Araştırma Makalesi
Research Article

Gönderim / Received: 14/07/2023
Kabul / Accepted: 13/01/2024

Hukuk Fakültesi Dergisi
Ankara Hacı Bayram Veli University
Faculty of Law Review

ISSN: 2651-4141 e-ISSN: 2667-4068
Cilt / Volume XXVIII Ocak / January 2024 Sayı / No. 1

SİBER ÇATIŞMADA SİVİL VERİLERİN ROMA STATÜSÜ AÇISINDAN DEĞERLENDİRİLMESİ

THE EVALUATION OF CIVILIAN DATA IN CYBER CONFLICT IN TERMS OF THE ROMA STATUTE

Berkant AKKUŞ*

10.34246/ahbvuhfd.1327670

ÖZET

Saldırı ve savunma amaçlı siber yeteneklerin gelişmesiyle birlikte siber operasyonlar artan bir şekilde savaş araç ve yöntemi olarak kullanılmaya başlamıştır. Bu gerekçeyle sivillerin, sivil altyapının, sivil verilerin oluşacak siber zararlardan korunması zaruridir. Bu makalenin ana araştırma sorusu, silahlı çatışma esnasında verilere yönelik gerçekleştirilen siber operasyonların Roma Statüsü doğrultusundan savaş suçu olarak kabulünün mümkün olup olmadığını tespit edebilmektir. Bilgisayar verilerinin statüsü tartışmalıdır. Siber çatışmalarda verilere yönelik gerçekleştirilen saldırılar somut nesneleri de etkilemektedir. Bu makalede, Roma Statüsü kapsamında bilgisayar verileri nesne veyahut mal olarak kabul edilebilir mi sorusunu netleştirmek amacıyla doktrindeki tartışmalar ve farklı hukuk sistemlerindeki mahkeme kararları değerlendirilmiştir. Suçta ve cezada kanunilik ilkesi doğrultusunda Roma Statüsü'nün yeniden yorumlanması gerekmektedir. Günümüzde teknolojide yaşanan gelişmeler yeni savaş metotlarını ortaya çıkarmıştır. Bu nedenle, Roma Statüsü'nün bu değişime uygun bir yanıt sağlayıp sağlamadığının değerlendirilmesi neticesinde, vahamet eşiği dikkate alınarak yalnızca ciddi sonuçları olan siber operasyonlar soruşturma konusu olmalıdır.

* **Dr. Öğr. Üyesi**, İstanbul Okan Üniversitesi Hukuk Fakültesi, Devletler Genel Hukuku Anabilim Dalı/İSTANBUL, **e-posta:** berkantakkus91@gmail.com, **ORCID:** 0000-0001-6652-2512, **DOI:** 10.34246/ahbvuhfd.1327670.

- Atıf Şekli | ***Cite As:*** Akkuş B, "Siber Çatışmada Sivil Verilerin Roma Statüsü Açısından Değerlendirilmesi", *AHBVÜ Hukuk Fakültesi Dergisi*, 28(1), 2024, s.393-434
- İntihal / ***Plagiarism***: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. / *This article has been scanned via a plagiarism software and reviewed by at least two referees.*

Anahtar Kelimeler: *Siber saldırı, Sivil veri, Roma Statüsü, Savaş suçları, Uluslararası Ceza Hukuku*

ABSTRACT

With the development of offensive and defensive cyber capabilities, cyber operations are increasingly being used as a means and method of warfare. For this reason, it is crucial to protect civilians, civilian infrastructure, and civilian data from cyber damage. The main research question of this article is to determine whether cyber operations against data during armed conflict can be considered as war crimes in line with the Rome Statute. The status of computer data is controversial. Attacks on data in cyber conflicts also affect tangible objects. This article will focus on the debates in the doctrine in order to clarify the question of whether computer data can be considered as object or property under the Rome Statute. At the same time, court decisions will be analyzed. The Rome Statute needs to be reinterpreted in line with the principle of legality in crime and punishment. Today, developments in technology have led to new methods of warfare. Therefore, it will be evaluated whether the Rome Statute provides an appropriate response to this change.

Keywords: *Cyber attack, Civil data, Rome Statute, War crimes, International Criminal Law*

EXTENDED ABSTRACT

This article explores the intricate relationship between cyber operations targeting civilian data and the provisions outlined in the Rome Statute regarding war crimes against protected objects and property. As cyber warfare becomes increasingly prevalent in modern conflicts, the study aims to scrutinize the legal implications of such operations within the context of international humanitarian law. The research commences with an in-depth analysis of the evolving landscape of cyber warfare and its impact on civilians. It emphasizes the distinctive nature of attacks on data, considering them as virtual, yet critical, components of the infrastructure. The study investigates how well the existing legal framework, specifically the Rome Statute, accommodates the nuances of cyber operations against civilian data.

The legality of cyber operations during armed conflict and whether they could amount to a war crime under the Statute of the International Criminal Court (ICC) is a complex and evolving area of international law. The Rome Statute of the International Criminal Court outlines specific war crimes in its text, such as intentionally directing attacks against civilians, using prohibited weapons, or attacking civilian objects. However, the Rome Statute was adopted in 1998, before the widespread use and understanding of cyber operations in the context of armed conflict.

There is ongoing debate among legal scholars and practitioners regarding the classification of cyber operations during armed conflict and whether they fall under existing definitions of war crimes. Some argue that certain cyber operations, such as those causing significant harm to civilians or civilian infrastructure, could potentially be considered war crimes under existing legal frameworks. Others contend that the traditional definitions of war crimes may not adequately capture the unique aspects of cyber operations. The applicability of international humanitarian law (IHL) principles, such as distinction, proportionality, and necessity, to cyber operations is also a subject of discussion. States are expected to adhere to these principles during armed conflicts to minimize harm to civilians and civilian objects.

Central to the analysis is the interpretation of "protected objects and property" as defined in the Rome Statute. The article delves into whether this definition adequately captures the multifaceted nature of civilian data and if it effectively addresses the unique challenges posed by cyber operations. This includes considerations of the intangible nature of data, potential long-term consequences, and the difficulties in attribution. The study likely explores relevant case studies or incidents where cyber operations against civilian data could be interpreted as violations of the Rome Statute. This examination helps to illustrate the practical challenges of applying traditional legal frameworks to the rapidly evolving landscape of cyber warfare.

The Rome Statute, which established the International Criminal Court (ICC), primarily focuses on war crimes, crimes against humanity, and genocide. Its language primarily addresses physical harm, destruction, or mistreatment of individuals rather than abstract entities such as data. However, legal interpretations and discussions around the applicability of the Rome Statute to cyber operations have evolved. Civilian data, being an intangible and non-physical entity, doesn't fit neatly into traditional conceptions of "object or property" as understood in the context of the Rome Statute. The Statute, in its provisions on war crimes, typically refers to tangible objects and property, such as buildings, infrastructure, or cultural heritage.

The challenge arises in adapting existing international legal frameworks to the unique aspects of cyber warfare, including attacks on data. While the Rome Statute might not explicitly address the protection of data, legal scholars and policymakers are engaged in discussions about whether the principles of the Statute can be interpreted or amended to encompass these emerging challenges. Some argue that attacks on civilian data can have severe consequences, equivalent to traditional attacks on property, and should be considered within the scope of international humanitarian law. Others believe that a more nuanced approach, possibly involving the development of new legal instruments specifically tailored for cyberspace, may be necessary. In summary, the direct application of the Rome Statute to civilian data is debatable due to its original intent and language. However, there is ongoing discourse within the legal community about the need for updated frameworks to address the unique challenges posed by cyber operations in the modern world.

In conclusion, the article synthesizes its findings and possibly proposes recommendations for enhancing the Rome Statute to better address the legal complexities arising from cyber operations against civilian data. This could involve suggesting amendments to the existing legal framework, advocating for the development of new international agreements, or promoting increased global cooperation to address the challenges posed by cyber warfare in the 21st century.

GİRİŞ

Siber operasyonlar devletler ve devlet dışı silahlı aktörler tarafından silahlı çatışmalarda artan bir şekilde kullanılmaya başlanmıştır. Bu doğrultuda siber operasyonlar Uluslararası Ceza Mahkemesi'nin (UCM) kuruluş belgesi Roma Statüsü'nün nasıl yorumlanması gerektiği konusunda yeni sorular ortaya çıkarmaktadır. Bu makale, silahlı çatışma sırasında verilere yönelik siber operasyonların bir savaş suçu teşkil edip etmeyeceğini değerlendirerek bu konuyu inceleyecektir. Makalenin araştırma konusu doğrultusunda uluslararası insancıl hukukun yorumlanması kritik öneme sahiptir. Bu hukuk sistemine yönelinmesinin nedeni uluslararası insancıl hukuktan doğan ihlallerin UCM Statüsü'nün savaş suçlarına ilişkin 8. Maddesinde, uluslararası ceza hukukuna dahil edilmesidir.

Sivil verilere yönelik siber operasyonlarda uluslararası insancıl hukukun uygulanabilirliği tartışmalıdır. Literatürde verilerin uluslararası insancıl hukukun hedef alma kuralları kapsamında bir nesne olarak değerlendirilmesinin gerekliliği tartışılmıştır. *Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Rehberi 2.0*'da[1] uzmanların çoğu verinin fiziki varlığı bulunmayan, soyut bir kavram olması dolayısıyla uluslararası insancıl hukuk tarafından bağımsız olarak korunan bir nesne olarak kabul edilemeyeceği görüşündedir. Diğer yaklaşım ise nesnenin tanımının veriyi de içerecek şekilde daha geniş yorumlanmasını savunmaktadır.[2] Buna ek olarak, verilere yönelik siber operasyonlar, verilerin mal olarak sınıflandırılmasının kabul edilmesi ve bu temelde korunması durumunda uluslararası insancıl hukuk kapsamına girebilir. Ancak UCM Statüsü'nün 8. Maddesinin doğrudan fiziksel zararın olmadığı durumlarda sivil verilere yönelik siber operasyonları düzenleme kapsamı, Uluslararası Ceza Mahkemesi'nin verileri hangi sınıfa dahil ederek, geliştireceği yorum yaklaşımına bağlı olacaktır.

Verilerin Roma Statüsü'ndeki nesne veyahut mal kategorilerinden hangisine dahil edilmesinin uygun olduğu bu makalede inceleme konusu yapılacaktır. Bu makalenin ilk bölümü, bilgisayar verileri kavramından ne anlaşılması gerektiğini inceleyerek, geleneksel nesne ve mal kavramlarını yeniden yorumlayıp, verilerin hangi kategoriye dahil edilmesinin uygun olduğunu araştırmaktadır. İkinci bölüm ise bilgisayar verilerine karşı veya

[1] Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2. Bası, Cambridge University Press, 2017, s. 437.

[2] Schmitt, *Tallinn Manual,* s. 438.

bilgisayar verileri aracılığıyla gerçekleştirilen farklı siber operasyon türlerine odaklanacaktır. Üçüncü bölüm, doğrudan kinetik etkileri bulunan ve nedensel olarak daha uzak, ölçülmesi zor etkileri olan siber operasyonlara dikkat çekmektedir.

Üçüncü bölüm, sivil bilgisayar verilerine yönelik gerçekleştirilen siber operasyonların hangi durumlarda UCM Statüsü kapsamında savaş suçu teşkil edebileceğini analiz etmektedir ve makalenin özünü oluşturmaktadır. Literatürdeki farklı görüşler değerlendirdikten sonra verilerin, nesne ve mal olarak nitelendirilen donanım, kablo ve bilgisayar çiplerinden oluşan ağların ve sistemlerin ayrılmaz bir parçası olarak anlaşılması gerektiği görüşü bu makalede savunulmaktadır. Yalnızca soyut olan veriler ile bilgisayar verilerini barındıran ve işlevlerini yerine getirmek için bunlara bağımlı olan somut, fiziksel sistemler arasında kesin bir ayrıma gitmek mümkün değildir. Verinin bağımsız bir nesne veya mal türü olarak ele alınmasının mümkün olmadığı kabul edilmelidir. Savaş suçunun kanıtlanabilmesi için, bilgisayar verileri ile korunan nesneler veya mallara yönelik ölçülebilir bir sonuç arasında illiyet bağının kurulması gereklidir.

Makaledeki tartışmaların UCM Statüsünün yorumlanmasına yönelik daha geniş neticelerinin olup olmadığının sorgulanması dördüncü bölümde incelenmektedir. UCM Statüsünün hukuki düzenlemelerin gelişmediği yeni savaş biçimlerine ayak uydurup uyduramayacağı, aynı zamanda kanunilik ilkesine de saygı gösterip gösteremeyeceğinin tartışılması gereklidir. Dördüncü bölümde ayrıca, sadece bilgisayar verilerinin yok edilmesiyle sonuçlanan ve başka hiçbir etkisi olmayan siber operasyonlar hakkında bir davanın UCM nezdinde kabul edilebilirlik için gereken vahamet eşiğini geçip geçemeyeceği de değerlendirilmektedir. Makale, Mahkemenin siber operasyonları incelerken izleyeceği yol ve karşılaşacağı zorluklar üzerine düşünülerek sonlandırılmaktadır.

I. BİLGİSAYAR VERİSİ VE TANIM SORUNU

Bu bölümde veri kavramının anlamı üzerinde durularak, hukuki metinlerde veriye yapılan atıflar incelenecektir. Veri kelime anlamı itibariyle bilgi olarak tanımlanmaktadır. Türk Dil Kurumu veriyi "olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi" olarak belirtmektedir.[3] Dijital haldeki bilgi, teknik olmayan bağlamda veridir. Oxford

[3] Türk Dil Kurumu, "Türk Dil Kurumu Sözlükleri", <https://sozluk.gov.tr/>, Erişim Tarihi 12 Temmuz 2023.

Sözlüğü veriyi toplu olarak değerlendirilen, bilimsel çalışma ile elde edilen ve referans, analiz veya hesaplama için kullanılan çoğunlukla sayısal bilgi öğeleri olarak tanımlar. Bilgi işlemle ilgili olarak ise veri, bir bilgisayar tarafından üzerinde işlem yapılan ve toplu olarak ele alınan nicelikler, karakterler veya sembollerdir.[4] Verilerin hayatımızın neredeyse tüm yönleri için önemi göz önüne alındığında, uluslararası örgütlerin, devletlerin ve mahkemelerin tam olarak verinin tanımı ve nasıl düzenlenmesi gerektiği konularını tartışmaları dikkate değerdir.

Bu makale, elektronik veya dijital yollarla kaydedilen ve bir insan veya makine tarafından algılanabilir olup olmadığına bakılmaksızın geri alınabilen herhangi bir bilgi olarak bilgisayar verilerine odaklanmaktadır.[5] Bu tür verilerin toplanıp toplanmayacağı ve nasıl toplanacağı konularının mevcut hukuk sistemlerinin kapsamında incelenmesi problemlidir. Jennifer Daskal, bilgisayar verilerinin hareketliliği, bölünebilirliği, konumdan bağımsızlığı, iç içe geçmesi ve üçüncü taraf kontrolü nedeniyle siber uzayı yarattığını ve egemenlik kavramını değiştirdiğini savunmaktadır. Bu değişim özellikle egemen devletlerin yetki alanları temelindedir. Bilgisayar verilerinin egemen devletlerin yargılamada yetki sınırlarını nasıl değiştirdiğini göstermek amacı araştırma yapmaya değerdir.[6]

Bilgisayar verileri hareketli ve bölünebilirdir. Hızı ve öngörülemezliği dolayısıyla bilgisayar verileri, hem bir yerden bir yere geçişin ne anlama geldiğini hem de dijital mallarımızı depolamanın ne anlama geldiğini yeniden yorumlamayı gerektirmektedir.[7] E-postalar aynı şehirdeki bir kişiye gönderilebilmektedir. Aynı zamanda e-postalar başka bir ülkedeki kablolar ve sunucular üzerinden seyahat edebilmektedirler. Bulutta depolanan verilerin özelliklerini incelediğimizde; kullanıcının haberi olmadan hareket ettirilip kopyalanabildikleri, bölünebildikleri ve birden fazla yerde depolanabildikleri sonucuna ulaşılmaktadır. Klasik anlamda belgeler de birden fazla kopya halinde bulundurulabilir ve farklı yerlerde saklanabilir ancak dijital çağda depolama anlayışında yaşanan değişimle beraber, verilerin kopyalanması ve taşınması hızlanmış, çok uluslu olan dünyanın farklı bölgelerinde bulunan

[4] Oxford Dictionaries, *Oxford English Dictionary*, Oxford University Press, 2019, s. 803.

[5] Jeffrey Ritter/Anna Mayer, "Regulating Data as Property: A New Construct for Moving Forward", *Duke Law and Technology Review*, 16(1), 2017, s. 224.

[6] Jennifer Daskal, "The Un-Territoriality of Data", *Yale Law Journal,* 125(2), 2015, s. 365.

[7] Daskal, s. 368.

depolama imkanları artmıştır. Veriye erişilen konum ile verinin kendisi arasında Daskal'ın konumdan bağımsızlık olarak adlandırdığı bir kopukluk ortaya çıkmaktadır.[8] Kullanıcının verilerin nerede tutulduğunu bilmesi veya önemsemesi gerekmemektedir. Bu durum aynı zamanda verilerin konumunun bilinmesinin, veri kullanıcısının konumu hakkında bir bilgiyi ortaya çıkarmayacağı anlamına da gelmektedir.

Nesne ve mal ifadelerinin genellikle somut varlıklara atıfta bulunduğu anlaşıldığından, bu ifadelerin bilgisayar verilerini kapsayıp kapsamadığını belirlemek amacıyla, verilerin de somut olup olmadığının değerlendirmesi gerekmektedir. Bilgisayar verileri depolanmalarına ve erişilmelerine olanak tanıyan bilgisayar donanımı içinde gömülüdür. Verilere farklı cihaz formatlarında erişmek mümkündür. Özellikle bir bilgisayar donanımı ancak görevlerini tamamlamak için kullandığı veriler sayesinde işlevseldir. Bu açıdan bakıldığında, veriler fiziksel bir nesnenin parçası olarak düşünülebilir. Verilerin nasıl depolandığına bağlı olarak değişim göstermekle beraber, veriler bir optik diskteki boyalarda, bir mikroçip üzerindeki anahtarların konumunda bulunabilir, manyetik bantlarda tutulabilir veya bir optik kablo aracılığıyla yoğunlaştırılmış atımlı ışık darbeleri yoluyla gönderilebilir. Bu örnek durumların her birinde veri fiziksel bir nesnenin içindedir. Verilerin bir fiziksel depolama biçiminden diğerine taşınabilmesi mümkündür. Ancak verileri değiştirmek, kopyalamak veya silmek için mutlaka donanım ile fiziksel etkileşim gerekmektedir. Bilgisayar verisi kavramında bilgi ve donanımın iç içe geçmesi, hukuki düzenlemelerin kapsamını belirlemeyi özellikle önemli kılmaktadır.

Veri hukuki açıdan tanımlanırken hem bilgiye hem de bu bilgiye erişim ve kullanım sağlayan sisteme atıfta bulunulmaktadır. Avrupa Konseyi Siber Suç Sözleşmesi veri kavramını iki ana eksende değerlendirmektedir. İlk olarak, veri bilgisayar sisteminin işlevlerini yerine getirmesine sağlayan bir programdır. İkinci olarak, bilgisayar sisteminde işlenmeye uygun bir biçime getirilmiş bilgilerin veya kavramların temsilini ifade etmektedir.[9] Bilgisayar sistemleri ise Avrupa Konseyi Siber Suç Sözleşmesi tarafından, yazılım yardımıyla verilerin otomatik olarak işlenmesini gerçekleştiren cihaz veya birbirine bağlı ya da birbiriyle ilgili cihazlar grubu olarak tanımlanmıştır.[10]

[8] Daskal, s. 369.

[9] Madde 1(b), Avrupa Konseyi Siber Suç Sözleşmesi (23 Kasım 2001, ETS No 185).

[10] Madde 1(a), Avrupa Konseyi Siber Suç Sözleşmesi.

Bu tanım, verileri bir bilgisayar tarafından doğrudan işlenebilen elektronik formdaki bir bilgi biçimi olarak tanımlayan Uluslararası Standartlar Teşkilatı'nın çalışmasına dayanmaktadır.[11] Benzer şekilde, *Tallinn Rehberi 2.0* da veriyi, bayt cinsinden ölçülen bilgiyi iletmek için bir bilgisayar tarafından işlenebilen veya üretilebilen temel unsur olarak tanımlamaktadır.[12]

Verilere ilişkin hukuki düzenlemelerin bazıları daha geniş kapsamlıdır ve yalnızca bilgiye odaklanan, teknolojik olarak tarafsız bir veri tanımını benimsemektedirler. Örneğin, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), kişisel verileri "kimliği belirli veya belirlenebilir bir gerçek kişiye ilişkin herhangi bir bilgi" olarak tanımlamaktadır.[13] Avrupa Birliği'nin Genel Veri Koruma Tüzüğü veri tanımı, hem yalnızca internet nedeniyle var olan konum verilerini, IP adreslerini, çerez kimliklerini e-posta adreslerini içermektedir hem de siber alana özgü olmayan bilgiler olan kişilerin adları ve adreslerini de kapsamına almaktadır.[14]

Bilgi olarak değerlendirilen verinin, saklandığı veya erişildiği bilgisayar donanımından ayrı bir varlık olarak ele alınması mümkün olacaktır. Verinin nerede depolandığı, verilere kimlerin erişim hakkının bulunduğu, verilerin kime ait olduğu konularında belirsizlik bulunduğundan; bulutta depolanan veriler, verileri donanımdan ayırmanın neden faydalı olabileceğine iyi bir örnek teşkil edecektir. Örneğin, devletlere ve özel kuruluşlara ait verilerin çoğu Amazon Bulut Bilişim Hizmetleri (Amazon Web Services) gibi şirketler tarafından depolanır. Bu şirketler verilerin depolandığı donanımın bakımını yapar. Aynı zamanda donanımın da sahibidir ancak verilerin kendisine sahip değildirler. Amazon Bulut Bilişim Hizmetleri sunucusuna karşı düzenlenen ve sivil verilere ulaşmayı ya da yok etmeyi başaran bir siber saldırı, verilerin depolanmasını ve geri alınmasını destekleyen fiziksel altyapıyı sağlam bırakabilme potansiyeline sahiptir.

Roma Statüsü'nde ve uluslararası insancıl hukuk belgelerinde bilgisayar verilerine ilişkin bir tanım bulunmamaktadır. Uluslararası insancıl hukuk

[11] Avrupa Konseyi, "Explanatory Report to the Convention on Cybercrime", European Treaty Series - No. 185, 2001, <https://rm.coe.int/16800cce5b>, Erişim Tarihi 12 Temmuz 2023, s. 25.

[12] Schmitt, *Tallinn Manual,* s. 564.

[13] Madde. 4, Regulation (EU) 2016/679 (General Data Protection Regulation).

[14] Avrupa Komisyonu, "What is Personal Data?", <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> Erişim Tarihi 12 Temmuz 2023.

açısından bilgisayar verilerinin fiziksel nesne veya mal olarak yorumlanması gerektiği konusu tartışmalara açıktır. Uluslararası ceza hukuku ve uluslararası insancıl hukukun yeni teknolojilere doğru bir şekilde uygulanabilmesi için, UCM'nin veriler ile verilerin kullanımına imkân veren fiziksel sistemler arasındaki ilişkiyi belirlemesi gerekmektedir. Özellikle verilerin saldırıya uğraması, imha edilmesi, el konulması veya ele geçirilmesi kavramlarının Mahkeme tarafından nasıl yorumlanacağını anlamak önem taşımaktadır.

II. SİLAHLI ÇATIŞMA ESNASINDA VERİLERE YÖNELİK SİBER OPERASYONLAR

Gerçekleşen siber operasyonları tespit etmek ve siber operasyonların hükümetler, şirketler ve bireyler üzerindeki etkisi hakkında bilgi edinmek zordur. Siber operasyonların bir kısmı, kinetik etkiler üreten geleneksel askeri operasyonlarla doğrudan benzerlik gösteren sonuçlar ortaya çıkarmaktadır. Örneğin, solucan bir yazılım olan Stuxnet virüsü İran'ın nükleer tesisindeki santrifüjlerini hedef alarak, nükleer tesisin çalışmasını yöneten kontrol sistemini dijital olarak manipüle ederek yok etmiştir.[15] Santrifüjlerde fiziksel hasar oluştuğundan, operasyon yöntemi yeni olarak nitelendirilse de meydana gelen sonucun yeni olmadığı açıktır. Fiziksel hasarın doğrudan siber operasyondan kaynaklandığı durumdan farklı olarak, eğer bir sistemin işleyişi siber operasyonlarla bozulursa da siber saldırılar zararın ortaya çıkmasına sebebiyet verebilir. Bu konuyu detaylandırmak açısından örneğin, Mayıs 2020 tarihinde İsrail tarafından gerçekleştirilen siber operasyonun sonucu olarak, İran'a ait bir limanın birkaç gün boyunca işlevselliğinin kaybettiği ve taşımacılık sektöründe önemli gecikmelerin meydana geldiği bildirilmiştir. İsrail tarafından gerçekleştirilen siber operasyonun, İran tarafından İsrail su dağıtım tesisinin komuta ve kontrol sistemlerine karşı gerçekleştirilen başarısız siber operasyona misilleme olarak yapıldığı iddia edilmektedir.[16] Siber operasyonların bir kısmı da gözlemlenebilir ancak ölçülmesi zor zararlara yol açmaktadır. Özellikle şirketlerin veya bireylerin devletin kritik hizmetlerine veya kişisel verilere sınırlı bir süre için erişememesi bu konuda en önemli örneklerdir. Bu konuda güncel bir olay olarak, Şubat 2020 tarihinde pek çok ülke Rusya'yı, Gürcistan'a karşı gerçekleştirilen ve neticesinde özel sektöre, devlete ve medya sektörüne ait binlerce web sitesinin çevrimdışı

[15] Samuli Haataja, *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, Routledge, 2018, s. 145.

[16] Sarah Chen, "Conventional Retaliation and Cyber Attacks", *The Cyber Defense Review*, 8(1), 2023, s. 77.

hale getirilmesiyle sonuçlanan bir siber operasyonun yürütücüsü olmakla suçlamıştır.[17]

Tüm siber operasyonlar gibi, yukarıda açıklanan örnek olaylar da veriler aracılığıyla veya verilere karşı yapılan siber operasyonları temsil etmektedirler. Siber operasyonlarda bilgisayar ağları, sistemlerin kontrol verilerini ve yazılımlarını manipüle ederek düzgün çalışmalarını engellemek için kullanılmaktadırlar. Bununla birlikte, bu makalede belirtilen siber operasyon örnekleri verinin kendisine yönelik saldırılar değildir. Daha geniş anlamda siber operasyonların sisteme yönelik saldırılar olarak kabulü uygun olacaktır. Stuxnet operasyonu santrifüjlere siber yollarla yapılan kinetik bir saldırı olarak görülebilir. Stuxnet siber operasyonu neticesinde İran'a ait limanda işlemlerin kesintiye uğraması, fiziksel sonuçları nedeniyle limana yönelik bir saldırı olarak anlaşılabilir. Gürcistan siber altyapısına yönelik saldırı ise işlettikleri sistemler dolayısıyla özel sektöre ve devlet kurumlarına yönelik bir saldırı olarak görülebilir.

Uluslararası insancıl hukuk literatüründe bazı yazarlar tarafından siber operasyonlar silahlı çatışma bağlamında değerlendirilirken muhafazakâr bir yaklaşım tercih edilmektedir. Bu doğrultuda, siber operasyonlarda sistem üzerinde ölçülebilir bir kinetik etki gerekliliği arandığından[18], bu kriteri sadece Stuxnet örneği sağlamaktadır. Ancak bu yaklaşımı tercih etmek, uluslararası insancıl hukukun sivillere ve sivillerin bilgisayar ağlarını kullanımına koruma sağlamadığını göstermektedir ve çağdaş silahlı çatışmaların gerekliliklerini reddetmektir.

Uluslararası insancıl hukuk silahlı çatışmalarda geçerli olan tek hukuk sistemi olmasa da, savaş suçlarını oluşturan kriterler karşıladığında, bireysel cezai sorumluluk gerektiren düşmanca eylemlerin ve ihlallerin idaresini düzenleyen hukuk sistemidir. Siber operasyonların sebebiyet verebileceği potansiyel insani zararlar korumadaki bu boşluğu önemli hale getirmektedir.[19] Veri, dijital dünyanın temel bir bileşenidir, aynı zamanda birçok toplumda yaşamın temel taşıdır ve çoğu sivil yaşamın işleyişi için kilit

[17] Jonathan Lancelot, "Cyber-diplomacy: Cyberwarfare and the Rules of Engagement", *Journal of Cyber Security Technology*, 4(4), 2020, s. 249.

[18] Schmitt, *Tallinn Manual,* s. 415.

[19] International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper", *International Review of the Red Cross*, 102(913), 2020, s. 484.

öneme sahiptir.[20] Yaşanan güven neticesinde bilgi ve iletişim teknolojileri toplumun her katmanına sızmıştır. Bu doğrultuda gerçek dünyadaki hedefler bozulmaktadırlar, değişime uğramaktadırlar ve meydana gelebilecek zararlara karşı savunmasızlıkları artmaktadır.[21] Siber operasyonlar tüm endüstrileri kapsayabilir. Özellikle altyapılar, telekomünikasyon, ulaşım, hükümet ve finans sistemleri, kritik sivil altyapı üzerinde siber operasyonlar yıkıcı etkilere sahip olabilmektedir. Sağlık sektörü, elektrik, su dağıtım sistemleri dahil olmak üzere bazı alanlar özellikle savunmasızdır.[22] Örneğin, Şubat 2021 tarihinde bilgisayar korsanları, Florida'nın Oldsmar kasabasına hizmet veren su arıtma tesisini yöneten yazılım programına başarıyla uzaktan erişim sağlamıştır. Bilgisayar korsanları sudaki sodyum hidroksit miktarını tehlikeli seviyelere çıkarmaya çalışmışlardır, ancak saldırı şans eseri değişiklikler yürürlüğe girmeden önce tespit edilip sonlandırılmıştır.[23]

A. Verilere Yönelik Siber Operasyonlar Ne Zaman Roma Statüsü Kapsamında Savaş Suçu Oluşturur?

İnternetin yaygınlaşması ile beraber Roma Statüsü'nde yer alan birçok suç çevrimiçi olarak işlenebilmektedir. Örneğin, soykırıma teşvik suçu sosyal medya aracılığıyla işlenebilir.[24] Özellikle verilere yönelik siber operasyonlar bazı durumlarda Roma Statüsü'nde tanımlandığı üzere savaş suçu anlamına gelebilir. Nesne kelimesi suç tanımının bir parçası olarak birkaç kez Roma Statüsü'nde geçmektedir.[25] Veriler nesne kategorisi altında yorumlanabilir

[20] Laurent Gisel/Tilman Rodenhauser/Knut Dorrmann, "Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflict", *International Review of the Red Cross*, 102(913), 2020, s. 317.

[21] Eitan Diamond, "Applying International Humanitarian Law to Cyber Warfare", *Law and National Security*, 67(1), 2014, s. 67.

[22] Samuli Haataja, "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law", *International Journal of Law and Information Technology*, 30(4), 2022, s. 426.

[23] Frances Robles, "Hackers Target Florida's Town Water Supply, Raising Level of Harmful Chemical", *The New York Times*, 2021, <https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html>, Erişim Tarihi 09 Temmuz 2023.

[24] Neema Hakim, "How Social Media Companies Could Be Complicit in Incitement to Genocide", *Chicago Journal of International Law*, 21(1), 2020, s. 83.

[25] Roma Statüsü Madde 8(2)(b)(ii): "Askeri olmayan, yani askeri maksatlı olmayan sivil hedeflere karşı kasten saldırı düzenlenmesi." Roma Statüsü Madde 8(2)(b)(iv): "Tahmin edilen somut ve doğrudan askeri avantajlara kıyasla, aşırı olacak şekilde, sivillerin yaralanmasına veya ölmesine veya sivil nesnelerin zarar görmesine yol açacağı ve geniş çapta, uzun vadeli ve ağır bir biçimde doğal çevreye zarar vereceğinin bilincinde olarak

veya veri bir nesnenin içine gömülü olarak düşünülebilir. Netice itibariyle veriye yönelik bir işlem aynı zamanda nesneye yönelik bir işlemdir. Roma Statüsü'nde çeşitli savaş suçu hükümleri mallara atıfta bulunmaktadır.[26] Veri ya da içine gömülü olduğu sistem mal olarak nitelendirilebilir.

Doğru bir analiz için Roma Statüsü hükümlerinin yanı sıra savaş suçlarına karşılık gelen uluslararası insancıl hukuk hükümlerinde yer alan nesne ve mal tanımları incelenmelidir. Bu iki ifade arasındaki ilişki net değildir. Roma Statüsü Madde 8(2)(b)(ii)'de yer alan askeri hedef olmayan nesneler ifadesi tüm sivil malları kapsıyor olabilir veya daha dar bir materyal kapsamı koruyor olabilir. Ancak, nesne ve mal tanımlarını irdelemeden önce, uluslararası insancıl hukuk ve savaş suçlarının amaçları açısından öneme sahip olan saldırı kavramının, yani hem hücum hem de savunma niteliğine sahip, düşmana karşı yöneltilen şiddet eylemlerinin neleri kapsadığına dair bazı tartışmalar olduğunu belirtmek gerekmektedir.[27] Şiddet eylemlerinin tam olarak ne olduğu ve saldırı niteliği taşıyan siber operasyonların saldırı niteliğine sahip olmayan siber operasyonlardan nasıl ayırt edilebileceği belirsizdir.[28] Ayrıca, uluslararası insancıl hukuk açısından saldırılar silahlı çatışma bağlamında gerçekleştiğinden, saldırıların gerçekleşmesi için düşmanca eylemlerin ne zaman ve nerede gerçekleşmesi gerektiği ve saldırıların belirli bir amaç doğrultusunda yapılmasının gerekip gerekmediği konusunda da tartışmalar bulunmaktadır.[29]

Siber saldırılarda saldırı kavramı konusunda devam eden tartışmaların tam bir analizi bu makalenin kapsamı dışında olmakla birlikte, ortaya konulan argümanlar dikkate değerdir. Eğer veri fiziksel nesnelere gömülü ve onların

saldırı başlatılması." *Rome Statute of the International Criminal Court* (entered into force 1 July 2002) 37 ILM 1002 (1998); 2187 UNTS 90.

[26] Roma Statüsü Madde 8(2)(a)(iv): "Askeri gereklilik olmadan, yasadışı ve keyfi olarak malların yaygın yok edilmesi veya sahiplenilmesi." Roma Statüsü Madde 8(2)(b)(xiii): "Savaşa dair ihtiyaçlar zorunlu olarak gerektirmedikçe, düşman mallarının imha edilmesi veya bu mallara el konulması." *Rome Statute of the International Criminal Court* (entered into force 1 July 2002) 37 ILM 1002 (1998); 2187 UNTS 90.

[27] Yunus Emre Gül, "War Crimes and Individual Criminal Responsibility Arising out of Cyber Operations", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 26(2), 2020, s. 1067.

[28] Michael Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations", *International Review of the Red Cross*, 101(910), 2019, s. 339.

[29] Mike Newton, "A Radical Reimagining of the Concept of Attack", *Articles of War*, 2020, <https://lieber.westpoint.edu/radicalreimagining-attack-ntaganda/>, Erişim Tarihi 09 Temmuz 2023.

bir parçası olarak görülürse; verilerin imhası, silinmesi, el konulması aynı zamanda fiziksel nesnenin bir kısmının imhası, silinmesi, el konulması anlamına gelecektir. Bu doğrultuda, somut nesnelere doğrudan fiziksel zarar vermekle sonuçlanan ve verilere yönelik saldırı anlamına gelmekte olan siber operasyonlar uluslararası insancıl hukuka tabi olmalıdır.[30] Ancak doğrudan somut sonuçları olmadığında, siber operasyonları saldırı olarak sınıflandırmak sorunludur. Sorunu netleştirmek gerekirse; bir bilgisayar sisteminin bozulmasına veya doğrudan fiziksel sonuçlara yol açmayan bilgilere erişimin geçici veya kalıcı olarak kaybedilmesine neden olan siber operasyonların bir nesneye saldırmak veya bir malı imha etmek, el koymak veya ele geçirmek olarak değerlendirilip değerlendirilemeyeceğinin belirlenmesi önemlidir. Makalenin bir sonraki bölümünde bu sorular yanıtlanmaya çalışılacaktır.

B. Veriler Nesne Olarak Kabul Edilebilir mi?

Temel sorun verilerin nesne olarak nitelendirilip uluslararası insancıl hukuk ve Roma Statüsü'ndeki savaş suçları açısından koruma altına alınmasının gerekliliğidir. Akademik tartışmaların yanı sıra, devletlerin verilerin nasıl kategorize edilmesi gerektiğine ilişkin kamuoyu yorumları sınırlı ve tutarsızdır. Yalnızca fiziksel bir sivil nesneye kinetik zarar veren siber operasyonlar suç için gerekli maddi unsurları karşılayabilir. Bu yaklaşım, sadece sistemin işleyişini bozan ancak daha sonra eski haline geri döndürülebilir operasyonları hariç tutmaktadır. Bu durumda, ilgili nesne veri değil, fiziksel olarak zarar gören somut öğedir. Daha farklı bir yaklaşımla, veriler fiziksel bilgisayar sistemlerinin içine gömülü ve bu sistemlerin ayrılmaz bir parçası olarak kabul edilebilir. Böylelikle verilere yapılan ve sistemin işlevselliğini azaltan bir saldırı, bu sisteme yapılmış bir saldırı olarak değerlendirilebilir. Ayıca verinin kendisi yok edilebilecek ya da kullanımı engellenerek saldırılabilecek bir nesne olarak da değerlendirilebilir. Bütün olasılıklar bu bölümde değerlendirilecektir.

Savaş suçları, askeri hedef olmayan nesneler olarak tanımlanan sivil nesneleri korumayı amaçlamaktadır. Roma Statüsü ve suçun unsurları bu kavramların anlamlarına açıklık getirmemektedir. Uluslararası insancıl hukuk açısından özel bir anlama sahip olan sivil hedef ve askeri hedef kavramlarını incelemek için uluslararası insancıl hukuk andlaşma ve örf ve âdet hukukuna atıfta bulunmak gerekmektedir.[31]

[30] Schmitt, *Tallinn Manual,* s. 417.

[31] Knut Dorrmann, "Article 8 Para 2: Meaning of War Crimes", Kai Ambos (Ed.), *Rome Statute*

Cenevre Sözleşmelerine Ek Protokol I'in 52. Maddesi, örf ve âdet hukuku olarak kabul edilmektedir.[32] 52. Madde saldırıların askeri hedeflerle sınırlı olması gerektiğini öngörmektedir.[33] Bugüne kadar gerçekleştirilen tartışmaların ana ekseni, nesnelerin somut olmasının gerekip gerekmediği üzerinedir.[34] Uluslararası Kızılhaç Komitesi'nin Cenevre Sözleşmelerine ilişkin şerhi internetin yaygınlaşmasından önce hazırlanmıştır. Bu yüzden nesnelerin maddi ve somut şeylerle sınırlı olduğunu öne sürmektedir.[35] Şerh analog bir savaş fikri doğrultusunda oluşturulduğundan, bilgisayar kavramı sadece iki noktada ve nispeten önemsiz bir şekilde belirtilmiştir. Şerhin yazarları, silahlı çatışma durumunda uygulanabilecek tüm uluslararası hukuk hükümlerinin bir bilgisayarın hafızasında saklanmasının o zamanlar için yeni bir olasılık olduğunu vurgulamaktadırlar. Şerhin yazarları, Ek Protokol I Ek I kapsamında kimlik kartları için gereklilikleri tartışırken, bilgisayar bilimindeki mevcut gelişmeler ışığında elektronik bir kimlik kartın üretilebilme olasılığını reddetmektedirler.[36] *Siber Savaşa Uygulanacak Uluslararası Hukuk Hakkında Tallinn Rehberi 2.0* ise askeri hedeflerin ve dolayısıyla nesnelerin bilgisayarları, bilgisayar ağlarını ve siber altyapıyı içerebileceği, ancak bilgisayar verilerinin kendisini içermeyeceği sonucuna ulaşmıştır.[37]

Devletlerin verilerin statüsünün belirlenmesi problemine ilişkin görüşleri tutarsızdır. İsrail, somut varlığın bulunması gerekliliği şartı olduğu

of the International Criminal Court: A Commentary, Nomos, 2016, s. 355.

[32] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict,* 3. Bası, Cambridge University Press, 2016, s. 105.

[33] Cenevre Sözleşmelerine Ek Protokol I'in 52. Madde metni: "Saldırılar sadece askeri hedeflerle sınırlı olacaktır. Mallar söz konusu olduğunda askeri hedefler, doğaları, konumları, amaçları ya da kullanımları gereği askeri eylemlere etkin bir katkıda bulunan ve tamamen ya da kısmen yok edilmesi, ele geçirilmesi ya da etkisiz hale getirilmesi durumunda, mevcut koşullar altında, kesin bir askeri avantaj sağlayan objelerle sınırlıdır." *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3.

[34] International Law Association Study Group on the Conduct of Hostilities in the 21st Century, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", *International Law Studies*, 93(1), 2017, s. 338.

[35] Yves Sandoz/Christophe Swinarski/Bruno Zimmerman, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, International Committee of the Red Cross, 1987.

[36] Kubo Macak, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, 48(1), 2015, s. 67.

[37] *Tallinn Rehberi 2.0*, Kural 38.

gerekçesiyle verileri nesne kategorisinin dışında tutmaktadır.[38] Fransa ise dijital bağımlılığın artması dolayısıyla verileri nesne tanımından hariç tutmanın uluslararası insancıl hukukun amacına ve hedefine aykırı olacağını belirtmektedir. Sivil veriler maddi olmamasına rağmen uluslararası insancıl hukuk kapsamında korunan bir nesne olduğunun kabulü gerekmektedir.[39] Benzer bir yaklaşımla Norveç askeri talimatnamesi de verilerin bir nesne olarak sınıflandırılabileceğinim kabul etmektedir. Askeri veriler gibi hukuka uygun hedefler olduğu sürece, Norveç askeri talimatnamesi verilere doğrudan saldırı yapılabileceğini kabul etmektedir.[40]

Diğer devletlerin yaklaşımlarında ise belirsizlik ortaya çıkmaktadır. Danimarka askeri talimatnamesi, uluslararası insancıl hukuk kapsamında verileri nesne olarak nitelendirmemektedir. Ancak istisnai olarak veriler zarar görür veya silinir ise siviller üzerinde fiziksel bir nesneye verilen zararla aynı etkiye sahip olacaktır. Bu kapsamda, Danimarka Silahlı Kuvvetleri yeri doldurulamaz veriler üzerinde meydan gelen hasarı tali hasar olarak kabul etmektedir.[41] Peru ve Şili devletleri askeri bir amaç taşımadığı sürece verilerin korunması gerekliliğine vurgu yapmaktadır.[42] Guyana ise siber operasyonların etkilerine odaklanmaktadır. Bu doğrultuda verilerin silinmesi, gizlenmesi ve bozulmasının kapsamlı sonuçlar ortaya çıkarabileceğine dikkat çekmektedir.[43] Avustralya devleti verilerin uluslararası insancıl hukuk tarafından korunması gerektiği görüşünü dışlamamakla birlikte, somut etkilerin oluşması şartını öne sürmektedir. Uluslararası insancıl hukuk kapsamında siber operasyon, kinetik bir saldırı ile aynı eşiğe ulaşır ise somut etki ortaya çıkmaktadır. Somut etki var ise silahlı çatışma sırasında saldırıları düzenleyen kurallar siber operasyona da

[38] Roy Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, 97(1), 2021, s. 401.

[39] Jean Drian, *Stratégie Internationale de la France Pour le Numérique*, Ministre de l'Europe et des Affaires Etrangères, 2017.

[40] Norwegian Chief of Defence, *Manual on the Law of Armed Conflict*, Department of Security Policy at The Norwegian Ministry of Defence, 2013, s. 210.

[41] Peter Bartram/Jes Knudsen, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Danish Ministry of Defence, 2016.

[42] Gisel/Rodenhauser/Dorrmann, s. 320

[43] Organisation of American States, *Improving Transparency: International Law and State Cyber Operations, Fifth Report, Presented by Professor Duncan B. Hollis ('Hollis Report')*, OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 Ağustos 2020, para. 36.

uygulanacaktır.[44] İran devleti siber operasyonların, mallara veya kişilere maddi zarar verdiği durumlarda kuvvet kullanma teşkil edeceğini belirtmektedir.[45] ABD Dışişleri Bakanlığı Hukuk Danışmanı siber operasyon bir saldırı teşkil ettiği sürece, verilerin uluslararası insancıl hukukun amaç ve hedefleri doğrultusunda nesne olarak kabul edilmesi gerektiğini öne sürmektedir.[46]

Çek Cumhuriyeti verilerin uluslararası insancıl hukuk tarafından korunan nesneler arasında yer alıp almadığı tartışmasında görüş bildirmemektedir. Sadece uluslararası hukukun siber operasyonlara uygulanması gerektiğini belirtmektedir. Çek Cumhuriyeti siber operasyonun ulusal güvenlik, ekonomi, kamu sağlığı, çevre üzerinde önemli bir etkiye sahip altyapılara zarar vermesi, bozması durumunda veya siber operasyonun hükümet işlevlerinin yerine getirilmesi için gerekli olan veri ya da hizmetlere müdahale etmesi sonucunda işlevlerin yerine getirilmesini önemli ölçüde engellenmesi halinde bir devletin egemenliğinin ihlal edileceğini belirmektedir.[47] Bankacılık sistemine yapılan saldırı ile emekli maaşlarının ödenmesinde önemli ölçüde gecikmelere sebebiyet veren bir siber operasyon bu konuda dikkate değer bir örnektir. Bu örnek açısından operasyondan etkilenen verilerin uluslararası insancıl hukuk kapsamında korunan bir nesne kabul edilip edilmeyeceği net değildir. Yeni Zelanda da veriler konusunda görüşünü belirtmemekle birlikte, uluslararası hukukun maddi olmayan, sanal bileşenleri de kapsayacak şekilde siber uzaydaki tüm devlet faaliyetleri için geçerli olduğunu belirtmektedir.[48]

[44] Commonwealth of Australia, *Australia's International Cyber Engagement Strategy*, Department of Foreign Affairs and Trade, 2017.

[45] The General Staff of the Iranian Armed Forces, "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace", 2020, <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>, Erişim Tarihi 10 Temmuz 2023.

[46] Brian Egan, "International Law, and Stability in Cyberspace", *The Berkeley Journal of International Law*, 35(1), 2017, s. 173.

[47] Richard Kadlcak, "Statement by Richard Kadlcak at the 2nd Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the General Assembly of the United Nations", 2020, <https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>, Erişim Tarihi 12 Temmuz 2023.

[48] New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace*, Department of the Prime Minister and Cabinet, 2020.

Estonya,[49] Finlandiya,[50] Hollanda[51] ve Birleşik Krallık[52] uluslararası insancıl hukuk sisteminin veriler için koruma sağladığı tartışmasında taraf belirtmeden sadece uluslararası hukukun siber operasyonlar için uygulanması gerekliliğini belirtmektedirler.

Uluslararası Kızılhaç Komitesi sivil verilerin sivil nesneler kapsamında değerlendirilmesinin gerekli olup olmadığı sorununun henüz çözülmemiş olduğunu kabul etmektedir ve daha geniş yorum metodunu tercih etmektedir. Uluslararası Kızılhaç Komitesi uluslararası insancıl hukukun amaç ve hedeflerini doğrultusunda, siber operasyonlar eğer devlet hizmetlerini ve özel sektörün faaliyetlerini durdurmayı amaçlıyorsa ve sivillerin zarar görme riski reddedilemezse; bu durumda, verilerin nesne kategorisine dahil olması gerektiği görüşündedir.[53]

Doktrindeki veriye ilişkin görüşleri incelediğimizde, Schmitt veriyi nesne kategorisinin dışında tutan daha dar yorumu tercih etmektedir. Psikolojik harekât metodu olarak verilerin yok edilmesi veya değiştirilmesi kabul edilebilirse de, Schmitt, verileri bir nesne olarak değerlendirmenin aşırı genişletici bir yorum metodu olduğunu açıklamaktadır. Ordular günümüzde düşman olarak kabul edilen hükümetlere ya da politikalarına verilen halk desteğini en aza indirmek için bilgi harekatları yürütmektedirler. Siber araçlarla yürütülmekte olan bilgi harekatları neticesinde sivil medyanın faaliyetleri dijital yıkıma, değişime uğratılmaktadır. Bilgi harekatları verilerin yok edilmesi ve değiştirilmesini de içermektedir.[54]

Nesne kelimesi anlam bakımından genel ve geniş bir kategoriyi ifade etmektedir ve yeni nesne biçimlerini içerecek şekilde değişime uğrayabilir. Macak, günümüz koşulları ışığında yorumlandığında, özellikle uzun bir

[49] Kersti Kaljulaid, *President of the Republic at the Opening of CyCon 2019*, Estonian Ministry for Foreign Affairs, 2019.

[50] Marja Lehto, *International Law and Cyberspace: Finland's National Positions*, Finnish Ministry for Foreign Affairs, 2020.

[51] Dutch Minister of Foreign Affairs, *Letter for the Parliament on the International Legal Order in Cyberspace — Appendix: International Law in Cyberspace*, Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, 2019.

[52] Jeremy Wright, *Cyber and International Law in the 21st Century*, Attorney General's Office, 2018.

[53] International Committee of the Red Cross, Cyber Operations during Armed Conflicts, s. 8.

[54] Schmitt, Wired Warfare, s. 342.

süre önce akdedilmiş bir andlaşma olan Cenevre Sözleşmeleri'nin somutluk gerektirmediğini savunmaktadır.[55] Farklı dillerde verinin nasıl yorumlandığı açısından, Cenevre Sözleşmelerine Ek Protokol I'in Fransızca ve İspanyolca metinleri incelendiğinde nesne için gerçek dünyada fiziksel varlığı olan, nesnelerle sınırlı olmayan ve dolayısıyla somutluk gerektirmeyen bir kelime olan *bien* kullanılmaktadır.[56] Nesne kelimesi Türk Dil Kurumu tarafından belli bir ağırlığı ve hacmi, rengi olan her türlü cansız varlık, şey, obje olarak tanımlanmaktadır ve somutluk gerektirmektedir.[57] Veriler imha edilebilir, ele geçirilebilir veya el konulabilir. Aslında, veriler toplumun moral düzeyi gibi soyut kavramlardan çok köprüler gibi somut nesnelere benzemektedir. Moral düzeyi saldırılardan etkilenebilir fakat varlığı ya da kapsamı nesnel olarak belirlenemeyen öznel bir kategoridir. Öte yandan bir köprü zarar görmeden mevcudiyetini sürdürebilir, hasara uğrayabilir, tamamen yok edilebilir. Köprünün varlığı ve durumu öznel bir değerlendirmeye bağlı değildir. Teleolojik yorum metodundan hareketle, verilerin nesne kapsamında değerlendirilmesi sivillere daha iyi koruma sağlayacaktır ve uluslararası insancıl hukukun amaç ve hedeflerini daha iyi yansıtma potansiyeline sahip olacaktır.[58] Sivil nesnelerin dar tanımının tercih edilmesi, uluslararası insancıl hukuk kapsamında önemli bir koruma boşluğunu ortaya çıkaracaktır. Dar tanımın tercih edilmesi durumunda; siber operatörlerin, orantısız saldırılarda bulunmadıklarından emin olmak için yapmaları gereken hesaplamalarda sivil verilerin imhasını göz ardı etmeleri gerekecektir.[59] *Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Rehberi* 2.0'da azınlık bir görüşü temsil eden uzman grubu, çoğunluğun pozisyonunun kapsayıcı olduğunu belirtmektedir. Sosyal güvenlik verileri, vergi kayıtları ve banka hesapları gibi temel sivil veri kümelerinin silinmesi potansiyel olarak silahlı çatışma hukukunun düzenleyici kapsamı dışında kalacaktır. Bu durumda, sivil halkın düşmanca eylemlerin etkilerinden genel olarak korunması gerekliliği ilkesine aykırı bir

[55] Macak, s. 71.

[56] Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, 48(1), 2015, s. 43.

[57] Türk Dil Kurumu, "Türk Dil Kurumu Sözlükleri", <https://sozluk.gov.tr/>, Erişim Tarihi 12 Temmuz 2023.

[58] Laurent Gisel/Tilman Rodenhauser, "Cyber Operations and International Humanitarian Law: Five Key Points", 2019, *Humanitarian Law & Policy,* <https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/>, Erişim Tarihi 12 Temmuz 2023.

[59] Jonathan Horowitz, "Cyber Operations under International Humanitarian Law: Perspectives from the ICRC", *ASIL Insights*, 24(11), 2020, s. 2.

durum ortaya çıkacaktır.[60]

Verilerin nesne kategorisinden çıkarılması durumunda, fiziksel eşdeğerleri uluslararası insancıl hukuk tarafından sıkı bir şekilde korunan birçok hedef, saldırının etkileri siber uzayda kaldığı sürece meşru bir hedef olarak kabul edilebilecektir.[61] Siber operasyonlar sivil ağları, sistemleri ve altyapıyı hedef almak için tercih edilen bir saldırı metodu olduğundan, verilerin nesne kategorisinin dışında tutulmasının sonuçları önem kazanmaktadır.[62] Verilerin yok edilmesi sistemin işleyişine müdahale etmemektedir. Aynı zamanda sistemin fiziksel olarak yeniden inşası gerekli değildir. Ancak bu durumlarda bile zararlı sonuçlar ortaya çıkacaktır. Silahlı çatışma hukukundaki hedefleme kurallarının amaçları doğrultusunda, nesnenin maddi bir varlığa sahip olmasının zaruriyeti tekrar değerlendirilmelidir.[63]

Verilere yönelik tüm siber operasyonlar bir nesneye saldırı anlamına gelmeyecektir. Gerekli zarar yoğunluğunu belirli nesne türlerinin zarar görmeye uygunluğu doğrultusunda ayırmak gerekmektedir. Bu nedenle, tüm veriler zarar görmeye uygun olsa da, verilere yapılan her müdahale yeterli yoğunlukta zarar anlamına gelmeyecektir. Verilerin kötüye kullanılması veya suistimal edilmesi zarar oluşturmayabilirken, verilerin silinmesi veya değiştirilmesi zararın oluşmasına sebebiyet verecektir. Zararın vahamet eşiğini aşıp aşmadığını değerlendirmek zorluklar içermektedir. Verileri tamamen yok etmek yerine, veri bütünlüğünü ortadan kaldırmak ya da parçalara ayırmak taktiksel açıdan daha mantıklı olabilir. Ayrıca veriler kalıcı olarak silinmeyebilir ve bazı durumlarda sabit sürücüden kurtarılabilir. Veriler zarar eşiğine ulaşmayacak düzeyde müdahalelere açıktır. Bu durumda, verilerin zarar görmeyeceği anlamına ulaşmak doğru değildir. Veriler tahribata açıktır ve bu tahribat nesnel olarak doğrulanabilir.[64]

Harrison Dinniss nesne tanımını dar bir şekilde yorumlamaktadır. Dinniss verilerin niteliklerine göre ikili bir ayrıma gitmektedir. İçerik düzeyindeki verilerin kapsamına araştırma makalelerinin metni, tıbbi veri tabanları,

[60] Schmitt, *Tallinn Manual,* s. 437.

[61] Macak, s. 78.

[62] Cordula Droege, "Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross*, 94(886), 2012, s. 561.

[63] Rain Liivoja/Tim McCormack, "Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello", *Yearbook of International Humanitarian Law*, 15(1), 2012, s. 53.

[64] Macak, s. 74.

kütüphane katalogları ve benzerleri girmektedir. Koruma sağlanması gereken veriler ise uluslararası insancıl hukuk açısından özel koruyucu hükümlere sahip olan sağlık kayıtları ve kültürel varlıklar olacaktır.[65] Operasyonel düzeydeki veriler ise program verileridir, yani donanıma işlevselliğini ve ihtiyaç duyduğumuz görevleri yerine getirme yeteneğini veren veri türleridir. Bu ikili ayrıma gidilmesinin nedeni verilere verilen zararın farklı türlerde olmasıdır. Operasyonel düzeydeki verilerin veya kodların imha edilmesi durumunda sistem işlevselliğini tamamen kaybetmektedir. İçerik düzeyindeki verilerin imha edilmesi durumunda ise bozuk veya eksik verilerle de olsa sistem sağlam kalacaktır.[66]

Siber operasyonlarda verilerin hedef alınması ile ilgili çok az devlet uygulaması olduğu açıktır. Devletlerin düşük seviyeli siber operasyonlar yürütmesi olasılığında, içerik düzeyindeki verilerin kaybı, sistemin işlevinin durmasıyla sonuçlanan operasyonel düzeydeki verilere ilişkin işlemlerden farklı şekilde ele alınmalıdır. Bu nedenlerle iki veri türünü ayrı ayrı ele almak doğru bir yaklaşım olacaktır.

Verilerin hedef alındığı siber saldırıların nesnelere yönelik saldırı olarak nitelendirilebilmesi için zarar temelli yaklaşımların varlığına rağmen, amaç ve hedefe uygunluk gibi oldukça genel bir iddianın ötesinde hukuki bir gerekçe bulamamaktadır. Verilerin nesne kategorisine dahil edilmesini destekleyen bir devlet uygulaması ve *opinio juris* eksikliği olduğu kabul edilmelidir.[67] Bu durum değişene kadar, *Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Rehberi 2.0*'da kabul edilen yaklaşımın esas alınması doğru olacaktır.

C. Siber Saldırı Altındaki Nesneyi Nitelendirmenin Önemi

Savaş suçlarının meydana gelebilmesi için nesnelere yönelik bir saldırının bulunması gerekmektedir. Bu gerekçeyle, hangi nesnenin saldırı altında olduğunu belirlemek önem kazanmaktadır. Veri saldırı altında bulunan ilgili nesne değilse, verilerin statüsü hukukun nasıl uygulanacağı konusunda belirleyici olmayacaktır. Literatürde farklı yaklaşımlar bulunmasının nedeni, saldırı altında bulunan nesnenin nasıl tespit edileceğine dair farklı yorumlardan kaynaklanmaktadır.

Veriler sistemlere, nesnelere gömülü olarak bulunabileceğinden

[65] Dinniss, s. 41.

[66] Dinniss, s. 42.

[67] Schmitt, Wired Warfare, s. 342.

verinin soyut bir nesne olarak kabulü her zaman doğru bir yaklaşım olmayacaktır. Soyutlama riski, verilerin neden bir nesne olarak düşünülmesi ya da düşünülmemesi gerektiğini gösteren olasılıkların oluşturulmasının ana nedenidir. Silah kayıtları ve hava trafik kontrol bilgileri gibi önemli askeri veriler, askeri nesne olarak sınıflandırılabilir.

Sivil hastane verileri tartışılması gereken bir diğer önemli noktadır. Sivil hastane verileri gizlice silinir ya da değiştirilirse, hastaların yaşamları ve sağlıkları tehlike altında olacaktır. Sivil hastane verileri askeri hedef kriterine uymamaktadır. Sivil hastane verilerinin hedef alınarak yok edilmesi sivil nesneler olan verilerin bütünlüğünü bozacaktır. Sivil hastane verilerine yönelik bir saldırı, sivil nüfus olarak hastanede bulunan hastaların güvenliğini de etkileme potansiyeline sahiptir.

Hastane verilerinin siber saldırılarda hedef alınması hastalara yönelik potansiyel öngörülebilir zararın varlığı nedeniyle, verilerin hedeflenmesinden bağımsız olarak hastaneye yönelik bir saldırı olarak da kabul edilebilir.[68]

Hastane verilerine yönelik siber operasyonlar, tıbbi tesis ve hizmetlerin uluslararası insancıl hukuk kapsamında özel olarak korunması ve bu tür operasyonların hastalar üzerinde yaratabileceği dijital olmayan etkiler nedeniyle hukuka aykırı olacaktır. Savaşan taraflar, tıbbi tesislere ve personele her zaman saygı göstermeli ve korumalıdır.[69] Savaşan tarafların sivil nüfusun hayatta kalması için vazgeçilmez olan nesneleri koruma yükümlülüğü de bulunmaktadır.[70] Bu yükümlülükler saldırı anlamına gelen operasyonlardan daha fazlasını kapsamaktadır. Tıbbi personele ve tesislere herhangi bir şekilde zarar vermek yasaktır. Bu kapsamda, tıbbi malzemelerin geçmesi engellenmemelidir veya bakım altındaki yaralı ve hastalara tedavi vermeye devam etme olasılığı engellenerek tıbbi personelin çalışmalarına müdahale

[68] Michael Schmitt, "The Notion of Objects during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review*, 48(1), 2015, s. 81-109.

[69] Jean Henckaerts/Louise Beck, *Customary International Humanitarian Law Vol I*, Cambridge University Press, 2005, Kural 25, 28, 29.

[70] Art. 19 Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949 (GC I); Art. 12 Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949 (GC II); Art. 18 Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949 (GC IV); Art. 12 AP I; Art. 11 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), 8 June 1977.

edilmemelidir.[71] Uluslararası Hukuk Derneği verilerin nesne olarak korunması gerekliliği konusunda fikir birliğine ulaşamamıştır. Tıbbi birimler, kültürel varlıklar, su sistemleri gibi belirli nesne kategorilerinin kendilerine ait verileri de kapsayacak şekilde yorumlanması gerekmektedir. Bu kapsamda yer alan verilerin silinmesine, zarar görmesine, manipüle edilmesine veya gizlice müdahale edilmesine yönelik işlemlerin yasak olması gerekliliği konusunda fikir birliğine ulaşılmıştır.[72]

Verileri depo eden sistemleri fiziksel zarara uğratan siber operasyonlar ile verileri depolayan sisteme zarar vermeyen ancak ikinci dereceden maddi veya fiziksel etkilere neden olan siber operasyonlar farklı değerlendirilmelidir. Siber operasyon ile doğrudan fiziksel bir zararın oluşmadığı zarar kavramı arasındaki boşluk, hastane örneklerinde açık olduğu üzere hala mevcuttur. Siber operasyonlar neticesinde hastane sistemlerinde yer alan bilgiye erişimin engellenmesi, tedavi sürecinde doktor ve hemşirelerin doğru kararlar almasını zorlaştıracaktır. Aynı zamanda hastanedeki hasta akışı için hayati öneme sahip yönetim sistemleri kesintiye uğrayacağından hastalarda fiziksel zarar ortaya çıkabilecektir. Eylül 2020'de Almanya'da bir hasta, en yakın hastanenin fidye yazılımı saldırısıyla mücadele etmesi gerekçesiyle kendisini kabul edememesi ve tedavisinin bir saat gecikmesi sonucunda hayatını kaybetmiştir. Alman savcılar bilgisayar korsanlarını taksirle ölüme sebebiyet verme suçundan soruşturmuşlardır. Ancak hastanın tıbbi teşhisinin ciddiyeti doğrultusunda, hastanın yaşamının sona ereceğinin anlaşılması üzerine dava düşürülmüştür.[73] Fidye yazılımlarının doğrudan bir ölüme neden olması yakın gelecekte mümkün olabilir.

Devlete ait bilgisayar sistemlerine yönelik bir siber saldırı neticesinde sosyal yardımların ödenmesi engellenebilir. Böylelikle potansiyel olarak yoksulluk ve intihar oranlarının artmasına sebebiyet verilebilir. Adalet Bakanlığı'na ait sistem üzerinden gerçekleştirilen siber operasyonlar ile hapishanelerin, mahkemelerin ve polisin yönetiminde kilit rol oynayan adalet sistemi ağları kullanılamaz hale getirilebilir. Bu doğrultuda, insanların daha uzun süre hapishanelerde tutulmasına sebebiyet verilebilir ve polisin suça müdahale etmesi engellenebilir. Bu örneklerdeki siber saldırılar sonucunda

[71] Sandoz/Swinarski/Zimmerman, para. 517.

[72] ILA Study Group, s. 340.

[73] William Banks, "Cyber Attribution and State Responsibility", *International Law Studies*, 97(1), 2021, s. 1049.

meydana gelen zararlar, ölçülebilen ve hayatın akışına zarar verme potansiyeline sahip somut, gerçek sonuçlardır.

Siber operasyon ile ortaya çıkardığı etki arasındaki nedensellik bağı karmaşıktır ancak öngörülemez değildir. Siber operasyonlar kritik bilgilere erişimi engelleyerek sistemlerin çökmesine ve sivillerin zarar görmesine neden olmaktadır. Bu özelliklere sahip siber operasyonları, verilere yönelik bir saldırı olarak kavramsallaştırılmak yerine, verilerin içinde bulunduğu sisteme veya altyapıya yönelik bir saldırı olarak kabul etmek daha doğru bir yaklaşım olacaktır.

Saldırıya uğrayan verilerin bilgisayar kodu, elektromanyetik darbe, saklanmasına ve erişilmesine izin veren donanım ve bu verileri kullanıma sokan sistem olarak kabulü yerine yalnızca bilgi olarak kavramsallaştırmak yanlış yorumlamalara sebebiyet verebilir.

Veri her zaman fiziksel bir varlığı olan bir sistemin içine gömülü olarak bulunmaktadır. Analoji yoluyla bir klasör dolabındaki kâğıt dosyalar uluslararası insancıl hukuk sistemi açısından incelendiğinde, kağıtlardaki bilgileri kağıtların kendisinden ayrı bir varlık olarak değerlendirmek doğru olmayacaktır.[74] Klasör dolabı, içerisindeki çatışma planları dolayısıyla askeri bir hedef olarak kabul edilir ise hedef alınabilir. Bu durumda, saldırıyı yapmanın gerekçesi olarak askeri bir hedef olarak sınıflandırılan klasör dolabı, içerisindeki kâğıt dosyalar dolayısıyla değil içerdiği bilgi nedeniyle askeri hedef olacaktır. Aynı örnek farklı bir olasılıkla incelendiğinde; eğer bilgiler tamamen sosyal güvenlik sistemi ile ilgili olsaydı, klasör dolabı askeri bir hedef olmayacaktır ve saldırıdan korunacaktır.

Verilere yönelik veya veriler aracılığıyla yapılan saldırılarla ilişkili olarak ortaya çıkan zararların, uluslararası insancıl hukuk sistemine tabi olması için somut sonuçlarla nedensellik bağının varlığını ortaya çıkarmak zor olacaktır. Zararlı sonuçlar için bir vahamet eşiği belirlenmesi ve zararlı sonuçların makul ölçüde öngörülebilir olanlarla sınırlandırılması mantıklı olacaktır. Daha basit ve koruyucu olan seçenek, verileri saldırıya uğrayabilecek fiziksel bir sistemin parçası olarak kabul etmek olacaktır. Gerçek hayat örneklerinde saldırıyla ilgili nesne veri değildir, verinin içine gömülü olduğu sistemler ve altyapı siber saldırıların hedefidir.

Genellikle verilere karşı gerçekleştirilen siber operasyonlar saldırı

[74] International Committee of the Red Cross, Challenges Report, s. 21.

eşiğini aşacak kadar ciddi ve makul ölçüde öngörülebilir sonuçlara yol açmayan operasyonlar olacaktır, ancak bazı siber operasyonlar bu eşiği karşılayabilecektir. Eğer Uluslararası Ceza Mahkemesi geniş anlamda bir hukuki yorum yaklaşımını benimseyecek olursa, sivillere daha fazla koruma sağlanmış olacaktır. Böylelikle uluslararası ceza hukuku ve uluslararası insancıl hukukun gelişimi teşvik edilecektir. Uluslararası Ceza Mahkemesi dar yorumu tercih ederse, bilgisayar verileri savaş suçları açısından nesnenin bir parçası olarak kabul edilmeyecektir. Devletlerin yaklaşımlarında ve akademik literatürde bu konuda bir fikir birliği bulunmamaktadır.[75]

III. İMHA EDİLMEYE, EL KONULMAYA VEYA ELE GEÇİRİLMEYE ELVERİŞLİ MAL OLARAK BİLGİSAYAR VERİLERİ

Köklerini Cenevre Sözleşmelerinde ve 1907 Lahey Düzenlemelerinde[76] bulan malın imha edilmesi, el konulması veya ele geçirilmesine atıfta bulunan savaş suçları, sivil verilere yönelik siber operasyonlarda cezai hesap verebilirlik için başka bir yol sunmaktadır.[77] Veri ya da içinde bulunduğu sistem mal olarak kabul edilebilir. Malların verileri içerip içermediği Roma Statüsü, Cenevre Sözleşmeleri veya Lahey Düzenlemeleri'nin hazırlanması sırasında dikkate alınmamıştır. Ek Protokol I kapsamında, saldırılara ilişkin kuralların zamansal sınırları hakkında bazı tartışmalar olsa da,[78] uluslararası insancıl hukuk sisteminde malların temel korumasının kapsamı, saldırı anlamına gelmeyen davranışlara uygulandığı için daha geniş olarak kabul edilmektedir.[79]

A. Mal Kavramını Anlamlandırmak

Mal kelimesinin anlamı "bir kimsenin, bir tüzel kişinin mülkiyeti altında bulunan, taşınır veya taşınmaz varlıkların bütünüdür".[80] Savaş suçlarını

[75] ILA Study Group, s. 339.

[76] Madde. 50 GC I; Madde. 51 GC II; Madde. 147 GC IV; Madde 23(g) Regulation Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907.

[77] Roma Statüsü Madde 8(2)(a)(iv), 8(2)(b)(xiii), 8(2)(e)(xii).

[78] Eian Katz/Milena Sterio/Jonathan Worboys, "Attacks against Hospitals and Cultural Property: Broad in Time, Broad in Substance", *Articles of War*, 2020, <https://lieber.westpoint.edu/attacks-against-hospitals-cultural-property-broad/>, Erişim Tarihi 09 Temmuz 2023.

[79] ILA Study Group, s. 347.

[80] Türk Dil Kurumu, "Türk Dil Kurumu Sözlükleri", <https://sozluk.gov.tr/>, Erişim Tarihi 12 Temmuz 2023.

tanımlayan hükümler mal kavramının anlamını sınırlandırmadığından, mal sahip olunabilecek her şeyi kapsayacak şekilde geniş yorumlanmaktadır.[81] Bu yaklaşım benimsenirse, mal kavramı verileri de kapsayacak şekilde tanımlanabilir. Savaş suçları tanımlayan düzenlemelerin lafzi yorumu doğrultusunda, veriler imha edilebilir ve verilere el konulabilir. Araziye el koyma ile ilgili olarak ortaya çıkan sorun, malın devir işlemleri gibi resmi edinimlerin gerçekleşmesinin gerekip gerektirmediğidir. Fiili, *de facto* el koymanın yeterli olduğunun kabulü ile birlikte, malı fiilen kontrol eden, yöneten ve başka şekillerde kullananların kimliğine odaklanılması gerektiği yönündeki daha geniş görüş tercih edilmelidir.[82] Diğer mal türlerine kıyasla karşılaştırması zor olsa da, bu mantık verilere uygulanabilir.

Mal kavramı, uluslararası insancıl hukuk dışındaki hukuki sistemlerde de önemli bir rol oynamaktadır. Uluslararası ve yerel politika yapıcılar ve mahkemeler, çeşitli yaklaşımlar benimseyerek verilerin malı koruyan hukuki sistemlere dahil edilip edilmemesi gerektiğini sorgulamışlardır. Konuya ilişkin farklı yaklaşımlar bulunmaktadır. Bu yaklaşımlar, sorunun uluslararası insancıl hukuk ve uluslararası ceza hukuku kapsamında çözülmesi için model olarak kullanılabilir. Farklı hukuk sistemlerinden kararlar bu amaçla değerlendirilecektir.

Uluslararası mahkemelerin bilgisayar verilerinin mal olarak nitelendirilmesine ilişkin içtihadı sınırlıdır. *Bazı Belge ve Verilere El Konulması ve Alıkonulmasına İlişkin Sorular (Timor-Leste v Avustralya)* davasında Timor-Leste, hangi kuralların uygulanacağını belirlemek amacıyla verilerin taşınır mal olarak değerlendirilmesi gerektiğini belirtmiştir. Uluslararası Adalet Divanı verilerin mal statüsüne ilişkin bir karar vermemiş olsa da, bu görüşü açıkça reddetmemiştir.[83]

Yerel mahkemeler, verilerin taşınır ve taşınmaz malları düzenleyen mevcut rejimlere dahil edilip edilmeyeceğini değerlendirmiştir. Örneğin, Mayıs 2020'de İtalyan Yargıtay'ı verilerin taşınır mal olarak değerlendirilebileceğine

[81] Simon McKenzie, *Disputed Territories and International Criminal Law: Israeli Settlements and the International Criminal Court*, Routledge, 2019, s. 119.

[82] *Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Trial Judgement)*, IT-96-21-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 16 November 1998 § 590.

[83] *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) (Provisional Measures)*, ICJ Reports (2014), §§ 24-26.

karar vermiştir. Kararın gerekçesi verilerin fiziksel olarak alıkonulabilir, sahip olunabilir, el konulabilir ve kendi yapısal özelliklerini koruyarak bir dijital destekten diğerine aktarılabilir olmasıdır.[84]

ABD Mahkemeleri elektronik belge ve verileri mal olarak değerlendirmektedir. New York Temyiz Mahkemesi, bir kişinin başka bir kişinin malını alıp sahibinin haklarına aykırı bir şekilde kullanması olarak tanımlanabilecek dönüştürme haksız fiilinin amaçları doğrultusunda, bilgisayardaki bir belgenin dosya dolabındaki bir belgeyle aynı değere sahip olduğuna, çünkü değerinin fiziksel biçiminde değil içerdiği bilgide yattığına karar vermiştir.[85]

Kremen v. Cohen davasında ABD Dokuzuncu Daire Temyiz Mahkemesi, bir internet alan adının haksız fiil hukuku tarafından korunan soyut veyahut maddi olmayan mal olarak sınıflandırılabileceğine karar vermiştir.[86] Bu durumda, bir şirketin dosya odasını yakmak dönüştürme haksız fiili kabul edilebilecektir. Şirketin ana bilgisayarını hacklemek ve verilerini silmek ise dönüştürme haksız fiili olarak kabul edilmeyecektir. *Integrated Direct Marketing LLC v. May* davasında Arkansas Yüksek Mahkemesi bu davalara atıfta bulunarak, kâğıt belgelerin dönüştürme haksız fiil olarak kabulünün mümkün olup elektronik ortamda saklanan benzerlerine izin verilmemesinin makul bir dayanağı olmadığına karar vermiştir.[87] Diğer ABD Mahkemeleri, haksız fiil kavramını bu şekilde geniş yorumlamak konusunda isteksiz davranmaktadır,[88] bu konu akademik araştırmaların odak noktası olmaya devam etmektedir.[89]

Anglo Sakson hukukunu uygulayan mahkemeler genellikle *National Provincial Bank Ltd v. Ainsworth* davasında geliştirilen mal tanımını kararlarında esas almaktadır. Bu doğrultuda; mal ayırt edilebilir, tanımlanabilir, üçüncü şahıslar tarafından belirlenebilir, doğası gereği üçüncü şahıslar

[84] Italian Supreme Court of Cassation, Second Criminal Chamber, with the Judgment No. 11959 of April 10, 2020.

[85] *Thyroff v Nationwide Mutual Insurance Co* 8 NY 3d 283, at 292.

[86] *Kremen v. Cohen*, 337 F.3d 1024 (9th Cir.2003).

[87] *Integrated Direct Marketing, LLC v. May*, 495 S.W.3d 73, 2016 Ark. 281 (2016).

[88] *Epic Systems Corp. v. Tata Consultancy Services Ltd*., 2016 WL 4033276 at § 27 (W.D. Wisc. July 26, 2016).

[89] Joao Marinotti, "Tangibility as Technology", *Georgia State University Law Review*, 37(1), 2021, s. 53.

tarafından üstlenilebilir ve bir dereceye kadar kalıcılık veya istikrara sahip olmalıdır.[90] Bu tanım doğrultusunda, veriler bilgi niteliğinde olduklarından mal olarak tanımlanamayacaktır.

2014 yılında İngiliz Temyiz Mahkemesi, bilgisayar veri tabanının mal statüsünü ayrıntılı olarak incelemiştir. İngiliz Temyiz Mahkemesi veri tabanının depolandığı fiziksel ortam ile bilginin kendisi arasında bir ayrım yapmıştır. Veri tabanının depolandığı fiziksel ortam mal olarak tanımlanmıştır. Bilginin kendisi ise mal olarak tanımlanmamıştır. [91]

Yeni Zelanda mahkemeleri ise tam tersi bir yaklaşım benimsemiştir.[92] *R v. Cox* davasında Temyiz Mahkemesi, verilerin geçici olsa bile fiziksel varlığa sahip olduğu gerekçesiyle kısa mesajın bir nesne olmadığını reddetmiştir.[93] *Dixon v. R* davasında, veriler maddi olmasa da, 1961 tarihli Yeni Zelanda Suçlar Yasası kapsamında mal olarak kabul edilebileceklerine karar verilmiştir.[94] *Henderson v. Walker* davasında Yüksek Mahkeme, verilerin şifre koruması ve bilgisayar, depolama ortamı üzerinde fiziksel kontrol yoluyla hariç tutulabilip, dışlanabileceğini vurgulamıştır. Veriler aynı zamanda erişilemez hale getirmek için silinebilir veya değiştirilebilir yani tüketilebilir. Bu doğrultuda verilerin mal olarak tanımlanabileceğine karar verilmiştir.[95]

Japon Ekonomi, Ticaret ve Sanayi Bakanlığı, somut olmaması nedeniyle verilerin Japon Medeni Kanunu kapsamında mülkiyet haklarına tabi olamayacağını belirtmiştir.[96] *Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn Rehberi 2.0*'ın yorumunda belirtildiği üzere, somut materyalden ziyade bilgi ile ilgili olan ve yaygın olarak tanınan bir mülkiyet şekli olarak fikri mülkiyet bulunmaktadır.[97] Bu mülkiyet veriden oluşur ve sahip olunmasına, ticaretinin yapılmasına, edinilmesine ve çalınmasına izin veren bir rejim vardır. Çalınmasını ve kötüye kullanılmasını hayal etmekte hiçbir zorluk yoktur ve eğer bilginin başka bir kaydı yoksa, bilginin depolandığı yerin yok

[90] *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175, § 1248.

[91] *Denlay v Federal Commissioner of Taxation* (2011) 193 FCR 412, § 72.

[92] *Ruscoe v Cryptopia Limited (in liquidation)* [2020] NZHC 728, § 95.

[93] *R v Cox* (2004) 21 CRNZ 1, § 49.

[94] *Dixon v The Queen* [2015] NZSC 147, § 50.

[95] Sarah Green/John Randall, *The Tort of Conversion*, Hart Publishing, 2009, s. 118.

[96] Japanese Ministry of Economy, Trade and Industry, *Contract Guidelines on Utilization of AI and Data*, IP Policy Office, Economic and Industrial Policy Bureau, 2018, s. 23.

[97] Schmitt, *Tallinn Manual,* s. 535.

edilmesi onun ortadan kaldırılmasına yol açacaktır.[98]

Türk hukuk öğretisi açısından, bilişim sistemlerinde yer alan verilerin alınması ya da başka bir yere nakledilmesi hırsızlık suçunu oluşturmamaktadır.[99] Veriler menkul mal kapsamında değillerdir. Verilerin taşınır mal statüsü bulunmamaktadır, bu gerekçeyle suçta ve cezada kanunilik ilkesi kapsamında Türk Ceza Kanunu'nda kanun koyucu tarafından suç olarak tanımlanan fiiller için cezai sorumluluk oluşacaktır. Verilerin izinsiz bir şekilde ele geçirilmesi hırsızlık suçunun unsurları ile benzerlikler taşısa dahi, hırsızlık suçunun maddi unsurlarında taşınır mal ve ekonomik değer taşıyan enerji üzerindeki kullanım hakkının izinsiz bir şekilde sona erdirilmesi öngörülmüştür. Veriler bu nitelikleri taşımadıklarından kapsam dışında kalacaklardır. Türk Ceza Kanunu'nda yer alan hiçbir maddede veri taşınır bir mal olarak belirtilmemiştir. Verilerin içeriği konusunda bir ayrıma gitmek daha doğru bir yaklaşım olacaktır. Bilgisayarda bulunana verilerin, programların, bilgilerin hırsızlık suçu kapsamında değerlendirilebilmesi için belirli niteliklere haiz olması gerekmektedir. Bu nitelikler taşınır mal olma ve iktisadi bir nitelik taşımaktır. Yargıtay Ceza Genel Kurulu'nun 17.11.2009 tarihinde oy çokluğu ile verdiği 2009/11-193 E. ve 2009/268 K. sayılı kararı da bu görüşü benimsemektedir; "… failin eylemdeki kastı, katılanın banka hesabında bulunan taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi hesabına geçirmeye katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya, başka bir anlatımla mevcut veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alıp mal edinmeye yöneliktir. Kaldı ki sanığın, katılanın internet bankacığında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCK m.142/2-e'de düzenlenen bilişim sistemini kullanmak suretiyle hırsızlık suçunun gerçekleştiği kabul edilmelidir. Sanığın eyleminin TCK m.142/2-e de düzenlenen nitelikli hırsızlık suçunu oluşturduğunun kabul edilmesi karşısında, bilişim sistemini engelleme, bozma, verileri yok etme, değiştirme veya başka yere gönderme fiillerini suç olarak düzenleyen 244. maddenin dördüncü fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır".[100] Netice itibariyle, farklı hukuk sistemlerinden tespit edilen kararlar ışığında verilerin statüsü konusunda fikir birliği bulunmamaktadır.

[98] Mark Lemley, "Property, Intellectual Property, and Free Riding", *Texas Law Review*, 83(4), 2005, s. 1031.

[99] Ersan Şen, "Hırsızlık Suçları", *Ankara Barosu Dergisi*, 3(1), 2012, s. 325.

[100] Yargıtay Ceza Genel Kurulu, E. 2009/11-193, K. 2009/268, T. 17.11.2009.

B. Verilerin İmha Edilmesi, El Konulması veya Ele Geçirilmesinin Hukuka Aykırı Olduğu Durumları Değerlendirmenin Yarattığı Zorlukların İncelenmesi

Uluslararası Ceza Mahkemesi ve literatür verilerin mal olarak sınıflandırılmasını kabul etse bile, verilerin imha edilmesinin, el konulmasının veya ele geçirilmesinin uluslararası insancıl hukuk ve buna bağlı olarak Roma Statüsü açısından hukuka aykırı olup olmayacağı sorusu varlığını sürdürmektedir.[101]

Uluslararası insancıl hukukta kuralın kökenlerine odaklanılırsa; 23(g) Maddesi ile 1899 ve 1907 tarihli Lahey Düzenlemeleri, savaşan tarafların, savaşın gerekleri gerektirmedikçe düşmanın mallarını imha etmesini veya ele geçirmesini yasaklamıştır.[102] Cenevre Sözleşmeleri belirli korunan mallar için farklı standartlar ortaya koymaktadır.[103] Sivil hastaneler ve işgal altındaki topraklardaki özel mallar için farklı standartların varlığı bu konudaki net bir örnektir. İşgal sırasında sivil ve devlet mallarına yönelik koruma ise daha kapsayıcıdır. Dördüncü Cenevre Sözleşmesinin 53. Maddesi şunu öngörmektedir:

"Ferden veya müştereken hususî şahıslara, devlete veya amme topluluklarına, içtimai teşekküllere veya kooperatiflere ait menkul ve gayrimenkul malların imhası, askerî harekât bu imhayı kat'i olarak zaruri kıldığı haller müstesna, yasaktır."

Verilerin Ek Protokol I'in 52. Maddesi doğrultusunda bir nesne olarak sınıflandırılmadan, verilerin uluslararası insancıl hukuk kapsamında korunan mal olarak kabul edilebilmesinin bir temeli olup olmadığı değerlendirilmelidir.

İkinci Dünya Savaşı sonrası içtihatlarda maddi olmayan varlıkları da içeren mülkiyete yönelik kararlar bulunmaktadır.[104] Örneğin *Krupp* ve *IG Farben* davalarında, mülkiyet gayri maddi hisse paylarından ve kurumsal mülkiyet haklarından oluşmasına rağmen sanıklar mülkiyet suçlarından suçlu bulunmuştur.[105]

[101] McKenzie, s. 143.

[102] Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulation Concerning the Laws and Customs of War on Land, The Hague, 18 October 1907.

[103] Dormann, s. 339.

[104] Dinniss, s. 47.

[105] *The IG Farben and Krupp Trials*, United States Military Tribunal, 14 August 1947–29 July

Ancak daha yakın bir tarihte, Uluslararası Ceza Mahkemesi Ön Yargılama Dairesi, *Katanga* ve *Chui* davasında sivil mülklerin Ek Protokol I Madde 52(2)'de öngörülen askeri hedef tanımı kapsamında bulunmayan nesneleri oluşturduğunu açıklayarak, mal tanımını nesne tanımıyla açıkça ilişkilendirerek daha dar bir yaklaşım benimsemiştir.[106] Bu yaklaşım, dar kapsamlı olsa da farklı suçlarda mal ve nesnelerin anlamı arasında tutarlılık sağlama avantajına sahiptir.

Verilerin mal olarak statüsü *Tallinn Rehberi 2.0*'da değerlendirilmiştir. *Tallinn Rehberi 2.0*'ın 149. kuralı, işgal sırasında malların ele geçirilmesini ve el konulmasını kapsamaktadır. *Tallinn Rehberi 2.*0 38. kuraldaki nesne kavramında olduğu gibi, bu kural da bilgisayar donanımı ile üzerinde bulunan veriler arasında bir ayrıma gitmektedir.[107] *Tallinn Rehberi 2.0* devletin taşınır mallarının kapsamını bilgisayarlar, bilgisayar sistemleri, bilgi işlem ve bellek cihazları olarak belirtmektedir. *Tallinn Rehberi 2.0* şerhinde, veriler mal olarak nitelendirilmese dahi işgalci gücün devlet verilerini askeri operasyonları için kullanması önünde engel olmadığı açıklanmaktadır.[108]

Kontrol altına alma kavramı genellikle malları müsadere etmeyi veya mallara fiziksel olarak el koymayı kapsamaktadır. Yeni ortaya çıkan sanal el koyma veya müsadere etme kavramı ise işgalci gücün malları kendi amaçları doğrultusunda kullanabilmesini ve malın gerçek sahibinin kullanımına izin verilmemesini kapsamaktadır.[109] Dolayısıyla bu bulgular verinin kendisinden ziyade sadece bilgisayar donanımının kullanımı için geçerli olacaktır. Bu görüş evrensel olarak kabul görmese de nesnelerle ilgili kurallara benzer şekilde, azınlık görüşü verilerin mal olarak nitelendirilebileceğini savunmaktadır.[110]

Problemi farklı bir açıdan incelemek amacıyla belirli veri türlerini korunan mal kapsamında kabul etmenin mümkün olup olmadığı değerlendirilmelidir. Kültürel varlıkların korunmasına ilişkin tartışma açısından, bazı durumlarda verilerin yok edilmesinin kültürel varlıkların yok edilmesi anlamına

1948 and 17 November 1947–30 June 1948, in Law Reports of the Trials of War Criminals, Vol. X (1949) at 46, 164.

[106] Decision on Confirmation of Charges, Katanga and Chui (ICC-01/04-01/07-717), Pre-Trial Chamber I, 30 September 2008, §§ 312-313.

[107] Schmitt, *Tallinn Manual,* s. 549.

[108] Schmitt, *Tallinn Manual,* s. 550.

[109] Schmitt, *Tallinn Manual,* s. 551.

[110] Schmitt, *Tallinn Manual,* s. 550.

gelebileceği fikri daha geniş kabul görmektedir.[111] *Tallinn Rehberi 2.0*'ın kültür varlıklarıyla ilgili 142. kuralının yorumunda, uzmanların maddi olmayan öğelerin mal olarak nitelendirilip nitelendirilemeyeceğini değerlendirdikleri açıktır. Cenevre Sözleşmeleri Ek Protokol I 53. Maddede nesnelere yapılan atfın, veriler hariç kültürel varlıkların somut olması gerektiği anlamına geldiği şeklinde bir yorumda bulunulabilir. Ancak fikri mülkiyet hukuku kapsamında malın her zaman somut olmadığı açıktır. Tamamen bilgisayar ortamında oluşturulan ve depolanan nesneler yalnızca dijital biçimde varlıklarını sürdürmektedir. Bu konuda uygun örnekler; müzik notaları, dijital filmler, e-devlete ilişkin belgeler ve bilimsel veriler olarak sıralanabilir. Kopyalarını oluşturmak amacıyla kullanılabilecek fiziksel bir varlığı bulunan nesnelerin belirli kopyaları da kültür varlığı olarak nitelendirilebilir.[112]

Kültür varlıklarının tüm dijital tezahürlerinin koruma hakkına sahip olduğunu savunmak doğru bir yaklaşım olmayacaktır. Korumanın kapsamı sınırlandırılmalıdır. Bu durumda sadece orijinalin erişilemez olduğu, yok edildiği ya da yapılabilecek dijital kopya sayısının sınırlı olduğu durumlar için koruma söz konusudur.[113] Kültür varlıklarının korunması orijinal sanat eserinin değerine, yeri doldurulamazlığına göre değerlendirilmelidir. Orijinal eserin aslına uygun kopyalarını üretmenin zorluğu, harcanan zaman ve masraflara bağlı olarak koruma sağlanmalıdır. Bu doğrultuda, çok sayıda ve yüksek kaliteli reprodüksiyonların yapılabildiği durumlarda koruma geçerli olmayacaktır.[114]

Tallinn Rehberi 2.0 şerhi, sadece verilerin değiştirilmesi, zarar verilmesi, silinmesi veya imha edilmesinin yanı sıra örneğin soykırım işlenmesine yardımcı olmak için dijitalleştirilmiş tarihi arşivlerin kullanılması gibi askeri amaçlarla verinin kullanılmasının da hukuka aykırı olacağını belirtmektedir.[115] Bu doğrultuda, örneğin erişim için kullanılan elektronik cihazların işleyişini etkilemek yani sadece erişimi geçici olarak engellemek veya bozmak, kültür varlıklarının korunması kapsamı dışında kalmaktadır. Normatif açıdan bakıldığında, dijital kültür varlıklarına yönelik bu yaklaşımın, verileri tamamen koruma dışında bırakmaya tercih edilebileceği açıktır. Bu yaklaşım temelde

[111] Liivoja, McCormack, s. 53.

[112] Schmitt, *Tallinn Manual,* s. 535.

[113] Schmitt, *Tallinn Manual,* s. 536.

[114] Schmitt, *Tallinn Manual,* s. 535.

[115] Schmitt, *Tallinn Manual,* s. 536.

vahamet eşiği yaklaşımının benimsenmesinden ibarettir. Verilere koruma sağlanması verinin mal olarak nitelendirilmesi nedeniyle sağlanmaz aksine verinin yok edilmesinin sonuçları ile doğrudan bağlantı kurulmaktadır.[116]

Verinin kendisinin bir mal biçimi olduğu konusunda güçlü bir mutabakat bulunmamaktadır. Temel uluslararası insancıl hukuk belgelerinde açık bir yönlendirmesinin olmaması ve devletlerin mal kavramına farklı yaklaşımlarının bulunması nedeniyle, tüm veriler mal olarak kabul edilmelidir şeklindeki en korumacı yorum temelsiz kalmaktadır. Veri mal olarak kabul edilmese de, veriler mal olarak sınıflandırılabilen bilgisayar ağ ve sistemleri altyapısının içine gömülüdürler. Böylelikle verinin altyapının bir parçası olduğu anlaşılabilir.

IV. ANDLAŞMA VE TEAMÜL HUKUKUNDAKİ DEĞİŞİM ROMA STATÜSÜ'NE DAHİL EDİLMELİ MİDİR?

Uluslararası insancıl hukuk hükümlerinde ve savaş suçlarının tanımında kullanılan nesneler ve mallar ifadelerinin sivil verileri kapsayabileceği görüşü reddedilmemektedir. Ancak Roma Statüsü'nü yorumlama aşamasında ilerici bir yaklaşımı benimsemek tartışmalara meydan verebilir. İlerici bir yorum yönteminin kullanılmasında yaşanabilecek temel zorluk; devletler, ordular ve uluslararası mahkemeler tarafından bu yaklaşımı benimseyen yeterli uygulama bulunmamasıdır.[117] Günümüz teknolojik gelişmeleri ışığında, uluslararası insancıl hukuk açısından bilgisayar ağlarındaki verilerin statüsünün önemi ortaya çıkmıştır. Özellikle yeni teknolojileri hukuki açıdan değerlendirirken, devlet uygulamalarını *opinio juris* olarak arayan bir yaklaşımın benimsenmesi kısıtlayıcı olacaktır. Macak, *lex lata* ve *lex ferenda* arasındaki yakın ilişkiye dikkat çekerek, bir yorum lehine devlet uygulamasının bulunmamasının, alternatif bir yorumun otomatik olarak geçerli olması gerektiği anlamına gelmediğini savunmaktadır.[118] Yaşanan hızlı teknolojik değişimler, herhangi bir devlet uygulamasının veya *opinio juris'*in yetişemeyeceği yeni kavram ve kategorilerin oluşturulmasını gerekli kılmaktadır. Bu açıdan bakıldığında ilgili andlaşma hükümlerinin kapsamını anlamak için uzlaşılmış yorumlama yöntemleri kullanılabilir[119], ancak bu yaklaşımın tehlikeli bir uygulama

[116] Dinniss, s. 47.

[117] Schmitt, Wired Warfare, s. 343.

[118] Macak, s. 60.

[119] Droege, s. 578

olabileceği konusunda uyarılar da bulunmaktadır.[120]

Son zamanlarda savaş suçları bağlamında nesne veya mal olarak nitelendirilebilecek olan verilere yönelik geniş yorumun desteklenmesi zorlaşmıştır. Bu konuda görüşlerini açıklayan devletler tüm verilerin sivil nesnelere veya mallara uygulanan koruma rejimine dahil edilmesini desteklememiştir. Nihayetinde yorum farklılığı henüz çözüme kavuşmuş değildir. Bu çerçevede, Uluslararası Ceza Mahkemesi ilgili savaş suçları hükümlerinde yer alan nesneler ve mal ifadelerinin kapsamlı bir yorumunu benimseyerek hukuki tartışmayı farklı bir yöne doğru ilerletmeli midir? Bu soru, Roma Statüsü'nün kanunilik ilkesine verdiği önem dikkate alındığında özellikle hassastır. Roma Statüsü için geçerli olan yorumlama kuralları, uluslararası insancıl hukuk andlaşmaları dahil olmak üzere genel uluslararası hukukta geçerli olan yorum kurallarından farklıdır. Roma Statüsü Madde 22(2) uyarınca Statü'nün daha kısıtlayıcı bir şekilde yorumlanması gerekebilir:

"Bir suçun tarifi, dar anlamda yorumlanır ve bu tarif kıyas yoluyla genişletilemez. Suç tarifinin belirsiz olması halinde; bu tarif, soruşturulan, yargılanan veya mahkûm edilen şahıs lehine yorumlanır." [121]

Roma Statüsü Madde 22(2)'nin amacı, hangi davranışın suç olduğunu önceden tahmin etmelerine izin vererek, failler için yasanın erişilebilirliğini ve öngörülebilirliğini koruyarak kanunilik ilkesini Roma Statüsü'ne yerleştirmektir.[122]

Yargıcın takdir yetkisi kanunun kesin olması, belirsiz bölgelerin ortadan kaldırılması neticesinde davaların büyük çoğunluğunda sınırlandırılmalıdır.[123] Dar yorum, mahkemelerin bir suçun sınırlarını yorumlamasını ve netleştirmesini engellememelidir. Ancak yargıçların hukuk yaratma yetkisi hukuki boşluk durumlarında içtihat yoluyla ve sınırlı olmalıdır.[124] Roma Statüsü metni

[120] Tim McCormack, "International Humanitarian Law and the Targeting of Data", *International Law Studies*, 94(1), 2018, s. 240.

[121] *Rome Statute of the International Criminal Court*, opened for signature 17 July 1998, 2187 UNTS 90 (entered into force 1 July 2002) ('Rome Statute').

[122] Daniel Peat, *Comparative Reasoning in International Courts and Tribunals*, Cambridge University Press, 2019, s. 201.

[123] Leila Sadat/Jarrod Jolly, "Seven Canons of ICC Treaty Interpretation: Making Sense of Article 25's Rorschach Blot", *Leiden Journal of International Law*, 27(3), 2014, s. 768.

[124] Leena Grover, *Interpreting Crimes in the Rome Statute of the International Criminal Court*, Cambridge University Press, 2015, s. 400.

olası anlamları tek bir anlamla sınırlandırmaz. Yorum kurallarının yaptığı tek şey anlam sınırlarının belirlenmesine yardımcı olmak ve nerede bittiğini göstermektir. Hiçbir yorumlama metodu mümkün olan tek seçim ya da gerçek anlam olmayacaktır. Ancak doğası gereği taraflı veya siyasi olacaktır.[125]

Uluslararası insancıl hukukta verinin bir nesne veya mal olarak statüsüne ilişkin tartışma daha dar bir bakış açısının hâkim olduğunu göstermektedir. Verilerin veya daha doğrusu bilginin tek başına bir nesne veya mal olarak yorumlanabileceğine ilişkin en geniş görüş, suçların makul yorumlarının kabul edilebilir sınırları içinde olması muhtemel değildir. Uluslararası Ceza Mahkemesi'nin geniş yorum metodunu seçmesi halinde, daha fazla devlet verinin kendisinin bir nesne veya mal olarak kabul edilmesi gerektiği görüşünü destekleyen bir devlet uygulaması ve *opinio juris* oluşturmaya istekli olmadıkça, mahkemenin güvenilirliğinin zedelenme riski ortaya çıkacaktır. Ancak dar yorum metodu tercih edilir ise özellikle internetin günlük yaşamın her alanını etkilediği göz önünde bulundurulduğunda, Roma Statüsü'nün bilgisayar verilerine karşı ve bilgisayar verileri aracılığıyla gerçekleştirilen siber operasyonlarla sivil sistemlere ve altyapıya verilen zarara tamamen cevap vermemesi bir eksiklik olacaktır.

Tercih edilmesi gereken yaklaşım, bilgisayar verilerinin uluslararası insancıl hukuk tarafından korunabilen nesnelerin ve/veya malların bir parçası olduğunun kabul edilmesidir. Bu yaklaşım, savaş suçlarının amaçları doğrultusunda açık bir şekilde nesne ve mal olarak tanımlanabilen fiziksel sistemler içindeki verilerin gömülü olma durumunu daha doğru bir şekilde yansıtmaktadır. Yeni suç tanımları oluşturmak yerine mevcut suç tanımlarını yorumlayarak ve uygulayarak Roma Statüsü'nün değerlendirilmesi, nesne ve mal kategorilerini yalnızca maddi olmayan bilgilere genişletmeyi amaçlamadığı için kanunilik ilkesine saygı göstermektedir.[126] Verilere ilişkin doğru bakış açısını kullanan Mahkeme, siber operasyonların gerçek dünyadaki etkilerini hukuken dışlamamış olur. Örneğin, doğrudan ve geri döndürülemez fiziksel sonuçları olmayan ancak bilgisayar sistemlerinin artık olması gerektiği gibi çalışmamasına neden olabilecek siber operasyonların, nesnelere yönelik saldırılar olarak değerlendirilmesi doğru yaklaşım olacaktır. Geniş yorum metodunun kullanılması halinde verilerin dünyada fiziksel bir varlığı olan sistemlere, altyapılara ve donanımlara gömülü olduğunun kabulü

[125] Mehmet Dalar, "Uluslararası Ceza Mahkemesi'ne Yönelik Eleştirilerin Değerlendirilmesi", *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 17(2), 2017, s.155.

[126] Grover, s. 202.

gerekecektir. Örneğin, bankacılık altyapısına yönelik bir siber operasyon sivillerin ve işletmelerin uzun bir süre boyunca finansal işlem yapmasını engelleyerek tedarik zincirlerinin çökmesine sebebiyet verebilir. Siber operasyonların doğrudan etkilerinin bilgisayar verilerinin geri yüklenmesi veya bilgisayara erişimin yeniden sağlanması anlamında geri döndürülebilir olduğu durumlarda bile sistemler üzerinde oluşacak ikincil zararlar, hukuk tarafından tanınması gereken kalıcı izler bırakacaktır. Önerilen yaklaşım doğrultusunda; bilgisayar verileri sivil bankacılık sisteminin ayrılmaz bir parçası olarak ele alınacak ve bu verilere erişim sağlayan bilgisayarlar, verilerin depolandığı sunucular ve bunları birbirine bağlayan ağlar da fiziksel bir biçime sahip olacaktır. Bankacılık altyapısının tüm bu fiziksel bileşenleri, nesne ve mal olarak sınıflandırılabilir. Geniş yorum metoduyla bilgisayar verilerinin gerçek dünyadaki rolü daha net bir şekilde açıklandığında, uluslararası hukukun işleyişi sanıklar için öngörülebilir hale gelecektir; aynı zamanda kanunilik ilkesine saygılı bir şekilde suç açıklığa kavuşturulacaktır. Kuşkusuz, dar ya da geniş yorum metodundan hangisinin seçileceği problemi, kesin bir çözüme kavuşturulması mümkün olmayan bir yargı sorunudur.

Uluslararası Ceza Mahkemesi, verilerin tek başına bir nesne ya da mal olarak nitelendirildiği geniş yorum ile bu makalede önerilen, verilerin nesne ya da malın bir parçası olarak kabul edildiği dar yorum arasındaki farkın belirleyici olacağı bir davayla hiçbir zaman karşılaşmayabilir. Siber uzayın dışında hiçbir etki yaratmayan ya da çok az etki meydana getiren bir siber operasyon, Roma Statüsü Madde 17(1)(d)'de belirtilen kabul edilebilirlik değerlendirmesi için öngörülen vahamet eşiğini karşılamayacaktır. *Lubanga* davasında, Ön Yargılama Dairesi I'in belirttiği üzere vahamet eşiğinin karşılanması için davranış sistematik ya da büyük ölçekli olmalıdır. Aynı zamanda uluslararası toplumda meydana gelen sosyal alarmın da dikkate alınması gerekmektedir.[127] Ön Yargılama Dairesi II, Kenya'da yaşananlarla ilgili kararında, suçun boyutu, niteliği ve işlenme araçlarının suçun mağdurlar üzerindeki etkisi ile beraber dikkate alınması gerektiğini vurgulamıştır.[128] Somut bir örnek vermek gerekirse, *MV Mavi Marmara* olayına ilişkin kararında Savcı, gemide bulunan beş yüz yolcudan sadece on kişinin öldürülmesinin

[127] Decision on the Prosecutor's Application for Warrants of Arrest, Article 58, *Situation in the Democratic Republic of the Congo* (ICC-01/04-520-Anx2), Pre-Trial Chamber I, 10 February 2006, § 46.

[128] Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, *Situation in the Republic of Kenya* (ICC-01/09-19-Corr), Pre-Trial Chamber II, 31 March 2010, § 62.

ve elli beş kişinin yaralanmasının yetersiz olduğuna karar vermiştir.[129] Bu örnekler doğrultusunda, somut sonuçlar yaratmayan, sadece siber operasyon etrafında şekillenen davalar kabul edilebilirlik açısından vahamet eşiğini sağlamaktan uzaktır.

SONUÇ

Uluslararası insancıl hukuk ve Uluslararası Ceza Mahkemesi (UCM) Statüsü'ndeki ilgili savaş suçu hükümleri doğrultusunda, sivil veriler, korunan nesnelerin ve malların bir parçası olarak değerlendirilmelidir. Mahkemenin bu suçları incelemesi durumunda, ilgili siber operasyondan kaynaklanan doğrudan kinetik hasarın kanıtlanmasına gerek olmadığı en iyi yorum olacaktır. Bunun yerine, verilere karşı veya veriler aracılığıyla gerçekleştirilen siber operasyonun makul olarak öngörülebilir bir sonucu olması koşuluyla, etkilenen sivil sistem veya altyapı bozulduğu veya başka bir şekilde işlevselliğini kaybettiği sürece ilgili suçların işlendiği şeklinde bir yoruma başvurulmalıdır. Veriler her zaman, bu makalede tartışılan uluslararası hukuk kuralları tarafından kesin olarak korunan somut, fiziksel sistemlere gömülüdür. Daha dar bir yorum, çok çeşitli siber operasyonlara karşı sivillerin korunması açısından boşluğa yol açacaktır.

Bunun yerine önerilen yorum, en kısıtlayıcı yorum olmamakla birlikte UCM Statüsü'nün yorum kurallarıyla uyumludur. Önerilen yorum, her siber operasyonun Mahkeme önünde potansiyel olarak kovuşturulmasına engel olmaktadır. Roma Statüsü Madde 17(1)(d)'de yer alan vahamet eşiği, yalnızca yeterince ciddi sonuçları olan siber operasyonların soruşturma ve potansiyel kovuşturma konusu olacağı anlamına gelmektedir. Bu tür bir vahamet eşiğinin siber operasyonlara uygulanmasında, özellikle sorumluların tespit edilmesinde zorluklar yaşanacağı açıktır. Netice itibariyle siber operasyonların Mahkemenin yetki alanına girecek kadar ciddi olabilmesi için UCM Statüsü'ndeki nesne ve mal kelimeleri bu yoruma izin verecek şekilde değerlendirilmelidir.

[129] Article 53(1) Report, *Situation on Registered Vessels of Comoros, Greece and Cambodia*, ICC Office of the Prosecutor, 6 November 2014, § 138.

KAYNAKÇA

Article 53(1) Report, *Situation on Registered Vessels of Comoros, Greece and Cambodia*, ICC Office of the Prosecutor, 6 November 2014.

Avrupa Komisyonu, "What is Personal Data?", <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> Erişim Tarihi 12 Temmuz 2023.

Avrupa Konseyi Siber Suç Sözleşmesi (23 Kasım 2001, ETS No 185).

Avrupa Konseyi, "Explanatory Report to the Convention on Cybercrime", European Treaty Series - No. 185, 2001, <https://rm.coe.int/16800cce5b>, Erişim Tarihi 12 Temmuz 2023.

Banks W, "Cyber Attribution and State Responsibility", *International Law Studies*, 97(1), 2021, s. 1039-1072.

Bartram P/Knudsen J, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Danish Ministry of Defence, 2016.

Chen S, "Conventional Retaliation and Cyber Attacks", *The Cyber Defense Review*, 8(1), 2023, s. 67-86.

Commonwealth of Australia, *Australia's International Cyber Engagement Strategy*, Department of Foreign Affairs and Trade, 2017.

Dalar M, "Uluslararası Ceza Mahkemesi'ne Yönelik Eleştirilerin Değerlendirilmesi", *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 17(2), 2017, s.153-165.

Daskal J, "The Un-Territoriality of Data", *Yale Law Journal,* 125(2), 2015, s. 326-398.

Decision on Confirmation of Charges, Katanga and Chui (ICC-01/04-01/07-717), Pre-Trial Chamber I, 30 September 2008.

Decision on the Prosecutor's Application for Warrants of Arrest, Article 58, *Situation in the Democratic Republic of the Congo* (ICC-01/04-520-Anx2), Pre-Trial Chamber I, 10 February 2006.

Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, *Situation in the Republic of Kenya* (ICC-01/09-19-Corr), Pre-Trial Chamber II, 31 March 2010.

Denlay v Federal Commissioner of Taxation (2011) 193 FCR 412.

Diamond E, "Applying International Humanitarian Law to Cyber Warfare", *Law and National Security*, 67(1), 2014, s. 67-84.

Dinniss H, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, 48(1), 2015, s. 39-54.

Dinstein Y, *The Conduct of Hostilities under the Law of International Armed Conflict,* 3. Bası, Cambridge University Press, 2016.

Dixon v The Queen [2015] NZSC 147.

Dorrmann K, "Article 8 Para 2: Meaning of War Crimes", Kai Ambos (Ed.), *Rome Statute of the International Criminal Court: A Commentary*, Nomos, 2016, s. 296-580.

Drian J, *Stratégie Internationale de la France Pour le Numérique*, Ministre de l'Europe et des Affaires Etrangères, 2017.

Droege C, "Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross*, 94(886), 2012, s. 533-578.

Dutch Minister of Foreign Affairs, *Letter for the Parliament on the International Legal Order in Cyberspace — Appendix: International Law in Cyberspace*, Minister of Foreign Affairs to the President of the House of Representatives on the International Legal Order in Cyberspace, 2019.

Egan B, "International Law, and Stability in Cyberspace", *The Berkeley Journal of International Law*, 35(1), 2017, s. 168-180.

Epic Systems Corp. v. Tata Consultancy Services Ltd., 2016 WL 4033276 at § 27 (W.D. Wisc. July 26, 2016).

Gisel L/Rodenhauser T, "Cyber Operations and International Humanitarian Law: Five Key Points", 2019, *Humanitarian Law & Policy,* <https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/>, Erişim Tarihi 12 Temmuz 2023.

Gisel L/Rodenhauser T/Dorrmann K, "Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflict", *International Review of the Red Cross*, 102(913), 2020, s. 287-334.

Green S/Randall J, *The Tort of Conversion*, Hart Publishing, 2009.

Grover L, *Interpreting Crimes in the Rome Statute of the International Criminal Court*, Cambridge University Press, 2015.

Gül Y, "War Crimes and Individual Criminal Responsibility Arising out of Cyber Operations", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 26(2), 2020, s. 1063-1078.

Haataja S, "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law", *International Journal of Law and Information Technology*, 30(4), 2022, s. 423–443.

Haataja S, *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, Routledge, 2018.

Hakim N, "How Social Media Companies Could Be Complicit in Incitement to Genocide", *Chicago Journal of International Law*, 21(1), 2020, s. 81-117.

Henckaerts J/Beck L, *Customary International Humanitarian Law Vol I*, Cambridge University Press, 2005.

Horowitz J, "Cyber Operations under International Humanitarian Law: Perspectives from the ICRC", *ASIL Insights*, 24(11), 2020, s. 1-5.

Integrated Direct Marketing, LLC v. May, 495 S.W.3d 73, 2016 Ark. 281 (2016).

International Committee of the Red Cross, "International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper", *International Review of the Red Cross*, 102(913), 2020, s. 481-492.

International Law Association Study Group on the Conduct of Hostilities in the 21st Century, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", *International Law Studies*, 93(1), 2017, s. 323-388.

Kadlcak R, "Statement by Richard Kadlcak at the 2nd Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the General Assembly of the United Nations", 2020, <https://www.nukib.cz/download/publications_en/

CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf>, Erişim Tarihi 12 Temmuz 2023.

Kaljulaid K, *President of the Republic at the Opening of CyCon 2019*, Estonian Ministry for Foreign Affairs, 2019.

Katz E/Sterio M/Worboys J, "Attacks against Hospitals and Cultural Property: Broad in Time, Broad in Substance", *Articles of War*, 2020, <https://lieber.westpoint.edu/attacks-against-hospitals-cultural-property-broad/>, Erişim Tarihi 09 Temmuz 2023.

Kremen v. Cohen, 337 F.3d 1024 (9th Cir.2003).

Kubo Macak, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, 48(1), 2015, s. 55-80.

Lancelot J, "Cyber-diplomacy: Cyberwarfare and the Rules of Engagement", *Journal of Cyber Security Technology*, 4(4), 2020, s. 240-254.

Lehto M, *International Law and Cyberspace: Finland's National Positions*, Finnish Ministry for Foreign Affairs, 2020.

Lemley M, "Property, Intellectual Property, and Free Riding", *Texas Law Review*, 83(4), 2005, s. 1031-1076.

Liivoja R/McCormack T, "Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello", *Yearbook of International Humanitarian Law*, 15(1), 2012, s. 45-58.

Marinotti J, "Tangibility as Technology", *Georgia State University Law Review*, 37(1), 2021, s. 2-68.

McCormack T, "International Humanitarian Law and the Targeting of Data", *International Law Studies*, 94(1), 2018, s. 221-240.

McKenzie S, *Disputed Territories and International Criminal Law: Israeli Settlements and the International Criminal Court*, Routledge, 2019.

National Provincial Bank Ltd v Ainsworth [1965] AC 1175.

New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace*, Department of the Prime Minister and Cabinet, 2020.

Newton M, "A Radical Reimagining of the Concept of Attack", *Articles of War*, 2020, <https://lieber.westpoint.edu/radicalreimagining-attack-ntaganda/>, Erişim Tarihi 09 Temmuz 2023.

Norwegian Chief of Defence, *Manual on the Law of Armed Conflict*, Department of Security Policy at The Norwegian Ministry of Defence, 2013.

Organisation of American States, *Improving Transparency: International Law and State Cyber Operations, Fifth Report, Presented by Professor Duncan B. Hollis ('Hollis Report')*, OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 Ağustos 2020.

Oxford Dictionaries, *Oxford English Dictionary*, Oxford University Press, 2019.

Peat D, *Comparative Reasoning in International Courts and Tribunals*, Cambridge University Press, 2019.

Prosecutor v. Zdravko Mucic aka "Pavo", Hazim Delic, Esad Landzo aka "Zenga", Zejnil Delalic (Trial Judgement), IT-96-21-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 16 November 1998.

Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia) (Provisional Measures), ICJ Reports (2014).

R v Cox (2004) 21 CRNZ 1.

Regulation (EU) 2016/679 (General Data Protection Regulation)

Ritter J/Mayer A, "Regulating Data as Property: A New Construct for Moving Forward", *Duke Law and Technology Review*, 16(1), 2017, s. 220-277.

Robles F, "Hackers Target Florida's Town Water Supply, Raising Level of Harmful Chemical", *The New York Times*, 2021, <https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html>, Erişim Tarihi 09 Temmuz 2023.

Ruscoe v Cryptopia Limited (in liquidation) [2020] NZHC 728.

Sadat L/Jolly J, "Seven Canons of ICC Treaty Interpretation: Making Sense of Article 25's Rorschach Blot", *Leiden Journal of International Law*, 27(3), 2014, s. 755-788.

Sandoz Y/Swinarski C/Zimmerman B, *Commentary on the Additional*

Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, International Committee of the Red Cross, 1987.

Schmitt M, "The Notion of Objects during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review*, 48(1), 2015, s. 81-109.

Schmitt M, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations", *International Review of the Red Cross*, 101(910), 2019, s. 333-355.

Schmitt M, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2. Bası, Cambridge University Press, 2017.

Schondorf R, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations", *International Law Studies*, 97(1), 2021, s. 396-406.

Şen E, "Hırsızlık Suçları", *Ankara Barosu Dergisi*, 3(1), 2012, s. 321-357.

The General Staff of the Iranian Armed Forces, "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace", 2020, <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>, Erişim Tarihi 10 Temmuz 2023.

The IG Farben and Krupp Trials, United States Military Tribunal, 14 August 1947–29 July 1948 and 17 November 1947–30 June 1948, in Law Reports of the Trials of War Criminals, Vol. X (1949).

Thyroff v Nationwide Mutual Insurance Co 8 NY 3d 283, at 292.

Türk Dil Kurumu, "Türk Dil Kurumu Sözlükleri", <https://sozluk.gov.tr/>, Erişim Tarihi 12 Temmuz 2023.

Wright J, *Cyber and International Law in the 21st Century*, Attorney General's Office, 2018.