CRYPTOLOCKER; BİR FİDYE VİRÜSÜNÜN CEZA HUKUKU AÇISINDAN ANALİZİ

Doç.Dr.Olgun DEGİRMENCİ* ,[687]

Özet

Bir fidye virüsü türü olan cryptolocker, bir bilgisayar virüsünün tüm özelliklerine sahiptir. Fidye virüsü olarak tasnif edilmesinin sebebi, girmiş olduğu sistemi enfekte etmesinin yanı sıra söz konusu zararın giderilmesi için menfaat talep etmesidir. Cryptolocker virüsü, kendini hedef bilişim sistemine yükledikten sona, güçlü bir şifreleme anahtarı kullanmak suretiyle, kullanıcıya ait olan verileri şifrelemek suretiyle erişilmez kılmaktadır. Verilerin erişilmez kılınmasının ardından, söz konusu şifreyi çözecek anahtarın verilmesi karşılığında mağdurdan kripto para ödemesi istenmektedir. Fidye virüsleri, genel olarak sistemin işleyişine zarar vermeksizin, kullanıcı açısından değerli olan verileri hedef almaktadırlar. Kullanıcı açısından değerli olan verinin erişilmez kılınması, temin edilecek menfaatin de miktarını artırmaktadır. Virüsün hedef seçici özelliğinin sonucunu, cryptolocker ile wannacry virüslerinin hedefleri arasındaki farkta görebiliriz. Nitekim birincisi daha çok bireysel kullanıcıları hedef alırken, sonuncusu verinin değerli olduğu sağlık sektörünü hedef almıştır. Fidye virüsünün oluşturulması, hedef sisteme yüklenmesi, verilerin erişilmez kılınması ve sonunda menfaatin temini, ceza kanunlarında düzenlenen ve suç teşkil eden hareketlerdir. Bu tebliğde, cryptolocker virüsünün özelinde fidye virüsüne özgü davranış şekilleri analiz edildikten sonra, oluşabilecek muhtemel suç tiplerine değinilecektir.

Anahtar Sözcükler: cryptolocker, fidye virüs, ceza hukuku, suç, bilişim suçu.

CryptoLocker: Analysis of a Ransom Virus in Terms of Criminal Law

Abstract

Cryptolocker, a ransom virus type, has all the features of a computer virus. The reason why it is classified as a ransom virus is that it infects the system it enters, as well as demanding the benefit

* Hukuk Fakültesi, TOBB Ekonomi ve Teknoloji Üniversitesi, Ankara, Türkiye.

[687] ORCID: https://orcid.org/0000-0002-0700-2549

of the damage. The Cryptolocker virus makes the data that belongs to the user inaccessible by encrypting, using a strong encryption key, after uploading itself to the target information system. After the data is inaccessible, the victim is required to pay crypto money in exchange for issuing the key to solve the password. In general, ransom viruses target data that are valuable to the user without damaging the functioning of the system. The invaluable data for the user increases the amount of the benefit to be provided. The result of the target selector feature of the virus, we can see the difference between the targets of cryptlocker and wannacry viruses. As a matter of fact, the first one targeted the individual users while the last one targeted the health sector where the data was valuable. Creation of the ransom virus, loading it into the target system, making the data inaccessible, and finally the provision of benefits are the criminal acts in criminal law. In this paper, after examining the behavior of the ransom virus specific behavior of the cryptolocker virus, the possible types of crime will be discussed.

Keywords: cryptolocker, ransomware, criminal law, crime, computer crime.

I. GENEL AÇIKLAMALAR

İnceleme konumuzu teşkil eden ve hukuki açıdan analize tabi tutulacak zararlı yazılım türü olan CryptoLocker, fidye yazılım (ransomware)[688] ailesine mensuptur. Fidye virüsler, yağmacı virüs şeklinde de ifade edebileceğimiz bir mantıkta çalışırlar ve bulaştığı sistemlerde, sistem kullanıcıları için değer ifade eden verileri erişilmez kılmak suretiyle menfaat elde etmeyi hedeflerler.[689] ABD Federal Ticaret Komisyonu (Federal Trade Commission) tarafından 2016 yılında "iş dünyası ve bireylerin karşılaştığı en ciddi çevrimiçi tehditlerden biri" ve "kullanılan en kârlı zararlı yazılım" olarak nitelenen[690] fidye virüsler, bilişim sistemlerine yapılan saldırılarda kullanılan araçların evrimleşme sürecini göstermesi açısından da bizim için incelemeye değerdir. Nitekim ilk geliştirilen zararlı yazılımlar (özelinde virüsler) sadece sisteme ve verilere zarar verme amacı

[688] Çalışmanın ilerleyen bölümlerinde *ransomware* karşılığı fidye yazılım veya fidye virüs kavramları birbirinin yerine aynı anlamda kullanılacaktır.

[689] **Liska, Allan / Gallo, Timothy**: Ransomware Defending Against Digital Extortion, O'Reilly, 2017, s. 3; **Sherer, James A. / McLellan, Melinda L. / Fedeles, Emily R. / Sterling, Nichole L.**: Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web, Richmond Journal of Law & Technology, Vol. XXIII, Issue 3, s. 1 (ss. 1 – 48); **Pascariu, Cristiona / Barbu, Ionut – Daniell / Bacivarov, Ioan C.**: Investigative Analysis and Technical Overview of Ransomware Based Attacks.Case Study: WannaCry, International Journal of Information Security and Cybercrime, Vol. 6, Issue 1, 2017, s. 57 (ss. 57 – 62).

[690] **Sherer / McLellan / Fedeles / Sterling**, s. 1 – 2.

taşırken, geçen yıllar içerisinde amaç farklılaşmış ve verilerin erişilemez kılınacağı tehdidi ile menfaat teminine yönelmiştir.

Fidye virüsler, bir zararlı yazılım çeşididir. Kategorik olarak yapılan sınıflandırmada ise bireylerde ortaya çıkan özel bilgilerinin ifşa edileceği, önemli verilerinin kayba uğratılacağı ya da donanımlarına zarar verileceği korkusundan yararlanılarak fayda sağlayan panik yazılım türü olan *scareware* olarak isimlendirilen yazılımların bir alt kümesinde yer almaktadır.[691]

Bireysel veya toplumsal hukuki menfaatlerin korunması araçlarından biri olan ceza hukukunun da, söz konusu toplumsal gelişime seyirci kalması düşünülemez. Bu kapsamda, fidye virüsler bakımından uygulanacak ceza hukuku normlarının belirlenmesi, kanunilik ilkesi bakımından uygulanabilecek bir normun tespit edilememesi durumunda ise kanunlaşma süreçlerinin başlatılması gereklidir. Shaw'ın, Uluslararası Hukuk kitabının girişinde de ifade ettiği gibi *"İnsanoğlunun mağara kovuğundan bilgisayarlara kadar uzun yürüyüşünde, düzenin gerekliliği ve düzensizliğin ise makul ve istikrarlı varoluşa düşman olduğuna dair hukuk ideası merkezi bir rol oynamıştır."*[692]. Dolayısıyla düzensizliğin, düzene evrilmesi gereklidir. Nitekim bu durum teknoloji ile hukuk arasındaki ilişkinin de belgesi olarak karşımıza çıkmaktadır. Faydalı amaçlarla çevrenin insan tarafından belli bir bakış açısıyla değiştirilmesi olarak da tanımlanan teknoloji ile hukuk arasındaki ilişki bağımlı ve karşılıklı bir ilişki olarak karşımıza çıkmaktadır.[693] *"İnsanlık ilk önce kendi araçlarını inşa eder, sonra kendi tarafından inşa edilen araçlar da insanlığı"*[694] ifadesi aslında bu açıdan bakıldığında bir doğruya da işaret etmektedir. Teknolojik sistemlerin büyüyüp gelişmesi toplum ile aralarındaki şekillenme – şekillendirme ilişkisine ters yönde etki etmekte ve toplumu daha fazla şekillendirirken, kendisi toplum tarafından daha az şekillendirilmektedir.[695]

---

[691] Bu kapsamda malware – scareware – ransomware alt gruplandırması yapılmaktadır. Bkz. **Kharraz, Amin / Robertson, William / Balzarotte, Davide / Bilge, Leyla / Kirda, Engin**: Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks,M. Almgren et al. (Eds.): DIMVA 2015, LNCS 9148, pp. 3–24, Springer 2015, s. 3.

[692] **Shaw, Malcolm N.**: International Law, 6 th Edition, Oxford University Press 2008, s. 1; Bakınız aynı şekilde **Kettemann**, **Matthias C.**: Ensuring Cybersecurity Through International Law, 69 R.E.D.I. 281, 2017, s. 281 (ss. 281 – 289).

[693] **Flint**, **David**, Law Shaping Technology: Technology Shaping the Law, International Review of Law, Computers and Technology, Vol. 23, No. 1 – 2, March – July 2009, s. 5 – 11.

[694] **McLuhan**, **Marshall**, Understanding Media: The Extension of Man, McGraw Hill, New York 1996, s. 23.

[695] **Hugher**, **Thomas** P., Technological Momentum, in: Does Technology Drive History? The Dilemma of Technological Determinism (Edited by Merritt Roe Smith and Leo Marx), Cambridge, MIT Press, 1994, s. 113.

Bu çalışmamızda ülkemizi de etkileyen *CryptoLocker* özelinde fidye virüslerin anatomisi incelenecek ve bu inceleme ışığında oluşabilecek suç tiplerine işaret edilecektir. Çalışmamıza konu olarak fidye virüslerin seçilmesinin nedenleri arasında, fidye virüslerin (genel olarak zararlı yazılım türü olarak), sınır aşan bilişim suçları içerisinde giderek artan sayıda görülen bir yöntem olması da gelmektedir.[696] Çalışma öncelikle fidye virüsler bakımından mevcut durumu ortaya koyacak ve sonrasında ceza hukukunda mevcut normların, tespit edilen durumu yaptırım altına almaya yeterli olup olmadığı incelenecektir. Bu açıdan bakıldığında çalışmanın hipotezinin konusunu buyurgan (preskriptif) değil, betimsel (deskriptif) bir iddia oluşturmaktadır.[697]

II. FİDYE VİRÜSLERİN ANATOMİSİ

A. KONUYA İLİŞKİN GENEL AÇIKLAMALAR

Fidye virüslerin, hedef bilişim sistemine sızıp, kendisini bilişim sistemine yükleyip, zararlı etkiyi gerçekleştirip, menfaat teminine kadar geçen süreçte farklı yöntemler kullandığı görülmektedir. Fidye virüsler, bir virüs ailesi olarak kendi içinde yöntem bakımından da farklılaşmaktadır. Örneğin zararlı etki bakımından bazı fidye virüsler, kullanıcının verilerine ulaşmasını basit şekilde zorlaştırırken (örneğin ekranın açılır pencere sayısını sınırlamak, dosya adını değiştirmek veya sistemin çalışmasını engellemek gibi), inceleme konumuz olan *CryptoLocker* örneğinde olduğu gibi bazı fidye virüsler de güçlü şifreleme sistemleri kullanarak hem dosya içeriğini hem de dosya adını şifreleyebilmektedirler.[698]

Fidye virüsler bakımından ilk kayda geçen örnek, Dünya Sağlık Organizasyonu tarafından 1989'da düzenlenen AIDS Konferansı sırasında 20.000'den fazla diski enfekte eden ve aslen bir biyolog olan Joseph Popp tarafından geliştirilen *AIDS Trojan*dır. Simetrik şifreleme sistemi ile sadece dosya adlarını şifreleyen *AIDS Trojan* tarafından şifrelenen dosyalar kısa sürede deşifre edilebilmiştir.[699] 2005 yılına kadar duraksama gösteren fidye virüsler, 2005 yılında

---

[696] Nitekim Perloff – Giles yakın tarihli bir çalışmasında incelemiş olduğu sınır aşan bilişim suçlarında, fidye virüsleri, hizmetin engellenmesi saldırıları (DoS – Denial of Service) ile birlikte en yaygın bilişim suçları oduğunu belirtmiştir. Bu konuda bkz. **Perloff – Giles, Alexandra**: Transnational Cyber Offences: Overcoming Jurisdictional Challenges, 43 Yale J. Int'l L. (2018), s. 197 (ss. 191 – 227).

[697] Bu konuda bkz. **Volokh**, Eugene: Akademik Metinler Nasıl Yazılır? Hukukçular için Rehber (Çev.: Ertuğrul Uzun), Tekin Yayınları İstanbul 2019, s. 39

[698] **Liska / Gallo**, s. 6.

[699] **Richardson, Ronny / North, Max M.**: Ransomware: Evolution, Mitigation and Prevention, International Management Review, Vol.13, No.1, 2017, s. 12 (ss. 10 – 21); **Sherer / McLellan / Fedeles / Sterling**:, s. 3.

Trojan.Gpcoder fidye virüsü ile birlikte dosya isimlerinin şifrelenmesinden, dosyaların şifrelenmesine evrilmiştir. 2007 yılında *Locker* isimli fidye virüsü ortaya çıkmış ve şifreleme yöntemi yerine, sistem ekranını kilitleyerek ekranda pornografik bir görüntüyü sabitlemiş ve görüntünün giderilmesi için SMS metin mesajı veya bir telefon numarasının aranması istenmiştir. 2012 yılında ilk kez fidye virüs toolkitleri yapılmıştır. *Citadel* isimli toolkit sayesinde fidye virüsü oluşturmak ve dağıtmak kolaylaştırılmıştır. 2013 yılında inceleme konumuz olan *CryptoLocker* virüsü görülmüştür. Söz konusu virüs farklı versiyonları da var olmakla birlikte 500.000'den fazla kişiye zarar vermiş ve virüs sayesinde 27 milyon dolar menfaat temin edilmiştir.[700] Yukarıda genel olarak fidye virüsler bakımından kilometre taşlarına yer verilmiştir. Belirtmek isteriz ki fidye virüsler birbirinden çok farklı metodolojiler kullandığı gibi aynı fidye virüsün birden fazla farklı versiyonu da bulunmaktadır. 2015 yılında yapılan bir çalışmada fidye virüslerden etkilenme oranında ABD'nin 1'nci sırada yer aldığı görülürken, Türkiye 12'nci sırada yer almaktadır.[701]

Fidye virüsler, önceleri bireysel kullanıcıları hedef alırken, işletmeler bakımından verilerin değeri keşfedildikten sonra daha fazla menfaat temini için işletmeleri hedef almaya başlamıştır. Bu bakımdan 2016 yılı için *Wannacry* fidye virüsünün, verinin en değerli olduğu sektörlerden biri olan sağlık sektörünü hedef alması da tahmin edilemeyecek bir durum değildir. Fidye virüslerin geleceği bakımından yapılan öngörü ise fidye virüsler tarafından öncelikle mobil cihazların hedef alınacağı ve daha sonra ise nesnelerin interneti kapsamında veri iletişimi olan her cihazın fidye virüsler bakımından hedef olabileceği şeklindedir.[702] Fidye virüslerin farklılaşan zararlı etki yöntemleri, zararlı etkinin gerçekleştirilmesi safhası bakımından uygulanacak ceza normunda da farklılıklara neden olmaktadır. Bu açıdan fidye virüsün saldırı süreçleri ve etkilerinin belirlenmesi gereklidir.

Fidye virüslerin genel karakteristik özellikleri şu şekilde ifade edilebilir[703];

- Güçlü bir şifreleme algoritması kullanırlar (*CryptoLocker* RSA – 2048 şifreleme algoritmasını kullanmaktadır).

- Birçok dosya formatını şifreleme yetenekleri mevcuttur.

[700] **Richardson / North**, s. 13.

[701] **Richardson / North**, s. 14.

[702] **Sherer / McLellan / Fedeles / Sterling**, s. 44.

[703] **Rajput**, Toshima Singh: Evolving Threat Agents: Ransomware and their Variants, International Journal of Computer Applications, Vol. 164, No. 7, April 2017, s. 28 vd. (ss. 28 – 34).

- Dosya adlarını da şifrelediklerinden dolayı hangi dosyanın virüsten etkilendiğini tahmin etmek güçtür.
- Dosya adlarına *.docx.rsrc* gibi farklı uzantılar ekleyebilir.
- Ekranda bir fidye mesaj görüntüsü yer alır.
- Çoğunlukla kripto paralar menfaat olarak temin edilir.
- Mağdur bilişim sistemi ile fail bilişim sistemi arasındaki irtibatta TOR gibi güvenli iletişim ağları kullanılır.
- Antivirüs programları tarafından tespit edilmemek için karmaşık teknikler kullanır.
- Daha sonraki saldırılarda kullanılmak üzere çoğu zaman mağdur bilişim sistemini botnet haline dönüştürür.
- Bilişim sistemindeki verileri erişilmez kırarken çoğu zaman sistemin normal işleyişini aksatmaz.

B. FİDYE VİRÜSLERİN EVRİMİ

Fidye virüsler, ilk kez görüldüğü 1989 yılından beri bünyesine bazı özellikler katarak evrim geçirmiştir. Aynı biyolojik virüslerde olduğu gibi kendisine karşı alınan önlemleri aşarak bilişim sistem güvenliklerine karşı bağışıklık geliştirmeye çalışmışlardır. Kısaca bazı fidye virüsler ve gösterdiği etkiler liste olarak aşağıda sunulmuştur.[704]

Yıl	Adı	Gösterdiği Etki / Özellikleri
1989	AIDS Trojan	Bilgisayarların sınırlı bir grup tarafından kullanıldığı ve şifreleme sistemlerinin zayıf olduğu bir dönemde ortaya çıkmıştır. Şifreleme yapmamakta ve verilere zarar vermemektedir.
2005	Trojan.Gpcoder	Simetrik şifreleme sistemi kullanmaktadır. Kullanıcı tarafından sıklıkla kullanılan kullanıcı dosyalarının uzantılarını şifrelemektedir.
2011	Trojan.Ransom.C	Ekranda Windows güvenlik mesajı oluşturmakta ve bilgisayarı kilitleyerek ödemeli telefon sistemlerini aramasını istemektedir.
2013	CryptoLocker	Asimetrik şifreleme sistemi kullanarak kullanıcı dosyalarını şifrelemektedir.
2016	KeRanger	MAC işletim sistemlerini enfekte etmektedir. 300'den fazla dosya türünü şifreleyebilmektedir. Üretmiş olduğu kişisel anahtarını 3 gün

[704] **Rajput**, s. 30 – 32.

		süreyle sunumcuda saklamakta ve sürenin sonunda geriye dönüşü mümkün olmayacak şekilde imha etmektedir.
2016	Petya	Dosya yerine sisteme saldırıyı yöneltmektedir. Master boot Record üzerine yazmak suretiyle mavi ekranın çıkmasına yol açmaktadır. Sistem reboot edildiğinde ekranda kuru kafa ve kemik işareti belirmektedir.
2017	VirLock	Bilgisayar ekranını kilitlemenin yanı sıra dosyaları da enfekte etmektedir.

C. FİDYE VİRÜS SALDIRI SÜREÇLERİ

1. Yayılma (deployment)

Fidye virüs saldırıların ilk aşaması yayılma sürecidir. Bu süreçte fidye virüsün zararlı etkiyi gerçekleştireceği bilişim sisteminin tespit edilip, sisteme gönderilmesi gereklidir. Bu aşama için farklı yöntemler kullanılmaktadır; örneğin kullanıcı bilgisi olmaksızın zararlı yazılımın sisteme otomatik yüklenmesi (drive-by download), özellikle bir organizasyonun hedef alındığı durumlarda, ilgili organizasyon tarafından sık ziyaret edilen web sitelerinin tespit edilmesi suretiyle zararlı yazılımın ilgili siteye konması (watering-hole attacks), zararlı yazılımın gönderilen elektronik postalara bağlantı (link) olarak eklenmesi ve mağdurun yanıltılarak bağlantıyı tıklamasının sağlanması (phishing emails) gibi yöntemler kullanılmaktadır.[705]

2. Yükleme (installation)

İkinci aşamada, zararlı etkiyi gerçekleştirmek için fidye virüsün sisteme yüklenmesi söz konusudur. Bu aşamada önem kazanan husus, özellikle anti virüs programlarına yakalanmadan zararlı yazılımın sisteme giriş yapmasıdır. Kullanılan yöntemlerden birisi, önce anti virüs programının denetiminden kaçınmak ve failin komuta kontrol sistemi ile iletişimi sağlayacak küçük bir program parçacığının sisteme yerleştirilmesidir (download dropper methodology). Söz konusu program, zararlı yazılımın yüklenmesi için failden komut beklemekte ve gelen komut üzerine zararlı yazılımın yüklenmesi gerçekleştirilmektedir. Bunun yanı sıra güvenli olmayan elektronik marketlerden yapılan uygulama satın alınması işlemi sırasında da zararlı yazılımı sisteme sızabilmektedir (özellikle *jailbreak* yapılmış sistemlerde).

[705] **Liska / Gallo**, s. 7.

Bu aşamada fidye virüs, hangi sistemlerin enfekte olduğunu belirlemektedir. Bunun için zararlı yazılım bilişim sisteminin adı veya Mac adresi gibi tanıtıcı bilgisinin özet değerini (hash value) almak suretiyle, benzersiz bir kod yaratmaktadır.[706]

3. Komuta ve Kontrol (command-and-control)

Fidye virüsünün yayılması ve sisteme yerleşmesinden sonra, kendisine verilen komutları alması için komuta sunucularına ulaşması gereklidir. Yerleştirilen sistemde, şifrelenecek dosyaların tespiti ve sürecin başlaması için ne kadar beklenmesi gerektiği gibi hususlar zararlı yazılıma belli bir istek olarak gönderilmektedir. Zararlı yazılımın türüne göre yerleşilen sistemin bilgisi, IP adresi, alan adı, işletim sistemi, yüklü bulunulan ağ gezginleri ve varsa anti virüs programının türü gibi bilgiler raporlanmaktadır. Bu aşamada fail bakımından sistemin enfekte edilip edilmediğinin yanı sıra, hedefin içerdiği verilerin mağdur bakımından değeri de tespit edilmektedir. Bu tespit, menfaat temini aşamasında istenecek menfaatin türü ve miktarını belirlemek açısından önem kazanmaktadır.[707]

Bu aşamada virüs yerleştirilmiş bilişim sistemi ile failin sistemi arasındaki iletişim farklı kanallardan sağlanabilmektedir. Virüsün karmaşıklığına ve yerleştirildiği bilişim sistemindeki verinin değerine göre şifrelenmemiş http protokolü üzerinden haberleşme yapılabileceği gibi, gizliliğin sağlanması ve özellikle kolluk kuvvetleri tarafından faile ulaşılmasının engellenmesi için TOR[708] üzerinden de iletişim sağlanabilmektedir.[709]

Komuta ve kontrol aşamasının temel olarak iki amacı bulunmaktadır: İlki yukarıda da ifade edildiği üzere virüsün yerleştirildiği sistemin incelenmesidir. Bu inceleme hedef bilişim sistemindeki verinin değerinin belirlenmesinden, enfekte edilen bilişim sisteminin tespitinden, kolluk tarafından gerçekleştirilen bir operasyonun parçası olup olmadığını belirlemeye kadar geniş bir alanı kapsayabilmektedir. İkinci olarak sistemin tespiti ve güvenilir olduğunun

[706] **Liska / Gallo**, s. 9.

[707] **Liska / Gallo**, s. 9.

[708] TOR (The Onion Router), Amerikan Ulusal Bilim Vakfı tarafından fonlanan ve kar amacı gütmeyen bir organizasyon olan Tor Project tarafından işletilmektedir. 2000'li yılların başında hükümetin internet üzerindeki iletişimini korumak amacıyla oluşturulmuştur. Tor Network anonim bir yazılım tarafından yönetilir ve Internet trafiğini Tor düğüm noktalarına yönlendirmek suretiyle, söz konusu noktalarda IP adreslerini maskeler ve iletişimin hedef ve kaynağını takip edilemez hale getirir. İletişimi takip edilemez kılmasından dolayı özellikle organize suç örgütleri tarafından ciddi şekilde kullanılmaktadır. (**Dolliver, D.S. / Kenney, J.L.**: Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison, in: Victim & Offenders, Taylor & Francis Group, 2016, s. 601, 602 (ss. 600 – 620).

[709] **Liska / Gallo**, s. 9.

belirlenmesinden sonra üretilen şifreleme anahtarının, mağdurun bilişim sistemine gönderilmesidir. Bu noktada kullanılan fidye virüsünün karmaşık yapısına göre sadece dosya adlarını değiştiren şifreleme sistemlerinden, tek bir anahtarın kullanıldığı simetrik şifreleme sistemlerine veya birden fazla anahtarın kullanıldığı asimetrik şifreleme sistemlerine kadar değişik sistemler kullanılmaktadır. İnceleme konumuz olan CryptoLocker virüsünde asimetrik şifreleme sistemi kullanılmaktadır. Bu sistemde, iki adet anahtar üretilmekte ve ortak anahtar (public key – şifrelemeyi gerçekleştirecek anahtar) mağdurun bilişim sistemine (client – istemci) gönderilmektedir. Özel anahtar (private key – deşifrelemeyi gerçekleştirecek anahtar) ise failin bilişim sisteminde (server – sunumcu) tutulmaktadır.[710]

Kullanılan simetrik veya asimetrik şifreleme sistemlerinin birbirine göre fayda ve mahzurları bulunmaktadır. Simetrik şifreleme sistemlerinde, şifrelemenin gerçekleştirilmesi için mağdur bilişim sistemi kullanılmakta ve minimum sistem kaynağı harcanmaktadır. Sistem kaynaklarının minimizasyonu, şifreleme sisteminin anti virüs yazılımları tarafından tespitini güçleştirmektedir. İkinci olarak her bir sistemin şifrelenmesi için tek bir anahtarın kullanılması durumunda, virüsün yerleştirilmesi aşamasının fail tarafından takip edilmesi yeterli olacaktır. Ayrıca şifreleme için mağdurun bilişim sistemi ile failin bilişim sistemi arasında bir iletişim zorunlu olmayacak ve bu durumda, ağa bağlı olmadan da mağdurun bilişim sisteminde şifreleme işlemi başlatılabilecektir. Şifreleme bittikten sonra mağdurun bilişim sisteminde üretilen şifreleme anahtarı, menfaat temininde kullanılmak amacıyla bilişim suçu failinin bilişim sistemine gönderilecektir. Bunun için sadece mağdurun bilişim sisteminin ağ bağlantısını gerçekleştirmesi yeterli olacaktır.[711] Simetrik şifreleme sistemlerinin mahzuru ise mağdurun bilişim sisteminde üretilen şifreleme anahtarının, sistem ağa bağlı değilken RAM'den alınması ve deşifreleme için kullanılmasının mümkün olmasıdır. RAM'in kopyalanması farklı adli bilişim araçlarının kullanılması suretiyle mümkün olabilecektir.

Asimetrik şifreleme sistemleri ise şifreleme süreçleri için ortak ve kişisel olmak üzere iki farklı anahtar üretmektedirler. Ortak anahtar, mağdurun bilişim sisteminde, mevcut dosyaların şifrelenmesi için kullanılır. Kişisel anahtar ise deşifreleme amacıyla kullanılır ve failin bilişim sisteminde bulunur. Simetrik şifreleme sisteminde olduğu gibi dosyaların şifrelenmesi anında müdahale edilse dahi, kişisel anahtarın ele geçirilmesi olanaksızdır. Asimetrik şifrelemede,

[710] **Richardson / North**, s. 12.

[711] **Liska / Gallo**, s. 13.

şifreleme işleminin başlayabilmesi için anahtar üretimi gereklidir ve anahtarların üretilmesi için ise fail ve mağdurun bilişim sistemlerinin ağ üzerinden birbiri ile irtibat kurması gereklidir.[712]

4. Zararlı Etkinin Gerçekleştirilmesi (destruction)

Bu safhada fidye virüsün yüküne göre (payload – zararlı etki), mağdurun bilişim sistemini kilitlemekte veya sistemde yer alan verileri şifrelemektedir. Bu safhada şifrelenecek dosyalar, komuta kontrol safhasında belirlenen dosyalardır. Kullanılan fidye virüsün türüne göre dosya adları sadece küçük harf değişiklikleri ile değiştirilebilmekte, sadece dosya adları veya dosyalar tüm içerikleri ile şifrelenebilmektedir.[713] Örneğin *CryptoLocker* virüsünün Microsoft Office veri dosyaları da dâhil olmak üzere 67 farklı dosya türünü şifrelediği bilinmektedir.[714]

CryptoLocker virüsü genel olarak RSA 2048 şifreleme algoritmasını kullanmaktadır. Kullanılan bu güçlü algoritmanın şifrelediği bir dosyanın şifresinin çözülmesi neredeyse olanaksızdır. Örneğin sıradan bir masaüstü bilgisayar ile şifrenin çözülmesi yaklaşık olarak 6,4 katrilyon yıl sürmektedir.[715]

5. Menfaat Temini (extortion)

Fidye virüsün son aşamasında menfaat temini yapılmaktadır. Bu aşamaya kadar kullanılan virüs yapısına göre farklı şifreleme sistemleri ile şifrelemeler yapılmış ve mağdurun bazı durumlarda verilerine bazı durumlarda sistemine ulaşması engellenmiştir. Menfaat temini aşamasında da farklı sistemler kullanılmaktadır. Bazı fidye virüsler, diğer dosyaların çözülmesi için bir anahtara ihtiyaç olduğunu göstermek için şifrelenen dosyalardan sadece bir tanesine ücretsiz ulaşmaya müsaade etmektedirler. Diğer bazı fidye virüsleri ise fail ile iletişim kanallarını gösteren bir mesajı mağdurun bilişim sistemine göndermekte ve ilgili iletişim kanalları kullanıldıktan ve menfaat temin edildikten sonra şifre çözme anahtarını ulaştırmaktadırlar. CryptoLocker virüsünün daha sonraki sürümlerinde, şifre anahtarına ulaşmayı zaman bakımından sınırlamak suretiyle mağdur üzerinde baskı yaratılmaya çalışılmıştır. CryptoLocker için bu süre 3 gün olarak belirlenmiştir.

Temin edilecek menfaatin miktarı ve türü yine fidye virüse göre değişebilmektedir. Örneğin 2006 yılında yayılan Trojan.Cryzip isimli fidye virüsü mağdura bildirmiş olduğu bazı ilaçların

[712] **Liska / Gallo**, s. 15.

[713] **Liska / Gallo**, s. 11.

[714] **Richardson / North**, s. 12.

[715] **Sherer / McLellan / Fedeles / Sterling**, s. 8.

online eczanelerden sipariş edilmesi ve sipariş numarasının gönderilmesi durumunda deşifre anahtarını göndermektedir. Kripto paraların yaygınlaşmasına kadar SMS, belirli bir telefon numarasının aranması, önödemeli kartlar şeklinde değişik ödeme sistemleri üzerinden menfaat temini yapılmıştır. Ancak günümüzde kripto para (çoğunlukla bitcoin olmak üzere diğer alt coinlerde kabul edilmektedir) hemen hemen tüm fidye virüsler bakımından geçerli bir ödeme yöntemi olmuştur.[716]

CryptoLocker menfaat temini aşamasında kripto para (ve çoğunlukla bitcoin) kullanmaktadır. Kripto para transferleri, noktadan noktaya yapılmakta ve anonimlik sağlanmaktadır.[717] CryoptoLocker, tespit edilip tedbir alınıncaya kadar 27 milyon dolar değerinde Bitcoin ödeme olarak kabul etmiştir.[718]

III. SAFHALARINA GÖRE UYGULANACAK NORMLAR

A. GENEL OLARAK

Fidye virüsler kişisel veri niteliğinde olsun veya olmasın herhangi bir veriyi ele geçirmez veya ifşa etmezler. Bundan dolayı fidye virüsler bakımından TCK m. 135 ve 136'da yer alan suçların oluşmadığı kanaatindeyiz. Nitekim Wannacry fidye virüsünün sağlık sistemine yönelik saldırısından sonra yapılan incelemelerde bu husus tartışılmıştır. Bu kapsamda, ABD hukukunda Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (The Health İnsurance Portability And Accountability Act) uyarınca sağlık verilerin ifşası durumunda, ilgili kurum tarafından veri sahibine bilgi verilmesi gereklidir. Saldırıya uğrayan sağlık şirketlerinin de söz konusu yükümlülüğü yerine getirebilmesi için öncelikle sağlık verilerinin ifşa edilip edilmediği tartışılmıştır. Sonuç olarak fidye virüsün, kişisel verileri ifşa etmediği sonucuna varılmıştır.[719] Benzer bir tartışmanın 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 12'nci maddesinin 5'nci fıkrası gereğince ülkemiz bakımından da yapılması gerektiği kanaatindeyiz. Nitekim ilgili fıkra; *"İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir"* hükmünü amirdir. Bu

[716] **Richardson / North**, s. 10.

[717] **Paquet – Clouston, Masarah / Haslhofer, Bernhard / Dupont, Benoît**: Ransomware Payments in the Bitcoin Ecosystem, The 17th Annual Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria; **TK, Anjana**: Discussion on Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks, IJRTI, Vol. 2, Issue 6, 2017, s. 210 (ss. 210 – 214).

[718] **TK**, s. 211.

[719] **Sherer / McLellan / Fedeles / Sterling**, s. 24.

kapsamda veri işleyen birimler, işlenen kişisel verilerin başkaları tarafından ele geçirildiğini tespit etmesi durumunda, ilgilisini durumdan haberdar etmekle yükümlüdür.

Fidye virüsler kullanılarak menfaat temini siber yağma (cyber extortion) olarak da isimlendirilmektedir. İncelemiş olduğumuz ülke kanunlarında, bir örnek dışında bu isimle anılan ve tüm süreçleri cezalandıran bir düzenlemeye rastlamadık. İstisna düzenleme Güney Afrika Bilgisayar Suçları ve Bilgisayar Güvenliği Kanunu'nun 10'ncu Bölümünde "siber yağma" olarak isimlendirilen bir suç tipidir. Söz konusu düzenlemeye göre bazı bilişim suçlarının işlenmesi veya işlenmesi tehdidi ile bir kişiden fayda sağlayan veya bir kişiyi bir şeyi yapmaya veya yapmaktan kaçınmaya zorlayan kişi cezalandırılmaktadır.[720] Siber yağmayı tek başına cezalandıran düzenleme dışında, ülkeler mevzuatında fidye yazılımların safhalarına göre farklı suç tipleri uygulanabilmektedir.

B. TCK m. 245/A YASAK CİHAZ VEYA PROGRAMLARLA İLGİLİ SUÇ TİPİ

a. Zararlı Yazılımların Oluşturulması, Bulundurulması ve Ticaretinin Cezalandırılması Gerekliliği

Fidye virüs saldırısının gerçekleştirilebilmesi için öncelikle kullanılacak zararlı yazılımın oluşturulması gereklidir. Söz konusu zararlı yazılım fail veya failler tarafından oluşturulabileceği gibi, sanal yeraltı dünyasından satın da alınabilirler. Dolayısıyla öncelikle söz konusu zararlı yazılımın oluşturulması veya satın alınması gibi hareketlerin cezalandırılabilirliği konusunu ele alacağız.

Bilişim sistemlerinin sosyal hayatta rolünün artması, söz konusu sistemlerin ve sistemler üzerinde işlenen verilerin de ekonomik olarak değerinin artmasına neden olmuştur. Bu durum ise failleri, sistemler üzerindeki verilere yönlendirmiştir. Daha önceleri sadece kredi kart bilgilerine veya bazı hizmetlerden ücretsiz istifadeye yönelen ilgi, daha az yetenekli faillere teknik destek vermeye doğru evrilmiştir. Bugün sanal yeraltı dünyasında aynen fizik dünyada yasal herhangi bir ürünün satış öncesi ve satış sonrası hizmetlerine benzer hizmetler verilmektedir. Nitekim istenen bir zararlı yazılımın oluşturulması için "kendin yap" kitlerinden, zararlı yazılımın oluşturulması, yayılması, zararlı etkinin oluşturulması ve menfaatin teminine kadar süreçlerde verilen hizmetlere kadar sanal yeraltı dünyası geniş bir yelpazede potansiyel bilişim suç faillerini desteklemektedir. Sanal yeraltı dünyasında sunulan ürünler de geniş bir alana yayılmaktadır. Örneğin bilişim

[720] **Mabunda, Sagwadi**: Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill, Statute Law Review, 2017, s. 1 vd.

sistemine yetkisiz erişimi sağlayan araçlar, yetkisiz erişim sonucunda elde edilen mali bilgiler, veri kayıtları, IP adresleri gibi sayısal varlıklar (digital assets), aynen bir bulut hizmeti gibi belli platformda sunulan bilişim suçlarına ilişkin hizmetler bu kapsamda sayılabilir. Sanal yeraltı dünyasında 16 - 325 dolar arasında değişen ücretlerle herhangi bir bilişim sistemine yetkisiz giriş hizmeti alabilir, web saldırıları için kendin yap kitlerini 15 – 20 dolar arasında oluşturabilir veya onlarca dolardan binlerce dolara varan fiyatlarla herhangi bir yazılımı hayat boyu garanti ile edinebilirsiniz. Bu söz konusu sanal yeraltı pazarlarına örnek olarak Ekim 2013'de kapatılan Silk Road, Mayıs 2013'de kapatılan Liberty Reserve, Ekim 2013'de kapatılan Blackhole Exploit Kit verilebilir.[721]

Zararlı yazılımların kullanılması suretiyle elde edilen menfaatlerin artması, zararlı yazılım araçlarını daha kolay ulaşılabilir kılmıştır. Bir zararlı yazılımı oluşturma, elinde bulundurma veya zararlı yazılımın ticaretini yapma eylemlerinin, daha sonra işlenecek suçların önlenebilmesi bakımından cezalandırılması düşünülmüştür. Suç ve ceza politikası açısından bakıldığında, daha sonra işlenecek olan suçlar bakımından hazırlık hareketi niteliğinde olan zararlı yazılımların oluşturulması, bulundurulması ve ticareti eylemleri, ceza politikalarında yaşanan değişimin sonucunda cezalandırma alanının hazırlık hareketlerine doğru genişletilmesi suretiyle[722] cezalandırılabilir eylemler arasına alınmışlardır. Özellikle zararlı yazılım ticaretinin cezalandırılmasının amaçlarından birisi de, sanal yeraltı pazarının cezalandırılabilir alana dâhil edilmesidir.

b. Zararlı Yazılımların Silah Olarak Değerlendirilmesine İlişkin Tartışmalar

Zararlı yazılımların oluşturulası veya daha bilinen adıyla virüs yazımının suç olup olmadığının özellikle 1900'lü yılların sonundan itibaren ciddi şekilde tartışıldığı bilinmektedir. 2000'li yılların başlarında özellikle Avrupa Konseyi Siber Suç Sözleşmesi'nin oluşturulmasına yönelik gayretler esnasında, virüs yazımının cezalandırılması tartışmaları yeniden alevlenmiştir. ABD mevzuatına göre bir virüsün sadece yazılması, bilişim sistemine zarar vermek veya yetkisiz erişmek için kullanılması veya yayılması saiki bulunmadığı sürece suç teşkil etmemesi hususları da

[721] Sanal yeraltı dünyası ile ilgili detaylı bir alan çalışması için bkz. **Ablon, Lilian / Libicki, Martin C. / Golay, Andrea A.**: Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, RAND 2014, s. 3 – 19.

[722] Bu konuda bkz. **Tekin, Derya**: Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi, Terazi Hukuk Dergisi, C. 13, S. 146, Kasım 2018, s. 50 vd. (ss. 48 – 60).

eleştirilmiştir (18 U.S.C. § 1030 (a)(5)(A)(i)).[723] Virüs yazımının, her ne kadar anti sosyal bir davranışa işaret etse de, cezalandırılmamasının en kuvvetli gerekçesi virüslerin faydalı amaçlar için de kullanılabileceği, faydalı amaç ile zararlı amacın yazım aşamasında ayırt edilmesinin olanaklı olmadığıdır. Ancak maksadın açık bir şekilde ortaya konulduğu durumlarda, örneğin zararlı yazılım oluşturma kitlerinin ticaretinde olduğu gibi cezalandırılmanın gerekli olduğu ifade edilmiştir.[724]

Zararlı yazılım oluşturma ve bulundurma eylemlerinin cezalandırılmasında fizik dünyada silah kontrolüne ilişkin düzenlemelerden hareketle birtakım görüşler de ileri sürülmüştür. Öncelikle belirtelim ki, zararlı yazılımların oluşturulması ve bulundurulması eylemlerinin suç oluşturup oluşturmadığı konusunda iki farklı eğilim oluşmuştur. Birinci eğilim, yasa dışı hareket üzerine odaklanılması, zararlı yazılımın sadece oluşturulması ve bulundurulmasının suç olarak düzenlenmemesi gerektiği yönündedir.[725] Bu kapsamda zararlı yazılımların, ruhsatsız silah gibi düşünülerek bulundurulmasının yasaklanması gerektiği de ifade edilen diğer bir görüştür.[726]

Zararlı yazılımların silah olarak kabul edilmesine ilişkin özellikle uluslararası hukukta başlayan ve ulusal hukuklara da sirayet eden bir tartışma mevcuttur. 2010 yılında İran'a yönelik Stuxnet saldırısı sonrasında, başka bir ülkenin bilişim sistemlerine yapılan saldırıların Birleşmiş Milletler Sözleşmesi'nin 51'nci maddesinde yer alan "silahlı saldırı" niteliğinde olup olmadığı yönündeki farklı görüşler, kullanılan zararlı yazılımların "silah" olarak kabul edilip edilmeyeceği noktasına yoğunlaşmıştır.[727]

---

[723] **Cesare, Kelly**: Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, The Transnational Lawyer, Vol. 14, 2001, s. 141 (ss. 136 – 170);

[724] **Kroczynski, Robert J.**: Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?, Fordham Intell. Prop. Media & Ent. L. J., Vol. 18, 2008, s. 845 (ss. 817 – 865).

[725] **Wang, Qianyum**: A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and Council of Europe, Ph.D. Thesis, Erasmus University, Rotterdam 2016, s. 91.

[726] **Downing, Richard**: Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime, 43 Colum. J. Transnat'l L. 705, (2005), S. 733 (ss. 705 – 762).

[727] Bu konudaki temel tartışmalar için bkz. **Brown, Gary D. / Metcalf, Andrew O.**: Easier Said Than Done: Legal Review of Cyber Weapons, Journal of National Security Law & Policy, Vol. 7, 2014, ss. 115 – 138; **Denning, Dorothy**: Reflections on Cyberweapons Controls, Computer Security Journal, Vol. XVI, No. 4, Fall 2000, ss. 43 – 53; **Dévai Dóra**, Proliferationf of Offensive Cyber Weapons. Strategic Implications and Non – Proliferation Assumptions, AARMS Vol. 15, No. 1, 2016, ss. 61 – 73; **Peterson, Dale**: Offensive Cyber Weapons: Construction, Development, and Employment, The Journal of Strategic Studies, Vol. 36, No. 1, 2013, ss. 120 – 124; **Maitra, Amit K.**: Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects, Environs Syst Decis, Springer 2014.

Uluslararası hukuktaki bu tartışmalar ulusal hukuklarda da karşılığını bulmuştur. Özellikle sanal ortamın silahlandırılması ifadesi ile sanal ortamda suç işlemek için kullanılan cihazların başka bir anlatımla donanımın yanı sıra yazılımın da kapsama alındığı ifade edilmiştir.[728] Dolaysıyla ateşli silahların üretimi, ticareti ve bulundurulmasının kontrolü için uygulanan yasal tedbirlerin, ateşli silahlarla işlenen suçları azaltmasından hareketle zararlı yazılımların bulundurulması ve ticaretinin de, bilişim suçlarında azalmaya yol açacağı ileri sürülmüştür.[729] Zararlı yazılımlar bünyesinde suç yaratıcı riskler taşımaktadır. Bunlar arasında elde edilmesinin ve kullanımının göreceli kolay, ancak sonuçlarının ciddi etkiler bırakacak olması sayılabilir. Bu, özellikle söz konusu zararlı yazılımlara talebi artıracaktır. Ayrıca zararlı yazılımların, sınır denetimleri olmaksızın ülkelere kolaylıkla girmesi, amaçları belli olmayan kişilerin elinde bulunması da olası suçlar için imkan sunmaktadır.[730] Bu tartışmaların ışığında bilişim suçları işlemek için kullanılan zararlı yazılımların oluşturulması, test edilmesi, dağıtımı ve satışının lisansa bağlanması, belirlenen zararlı yazılımların bunun dışında bulundurulması, satışı ve dağıtımının ceza kanunlarda suç olarak düzenlenmesi, DDoS saldırılarında kullanılan botnet yazılımlarında olduğu gibi bazı zararlı yazılımların yasa dışı bir amaç güdüp gütmediğine bakılmaksızın yasaklanması gibi tedbirler önerilmiştir.[731]

Zararlı yazılımların düzenleme altına alınmasında kanaatimizce karşılaşılabilecek en büyük zorluk, söz konusu zararlı yazılımların nasıl tasnif edileceğidir. Öğretide zararlı yazılımların saldırı amaçlı kullanılanlar, savunma amaçlı kullanılanlar ve her iki amaçlı da kullanılabilir olanlar şeklinde tasniflenmesi yönünde görüşler ileri sürülmüştür.[732]

Türk hukuku bakımından TCK'nın 6'ncı maddesinde yer alan "silah" tanımı incelendiğinde, genel olarak cismani varlığa sahip araçların silah olarak değerlendirildiği görülmektedir. İncelemiş olduğumuz çalışmaların hiçbirisinde, zararlı yazılımların silah olarak kabul edilip edilmeyeceğine değinilmediği gibi, incelemiş olduğumuz yargı kararlarında da bu hususa temas edilmemiştir.

[728] **Prunckun, Henry**: Weaponization of Computers, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, s. 4.

[729] **Prunckun, Henry**: The Rule of Law: Controlling Cyber Weapons, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, s.88 (Prunckun, Cyber Weapons olarak anılacaktır).

[730] **Prunckun**, Cyber Weapons, s. 89.

[731] **Prunckun**, Cyber Weapons, s. 95.

[732] **Prunckun**, Cyber Weapons, s. 96, 97.

Ancak özellikle bilişim sistemleri vasıtasıyla kontrol edilebilen fiziksel sistemlerin artması (SCADA) ve bilişim sistemlerindeki zararlı yazılımların fizik dünyada da etki doğurabilmesinden dolayı yakın bir zamanda bu hususstaki tartışmaların da Türk hukukunda yer bulacağını söylemek gerçekten uzak bir değerlendirme olmayacaktır.

c. Zararlı Yazılım Üretme, Bulundurma ve Ticaretini Yapma Fiillerinin Değerlendirilmesi

Bilişim suçlarının işlenmesinin önlenmesi, bilişim suç faillerinin bilişim suçlarını işleyecek donanım ve yazılımı üretmesi, tedarik etmesi ve bulundurmasının engellenmesi ve son olarak sanal yeraltı pazarındaki fiillerin müeyyideye bağlanması açısından hazırlık hareketi niteliğinde olan zararlı yazılı üretme, bulundurma ve ticaretini yapma fiillerinin ülke mevzuatlarında cezalandırılmaya başlandığı görülmektedir. Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi'nin[733] 6'ncı maddesinde "Cihazların Kötüye Kullanılması" (Misuse of Devices) başlığı altında, Sözleşmede düzenlenen bilişim suçlarının işlenmesi için kullanılmak üzere hazırlanan donanım ve yazılımların kullanım amacıyla üretilmesi, satışı, kullanım amaçlı tedarik edilmesi, kullanım amaçlı bulundurulması, ithal edilmesi, dağıtımı ve başka şekilde erişilebilir hale getirilmesi cezalandırılmaktadır.

Siber Suçlar Sözleşmesinin ilgili maddesi, bir cihaz, bilgisayar şifresi, erişim kodu veya benzeri veriyi suçun konusu haline getirmiştir. Genel olarak bakıldığında zararlı yazılımların "benzer veri" (similar data) kapsamında değerlendirileceği söylenebilir. Ancak "cihaz" (device) ibaresinin donanım ve yazılımı da kapsayan bir ifade olduğu ve zararlı yazılımların bu kapsamda değerlendirilmesi gerektiği genel olarak ifade edilmektedir.[734].

Gerek 6'ncı maddenin 2'nci fıkrası gerek hazırlık çalışmaları gerekse Açıklayıcı Rapora bakıldığında bu alanda ikinci tartışmalı husus hem suç aracı olarak kullanılabilecek hem de aynı zamanda bilişim sistemlerinde yasal amaçlı kullanılabilecek olan yazılımların (dual use), madde kapsamına dâhil olup olmadığıdır. Açıklayıcı Rapora göre Sözleşmenin oluşturulması aşamasında bazı hususlar tartışılmıştır. Bunlardan biri yaptırım altına alınacak donanım ve yazılımların

[733] Sözleşme TBMM tarafından 22.4.2014 tarih ve 6533 sayılı Kanun ile kabul edilmiş olup, 2.5.2014 tarih ve 28988 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

[734] **Walden, Ian**: Computer Crimes and Digital Investigations, Oxford University Press, New York 2007, s. 193; **Clough, Johathan**: Principles of Cybercrime, Cambridge University Press, 2010, s. 120; **Viano, Emilio C.**: Cybercrime: Definition, Typology, and Criminalization, in: Cybercrime, Organized Crime and Societal Responses, International Approaches (Ed. Emilio C. Viano), Springer 2017, s. 11.

münhasıran suç işlemek amacına özgülenmesinin aranıp aranmayacağıdır. Münhasıran suç işlemek amacına özgülenmesinin aranması durumunda aşılamayacak ispat problemleri ile karşılaşılabileceğinden, bu öneri taraftar bulmamıştır. İkinci olarak yasal amaçlarla üretilip üretilmediğine bakılmaksızın suç işlemek tüm cihazların kapsama alınması da, belirsizliklere yol açabileceği ve kavramın çok geniş olmasından dolayı kabul görmemiştir. Bu kapsamda orta bir yol bulunmuş ve cihazın bilişim suçlarını işleme amacıyla oluşturulması, bulundurulması, ticareti aranmış ancak sadece sübjektif unsura yer verilmemiş aynı zamanda ilgili cihazın da objektif olarak ilgili suçu işleyecek şekilde oluşturulması veya uyarlanması gerektiği ifade edilmiştir.[735] Dolayısıyla Avrupa Konseyi Siber Suçlar Sözleşmesinin bu kapsamda karma teoriyi benimsediği söylenebilir.

Yasal veya yasadışı kullanıma uygun olarak donanım ve yazılım araçlarına web sitesi yükleme kapasite test yazılımları (website load capacity testing) verilebilir. Bunlar web sitesi sahibine kaynaklarını etkin şekilde kullanma ve bu şekilde talepleri karşılama olanağı verirken, aynı zamanda hizmetin engellenmesi (denial of service) saldırıları için de kullanılabilir. Benzer şekilde otomatik sızma test yazılımları (automated penetration testing), bilişim sisteminin sızma testlerini yapmak için kullanılabileceği gibi, bir bilişim sistemine hukuka aykırı olarak erişme için de kullanılabilir.[736] Fidye virüslerin bir zararlı yazılım türü olduğu yukarıda ifade edilmişti. Bu kapsamda fidye virüsler veya fidye virüs oluşturma kitlerinin birden fazla kullanıma uygun olmadığı, bunların Siber Suçlar Sözleşmesi'nin 6'ncı maddesi kapsamına giren cihazlar olduğu hususu genel olarak kabul görmektedir.[737]

Zararlı yazılımların üretilmesi ve bulundurulması birçok ülke mevzuatında da, Siber Suçlar Sözleşmesine paralel olarak düzenlenmiştir. Avustralya'da, Ceza Kanunu'nun 478.3 maddesinde, Nitelikli Bilgisayar Suçlarını düzenlenen 477'nci Bölümde yer alan suçların işlenmesi veya işlenmesinin kolaylaştırılması amacıyla verinin bulundurulması veya kontrol edilmesi suç olarak kabul edilmiştir. Burada yer alan veri kavramının kapsamına sadece şifre ve parolalar değil, zararlı yazılımlar da girmektedir. Benzer şekilde 478.4 maddesinde de, verinin üretimi, tedariki ve elde edilmesi yaptırıma bağlanmıştır.[738] Birleşik Krallık'ta Bilgisayarın Kötüye Kullanılması

[735] Bu hususstaki tartışmalar için bkz. **Wang**, s. 92; **Downing**, s. 734; **Clough**, s. 122.

[736] Örnekler için bkz. **Sommer, Peter**: Criminalising Hacking Tools, Digital Investigation, Vol. 3, 2006, s. 70 (ss. 68 – 72).

[737] **Sommer**, s. 69.

[738] Clough, s. 123, 124.

Yasası'na, 2006 yılında Siber Suçlar Sözleşmesi'nin 6'ncı maddesi kapsamında uyumlaştırma amacıyla eklenen 3A maddesi ile zararlı yazılımların üretilmesi, uyarlanması, sağlanması ve sağlanmasının teklif edilmesi cezalandırılmıştır.[739] Benzer şekilde Hollanda Bilgisayar Suçları Kanunu'nun 139d maddesi[740], Macar Ceza Kanunu'nun 424.1 maddesi[741], Litvanya Ceza Kanunu'nun 198/2 maddesi[742], Siber Suçlar Sözleşmesinin 6'ncı maddesine benzer şekilde zararlı yazılımların üretilmesi, bulundurulması ve ticaretini yaptırım altına almıştır.

Siber Suçlar Sözleşmesi'nin iç hukuka aktarılmasından sonra özellikle Sözleşme ile iç hukukun uyumlaştırılması kapsamında, TCK'na 245a maddesi eklenmiştir.[743] Söz konusu maddeye göre Bilişim Alanında Suçlar başlıklı Onuncu Bölümde ve bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imali, ithali, sevki, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması cezalandırılmıştır. Madde geniş bir şekilde kaleme alınmış ve bilgisayar programlarına da maddede açıkça yer verilmiştir. Bu kapsamda fidye virüsün, bilişim sistemlerindeki verilere veya sisteme zarar vermek amacıyla oluşturulması, ticarete konu edilmesi ve bulundurulması TCK m. 245a kapsamında cezalandırılacaktır.[744]

C. TCK m. 244/2 SİSTEMDE YER ALAN VERİLERİ ERİŞİLMEZ KILMA SUÇ TİPİ

Fidye yazılımın yayılmasından önceki aşama olan virüsün oluşturulması, tedariki, bulundurulması eylemlerinin ayrı bir suç olarak değerlendirildiğini yukarıda belirttik. Fidye virüs ikinci aşamada hedef bilişim sistemine yerleşmektedir. Fidye yazılım önce kendisini mağdurun bilişim sistemine yerleştirmektedir. Bunu çok yaygın bir yöntem olarak sosyal mühendislik[745]

---

[739] **Clough**, s. 128.

[740] **Koops, B. J.**: Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, Vol. 14.3, December 2010, www.ejcl.org, Erişim Tarihi: 02 Nisan 2019.

[741] **Mezei**, Kitti: The Regulation of Crimes Against Information Systems in Hungary, Journal of Eastern – European Criminal Law, No. 2, 2017, s. 210 (ss. 203 – 216).

[742] **Sauliūnasi**, Darius: Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime, Jurisprudence, 2010, 4 (122), s. 213 (ss. 203 – 219).

[743] 24.03.2016 tarih ve 6698 sayılı Kanun'un 30'uncu maddesi ile.

[744] Bu konuda bkz. **Korkmaz**, İbrahim: Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu, Terazi Hukuk Dergisi, Vol. 13, Sayı 142, Haziran 2018, ss. 45 – 55.

[745] *"Sosyal mühendislik, bilgi sistemlerini tehlikeye atabilecek kullanıcıları bulma sanatıdır. Sistemlere yapılan teknik saldırılar yerine, sosyal mühendisler bilgiye erişimi olan insanları hedef alır ve gizli bilgileri*

saldırısı ile gerçekleştirmektedir. Mağdurun elektronik postasına ilgisini çekecek bir belge (çoğunlukla hizmet aldığı telefon şirketinden gelen yüksek bir fatura) gönderilmekte ve mağdurun söz konusu belgeye "tıklaması" suretiyle virüsün, mağdurun bilgisayarına indirilmesi gerçekleşmektedir.

Fidye yazılımda, fidye yazılımı gönderen fail, mağdur bilişim sistemine hukuka aykırı olarak erişmemektedir. Bu bakımdan fidye yazılımların kullanılmasında, bilişim sistemine hukuka aykırı erişim suçu (TCK m. 243/1) normal şartlar altında oluşmayacaktır. Bununla birlikte fidye yazılımın sisteme yerleştirilme şekline göre, bilişim sistemine hukuka aykırı erişim suçunun da oluşabileceği düşünülecektir. Örneğin bilişim sistemine fiziksel olarak erişip, taşınabilir bellek vasıtasıyla fidye yazılımın yüklenmesi veya bilişim sistemine hukuka aykırı erişerek, sisteme fidye yazılımın yerleştirilmesi durumunda ayrıca bilişim sistemine hukuka aykırı erişim suçunun oluşacağı söylenebilecektir.

Fidye yazılımın yüklenmesi aşamasında mağdurun bilişim sistemine veri yerleştirilmektedir. Dolayısıyla TCK m. 244/2'de yer alan sisteme veri yerleştirme suçunun oluştuğu söylenebilecektir. Fidye yazılım mağdur tarafından "tıklanmak" suretiyle indirildiğinden dolayı herhangi bir suçun oluşmadığı düşünülebilir. Çünkü TCK m. 244/2 bağlamında tipik hareket, verinin başkasının sistemine yerleştirilmesidir. Ancak burada mağdur, zararsız bir elektronik posta görüntüsü ile kandırılmakta ve suçu oluşturan (sisteme veri yerleştirme TCK m. 244/2) hareket, bizzat mağdurun kendisine yaptırılmaktadır.

Burada fidye yazılımı mağdurun bilişim sistemine yerleştirmek isteyen fail, araç durumunda bulunan mağdurun üzerindeki hâkimiyetini, mağdurda sebebiyet verdiği bir noksandan faydalanarak kurmaktadır. Başka bir anlatımla fidye yazılımı kendi bilişim sistemine yerleştiren mağdur, araç durumundaki kişidir ve hataya düşürülmek suretiyle hareketi gerçekleştirmektedir. Her ne kadar mağdurun gerçekleştirmiş olduğu hareket tipik değilse de, nitekim kendi bilişim sistemine kişinin kendi veri yerleştirmesi TCK m. 244/2'yi oluşturmamaktadır, aracının hareketinin tipik olmadığı durumlarda hataya düşüren şahıs bakımından dolaylı faillik gündeme gelebilecektir.[746]

---

açığa çıkarmaları için onları yanıltır veya başlamış olan kötü niyetli saldırılarını tamamlamak için onları etki altına alır ve ikna eder." Krombholz, Katharina - Hobel, Heidelinde - Huber, Markus – Weippl, Edgar: "Advanced Social Engineering Attacks" SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria, https://www.academia.edu/23907997/Advanced_social_engineering_attacks, Erişim Tarihi: 01 Nisan 2019.

[746] **Koca**, Mahmut – **Üzülmez**, İlhan, Türk Ceza Kanunu Genel Hükümler, 10. Baskı, Ankara 2017, s. 456.

Kanaatimizce sosyal mühendislik saldırısı gerçekleştirerek, mağdurda oluşturduğu bir hata sonucu, fidye yazılım olduğu gizlemek suretiyle mağdurun kendi bilişim sistemine fidye yazılımı indirmesine sebebiyet veren arkadaki kişi TCK m. 244/2 bakımından dolaylı faildir. Burada TCK m. 244/1 oluşmamaktadır çünkü söz konusu yazılım sistem dosyalarını şifrelememekte, sistem çalışmasına devam etmektedir. Bazı fidye virüs türlerinde, bilişim sisteminin işleyişinin engellenmesi de söz konusu olabilmektedir. Örneğin Locker fidye virüs ailesine mensup olan Reveton, bulaştığı bilişim sistemini kilitlemekte ve kullanıcının bilişim sistemini kullanmasını engellemektedir.[747]

Bazı fidye virüslerin verileri şifrelemekle kalmayıp, deşifre verileri de sildiği bilinmektedir.[748] Örneğin 2017 yılında yayılan SerbRansom fidye virüsü, 500 dolar ödenene kadar her 5 dakikada bir enfekte etmiş olduğu sistemden rastgele bir dosyayı silmektedir.[749] Dolayısıyla fidye virüsün türüne göre TCK m. 244/2'de yer alan seçimlik hareketlerden "silme" hareketi de söz konusu olabilecektir.

D. TCK m. 244/4 SİSTEMDE YER ALAN VERİLERİ ERİŞİLMEZ KILMA SURETİYLE HAKSIZ ÇIKAR SAĞLAMA SUÇ TİPİ

Bir sonraki aşamada, sistemde yer alan verilerin erişilmez kılınmasından sonra, fail, mağdura ulaşarak, verilerine tekrar erişebilmesi için belli bir menfaati kendisine temin etmeye zorlamaktadır. Burada menfaat temini, verilerin hâlihazırda geçici gelecekte ise daimi olarak erişilmez kılınacağı tehdidi ile gerçekleştirilmektedir. Fail tarafından gelecekte gerçekleştirilecek kötülüğün konusu, mağdurun bazen özel hayatı bazen de malvarlığı bakımından önemi bulunan verileridir. Fail, söz konusu verilere, mağdur tarafından bir daha erişilemeyeceği beyanını gerçekleştirmektedir. Güçlü şifreleme sistemleri göz önüne alındığında, söz konusu beyanın, verilerine bir daha erişilememe tehlikesi yaşayan mağdur bakımından da ciddi bir kaygıya neden olacağı açıktır.

Bu aşamada meseleyi, sistemde yer alan veriye erişilmesinin imkânsız kılınması suretiyle mağdurdan menfaat temini edilmesi kapsamında dar açıdan ele alırsak, TCK m. 244/4'ün oluşumu düşünülebilir. Kanun koyucu, TCK m. 244/4'de yer alan suçu tali bir norm olarak düzenlemiş ve

[747] **Rajput**, s. 30.

[748] **Liska / Gallo**, s. 11.

[749] **Rajput**, s. 32.

eylemin başka bir suçu oluşturmaması durumunda TCK m. 244/4'ün oluşabileceğini belirtmiştir.[750] TCK m. 244/4'ün tali bir norm olmasından dolayı, başka bir suçun oluşup oluşmadığı hususu da incelenmelidir.

E. TCK m. 148 YAĞMA SUÇ TİPİ

Fail, mağdura ait verileri şifrelemek suretiyle erişilmez kılmakta ve verilere tekrar erişemeyeceği beyanı ile menfaat temin etmektedir. Mağdur bakımından söz konusu verilerin malvarlığına dâhil olduğu ve bazı durumlarda verilerin kaybının, malvarlığı bakımından büyük bir zararı oluşturacağı hususu daha önce de ifade edildiği üzere olasıdır. Bu durumda, TCK m. 148'de yer alan yağma suçunun tatbiki de incelenmelidir. Yağma suçunda; *"bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden ya da malvarlığı itibarıyla büyük bir zarara uğratacağından bahisle tehdit ederek veya cebir kullanarak, bir malı teslime veya malın alınmasına karşı koymamaya mecbur kılınması"* gereklidir. Bu açıdan ilerleyen bölümlerde, yağma suçunun oluşup oluşmayacağı kısaca incelenecektir.

Fidye virüslerinde, verilerin kalıcı olarak erişilmez kılınacağı tehdidi ile mağdurdan kripto para temini eyleminin yağma suçunu oluşturup oluşturmadığı belirlenirken kanaatimizce iki husus açıklanmalıdır. Birinci olarak verilerin kalıcı olarak erişilmez kılınmasının, yağma suçunun oluşumu için tehdidin konusu bakımından *"mağdurun malvarlığı açısından büyük bir zarar"* oluşturup oluşturmayacağı meselesi çözülmelidir. İkinci olarak mağdur tarafından faile yapılan ödemede kullanılan kripto paranın, TCK m. 148'de yer alan *"bir malı teslime veya malın alınmasına karşı koymama"* kapsamında mal olarak değerlendirilip değerlendirilmeyeceği açıklanmalıdır.

Öncelikle suçun oluşması bakımından failin gerçekleştirdiği tehdit, verilerin kalıcı olarak erişilmez kılınacağına ilişkindir. Tehdidin konusu bazı durumlarda "malvarlığı" da olabilir. Nitekim sistemde yer alan veriler, malvarlığı değeri olarak da kabul görmektedir. Özellikle bankacılık sisteminde yer alan kaydi paralarda durum böyledir. Bankacılık sisteminde yer alan ve parasal anlamda malvarlığını, bilişim sistemlerinde yer alan veri temsil etmektedir. Malvarlığını temsil eden, mağdur açısından mali değeri olan bilişim sistemindeki verinin erişilmez kılınacağı yönündeki bir beyanın, genel bir kural olarak ifade edilemese de *"malvarlığı açısından büyük bir zarar"* oluşturması ihtimali mevcuttur. Benzer şekilde, *wannacry* örneğinde olduğu gibi sağlık sisteminde sağlık hizmeti alan kişilere ait veriler de, sağlık hizmeti veren birim bakımından

[750] **Koca / Üzülmez**, Özel Hükümler, s. 842.

malvarlığı açısından büyük bir zarar oluşturabilecektir. Nitekim söz konusu verilere ulaşılamaması sağlık hizmetinin sunulamamasına ve dolayısıyla da sağlık hizmeti veren birimin kazanç elde edememesine neden olmaktadır. Bu açıdan verilerin kalıcı olarak erişilemez kılınması tehdidi, malvarlığı açısından büyük bir zarar oluşturma tehdidi olarak değerlendirilebilecektir. Ayrıca yine wannacry örneğinde olduğu gibi çalışan bir sağlık tesisinden hizmet alan kişilere ait verilere ulaşılamaması, teşhis ve tedavi süreçlerini aksatacağından kişiler bakımından vücut bütünlüğü ve hatta yaşam bakımından da tehdit oluşturabilecek niteliktedir.

Tehdidin gerçekleştiğini tespit ettikten sonra *"malın teslime veya malın alınmasına karşı koymamaya mecbur kılınması"* unsurunun gerçekleşip gerçekleşmediği değerlendirilmelidir. Yağma suçunda, her ne kadar sadece "*mal*" terimi kullanılmış ve söz konusu terimin "*taşınabilir*" olma özelliği belirtilmemişse de, gerek madde gerekçesinde gerekse de öğretide, yağma suçunun kanuni tanımında yer alan malın, *"taşınabilir mal*" olduğu konusunda görüşler mevcuttur.[751] Bu durumda fail tarafından temin edilen menfaatin [çoğunlukla kripto/elektronik para (bitcoin) şeklindedir] madde metninde geçen "*mal*" terimi kapsamında olup olmadığı değerlendirilmelidir. Öğretide bazı yazarlar tarafından verinin, hırsızlık suçunun konusunu oluşturan taşınabilir bir mal olmadığı ileri sürülmektedir.[752] Karşı görüşte olan yazarlar, internet bankacılığı üzerinden yapılan para göndermelerinde bilişim sistemlerinin araç olarak kullanıldığını, burada yer alan eylemin paranın mağdurun çantasından alınmasından bir farkının olmadığını belirtmektedirler.[753]

Yargıtay Ceza Genel Kurulu, kişilerin internet bankacılığı hesap şifrelerinin kullanılarak, hesaplarında yer alan parayı temsil eden verilerin, başka hesaplara nakledilmesi fiillerinde oluşan suçun "Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık" olduğunu

---

[751] **Tezcan**, Durmuş – **Erdem**, Mustafa Ruhan – **Önok**, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, 12. Baskı, Ankara 2015, 656; **Koca / Üzü**lmez, Özel Hükümler, s. 585; **Malkoç**, İsmail, Açıklamalı Türk Ceza Kanunu, 2. Cilt, Ankara 2013, s. 2427; **Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker**, Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara 2018, s. 656.

[752] Bkz. **Yazıcıoğlu**, Yılmaz, "Yeni Türk Ceza Kanunu'ndaki Bilişim Suçlarının Genel Değerlendirilmesi", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.II, S.2, 2005, s. 398; **Özbek**, Veli Özer, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof.Dr. Ünal Narmanlıoğlu'na Armağan, C. 9, 2007, s. 1058; **Başbüyük**, İsa, "İnternet Bankacılığı Aracılığı ile Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi, Ceza Hukuku Dergisi, Y. 8, S. 21, Nisan 2013, s. 199.

[753] **Kurt**, Levent, Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara 2005, s. 169; Başbüyük, s. 199; **Taşkın**, Şaban Cankat, Bilişim Suçları, Bursa 2008, s. 116.

kararlaştırmıştır.[754] Yargıtay uygulaması söz konusu Ceza Genel Kurul kararından sonra da, benzer şekilde devam etmektedir.[755]

Yargıtay Ceza Genel Kurulu ve sonrasında ise özel dairelerin kararlarında yer alan veri, bankacılık bilişim sisteminde yer alan ve karşılığı para olarak temsil edilen bir veridir. Söz konusu verinin gönderilmesi durumunda, TCK m. 142/2-e veya TCK m. 244/2-4 kapsamında değerlendirilmesi noktasında görüş farklılıkları bulunmakla birlikte, inceleme konumuz olan olayda verilmesi istenen şey (bitcoin) bir sanal para çeşididir.[756] Sanal paraların kanuni düzenlemesi bulunmamakla beraber, günümüzde mal mübadelesinde kullanılmakta ve bir ekonomik değeri temsil etmektedir.

Kanaatimizce konuyu birbirinden farklı iki ihtimale göre ayırarak incelemek gereklidir. Öğretide yağma suçuna konu olan malın; "maddi bir varlığa sahip olma", "hâkimiyete elverişlilik" ve "kişilik dışı olma" şeklinde üç özelliğinin bulunduğu ifade edilmektedir.[757] Kripto paraların[758] kişilik dışı ve hâkimiyete elverişli olduğu noktasında büyük bir tartışma olmadığı kanaatindeyiz. Ancak maddi bir varlığa sahip olup olmadığı değerlendirilmelidir. Kripto para belli algoritmalarla matematiksel işlemler sonucunda üretilen ve benzeri bulunmayan veri parçalarıdır. Söz konusu veriler, bilişim sistem araçlarında tutulabilmektedir. Bu bilişim sistem araçları, sisteme bağlı olduğu zaman "online - sıcak cüzdan", sisteme kullanıcı tarafından istendiği zaman bağlı olduğunda "offline – soğuk cüzdan (cold wallet)" olarak adlandırılmaktadır. Soğuk cüzdanda kripto para çoğunlukla, bir veri taşıma aracında bulunmaktadır. Bu kapsamda kripto paranın, soğuk cüzdanda bulunması durumunda, söz konusu veri taşıma aracının içindeki kripto para ile birlikte mal olarak değerlendirileceği açıktır.[759] Sıcak cüzdanda, başka bir anlatımla sistem üzerinde manyetik veri olarak tutulduğunda, sadece bu verinin ekonomik değer olduğundan hareketle mal

---

[754] Yargıtay Ceza Genel Kurulu, 17.11.2009, 11-193/268.

[755] Yargıtay 13.CD, 11.4.2017, 2015/15567, 2017/3907; Yargıtay 17.CD, 20.6.2016, 2015/16533, 2016/9189; Yargıtay 22.CD, 13.6.2016, 2015/17809, 2016/10066.

[756] **Bozkurt Yüksel**, Armağan Ebru, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış", İÜHFM, C. LXXIII, S. 2, s 173-220, 2015, s. 197.

[757] **Koca**, Mahmut, Yağma Cürümleri, Ankara 2003, s. 92.

[758] *"Kripto para; güvenliğin sağlanması için kriptografi (şifreleme bilimi) kullanan dijital veya sanal bir para birimidir. Bu paralar sanal cüzdanlara şifreler kullanılarak yerleştirilmekte ve aynı şekilde şifreler aracılığıyla kullanıldığı için de bu adı almaktadır."* **Günay, Furkan / Kargı, Veli**, "Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi", Journal of Life Economics, C. 5, S. 3, Temmuz 2018, s. 62.

[759] Bu konuda benzer bir değerlendirme için bkz. **Sirmen**, Lale, Eşya Hukuku, 3. Bası, Ankara 2015, s. 5.

olarak kabul edilip edilemeyeceği hususunun bu kadar açık olmadığını ifade etmeliyiz. Hırsızlık suçunun konusunun taşınabilir mal olduğu değerlendirildiğinde[760], Yargıtay'ın söz konusu verinin temsil ettiği değeri esas alarak ulaştığı sonuç göz önünde bulundurulduğunda, mağdurun kripto parayı teslime zorlanması durumunda da "yağma" suçunun oluşacağı söylenebilir. Ayrıca yağma virüslerde çoğunlukla, belli bir dolar karşılığı kripto para istendiğinden dolayı, teslime zorlananın mal olduğu da rahatlıkla söylenebilecektir.

5237 sayılı TCK'da Yağma suçunun, 765 sayılı TCK'nın aksine "Mal Aleyhine Cürümler" değil, "Malvarlığına Karşı Suçlar" arasında düzenlenmiş olması da, yukarıda varmış olduğumuz sonucun desteklenmesi açısından önemlidir. Nitekim 765 sayılı TCK'nın mehazı olan Zanardelli Kanunu'nda "mal" kavramı kullanılmasına rağmen, Rocco Kanunu, mal teriminin yetersizliğinden hareketle "malvarlığı" (il patrimonio) terimini kullanmıştır.[761] Söz konusu tercih, Türk kanun koyucusu tarafından kabul görmüş ve 5237 sayılı Kanunda "Malvarlığı" terimi kullanılmıştır.[762] Kripto paraların da, kişinin malvarlığına dâhil olduğu ve bu anlamda da yağma suçunun konusunu oluşturabileceği kanaatindeyiz.

F. ŞANTAJ SUÇU (TCK m. 107)

Burada kısaca şantaj suçunun uygulanma olanağının bulunup bulunmadığı hususunu da değerlendirmek istiyoruz. Fidye virüslerde, fail, mağdura ait ve bazen özel hayat alanına ait olan verileri de şifrelemekte ve menfaat karşılığında mağdura verilerine tekrar erişme olanağı sunmaktadır. Mağdurun menfaat temin etmemesi durumunda, verilerine bir daha ulaşamayacağı tehdidini de gerçekleştirmektedir.

TCK'nın 107'nci maddesinde düzenlenen şantaj suçunda; a. Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle çıkar sağlama ve b. Çıkar sağlamak amacı ile kişinin şeref ve saygınlığına zarar verecek nitelikteki hususların açıklanması veya isnat edilmesi yaptırım altına alınmıştır. Bu düzenleme, fidye virüslerin yarar sağlanması amacı ile yayılması dikkate alındığında, "yarar sağlama" noktasında uygulanabilir görünmektedir.[763]

---

[760] Değerlendirme için bkz. **Evik**, Ali Hakan, "Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık' Suçuna İlişkin Bir Yargıtay Kararının Değerlendirilmesi, Köksal Bayraktar'a Armağan, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2010/1, C.1, s. 703 vd.

[761] **Hafızoğulları**, Zeki / **Özen**, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara 2016, s. 302

[762] **Taşkın**, Ahmet, "Yağma Suçunda Mal Kavramı", Terazi Hukuk Dergisi, Nisan 2008, S. 20, s. 95.

[763] **Taner**, Fahri Gökcen, "Türk Ceza Hukukunda Şantaj Suçu", Türkiye Barolar Birliği Dergisi, 2011 (92), s. 127 vd.

Kanaatimizce TCK'nın 107'nci maddesinin uygulanma olanağı fidye virüsler bakımından yoktur. Nitekim, fidye virüsler çıkar sağlamayı amaçlamakta ancak söz konusu çıkarı sağlamak için mağdurun verilerine erişememesi tehdidini gerçekleştirmektedir. Söz konusu durum fidye virüs faillerinin hakkı olan veya yükümlü olduğu bir durum olmadığından dolayı TCK m. 1071/1'in uygulanma olanağı yoktur. Benzer şekilde TCK m. 107/2'de de, kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği düzenlenmektedir. Mağdurun, niteliği ne olursa olsun verilerine tekrar ulaşamaması ve buna yönelik tehdit, "hususun açıklanması veya isnadı" kapsamında değerlendirilemeyecektir. Hatta söz konusu verilere ulaşamadığından dolayı kişinin şeref ve saygınlığı doğrudan veya dolaylı olarak zarar görmüş olsa bile, fidye virüsler bakımından "açıklama veya isnat" söz konusu olmayacaktır.

IV. SUÇLARIN İÇTİMAI KAPSAMINDA DEĞERLENDİRME

Son olarak durumu suçların içtiması bakımından da ele almalıyız. Bilinmektedir ki, genel kural *"ne kadar fiil, o kadar suç", "ne kadar suç, o kadar ceza"* şeklindedir. Dolayısıyla öncelikle fiil/hareket[764] sayısının belirlenmesi gereklidir. Fidye virüsün, daha sonraki eylemler bakımından oluşturulması, bulundurulması ve ticareti, TCK m. 245a kapsamında bağımsız bir suç tipidir. Fidye virüsün daha sonra kullanılıp kullanılmayacağından bağımsız olarak, TCK m. 245a'nın oluştuğu ifade edilebilir.

Birinci adımda gerçekleştirilen ve mağdurun, sistemine veri eklenmesini sağlayan hareket ile mağdurun sistemine bulaşan virüsün sistemdeki veriyi şifrelemesindeki hareket *"doğal anlamda fiil tekliği"*[765] kapsamında değerlendirilemeyecek şekilde birbirinden farklıdır. Ancak *"sisteme veri yerleştirme"* ve *"sistemde yer alan veriyi erişilmez kılma"* hareketleri aynı suçun seçimlik hareketleri olduğundan ve aynı konu üzerinde işlendiği müddetçe seçimlik hareketlerin birden fazlasının icrası *"tipik fiil tekliği"* kapsamında değerlendirileceğinden tek bir suç oluşacaktır.

Sistemde yer alan verinin kalıcı olarak erişilmez kılınmasına yönelik tehdidin sonrasında kripto paranın temini durumunda, oluşabilecek suç tipine göre farklı sonuçlara varmak gereklidir. Kripto paranın mal olarak değerlendirilemeyeceği ve dolayısıyla TCK m. 148'in oluşmadığı düşünülürse, TCK m. 244/4 oluşacaktır. TCK m. 244/1 ve 2'de yer alan fiiller, TCK m. 244/4'ün

[764] Bu konuda detaylı açıklamalar ve teoriler için bkz. **Göktürk**, Neslihan, Fikri İçtima, Ankara 2013, s. 17 vd.

[765] **Göktürk**, s. 99.

unsuru olduğundan dolayı ayrıca cezalandırılmayacaktır. Ancak TCK m. 148'in oluştuğu düşünülürse, yağma suçu da bileşik bir suç olduğundan dolayı bünyesinde yer alan tehdit suçundan dolayı ayrıca cezalandırma yapılmayacaktır. Eğer TCK m. 244/4 ve TCK m. 148'in beraber oluştuğu düşünülecek olursa, TCK m. 244/4'ün tali norm olmasından dolayı TCK m. 148 uygulanacaktır.

IV. SONUÇ VE DEĞERLENDİRME

Zararlı yazılım yasa dışı pazarı, vaat ettiği kazanca paralel olarak büyümekte ve karmaşıklaşmaktadır. Daha önceleri basit birkaç zararlı etkiye sahip virüslerle karşılaşılırken, bugün yayılmasından, sistemi enfekte etmesine; zararlı yazılım faili ile iletişim kurmasından, menfaatin belirlenmesine kadar karmaşık ve bir o kadar da mağdurun savunmasını zayıflatan virüslerle karşı karşıyayız.

Bu çalışmada farklı bir açıdan ele almak istediğimiz cryptolocker özelinde fidye yazılımlar, yayılmasından menfaatin temini aşamasına kadar farklı suçların oluşumuna sebebiyet vermektedir. Bu kapsamda virüsün temini veya üretimi açısından TCK m. 245a maddesinin oluşumu düşünülebilecektir. Nitekim karmaşık bir yapıya ve farklı bir modus operandiye sahip olan virüs, bireysel üretimin yerine sanal yeraltı pazarlarından temin edilmektedir. Söz konusu sanal yeraltı pazarlarında virüsün yazımı, üretime hazır hale getirilmesi, yerleştirilmesi ve hatta menfaatin temini aşamasına kadar hizmetler de sunulmaktadır.

İkinci olarak virüsün, mağdurun sistemine yerleştirilmesinde mağdurun iradesinin yanıltılarak sisteme yerleştirme hareketinin mağdura yaptırıldığını görmekteyiz. Bu durumda TCK m. 244/2'de yer alan sisteme veri yerleştirme hareketi söz konusudur ancak zararlı yazılım failinin sorumluluğu dolaylı fail şeklinde olacaktır.

Üçüncü aşamada sistemin enfekte edilerek bazı verilerin ulaşılmaz kılınması söz konusudur. Bu aşamada ise TCK m. 244/2'de yer alan seçimlik hareketlerden biri olan "sistemde yer alan verinin erişilmez kılınması" gündeme gelebilecektir. Bazı fidye virüslerin, sistemin çalışmasını da etkilediği bilindiğinden TCK m. 244/1'in oluşumu da olası olacaktır.

Sistemi enfekte eden fidye virüs, söz konusu erişilmez kılınmanın daimi olacağı tehdidi ile menfaati temin etmeye çalışmaktadır. Menfaat çoğunlukla belli bir para karşılığı olan kripto paradır. Burada ise yukarıda belirttiğimiz esaslar kapsamında yağma suçunun oluşacağı kanaatindeyiz.

KAYNAKÇA

Ablon, Lilian / Libicki, Martin C. / Golay, Andrea A.: Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, RAND 2014, s. 3 – 19.

Başbüyük, İsa, "İnternet Bankacılığı Aracılığı ile Yapılan Hukuka Aykırı Havalenin Bilişim Suçları Bakımından Değerlendirilmesi, Ceza Hukuku Dergisi, Y. 8, S. 21, Nisan 2013.

Bozkurt Yüksel, Armağan Ebru, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış", İÜHFM, C. LXXIII, S. 2, s 173-220, 2015.

Brown, Gary D. / Metcalf, Andrew O.: Easier Said Than Done: Legal Review of Cyber Weapons, Journal of National Security Law & Policy, Vol. 7, 2014, ss. 115 – 138.

Cesare, Kelly: Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution, The Transnational Lawyer, Vol. 14, 2001, s. 141 (ss. 136 – 170).

Clough, Johathan: Principles of Cybercrime, Cambridge University Press, 2010, s. 120; **Viano, Emilio C.**: Cybercrime: Definition, Typology, and Criminalization, in: Cybercrime, Organized Crime and Societal Responses, International Approaches (Ed. Emilio C. Viano), Springer 2017.

Denning, Dorothy: Reflections on Cyberweapons Controls, Computer Security Journal, Vol. XVI, No. 4, Fall 2000, ss. 43 – 53.

Dévai Dóra, Proliferationf of Offensive Cyber Weapons. Strategic Implications and Non – Proliferation Assumptions, AARMS Vol. 15, No. 1, 2016, ss. 61 – 73.

Dolliver, D.S. / Kenney, J.L.: Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison, in: Victim & Offenders, Taylor & Francis Group, 2016, s. 601, 602 (ss. 600 – 620).

Downing, Richard: Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime, 43 Colum. J. Transnat'l L. 705, (2005), (ss. 705 – 762).

Evik, Ali Hakan, "Bilişim Sistemlerinin Kullanılması Suretiyle İşlenen Hırsızlık' Suçuna İlişkin Bir Yargıtay Kararının Değerlendirilmesi, Köksal Bayraktar'a Armağan, Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2010/1, C.1.

Flint, **David**, Law Shaping Technology: Technology Shaping the Law, International Review of Law, Computers and Technology, Vol. 23, No. 1 – 2, March – July 2009, s. 5 – 11.

Göktürk, Neslihan, Fikri İçtima, Ankara 2013.

Günay, Furkan / Kargı, Veli, "Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi", Journal of Life Economics, C. 5, S. 3, Temmuz 2018.

Hafızoğulları, Zeki / **Özen**, Muharrem, Türk Ceza Hukuku Özel Hükümler, Kişilere Karşı Suçlar, Ankara 2016.

Hugher, **Thomas** P., Technological Momentum, in: Does Technology Drive History? The Dilemma of Technological Determinism (Edited by Merritt Roe Smith and Leo Marx), Cambridge, MIT Press, 1994.

Kharraz, Amin / Robertson, William / Balzarotte, Davide / Bilge, Leyla / Kirda, Engin: Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks,M. Almgren et al. (Eds.): DIMVA 2015, LNCS 9148, pp. 3–24, Springer 2015.

Koca, Mahmut – **Üzülmez**, İlhan, Türk Ceza Kanunu Genel Hükümler, 10. Baskı, Ankara 2017, s.

Koca, Mahmut, Yağma Cürümleri, Ankara 2003.

Koops, B. J.: Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, Vol. 14.3, December 2010, www.ejcl.org, Erişim Tarihi: 02 Nisan 2019.

Korkmaz, İbrahim: Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu, Terazi Hukuk Dergisi, Vol. 13, Sayı 142, Haziran 2018, ss. 45 – 55.

Kroczynski, Robert J.: Are the Current Computer Crime Laws Sufficient or Should the Writing of Virus Code Be Prohibited?, Fordham Intell. Prop. Media & Ent. L. J., Vol. 18, 2008, (ss. 817 – 865).

Krombholz, Katharina - Hobel, Heidelinde - Huber, Markus – Weippl, Edgar: "Advanced Social Engineering Attacks" SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria, https://www.academia.edu/23907997/Advanced_social_engineering_attacks, Erişim Tarihi: 01 Nisan

Kurt, Levent, Açıklamalı ve İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara 2005.

Liska, Allan / Gallo, Timothy: Ransomware Defending Against Digital Extortion, O'Reilly, 2017.

Mabunda, Sagwadi: Cyber Extortion, Ransomware and the South African Cybercrimes and Cybersecurity Bill, Statute Law Review, 2017.

Maitra, Amit K.: Offensive Cyber-Weapons: Technical, Legal, and Strategic Aspects, Environs Syst Decis, Springer 2014.

Malkoç, İsmail, Açıklamalı Türk Ceza Kanunu, 2. Cilt, Ankara 2013.

McLuhan, **Marshall**, Understanding Media: The Extension of Man, McGraw Hill, New York 1996.

Mezei, Kitti: The Regulation of Crimes Against Information Systems in Hungary, Journal of Eastern – European Criminal Law, No. 2, 2017, (ss. 203 – 216).

Özbek, Veli Özer / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker, Türk Ceza Hukuku Özel Hükümler, 13. Baskı, Ankara 2018.

Özbek, Veli Özer, "Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Prof.Dr. Ünal Narmanlıoğlu'na Armağan, C. 9, 2007.

Paquet – Clouston, Masarah / Haslhofer, Bernhard / Dupont, Benoît: Ransomware Payments in the Bitcoin Ecosystem, The 17th Annual Workshop on the Economics of Information Security (WEIS), June 2018, Innsbruck, Austria.

Pascariu, Cristiona / Barbu, Ionut – Daniell / Bacivarov, Ioan C.: Investigative Analysis and Technical Overview of Ransomware Based Attacks.Case Study: WannaCry, International Journal of Information Security and Cybercrime, Vol. 6, Issue 1, 2017, s. 57 (ss. 57 – 62).

Perloff – Giles, Alexandra: Transnational Cyber Offences: Overcoming Jurisdictional Challenges, 43 Yale J. Int'l L. (2018), s. 197 (ss. 191 – 227).

Peterson, Dale: Offensive Cyber Weapons: Construction, Development, and Employment, The Journal of Strategic Studies, Vol. 36, No. 1, 2013, ss. 120 – 124.

Prunckun, Henry: The Rule of Law: Controlling Cyber Weapons, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018, (Prunckun, Cyber Weapons olarak anılacaktır).

Prunckun, Henry: Weaponization of Computers, in : Cyber Weaponry, Issues and Implications of Digital Arms (Ec. Henry Prunckun), Springer 2018.

Rajput, Toshima Singh: Evolving Threat Agents: Ransomware and their Variants, International Journal of Computer Applications, Vol. 164, No. 7, April 2017, s. 28 vd. (ss. 28 – 34).

Richardson, Ronny / North, Max M.: Ransomware: Evolution, Mitigation and Prevention, International Management Review, Vol.13, No.1, 2017, s. 12 (ss. 10 – 21).

Sauliūnasi, Darius: Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with the Convention on Cybercrime, Jurisprudence, 2010, 4 (122), (ss. 203 – 219).

Shaw, Malcolm N.: International Law, 6 th Edition, Oxford University Press 2008, s. 1; Bakınız aynı şekilde **Kettemann**, **Matthias C.**: Ensuring Cybersecurity Through International Law, 69 R.E.D.I. 281, 2017, s. 281 (ss. 281 – 289).

Sherer, James A. / McLellan, Melinda L. / Fedeles, Emily R. / Sterling, Nichole L.: Ransomware – Practical and Legal Considerations for Confronting the New Economic Engine of the Dark Web, Richmond Journal of Law & Technology, Vol. XXIII, Issue 3, s. 1 (ss. 1 – 48).

Sirmen, Lale, Eşya Hukuku, 3. Bası, Ankara 2015.

Sommer, Peter: Criminalising Hacking Tools, Digital Investigation, Vol. 3, 2006, (ss. 68 – 72).

Taner, Fahri Gökcen, "Türk Ceza Hukukunda Şantaj Suçu", Türkiye Barolar Birliği Dergisi, 2011 (92) (ss. 118 – 156).

Taşkın, Şaban Cankat, Bilişim Suçları, Bursa 2008.

Taşkın, Ahmet, "Yağma Suçunda Mal Kavramı", Terazi Hukuk Dergisi, Nisan 2008, S. 20.

Tekin, Derya: Bir Ceza Politikası Olarak Hazırlık Hareketlerinin Cezalandırılması: Türk ve İngiliz Yasal Düzenlemelerinin Karşılaştırmalı Analizi, Terazi Hukuk Dergisi, C. 13, S. 146, Kasım 2018, (ss. 48 – 60).

Tezcan, Durmuş – **Erdem**, Mustafa Ruhan – **Önok**, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, 12. Baskı, Ankara 2015.

TK, Anjana: Discussion on Ransomware, Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks, IJRTI, Vol. 2, Issue 6, 2017, s. 210 (ss. 210 – 214).

Volokh, Eugene: Akademik Metinler Nasıl Yazılır? Hukukçular için Rehber (Çev.: Ertuğrul Uzun), Tekin Yayınları İstanbul 2019.

Walden, Ian: Computer Crimes and Digital Investigations, Oxford University Press, New York 2007.

Wang, Qianyum: A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and Council of Europe, Ph.D. Thesis, Erasmus University, Rotterdam 2016.

Yazıcıoğlu, Yılmaz, "Yeni Türk Ceza Kanunu'ndaki Bilişim Suçlarının Genel Değerlendirilmesi", Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C.II, S.2, 2005.