemleri kısmen ortaya koyuyor. Yazar ayrıca siber suç tipolojisinin nasıl belirlenebileceğine dair zorluklar hakkında bilgiler veriyor. "Siber suç" terimi, çok çeşitli cezai davranışları kapsamak için kullanıldığını öğreniyoruz. Sözleşme'de bir yaklaşım bulunabilir. Dört farklı suç türü arasında ayrım yapan Siber Suçlar hakkında:b

1. Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar;

2. Bilgisayarla ilgili suçlar;

3. İçerikle ilgili suçlar ve

4. Telif hakkıyla ilgili suçlar. (s.12)

Bu tipoloji, kategoriler arasında ayrım yapmak için tek bir kritere dayanmadığından yazar tarafından çok tutarlı bulunmuyor. İlk üç kategori, yasal koruma nesnesine odaklanır: "bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar"; içerikle ilgili suçlar; ve telif hakkı ile ilgili suçlar. "Bilgisayarla ilgili suçların" dördüncü kategorisi, yasal korumanın amacına değil, suçun işlenmesinde kullanılan yönteme odaklandığını açıklıyor. Ayrıca, suç eylemlerini tanımlamak için kullanılan bazı terimlerin (siber terörizm veya kimlik avı gibi) birkaç kategoriye giren eylemleri kapsadığını belirtiyor. Dolayısıyla çok tutarlı olmasa da bu kategorilerin, siber suç olgusunu tartışmak için yararlı bir temel olarak hizmet edebileceğini düşünüyor. Bilgisayar suçları ve siber suçların gelişimi alt başlığında, 60'lar, 70'ler, 80'ler, 90'lar ve 21. yüzyıl boyunca gelişmelerin ne şekilde olduğunu ortaya koyuyor. İçinde bulunduğumuz 21. yüzyıl hakkında verdiği bilgi ile örneklendirecek olursak; 21. yüzyılı bilgisayar suçları ve siber suçlarda yeni eğilimlerin keşfedildiği bir yüzyıl olarak görüyor. Yeni milenyumun ilk on yılına, "phishing", ve "botnet saldırıları" (VoIP) iletişimi" ve "bulut bilişim" gibi yeni, son derece karmaşık suç işleme yöntemleri ve kolluk kuvvetlerinin ele alması ve soruşturması daha zor olan konuların hakim olduğunu ifade ediyor. Ona göre değişen sadece yöntemler değil, aynı zamanda etkisidir. (s.13) Çünkü eserden de anlaşılıyor ki, suçlular saldırıları otomatikleştirebildikçe, suçların sayısı arttı. Bu suçların çoğu bilgilerin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar, veri ve sistemler üzerinden gerçekleştiriliyor. Bildiğimiz gibi, hassas içerikli veriler genellikle bilgisayar sistemlerinde depolanıyor. Bununla birlikte, bilgisayar sistemi İnternet'e bağlıysa, suçlular dünyanın hemen her yerinden İnternet aracılığıyla bu bilgilere erişmeye çalışabilirler. Bu nedenle de internet, ticari sırları elde etmek için giderek daha fazla kullanılmaktadır. Fakat hassas içerikli verilerin değeri ve erişim yeteneği uzaktan veri casusluğunu oldukça ilginç hale getirmiş durumda olduğunu öğreniyoruz. Bir veri casusluğu örneği olarak, 1980'lerde, bir dizi Alman bilgisayar korsanı ABD hükümetine ve askeri bilgisayar sistemlerine girmeyi, gizli bilgileri elde etmeyi ve bu bilgileri farklı bir ülkeden ajanlara satmayı başarmışlar. (s.18) Özellikle de bu konularda OECD'nin, kriptografinin önemini vurguladığını belirtiyor. Yazara göre, bilgi depolayan kişi veya kuruluş uygun koruma önlemleri alırsa, kriptografik koruma herhangi bir fiziksel korumadan daha verimli

olabilir. Suçluların hassas bilgileri elde etmedeki başarısı genellikle koruma önlemlerinin olmamasından kaynaklanmakta olduğunu vurguluyor. Ona göre, suçlular genellikle ticari sırları hedef alsalar da, özel bilgisayarlarda depolanan veriler de giderek daha fazla hedef alınıyor. Yazar, kullanıcıların genellikle bilgisayarlarında banka hesabı ve kredi kartı bilgilerini depoladığını ve suçluların bu bilgileri (örneğin banka hesap bilgileri, para transferleri yapmak veya üçüncü bir tarafa satmak gibi) kendi amaçları için kullanabildiklerini anlatıyor. Örneğin bu bilgilerin 60.238 USD'ye kadar satıldığını, Hacker'ların özel bilgisayarlara odaklanmasının arkasındaki nedenin özel bilgisayarlar genellikle daha az iyi korunduğundan, özel bilgisayarlara dayalı veri casusluğu muhtemelen daha da karlı görüldüğünü anlatıyor. Yazar ayrıca telif hakkı ve ticari markayla ilgili suçlar, bilgisayarla ilgili suçlar ya da bunların karması halinde kombine başkaca suçların da işlenebildiğini yine örneklerle açıklıyor. (s.18)

Suçluların, mağdurların bilgisayarlarına erişmek için çeşitli teknikler kullanıldığını, korumasız portları taramak için yazılımlar veya koruma önlemlerini atlatmak için yazılımlar ve ayrıca "sosyal mühendislik" yollarıyla büyük ölçüde insan etkileşimine dayanan ve genellikle diğer insanları normal güvenlik prosedürlerini kırmaları için kandırmayı içeren eylemleri hakkında bilgilendiriyor. Bunu yasa dışı erişim bağlamında, bilgisayar sistemlerine erişim sağlamak amacıyla insanların manipülasyonunu olarak tanımlıyor. Sosyal mühendislik yoluyla suç işlemenin genellikle çok başarılı olduğunu çünkü bilgisayar güvenliğindeki en zayıf halkanın genellikle bilgisayar sistemini çalıştıran kullanıcılar olarak belirlendiğini öğreniyoruz. Bir örnek olarak, yazar, son zamanlarda siber uzayda işlenen önemli bir suç haline gelen ve görünüşte resmi bir elektronik iletişimde güvenilir bir kişi veya işletme (örneğin finans kurumu) gibi davranarak hassas bilgileri (şifreler gibi) hileli bir şekilde elde etme girişimlerini tanımlayan "phishing"i veriyor. (s.19) Bunun yanında iyi eğitimli bilgisayar kullanıcılarının, sosyal mühendislik kullanan suçlular için kolay kurbanlar olmadığını vurguluyor. Sonuç olarak, kullanıcı eğitimi herhangi bir siber suçla mücadele stratejisinin önemli bir parçası olması gerektiği konusunda uyarıyor. Ek olarak, yasa dışı erişimi önlemek için teknik önlemler de alınması gerektiğinin de altını çiziyor.

Üçüncü ve dördüncü bölümlerde ise siber suçlarla mücadelede uluslararası ve bölgesel kuruluşlar tarafından üstlenilen bazı faaliyetlerin bir özetinin verildiğini görüyoruz. Siber

suçlarla mücadelenin zorlukları, yasal zorluklar ile birlikte açıklanıyor. Siber suçla mücadele stratejileri ve siber güvenlik stratejisinin ayrılmaz bir parçası olarak siber suç mevzuatlarının nasıl düzenlenmeleri gerektiğine dair fikirler yer alıyor. (s.82) Bu bağlamda siber suçlarla mücadelede mevzuatları düzenleyicilerin rolü ve bu yönde geliştilmesi gereken politikaları tartışıyor. (s. 101) Siber suçların soruşturulması ve kovuşturulması, kolluk kuvvetleri için zorluklar içermesiyle alakalı, sadece siber suçlarla mücadelede yer alan kişileri eğitmek değil, aynı zamanda yeterli ve etkili mevzuat taslağı hazırlamanın da önemini vurguluyor. Bu bölümde kısaca, siber güvenliğin desteklenmesine yönelik temel zorluklar ve mevcut araçların yetersiz kalabileceği ve özel araçların uygulanmasının gerekli olabileceği alanları belirlemiş.

Beşinci bölümde ise, maddi ceza hukuku, usul hukuku, dijital delil, uluslararası işbirliği ve uluslararası işbirliği ile ilgili farklı hukuki yaklaşımların analizi ile devam etmektedir. Ulusal çözümlerden uygulama örneklerinin yanı sıra uluslararası yaklaşım örnekleri de dahil olmak üzere tüm yönleri ile ele alıyor. Kolluk kuvvetleri artık bilgisayar sistemlerinin ve karmaşık adli tıp yazılımlarının artan gücünü, soruşturmaları hızlandırmak ve arama prosedürlerini otomatikleştirmek için kullanabileceklerini öğreniyoruz. (ss:114-123) Fakat bu alanda, yasadışı içerik için anahtar kelime tabanlı bir arama kolayca gerçekleştirilebilirken, yasa dışı resimlerin belirlenmesinin daha sorunlu olduğunu belirtiyor. Yine bir diğer örneği adli yazılım konusunda veriyor; mesela şüphelilerin sabit diskindeki dosyaları bilinen görüntülerle ilgili bilgilerle karşılaştırarak çocuk pornografisi görüntülerini otomatik olarak arayabileceğini öğreniyoruz. 2007 sonlarında yetkililer çocukların cinsel istismarına ilişkin çok sayıda resim bulmuşlar. Suçlu, kendi kimliğinin tespit edilmesini önlemek için, bu resimleri İnternet üzerinden yayınlamadan önce resimlerin yüzünü gösteren kısmını dijital olarak değiştirmiş. Fakat adli bilişim uzmanları değişiklikleri seçmeyi ve şüphelinin yüzünü yeniden oluşturmayı başarmışlar. Yazar yine de bu vakanın, çocuk pornografisi soruşturmasında bir ilerlemenin kanıtı olmadığını düşünüyor. Çünkü açıklamasına göre, suçlu sadece yüzünü beyaz bir noktayla kapatmış olsaydı, kimlik tespiti imkansız olacaktı. (ss.74-75) Uygun yasal altyapının oluşturulması, ulusal bir siber güvenlik stratejisinin ayrılmaz bir bileşeni olarak belirleniyor. Bu alandaki hukuki zorluklar ise uygun mevzuat, siber suçların soruşturulması ve kovuşturulması temelinde problemler olarak ortaya konuyor. Fakat yasa koyucuları, özellikle ağ teknolojisindeki gelişmelerin hızı göz önüne alındığında, internet gelişmelerine sürekli olarak yanıt vermek ve mevcut hükümlerin etkinliğini izlemek zorunda oldukları konusunda uyarıyor. Tarihsel olarak, bilgisayarla ilgili hizmetlerin veya İnternet ile

ilgili teknolojilerin tanıtılması, teknolojinin tanıtılmasından kısa bir süre sonra yeni suç biçimlerine yol açtığını çeşitli dönemler üzerinden anlatıyor. 1970'lerde bilgisayar ağlarının gelişmesinden sonra bilgisayar ağlarına ilk yetkisiz erişimlerin kısa bir süre sonra gerçekleştiğini; benzer şekilde, ilk yazılım suçlarının, 1980'lerde kişisel bilgisayarların piyasaya sürülmesinden kısa bir süre sonra olduğunu, bu sistemlerin yazılım kopyalamak için kullanıldığı zamanlarda ortaya çıktığını hatırlatıyor. Bu açıdan bakıldığı zaman, yeni çevrimiçi siber suç biçimlerini kovuşturmak için ulusal ceza kanununu güncellemenin zaman alıcı olmasının tehlikesini açığa çıkarıyor. Ulusal ceza hukuku kapsamında suç sayılan suçların gözden geçirilmesi ve güncellenmesi gerektiğini anlatıyor. Örneğin, dijital bilgilerin geleneksel imzalar ve çıktılar ile eşdeğer statüye sahip olması bu konuda önemli buluyor. Çünkü ona göre, ulusal ceza hukuku sistemleri için temel zorluk, yeni teknolojilerin olası suistimallerinin tanınması ile ulusal ceza hukukunda yapılması gereken değişiklikler arasındaki gecikmedir. Birçok ülkenin yasal düzenlemeleri yakalamak için çok çalıştığını belirtiyor. Buna göre genel olarak uyum sürecinin üç adımı olduğunu vurguluyor:

1-ulusal hukuka uyum,

2-ceza kanunundaki boşlukların belirlenmesi ve

3- yeni mevzuat taslağının hazırlanması. (s-82)

Yazarın verdiği bilgiler arasında, siber suçlarda iş birliğini geleneksel karşılıklı hukuki yardım ilkelerine dayandırmanın zorluğu da yer alıyor. Çünkü yabancı kolluk kuvvetleri ile iş birliği yapmak için gereken resmi prosedürler ve zaman, genellikle soruşturmaları engelleyecek nitelikte olduğunu belirtiyor. Ayrıca "çifte suçluluk ilkesi", eğer suç soruşturmaya dahil olan ülkelerden birinde suç kapsamına alınmamışsa, zorluklar doğuracağını vurguluyor. Suçluların kasıtlı olarak kendi ülkeleri dışındaki hedefleri seçebileceğini ve siber suç mevzuatının yetersiz olduğu ülkelerden hareket edebileceklerini anlatıyor. (s.145) Bu nedenle ancak siber suçlarla ilgili yasaların ve uluslararası iş birliğinin uyumlaştırılması durumunda işe yarayacaklarını vurguluyor. Siber suç soruşturmalarında uluslararası iş birliğinin hızını artırmaya yönelik iki yaklaşımın, G8 24/7 Ağı ve Avrupa Konseyi Siber Suçlar Sözleşmesi'ndeki uluslararası iş birliğine ilişkin hükümler olduğunu belirtiyor. Ayrıca suçlular tarafından şifreleme teknolojilerinin kullanımı, kolluk kuvvetleri için bir zorluk olarak belirleniyor. (s.148) Şu anda sorunu çözmek için çeşitli yasal yaklaşımların tartışıldığını ve bunların yazılım geliştiricilerinin kanun uygulayıcı kurumlar için bir arka plan kurması için olası yükümlülükler; anahtar gücü üzerindeki sınırlamalar; cezai soruşturmalar durumunda

anahtarları ifşa etme yükümlülükleri gibi konuları içerdiğini öğreniyoruz. Anlaşılan o ki, şifreleme teknolojisi yalnızca suçlular tarafından kullanılmıyor, bu tür teknolojinin yasal amaçlarla kullanılmasının çeşitli yolları var.

Altıncı ve son bölümde ise, mevcut ulusal ve bölgesel yasal tedbirlerle birlikte işlevsel olacak, küresel olarak uygulanabilir bir siber suç mevzuatının geliştirilmesi için stratejilerin görüşüldüğü ITU Küresel Siber Güvenlik Gündeminden stratejik hedeflerden bahsediyor. Bu bağlamda öncelikle teknik kavramların yasal çerçevede ulusal ve uluslararası tanımlamalarından örnekler veriyor. Yasaya tabi olan tanımlar nicelik bakımından çeşitli hukuk düzenlemelerinde farklılık arz edebiliyor. Örneğin "Siber Suçlara İlişkin Sözleşme" yalnızca beş tanım içerirken, "Siber Suçlara İlişkin Yasama Modeli Metni"'nin yaklaşık yirmi tanım içerdiğini öğreniyoruz. Kriptoloji, Adli Yazılım gibi kavramları nasıl tanımlandıklarına dair sözleşe ve ilgili metinden örneklerle açıklıyor. (ss:169-177) Değinilen önemli konulardan bir diğeri ise dijital delillerle alakalı. Anlatıldığına göre, özellikle fiziksel belgelerin saklanmasına kıyasla düşük maliyetleri nedeniyle dijital belge sayısı artmaktadır. Bir suçun nasıl meydana geldiğine dair teoriyi destekleyen bilgisayar teknolojisi kullanılarak depolanan veya iletilen herhangi bir veri olarak tanımlanıyor. Dijital kanıtların ele alınmasına pek çok zorlukların eşlik ettiğini ve özel prosedürler gerektirdiğini öğreniyoruz. Çünkü yazarın verdiği bilgilere göre, dijital veriler son derece hassas ve kolayca silinebilir veya değiştirilebilir. Özellikle sistem kapatıldığında otomatik olarak silinen sistem belleği olan RAM'de saklanan bilgiler için özel koruma teknikleri gerektiğini vurguluyor. Ek olarak, yeni gelişmelerin dijital kanıtların ele alınmasında büyük etkisi olabileceğini anlatıyor. Bir örnek olarak bulut bilişimi veriyor. Şöyle ki eserde anlatıldığına göre, geçmişte, müfettişler bilgisayar verilerini ararken şüphelilerin bulunduğu yere odaklanabiliyordu. Günümüzde dijital bilgilerin yurt dışında saklanabileceğini ve gerektiğinde sadece uzaktan erişilebileceğini göz önünde bulundurmaları gerekiyor ve dijital kanıt, siber suç soruşturmalarının çeşitli aşamalarında önemli bir rol oynuyor. Dijital delillerin mahkemede sunulmasıyla ilgili prosedürlere ek olarak, dijital delillerin toplanma yolları da özel dikkat gerektiriyor. Yazar, dijital kanıtların toplanmasının adli bilişimle bağlantılı olduğunu vurgulayarak, 'Adli bilişim' terimini, dijital kanıt aramak amacıyla BT ekipmanının sistematik analizi şeklinde tanımlıyor. Bu kısımda anlıyoruz ki; spesifik soruşturmanın gerekliliğine bağlı olarak, adli bilişim, örneğin bir şüpheli tarafından kullanılan donanım ve yazılımın analiz edilmesini, ilgili kanıtların belirlenmesinde müfettişlerin desteklenmesini, silinen dosyaların kurtarılmasını, dosyaların şifresinin

çözülmesini ve trafik verilerini analiz ederek İnternet kullanıcılarının belirlenmesini içerebiliyor. (ss:225-233)

Bu kısımda değinilmesi gereken bir diğer mesele yargılama sorunları ile alakalı. Çünkü siber suç, birkaç ülkenin etkilenmesi bağlamında farklı yargı alanlarını içeren ulusötesi bir suçtur. Mesela kitapta verilen örneğe göre; suçlu A ülkesinden hareket etmiş, B ülkesinde bir internet hizmeti kullanmış ve mağdur C ülkesinde ikamet ediyor olabilir. Böylesi bir durumda, ceza kanununun uygulanmasıyla ilgili zorluklar çıkacaktır ve hangi ülkelerin yargı yetkisine sahip olduğu konusunda sorunlara yol açmaktadır. (s.234) "Yargı yetkisi" terimi, Uluslararası kamu hukuku ilkelerine dayalı olarak egemen bir devletin belirli davranışları düzenleme yetkisini tanımlar. Dolayısıyla ulusal egemenlik ile alakalı olarak siber suç soruşturması bağlamında bir devletin kendi iç hukukunu uygulama yetkisini ifade ediyor. Bu nedenle kolluk kuvvetleri yalnızca ülkenin yargı yetkisi varsa soruşturma gerçekleştirebilir. Yani yargı yetkisinin en temel ilkesi ve en yaygın dayanağı siber suçlar konusunda da **ülkesellik ilkesi** olarak beliriyor. (s.235) **Bayrak ilkesi** ise ulusal yasaların uygulanmasını uçak ve gemilere kadar genişletir. Deniz ve hava taşımacılığı için internet erişim çözümlerinin mevcudiyeti dikkate alındığında, suçlunun, mağdurun veya etkilenen bilgisayar sistemlerinin bölge içinde değil, ülke sınırları dışında bulunduğu durumlarda ceza kanununun uygulanmasına ilişkin soruları gündeme getirmektedir. (s. 236) **Koruyucu ilke** ya da etki doktrini, yabancı bir ülke vatandaşı tarafından işlenen, ülke dışında meydana gelen, fiilin hiçbir unsurunun ülke içinde gerçekleşmediği ancak yine de ülke içinde önemli bir etkiye sahip olan bir suç için yargı yetkisinin kurulmasıyla ilgilenir. (s. 237) **Aktif vatandaşlık ilkesi**, vatandaşların yurtdışındaki faaliyetlerine ilişkin olarak kullanılan yargı yetkisini ifade eder. Devletin, vatandaşlarının sadece kendi sınırları içinde değil, yurtdışında da davranışlarını düzenleme yetkisi ile ilgilidir. İnternetle ilgili suçların ülkeyi terk etmeden işlenebileceği gerçeğiyle ilgili olarak, siber suç davaları söz konusu olduğunda bu ilke daha az alakalıdır. Ancak, kitapta bilgisayar ağları aracılığıyla dağıtmak amacıyla çocuk pornografisi üretimi bağlamında oldukça alakalı bir ilke olabileceği vurgulanıyor. (s.237) **Pasif vatandaşlık ilkesi,** mağdurun uyruğuna dayalı yargı yetkisini ifade eder; yalnızca bir vatandaşın ülke dışındayken bir suçun mağduru olması durumunda geçerlidir. **Evrensellik ilkesi**, özellikle insanlığa karşı suçlar ve savaş suçları gibi ciddi suçlarla ilgilidir. Bununla birlikte, yazar ilkenin belirli koşullar altında siber suçlar açısından da geçerli olduğunu belirtiyor. (s.238)

Kitapta usul hukuku konusunda siber suçla mücadele maddi ceza hukuku hükümlerinin yeterli düzeyde olmasının önemine dikkat çekiyor. En azından medeni hukuk ülkelerinde, kolluk kuvvetleri bu yasalar olmadan suçları soruşturamayacağını vurguluyor. Ancak, kolluk kuvvetlerinin soruşturmaları yürütmek için eğitim ve donanıma ek olarak, kendilerinin suç duyurusunda bulunmalarını sağlayan, suçlunun kimliğinin tespit edilmesi ve cezai kovuşturma için gerekli delillerin toplanması için gerekli tedbirlerin alınması gibi usuli araçları üstlenmeleri gerektirdiğini belirtiyor. Yine kitaptan öğrendiğimize göre, farklı soruşturma tekniklerinin gerekli olmasının nedeni sadece olay yerinin ve olay yerinin bağımsızlığı değildir. Çoğu durumda, siber suç soruşturmalarını benzersiz kılan, kolluk kuvvetleri için belirtilen bir dizi zorluğun birleşimi nedeniyle gerçekleştiğini açıklıyor. Maddi ceza hukukunda olduğu gibi, Avrupa Konseyi Siber Suçlar Sözleşmesi siber suç soruşturmaları için gerekli olan usule ilişkin araçlara ilişkin geniş kabul görmüş asgari standartları yansıtan bir dizi hükmü içerdiğini belirtiyor.

Sonuç

Eser bütün olarak değerlendirildiğinde, kritik bilgi altyapılarının bütünlüğünü etkilemeye yönelik faaliyetler de dahil olmak üzere, bilişim teknolojilerinin kötüye kullanımına karşı tüm ülkeler tarafından uygun mevzuatın benimsenmesi, küresel siber güvenliğin sağlanmasında hayati öneme sahiptir. Tehditler dünyanın herhangi bir yerinden kaynaklanabileceğinden, bu konudaki sorunlar ve zorluklar uluslararası niteliktedir ve uluslararası iş birliği ve ortak yasal düzenlemeleri gerektiriyor. Bu nedenle, ülkelerin siber suçlarla mücadele etmek ve uluslararası iş birliğini kolaylaştırmak için yasal çerçevelerini uyumlu hale getirmeleri önemlidir.

Eser, siber suçların hukuki yönleriyle bağlantılı en alakalı konulara oldukça kapsamlı bir bakış kazanılmasını sağlıyor. Bunu amaçlarken üstelik daha ziyade gelişmekte olan ülkelerin taleplerine odaklanan bir yöntemle gerçekleştirmesi önemli. Çünkü eserden de anlaşılacağı gibi, siber suçların ulusötesi boyutu nedeniyle, gelişmekte olan ve gelişmiş ülkeler için yasal süreçler ve usulleri neredeyse aynı olmak zorundadır. Bununla birlikte, yazarın eseri oluştururken kullandığı referanslar, farklı konuların daha derinlemesine incelenmesi için sağladığı geniş literatür taramasından özellikle gelişmekte olan ülkelerin ihtiyacına göre seçmesi bakımından faydalı bir eser.

Bilişim teknolojilerinin sağladığı altyapı artık kaçınılmaz bir biçimde ekonomik gelişim konusunda kritik bir öneme sahip. Fakat bunun yanında eserin ortaya koyduğu tehlikeler bakımından siber suçlara karşı kolluk kuvvetlerinin bu sorunla yakından ilgilenmesinin zorunlu hale geldiği oldukça açık bir şekilde ortaya konuluyor. Fakat bu konuda da kolluk kuvvetlerinin çalışmaları çoğunlukla İnternet sağlayıcılarının iş birliğine ve onlarla iş birliğine bağlı. Şu an için sanki İnternet sağlayıcılarının sorumluluğunun sınırlı olduğu şeklinde bir algının hem günümüz için hem de ileriye dönük bazı endişeler uyandırdığını ifade edebiliriz.