T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

AVRUPA SİBER SUÇLAR SÖZLEŞMESİ ÇERÇEVESİNDE ADLİ YARDIMLAŞMA

YÜKSEK LİSANS TEZİ

Mücahid ÖZBEK

Tez Danışmanları:
Yrd. Doç. Dr. E. Eylem AKSOY RETORNAZ
Yrd. Doç. Dr. Murat Volkan DÜLGER

EYLÜL 2015

T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

AVRUPA SİBER SUÇLAR SÖZLEŞMESİ ÇERÇEVESİNDE ADLİ YARDIMLAŞMA

YÜKSEK LİSANS TEZİ

Mücahid ÖZBEK

Tez Danışmanları:
Yrd. Doç. Dr. E. Eylem AKSOY RETORNAZ
Yrd. Doç. Dr. Murat Volkan DÜLGER

EYLÜL 2015

ÖNSÖZ

İlk kapsamlı akademik çalışmam olan bu yüksek lisans tez çalışması, yorucu olduğu kadar öğretici de olan uzun bir sürecin meyvesi olarak meydana geldi. Akademik kriterlere uygun, alanda daha önce yapılmış çalışmaları dikkate alan ve bunların üzerine yeni bir şeyler söyleyen, böylelikle alanın daha iyi anlaşılmasına katkı sağlayan bir çalışma ortaya koymaya çalıştım; umarım başarılı olabilmişimdir. Çalışmanın beğenilmesini ve faydalı olmasını dilerim.

Tez çalışmamda büyük pay sahibi olan, bu süreçte her türlü destek ve ilgilerini her an hissettiğim değerli danışman hocalarım Sayın Yrd. Doç. Dr. Emine Eylem AKSOY RETORNAZ ve Sayın Yrd. Doç. Dr. Murat Volkan DÜLGER'e teşekkürlerimi sunmayı bir borç bilirim. Gerçekten bu çalışmadaki tüm eksiklikler bana ait olmakla birlikte, çalışmanın tüm olumlu yönlerinin altında onların imzasının olduğu söylenebilir.

Hayatta büyük küçük tüm başarılarımın gerçek mimarı olan sevgili anne babam Tazegül ÖZBEK ve Hayrettin ÖZBEK'i de anmak, minnet ve şükranlarımı dile getirmek istiyorum; arkamda varlığınızı ve desteğinizi hissetmek paha biçilemez, iyi ki varsınız.

İÇİNDEKİLER

İkinci Bölüm
AVRUPA SİBER SUÇLAR SÖZLEŞMESİ

Üçüncü Bölüm
AVRUPA SİBER SUÇLAR SÖZLEŞMESİNDE ULUSLARARASI ADLİ İŞBİRLİĞİ

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

ASEAN : Güney Doğu Asya Ülkeleri Birliği

ASENAPOL : Güney Doğu Asya Ülkeleri Polis Müdürleri Derneği

bkz. : Bakınız

CDPC : Avrupa Siber Suç Sorunları Komitesi

CDPC : Avrupa Suç Sorunları Komitesi

CİYAKAS : Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi

CMK : 5271 sayılı Ceza Muhakemesi Kanunu

C-PROC : Avrupa Konseyi Siber Suç Program Ofisi

ENISA : Avrupa Birliği Bilgi ve Ağ Güvenliği Ajansı

EUROJUST : Avrupa Birliği Adli İşbirliği Örgütü

EUROPOL : Avrupa Polis Ofisi

FSEK : 5846 sayılı Fikir ve Sanat Eserleri Kanunu

INTERPOL : Uluslararası Polis Teşkilatı

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

m. : Madde

MÜHFHAD : Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi

Nyuj Int'L L. & Pol. :

OECD : Ekonomik İşbirliği ve Kalkınma Örgütü

OSCE : Avrupa Güvenlik ve İşbirliği Örgütü

par. : Paragraf

PC-CY : Siber Alemde İşlenen Suçlar Uzmanları Komitesi

s. : Sayfa

Sözleşme : Avrupa Siber Suçlar Sözleşmesi

sy. : Sayı

T- CY	: Siber Suçlar Sözleşmesi Komitesi
TCK	: 5237 sayılı Türk Ceza Kanunu
UHDİGM	: Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü
UNODC	:Birleşmiş Milletler
vb.	: Ve benzeri
vd.	: Ve devamı

RESUME

Le sujet de cette étude est la coopération judiciaire dans le cadre de la Convention Européenne sur la Cybercriminalité. L'objectif de l'étude est de contribuer à une meilleure compréhension du régime de coopération judiciaire qui devait être établi par la Convention et les obligations des Etats contractants. Le sujet est examiné sous trois chapitres : Le premier chapitre présente les problèmes rencontrés sur la lutte contre la cybercriminalité et la nécessité de la coopération internationale; Le deuxième chapitre examine la Convention européenne sur la cybercriminalité; et enfin le troisième chapitre traite du régime de la coopération judiciaire prévu par la Convention.

Cybercriminalité, qui signifie les crimes commis par ou contre les systèmes d'information et passe la plupart du temps sur l'Internet, a des caractéristiques spécifiques en raison de la contexture sui generis de l'Internet et d'autres systèmes d'information. Pour cette raison, à droite avec les mesures de police classiques en deçà, également les mesures d'enquête traditionnelles restent incapables dans la lutte contre la cybercriminalité. De plus, même si les toutes les mesures nécessaires soient prises sur le plan national, ils sont condamnés à l'échec en raison de la caractéristique transfrontalière de la cybercriminalité. Ci-joint, la nécessité de la coopération internationale émerge.

Augmentation quantitative et qualitative de la cybercriminalité fait la cybersécurité un des sujets chauds de la politique de sécurité des Etats et par conséquent il est devenu l'une des priorités de la sécurité de la société internationale. La cybercriminalité, qui ignorent les frontières nationales dans ses origines et les conséquences, fait de la coopération internationale obligatoire. Pour cette raison, de nombreuses organisations internationales, tant civils et politiques, le travailent par le biais de la préparation des conventions, des ateliers et des rapports, pour la création et le renforcement de la coopération internationale dans la lutte contre la cybercriminalité.

La lutte contre la cybercriminalité a quelques difficultés sur la base de la structure technique du cyberespace et la cybercriminalité, comme; sui generis contexture du cyberespace, cybercriminalité étant une notion relativement nouvelle et en renouvelant continuellement, la collecte de preuves et de processus d'évaluation nécessitant l'ingénierie sur le terrain, anonymat des acteurs, une résistance de commande de la technique de transmission de données et distance entre auteurs et victimes. En plus de cela, il ya des difficultés sur la base des instruments juridiques comme; l'insuffisance des législations nationales, conflits de compétence, lois problématiques d'assistance mutuelle et dissonance des systèmes judiciaires différents.

La lutte contre la cybercriminalité serait à l'échelle internationale ou aurait aucune chance, comme indiqué à l'unanimité dans la doctrine. Sur d'autres termes, la coopération internationale est pas un "devrait", mais "doit" condition de la lutte

contre la cybercriminalité. Prévention, enquête et le procès de la cybercriminalité nécessitent la coopération internationale.

Malgré le décalage de motivation entre les Etats en raison de préoccupations que ces mécanismes de coopération pourraient être l'objet de manipulations à des fins de renseignement et d'espionnage, la coopération internationale dans la lutte contre la cybercriminalité est inévitable dans le visage de gravité de la menace posée par la cybercriminalité et le manque d'impossibilité de succès des tentatives nationales. En conséquence de l'inévitabilité de la coopération internationale, il existe de nombreuses institutions et initiatives au niveau international, ainsi que des textes juridiques aux fins de l'établissement et le renforcement de la coopération internationale.

La Convention européenne sur la cybercriminalité a été préparé dans le corps du Conseil de l'Europe par les Etats membres et observateurs. La Convention, signée en 2001, est le premier instrument juridique international bondissant sur la lutte contre la cybercriminalité. En étant le premier instrument juridique et son vaste contenu, la Convention est étiqueté comme le texte juridique le plus important sur le terrain.

La Convention définit une série d'obligations à respecter par les parties contractantes au niveau national et il traite de la coopération judiciaire en vue d'organiser la lutte commune des parties contractantes, en collaboration contre la cybercriminalité. La Convention, en imposant les mesures à prendre au niveau national vise à rendre les lois nationales d'un niveau suffisant et à les harmoniser. La partie la plus important de la Convention est la coopération judiciaire internationale. Parce que, autant que les lois nationales seraient habilitées et harmonisée, mais un instrument juridique mécanisme concret pour mener à bien la coopération judiciaire est nécessaire afin d'être en mesure de répondre au problème mondial de la cybercriminalité.

Bien que la Convention dispose la coopération judiciaire principalement par les dispositions spécifiques dédiées à la coopération judiciaire et en particulier à l'assistance mutuelle, ces dispositions ne sont pas indépendantes de celles qui régissent les mesures à prendre au niveau national. Parce que le but ultime des mesures à prendre au niveau national est de fournir une infrastructure appropriée pour une coopération judiciaire effective par les qualifications et l'harmonisation des lois nationales. Voilà pourquoi, dans cette étude de la structure générale et mesure à prendre au niveau national en termes de droit pénal matériel et de procédure sont examinées pouvoirs avant d'entrer dans les dispositions de coopération judiciaire.

La convention a trois objectifs principaux: 1) Permettre d'harmoniser les législations nationales en fournissant une définition commune de certains crimes ; 2) Assurer l'uniformité entre les différentes législations nationales grâce à la détermination de pouvoirs procéduraux communs qui cadrerait la caractéristique spécifique du cyberespace et de faciliter les enquêtes en matière de cybercriminalité; 3) offrir un régime efficace de la coopération judiciaire, à la fois traditionnelle et moderne, et de rendre son application possible.

La Convention européenne sur la cybercriminalité a quatre chapitres et quarante-huit articles. Les chapitres sont les suivants: (I) les définitions; (II) Mesures à prendre au niveau nationale - du droit pénal matériel et de droit de procédure pénale; (III) la coopération internationale ; et (IV) des dispositions finales.

Le premier chapitre comprenant le premier article et intitulé «Définitions» donne les définitions des quatre principales notions souvent ayant lieu dans la Convention. Ces notions sont; système d'information, des données d'information, fournisseur de services, et des données de trafic. Il n'y a pas unanimité sur les définitions de ces notions dans la pratique, ni dans la doctrine. Les définitions prévues par la Convention de ne pas apporter une obligation pour l'adaptation de la législation nationale pour les Etats parties; ils sont consultatif.

Dans le deuxième chapitre intitulé «Mesures à prendre au niveau national", premièrement définitions de certains crimes sont donnés (articles 2-12), puis certains pouvoirs de procédure et principes de compétence sont donnés place en termes de droit de procédure pénale (articles 13-22). Il n'y a pas une telle obligation de copier ces dispositions in extenso à la législation nationale.

La Convention apporte les normes minimales à respecter. Les parties contractantes sont libres de prendre les dispositions nécessaires dans leur législation nationale en conformité avec leur système de droit national. Ils ont la possibilité d'organiser les crimes et les pouvoirs de procédure avec une formulation différente de celle de la Convention et ils peuvent adopter d'autres crimes et pouvoirs procéduraux ainsi. La raison derrière l'évitement des rédacteurs de la Convention de déterminer strictement les éléments structurels des crimes et les pouvoirs de procédure et de les imposer aux parties contractantes est de rendre les dispositions de la Convention pour être applicable pour les crimes et les procédures à être levées à l'avenir. Bien que le Rapport explicatif de la Convention donne quelques conseils de base, il n'y a aucune explication claire et pratique sur la façon dont les parties contractantes devraient adopter ces mesures à prendre au niveau national. L'absence de dispositions détaillées et Directive sur les mesures à prendre au niveau national est un facteur négatif pour l'objectif très primaire de la Convention, à savoir, la qualification et l'harmonisation des lois nationales.

Le but principal de la Convention européenne sur la cybercriminalité est de permettre une lutte collective contre la cybercriminalité dans l'harmonie et la collaboration. En fait, les mesures imposées à prendre au niveau national, à la fois sur le droit pénal matériel et de droit pénal procédural servent à cette fin. Elle vise que ces mesures fournissent une infrastructure pratique pour collaboration et la coopération. Toutefois, la qualification et l'harmonisation des seules lois nationales ne sont pas suffisantes pour une lutte contre la cybercriminalité doit être menée au niveau international. Par conséquent, il est nécessaire d’apporter des instruments et mécanismes juridiques applicables pour faire l'assistance mutuelle possible entre les autorités de différentes nationalités sur les enquêtes transnationales de la cybercriminalité.

Dans le troisième chapitre intitulé «Coopération internationale», la coopération judiciaire est disposée. Dans ce chapitre, les conditions générales de l'application de pouvoirs procéduraux mentionnés ci-dessus sont déterminées.

L'objectif de la Convention est pas remplacer les conventions et les traités existants sur la coopération judiciaire, mais de les compléter. La Convention, qui vise principalement à être appliquée dans l'intégrité des régimes de coopération existants, détermine les principes et les règles à appliquer en l'absence de tout autre instrument applicable. De cette façon, tous les traités et conventions de coopération actuels sont maintenus valide et applicable et la Convention prévoit un régime substitut de coopération ou d'un régime de sauvegarde en d'autres termes. En outre, les pouvoirs

de procédure réglementés dans la deuxième partie de la deuxième chapitre sont soumis à des dispositions spécifiques d'assistance mutuelle. Les parties contractantes, non seulement l'adoptant ces pouvoirs de procédure dans leurs législations nationales, mais aussi de les rendant disponibles pour l'assistance mutuelle, offriraient ces pouvoirs au service des autorités étrangers sur demande d'assistance mutuelle.

La Convention préfère être appliquée dans les régimes actuels de coopération au lieu de les remplacer. En plus de cela, il apporte substitut régime en déterminant les principes et les règles à appliquer en l'absence de tout autre instrument applicable. Les dispositions spécifiques d'assistance mutuelle ne sont que les reflets de pouvoirs procéduraux à accorder au droit national dans la loi sur l'assistance mutuelle. Ces pouvoirs pourraient être appliqués dans le cadre de tout autre instrument d'assistance mutuelle qui ne contient pas de restriction en la matière étant donné que ces dispositions sont déjà données lieu dans les lois nationales. Le vrai rôle de la Convention est de fournir une garantie contre le cas où une règle internationale ou nationale sur l'assistance mutuelle interdit l'assistance mutuelle sur ces sujets.

La Convention ne fonctionne pas comme il est censé être en raison de la qualité secondaire de ses dispositions d'assistance mutuelle. Surtout, l'assistance mutuelle sur la conservation rapide de données stockées peut être triste de ne pas existant. La solution à ce problème commence avec l'adoption et l'application des outils nécessaires dans les lois nationales.

En droit turc, l'assistance mutuelle et la coopération internationale judiciaire en général sont menées dans le cadre des traités internationaux bilatéraux ou multilatéraux signés et ratifiés sur ces questions et le principe de la criminalité mutuelle en l'absence de traité international applicable. Le législateur turc ne préfère pas faire une loi distincte réglementant la coopération judiciaire et d'assistance mutuelle contrairement allemands, autrichiens, suisses et les législateurs qui adoptent une loi distincte.

Il n'y a aucune législation nationale régissant la façon dont les enquêteurs nationaux devraient agir et procédures à suivre dans le cas où une autorité turque besoin d'une opération d'enquête dans un pays étranger, autrement dit l'assistance mutuelle internationale. À cet égard, il n'y a pas de cadre commun à appliquer. Différentes pratiques de coopération sont soumis à un grand nombre de différents traités internationaux bilatéraux ou multilatéraux. Bien qu'il n'y ait pas de base juridique pour la coopération judiciaire en général, certaines dispositions relatives à l'extradition sont donnés dans l'article 38 de la Constitution Turque et l'article 18 du Code Pénal Turc.

ABSTRACT

The subject of this study is the judicial cooperation within the frame of European Cybercrime Convention. The goal of the study is to contribute to a better understanding of the judicial cooperation regime that supposed to be established by the Convention and the obligations of the contracting states thereof. The subject is examined under three chapters: The First Chapter presents the problems encountered on the fight against cybercrime and the need for international cooperation; The Second Chapter examines the European Cybercrime Convention and finally The Third Chapter address the judicial cooperation regime provided by the Convention.

Cybercrime, which are the crimes committed through or against information systems and happening mostly on the Internet, have some specific characteristics because of the sui generis contexture of the Internet and other information systems.

Because of this, right along with the conventional police measures falling short, also the traditional investigative measures remain incapable in the fight against cybercrime. Furthermore, even if the all necessary measures are taken on the national level, they are condemned to fail due to the transboundary characteristic of cybercrime. Herewith, the need for international cooperation emerges.

Quantitative and qualitative increase of cybercrime made the cybersecurity one of the hot topics of the security policies of states and consequently it became high on the international society's security agenda. Cybercrime, which ignore the national borders in its origins and consequences, made the international cooperation obligatory. For this reason, many international organizations, both civil and political, work, through preparation of conventions, workshops and reports, for the establishment and strengthening of the international cooperation in the fight against cybercrime.

The fight against cybercrime has some difficulties based on technique structure of the cyberspace and cybercrime, such as sui generis contexture of cyberspace, cybercrime being a notion comparatively new and constantly renewing, evidence collection and evaluation process requiring field engineering, anonymity of actors, control resistance of data transmission technique, and distance between perpetrators and victims. In addition to these, there are difficulties based on legal instruments, such as insufficiency of national legislations, jurisdiction conflicts, problematical mutual assistance laws and dissonance of different judicial systems.

The fight against cybercrime would be on international scale or would have no chance, as unanimously indicated in the doctrine. On other words, international cooperation is not a "should", but "must" condition of the fight against cybercrime. Prevention, investigation and trial of cybercrime necessitate international cooperation.

Though the shift of motivation among states due to concerns that those cooperation mechanisms could be subject to manipulation for the purpose of intelligence and espionage, international cooperation in the fight against cybercrime is inevitable in the face of graveness of the threat posed by cybercrime and lack of impossibility of success of national attempts. As a result of inevitability of international cooperation, there are many institutions and initiatives on international

level, as well as legal texts for the purpose of establishment and strengthening of international cooperation.

The European Cybercrime Convention was prepared within the body of Council of Europe by member and observer states. The Convention, signed in 2001, is the first bounding international legal instrument on the fight against cybercrime. By being the first legal instrument and its extensive content, the Convention is labeled as the most important legal text on the field.

The Convention defines a series of obligation to be respected by contracting parties at national level and address the judicial cooperation in order to organize the common fight of contracting parties in collaboration against cybercrime. The Convention, by imposing the measures to be taken at national level aims to bring national laws into a sufficient level and harmonize them. The most conspicuous part of the Convention is the international judicial cooperation. Because, as much as the national laws would be habilitated and harmonized, yet a concrete legal instrument and mechanism to carry out judicial cooperation is needed in order to be able to respond the global cybercrime problem.

Although the Convention disposes the judicial cooperation primarily by the specific provisions dedicated to judicial cooperation and especially to mutual assistance, these provisions are not independent from those regulating the measures to be taken at national level. Because the ultimate goal of the measures to be taken at national level is to provide an appropriate infrastructure for an effective judicial cooperation through qualifying and harmonizing national laws. This is why, in this study the general structure and measure to be taken at national level in terms of substantive criminal law and procedural powers are examined before getting into judicial cooperation provisions.

The convention has three main objectives: 1) To make it possible to harmonize national legislations through providing common definition of certain crimes; 2) To provide uniformity among different national laws through determining common procedural powers that would fit the specific characteristic of the cyberspace and facilitate cybercrime investigations; 3) To offer an effective judicial cooperation regime, both traditional and modern, and to make its application possible.

The European Cybercrime Convention has four chapters and forty-eight articles. The Chapters are as following: (I) Definitions; (II) Measures to be taken at national level- substantive criminal law and procedural criminal law; (III) International Cooperation and (IV) Final provisions.

In the First Chapter consisting of the first article and titled “Definitions” give the definitions of four main notions that frequently given place in the Convention. These notions are; information system, information data, service provider, and traffic data. There is no unanimity on the definitions of these notions in the practice, nor in the doctrine. The definitions provided by the Convention do not bring an obligation for adaptation of national law for party states; they are advisory.

In the Second Chapter titled “Measures to be taken at national level”, first definitions of certain crimes are given (articles 2-12), then some procedural powers and jurisdictional principles given place in terms of procedural criminal law (articles

13-22). There is not such an obligation to copy these provisions verbatim to national law.

The Convention brings the minimum standards to be respected. The contracting parties are free to make the necessary arrangements in their national law in line with their national law system. They have the opportunity to arrange the crimes and procedural powers with a different formulation then the Convention's and they can adopt further crimes and procedural powers as well. The reason behind the avoidance of the drafters of the Convention from strictly determining the structural elements of the crimes and procedural powers and imposing them to the contracting parties is to make the Convention provisions to be applicable for the crimes and procedures to be emerged in the future. Although the Explanatory Report of the Convention gives some basic advices, there is no clear and practical explanation on how the contracting parties would adopt these measures to be taken at national level. The lack of detailed and directive provisions on the measures to be taken at national level is a negative consideration for the very primary objective of the Convention namely, qualifying and harmonizing national laws.

The main purpose of the European Cybercrime Convention is to make it possible a collective fight against cybercrime in harmony and collaboration. Actually, the measures imposed to be taken at national level, both on substantive criminal law and procedural criminal law serve this purpose. It is aimed that these measures provide a convenient infrastructure for collaboration and cooperation. However, qualification and harmonization of national laws alone is not sufficient for a fight against cybercrime to be conducted at international level. Therefore, there is need for applicable legal instruments and mechanisms to make the mutual assistance possible between investigators from different nationalities on the transnational investigations of cybercrime.

In the Third Chapter titled "International Cooperation", the judicial cooperation is disposed. In this chapter, the general terms of the application of above-mentioned procedural powers are determined.

The goal of the Convention is not replace the existing conventions and treaties on judicial cooperation but to supplement them. The Convention, primarily aiming to be applied in integrity with existing cooperation regimes, determines the principles and rules to be applied in the absence of any other applicable instrument. That way, all current cooperation treaties and conventions are kept valid and applicable and the Convention provides a substitute cooperation regime or a backup regime in other words. Also, the procedural powers regulated in the second part of the Second Chapter are subjected to some specific mutual assistance provisions. The Contracting parties, not only adopting these procedural powers in their national laws but also making them available for mutual assistance, would offer these powers in the service of foreign investigators upon mutual assistance request.

The Convention prefers to be applied within the current cooperation regimes instead of replacing them. In addition to this, it brings substitute regime determining principles and rules to be applied in the absence of any other applicable instrument. The specific mutual assistance provisions are nothing but the reflections of procedural powers to be granted at national law in the mutual assistance law. These powers could be applied within the context of any other mutual assistance instrument that do not contain subject matter restriction as these provision are already given place in the national laws. The true role of the Convention is to provide a guaranty

against the case that an international or national rule on mutual assistance prohibits the mutual assistance on these subjects.

The Convention is not functioning as it is supposed to be because of the secondary quality of its mutual assistance provisions. Especially, the mutual assistance on the expedited preservation of stored data can be sad not existing. The solution for this problem begins with the adoption and application of necessary tools in national laws.

In Turkish law, the international mutual assistance and judicial cooperation in general is conducted within the scope of bilateral or multilateral international treaties signed and ratified on these matters and the mutual criminality principle in the absence of applicable international treaty. The Turkish legislator does not prefer making a separate law regulating judicial cooperation and mutual assistance unlike German, Austrian, and Swiss legislators which adopt a separate law.

There is no national legislation regulating how the national investigators should act and procedures to be followed in case that a Turkish authority needs an investigatory operation in a foreign land, namely international mutual assistance. In this regard there is no common frame to be applied. Different cooperation practices are subject to a large number of different bilateral or multilateral international treaties. Although there is no legal base for judicial cooperation in general, some provisions on extradition are given place in the article 38 of the Turkish Constitution and the article 18 of Turkish Criminal Code.

ÖZET

Bu çalışmanın konusu Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli İşbirliğidir. Çalışmada Sözleşme'nin tesis etmeye çalıştığı adli işbirliği rejiminin ve bu çerçevede taraf devletlerin yerine getirmek zorunda oldukları yükümlülüklerin anlaşılması amaçlanmaktadır. Konu, üç ana bölüm altında ele alınmaktadır: Birinci bölümde; siber suçlarla mücadelede sorunlar ve uluslararası işbirliği ihtiyacı ortaya konmakta, İkinci Bölümde; Avrupa Siber Suçlar Sözleşmesi incelenmekte ve nihayet Üçüncü Bölümde; Sözleşme'de öngörülen adli işbirliği rejimi ortaya konmakta ve değerlendirilmektedir.

Bilişim sistemleri aracılığıyla ya da bu sistemlere karşı işlenen ve genellikle internette işlenen suçlar olan siber suçlar, internetin ve diğer bilişim teknolojilerinin kendine özgü yapısından kaynaklı teknik bazı özellikler gösterirler. Bu bağlamda; suçla mücadelede geleneksel polisiye tedbirlerin yetersiz kalmasının yanı sıra, suçların soruşturmasında geleneksel ceza muhakemesi tedbirleri yetersiz kalmaktadırlar. Dahası siber suçların sınır aşan yapısı nedeniyle ulusal düzlemde alınan tedbirler çoğunlukla yetersiz ve anlamsız kalmaktadır. Bu durumda uluslararası işbirliği ihtiyacı ortaya çıkmaktadır.

Siber suçların sayıca ve zarar verme kabiliyeti olarak niteliksel artışı sonucu siber güvenlik kavramı ve siber suçlarla mücadele, son yıllarda devletlerin güvenlik gündemlerinin en önemli konularından birisi haline gelmiş, uluslararası toplum açısından da gündeminin ilk sıralarında yerini almıştır. Etkileri ve kaynakları itibariyle ulusal sınırları yok sayan siber suçluluk, uluslararası düzlemde işbirliğini ve ortak mücadeleyi zorunlu hale getirmiştir. Pek çok uluslararası siyasi ve sivil örgüt siber suçlarla mücadelede uluslararası işbirliğini sağlamaya ve güçlendirmeye yönelik çalışmalar yürütmekte; sözleşmeler, çalıştaylar ve raporlar hazırlamaktadır.

Siber suçlarla mücadele siber alemin kendine has yapısı, siber suçluluğun yeni bir kavram olması ve sürekli olarak kendini yenilemesi, siber alemin süjelerinin anonim kalma şansı ve veri iletim tekniğinin kontrol direnci, delil elde etme ve değerlendirme süreçlerinin uzmanlık gerektirmesi ve faille mağdur arasında mekansal mesafe bulunması gibi siber alemin ve siber suçların teknik yapısından kaynaklı zorluklar söz konusudur. Bunlara ilave olarak ulusal mevzuatların yetersiz olması, uluslararası yetki sorunları, adli yardımlaşma hukukuna ilişkin sorunlar ve hukuk sistemlerinin uyum direnci gibi hukuki zorluklar da siber suçlarla mücadeleyi zorlaştırmaktadır.

Doktrinde belirtildiği gibi, "siber suçlara karşı mücadele ya global olacaktır ya da hiç anlamı yoktur". Yani siber suçlarla mücadelede uluslararası işbirliğinin tesis edilmesi "olursa faydalı olur" şeklinde ifade edilebilecek bir tavsiye değil, "olmazsa olmaz" bir koşuldur. Siber suçların soruşturulabilmesi, kovuşturulabilmesi ve siber suçluluğun önlenebilmesi uluslararası işbirliğinin etkin bir şekilde yürütülmesini gerektirir.

Uluslararası düzlemde işbirliği mekanizmalarının istihbarat ve casusluk faaliyetleri şeklinde kötüye kullanılması yönündeki endişelerden dolayı devletlerde siber suçlarda işbirliği yönünde bir niyet kayması söz konusu olsa da, siber suçluluğun arz ettiği tehlike ve ulusal düzlemde mücadelenin başarısızlığa mahkum olması karşısında uluslararası işbirliği kaçınılmazdır. Uluslararası işbirliğinin kaçınılmaz olması nedeniyle, günümüzde siber suçlulukla mücadelede işbirliğini sağlamaya yönelik uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır.

Avrupa Siber Suçlar Sözleşmesi, Avrupa Konseyi bünyesinde, üye ve gözlemci devletler tarafından hazırlanmıştır. Sözleşme, 2001 yılında imzalanmış olup, siber suçlarla mücadele alanındaki ilk bağlayıcı uluslararası düzenlemedir. Sözleşme, hem ilk olması hem de kapsamlı içeriği itibariyle alanındaki en önemli uluslararası hukuki metin olarak görülmektedir.

Sözleşme, taraf devletlere siber suçlarla mücadele konusunda ulusal düzeyde uymaları gereken bir dizi yükümlülük getirmekte ve tarafların siber suçlara karşı işbirliği içinde mücadele edebilmelerini sağlamak amacıyla uluslararası adli işbirliğini düzenlemektedir. Ulusal düzeyde alınması öngörülen önlemlerle taraf devletlerin ulusal mevzuatlarının siber suçlarla mücadele edebilecek yeterli seviyeye getirilmesi ve uyumlulaştırılması amaçlanmaktadır. Sözleşme'nin en dikkat çeken fonksiyonu ise siber suçlarla mücadele özelinde kurmaya çalıştığı uluslararası adli işbirliği rejimidir. Zira her ne kadar ulusal mevzuatlar yeterli ve uyumlu hale getirilse de, global siber suç sorunuyla etkin ve işbirliği içinde mücadele edilebilmesi için adli işbirliğinin somut bir düzenleme ve mekanizma çerçevesinde yürütülmesi gerekir.

Uluslararası adli işbirliği, temel olarak Sözleşme'de yer alan adli yardımlaşma hükümleri aracılığıyla sağlanmakla birlikte; öngörülen adli yardımlaşma hükümleri maddi hukuka ve usul hukukuna ilişkin önlemlerden bağımsız değildir. Zira bu önlemler, ulusal mevzuatları siber suçlarla mücadelede yeterli bir seviyeye çekmeyi ve birbirleriyle uyumlulaştırmayı, bu sayede de etkin bir uluslararası adli işbirliği sistemine uygun alt yapıyı sağlamayı amaçlamaktadır. Bu nedenle Sözleşme'nin adli işbirliği konusunda önerdiği sistemin incelenmesinden önce, genel olarak Sözleşme'nin yapısını, ulusal düzeyde alınmasını öngördüğü maddi ceza hukukuna ve usul hukukuna ilişkin önlemler incelenmektedir.

Sözleşme'nin başlıca üç amacı olduğu söylenebilir: 1) Bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını mümkün kılmak; 2) Siber suçların soruşturulması açısından, siber aleme uygun düşen ortak usul kurallarını tanımlayarak, devletler arasındaki muhakeme kurallarının yeknesaklaştırılmasını mümkün kılmak; 3) Hem geleneksel hem de yeni türden uluslararası işbirliği yöntemlerini belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını mümkün kılmak.

Avrupa Siber Suç Sözleşmesi, dört bölüm ve kırk sekiz maddeden oluşmaktadır, bunlar sırasıyla (I) Terimler; (II) Ulusal düzeyde alınacak önlemler - maddi hukuk ve usul hukuku; (III) Uluslararası işbirliği ve (IV) Diğer hükümlerdir.

Sözleşme'nin 1. maddesinden ibaret olan "Terimler" başlıklı Birinci Bölümde, Sözleşme'de kullanılan dört ana terime ilişkin tanımlar yer almaktadır. Bunlar; bilişim sistemi, bilişim verisi, hizmet sağlayıcı ve trafik verisi terimleridir. Uygulama ve öğretide yeknesak tanımları bulunmayan bu kavramların Sözleşme kapsamında nasıl anlaşılması gerektiğini göstermesi bakımından yer verilen bu tanımlar, taraf devletler bakından ulusal mevzuata aktarma yükümlülüğü içermeyip yol gösterici niteliktedir.

"Ulusal Düzeyde Alınacak Önlemler" başlıklı İkinci Bölümde; öncelikle maddi ceza hukuku bağlamında birtakım suç tiplerine (m. 2-12), ardından da ceza muhakemesi hukuku bağlamında birtakım usuli tedbirlere ve yargı yetkisi meselesine dair bazı genel ilkelere (m. 13-22) yer verilmektedir. Sözleşme'nin bu bölümünde yer verilen suç tipleri ve muhakeme tedbirlerini bire bir kopyalayarak ulusal mevzuata uyarlama zorunluluğu bulunmamaktadır.

Sözleşme, ulusal düzeyde alınacak önlemler noktasında minimum bir standart belirlemekte, taraf devletlerin bu standardı sağlamak koşuluyla bu suç tiplerini ve usuli yetkileri farklı bir formülasyonla düzenlemelerine veya başkaca siber eylemleri suç haline getirmelerine ve gerekli görülen farklı muhakeme tedbirlerini benimsemelerine imkan tanımaktadır. Sözleşmenin öngördüğü suç tiplerinin ve usuli yetkilerin yapısal unsurlarını kesin bir şekilde belirleyip taraf devletlere empoze etmemesinde, gelecekte ortaya çıkabilecek yeni suç işleme şekillerini de kapsayabilecek bir üslup benimseme kaygısı da rol oynamaktadır. Taraf devletlerin öngörülen maddi ve usuli önlemeleri ulusal mevzuatlarına ne şekilde uyarlayacakları konusunda Açıklayıcı Rapor bazı yol gösterici ilkeler içerse de, bu ilkeler son derece soyut ve yetersiz kalmaktadır. Sözleşme'nin ulusal düzeyde alınacak önlemler konusundaki bu esnek tutumu ve ilgili önlemleri yeterince detaylı olarak düzenlememesi ulusal mevzuatların yeterli ve uyumlu olası amacı bakımından önemli bir eksiklik olarak değerlendirilmektedir.

Avrupa Siber Suçlar Sözleşmesi'nin asıl amacı devletlerin global siber suç sorunuyla işbirliği ve uyum içinde mücadele etmelerini sağlamaktır. Sözleşme'nin, taraf devletlerin ulusal düzeyde almasını öngördüğü maddi hukuka ve usul hukukuna ilişkin önlemler de esasında bu amaca yöneliktir. Bu düzenlemeler sayesinde işbirliği ve uyum içinde yürütülecek ortak mücadeleye uygun bir zemin inşa edilmesi amaçlanmaktadır. Ancak ulusal mevzuatların etkin ve uyumlu bir hale getirilmesi, siber suçlarla uluslararası düzeyde mücadele edilmesi için tek başına yeterli değildir. Bunun için, sınır aşan siber suçların soruşturma ve kovuşturmalarında farklı devletlerin adli makamlarının işbirliğini mümkün kılacak uluslararası adli işbirliği mekanizmalarının da mevcut olması ve etkin bir şekilde işlemesi şarttır.

Sözleşme'nin "Uluslararası İşbirliği" başlıklı Üçüncü Bölümünde adli işbirliği ele alınmaktadır. Bu bölümde; adli işbirliğinin yukarıda anılan usuli yetkilerin kullanımı bakımından adli yardımlaşmanın çerçevesi çizilmektedir.

Sözleşme, adli işbirliğine dair mevcut diğer antlaşmaların yerini almayı değil; onları tamamlamayı amaçlamaktadır. Adli işbirliğine ilişkin diğer antlaşmalarla kurulu mevcut işbirliği rejimi kapsamında uygulanmayı hedefleyen Sözleşme, bunun yanı sıra ilgili devletler arasında bir antlaşma hükmünün bulunmaması durumunda uygulanacak ilke ve kuralları da belirlemektedir. Böylelikle, taraf devletler bakımından uluslararası adli işbirliğine yönelik tüm çok taraflı ve ikili antlaşmalar geçerliliği sürdürmekte ve uygulanmakta, Sözleşme ise ikincil nitelikte ya da diğer bir deyişle yedek bir adli yardımlaşa rejimi sunmaktadır. İkinci Bölümün İkinci Kısmında ulusal düzeyde alınması gereken usuli önlemlerin adli yardımlaşma hukukundaki yansımaları olan bazı özel düzenlemeler getirilmiştir. Taraf devletler, İkinci Bölümde yer alan usuli yetkilere mevzuatlarında yer vermenin yanı sıra, Üçüncü Bölüm uyarınca sınır aşan siber suçların yabancı devletlerce soruşturulmasında da bu yetkileri onların istifadesine sunmuş olacaktır

Sözleşme bağımsız bir adli işbirliği sistemi getirmek yerine, mevcut sistemlerin uygulanmasını tercih etmiştir. Bunun yanı sıra, uygulanabilir bir adli yardımlaşma zemini – uluslararası sözleşme veya iç hukuk normu- bulunmadığı durumlarda

uygulanacak rejimi belirlemek üzere yedek normlar konulmuştur. Sözleşme'de bunun dışında bazı özel yardımlaşma usulleri düzenlenmiş olup, aslında bunlar ulusal düzeyde tesis edilmesi gereken muhakeme tedbirlerinin, uluslararası adli yardımlaşma hukukundaki yansımalarından ibarettir. Bu tedbirler, ulusal düzeyde doğru bir şekilde tesis edilmiş olmaları halinde, konu sınırlaması getirmeyen mevcut adli yardımlaşma sözleşmeleri çerçevesinde zaten uygulanabilecektir. Sözleşme yalnızca, uluslararası ya da ulusal mevzuatın herhangi bir hükmünün söz konusu adli yardımlaşma yollarını yasaklaması ihtimaline binaen, garantör hükümler getirmektedir.

Sözleşme, adli yardımlaşma konusunda benimsediği ikincil nitelikte olma ilkesi dolayısıyla, uygulamada beklenen şekilde bir işlerlik sağlayamamaktadır. Özellikle depolanmış verilerin korunması konusunda adli yardımlaşma uygulaması yok denecek kadar azdır. Bu sorunun çözümü öncelikli olarak ulusal düzeyde bu tedbirlerin tesis edilmesi ve uygulanmasıdır.

Türk hukukunda genel olarak uluslararası adli işbirliği ve özel olarak uluslararası adli yardımlaşma, bu alanda imzalanarak kabul edilmiş çok taraflı ve iki taraflı uluslararası antlaşmalar çerçevesinde, uygulanabilir bir uluslararası antlaşmanın bulunmadığı hallerde ise karşılıklılık esasına göre yürütülmektedir. Türk kanun koyucu Almanya, Avusturya, İsviçre gibi bazı devletlerin benimsediği şekilde adli işbirliğinin çeşitli yönlerini düzenleyen bağımsız bir kanunu yürürlüğe koymayı tercih etmemiştir.

Yurtdışında gerçekleştirilmesi gereken muhakeme işlemleri konusunda, diğer bir deyişle yabancı makamlardan adli yardımlaşma talep edilirken Türk makamlarının nasıl hareket etmesi gerektiği veya yurtdışından gelen adli yardımlaşma taleplerini karşılarken Türk ulusal makamlarının takip etmesi gereken usul noktasında da yasal bir düzenleme mevcut değildir. Bu bakımdan, genel olarak uygulanabilir ortak bir çerçeve yoktur. Farklı işbirliği türleri, dayanak alınan çok taraflı ya da iki-taraflı uluslararası antlaşmalarda yer alan hüküm ve usullere tabi olmaktadır. Adli işbirliğine ilişkin genel olarak uygulanabilir yasal düzenleme bulunmamakla birlikte, Anayasa'nın 38. maddesinde ve 5237 sayılı Türk Ceza Kanunu'nun 18. maddesinde geri vermeyle ilgili hükümler yer almaktadır.

GİRİŞ

İnternet ve diğer bilişim teknolojileri, günümüzde kamu hizmetlerinin, bürokrasinin, ticari ve sosyal hayatın, kısacası hayatın hemen her alanının vazgeçilmez bir parçasıdır. Teknolojinin gelişimiyle paralel olarak giderek artan bilişim teknolojilerine bağımlılık, güvenlik sorunlarını da beraberinde getirmiştir. Teknolojik gelişmeler, bir yandan kullanıcılarına meşru faydalar sağlarken diğer yandan yeni suç tiplerinin ve bazı geleneksel suçların yeni işleniş biçimlerinin doğmasına zemin hazırlamıştır. Siber suçlar olarak ifade ettiğimiz, bilişim sistemleri aracılığıyla ya da bu sistemlere karşı işlenen suçlar sanal olarak işlenmekte ancak oldukça gerçek zararlara yol açmaktadır.

Siber suçlar, yıllık milyarlarca lira olarak ifade edilen maddi zararın yanı sıra, kamu hizmetlerinin aksaması, emek ve bilgi kayıpları, hassas verilerin ifşa olması, bireysel ya da toplumsal güvensizlik hissi gibi değeri maddi anlamda tam olarak ölçülemeyen çok ciddi manevi zararlara da yol açmaktadır. Bu nedenle siber suçluluğun önlenmesi ve siber suçların etkin bir şekilde soruşturulması devletlerin birincil gündem maddesi haline gelmiştir.

Siber suçlar, doğası gereği sınır aşan niteliktedir ve bu suçların fail, mağdur, konu vb. unsurları siyasi veya coğrafi sınırları gözetmeksizin dünyanın herhangi bir yerinde hatta aynı anda birden fazla yerinde olabilmektedir. Çoğu siber suç vakası birden çok ülkeyi, hatta tüm ülkeleri etkilemektedir. Yetkileri ulusal sınırlarla belirlenmiş soruşturma makamları bu durum karşısında çaresiz kalmakta, devletlerin tek başlarına veya birbirlerinden bağımsız olarak yürütmeye çalıştıkları mücadele genellikle başarısız olmaktadır. Siber suçlarla mücadeleyi ve özellikle siber suçların soruşturulmasını önemli ölçüde zorlaştıran bu sorunlu tablo, ancak uluslararası adli işbirliğinin kapsamlı bir şekilde tesis edilmesi yoluyla çözüme kavuşturulabilir. Siber suçlarla mücadelenin etkinliği konusunda çalışan yazarlar ve bu alanda faaliyet gösteren kuruluşlar ağız birliği ile uluslararası işbirliğine duyulan ihtiyaca vurgu yapmaktadırlar.

Avrupa Siber Suçlar Sözleşmesi, siber suçlarla mücadelede ortaya çıkan bu ihtiyacı karşılamak amacıyla kabul edilmiş, bu alandaki ilk bağlayıcı hukuki metindir. Sözleşme'nin temel amacı adli işbirliğini en geniş şekilde tesis etmektir. Sözleşme, bu amacını sağlamak üzere öncelikle, taraf devletlerin ulusal düzeyde maddi hukuka ve usul hukukuna ilişkin gerekli tedbirleri almaları yönünde bir dizi yükümlülük getirmekte, sonrasında ise adli işbirliği ve özel olarak adli yardımlaşmaya ilişkin ilkeler ve usullere yer vermektedir. Sözleşmenin tesis etmeye çalıştığı adli işbirliği sisteminin etkin bir şekilde işlemesinin birinci şartı; tüm taraf devletlerin Sözleşme'yi doğru bir şekilde yorumlayıp, gereğince uygulamalarıdır.

Türkiye, Sözleşme'yi imzalamış ve yürürlüğe koymuştur. Ancak Türk mevzuatının Sözleşme'yle uyumluluğunun sağlanması yönünde atılması gereken adımlar mevcuttur. Siber suçlarla mücadelede gerekli yasal önlemleri almada gelişmiş ülkeleri geriden takip eden Türkiye'nin, hem ulusal düzeyde gerekli korumayı sağlayabilmek hem de uluslararası hukuk uyarınca yüklenmiş olduğu sorumluluğu yerine getirmek ve parçası olmayı kabul ettiği işbirliği mekanizmasına uyum sağlamak için Sözleşme'nin gerekliklerini hızla yerine getirmesi gerekmektedir. Bu nedenle Sözleşme'nin ve öngördüğü adli işbirliği sisteminin inceleneceği bu çalışmayı yapmayı gerekli gördük.

Çalışmamızın konusu Avrupa Siber Sözleşmesi çerçevesinde adli işbirliği olup, Sözleşme'de öngörülen adli işbirliği sistemini ortaya koymayı ve Türkiye bakımından nasıl uygulanacağını belirlemeyi amaçlıyoruz. Bu doğrultuda çalışmamızda Sözleşme'nin ilgili hükümlerini incelerken yer yer Türk hukukunun ve uygulamasının Sözleşme karşısındaki durumuna değinecek ve önerilerimizi aktarmaya çalışacağız.

Çalışmamızda konuyu üç ana bölüm altında ele alacağız: 1) Siber Suçlarla Mücadelede Sorunlar ve Uluslararası İşbirliği İhtiyacı, 2) Avrupa Siber Suçlar Sözleşmesi, 3) Avrupa Siber Sözleşmesinde Uluslararası Adli İşbirliği.

Birinci Bölümde siber suçlarla mücadelede yaşanan zorlukları, sorunları ve adli işbirliği ihtiyacını ortaya koymayı ve sonrasında bu konuda öne çıkan bazı girişimleri incelemeyi amaçlıyoruz. Siber suçların yapısının anlaşılması ve bu suçlarla mücadelede teknik yapıdan kaynaklı sorunların anlaşılmasının önemli olduğu kanaatindeyiz. Bu konuda yeterli farkındalık sağlanmadan, siber suçlarla mücadeleyi mümkün kılacak gerekli mevzuatın oluşturulması ve uygulanması

mümkün olmayacaktır. Nitekim halihazırda Sözleşme'nin taraf devletler ve bunların ilgili makamlarınca doğru şekilde anlaşılamaması nedeniyle Sözleşme'nin işlevini tam olarak yerine getiremediğini görmekteyiz. Çalışmamızın asıl konusu olan adli işbirliğine duyulan ihtiyacın nedenlerini ortaya koyması itibariyle bu bölümde şu gerçeği farklı yönleriyle ele almaya çalışacağız: Siber suçlar yapıları itibariyle geleneksel suçlardan farklıdır ve bu suçlarla mücadele edebilmek için geleneksel araç ve yaklaşımlar terk edilerek yeni yöntem ve araçlara başvurulmalıdır. Sınır aşan nitelikte olan siber suçlarla mücadelede benimsenecek yöntemin en önemli unsuru da uluslararası işbirliğidir. Bu önermelerin hükümetler ve uygulamacılar tarafından anlaşılması ve benimsenmesi ile adli işbirliğinin sağlanması adına yol yarılanmış olacaktır. Bu bölümdeki tespitlerimiz birbirinin tekrarı görünümünde olabilir ancak, esasında yapmaya çalışacağımız şey aynı gerçeğin farklı yönleriyle ortaya koymaktır.

İkinci Bölümde, Avrupa Siber Sözleşmesi'nin, amaçları, ilkeleri ve öngördüğü hükümlerin bir bütün olarak anlaşılmasını amaçlıyoruz. Sözleşme, adli işbirliğinin tesis edilmesi adına öncelikle taraf devletlerin ulusal mevzuatlarının yeterli ve uyumlu hakle getirilmesini amaçlamaktadır. Sözleşme'de öngörülen suç tipleri ve muhakeme tedbirleri, yalnızca ulusal düzeyde anlam ifade etmemekte, aynı zamanda bunlar vasıtasıyla adli işbirliğinin ve özel olarak adli yardımlaşmanın temeli oluşturulmaktadır. Bu nedenle, Sözleşme'de yer alan maddi hukuka ve usul hukukuna ilişkin hükümleri ayrıntılı olarak inceleyecek ve Türk mevzuatının bu hükümler karşısındaki durumunu tespit edeceğiz.

Nihayet Üçüncü Bölümde, Sözleşme'nin öngördüğü adli işbirliği sistemini ve adli yardımlaşma rejimini inceleyeceğiz. Öncelikle belirtmek gerekir ki; Sözleşme, bağımsız bir adli işbirliği sistemi öngörmeyip, mevcut sistemlerin eksik kaldığı yönlere çözüm öneren yedek ve garantör hükümler getirmekte, adli yardımlaşma konusunda ise bazı özel yardımlaşma konularını düzenleyerek bu konularda yardımlaşmayı mümkün kılmayı amaçlamaktadır. Sözleşme'nin adli işbirliğini sağlama noktasındaki asıl önemli aracı, işbirliği ve adli yardımlaşma usullerine yönelik düzenlemeler değil, ulusal düzeyde tesis edilmesini şart koştuğu tedbirlerdir Sözleşme'nin bağımsız bir işbirliği mekanizması getirmeyip, mevcut işbirliği sözleşmelerine ve mekanizmalarına gönderme yapması ve İkinci Bölümde ilgili tedbirlerin ayrıntılı şekilde ortaya konulacak olması nedeniyle bu bölüm, ilk iki bölüme göre daha dar bir kapsamda ele alınacaktır. Bu bölümde ayrıca Türkiye

bakımından adli işbirliğinin hukuki dayanaklarını ortaya koyacak ve uygulamaya ilişkin bazı temel açıklamalar yapacağız.

Çalışmamızın sonunda, Sözleşme çerçevesinde adli işbirliğinin esaslarının, Sözleşme'nin bu konudaki hükümlerinin etkin bir şekilde uygulanması için taraf devletlere ve ulusal uygulamacılara ne gibi görevler düştüğünün anlaşılmasını amaçlıyoruz.

Birinci Bölüm
SİBER SUÇLARLA MÜCADELEDE SORUNLAR VE ULUSLARARASI İŞBİRLİĞİ İHTİYACI

Bilişim sistemleri aracılığıyla ya da bu sistemlere karşı işlenen ve genellikle internette işlenen suçlar olan siber suçlar, internetin ve diğer bilişim teknolojilerinin kendine özgü yapısından kaynaklı teknik bazı özellikler gösterirler. Bu bağlamda; suçla mücadelede geleneksel polisiye tedbirlerin yetersiz kalmasının yanı sıra, suçların soruşturmasında geleneksel ceza muhakemesi tedbirleri yetersiz kalmaktadırlar. Dahası siber suçların sınır aşan yapısı nedeniyle ulusal düzlemde alınan tedbirler çoğunlukla yetersiz ve anlamsız kalmaktadır. Bu durumda uluslararası işbirliği ihtiyacı ortaya çıkmaktadır.

Siber suçların sayıca ve zarar verme kabiliyeti olarak niteliksel artışı sonucu siber güvenlik kavramı ve siber suçlarla mücadele, son yıllarda devletlerin güvenlik gündemlerinin en önemli konularından birisi haline gelmiş, uluslararası toplum açısından da gündeminin ilk sıralarında yerini almıştır. Etkileri ve kaynakları itibariyle ulusal sınırları yok sayan siber suçluluk, uluslararası düzlemde işbirliğini ve ortak mücadeleyi zorunlu hale getirmiştir. Pek çok uluslararası siyasi ve sivil örgüt siber suçlarla mücadelede uluslararası işbirliğini sağlamaya ve güçlendirmeye yönelik çalışmalar yürütmekte; sözleşmeler, çalıştaylar ve raporlar hazırlamaktadır.

Çalışmamızın asıl konusunu teşkil eden Avrupa Siber Suç Sözleşmesi ve öngördüğü adli işbirliği rejimininin açıklanmasına geçmeden önce siber suçlarla mücadeleye ve uluslararası işbirliğine ilişkin bazı genel açıklamalar yapmak, ve bu yöndeki bazı girişimleri incelemek yerinde olacaktır. Bu bölümde siber suçlarla mücadelenin gerektirdiği özellikleri, siber suçlulukla mücadelede uluslararası işbirliğinin önemini ve özelliklerini ve siber suçlarla mücadelede uluslararası işbirliğini oluşturma ve geliştirmeye yönelik bazı girişimleri inceleyeceğiz.

A. Siber Suçların Soruşturulmasında Zorluklar ve Sorunlar

1. Siber Suçların Teknik Yapısından Kaynaklı Zorluklar

a) Siber Alemin Yapısı

Bir yandan siber suçların işlenmesindeki kolaylık, diğer yandan bunların önlenmesindeki ve soruşturulmasındaki zorluk ancak siber alemin kendine özgü yapısı ve niteliği, teknik özellikleriyle birlikte değerlendirildiğinde anlaşılabilir. Alanımız olmadığı için siber alemin işleyiş ve sisteminin teknik açıklamasına girmeyecek olsak da; siber alem için çeşitli yazarlarca yapılan benzetmeler bu alemin suça elverişli yapısını anlamak için yeterli olacaktır[1]. Siber alem hakkında; fiziki gerçekliğin dışında bir alem oluşu ve bugün için en az fiziki alem kadar büyük ve hayatımızda önem sahibi oluşunu anlatmak için "yapay bir evren" (*artificial universe*) ve "metafizik uzay" (*metaphysical environment*)[2] , pek çok fırsat ve olanağın yanı sıra güvenlik tehditlerini beraberinde getirmesi, suç oranın yüksekliği ve suçluların elini kolunu sallayarak gezmesi itibariyle "Vahşi Batı" (*Wild West*)[3], işlemlerin hızlılığını, tehlikeye maruz kalma olasılığının yüksekliğini, faillerin kaçma şansının yüksekliğini ve korunma olanaklarının güçlüğünü ifade etmek için "güvensiz otoban" (*unsafe highway*)[4] ya da "bilgi otobanı" (*autoroute de l'information*)[5], fiziki mesafe olarak çok uzak ve farklı noktalarda bulunan internet süjelerinin küçük bir köydeki kişiler kadar kolay ve sık etkileşim içinde

---

1 Siber alemin yapısı ve işleyişine ilişkin ayrıntılı bilgi için bkz. Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku,** 5. Baskı, Ankara: Seçkin, 2014, s. 81 vd; Marco Gercke, Understanding cybercrime: phenomena, challenges and legal response", September 2012, **ITU 2012,** (erişim: 14.05.2015), www.itu.int/ITU-D/cyb/cybersecurity/legislation.html; Mahmoud Malmir/Sohrab Neshastehriz, "**Identify the Characteristics of Cyber Space Facilitator in Relation to Committing a Crime"**, Int. J. Rev. Life. Sci., sy. 5/3, s. 183 vd.; Mehmet Bedii Kaya, **Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi**, İstanbul: On İki Levha, Şubat 2010, ss. 5-21.

2 Denis L. Jamet, "What Do Internet Metaphors Reveal About The Perception Of The Internet?", s. 19, (erişim: 12.06.2015), http://www.metaphorik.de/sites/www.metaphorik. de-/files/ journal-pdf/18_2010_jamet.pdf.

3 Mike Keyser, "The Council of Europe Convention on Cybercrime", **Journal of Transnational Law and Policy**, sy. 12, 2003, s. 287.

4 Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime", **Policing: An International Journal of Police Strategies & Management**, sy. 29/3, 2006, s. 412.

5 Jamet, "What Do Internet Metaphors", s. 19; David Sulek/Ned Moran, "What Analogies Can Tell Us About the Future of Cybersecurity", **Nato Siber Savunma İşbirliği ve İstihbarat Merkezi, ccdoe.org**, (erişim: 12.06.2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/ 08_SULEK_-What%20Cyber%20Analogies%20Can%20Tell%20Us.pdf).

olabilmelerini anlatmak için "global bir köy" (*global village*)[6] benzetmeleri yapılmaktadır.

Klasik suçların takibinde fiziksel bir çevre söz konusudur ve suç takibi sınırları belirlenebilir veya öngörülebilir olan bu fiziksel ortamda gerçekleşir[7]. Fiziksel ortamda suçun delilleri çoğunlukla beş duyu organıyla gözlemlenebilmekte, delillerin yorumlanması teknik bilgi gerektirse de tespiti çoğunlukla vasıtasız bir şekilde gerçekleşebilmektedir[8]. Fiziki çevrenin sınırlandırılabilir ve belli ölçüde kuşatılabilir yapısı sayesinde devletler ve ulus üstü siyasi örgütler fiziki alemi büyük ölçüde kontrol edebilmektedir. Ancak siber alem; teknolojik imkanlar sayesinde işlemlerin çok hızlı bir şekilde gerçekleştiği, işlemlerin izlerinin kolayca kaybolabildiği ve yok edilebildiği, sınırlandırılamayan genişlikteki içeriği nedeniyle işlem ve kişi takibinin oldukça güç olduğu, elektronik veri işleme süreçlerinden oluşması itibariyle çoğunlukla kavramların fiziksel anlamda karşılığının bulunmadığı devasa ve kompleks bir dünyadır.

Siber alemi oluşturan internet ve diğer ağlar ile bunlara entegre bilişim sitemlerinin ve bunların işlemlerinin fiziki dünyada görünüşte bir karşılığı olmakla birlikte, bunların fiziksel (ontolojik) varlıkları hukuki anlamda değerlendirilmeleri için yetersizdir[9]. Örneğin, bir içerik internet üzerinde Türkiye'de yayına sunulduğunda, yayına sokma işleminin fiziki dünyadaki karşılığı dünyanın uzak bir ucunda gerçekleşen bir bilgisayar komutu, yani bilgisayarın işlemcisindeki elektrik akımı iletimidir[10]. İçeriği yayına sokma işlemini veren komut bir başka komut serisinin yani bir bilgisayar programının ürünü olabilir. Hatta yapay zekanın hayatımıza girmesi ve her geçen gün gelişmesiyle komut zincirinin başlangıcında dahi bir insan davranışı söz konusu olmayabilir[11]. Fiziksel aleme dünyanın uzak ve ücra bir köşesindeki bir bilgisayarın işlemcisindeki elektrik akımı olarak yansıyan içeriğin işleme sokulma işlemi sonrasında içeriğin nerede olduğu da muğlaktır.

---

6 Jamet, "What Do Internet Metaphor", s. 19.

7 Susan Brenner, "Transnatioanl Investigation of Cybercrime", **Cybercrime and The Law: Challenges, Issiues and Outcomes**, New Jamsphire: University Press of New England, 2012, s. 172.

8 Feridun Yenisey/Ayşe Nuhoğlu, **Ceza Muhakemesi Hukuku Ders Kitabı**, 2. Baskı, İstanbul: Bahçeşehir Üniversitesi Yayınları, Ekim 2014, s. 81.

9 Andrew Murray, **Information Technology Law: The Law and Society**, 2. Baskı, London: Oxford, 2013, s. 85.

10 Susan Brenner, "Approaches to Cybercrime Jurisdiction", **Journal of High Technology Law**, sy. 4, 2004, s. 44.

11 Ugo Pagallo, **The Laws of Robots: Crimes, Contracts, and Torts**, London: Springer, 2013, s. 154.

İçerikle etkileşime giren her bir bilişim sisteminde yine fiziksel anlamda elektrik akımından ibaret olan bir seri işlem gerçekleşir. Oysa bu içerik sosyal, ekonomik ve hukuki değeri itibariyle, tam olarak nerede gerçekleşeceği belli olmayan bir seri elektrik akımından fazlasını ifade etmektedir. Bu nedenle siber alemdeki kişi, nesne ve işlemlerin hukuki anlamları fiziki karşılıklarıyla değerlendirilemez. Söz konusu içerik; bir hukuki irade beyanı oluşturabilir, fikri mülkiyet hakkı konusu teşkil edebilir ve -çalışmamızın konusuyla ilgili olması bakımından en önemlisi- suç konusu veya delili olabilir. Bu itibarla siber alemin, hukuki değeri itibariyle fiziksel varlığından bağımsız bir varlığı olduğu anlaşılmalıdır[12]. Nitekim bu alemin "sanal" olarak adlandırılması bu gerçeklikten kaynaklanmaktadır. Siber alemdeki öznelerin, nesnelerin ve işlemlerin fiziki varlıkları bütünüyle göz ardı edilemez; hukuki değerlendirmede elbette ki bunların fiziki anlamda varlıkları üzeriden hareket edilmektedir[13]. Ancak siber alemin hukuki anlam ve değerinin sanal varlığı ve sanal kavramları ile birlikte anlaşılması gerektiği unutulmamalıdır.

Siber alemde işlemler ve nesneler "sanal" olmakla birlikte; bunların hayata etkisi son derece "gerçek"tir[14]. Kamu hizmetleri, devlet bürokrasisi, ticaret, sanat ve daha başka akla gelebilecek tüm hayat alanları siber alemle ilişki içindedir, hatta büyük ölçüde siber alemde yürütülmektedir. İşlemlerin ve nesnelerin sanal varlıkları, gerçek hayatta hukuki ve ekonomik anlamda büyük etkiler doğurmaktadır. Özellikle suç teşkil eden fiiller söz konusu olduğunda, devletlerin ve ulusal toplumun güvenliği, kişilerin can ve mal güvenlikleri, kişilerin ve toplumun huzuru hiç olmadığı kadar tehlike altında olabilmektedir[15]. Bu nedenle devletler ve ulus üstü siyasi örgütler aslında kontrol edemedikleri ve hükmedemedikleri bu alanı düzenleme iddia ve çabası içindedirler. Siber alemin düzenlenmesinin gerekli hatta zorunlu görülmesinin sonucu olarak, geleneksel hukuk alanlarından farklı olan siber aleme, fiziksel alem üzerinden kontrol altında tutulabildiği ölçüde hukuk kuralları uygulanmaya çalışılmaktadır[16].

---

[12] Dülger, **Bilişim Suçları**, s. 84; Tekin Memiş, "İnternet Ortamında Haksız Rekabet Halleri ve Türk Hukuku", **İnternet ve Hukuk**, Der: Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 100.

[13] Susan Brenner, "Toward a Criminal Law for Cyberspace: Distributed Security", **Boston University Journal of Science & Technology Law**, sy. 10, 2004, 67.

[14] Keyser, "The Council of Europe Convention on Cybercrime", s. 288.

[15] Örneğin neredeyse tüm kamu hizmetlerinin ve finans sektörünün bilişim sistemleri üzerinden online olarak yürütüldüğü Estonya'da 2007 yılında gerçekleştirilen siber saldırılar nedeniyle üç haftadan uzun bir süreyle neredeyse tüm kamu ve özel hizmet sektörü durma noktasına gelmiştir.

[16] Dülger, **Bilişim Suçları**, s. 85.

Siber alemi oluşturan en büyük ve önemli unsur olan internet herhangi bir otorite tarafından yönetilmemekte, daha doğrusu yönetilememektedir[17]. Herhangi bir kişinin buluşu ya da ticari malı olamayan, herhangi bir devletin üzerinde hak ve otorite iddia edemediği internet, sisteme giren herkesin katkısıyla oluşmuş anonim ve büyük bir ağ sistemidir[18]. Bu itibarla internetin aktif ya da pasif kullanıcısı olmak; yani internete girmek ve internette faaliyette bulunmak için yasal bir başvuruya, onaya ya da izne gerek yoktur[19]. Yalnızca gerekli özelliklere sahip bir bilişim sistemi ve bağlantı hattı ile internete girilebilir[20]. İnternet dışındaki ağlar çoğunlukla sınırlandırılabilir ve yönetilebilir ağlar olmakla birlikte bu ağlar bakımından da, özellikle global olanlarda teknolojik imkanlar sayesinde yönetim kurallarının ihlal edilme riski ve oranı oldukça yüksektir[21]. Yönetici bir siyasi otoritenin olmadığı siber aleme ilişkin pozitif hukuk kurallarının konulması söz konusu olsa da, bu kuralların gerçek anlamda yaptırımı söz konusu olamamaktadır[22]. Bu özelliği

---

[17] Andrew Sparrow, The **Law of Virtual Worldsand Internet Social Networks**, Burlington: Gower, 2010, s. 5.

[18] Pınar Memiş, "İnternet ve Ceza Hukuku: Fransa Örneği",**Prof. Dr. Çetin Özek Armağanı**, 2004, s. 607.

[19] Dülger, **Bilişim Suçları**, s. 85.

[20] Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, 2001, s. 30.

[21] İnternet dışında başta uydu ağları (Iridium,Globalstarand Orbcomm vb.), telefon ağları (GSM vb) olmak üzere çok sayıda global ağ mevcuttur. Ayrıntılı bilgi için bkz. Andrew Odlyzko, "The Internet and other networks: utilization rates and their implications", **Information Economics and Policy**, sy. 12/4, 2000, ss. 341-365.

[22] Pozitif hukuk, ortak kabul gören unsurlar üzerinden şu şekilde tanımlanabilir; belirli bir kara parçasında, belirli bir siyasi otorite tarafından yaptırımı sağlanan yazılı kuralları bütününe hukuk denilir. Ayrı bir hukuki alan olduğunu kabul ettiğimiz siber alem açısından bu tanımın güçlükle sağlandığını söylemek yanlış olmayacaktır. Çünkü pozitif anlamda hukuktan bahsedilebilmesi için belirlenmiş yazılı kuralların varlığının yanı sıra, bu kuralların hakim siyasi otorite tarafından etkin bir yaptırıma tabi tutulması gerekmektedir. Sınırları siber aleme göre çok daha belirli olan ve etkinliği tartışılsa da yönetici pozisyonunda siyasi otoritelerin mevcut olduğu uluslararası hukuk bakından dahi gerçekte bir hukukun var olmadığı tartışmalı iken siber alem bakımından hukuk kurallarının varlığı tartışmaya açıktır. Ancak fizik alemdeki yansımaları üzerinden hukuk kurallarının tatbiki söz konusu olabilmektedir. Netice olarak siber alemi hukuk dışı ya da hukuksuz bir alan olarak görmüyoruz, ancak; siber alemin ayrı bir hukuki alan olduğunu ve buna uygun hukuk kurallarının yaratılması ve tatbikinde bu farklı yapısı ve özellikleri dikkate alınması gerekliliğini hatırlatıyoruz. Konuyla ilgili Dülger'in şu ifadeleri önemlidir: *"...belirtilmesi gereken ilk husus, sanal alanın ve bunlar içindeki en yaygın ağ sistemi olan internetin kesinlikle "hukuki" bir alan olduğu ve bu alanı düzenlemek için internetin kendine özgün yapısına uygun hukuk kurallarına ihtiyaç duyulduğudur. İnternetin, her türlü ifadenin kendisine yer bulabildiği özgür bir ortam olduğu hususunda kuşku yoktur. Bunun yanı sıra internetin devletlerin egemenlik alanlarının dışında kaldığı ve kendine özgü bir sistem olduğu şeklinde bir anlayış da bulunmaktadır. Ancak internet kendine özgü bir sistem olmakla birlikte sanıldığı gibi devletlerin müdahalesinden uzak ve tamamen özgür bir alan değildir*" Dülger, **"Bilişim Suçları…**, s.837; Pozitif hukuk tartışmaları ve hukuk tanımın unsurları için bkz. Niyazi Öktem/Ahmet Ulvi Türkbağ, **Felsefe, Sosyoloji, Hukuk ve Devlet**, İstanbul: Der Yayınları, 2011, s. 79. ; uluslararası hukukun pozitif bir hukuk alanı olarak varlığına ilişkin tartışmalar için bkz. Hüseyin Pazarcı, **Uluslararası Hukuk**, Ankara: Turan Kitabevi, Haziran 2014, s. 6 vd.; Prosper Weil, "Le droit international en quête de son identité", **Recueil des Cours de l'Academie de Droit International**, sayı 237, 1992, s. 47 vd. Siber aleme ilişkin hukuki sorunların çözümünde uluslararası hukukun benzer problemlerini referans alan diğer yaklaşımlar için bkz. William M Stahl, "The Uncharted

itibariyle Vahşi Batıya da benzetilen[23] ve adeta hukukun doğmasından önce yaşandığı varsayılan doğal dönemin hüküm sürdüğü[24] siber alemde, hukuk kurallarının ve hukuki süreçlerin tatbiki oldukça güçtür.

Ceza hukuku ve ceza muhakemesi hukuku açısından siber alemin bu genel sorunlarına ilave olarak, suç teşkil eden fiillerin belirlenmesi ve soruşturulması sorunu özellikle zorluk arz etmektedir. Bu durumun en açık ve en önemli göstergesi olarak; modern ceza hukukunda "siber alemin güvenliği" bağımsız bir hukuki menfaat olarak değerlendirilmekte ve "bilişim alanında suçlar" ile tek başına bu menfaatin ihlal edilmesi suç sayılmaktadır[25].

Siber alemin kendine has özelliklerinden birisi de işlem yapma hızı ve kolaylığıdır. Bilişim sitemlerinin veri işleme hızları sayesinde çok büyük etkileri olan işlemler çok kısa sürelerde gerçekleşmektedir[26]. Bu durum bir yandan siber alemi suç işlemeye elverişli bir alan haline getirirken bir yandan da suç ve suçluların takibini ciddi ölçüde zorlaştırmaktadır. Örneğin siber alem dışında, yani herhangi bir bilişim sistemi kullanmaksızın 100.000.000 TL'lik bir banka soygunu yapmak için ya çok sayıda kişiyle birlikte ve büyük bir araçla bir banka şubesine gidip, uzun bir süre ve yoğun emekle kasaları açıp, aracınıza yükleyip gözden kaybolmanız ve bu süre boyunca güvenlik görevlileri, banka çalışanları, müşteriler tarafından müdahaleye uğrama, bunlar ve güvenlik kameraları tarafından görülme, bankadan ayrıldıktan sonra takip edilme, yolunuzun kesilmesi risklerini göze alıp, sonrasında aylarca saklanıp, paraların seri numaralarının alınmış olması ihtimaline karşı paraları sadece belirli yerlerde ve parça parça piyasaya sürmek zorundasınızdır. Ancak bu şekilde bu soygunu başarılı bir şekilde gerçekleştirebilirsiniz. Oysa aynı soygunu bilişim sitemleri aracılığıyla birkaç saniyede gerçekleştirebilir, birkaç saniye daha harcayarak paranızı dünyanın çeşitli yerlerinden yatırım işlemlerine tabi tutarak paranın izini kaybettirebilir ve bunları yatağınızda sırtüstü uzanmış bir şekilde, hiç kimseyle muhatap olmadan, neredeyse hiçbir fiziksel aktivite içine girmeden

---

Waters Of Cyberspace: Applying The Principles of International Maritime Law To The Problem Of Cybersecurity", **Ga. J. Int'l & Comp. Law Review**, sy. 40, ss.247-273.

23 Keyser, "The Council of Europe Convention on Cybercrime", s. 287.

24 Bkz. Yukarıda 21 nolu dipnot.

25 Dülger, **Bilişim Suçları…,** s. 340, 407, 432; Mehmet Emin Artuk/Ahmet Gökçen/Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 13. Baskı, Ankara: Adalet, 2013, s. 827, 843, 858. Siber alemin güvenliğinin bağımsız bir hukuki menfaat olmadığı yönünde karşı görüş için bkz. Mahmut Koca, "Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları", **Prof. Dr. Ali Güzel'e Armağan**, C. II, İstanbul, 2010, s. 1651-1660.

26 Teknolojinin bugün geldiği noktada gelişmiş bilişim sistemleri saniyede 54.000'den fazla işlem yapma kabiliyetine sahiptir.(erişim: 14.06.2015), http://www.top500.org/.

gerçekleştirebilirsiniz[27]. Elbette siber alemde bu ve benzeri suçların işlenmesini önlemeye yönelik tedbirler alınmaktadır[28]. Ancak suçu oluşturan hareket ya da hareketlerin çok küçük zaman dilimlerinde ve çok az fiziki çabayla gerçekleştirilebilmesi sayesinde siber alemde suç işleme ve suçların takipsiz kalma şansı her zaman yüksek olmaktadır[29].

Siber alemin suçun işlenmesi için sunduğu kolaylıklar suçun delillerinin karartılması bakımından da söz konusudur[30]. Suç faili, teknolojinin sunduğu imkanlar sayesinde kolaylıkla suç delillerini yok etme veya kendileriyle irtibatlandırılamaz kılma şansına sahiptirler[31]. Suçun delillerini tespit etmek için başvurulacak muhakeme tedbirine usulünce karar verilinceye kadar geçen sürede dahi suç failleri kolaylıkla delilleri karartabilirler.

Suç işlemenin ve delilleri karartmanın bu denli kolay olduğu siber alemde bu durumun sonucu olarak suç işlenme sayısının yüksekliği ve birim zamanda gerçekleşen saldırı sayısı, yani saldırıların yoğunluğu da sorun teşkil etmektedir[32]. Bir yandan da siber saldırı sayısı ve yoğunluğunun katlanarak artması söz konusudur[33]. Sistemde bulunan küçük bir güvenlik açığı sayesinde saniyede milyonlarca saldırı gerçekleşebilir. Bu durum sınırlı olanaklarla yürütülen suçla

---

27 22 Haziran 2009 günü Amerika Birleşik Devletlerinde Kentucky Federal Devlet Bankasından bir gecede 415.000$ tutarında para farklı hesaplara transfer edildi. Soruşturmayı yürüten FBI yetkilileri sadece soygunun Ukrayna'dan gerçekleştirildiğini tespit edebildi. Failler halen yakalanamadı, muhtemelen hiçbir zaman yakalanamayacaklar. Susan Brenner, "Law, Dissonance, And Remote Computer Searches", **North Carolina Journal of Law & Technology**, sy 14, 2012, s.44.

28 *"Türkiye'deki bankacılık uygulamasında, şifrenin çalınmasını güçleştirecek PIN-TAN gibi güvenlik uygulamaları bulunmamaktadır. Bu önlem, Alman Bankacılık uygulamasında oldukça yaygındır. Buna göre, banka tarafından kullanıcıya bir internet bankacılığı şifresi (PIN) atanır (veya kullanıcı bunu belirler) ve ayrıca banka müşterisinin bildirdiği adresine TAN (tek kullanımlık şifre) gönderir. Sistem ancak bu iki şifrenin bir araya getirilmesiyle açılabilir. Bir başka deyişle, bilişim hırsızlarının sisteme girebilmeleri için hem bu PIN kodunu öğrenmeleri hem de kullanıcının adresine giderek TAN numaralarını içeren bu belgeyi çalmaları gerekir."* Cankat Taşkın, "Bilişim Hukuku Uluslararası Uyuşmazlıklar**", Türkiye Barolar Birliği Dergisi**, sy. 85, 2009, s. 364-65.

29 Richard Clayton/Tyler Moore/Nicolas Christin, Concentrating Correctly on Cybercrime Concentration, Proceedings of the **Forteenth Workshop on the Economics of Information Security**, Delft, 2015, s. 2.

30 Albert . Aldesco, "The Demıse Of Anonymıty: A Constıtutıonal Challenge To The Conventıon On Cybercrıme", **Loyola of Los Angeles Entertainment Law Review**, sy. 23, 2003, s. 120.

31 Brenner, "Toward a Criminal Law for Cyberspace", s. 72.

32 Nicholas W. Cade, "An Adaptive Approach For An Evolving Crime: The Case For An International Cyber Court And Penal Code", **Brook. J. Int'l L**., sy 37, 2011, s.1141.

33 Çeşitli kuruluşlar tarafından hazırlanan siber saldırı haritaları siber saldırıların gerçek zamanlı simülasyonunu vermektedir. Siber saldırıların ne ölçüde sık gerçekleştiği konusunda fikir vermesi açısından bu haritalar incelenebilir: http://map.norsecorp.com/, http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=16656&view=map, http://www.sicherheitstacho.eu/, https://cybermap.kaspersky.com/.

mücadele ve suçların adli takibini bir kat daha zorlaştırır, hatta kimi zaman imkansız hale getirir.

Siber alemi oluşturan, birbiriyle sürekli veya zaman zaman ilişki içinde olan cihaz ve kullanıcı sayısını tespit etmek mümkün değildir[34]. Siber alemde, suç takibinde muhatap olunan veri de korkunç olarak tanımlanabilecek boyutlardadır. Siber alemin haritası dahi tam olarak çıkarılamamakla birlikte; erişilebilir bazı bilimsel çalışmalara göre sırf internette erişime açık olan 983.000.000'dan fazla internet sitesindeki toplam veri miktarının 300 ZB (zettabytes)[35] civarında olduğu tahmin edilmektedir. İnternet dışındaki global ağlarda erişime açık bulunan, *intranet* adı verilen lokal ağlarda bulunan ve diğer bilişim sistemlerinde depolanmış halde bulunan verilerin bütünü düşünüldüğünde siber alemin genişliğine dair ve bu alemde suç delili bulması gereken polis ya da adli kolluğun muhatap olduğu zorluğa dair bir fikir sahibi olunabilir.

Siber alemin suç işlemeye ve delillerini karartmaya elverişli yapısı, suç takibinde muhatap olunan aktör ve veri içeriğinin sınırsız denilebilecek ölçüde büyük olması nedeniyle siber suçlarla mücadelede kaynakların ne şekilde dağıtılması gerektiğini gösteren "suç haritaları" geliştirilmesi de oldukça zor olmaktadır[36].

b) Siber Suçun Yeni Bir Kavram Oluşu ve Sürekli Gelişmesi

Siber suçluluk görece yeni bir kavramdır. Teknolojik gelişmelerin suç işlemede araç olarak kullanılmasının tarihi çok eskilere dayansa da bilişim sistemleri aracılığıyla ya da bu sistemlere yönelik olarak işlenen suçların tarihi 1960'lı yıllara dayanmaktadır[37]. Geleneksel suçlarla mücadelede eski hukuk sistemlerinden beri süregelen binlerce yıllık tecrübeyle karşılaştırıldığında siber suçluluk kavramının ne derece yeni olduğu daha net anlaşılmaktadır.

---

[34] 2015 yılı itibariyle dünya genelinde 3.181.000.000'dan fazla internet kullanıcısı tespit edilmiştir. 2014 yılına oranla %40'lık bir artış gösteren kullanıcı sayısı her saniye artmaktadır. Günde ortalama 500.000'den fazla bilgisayar, 5.000.000'dan fazla akıllı telefon ve 1.000.000'a yakın tablet satılmaktadır. Güncel rakamları canlı olarak incelemek için bkz. http://www.internetlivestats.com/internet-users/.

[35] 1 ZB (zettabyte) 1099511627776 GB (gigabyte)'tır. http://www.v3.co.uk/v3-uk/news/2379626/internet-of-things-to-generate-400-zettabytes-of-data-by-2018.

[36] Brenner, "Toward a Criminal Law for Cyberspace", s. 33; Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Prof.Dr. Nur Centel'e Armağan, MÜHFHAD,** sy. 19/2, s. 1232.

[37] Dülger, Bilişim Suçları, s. 110.

Kavramın tarihsel kronolojideki yeri itibariyle yeni olmasının yanı sıra teknolojinin baş döndüren gelişim hızı sayesinde siber suçluluk her zaman "yeni" kalmaktadır[38]. Siber suçlar, işlenme yöntemleri itibariyle bazı tasniflere tabi tutulsa da[39], siber suçluluğun yeni olması ve yeni kalması nedeniyle suçun işleniş biçimleri hakkında net şablonlar çıkarmak mümkün olmamaktadır[40].

Siber alemde sürekli yeni suç işleme yöntemleri ortaya çıkmaktadır[41]. Bilişim sistemlerinin kullanıcılarına meşru zeminde daha etkin ve daha güvenli bir kullanım sunma amacına yönelik olarak geliştirilen teknolojik yeniliklerin suç işlemede kullanılmasının yanı sıra, sırf suç işleme ve adli takipten kaçma amaçlı teknolojilerin üretilmesi de söz konusudur[42]. Siber saldırı yöntemleri belirli kategoriler altında sınıflandırılsa da, bu saldırı kategorileri içinde de sürekli yeni suç işleme yöntemleri ortaya çıkmaktadır[43]. Örneğin "botnet saldırılar" bir siber saldırı türü olarak üst kategoriyi oluştursa da[44], bu saldırının sayısız farklı versiyonla işlenmesi mümkündür[45]. Nitekim Microsoft yetkilileri sırf son bir yıl içinde yedi farklı botnet saldırısı türünü tespit ettiklerini rapor etmiştir[46].

Siber alemin ve siber suçluluğun yeni oluşu dolayısıyla ceza adalet sisteminin bir çok aktörü konuya aşina değildir[47]. Özellikle hakim ve savcıların konunun teknik boyutlarından büyük ölçüde habersiz olmaları sorun teşkil etmektedir[48]. Yukarıda belirttiğimiz üzere siber alem sürekli yenilenme halinde olduğu için siber suçlulukla

---

38 Brenner, "Toward a Criminal Law for Cyberspace", s. 67.

39 Siber suçların işlenme şekilleri için bkz. Dülger, Bilişim Suçları, s. 113 vd.

40 Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1232.

41 Brenner, "Toward a Crımınal Law for Cyberspace", s. 68.

42 Andrea Renda, "Cybersecurity and Internet Governance", **Council on Foreign Relations**. (Erişim: 03.05.2013), http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621.

43 Janine S. Hiller, "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets", **Santa Clara High Technology Law Journal**, sy 31, 2015, s. 167.

44 "*Botnet "robot" kelimesinin ve network kelimesinin "net"'i kullanılarak oluşturulmuştur. Saldırganlar çeşitli yollarla kurban ismini verdikleri cihazları zararlı yazılımlar ile ele geçirirler. Bu ele geçirilen cihazlar zombi (bot) bilgisayar olarak adlandırılır. Bot programı, kurbanın bilgisayarına gizlice yüklenen ve saldırganın çeşitli iletişim kanalları (HTTP, IRC vb.) vasıtasıyla uzaktan kontrol etme olanağı sağlayan programlardır. Bu şekilde olan birçok bot programının bulaştığı cihazın bir araya gelerek büyük bir bot ağı oluşturmasına ve merkezden yönetilmesine botnet denir.*" Dülger, **Bilişim Suçları**, s. 127.

45 Hiller, "Civil Cyberconflict", s. 210.

46 Microsoft yetkilileri 2014 yılında "Rustock", "Kelihos", "Zeus", "Nitol", "Bamital", "Citadel" ve "ZeroAccess" isimli Botnet saldırılarını tespit ettiklerini bunların ilk beşini kendi imkanlarıyla, son ikisini de kolluk güçleriyle işbirliği halinde önlediklerini rapor etmiştir. Nate Cardozo, "What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business", **Electronic Frontier Foundation** (Erişim: 10.07.2015), http://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking.

47 Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1233.

48 Francesco Calderoni, "The European legal framework on cybercrime: striving for an effective implementation", **Crime Law Soc Change**, 2010, s.341.

mücadele eden ve siber suçları takip eden ceza adalet sistemi aktörlerinin bilgilerinin ve teknik donanımlarının da sürekli yenilenmesi gerekmektedir. Bu konuda ulusal ve uluslararası düzeyde bilgi ve tecrübe paylaşımı hayati önem arz etmektedir[49].

Siber suçluluğun yeni bir kavram olması dolayısıyla ceza adalet sistemi aktörlerinin bilgi ve tecrübe eksikliğinin yanında mağdurların bilgisizliği de söz konusudur[50]. Bilişim sistemlerini, bu sistemlerin teknik ayrıntılarını ve hatta olağan fonksiyonlarını dahi tam olarak bilmeden kullanan milyarlarca insan potansiyel suç mağdurudur. Buna karşın siber suçlular bilişim sistemlerinin teknik yönlerine son derece hakim, teknolojinin handikapları olan açık kapıları bu teknolojilerin üreticilerinden dahi iyi bilen uzman kişilerdir[51]. Her ne kadar siber güvenlik adına anti virüs programları, yüksek güvenlikli şifreleme programları gibi profesyonel koruma hizmetleri sunulsa da suç failleri ile mağdurları arasındaki bu bilgi ve olanak farkı siber suç mağdurlarını özellikle savunmasız kılmaktadır[52]. Hatta bazı suç işleme yöntemlerinde suç mağdurlarının suça maruz kaldıklarını dahi bir süre ya da hiçbir zaman anlayamamaktadırlar[53].

c) Siber Alemde Anonimlik ve Veri İletim Tekniğinin Kontrol Direnci

Siber alem, tümüyle anonim görüntü altında hareket etmeye imkan sağlamaktadır[54]. Suç işlendikten sonra şüphelinin geçmişe doğru takip edilmesi fizik aleme nazaran oldukça güçtür. Kural olarak bilişim sistemlerinin siber alemde gerçekleştirdikleri etkileşimler bu sistemlerin kendilerine özgü kimlikleri ve parmak izleri sayesinde tespit edilebilir. Örneğin İnternette IP adresleri üzerinden bir işlemin tarafı olan bilişim sistemleri teknik olarak açıkça tespit edilebilir ve takip edilebilir[55].

---

49 Önok, "Avrupa Konseyi Siber Suç Sözleşmesi…", s. 1233.

50 Ales Zavrsnik, "Cybercrime Definitıonal Challenges And Criminological Particularities", **Masaryk University Journal of Law and Technology,** sy. 2, 2008, s. 11.

51 Zavrsnik, "Cybercrime Definitıonal Challenges", s. 15; Dülger, **Bilişim Suçları**…, s. 133.

52 UNODC Uzmanlar Grubu Raporu, "Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector", Viyana, 2013, s. 6.

53 Ana I. Cerezo/Javier Lopez/Ahmed Patel, "International Cooperation to Fight Transnational Cybercrime", **2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA,** 2007, s. 15.

54 Ulrich Sieber, **İnternetteki Suçlar ve Suçun İnternette Takibi**, Ankara: Seçkin, 2014, s.55.

55 İnternet Protokolü (Internet Protocol) kelimelerinin ilk harflerinden oluşan IP sistemi hakkında şu şekilde anlaşılabilir ve basit bir tanım yapılabilir: "*IP adresi, bir gönderen ve bir alıcı adresi*

Ancak internete bağlanan cihaz sayısını karşılamaması nedeniyle IP adresleri statik değil dinamik olarak verilir[56]. Yani bir IP adresi farklı zamanlarda farklı bilişim sistemleri tarafından kullanılır. Bu durumda tek başına IP adresi etkileşimi gerçekleştiren bilişim sitemini göstermez, etkileşimin gerçekleştiği tarih ve saatte o IP adresinin hangi bilişim sistemine atandığının da bilinmesi gerekir. Trafik bilgileri de denilen bu bilgilerin tutulmasının ayrı bir teknoloji, masraf ve veri saklama alanı gerektirmesinin yanı sıra[57], kişisel verilerin ve özel hayatın gizliliğinin korunması endişelerini de beraberinde getirmektedir[58].

Bilişim sistemleri arasındaki etkileşimi sağlayan veri iletimi, kullanıcıların ekran başında gözlemlediği şekilde bir bütün halinde gerçekleşmez. Veri paketlerine bölünen bir içerik farklı bağlantılar üzerinden bilişim sistemleri arasında iletilir. Pratik bir anlatımla 100 mb büyüklüğünde bir içerik homojen olmayan binlerce veri paketine bölünür, her bir pakette aynı IP mührü olmakla birlikte bu paketler farklı yolları kullanarak iletilir. "Routing" denilen bu süreçte en kısa ve etkin yol kullanılmaya çalışıldığı için aynı içeriğe ait paketler dünyanın farklı uçları üzerinden farklı yollardan iletilebilir. Bu sayede siber alemde gerçekleştirilen bir eylemin kaynağı olan bilişim sistemini tespit etmek çok külfetli ve çok zordur. Bu durum da siber suçluların anonim kalmasına zemin hazırlar[59].

Siber alemdeki veri iletim sisteminin olağan karmaşıklığına ilaveten, IP adresi çeşitli yollarla değiştirilebilir, bazı özel programlama teknikleri kullanılarak içeriğin normalin çok üstünde karmaşık ve farklı yollardan geçtikten sonra iletilmesi sağlanarak kaynağı ya da hedefi tespit edilemez kılınabilir[60]. Özellikle TOR benzeri merkezi olmayan ağlar gibi anonimleştirilmiş servisler ve veri şifreleme (encryption)

---

içeren ve içinde veri paketinin bulunduğu bir veri zarfına benzetilebilir." Sieber, **İnternetteki Suçlar…**, s.56; Bir başka tanımla IP adresi *"İnternete erişen her bir bilişim sisteminin nüfus cüzdanıdır."* Dülger, **Bilişim Suçları…**, s.83, 733 vd.;IP protolü hakkında ayrıntılı bilgi için bkz. Kaya, **Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi,** s. 28 vd.

56 *"IP adresleri, dinamik ve statik olmak üzere ikiye ayrılır. İnternet servis sağlayıcı tarafından internete bağlanmak isteyen bilgisayara geçici olarak atanan IP adresleri dinamiktir. Statik IP adresleri ise, değişmeyen adresler-dir. Sunucu bilgisayarlarda statik IP kullanılır. Bir de Özel IP adresi (Private IP Adress) şeklinde adlandırılan yalnızca Yerel Ağ (LAN) da kullanılabilen IP adresleri vardır. Özel IP adreslerine örnekleri; 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0. - 192.168.255.255. Bu IP adreslerini kullanarak Geniş Ağ'a erişmek mümkün olmadığından, Geniş Ağ'a erişmek istenildiğinde "Network Address Translation (NAT)" Ağ Adresi Dönüştürme ile Özel IP adresi değiştirilerek bilgisayarın internete çıkışı sağlanır."* Dülger, **Bilişim Suçları…**, s.733.

57 Sieber, **İnternetteki Suçlar**, s.56.

58 Angeles Gutierrez Zarza, **Exchange of Information and Data Protection in Cross Border Criminal Proceedings in Europe**, Springer, 2015, s. 18.

59 Sieber, **İnternetteki Suçlar**, s.57.

60 Aldesco, "The Demise Of Anonymity", s. 89.

programları veri iletiminin güzergahının yanı sıra içeriğini de erişilemez hale getirir[61].

IP adresine ve bunun üzerinden kaynak bilişim sistemine erişilse dahi suç teşkil eden fiilin faili olan kişiyi tespit etmek halen oldukça güçtür. Birincisi siber alemde işlemler saniyeler içinde gerçekleşirken; mağdurun adli makamlara başvurması, adli makamlar ile servis sağlayıcılar vb. diğer özel veya kamusal aktörlerin irtibat kurup geriye doğru iletişim ağını tespit etmesi çok daha uzun, kimi zaman aylar alan bir süreçtir. Bu süre zarfında fail suça konu bilişim sisteminde veya başka bilişim sistemlerinde mevcut bulunan delilleri bilişim olanaklarıyla veya fiziksel olarak yok edebilir. Söz gelimi suçta kullandığı bilgisayarı yakarak yok edebilir.

İkinci sorun bilişim sisteminin belirli bir kişiye özgülenmemiş, kamu veya özel tüzel kişiliğine ait olup birden fazla kişinin kullanımına açık olması ihtimalidir. Örneğin "internet cafe" denilen toplu kullanım sağlanan yerlerde bulunan bir bilgisayar aracılığıyla işlenen suçta kaynak bilgisayara ulaşılsa dahi bu bilgisayar aracılığıyla suçu işleyen kişiyi tespit etmek neredeyse imkansızdır.

Kaynak bilişim sistemi tespit edilip, bilişim sisteminin sahibi gerçek kişi bulunsa dahi, soruşturulan somut suçu bu kişinin işlediğinin ayrıca ispatlanması gerekir. Ceza mahkumiyeti için failin isnat edilen suçu işlediğinin şüpheden uzak bir şekilde ispatlanması gerektiği ve şüpheden sanık yararlanır ilkesi uyarınca fail ikrar etmedikçe, bilişim sisteminin sahibi olması tek başına suçun faili olduğunu ispatlamaz[62]. Nitekim çoğu zaman Truva atları veya başkaca zararlı yazılımlarla bilişim sistemleri ele geçirilerek "zombi bilgisayar" haline getirilmekte, sahibinin müdahalesi ve haberi olmaksızın bilişim sistemlerine bazı işlemler yaptırılmaktadır[63]. Bu itibarla siber suçların soruşturulmasının en önemli aşaması IP adreslerinin düzgün

---

[61] Konuyla ilgili olarak: *"Günümüzde yürütülen yargılamalar, belirli bir zaman diliminde şifreden arındırılamayan büyük uzunluktaki geçici şifrelemeleri kullanmaktadırlar* (böyle şifrelerle muhatap olmaktadır). *Böylece soruşturma makamlarına birçok olayda yalnızca, başkasına ait bilgisayara gizlice henüz şifrelenmemiş adımlarda ve böylece hukuken ve teknik açıdan önemli sorunlarla bağlantılı gözetleme yapan Truva programlarını kullanmak olanağı kalmaktadır."* Sieber, **İnternetteki Suçlar…**, s.58.

[62] *"Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tesbit edilmemiş bulunması, IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden m. -k12.com adresine bağlantı yapıldığının tespit olunamaması "hack" programına rastlanmasının şikayetçiye ait siteye müdahale edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılınmamıştır. .. beraat kararı usul ve yasaya uygun bulunduğundan… ONANMASINA karar verildi."* 8. CD. 24.10.2013, E. 2012/21817, K. 2013/25428

[63] Dülger, **Bilişim Suçları…**, s. 733.

ve gereği gibi araştırılmasıdır[64]. Ancak IP adresinin tespiti soruşturma için bir sonuç değil bir başlangıç olabilir[65].

İnternetin bilinen ve elverişli cihazlarla herkes tarafından erişilebilen devasa büyüklükteki "su üstündeki" kısmı haricinde bir de "su altında" (underground web) ya da diğer tabirlerle "derin" (deepweb) ve "karanlık" (darknet) bir kısmı vardır. Ağlara erişimin ancak bazı özel programlar kullanılarak ya da ilgili adresin bilgisi ve müsadesi altında gerçekleşebildiği bu alanın herkes tarafından erişilebilir su üstündeki kısımdan kat kat büyük olduğu iddia edilmektedir[66]. Tümüyle anonim

---

[64] Yargıtay da IP adreslerinin doğru ve gerektiği gibi araştırılmamasını bozma nedeni yapmaktadır: *"…Sanığın, … elektronik posta adresini kullanarak mağdur adına bir internet sitesine verdiği ilanda, mağdura ait olduğu anlaşılan telefon numaralarını yayımlayarak TCK'nın 136. Maddesinde tanımlanan kişisel verileri hukuka aykırı şekilde yaymak suçunu işlediği iddiasıyla açılan davada…; mağdura ait kişisel verileri içeren elektronik posta gönderisinin, sanığa ait internet kafeden gönderildiğinin IP adresi ile tespit edilmesi, aynı elektronik posta adresi hesabının oluşturulması sırasında elektronik posta hizmeti veren şirkete beyan edilen bilgilerin de doğru olmadığının anlaşılması karşısında; elektronik posta adresi oluşturulurken kullanılan IP adresinin ve bu adresi kullanan kişinin, elektronik posta adresinin aktive edilmesi için …net adli internet sitesinin yedek elektronik posta adresi isteyip istemediğinin, istemişse bu adresin ne olduğu, hangi IP adresini kullandığı ve sahibinin kim olduğu … adındaki elektronik posta adresinin gerçek kullanıcısının, gerekirse bu adresten elektronik posta alan kişiler Türkiye İletişim Kurumu Başkanlığından sorulup, tespit edilerek dinlenilmek suretiyle belirlenmesinden sonra sanığın hukuki durumunun takdir ve tayini gerekirken eksik inceleme ile beraat kararı verilmesi Yasaya aykırı görüldüğünden HÜKMÜN BOZULMASINA… "* 4. CD. 13.12.2010, E. 2010/19559, K. 2010/20604.
"Osmaniye Valiliği Bilgi İşlem Şubesi servis sağlayıcılarının İsim Tescil İnternet Teknolojileri A.Ş olduğu ve yapılan araştırmada söz konusu şirketin www.osmaniye.gov.tr web sitesine 31.03.2012 günü saat 19:38'de siber saldırı düzenleyen ve www.osmaniye.gov.tr web sitesine erişim yapan bilgisayarların IP numaralarının tespiti istenildiği ve İsim tescil İnternet Teknolojileri A.Ş'nin cevabı yazısında 31.03.2012 günü saat 19:38'den 19:39'a kadar 88.252.161.194 IP numarası ile 31.03.2012 günü saat 19:38:02'de Mehmet Demirdağ isimli şahsa ait sabit telefonla bağlantı sağlandığından bahisle açılan davada; yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan mahkumiyet hükmü kurulmuştur. Sanığın suçlamayı kabul etmeyerek kullandığı modemin şifreli olduğunu, kötü niyetli kişiler tarafından şifresinin kırılıp kullanılabileceğini savunması karşısında, sanığın internet hattına izinsiz giriş yapan olup olmadığının sanığın internet hattının bağlı bulunduğu internet sağlayıcısından sorulması, dosya içinde suça konu valiliğe ait siteye giriş yapan IP numaralarının ilgili birim tarafından bildirildiği ancak sitenin erişilmez hale getirilip getirilmediği, veri değiştirme, yok etme veya yeni veri yerleştirme yapılıp yapılmadığına ilişkin bir tespite rastlanmadığı anlaşılmakla, erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde siteye erişimin ne zaman engellendiği sanık veya servis sağlayıcı tarafından bildirilen diğer IP numaralarından hangisi ile girişin yapıldığı araştırılmalı, siteye yapıldığı iddia olunan siber saldırının ne şekilde gerçekleştiği, niteliği, sitenin geçici veya daimi olarak erişilmez kılınıp kılınmadığı yahut mevcut verilerin yok edilip edilmediği veya varsa yerleştirilen resim, yazı v.s. nin neler olduğunun tespit edilip önekleri de alınmak suretiyle dosya içine konulmalı, sanığın bilgisayarına el konulup hard diski incelenerek suça konu siteye ait bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanmalıdır. Bu itibarla yukarıda açıklanan eksiklikler yerine getirilerek sonucuna göre tüm deliller birlikte değerlendirilip sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması, (BOZULMASINA)" 8. CD. 14.05.2014, E. 2014/3415, K. 2014/12298.

[65] Dülger, **Bilişim Suçları**, s. 734.

[66] Peter Biddle/Paul England/ Marcus Peinado/Bryan Willman, "The Darknet and the Future of Content Distribution", **Microsoft Corporation Yayınları**, (erişim: 04.07.2015), http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

aktörlerden oluşan bu alanın neredeyse tamamı konusu suç teşkil eden ya da suç delili niteliğindeki içeriklerden oluşur[67].

Siber suçlular da bu alanı kullanarak, polisiye ve adli tedbirlere karşı korunurlar[68]. Gerçek kimliklerinin tespit edilemeyeceğini bilen suçlular, bu alanda hiçbir sınırlama, engel ve yakalanma korkusu olmaksızın faaliyet gösterme şansına sahiptirler[69]. Uyuşturucu satışı, insan ticareti, kiralık katil hizmeti, devletlerin ulusal güvenliğine yönelik istihbari bilgilerin ve ticari sırların hukuka aykırı satışı, çocuk pornosu ve ağır içerikli pornografik materyaller, siyasilerin ve ünlülerin özel hayatlarına ilişkin gizli görüntü ve belgeler gibi çok ciddi suçların açıkça pazarlandığı ve teşhir edildiği bu alan tam olarak hukuksuz bir alandır[70]. Katmanlardan oluşan bu alanın bazı katmanlarına polis ve adli soruşturma makamları zaman zaman suçluların yöntemlerini kullanarak sızmakta ve burada suçun önlenmesi ve adli takibine yönelik işlemler yapabilmektedir. Ancak bu alanın asıl hakimi olan bilişim korsanları[71], bu tür istisnai girişimleri atlatmakta güçlük çekmemektedir. Polis ve adli makamlar bilişim marifetiyle erişmedikleri bu alandaki suçlulara kimi zaman yasal kimi zaman yasa dışı "geleneksel" yöntemlere başvurarak ulaşmaya çalışmaktadır[72].

İnternetin karanlık alanına ilişkin güvenilir bilgi kaynakları sınırlıdır, bu dünyanın "olağan" sakinleri dışında içerinin gözlemlenmesi mümkün değildir. Ancak belki efsaneleri gerçeklerin önüne geçmiş olsa da[73], internetin karanlık yüzünün bir

---

67 Michael Chertoff/Tobby Simon, "The Impact of the Dark Web on Internet Governance and Cyber Security", **Global Commission on Internet Governance**, Centre for International Governance Innovation and the Royal Institute for International Affairs, s. 6, (erişim: 04.07.2015), https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

68 Sieber, **İnternetteki Suçlar**, s 58.

69 Chertoff/ Simon, "The Impact of the Dark Web on Internet Governance and Cyber Security", s.7.

70 Silk Road adlı site aracılığıyla işlenen suçlar, bu suçların soruşturulmasında kullanılan teknikler ve davanın diğer ayrıntıları için bkz. AO 91 (Rev 11/11), **Criminal Complaint**, United States District Court, Northern District of California, San Fransisco Division, (erişim: 04.07.2015), http://www.justice.gov/sites/default/files/opa/pressreleases/attachments/2015/03/30/criminal_complaint_force.pdf; "How FBI brought down cyber-underworld site Silk Road", USA Today, (erişim: 04.07.2015), http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/ .

71 Kavram ve ayrıntılı bilgi için bkz. Dülger, Bilişim Suçları…, s. 116 vd.

72 Monica R. Shah, "The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace", **Columbia Law Review**, sy. 105, 2015, s. 251; "How FBI brought down cyber-underworld site Silk Road" .

73 Darknet'te yapay zekalı ölüm makineleri, yapay zeka işlemcileri, Tesla'nın planları, kristarilize güç kontrolörleri, hava durumunu değiştirebilen cihazlar, gizli HAARP projeleri, Atlantis'in yeri ve hakkındaki gizli araştırmalar hatta Atlantis'in bulunduğu yerin detaylı konumları, özel üretim motorların planları, Tanrı'nın olduğunu kabul etmeyenler ve ispatları, masonlar, illuminati, gizli algoritmalar ve hesaplamalar, global terör ağı, global cinayet ağı, global uyuşturucu ağı, global insan ticareti ağı, süper bilgisayarlar ve yapay zekalar, nükleer reaktörlerin komut şifreleri vb

şehir efsanesinden ibaret olmadığını belirtmek gerekir. Amerika kaynaklı Silkroad adlı site yıllarca uyuşturucu başta olmak üzere suç eşyaları ve hizmetleri(!) satış platformu olarak hizmet vermiştir. Amerikan polisi Silkroad'un yönetici ve kullanıcılarını IP takibi vb. teknik yöntemlerle bulamamış; kullanıcı kılığına girmiş gizli soruşturmacılarla izleyici olarak sızabildiği sitede kullanıcılarla buluşup, özel(!) sorgulama teknikleriyle sitenin yöneticilerine ulaşmıştır. Yine yakın zamanda Dünya gündeminde büyük infial uyandıran Wikileaks belgelerinin sızdırılması internetin bu var olduğu bilinen, etkileri görülen ancak nüfuz edilemeyen karanlık tarafı sayesinde gerçekleşmiştir[74]. Amerika Birleşik Devletleri bu belgelerin yayımlanmasına engel olamamış, belgeleri ele geçiren ve ilk olarak yayımlayan adresleri teknik ve coğrafi anlamda tespit edememiştir.

Siber alemde suç işleyen ya da işlediği suçun delilleri siber alemde bulunan kişilerin kimliğinin gizli kalması polis ve adliye teşkilatları için içinden çıkılmaz sorunlar teşkil etmeye devam ederken; teknolojinin hukuk dünyasına armağan ettiği yeni bir sorunsal, yapay zekanın hukuki niteliği ve yapay zeka sahibi bilişim sistemlerinin işlediği suçlardan dolayı sorumluluk konusudur. Yakın bir zamana kadar bilişim suçlarının faillerinin mutlaka gerçek kişiler olduğu, bilişim sistemleri aracılığıyla işlenen suçlarda mutlaka süreci başlatan bir insan aklının var olduğu kabul ediliyor, siber suçlar bu varsayım üzerinden değerlendiriliyordu[75]. Ancak programlama tekniklerindeki gelişmeler yapay zekaya sahip bilişim sistemlerinin bağımsız çıkarımlar yapma ve ilk programlayıcıya isnat etmekte zorlanılan hareketler yapmasını mümkün kıldı[76]. Bu durum hukuk sistemi için ve özellikle yalnızca gerçek kişilerin suç faili olabilmesi, kusur ilkesi, cezaların şahsiliği gibi ilkelere sahip olan ceza hukuku bakımından çok kritik tartışmaların fitilini ateşlemiştir. Bugün ceza hukukçuları siber suçların unsurlarının, işlendiği yer ve zamanın nasıl anlaşılması gerektiği gibi ceza hukukuna ilişkin ve faillerin ve delillerin ortaya çıkarılması

---

bilgilerin bulunduğuna dair iddialar bulunmaktadır. Ayrıntılı bilgi için bkz. İbrahim Filazi, "İnternetin Yeraltı Dünyası: DeepWeb", (erişim: 04.07.2015), http://www.ifilazi.net/deepweb.html.

74 Welcome To The Deep Web: The Internet's Dark And Scary Underbelly, Worldcrunch, (erişim: 06.05.2015), http://www.worldcrunch.com/tech-science/welcome-to-the-deep-web-the-internet-039-s-dark-and-scary-underbelly/invisible-internet-tor-onion-network/c4s10150/; Wikileaks belgelerine erişimn nasıl sağlandığı yönünde teknik açıklama için bkz. "WikiLeaks:Tor", (erişim: 06.05.2015), https://wikileaks.org/wiki/WikiLeaks:Tor.

75 Mrinalini Singh/Shivam Singh, "Cyber Crime Convention And Trans Border Crımınality", **Masaryk University Journal of Law and Technology**, sy 1., 2007, s. 53.

76 Pagallo, **The Laws of Robots**, s.73 vd; Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities", **Social Sicence Research Network**, s. 153 (erişim: 06.07.2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1564096.

şeklindeki ceza muhakemesine ilişkin sorunların yanı sıra yapay zeka ürünü fiillerden dolayı ceza sorumluluğunu tartışmaktadır. Konu teknik ve hukuki yönleriyle oldukça kapsamlı olmakla birlikte biz siber alemde suç ve suç faili takibinin zorluğuna dair fikir vermesi açısından yalnızca bu yöndeki tartışmaların mevcudiyetini zikretmekle yetiniyoruz[77].

d) Delil Elde Etme ve Değerlendirme Süreçlerinin Uzmanlık Gerektirmesi

Geleneksel suçların soruşturulmasında, soruşturmayı yürüten ceza adalet sistemi aktörleri, suçun ve failin fizik alemde bıraktığı muhtemel delillere yoğunlaşır[78]. Zira geleneksel suçlar, fail mağdura fiziksel anlamda yaklaşmadan işlenemeyeceği ve kusursuz suç olamayacağı için fail suç mahalline girerken ya da çıkarken görülmüş olabilir ya da suç mahallinde kendisini ele verecek deliller bırakmış olabilir. Bu suçlarda deliller çoğunlukla beş duyu organıyla doğrudan gözlemlenebilir ve yorumlanabilir niteliktedir. Soruşturmayı yürüten savcı veya yargılamayı yürüten hakim bizzat suç mahallini ve diğer delilleri inceleyebilir ve bu delillerin çoğunu bizzat yorumlayabilir[79].

Siber suçların delilleri ve diğer suçların siber alemde yer alan delillerinin toplanması, muhafazası ve yorumlanması ise uygun bir teknolojik altyapı, özel bir uzmanlık ve özen gerektirmektedir[80]. Siber suçlarda genellikle suç mahallinde beş duyu organıyla doğrudan gözlemlenecek bir delil yoktur, failin suçu işlerken fark edilme olasılığı da oldukça düşüktür, zira failin fiziksel olarak yaptığı hareket çoğunlukla tuşlara basmaktan ibarettir ki; bu hareketin doğrudan gözlenmesi ile de bir suç işlenmekte olduğu anlaşılamaz. Elektronik deliller denilen, dijital ortamda bulunan deliller ancak bilişim uzmanlığı ile gözlemlenebilir ve yorumlanabilir.

Diğer yandan elektronik deliller, uzaktan erişimle karartılabilir ve bilişim sistemlerinin veri saklama kapasiteleri nedeniyle kısmen veya tamamen kaybolabilir. Bu nedenle elektronik delillerin zaman kaybetmeden hızlı bir şekilde toplanması

---

77 Ayrıntlı bilgi ve bu konudaki tartışmalar için bkz. Gabriel Hallevy, "The Criminal Liability of Artificial Intelligence Entities".

78 Brenner, “Law, Dissonnence, and Remote Computer Searches”, s. 46.

79 Yenisey/Nuhoğlu, **Ceza Muhakemesi Hukuku Ders Kitabı**, s. 89.

80 Cristos Velasco, “Cybercrime jurisdiction: past, present and future”, **ERA Forum**, Springer, 2015, DOI 10.1007/s12027-015-0379-y.

gerekmektedir. Ancak bir yandan hızlı hareket ederken bir yandan da delilin bütünlüğüne ve güvenilirliğine zarar vermemeye çalışarak özenle hareket edilmelidir. Geçici bellekte bulunan verilerin bir süre sonra silinmesi, bellekte bulunan verilerin üzerine başka veri yazılmış olması sebebiyle verilere doğrudan erişilememesi veya verilerin geri döndürülemez şekilde silinmiş olması, verilerin izinsiz erişime karşı şifreli ya da kendini yok etmeye programlı olması, verilerin depolanmış olduğu belleğin fiziksel olarak zarar görerek verilerin erişilemez hale gelmesi gibi delillerin bütünlüğü ve güvenirliğine yönelik pek çok riski bertaraf etmek ve üstesinden gelmek ancak bilişim uzmanlarının uygulayacağı özel yöntemlerle mümkün olabilmektedir.

Elektronik deliller, yargılama makamlarınca fiziki delillere kıyasla daha az itibar edilebilir deliller olarak değerlendirilir[81]. Elektronik delillerin bu "şüpheli" konumunun ardında bunların kolayca tahrif edilebilmeleri ve sahte olarak üretilme ihtimalleri yatmaktadır[82]. Adli süreçlerde bu şüpheleri bertaraf etmek için elektronik delillerin adli bilişim kuralları çerçevesinde toplanması, değerlendirilmesi ve muhafaza edilmesi gerekir[83].

Elektronik delillerin saydığımız hassas özellikleri nedeniyle, siber suçların delil elde etme ve değerlendirme süreçleri adli bilişim uzmanlığı gerektirir. Kısaca delillerin hukuka uygun bir şekilde elde edilmesi amacıyla bilişim sistemleri üzerinde inceleme ve analiz teknikleri kullanılarak yapılan uygulamalar şeklinde tanımlanan adli bilişim[84],adli tıp alanları içinde yeni bir alan olmakla birlikte giderek gelişmektedir[85]. Adli bilişim hem ileri düzeyde bir araştırma, hem de bilgisayar uzmanlığını bir arada gerektiren bir disiplindir. Adli bilişim sürecinin doğru ve düzgün işleyişi bakımından, alandaki akademik ve bilimsel araştırmalar, bu araştırmalar doğrultusunda yapılacak yasal düzenlemeler, adli bilişim uzmanlarının eğitimi, ulusal ve uluslararası düzeyde kendi aralarında ve diğer adli personelle işbirliği içinde olması çok önemlidir[86]. Ancak bütün bunlar yeterli sayıda yetişmiş

---

81 Cerezo/ Lopez/ Patel, "International Cooperation to Fight Transnational Cybercrime", s 17.

82 Stephen Mason, **International Electronıc Evidence**, London: British Institute of International and Comparative Law, 2008, s. 17; Singh/Singh, "Cyber Crime Convention and Trans-Border Criminality", s.56.

83 Dülger, **Bilişim Suçları**, s. 736 vd.

84 Türkay Henkoğlu, **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, İstanbul: Pusula Yayıncılık, 2011, s. 1.

85 Hasan Sınar, "New Perspectives on Computer Forensics", **MHB Prof. Dr. Gülören Tekinalp'a Armağan**, 2003, s. 665.

86 Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s.56.

eleman, uzun vadeli teknoloji ve tecrübe yatırımı ve yüksek maliyet gerektirmesi itibariyle zorluk arz etmektedir.

Hayatın hemen her alanının, özellikle ticari hayatın dijitalleşme hızına kıyasla adli bilimlerde dijital çağa adaptasyonun çok yavaş kaldığı söylenebilir[87]. Elektronik verinin usulüne uygun şekilde toplanması, değerlendirilmesinde dikkat edilmesi gereken kriterler, delil niteliğini haiz olması için taşıması gereken özellikler konularında akademik tartışmalar henüz devam etmekte olup; bu konulara çözüm sunacak yasal çalışmalar tamamlanmış değildir[88].

e) Faille Mağdur Arasında Mekansal Mesafe Bulunması

Ceza hukuku derslerinde ve ceza hukuku kitaplarında sınır aşan suçluluk anlatılırken birbirine komşu olan iki ülkede bulunan kişilerden birinin, bulunduğu ülkeden ateş ederek diğer ülkedeki kişiyi öldürmesi veya bir ülkede vurulan kişinin yaralıyken sınırlarından içeri girdiği bir başka ülkede ölmesi örnekleri verilir[89]. Geleneksel suçlarda fail ve mağdurun mekansal anlamda yakınlık içinde olması zorunluluğu ceza hukuku hocalarını sınır aşan suçluluğu anlatmak için bu fantastik örnekleri üretmeye itmiştir. Evet gerçekten geleneksel suçlarda kural olarak fail ve mağdur aynı ya da yakın mekanlarda bulunmakta ve suç tek bir ülkenin sınırları içerisinde işlenmekte ve tamamlanmaktadır[90].

Siber suçlar bakımından ise bugün gelinen nokta itibariyle suçun yalnızca ulusal sınırlar içerisinden kalarak işlenmesi istisnai bir durum halini almıştır. Siber alem dünyanın dört bir yanından bilişim sistemlerinin birbiriyle sürekli veya zaman zaman bağlantı halinde olduğu ve teknoloji sayesinde etkileşimlerin coğrafi mesafelerden etkilenmeden çok küçük zaman dilimleri içinde gerçekleştiği bir ortam olması itibariyle suçun unsurları çoğunlukla birden fazla ülkede bulunabilmekte veya suçun delillerinin soruşturmanın yapıldığı ülkeden başka bir ülke ya da ülkelerde

---

87 Cerezo,/Lopez,/Patel, "International Cooperation to Fight Transnational Cybercrime", s 17.

88 Elektronik delilin toplanma ve değerlendirilme süreçlerine ilişkin ayrıntılı bilgi için bkz. Stephen Mason, **International Electronic Evidence**; Türk hukukunda elektronik delillerin toplanması ve değerlendirilmesine ilişkin yasal eksiklikler hakkında ayrıntılı bilgi için bkz. Henkoğlu, **Adli Bilişim,** s. 15 vd.; Dülger, **Bilişim Suçları**, s. 721 vd; Pınar Memiş Kartal, "Evidence and Proof of Cybercrime in Turkish Law", **Kazancı Hakemli Hukuk Dergisi**, sy.93-94, 2012, 109-116.

89 Dülger, **Bilişim Suçları**, s. 185.

90 Brenner, "Law, Dissonnence and Remote Compute Searches", s 46.

araştırılması gerekebilmektedir[91]. İnternette işlenen suçlar bakımından üst komşunun bilgisayarına yönelik gerçekleştirilecek bir saldırı ile Japonya'da, Hindistan'da, Somali'de, Bolivya'da ya da dünyanın başka herhangi bir yerinde yer alan bir bilgisayara yönelik gerçekleştirilecek bir saldırı arasında zorluk veya meşakkat bakımından bir fark bulunmaz. Hatta suç failinin psikolojik konforu düşünüldüğünde dünyanın uzak bir ucundaki bir bilgisayar sahibine karşı suç işlemenin üst komşuya karşı işlemeye nazaran daha kolay olduğu bile söylenebilir.

Bu halde siber suçları geleneksel bir yaklaşımla ulusal sınırlar içerisinde işlendiği varsaymak ve buna göre bir mücadele ve suç takibi politikası geliştirmek; sağlı sollu sıra sıra mağazaların bulunduğu bir caddede hiçbir gerekçe olmaksızın yalnızca yolun bir tarafındaki mağazalarda hırsızlık olayı yaşanabileceğini varsayıp sadece o taraftaki mağazalar bakımından ilgili tedbirleri almaya benzemektedir.

İnternette yayına sunulan bir içerik internete bağlı olan tüm ülkelerde erişime açıktır[92]. Bu içerik dünyanın herhangi bir ülkesinde ceza yasalarını ihlal edip suç oluşturabilir. Böylelikle bir suçun fail ve mağdurları onlarca farklı ülkede mevcut olabilir. Basit bir virüs yazılımın dakikalar içinde tüm dünyanın onlarca ülkesine milyonlarca bilişim sistemine yayılabildiği düşünüldüğünde[93], ulusal sınırlar içinde suç takibi yapmaya çalışan polis ya da adli soruşturmacının bu sorun karşısında düştüğü çaresiz durum daha net anlaşılabilir.

Siber alemde en büyük tehdidi oluşturan organize siber suç örgütlerinin üyeleri dünyanın dört bir köşesinde farklı ülkelerde ikamet etmektedir[94]. Bu örgütlerin siber alemde hareket ederken kimliklerini gizlemeleri, veri iletimlerini olağan dışı yollardan yapmalarına ilaveten fiziksel olarak da farklı coğrafyalarda olmaları ve global bir tehdit teşkil etmeleri, bu suçluluk türünü sınır aşan suçluluğun ötesinde global suçluluk sınıfına sokmaktadır[95].

---

91 Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s.56.

92 Brenner, "Approaches to Cybercrime Jurisdiction", s. 3.

93 Örneğin 2000 yılında Filipinler kaynaklı olarak yayılan Love Bug virüsü iki dakika gibi kısa bir süre içerisinde yirmiden fazla ülkede yaklaşık 35 milyon bilgisayara yayılmış ve hedef sistemlere zarar vererek 10 milyar dolara yakın zarara yol açmıştır.

94 Fatih S. Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, sy.1/2, 2001, s. 39.

95 Laviero Buono, "Gearing Up The Fight Against Cybercrime in The European Union: A New Set Of Rules And The Establishment Of The European Cybercrime Centre (Ec3)", **New Journal of European Criminal Law**, sy. 3., 2012, s. 365.

Bireysel suçların ve basit suç örgütlerinin yanı sıra terör örgütlerinin ve hükümetlerin de siber suçlara başvurması söz konusudur[96]. Siber terörizm ve siber savaş adı verilen bu aktivitelerle siber suçlar daha kapsamlı ve daha ciddi global riskler teşkil etmeye başlamıştır[97]. Siyasi, hukuki ve teknik boyutlarıyla incelenmesi gereken ve müstakil olarak üzerinde durulması gereken bu kavramları yalnızca siber suçluluğun global boyutları hakkında fikir vermesi açısından zikretmekle yetiniyoruz[98]. Yine siber suçların global risk boyutunu ortaya koyması açısından bir "Uluslararası Siber Suçlar Mahkemesi" kurulması yönünde öneri ve tartışmalar olduğunu da hatırlatmakla yetiniyoruz[99].

Siber suçlarda fail ve mağdur(lar)ın farklı ülkelerde ve uzak coğrafyalarda bulunmasının yanı sıra suçun delillerinin yani değerlendirilecek verilerin bulunduğu yer sorunu söz konusudur. Global bir medya olarak tanımlanan internette veriler fiziksel olarak belirli bir veri merkezinde depolanmış halde olsa da internet etkileşimleri sayesinde verilerin bir yerde değil her yerde olduğu söylenebilir[100]. Google, Yahoo, Twitter, Facebook gibi şirketlerin dünyanın her yerinde kullanıcıları varken, bu şirketlerin merkezi ABD'de, verileri tuttukları veri hangarları ise çeşitli ülkelerde bulunmaktadır. Pek çok gerçek ve tüzel kişi verilerini kendi bilişim sistemlerinde tutmak yerine depolama hizmeti veren –sıklıkla başka bir ülkenin sınırlarında bulunan- veri merkezlerinde tutmaktadır[101]. Özellikle son yıllarda gelişen bulut bilişim teknolojisiyle sorun ayrı bir boyut kazanmıştır. Bulut bilişimde veriler dünyanın dört bir yanında veri merkezlerinde dağılırlar ve ülke sınırları arasında süre giden bir akıcılık içinde hareket ederler[102]. Bu nedenle bulut bilişim sağlayıcıları genellikle bir verinin hangi bilişim sisteminde bulunduğunun net bilgisini veremez[103].

---

[96] Örneğin Amerika Birleşik Devletleri hükümeti 2011 yılında Libya Devrimi'ne müdahale sürecinde siber atakları bir müdahale aracı olarak kullanmayı, yine aynı tarihlerde İran'ın uranyum zenginleştirme aktivitelerine siber müdahalede bulunmayı planladıklarını kabul etmiştir. Cade, "An Adaptive Approach For An Evolving Crime", s.1140.

[97] Cade, "An Adaptive Approach For An Evolving Crime…", s.1141.

[98] Siber terörizm *"bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinliklerdir."* Ya da kısaca, *"klasik anlamdaki terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi"* olarak da tanımlanabilir. Dülger, **Bilişim Suçları**, s. 187.

[99] Ulusalrarası Siber Suçlar Mahkemesi kurulması yönündeki görüş ve tartışmalar için bkz. Cade, "An Adaptive Approach For An Evolving Crime", s. 1170 vd.

[100] Sieber, **İnternetteki Suçlar**, s.55.

[101] Cade, "An Adaptive Approach For An Evolving Crime", s. 1143.

[102] Cade, "An Adaptive Approach For An Evolving Crime", s.1144.

[103] Sieber, **İnternetteki Suçlar**, s.55

Siber suçların sınır aşan yapısı suçla mücadelede polis ve adli makamların önündeki en büyük engeldir. Siber suçlarla mücadelenin yukarıda sayılan diğer zorluklarını aşan; iletişimin takip ettiği yolu, kaynak bilişim sisteminin, failin ve suçun delillerinin bulunduğu yeri teknik yöntemlerle tespit eden soruşturmacı elde ettiği bulguların kendisine ve birbirine olan coğrafi uzaklığı karşısında çaresiz kalmaktadır.

Siber suçların sınır aşan yapısının dayattığı bir zorunluluk olarak; ulusal düzeyde siber güvenliğin sağlanması ancak uluslararası işbirliğinin etkin ve güçlü bir şekilde yürütülmesi ile mümkün olabilecektir[104]. Aksi halde, sınır tanımayan siber suçluluk karşısında ulusal makamlar ülkesel sınırlarla bağlanmış bir şekilde aciz kalmaktadır[105].

2. Siber Suçların Soruşturma ve Kovuşturmasında Hukuksal Sorunlar

Yukarıda çalışmamızın kapsamının elverdiği ölçüde anlatmaya çalıştığımız üzere siber alem; yeni olan, hızla kendini yenileyen, sınırları ve kapsamı belirlenemeyen, kontrol edilemeyen, mesafe ve ülke sınırlarını tanımayan, bundan dolayı uluslararası nitelikte olan kendine has bir alandır. Siber alemde işlenen suçlar da doğal olarak aynı karakter özelliklerini taşımaktadır[106]. Buna mukabil hukuk; ulusal, muhafazakar ve işlemesi belli bir süreç gerektiren bir bilimdir; zira hukuk dayanağını devletin egemenliğinden almaktadır, devletin egemenliği ulusal ülke sınırları içinde geçerlidir ve hukuk kurallarının oluşması ile hukuk pratiğinin oluşması kaçınılmaz olarak zamana ihtiyaç duymaktadır. Suçların tespit ve takibi, suçluların yargılama ve cezalandırılmasını konu alan ceza hukuku ise belki de hukuk alanları içinde en hantal olanıdır. Ceza hukukunun son çare olması, suçların ve cezaların kanuniliği gibi ceza hukukunun sıkı sıkıya bağlı olduğu ilkelerin yanı sıra ceza adalet sistemi aktörlerinin suç takibinde gelenekselleşmiş yöntemlerden

---

[104] Zhang Xinbao, "Establishing Common International Rules To Strengthen The Co-Operatıon Of Cyber Informatıon Security", **China Legal Science**, sy. 1, 2013, s 123.
[105] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1236.
[106] Ortiz Pradillo, "Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain", **European journal of Crime**, sy, 19, 2012, s. 365.

kopamaması ve yeniliklere adapte olamaması da bu durumun sebepleri arasındadır[107].

Siber suçlarla mücadelenin zorluklarına ilişkin yukarıda bahsettiğimiz zorlukların çözümünün dünya çapında ve işbirliği halinde mücadelede olduğunu tespit etmek zor değildir. Nitekim siber suçlarla mücadelenin nasıl olması gerektiği üzerine yıllardır farklı disiplinlerde ve disiplinler arası yapılan çalışmaların ortaya koyduğu çözüm de budur. Ancak, siber suçlarla mücadele edilmesinin önünde hem ulusal ve hem de uluslararası düzeyde bir takım ciddi hukuki zorluklar bulunmaktadır.

Ulusal düzlemde, ilgili önlemlerin alınabilmesi için ülkelerin ulusal mevzuatlarının maddi ve usuli yönden yeterli olması, sınır aşan nitelikteki adli işlemlerde uluslararası düzlemde karmaşaya yer vermemek adına yetki sorunlarının çözülmesi ve başka bir devletin yetki alanına giren konularda ilgili devletin işbirliğinin sağlanabilmesi için etkin adli yardımlaşma mekanizmalarının mevcut olması gerekir. Hukuk sistemlerinin birbirlerinde farklı yanları ve uyum dirençleri de sorunun ayrı bir boyutudur. Bu bölümde amacımız bu sorunları kuşatıcı ve bütüncül yaklaşımla incelemek ve çözüme kavuşturmak değil; siber suçlara ilişkin hukuki tablonun genel olarak anlaşılmasıdır.

a) Ulusal Mevzuatlardan Kaynaklı Sorunlar

Kendine özgü yapısı dolayısıyla, ceza hukuku, idare hukuku, medeni hukuk, ticaret hukuku gibi pek çok farklı hukuki alanı ilgilendiren ve bazen de bu alanların çakıştığı kavşak noktalarında karmaşık hukuki sorunlar teşkil eden siber alem, bu özelliklerine cevap verebilecek özel hukuki düzenlemeler yapılmasını gerektirir. Siber alemin özelliklerini ve farklı yönlerini dikkate almaksızın yapılmış genel düzenlemeler, siber alemden kaynaklanan hukuki uyuşmazlıklara belli bir ölçüde uygulanabilse de bazı noktalarda bu düzenlemeler yetersiz kalmakta ve gerek maddi hukuk gerekse usul hukuku anlamında siber aleme özgü düzenlemelere ihtiyaç duyulmaktadır[108].

---

[107] Brenner, "Law, Dissonnence, and Remote Computer Searches", s. 46.
[108] Mary Thompson, "Distributed Security Architecture", Journal Of Computer & Informatıon Law, sy. 23, 2001, s. 700.

Suçta ve cezada kanunilik ve kıyas yasağı gibi iki çok önemli iki ilkeyi benimsemiş olan ceza hukuku bakımından özel düzenlemeler yapılması özellikle önemlidir[109]. Siber alemde işlenen fiiller dolayısıyla ihlal edilen menfaatlerin büyük kısmının hırsızlık, dolandırıcılık, sahtecilik suçları, hakaret suçları, terör propagandası, fuhşa aracılık, kumar oynatma, güveni kötüye kullanma, zimmet, haberleşme özgürlüğünün ihlali, mala zarar verme, pornografi ve müstehcenlik gibi geleneksel suçları oluşturuyor olması dolayısıyla siber suçların özel olarak düzenlenmesine ihtiyaç olmadığı, geleneksel suç tiplerinin siber alemde gerçekleştirilen ihlallerin cezalandırılması için yeterli olacağı da savunulmuştur[110]. Daha ziyade siber alemin ve siber suçların yapısının hukukçular tarafından ayrıntılı olarak bilinmediği ve dikkate alınmadığı dönemlerde savulan bu görüşe mukabil; ilerleyen dönemlerde bilişim teknolojilerinin gelişmesi, kullanıcı sayısının ve siber elemdeki ihlallerin de artmasıyla bu ihlal türlerinin önlenmesi ve yaptırıma bağlanması için benzerlik içeren klasik suç tiplerine bilişim sistemleri boyutunun eklenmesinin mümkün ve yeterli olamayacağı ve bunun yapılmasıyla istenilen sonucun elde edilemeyeceği anlaşılmıştır[111]. Ceza hukuku mevzuatlarının mutlaka gerekli suç tiplerini içermesi ve ayrıntılı olarak düzenlemesi gerekir. Maddi ceza hukuku kuralları, sağlanmaya çalışılan koruma ve siber suçlarla mücadelenin yalnızca bir boyutudur. Ayrıca siber sçların soruşturulması ve kovuşturulması ve genel olarak elektronik delillerin toplanması, soruşturma makamlarına yetki veren özel muhakeme kurallarının bulunmasını gerektirir[112]. Ulusal ceza adalet sistemlerinin mevzuatlarının maddi ve usuli hükümler bakımından eksik olması halinde siber suç vakaları hukuki bir mecburiyet sonucu olarak takipsiz ve sonuçsuz kalmaktadır.

Siber suçların soruşturulması ve kovuşturulmasında ulusal mevzuatların yetersiz olması sorununu ve ceza adaleti sistemi aktörlerinin karşılaştığı diğer hukuki sorunların çoğunu ortaya koyması bakımından "Love Bug" virüsü örneği önemlidir[113]. Siber suçlarla mücadeleye ilişkin pek çok önemli eserde, özellikle

---

[109] Gerard Conway, The Council of Europe as a Normative Backdrop to Potential European Integration in the Sphere of Criminal Law, **The Denning Law Journal**, sy. 19, 2007, s. 123.
[110] Caner Yenidünya/ OlgunDeğirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003, s. 109.
[111] Dülger, **Bilişim Suçları…**, s. 223-24.
[112] Dülger, **Bilişim Suçları**, s. 721.
[113] Brenner, "Approaches to Cybercrime Jurisdiction", s. 5.

mevzuatların yetersizliği ve uyumsuzluğu bakımından bir "farkındalık" noktası olarak gösterilen bu olay, 2000 yılında dünya çapında yaşanmış bir virüs krizidir.

Bilgisayarlardaki verilere zarar veren ve şifreleri çalan Love Bug virüsü, 11 Mayıs 2000'de Hong Kong'da ortaya çıktı ve iki saat içinde dünyanın 25 ülkesinde otuz dört milyondan fazla kullanıcının bilgisayarına yayıldı. Devletlerin kritik birimlerinin de etkilendiği[114] bu virüs salgınının maliyetinin 10 milyar doları geçtiği tahmin edilmektedir[115].

Bilişim uzmanları kısa süre içerisinde virüsün kaynağının Filipinler olduğunu tespit ettiler. Filipin ulusal soruşturma makamları ve FBI, yerel bir servis sağlayıcıdan aldıkları bilgiler üzerinden virüsü ürettiğinden ve yaydığından şüphelendikleri Onel de Guzman adlı kişiyi tespit ettiler. Ancak soruşturmayı yürütenler için asıl sorun bu noktada başlamaktaydı; Filipinler'de siber suçlar ayrıca düzenlenmemişti ve virüs üretmeyi ve yaymayı suç sayan bir ceza normu yoktu. Soruşturmacılar bu nedenle şüpheli hakkında arama kararı çıkartmak için dahi günlerce uğraştılar ki; bu süre şüpheliye ilgili verileri yok etmesi için yeteri kadar süre tanımış oldu. Nihayetinde arama kararı alınarak uygulandı ve Filipin ceza usul yasası yalnızca fiziki varlığı olan eşyalara el konulmasını öngörmesine ve bilişim sistemlerinde yapılacak arama ve el koyma tedbirlerine ilişkin hiçbir özel düzenleme içermemesine rağmen, şüphelinin evinde bulunan, Love Bug virüsünü ürettiği ve yaydığına ilişkin delillere el konuldu. Filipin ceza hukuku, bilişim virüsü üretilmesi ve yayılması fiillerini suç saymadığı için şüpheli hakkında hırsızlık ve dolandırıcılık suçlamalarıyla dava açıldı. Ancak Filipin mahkemeleri toplanan delillerin bir kısmını ispat bakımından elverişsiz buldu, bir kısım delilleri yabancı bir devletin adli makamlarınca toplanmış olduğu gerekçesiyle kabul etmedi ve hırsızlık veya dolandırıcılık suçlarının oluşmadığını belirterek davaları reddetti[116].

Amerika Birleşik Devletleri şüphelinin kendisine iadesi ve Amerika'da yargılanması için Filipinler'e başvuruda bulundu ancak; şüphelinin eylemleri Filipinler'de suç teşkil etmediği ve suçlu iade anlaşmaları karşılıklı cezalandırılabilirlik koşulu içerdiği için Guzman'ın Amerika Birleşik Devletleri ya

---

[114] Örneğin Amerika Birleşik Devletleri'nde Uzay Araştırmaları Merkezi (NASA) ve Merkezi İstihbarat Teşkilatı (CIA) Love Bug virüsünden etkilendiğini bildirmiştir. Marc Goodman/Susan Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace", **International Journal of Law and Information Technology**, sy. 10/2, 2002, s 140.

[115] Goodman/Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace, s 140.

[116] Brenner, "Approaches to Cybercrime Jurisdiction", s. 5.

da virüsün etkilediği bir başka ülkeye iadesi ve burada yargılanması da söz konusu olamadı. Onlarca ülkedeki binlerce mağdur ve milyarlarca dolar zarara rağmen Love Bug virüsü sorumlusu serbest bırakıldı ve hiçbir ceza almadı.

Siber suçların tarihi çok daha eskilere dayanmakla birlikte[117], Love Bug hadisesinden sonra şu hususlar noktasında ciddi bir farkındalık oluştu: Siber suçlar yapısal özellikleri itibariyle klasik suçlardan farklıdır, bu suçların soruşturma ve kovuşturmasında siber suçlara özgü maddi ceza hukuku kurallarının ve siber aleme özgü ceza muhakemesi tedbirlerinin varlığı ön şarttır; herhangi bir devletin ulusal düzeyde bu tedbirleri almamış olması yalnızca bu devlet için değil, tüm devletler için güvenlik riski teşkil etmektedir[118]. Love Bug olayı özellikle devletlerin ulusal düzlemde siber suçlara özgü düzenlemeler yapmasının önemini ortaya koymuş oldu[119]; nitekim Filipinler, Love Bug hadisesinden hemen sonra ceza yasalarında bir seri değişiklik yaptı[120].

Bir devletin suç politikası gereği bir fiili suç olarak saymasının veya saymamasının sonuçları büyük ölçüde o devletin sınırları içersinde bir sorun teşkil etmektedir. Ulaşım olanaklarının gelişmesiyle ülkesel sınırlar öncesine nazaran daha az anlam ifade etse de, fiziki alemde ceza yasalarının birincil etki alanı şüphesiz ulusal sınırların içidir. Oysa siber suçlar söz konusu olduğunda, Love Bug olayının da acı bir şekilde öğrettiği üzere bir devletin ulusal mevzuatındaki eksiklik global bir risk oluşturmak için yeterlidir[121] ve mevzuatları itibariyle siber suçlarla mücadelede gereken adımları atmamış olan devletler siber suçlular için emniyetli limanlar teşkil

---

[117] Siber suçlar 1960'lı yıllarda hukukçular tarafından tartışılmaya başlamış olup, 1970'li yıllardan itibaren ulusal mevzuatlarda siber suçlara yer verilmeye başlanmıştır (İsveç 1973, ABD 1974, Almanya 1977, Fransa 1978, Kanada 1982, İngiltere 1984, Japonya 1988, Portekiz 1991, Belçika 1995, İspanya 1995, İsviçre 1995, İtalya 1997). Bu girişimler başlangıç seviyesinde girişimler olup zaman içinde yetersiz kalmış ve özellikle 1980'li yıllardan itibaren uluslararası kuruluşlar tarafından yürütülen çalışmalarla geliştirilmiştir. Siber suçlarla mücadelede mevzuatların geliştirilmesi yönündeki uluslararası girişimler hakkında ayrıntılı bilgi için bkz. Stein Schjolberg, "Harmonizing National Legal Approaches On Cybercrime", **WSIS Thematic Meeting on Cybersecurity,** International Telecomunication Union, 1 Temmuz 2005, (erişim: 17.08.2015), http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf ;Siber suç mevzuatlarının tarihçesiyle ilgili ayrıntılı bilgi için bkz.Stein Schjolberg, **The History of Cybercrime**, Norderstedt: Cybercrime Research Instıtute GmBh, 2014.

[118] Yine Love Bug hadisesinden çıkarılan diğer sonuçlar: siber suçlar söz konusu olduğunda yetki sorunları hiç olmadığı kadar ciddi anlam ifade etmektedir ve geleneksel adli yardımlaşma yöntemleri son derece yavaş ve karmaşık kalmaktadır. Goodman/Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace", s 141.

[119] Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s.62.

[120] Goodman/Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace", s 139.

[121] Brian C. Lewis, "Preventıon Of Computer Crıme Amıdst Internatıonal Anarchy", **Amerıcan Crımınal Law Revıew**, sy. 41, 2015, s. 1359.

edebilmekte[122], bu ülkelerden kaynaklı saldırılarla dünyanın farklı köşelerindeki hedeflere karşı suç işleyen kişiler bu ülkelerin sağladığı koruma(!) ve konfor sayesinde adli takipten emin olabilmektedir[123].

Siber suçların özel olarak düzenlenmesi şarttır ancak düzenlemenin müstakil bir yasa ile yapılması zorunlu değildir[124]. Önemli olan bazı genel kabul görmüş siber aleme özgü suç tiplerinin (bilişim sistemlerine izinsiz girilmesi, bilişim verilerinin izinsiz elde edilmesi, transferi, silinmesi, bilişim sistemlerine zarar verilmesi) ve bazı geleneksel suçların siber aleme özgü işlenme şekillerinin (hırsızlık, dolandırıcılık, kumar, çocuk pornografisi, hakaret, nefret söylemi, terörizm) siber alem dikkate alınarak düzenlenmesidir. Bu düzenlemenin müstakil bir yasayla veya genel ceza yasaları içinde ilgili yerlerde yapılması ülkelerin kanun yapma politikalarına ilişkin bir tercih meselesidir[125].

Siber suçların adli takibi bakımından ceza muhakemesi hukuku alanında da bir takım özel düzenlemeler yapılması gerekir. Bunların başında bilişim sistemlerine özgü arama ve el koyma tedbirlerinin mümkün olması gelir. Bunun yanı sıra bir takım idari düzenlemelerle de bağlantılı olarak siber alemde trafik bilgisi ve veri takibinin mümkün olması ve usullerinin düzenlenmesi şarttır[126].

Ulusal düzlemde yapılması gereken düzenlemelerin neler olduğu konusunda dünya çapında geçerli ve bağlayıcı bir liste olmamakla birlikte; Avrupa Konseyi Siber Suç Sözleşmesi gibi hukuki metinler ve Uluslararası Güvenlik ve İşbirliği Merkezi Bildirgesi[127] gibi sivil girişimler üyelerine bir takım suç kategorileri ve ceza muhakemesi tedbirleri kategorileri sunmakta ve ulusal mevzuatlarını bu kategorik listelere uyumlu hale getirmelerini istemektedirler[128]. Bu listelerin ayrıntısına burada girmeyip, bunlardan Avrupa Siber Suç Sözleşmesi'nin öngördüğü maddi ve usuli hükümlere çalışmamızın ikinci kısmında yer vereceğiz.

---

[122] Mırıam F. Mıquelon, "The Convention On Cybercrıme: A Harmonized Implementatıon Of International Penal Law :What Prospects For Procedural Due Process?", **Journal Of Computer & Informatıon Law**, sy 23, 2005, s. 336.

[123] Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s. 55.

[124] Rizgar Mohammed Kadir, "The Scope and the Nature of Computer Crimes Statutes -A Critical Comparative Study", **German Law Journal**, sy. 11/6, 2010, s. 632.

[125] Dülger, **Bilişim Suçları**…, s. 225.

[126] Ian Walden, "Harmonising Computer Crime Laws in Europe", **European Journal of Crime**, Criminal Law and Criminal Justice, sy. 12/4, 2004, s.334.

[127] Uluslararası Güvenlik ve İşbirliği Merkezi, ABD'de Stanford Üniversitesi bğnyesinde faaliyet gösteren bir araştırma merkezi olup, 1999 yılında siber suçlar konusunda bir bildirge hazırlayıp, üyelerinin imzasına açmıştır.

[128] Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace", s. 173.

Love Bug gibi olayların siber suçlarla mücadelede yasal önlemlerin önemini ortaya koymuş olmasına ve devletleri ulusal düzlemde gerekli düzenlemeleri yapmaya zorlayan uluslararası girişimlere rağmen ulusal mevzuatların eksikliğinden kaynaklı sorunlar devam etmektedir. Avrupa ülkeleri büyük ölçüde mevzuatlarını güncellemiş ve gerekli maddi ve usuli düzenlemeleri yapmış durumda iken[129]; Afrika, Asya ve Güney Amerika'da halen "siber suç cennetleri" mevcuttur[130]. Ulusal mevzuatların yetersizliği konusunda örnekleri çok da uzak coğrafyalarda aramaya da gerek yoktur. Avrupa Siber Suç Sözleşmesi'ni imzalamış ve yürürlüğe sokmuş olan Türkiye'nin ulusal mevzuatı büyük ölçüde Sözleşme'nin öngördüğü maddi ve usuli hükümleri karşılasa da; henüz sözleşmeyle tam bir uyum içerisinde değildir[131]. Türk ulusal mevzuatının maddi ve usuli yönden Sözleşme'yle uyum içinde olmayan yönlerini çalışmamızın ikinci kısmında ele alacağız.

Ulusal mevzuatların yetersizliği sorunu, bir defaya mahsus seferberlikle üzerine gidilip çözülüp rafa kaldırılabilecek bir sorun değildir. Zira siber alem ve siber suçlar sürekli kendini yenilemektedir[132]. Bu nedenle mevzuatların da buna paralel olarak güncellenmesi gerekmektedir[133].

Siber suçları oluşturan fiillerin çoğunlukla tamamen yasal nitelikteki uzun süren hazırlık hareketleri ve çok kısa bir süre içinde gerçekleşen icra hareketlerinden oluşması ve ceza hukukunda hazırlık hareketlerinin cezalandırılmaması prensibinin benimsenmiş olması, internetin sınırsız bir özgürlük mecrası olarak algılanması ve özel hayatın gizliliği ve kişisel verilerin korunması noktasındaki endişeler de siber suçların adli takibi için gerekli maddi ve usuli düzenlemelerin yapılmasını zorlaştırmaktadır.

b) Uluslararası Düzlemde Hukuki Sorunlar

Dünya toplumunu oluşturan her bir ülkenin ulusal düzeyde siber suçlara karşı kendilerince mükemmel düzenlemeler yapması, siber suçlulukla etkin ve anlamlı bir

---

[129] "Comprehensive study of the problem of cybercrime", s. 4.
[130] Goodman/Brenner, "Emerging Consensus on Criminal Conduct in Cyberspace", s. 216.
[131] Mücahid Özbek, "The Impacts of European Cybercrime Convention on Turkish Criminal Law", **GSI Articletter Law Review**, s. 13, 2015, s. 74.
[132] Brenner, "Toward a Crımınal Law for Cyberspace", s. 67.
[133] Andreea Verte Olteanu, "Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime", **Journal Of Eastern-European Criminal Law**, sy. 1, 2014, s. 90.

mücadele için bir başlangıç noktası olabilse de yeterli olmayacaktır. Yukarıda farklı yerlerde anlatmaya çalıştığımız üzere siber suçlar söz konusu olduğunda ulusal sınırlar bir anlam ifade etmezler, siber suçluluk ulus aşan hatta global niteliktedir[134]. Bu nedenle ülke sınırları içinde yaşayan toplumun güvenliğini sağlamaya yönelik ulusal tedbirler tek başına yetersiz ve hatta anlamsız kalırlar[135].

Siber suçlar söz konusu olduğunda adeta tek bir toplum; dünya toplumu söz konusudur[136]. Buna göre düz bir mantıkla dünya toplumunun ortak genel ihtiyaçları çerçevesinde, ortak bir suç siyaseti belirlenmeli ve bunun ürünü olarak ortak bir evrensel ceza mevzuatı ortaya konulmalıdır[137] ve bu mevzuatı global bir polis teşkilatı ve global bir adli sistem uygulamalıdır[138]. Mevcut uluslararası toplumda bunların teorik ve pratik anlamda mümkün olmaması karşısında tek bir çözüm gündeme gelmektedir: Farklı devletlerin bir arada mücadele etmesi ya da diğer bir ifadeyle uluslararası işbirliği.

Birden çok devleti ilgilendiren siber suç vakalarında uluslararası düzlemde işbirliğinin sağlanması ve etkili bir şekilde sürdürülebilmesi için; ilgili devletlerden hangisinin hukukunun uygulanacağı ve hangi devletin adli işlemleri gerçekleştireceğinin, yani yetkinin kime ait olduğunun belirlenmesi; yetki sahibi olmayan devletin yetki sahibi olan devletten adli yardım talep etmesi ve böylelikle farklı sistemler uyum içinde bir arada uygulanarak uluslar arası koordinasyonun sağlanması gerekir. Ancak bu aşamaların her birinde yaşanan ve yaşanması muhtemel sorunlar vardır. Dolayısıyla bu bölümde yetkiye, uluslararası adli yardımlaşma hukukuna ve hukuk sistemlerinin uyum direncine ilişkin sorunları inceleyeceğiz.

---

[134] Dülger, **Bilişim Suçları**, s. 184.
[135] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1232.
[136] Konuyla ilgili bir diğer kavram olan "internet vatandaşlığı" kavramı için bkz. Dülger, **Bilişim Suçları**, s. 187.
[137] Bu yöndeki görüş ve girişimler için bkz. Ellen Podgor, "International Computer Fraud: A Paradigm For Limiting National Jurisdiction", **University of California Davis Law Review**, s. 35, 2012.
[138] Bu yöndeki görüş ve girişimler için bkz. Cade, "An Adaptive Approach For An Evolving Crime".

(1) Yetki Sorunları

(a) Yetki Kavramı

Uluslararası hukukta yetki; bir devletin toprakları üzerindeki kişiler ve eşyalar hakkında hukuki tasarruf hakkının sınırları olarak ifade edilir[139]. Yetki; devletin kural koyma ve belirli bir hukuki alanı düzenleme hakkını ifade eden *"yasa koyma yetkisi" (jurisdiction to prescribe)*, kişileri ulusal mahkemelerinde yargılama ve diğer adli işlemlere tabi tutma yetkisini ifade eden *"yargılama yetkisi" (jurisdiction to adjudicate)* ve hukuk kurallarını ve prosedürlerini tatbik ve infaz etme yetkisini ifade eden *"uygulama yetkisi" (jurisdiction to enforce)* şeklinde alt kavramlardan oluşur[140].

Ceza ve ceza muhakemesi hukuku açısından yetkinin belirlenmesinde geleneksel olarak kabul gören temel prensip *"ülkesellik" (teritoriality) prensibi*dir[141]. Yani her devlet, egemenlik haklarının bir yansıması olarak kendi ülkesel sınırları dahilinde geçerli olmak üzere ulusal maddi ve usuli ceza hukukunu belirlemek, bu sınırlar üzerinde gerçekleşen vakıaları soruşturmak, kovuşturmak ve failleri yargılamak ve yine bu sınırlar içerisinde tüm kural ve prosedürlerini tatbik etmek hakkına sahiptir. Bu kural -mefhumu muhalifinden- devletlerin sınırları dışında gerçekleşen fiiller hakkında yetkisiz olmasını da ifade etmektedir[142].

Genel kural olarak ülkesellik prensibi benimsense de, bu kural mutlak değildir. 20. ve 21. yüzyılda yaşanan gelişmelerin getirdiği coğrafi hareketlilik ve telekomünikasyon olanakları geleneksel olarak benimsenen ülkesellik prensibini boşa çıkaran senaryoları beraberinde getirmiştir[143]. Buna bağlı olarak ülkesellik prensibinin bazı istisnaları doğmuştur. Bunlar; devletin, failin vatandaş ya da oturmacı olması durumunda kendini yetkili saymasını ifade eden faile göre şahsilik ilkesi; mağdur veya suçtan zarar görenin vatandaş ya da oturmacı olması durumunda kendini yetkili saymasını ifade eden mağdura göre şahsilik ilkesi; devlete ve ulusal

---

[139] Masaki Hamano, Comparative Study in the Apporach to Jurisdiction in Cyberspace, (erişim 03.07.2015), http://www.oocities.org/siliconvalley/bay/6201/.

[140] Brenner, "Approaches to Cybercrime Jurisdiction", s. 5.

[141] Mehmet Emin Artuk/Ahmet Gökçen/Caner Yenidünya, **Ceza Hukuku Genel Hükümler**, 8. Baskı, Ankara: Adalet, 2014, s. 959;Mahmut Koca/İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**,7. Baskı, Ankara: Seçkin, 2014, s. 705; Timur Demibaş, Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara: Seçkin, 2014, s. 143.

[142] Brenner, "Approaches to Cybercrime Jurisdiction", s. 6.

[143] Brenner, "Approaches to Cybercrime Jurisdiction", s. 6.

güvenliğine yönelik tehdit oluşturan durumlarda kendisini yetkili saymasını ifade eden koruma ilkesi ve belirli suçlar nerede, kim tarafından kime karşı işlenmiş olursa olsun kendisini yetkili saymasını ifade eden evrensellik ilkesidir[144].

Egemen bir devlet yetki ilkelerini ve yetkisinin sınırlarını kendisi belirler. Daha somut bir ifadeyle hangi hallerde hangi yetki ilkesinin geçerli olacağını bizzat kendisi tayin eder[145]. Uluslararası hukukta devletlerin yetkilerini düzenleyen veya yetki uyuşmazlıklarını çözümleyen bir üst norm veya mercii yoktur[146]. Bunun doğal sonucu olarak birden fazla hukuk sistemini ilgilendiren hukuki uyuşmazlıklarda yetki uyuşmazlıkları söz konusu olur[147]. Yetki uyuşmazlıkları çoğunlukla pozitif uyuşmazlık; yani aynı uyuşmazlık konusu üzerinde birden fazla devletin yetki iddiasında bulunması şeklinde, nadiren de negatif uyuşmazlık; yani belirli bir uyuşmazlık konusu üzerinde ilgili devletlerin tümünün yetkisizlik iddiasında bulunması şeklinde gerçekleşir[148].

Devletlerin yetki sınırlarını bizzat kendilerinin belirlemesinin sonucu olarak yetki sorununun gündeme geldiği ve çözüme kavuştuğu yer ulusal yargılama makamlarıdır. Ulusal makamlar ulusal hukukun öngördüğü yetki kuralları çerçevesinde somut uyuşmazlık üzerinde yetki sahibi olup olmadıklarına karar verirler. Pozitif yetki uyuşmazlığı söz konusu olan hallerde yine ulusal yargı makamları, yetkiyi kullanmalarının makul olup olmadığına karar verirler[149].

(b) Siber Suçlarda Yetki Sorunları

Siber alem genel olarak genel yetki kurallarına tabidir[150]. Bununla birlikte, fiziksel olarak bir ülkenin sınırları içerisinde bulunmaksızın bir başka ülkede hatta

---

144 Yetki türleri ve yetkinin belirlenmesinde kabule edilen ilkelerin ayrıntıları için bkz.Brenner, "Approaches to Cybercrime Jurisdiction".

145 Cristos Velasco, "Cybercrime jurisdiction: past, present and future", **ERA Forum**, 2015.

146 Jeanne Pia Mifsud Bonicci, **Self Regulation in Cyberspace**, Leiden: Asser Press, 2008, s. 189.

147 Podgor, "International Computer Fraud", s. 316.

148 Velasco, "Cybercrime jurisdiction: past, present and future".

149 Yetkinin belirlenmesinde "makullük" kavramı ve makul yetkinin unsurları için bkz. Brenner, "Approaches to Cybercrime Jurisdiction", s. 31.

150 "Siber-yetki" (cyber-jurisdiction) kavramı, devletlerin tasarruflarından bağımsız olarak internet sistem operatörlerinin veya kullanıcılarının siber alemin belirli bir alanında kural koyma ve düzenleme yapma yetkisi için de kullanılmaktadır. Örneğin Facebook sosyal paylaşım sitesi yöneticilerinin genel kullanım kurallarını koyması ya da belirli bir Facebook kullanıcısının kendi sayfasına ilişkin kuralları belirlemesi ve uygulaması vb. Biz çalışmamızda yetki kavramını klasik anlamda yani devletin tasarruf hakkı anlamında kullanıyoruz.

birden çok ülkede, hatta dünyanın tüm ülkelerinde suç işlemenin çok kolay ve olağan olduğu siber alemde yetki sorunları çok daha sık gündeme gelmektedir[151]. Siber suçlar sınır aşan yapıları nedeniyle çoğunlukla birden fazla devletin yetki alanına girmekte, çoğunlukla olumlu, istisnaen de olumsuz yetki sorunlarına sebebiyet vermektedir. Özellikle 2000'li yılların başlarında tecrübe edilen Love Bug, Melissa, Code Red, Zeus, MyDoom gibi etkileri dünya çapında onlarca ülkede görülen siber saldırılar sonrasında siber suçlarda yetki sorunları gündeme gelmiştir[152]. Dünyanın farklı coğrafyalarında boy gösteren bu karmaşık yetki sorunları karşısında ulusal mahkemeler kendi hukuk sistemleri açısından çözümler üretmeye çalışmış ve önemli kararlara imza atmışlardr[153].

Siber suçların sık sık yetki sorunlarına yol açması karşısında bazı ülkeler siber suç yasalarında özel yetki hükümlerine yer vermektedirler[154]. Bununla birlikte çoğu ülkede siber suçlar bakımından özel bir yetki hükmü bulunmayıp, ceza yasalarındaki genel yetki hükümleri uygulanır[155]. Ülkelerin siber suç yasalarında özel yetki hükümlerine yer vermesi yetki konusunda bu ülkelerin kendi sorunlarına çözüm sunması bakımından elverişli bir yöntem olsa da, nihayetinde her devlet kendi yetkisini kendisi belirlediği için uluslararası düzlemde yaşanan yetki sorunları bakımından sorun aynı şekilde devam etmektedir.

Avrupa Konseyi Siber Suçlar Sözleşmesi ve Avrupa Birliği Konseyi Çerçeve Kararları gibi uluslararası metinler siber suçlarda yetki konusunda üye devletlere yol haritası çizme ve en azından ortak bir yetki politikası gütme çabası içinde olsa da, bu metinlerin sunduğu soyut tavsiyeden öteye geçemeyen çözümlerin yetki sorunlarına çözüm olabildiğini söylemek oldukça güçtür[156]. Siber suçlarda fiilin işlendiği yer ve uygulanacak hukukun belirlenmesi, hangi ülkenin yargılama yetkisine sahip olduğu ve sınır aşan soruşturmaların yürütülmesi konusunda yetki sorunları yaşanmaya devam etmektedir.

---

[151] Valesco, "Cybercrime jurisdiction: past, present and future".

[152] Adı geçen saldırılar ve 2000'li yılların başlarında gerçekleşen diğer büyük siber saldırılar hakkında ayrıntılı bilgi için bkz. http://www.smithsonianmag.com/ist/?next=/science-nature/top-ten-most-destructive-computer-viruses-159542266/.

[153] Örneğin ABD'de *US v. Aleksey Vladimirovic Ivanov* ve *Yahoo Inc. v, LICRA*, Avusturalya'da *Gutnick vs. Down Jones&Co. Inc*,Filipinler'de *I Love You*, Almanya'da *Frederick Töben,* Belçika'da *Yahoo Corp.* davaları uluslararası yetki sorunlarına ilişkin önemli dava ve karar örnekleridir.

[154] Örneğin ABD siber suç mevzuatı farklı suç tipleri ve muhafaza tedbirleri için özel yetki hükümleri içermektedir. Müstakil bir Siber Suçlar Kanunu'na sahip olan Portekiz de yetki konusunu bu kanunda siber suçlar bakımından özel olarak düzenlemiştir.

[155] Brenner, "Approaches to Cybercrime Jurisdiction", s. 19.

[156] Velasco, "Cybercrime jurisdiction: past, present and future".

(i) Fiilin İşlendiği Yer ve Uygulanacak Hukuk Sorunu

En yaygın olarak kabul gören ülkesellik prensibinin uygulanması için öncelikle suçun işlendiği yerin tespit edilmesi gerekir[157]. Oysa siber suçlarda suçun unsurları çok sayıda farklı ülkede bulunabilir. Fail, hareket, netice gibi suçun unsurlarından hangisinin bulunduğu yerin suçun işlenmiş sayılacağı yer kabul edileceği sorununun yanı sıra; bu unsurların bulunduğu ya da gerçekleştiği yerin neresi kabul edileceği de sorundur[158].

ABD ve Avrupa ülkeleri başta olmak üzere bir çok ülke suçun işlendiği yeri hareketin yapıldığı yer olarak kabul etmektedirler. Ceza hukukunda genel olarak hareketin esas alınmasının yanı sıra Avrupa Siber Suçlar Sözleşmesi'nin bu yöndeki hükmünün etkisi büyüktür[159]. Bununla birlikte hareketin yapıldığı yerin neresi sayılacağı da ayrı bir sorundur. Hareketin gerçekleştiği yer, failin ilk komutu verdiği anda bulunduğu ülke mi, verilerin üzerinden geçtiği ülke mi, aracı olarak kullandığı bilişim sistemlerinin bulunduğu ülke mi kabul edilecektir? Bazı siber suç mevzuatları failin suçu işlemek için verdiği komuta ilişkin elektronik etkileşimin kaynak noktasını, bazı mevzuatlar hedef noktasını bazı mevzuatlar da her ikisini de hareketin işlendiği yer olarak kabul etmektedirler[160]. En sık rastlanan formülasyon ise elektronik etkileşimin kullandığı yolda geçtiği tüm noktaların hareketin gerçekleştiği yer kabul edilmesidir[161]. Bu durumda failin komutu verdiği, verilerin depolandığı, elektronik iletişimin geçtiği, aracı bilişim sistemlerinin bulunduğu ve hedef bilişim sistemlerinin bulunduğu noktaların tamamı suçun işlendiği yer sayılmakta ve bulundukları ülkeyi işlenen suç üzerinde yetki sahibi kılmaktadır[162].

---

[157] Henrique Kaspersen, "Cybercirme and Internet Jurisdiction", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 5 Mart 2009, s. 8.

[158] Memiş, "İnternet ve Ceza Hukuku", s. 605; Brenner, "Approaches to Cybercrime Jurisdiction", s. 15.

[159] Valesco, "Cybercrime jurisdiction: past, present and future".

[160] Örneğin Amerikan siber suç mevzuatında bazı bilişim suçları bakımından elektronik iletişimin kaynak noktası (N.C. Gen. Stat. § 14-453.2), bazı suçlar bakımından hedef noktası (Conn. Gen. Stat. Ann. § 53a-261), bazı suçlar bakımından da her ikisi de (Oh. Rev. Code Ann. § 2901.11) hareketin işlendiği yer kabul edilmektedir.

[161] Bu şekilde formülasyonlara Almanya (Alman Ceza Kanunu m.3, 9/2,), Belçika (Belçika Ceza Kanunu m.2) ve Hollanda (Hollanda Ceza Kanunu m. 2) mevzuatları örnek gösterilebilir.

[162] Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, sy. 4/1, 2002, s. 117.

Singapur, Malezya gibi Asya ülkelerinde kaynak bilişim sisteminin bulunduğu yer suçun işlendiği yer olarak kabul edilmektedir. Bilişim sisteminin bulunduğu yer kriteri hareketin işlendiği yere göre daha somut bir kriter olması itibariyle daha kolay tespit edilebilir ve birden fazla ülkenin yetkili olması sonucunu doğurması daha az muhtemeldir. Bununla birlikte tam olarak nerede bulunduğu belli olmayan veya aynı anda birden fazla ülkede bulunan bulut bilişim sistemleri ve uydu sistemleri gibi bilişim sistemleri söz konusu olduğunda bilişim sisteminin bulunduğu yeri tespit etmek ve yetkili ülkeyi tespit etmek zor olmaktadır[163].

Çocuk pornografisi ve nefret söylemi gibi içerik bağlantılı suçlar söz konusu olduğunda suçun işlendiği yerin belirlenmesi ayrı bir güçlük teşkil eeder. Çünkü ne hareketin yapıldığı yer, ne kaynak ve araç bilişim sistemlerinin bulunduğu yer net olarak belirlenebilmekte ne de yapılan belirleme bu suçlar bakımından sağlıklı sonuçlar doğurmaktadır. Zira fail içeriği oluşturmak ve erişime sunmak şeklinde gerçekleştirdiği hareketin ardından fiziksel olarak başka bir ülkede bulunuyor olabilir, içeriğin bulunduğu sistem bir bulut bilişim sistemi olabilir ve yeri tespit edilemeyebilir vs. Bu ve benzeri sorunlar nedeniyle Kanada, Almanya, Hollanda, Singapur gibi pek çok ülke içerik bağlantılı suçlarda fiilin işlendiği esnada failin bulunduğu yeri, yani içerik erişime açık bulunduğu müddetçe failin bulunduğu herhangi bir yeri suçun işlendiği yer kabul ederler[164].

Ülkesellik prensibinin uygulanması için öncül şart olarak belirlenmesi gereken suçun işlendiği yer noktasında karşılaşılan bu yaklaşım farklılıklarına ilaveten, devletler ülkesellik ilkesinin istisnası olarak mağdura ya da faile göre şahsilik, koruma ve evrensellik ilkelerini de benimsemektedirler. Üstelik siber suçlarda suça ilişkin her bir unsurun birden fazla noktada bulunma veya yerinin kesin olarak tespit edilememe ihtimalinin yüksekliği yetki sorunlarının çözümünü daha da içinden çıkılmaz hale getirmektedir. Çoğu siber suç vakasında birden fazla devlet ulusal mevzuatı itibariyle kendisini yetkili saymakta, yetki sorununun çözümü ulusal mahkemelerin yetkiyi kullanmalarının makul olup olmadığı noktasında aynı yönde karar verebilmelerine bağlı olmaktadır[165].

Birden fazla devletin kendisini yetkili saydığı durumlarda hangi devletin yetkiyi kullanmasının makul olduğunu belirleyecek kriterler ulusal mahkemeler ve

---

[163] Susan W. Brenner/Joseph J. Schwerha "Transnational Evidence Gathering And Local Prosecution of International Cybercrime", **Journal of Computer & Informatıon Law**, sy. 20, 2002, s. 353.
[164] Brenner, "Approaches to Cybercrime Jurisdiction", s. 19.
[165] Brenner, "Approaches to Cybercrime Jurisdiction", s. 16.

doktrin tarafından geliştirilmekte, ancak ortak bir anlayışı yansıtacak bir üst norm veya mercii bulunmaması sebebiyle sorun çözülememektedir[166]. Birden fazla devletin kendisini yetkili sayması karşısında *çifte cezalandırma (double jeopardy)* sorunu gündeme gelmektedir. Roma hukukundan beri ceza hukukunun önemli ilkeleri arasında yer alan ve Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi ve Avrupa İnsan Hakları Sözleşmesi gibi uluslararası metinlerle teyit edilen ve koruma altına alınan *çifte cezalandırma yasağının* (*ne bis in idem*) ihlal edilmesi önemli bir sorundur. Bu sorunun çözümü için mutlaka tek bir yetkili hukuk sisteminin belirlenmesi gerekir. Bu konuda kimi hukukçular ise bazı siber suçların (örneğin birden fazla ülkede yayılan bir bilgisayar virüsü) farklı egemen devletlerde farklı menfaatleri ihlal etmiş olması durumunda (virüsün bir ülkede yalnızca bilişim sistemlerini araç olarak kullanıp izinsiz erişim suçunu, bir başka ülkede banka hesaplarından para çalarak bilişim suretiyle hırsızlık suçunu oluşturması); ilgili devletlerin aynı fiilden kaynaklı suçları ayrı ayrı soruşturup cezalandırmasının çifte cezalandırma anlamına gelemeyeceğini savunmaktadır[167].

(ii) Sınır Aşan Adli İşlemlerin Yürütülmesi

Bir siber suç vakasına uygulanacak hukukun ve hangi devletin mahkemelerinin yargılama yetkisine sahip olduğunun belirlenmesi konusundaki uyuşmazlıkların dışında, delillerin toplanması başta olmak üzere adli işlemlerin yapılması bakımından da yetki sorunları gündeme gelebilmektedir. Zira siber suçlar söz konusu olduğunda suçun delillerinin, failinin ya da mağdurunun kısacası adli işlemlerin konusunu oluşturacak kişi veya eşyaların ulusal sınırlar dışında bulunuyor olması oldukça muhtemeldir[168].

Uygulanacak hukukun belirlenmesine ilişkin sorunlara nispeten, sınır aşan nitelikteki adli işlemlerin yürütülmesine ilişkin yetki sorunları oldukça basit ve uyuşmazlık sayısı da azdır. Zira uygulama yetkisi uluslar arası hukuk tarafından daha net çizgilerle sınırlandırılmıştır[169]. Uluslararası hukukun en temel ilkelerinden birisi olan ve Uluslararası Adalet Divanı'nın 1926 tarihli *Lotus* kararında net ve ayrıntılı

[166] Brenner, "Approaches to Cybercrime Jurisdiction", s. 42.
[167] Brenner, "Approaches to Cybercrime Jurisdiction", s. 42.
[168] Brenner/Schwerha "Transnational Evidence Gathering", s. 354.
[169] Kaspersen, "Cybercirme and Internet Jurisdiction", s. 8.

bir şekilde ifade edilen *"egemenlik ilkesi"* uyarınca bir devlet kendi sınırları içerisinde her türlü yetkiyi kullanabilir, ancak bir başka devletin egemenlik sınırları içinde hiçbir yetkisi söz konusu olamaz. Kendi sınırları dışında bir adli işlem yapma ihtiyacı duyan soruşturma makamları adli yardımlaşma mekanizmaları ile muhatap devletten yardım almak zorundadır.

Uluslararası hukukta uygulama yetkisine ilişkin kurallar, bir ülkenin adli makamlarının fiziksel olarak bir başka ülkede bulunarak adli işlemleri yapmasını açıkça yasaklamakla birlikte; siber alemde fiziksel olarak orada bulunmaksızın bir başka ülkede bazı adli işlemleri yapabilmek mümkündür[170]. Egemen devletin izni ve rızası alınmadan, iletişim teknolojilerinin sağlamış olduğu imkanlarla fiziksel olarak da ilgili devletin sınırları içinde bulunmadan bu devletin sınırları içerisinde bulunan bir bilişim sisteminde arama yapılması veya bu devletin sınırları içerisinde gerçekleşen bir etkileşimin takip edilmesi egemenlik haklarının ihlali oluşturacak mıdır, yoksa bu işlemleri gerçekleştiren adli makamların uygulama yetkisi içinde hareket ettikleri mi kabul edilecektir?

İngiltere, İspanya, Amerika Birleşik Devletleri gibi bazı ülkelerin adli makamları fiziksel olarak sınırın ötesine geçmeden gerçekleştirilen soruşturma işlemleri bakımından yetkili olduklarını kabul etmekte ve sınır ötesi dijital soruşturma işlemlerine sıklıkla başvurmaktadırlar[171]. Özellikle Amerikalı soruşturmacıların uyguladığı sınır ötesi arama işlemleri çok defa başka devletlerle uygulama yetkisi konusunda sorunlara sebebiyet vermiştir[172].

---

[170] Brenner, "Approaches to Cybercrime Jurisdiction", s. 22.

[171] Edward Snowden tarafından ifşa edilen NSA faaliyetleri Amerikan kolluk güçlerinin siber suçlara ilişkin soruşturmalarda sıklıkla internet üzerinde gözetleme ve erişim ve sınır ötesi bilişim sistemlerinde delil arama el koyma tedbirine başvurduğunu ortaya koymuştur. Valesco, "Cybercrime Jurisdiction: past, present and future".

[172] ABD'nin bu konuda yabancı devletlerle yaşadığı sorunların en büyük örneği *Invita* olayıdır. Amerikan şirketlerine gerçekleşen yoğun saldırıların Rusya'da bulunan Vasiliy Gorshkov ve Alexey Ivanov isimli bilişim korsanları tarafından düzenlediğini tespit eden Amerikan makamları ABD ile Rusya arasında suçlu iade anlaşması olmadığı için şüphelileri ABD'ye çekmeye bu şekilde soruşturma ve kovuşturmayı yapmaya karar verirler. *Invita* ismini verdikleri, aslında gizli soruşturmacı FBI ajanlarından oluşan bir bilişim şirketi üzerinden şüphelileri ABD'ye getiren soruşturmacılar şüphelilerin ABD'de kullandıkları bilgisayarlarına bazı casus yazılımlar yükleyerek Rusya'daki bilgisayarlara ve verilere erişmek için gerekli şifreleri elde ederler. Bu sayede Rusya'da bulunan bilgisayarlarda arama yapılır ve şüpheliler mahkum edilir. Şüphelilerin Rus makamları haberdar etmesi üzerine Rusya, diplomatik yollardan FBI ajanlarının gerçekleştirdikleri işlemlerin suç olduğunu ve iligililerin kendisine iadesini talep eder. ABD ile Rusya arasında suçlu iade anlaşması olmadığı için Rusya'nın bu talebi cevapsız bırakılır. Brenner, "Approaches to Cybercrime Jurisdiction", s. 21.

Bazı hukukçular sınır ötesine yönelik işlemlerin ilgili devletlerin egemenlik haklarının ihlali olduğunu[173], bazıları ise bunların uygulama yetkisinin kapsamında olduğunu savunmaktadırlar[174]. Orta yolu bulmaya çalışan üçüncü bir grup ise herkes tarfından erişilebilir veriler bakımından herhangi bir egemenlik hakkının ihlal edilemediğini ve soruşturmacıların bu tür veriler bakımından sınır ötesi işlemleri yapmaya yetkili olduğunu savunmaktadır[175]. Avrupa Siber Suçlar Sözleşmesi de bir başka orta yol tutumunu benimsemekte ve 32. maddede herkesin erişimine açık olan ve ilgilisinin rızası ile elde edilen veriler bakımından soruşturma makamlarının sınır ötesi soruşturma işlemleri yapmaya yetkili olduğunu ifade etmektedir. Sözleşmenin çokça eleştirilen bu hükmüne çalışmamızın ikinci bölümde ayrıntılı olarak değineceğiz. Netice olarak sınır ötesinde gerçekleştirilen soruşturma işlemlerinde uygulama yetkisi sorununa ilişkin henüz bir çözüm bulunabilmiş değildir[176].

(2) Uluslararası Adli Yardımlaşma Hukukuna İlişkin Sorunlar

Siber suç soruşturmasında ya da kovuşturmasında yetki sorunları çözümlenip, bir takım adli işlemlerinin yerine getirilmesinde bir başka devletin adli makamlarının yetkili olduğu anlaşıldığı taktirde, bu yetkili makamdan hukuki yardım alınması yani adli yardımlaşma gündeme gelir. Şüpheli ve sanıkların ifadelerinin alınması veya sorgularının yapılması; mağdur, müşteki, katılan, tanık ve bilirkişilerin dinlenilmesi, bilgi ve delil temini, banka kayıtları, muhasebe belgeleri, şirket dosyaları ve ticari belgeler de dâhil olmak üzere, ilgili belge ve kayıtların asıllarının veya tasdikli suretlerinin sağlanması, delil toplamak amacıyla kazançların, malvarlıklarının, araç-gerecin ya da diğer hususların belirlenmesi veya izlenmesi, delil amaçlı arama ve el koyma, eşya ve yer incelemesi, el koyma ve müsadereye dair yabancı mahkeme kararlarının infazı adli yardımlaşmanın konusunu teşkil edebilir[177].

---

[173] Jack Goldsmith, "The Internet and the Legitimacy of Cross-Border Searches", **Chicago Public Law and Legal Theory**, (erişim: 07.07.2015)http://www.law.uchicago.edu/academics/publiclaw/resources/16.JG.Internet.pdf.

[174] Nicolai Seitz, "Transborder Search: A New Perspective in Law Enforcement", **Yale Law School**, (erişim: 07.07.2015), http://islandia.law.yale.edu/isp/digital%20cops/papers/Seitz_Nicolai.pdf.

[175] Brenner, "Approaches to Cybercrime Jurisdiction", s. 23.

[176] Kaspersen, "Cybercirme and Internet Jurisdiction", s. 28.

[177] Kemal Şimşek, "Uluslararası Adli Yardımlaşma Konusunda Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri Üzerine", **Adalet Dergisi**, sy. 45, 2013, s.148.

Farklı hukuk sistemlerinin ceza adalet sistemi aktörlerinin işbirliği içinde hareket etmesinin somut yansıması ve aksiyona dökülmüş hali olan adli yardımlaşma, hukuki sorunların siber suçlara karşı uluslararası işbirliğine engel teşkil etmesinin en somut yaşandığı alandır. İki devlet arasında adli yardımlaşma anlaşmasının olmaması çoğu zaman adli yardımlaşmayı imkansız hale getirir[178]. Var olan adli yardımlaşma sözleşmelerinin karşılıklı cezalandırılabilirlik koşullarının veya bazı adli yardımlaşma türleri için dayanak suçun cezasının belirli bir sınırın üstünde olması gibi diğer koşulların çok ağır olması, adli yardımlaşma prosedürlerinin zahmetli ve hantal olması gibi hukuki sorunlar ve bunlara ilaveten uygulamada yaşanan fiili sorunlar da siber suçlar söz konusu olduğunda adli yardımlaşmanın etkisiz kalmasına neden olabilir.

(a) Adli Yardımlaşma Anlaşmalarının Eksikliği

Uluslararası adli yardımlaşma ilgili devletler arasında yürürlükte bulunan ikili ya da çok taraflı sözleşmeler vasıtasıyla gerçekleştirilir. Bu sözleşmeler muhatap devleti adli yardımlaşma talebini yerine getirmeye zorlar. İki devlet arasında bu şekilde adli yardımlaşma sözleşmesi bulunmaması halinde de, uluslararası teamül hukuku kuralları ve mütekabiliyet (karşılıklılık) ilkesi çerçevesinde yürütülür[179].

Çok taraflı adli yardımlaşma sözleşmeleri çoğunlukla bölgesel niteliktedir[180]. İkili sözleşmeler bakımından ise birbirine coğrafi olarak yakın olan ve siyasi, sosyal ve ticari ilişkileri yoğun olan devletler arasında çoğunlukla adli yardımlaşma sözleşmeleri mevcut olmakla birlikte, coğrafi anlamda uzak olan ve geleneksel olarak ilişkileri yoğun olmayan devletler arasında herhangi bir sözleşme bulunmayabilir[181]. Bu halde tek çözüm diplomatik yollardan irtibata geçerek müstakil her bir olay için muhatap devletten adli yardım talep etmektir. Aralarında adli yardımlaşma sözleşmesi bulunmayan iki devletin diplomatik ilişkilerinin zaten

---

[178] Seitz, "Transborder Search", s. 44.

[179] Şimşek, "Uluslararası Adli Yardımlaşma", s. 146.

[180] Ceza hukuku alanında adli yardımlaşma konusunda birçok çok taraflı uluslararası sözleşme bulunmaktadır. Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (CİKAYAS), Suçluların İadesine Dair Avrupa Sözleşmesi, Hükümlülerin Nakline Dair Avrupa Sözleşmesi, Ceza Yargılarının Milletlerarası değeri Konusunda Avrupa Sözleşmesi, Ceza Kovuşturmalarının Aktarılması Konusunda Avrupa Sözleşmesi, Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El Konulmasına İlişkin Sözleşme örnek olarak verilebilir.

[181] Jordan Paust, "Cybercrimes and the Domestication of International Criminal Law", **Santa Clara Journal of International Law**, sy 5/2, 2007, s. 437.

zayıf olduğu düşünüldüğünde bu ihtimalin gerçekleşmesi çok zor, mümkün olduğu halde de oldukça zaman kaybettiricidir[182]. Halbuki siber suçların coğrafi uzaklıktan etkilenmeksizin kolaylıkla dünyanın herhangi bir noktasından bir başka noktasına yönelik olarak işlenebilmesi dolayısıyla geleneksel anlamda ilişkileri zayıf olan devletler sıklıkla aynı siber suç vakasının tarafları olabilmektedir[183].

(b) Adli Yardım Taleplerinin Ret Sebepleri

Adli yardımlaşma ile ilgili oluşturulan gerek çok taraflı gerekse iki taraflı tüm uluslararası metinler adli yardım taleplerinin ret sebeplerini öngörmektedir. Adli yardımlaşma sözleşmelerinde ret nedenleri mutlak ve nisbi ret nedenleri olarak öngörülebilmekle birlikte, özellikle devletlerin adli yardımı reddetme niyeti söz konusu olduğunda ret nedenleri geniş yorumlanarak öngörülen çerçevenin dışında yardım taleplerinin reddine de gerekçe teşkil edebilir[184]. Zira bu nisbi ret sebepleri çoğu kez yardım talep edilen devlete adli yardımlaşmayı işlemez hale getirecek kadar geniş bir takdir hakkı verir[185].

Adli yardımlaşma sözleşmelerinde en sık rastlanan ret sebebi karşılıklı cezalandırılabilirlik (mutual criminality) koşulu ya da diğer bir ifadeyle çifte cezalandırma (double criminality) ilkesidir[186]. İlke, yardım talebine konu fiilin, talep eden ülkenin yanı sıra, talep hakkında karar verecek ülkede de suç sayılması gerekliliğini ifade eder[187]. Suçluların iadesi ve arama el koyma kararlarının infazı başta olmak üzere pek çok yardımlaşma konusu açısından karşılıklı cezalandırılabilirlik koşulu vazgeçilmez bir ret sebebidir[188]. Karşılıklı cezalandırılabilirlik koşulu talep eden ülkede suça konu olan fiilin her iki ülkede de suç sayılması şeklinde (*in abstacto*) olabildiği gibi fiilin talep edilen ülkede tüm koşullarıyla cezalandırılabilirlik şartlarını taşıması şeklinde(*in concreto*) de olabilir.

---

[182] Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s.63.

[183] Örneğin ABD ve Rusya arasında 2002 yılına kadar adli yardımlaşma sözleşmesi mevcut olmadığı için 1990'lı yıllarda yükselen siber suçluluk vakalarında iki devletin adli makamları adli yardımlaşmaya başvuramamıştır. Bu konuda daha önce bahsettiğimiz *Invita* olayı güzel bir örnektir.

[184] Candaş Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", **İstanbul Barosu Dergisi**, sy. 84/3, 2010, s. 1703.

[185] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma, s. 1702.

[186] Singh/Singh, "Cyber Crime Convention And Trans Border Crımınality", s.62.

[187] Ümit Kocasakal, **Avrupa Birliği Ceza Hukuku'nun Esasları**, İstanbul: Vedat Kitapçılık, 2004, s.142.

[188] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", s. 1705.

Özellikle ikinci halde, yani fiilin tüm unsurlarıyla cezalandırılabilir olması şartı arandığı hallerde adli yardımlaşma çok ciddi ölçüde zorlaşır[189].

Çifte cezalandırılabilirlik dışında adli yardımlaşma sözleşmelerinde sıklıkla rastlanan diğer ret sebepleri; yakalama ve tutuklama kararlarının adli yardımlaşma haricinde tutulması[190], askeri suçların adli yardımlaşma dışında tutulması[191], talep konusu fiilin siyasi[192] veya mali[193] suç sayılmasının ihtiyari ret sebebi sayılmasıdır.

(c) Prosedürlerin Karmaşık ve Uzun Olması

Adli yardıma ihtiyaç duyan devletin adli makamlarının ilgili talebi yetkili devletin adli makamlarına iletmesi her iki devletin kendi bürokrasilerinde belirledikleri uluslararası adli yardımlaşma talebi iletme ve kabul etme mekanizmaları üzerinden gerçekleşmektedir. Bu mekanizmalar çoğunlukla birkaç

---

189 Aldesco, "The Demıse Of Anonymıty", s. 96.

190 Ceza İşlerinde Adli Yardımlaşma Konusunda Avrupa Sözleşmesi ve iki taraflı sözleşmelerin çok büyük bir kısmı bu hususta hüküm içerirler. Tutuklama ve mahkûmiyet kararlarının infazının bu sözleşmelerce mutlak bir ret sebebi olarak öngörülmüş oluşunun iki temel nedeni olduğu ileri sürülmüştür: Öncelikle ceza kararlarının bir diğer ülkede geçerliliği ve uygulanabilirliği hususunda adli yardımlaşma bünyesinde telakki edilmeyen bir yapılanma söz konusudur. Ve devletler kural olarak bilgi sahibi olmadıkları bir yasa metnine ve yine kural üzerinde geniş bir fikir sahibi olmadıkları bir ceza prosedürü takip edilerek alınmış kararların icrasında belirleyici rol oynamak ve bu suretle sorumluluk almayı çok da tercih etmemektedir. Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", s. 1703.

191 Ceza İşlerinde Adli Yardımlaşma Konusunda Avrupa Sözleşmesi ve Fransa'nın Kolombiya, Uruguay, Amerika Birleşik Devletleri ve Avustralya ile yapmış olduğu iki taraflı ceza işlerinde adli yardımlaşma sözleşmeleri bu duruma örnek gösterilebilir.

192 Buna en somut örnek Terörizmin Cezalandırılması Hakkında Avrupa Sözleşmesi'dir. Sözleşme'nin temel amacı, terör suçlularının iade taleplerinin, bu suçların siyasal suç olmaları nedeniyle reddedilmesinin önüne geçmektir. Zira geçmişte Avrupa'da Fransa başta olmak üzere diğer Avrupaülkeleri siyasal suç olduğundan bahisle birçok iade ve adli yardım talebini reddetmiştir.

193 Türkiye'nin Avustralya, Azerbaycan ve Hindistan ile imzaladığı adli yardımlaşma anlaşmaları mali suçlarla ilgili taleplerin reddedilebileceğini düzenlemektedir. Aynı yönde düzenlemeler Fransa'nın Avustralya, Mısır, Kanada, Cibuti, Tunus'la imzalamış olduğu adli yardımlaşma sözleşmelerinde de mevcuttur.

aşamadan oluşan, uzun ve meşakkatli süreçleri içerirler[194]. Bir yardımlaşma talebinin tamamlanması hiç değilse aylar alabilir[195].

Adli yardımlaşmanın tarafı olan devletler bu konuda ne kadar iyi niyetli ve istekli olurlarsa olsunlar ve bu iyi niyet ve isteklerini imzaladıkları adli yardımlaşma anlaşmalarının maddi koşullarına ne ölçüde yansıtmış olurlarsa olsunlar, bu şekilde uzun, gereksiz ve zahmetli prosedürlerin varlığı adli yardımlaşmayı anlamsız kılmaktadır[196]. Ulusal kurumlar arasında dahi resmi yazışmaların iletilme ve işlem görme hızı düşünüldüğünde siber suçlar gibi çok kısa süre içinde hareket edilmesi gereken durumlarda mevcut adli yardımlaşma mekanizmaları hantal ve işlevsiz kalmaktadır[197].

Adli makamların zaman kaybetmeden ve mümkünse vasıtasız olarak, gerekirse resmi yazışma yollarının dışında e-posta, telefon vb. iletişim araçlarıyla irtibata geçmelerini mümkün kılacak usullerin kabul ve tatbik edilmesi bu sorunu çözecektir. Avrupa Birliği üyesi ülkeler arasında yargısal işbirliğini öngören EUROJUST, Avrupa Birliği Konseyi tarafından üye devletler arasında adli yardımlaşma prosedürlerini kolaylaştırmak ve hızlandırmak için 2002 yılında 2002/584/ JHA nolu Çerçeve Kararla kabul edilen Avrupa Yakalama Müzekkeresi (European Arrest Warrant) ve 2008 yılında 2008/978/JHA nolu çerçeve kararla kabul edilen Avrupa Delil Müzekkeresi (European Evidence Warrant) adli makamların doğrudan birbirleriyle irtibata geçerek adli yardımlaşma sağlamalarına zemin sağlaması itibariyle örnek alınabilecek önemli uygulama örnekleridir[198].

---

[194] Örneğin Türkiye bakımından adli yardımlaşma taleplerinin nasıl iletileceği Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün yayınladığı genelgelerle belirlenmekle ve adli yardımlaşmanın konusuna göre prosedür değişmekle birlikte genel olarak; adli yardımlaşmaya ihtiyaç duyan bir yerel mahkeme adli yardımlaşma evraklarını tamamlayarak bulunduğu yargı yerindeki Cumhuriyet Başsavcılığı'na vermekte (verilen başsavcılığın bulunduğu yerde ağır ceza mahkemesi yoksa başsavcılık bu talebi en yakın ağır ceza mahkemesinin bulunduğu Cumhuriyet Başsavcılığına göndermekte), Cumhuriyet Başsavcılığı bu talebi Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'ne iletmektedir.

[195] Stahl, "The Uncharted Waters Of Cyberspace", s. 250.

[196] Sibyl Stein, "Combating Crime in the European Union: The Development of EU Policy after the Convention", **European Journal of Crime, Criminal Law and Criminal Justice**, sy 12/4, 2004, s. 353.

[197] Şimşek, "Uluslararası Adli Yardımlaşma", s. 153.

[198] Avrupa Yakalama Müzekkeresi ve Avrupa Delil Müzekkeresinin ayrıntıları için bkz. European Arrest Warrant, Summaries of European Union Legistlation, (erişim 01.08.2015), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33167; European Evidence Warrant, Summaries of European Union Legistlation, (erişim 01.08.2015), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0015.

(d) Uygulama Sorunları

Adli yardımlaşma mekanizmalarında ulusal ve uluslar arası mevzuatlardaki maddi ve usuli eksikliklerden başka uygulamacıların eksiklikleri ve hataları da mevcut sistemlerin işleyişini aksatır. Ülkeden ülkeye değişmekle birlikte; adli makamların uluslararası adli işbirliği mevzuatlarına hakim olmaması, soruşturma ve yazışma işlemlerinin eksik yapılması ve adli yardımlaşma evraklarındaki her türlü eksikliğin iade nedeni yapılması, yabancı dil bilen yeterli sayıda personel bulunmaması öne çıkan sorunlar olarak sayılabilir[199].

(e) Polisiye İşbirliği ve Adli Yardımlaşmanın Ayrı İşlemesi

Ceza işlerinde işbirliği ya da ceza hukukunda adli yardımlaşma denildiğinde çoğu zaman adli işbirliği ve polisiye işbirliği bir arada kastedilmekle birlikte bu iki kavram birbirinden farklıdır[200]. Adli işbirliği suç işlenmesinden sonra başlayan adli süreçte adli makamların yaptığı adli işlemlere ilişkin iken, polisiye işbirliği polis teşkilatlarının gerçekleştirdiği adli işlevler de dâhil olmak üzere ve bunun yanında suçun önlenmesi ve henüz adli süreç başlamadan suç vakalarının ortaya çıkarılmasına yönelik idari nitelikteki işlemlere ilişkindir[201].

Polisiye işbirliğinde zikredilmesi gereken işbirliği mekanizmalarının başında Uluslararası Polis Teşkilatı (INTERPOL), Avrupa Polis Ofisi (EUROPOL), Amerika Polis Birliği (AMERİPOL) ve Güney Doğu Asya Ülkeleri Polis Müdürleri Derneği (ASEANAPOL) gelmektedir. Bu tamamıyla hukuki ve bilinen kurumların yanı sıra teknolojik ve bilimsel açıdan temellendirilmiş olsa da hukuki açıdan temellendirilmemiş pragmatik yolları kullanan, medya ve toplumun daha az bilgi sahibi olduğu ikinci bir tür polisiye işbirliği daha mevcuttur[202].

---

[199] Şimşek, "Uluslararası Adli Yardımlaşma Konusunda Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri Üzerine", s. 149-156.

[200] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", s. 1692.

[201] Cezar Peta, "Community and National Structures for Police and Judicial Cooperation", **Public Security Studies**, sy. 3, 2014, s. 269.

[202] Bunlara örnek olarak TREVI, Cross Channel Inteligence Konferansı, NEBEDEACPOL, STAR, Güney Batı Çalışma Grubu, Hazeldonk Grubu, Bern Kulübü, Viyana Kulubü, QUANTICO, Egmont Grubu verilebilir. Bu girişimler hakkında ayrıntılı bilgi için bkz. Jacqueline Klosek, "The Development of International Police Cooperation within the EU and Between the EU and Third

Bazı yönleriyle teknik hukuk açısından yasak, yapısal açıdan imkansız, demokrasi açısından ise tehlikeli olarak görülen bu ikinci tür polisiye işbirliği, suçlulukla mücadele ve güvenlik alanlarında meydana çıkan toplumsal zorunluluklar nedeniyle günümüzde kaçınılmaz hale gelmiştir ve siyasi açıdan da tercih edilmektedir[203]. Bu tür polisiye işbirliği istihbarat faaliyetlerini de kapsadığı ve çoğu zaman hukuken kabul edilebilirliği tartışmalı olan yöntemleri içerdiği için, polisiye işbirliğine yönelik anlaşmalar ve sözleşmeler çoğunlukla gayrı resmi niteliktedir ve bu nedenle çalışmaları erişilebilir ve kontrol edilebilir değildir[204].

Hukuki açıdan sakıncalı yanlarına rağmen pratik yöntemler kullanan ve başarılı sonuçlar veren polisiye işbirliği girişimleriyle adli işbirliği girişimlerinin bir arada ve koordineli yürümesi suçla etkin mücadele edilmesi bakımından önemlidir[205]. Özellikle siber suçlulukla mücadelede hem adli süreçleri pratikleştirmek ve hızlandırmak hem de polisiye tedbirleri hak ihlalleri bakımından adli kontrol altında tutabilmek amacıyla polisiye ve adli işbirliği girişimlerinin mutlaka koordineli olması gerekir.

(3) Hukuk Sistemlerinin Uyum Direnci

Farklı toplumsal gerçekliklere dayanan, farklı egemen güçlerin ürünü olan farklı hukuk sistemlerinin her biri kendine has özellikler ve diğer sistemlerle uyumsuzluklar içerirler[206]. Yasalar, toplumsal ihtiyaçların ve gerçekliklerin şekillendirdiği, egemen gücün somutlaştırdığı bir ceza siyasetinin ürünü olarak meydana gelirler. Her devlet kendi ulusal sınırları içerisinde toplumsal huzuru korumak amacıyla, kendi kültürel, tarihi, sosyal, coğrafi dinamiklerini göz önüne alarak maddi ve usuli ceza yasalarını yapar[207]. İnsan doğasının coğrafyadan bağımsız ortak yanları, devletlerin ceza siyasetlerinin evrensel bilimsel çalışmalar etrafında

---

Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof", **American University International Law Review**, sy. 14/3, 1999, s.599-656.

[203] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", s. 1692.

[204] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", s. 1693.

[205] Pedro Verdelho, "The Effectiveness of International Cooperation Against Cybercrime: Examples of Good Practice", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 12 Mart 2008, s. 39.; Libor Klimek, "Combating Attacks Against Information Systems", **Masaryk University Journal of Law and Technology**, sy.6, 2012, s. 89.

[206] Thomas Elholm, "Does EU Criminal Cooperation Necessarily Mean Increased Repression?",**European Journal of Crime**, Criminal Law and Criminal Justice, sy. 17, 2009, s. 224.

[207] Artuk/Gökçen/Yenidünya, **Ceza Hukuku Genel Hükümler**, s. 3.

şekillenmesi, tarihsel süreçte ulaşım ve haberleşme olanaklarının gelişmesi sayesinde farklı coğrafyalardaki insan topluluklarının etkileşiminin artması ve özellikle son yüzyıllardaki globalleşmenin etkisiyle modern hukuk sistemlerinin büyük ölçüde benzerlik göstermesi söz konusu olsa da, her hukuk sistemi kendine has ve diğerleriyle çelişen yönler barındırırlar[208].

Ülkesellik prensibinin geçerli olduğu ceza hukuku açısından sınırları içerisinde bulunduğu devlet dışındaki ceza yasaları bir kişiyi istisnaen ilgilendirir[209]. Nihayetinde her ulusal ceza mevzuatı kendi toplumuna uygulanır, toplumlar arasındaki farklılıklar yasalara da paralel olarak yansırlar ve bu farklılıklar global sistemde büyük krizlere sebebiyet vermezler[210].

Siber suçlarla mücadele söz konusu olduğunda farklı hukuk sistemlerinin işbirliği halinde uygulanmasında ve özellikle uluslararası adli yardımlaşmada bu hukuk sistemlerinin birbirlerinden farklı ve birbirleriyle uyuşmayan yanları sorun olarak öne çıkar. Farklı hukuk sistemlerinin maddi ceza hukuku, ceza muhakemesi hukuku ve diğer ulusal hukuk kuralları birbiriyle uyumsuz olabilir ve bu durum adli yardımlaşma mekanizmalarının işlemesini zorlaştırıp farklı hukuk sistemlerinin ceza adalet sistemi aktörlerinin sınır aşan siber suçluluğa karşı işbirliği halinde mücadele etmelerini engeller[211].

Farklı hukuk sistemlerinin siber suçlara karşı uyum ve işbirliği içinde mücadele etmesinin önündeki en büyük engel siber suç mevzuatlarının sözü ve manası itibariyle farklı olmasıdır. Bilişim sistemlerine ve bilişim verilerine karşı işlenen suçlar gibi bazı siber suç kategorileri üzerinde giderek yaygınlaşan bir uzlaşı söz konusu olmakla birlikte[212], özellikle bilişim sistemleri kullanılarak işlenen diğer suçlar bakımından ciddi farklılıklar ortaya çıkmaktadır. Bir ülkede suç sayılan bir fiil bir başka ülkede tümüyle yasal hatta korunan bir değer teşkil edebilir[213], aynı suç tipi görünüşte her iki ülkenin ceza yasalarında da yer almasına karşın suçun unsurları

---

[208] Elholm, "Does EU Criminal Cooperation Necessarily Mean Increased Repression?", s. 224.
[209] Pardis Moslemzadeh Tehrani/Nazura Abdul Manap, "A Rational Jurisdiction For Cyber Terrorism", **Computer Law and Security Review**, sy, 29/6, 2013, s. 90.
[210] Podgor, "International Computer Fraud", s.224.
[211] Paul Rosenzweig, "The Internatıonal Governance Framework For Cybersecurity", **Canada-Unıted States Law Journal**, sy. 37, 2012, s. 418.
[212] Goodman/Brenner, "Emerging Consensus on Criminal Conduct", s. 199.
[213] Örneğin Avrupa ülkelerinin birçoğunda nefret suçu oluşturacak bir içerik Amerika'da Anayasa'nın 1. Ek Maddesi ile korunan ifade özgürlüğü içinde değerlendirilebilmektedir.

farklı olabilir[214], suç tipi bire bir aynı kavramlar kullanılarak tanımlanmış olsa bile kavramlara yüklenen anlamlar ve farklı diller arasındaki çeviri sorunları bile hukuk sistemlerinin maddi normlar itibariyle zıtlık içinde olmaları sonucunu doğurabilir[215]. Siber aleme yönelik bilişim sistemi, siber suç gibi temel kavramların tanımında dahi görüş birliği olmadığı göz önüne alındığında görünüşte ortak kavramlar söz konusu olduğunda dahi hukuk sistemlerinin çatışması muhtemeldir[216]. Özellikle ifade özgürlüğü gibi kritik konular söz konusu olduğunda kültürel farklılıklardan kaynaklı hukuki farklılıklar çözümsüz bir hal alabilir[217].

Ülkelerin siber suçlulukla mücadelede kabul ettiği ve uyguladığı ceza muhakemesi tedbirlerindeki farklılıklar da uyumsuzluk ve dolayısıyla sorun teşkil edebilmektedir[218]. Farklı adli teşkilatların delil elde etmede diğerlerinin aşina olmadığı farklı teknik yöntemleri kullanmasının yanı sıra[219], asıl sorun bir hukuk sisteminde benimsenen tedbirlerin diğerinde hukuka aykırı olarak değerlendirilmesi ve bu yolla elde edilen delillerin soruşturma ve kovuşturmada kullanılamamasıdır[220].

---

214 Örneğin 2004 yılında İnternet üzerinden yetişkinlere özel içerik sunan bir Alman firması, sitesinde 17 yaşındaki kişilere ait yetişkin içerikli görüntülerin yer alması dolayısıyla Singapur ve Belçika'da çocukların erişimine açık pornografik içerik yayınlamak suçuyla dava edildi. Almanya'da yetişkin içerikler için yaş sınırı o dönem 14 olduğu için Alman makamları söz konusu site sahibi ve sorumlularının iadesine ilişkin adli yardımlaşma taleplerini iddia konusu eylemler Almanya'da suç teşkil etmediği gerekçesiyle reddetmiştir. Brenner, "Approaches to Cybercrime Jurisdiction", s. 3.

215 İngiltere ve Amerika Birleşik Devletleri gibi benzer hukuk sistemlerine ve benzer kültürel altyapıya sahip iki ülke arasında bile aynı kavrama yüklenen anlamlar farklılık gösterebilmektedir. Örneğin 2004 yılında çocuklara ilişkin müstehcen içerikli bir web sitesine ilişkin İngiltere'den ABD'ye yöneltilen bir adli yardımlaşma talebi, Amerikan makamlarının içeriği müstehcen bulmamaları üzerine reddedilmiştir. Aynı dili kullanan, benzer kültürel altyapıdan gelen ve benzer hukuk sistemlerinin parçası olan iki adli makam arasında müstehcenlik (obscenity) kavramının içeriği konusunda yaşanan bu uyuşmazlık, farklı dili kullanan hukuk sistemlerine, farklı kültürel altyapılara ve farklı dillere mensup iki adli makam arasındaki olası yorum farklılıklarına ilişkin fikir vermesi bakımından enteresan bir örnektir. Brenner, "Approaches to Cybercrime Jurisdiction", s. 17.

216 Nadina Foggetti, Transnational Cyber Crime, Differences Between National Laws and Development of European Legislation: by Repression?", **Masaryk University Journal of Law and Technology,** sy. 2, 2008, s. 35.

217 Nefret suçları konusunda ifade özgürlüğü konusundaki yaklaşım farklılıklarından kaynaklı olarak ortaya çıkan çözümü zor sorunları önemli bir örnektir. Ayrıca 2007 yılında İran'da görülen bir dava sorunun kültürel farklılıklarla ne kadar ilgili olduğunu ortaya koyması bakımından enteresandır. İran'da internet üzeriden su savaşı organize eden bir grup kadın ve erkek genel ahlaka karşı suç işledikleri suçlamasıyla yargılandılar. İnternet üzeriden su savaşı organize etmenin suç teşkil etmesi İran'ın yerel dinamikleri dışında açıklanamaz ve anlaşılamaz görünmektedir. Cade, "An Adaptive Approach For An Evolving Crime", s.1150.

218 Brenner, "Law, Dissonnence, and Remote Computer Searches", s. 51.

219 Janet Reno, United States Attorney General, Keynote Address at the Meeting of the G8 Senior Experts' Group on Transnational Organized Crime, (erişim 11.07.2015), http://www.usdoj.gov/criminal/cybercrime/agfranc.htm.

220 Brenner, "Law, Dissonnence, and Remote Computer Searches", s. 50. Siber alemde hukuka aykırı delillerin dışlanması sorununa ilişkin ayrıntılı bilgi için bkz. Shah, "The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace", s. 250-278; Ayrıca hukuka aykırı delillerin ceza muhakemesi süreçlerinden dışlanmasına ilişkin genel teori ve

Başvurulan genel muhakeme tedbirlerinde yaşanması muhtemel sorunlar bir yana[221]; *uzaktan erişimle arama*[222] tedbiri gibi siber aleme özgü tedbirler söz konusu olduğunda ulusal mevzuatların çatışması kaçınılmazdır[223]. Amerika Birleşik Devletleri gibi az sayıdaki ülkede uzaktan erişimle arama yoluyla elde edilmiş deliller hukuka uygun olarak kabul edilirken pek çok ülkede hukuka aykırı hatta suç olarak değerlendirilmektedir[224].

Siber alemin aktörü olan ve suçları ve suçluları tespit etme, delil elde etme gibi siber suçlarla mücadele süreçlerine dahil olan kamu (Türkiye'deki Telekomünikasyon İletişim Başkanlığı gibi) ve özel hukuk (servis sağlayıcılar gibi) kişileri hakkındaki özel hukuk ve idare hukukuna ilişkin düzenlemelerdeki farklılıklar da söz konusudur ve bunlar da sorun teşkil edebilmektedir. Söz gelimi yabancı bir ülkede bulunan bir servis sağlayıcıdan elde edilmesi gereken trafik verileri söz konusu olduğunda, ilgili servis sağlayıcının tabi olduğu ulusal mevzuat uyarınca veri saklama yükümlülüğü önem arz etmektedir.

B. Siber Suçlarla Mücadelede Karşılaşılan Sorunların Çözümü Olarak Etkin Uluslararası İşbirliği

1. Uluslararası İşbirliğinin Önemi

Siber suçlarla mücadele siber alemin kendine has yapısı, siber suçluluğun yeni bir kavram olması ve sürekli olarak kendini yenilemesi, siber alemin süjelerinin anonim kalma şansı ve veri iletim tekniğinin kontrol direnci, delil elde etme ve değerlendirme süreçlerinin uzmanlık gerektirmesi ve faille mağdur arasında mekansal mesafe bulunması gibi siber alemin ve siber suçların teknik yapısından kaynaklı zorluklardır. Bunlara ilave olarak ulusal mevzuatların yetersiz olması,

---

karşılaştırmalı hukuk incelemesi için bkz. Murat Volkan Dülger, **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)**, Ankara, Seçkin, 2014.

221 "*Bodrum ... Sulh Ceza Mahkemesinin .. Esas sayılı dosyasında, sanık savunmasının alınması için Rusya Federasyonuna istinabe talebinde bulunulduğu, Rusya Federasyonu kendi mevzuatına uygun olmadığı gerekçesi ile bu şekilde bir talebi yerine getiremeyeceğini belirterek, sanık savunması alınması talebini içerir Bodrum Sulh Ceza Mahkemesinin evraklarını bila ikmal iade etmiştir.*", Şimşek, "Uluslararası Adli Yardımlaşma", s.156.

222 Uzaktan erişimle arama; adli soruşturma makamlarının delil elde etmeyi umdukları hedef bir bilişim sistemine, fiziksel olarak müdahale etmeksizin; virüs yazılım (Trojan Horse) göndererek bilişim sisteminde yer alan veriler içinde arama yapmalarını ifade eder.

223 Brenner, "Law, Dissonnence, and Remote Computer Searches", s. 21.

224 Brenner, "Law, Dissonnence, and Remote Computer Searches", s. 51.

uluslararası yetki sorunları, adli yardımlaşma hukukuna ilişkin sorunlar ve hukuk sistemlerinin uyum direnci gibi hukuki zorluklar da siber suçlarla mücadeleyi zorlaştırmaktadır.

Yukarıda Siber Suçlarla Mücadelenin Zorluğu ve Mevcut Sorunlar (I.A) başlığı altında açıklamaya çalıştığımız, genel olarak siber suçların sınır aşan ve global yapısının farklı yansımaları olan bu zorlukların tümünün tek bir sihirli çözümle üstesinden gelinmesi mümkün değildir. Ancak siber suçlarla mücadelenin ortaya koyduğu bu zorluklarla dolu tablonun mecbur kıldığı bir mücadele yöntemi vardır; bu da uluslararası işbirliğidir.

Doktrinde belirtildiği gibi, *"siber suçlara karşı mücadele ya global olacaktır ya da hiç anlamı yoktur"*[225]. Yani siber suçlarla mücadelede uluslararası işbirliğinin tesis edilmesi "olursa faydalı olur" şeklinde ifade edilebilecek bir tavsiye değil, "olmazsa olmaz" bir koşuldur[226]. Siber suçların soruşturulabilmesi, kovuşturulabilmesi ve siber suçluluğun önlenebilmesi uluslararası işbirliğinin etkin bir şekilde yürütülmesini gerektirir[227].

Uluslararası düzlemde işbirliği mekanizmalarının istihbarat ve casusluk faaliyetleri şeklinde kötüye kullanılması yönündeki endişelerden dolayı devletlerde siber suçlarda işbirliği yönünde bir niyet kayması söz konusu olsa da[228], siber suçluluğun arz ettiği tehlike ve ulusal düzlemde mücadelenin başarısızlığa mahkum olması karşısında uluslararası işbirliği kaçınılmazdır[229].

2. Etkin Uluslararası İşbirliğinin Unsurları ve Özellikleri

Uluslararası işbirliği devletlerin ulusal, bölgesel ve global menfaatlerini koruma ve geliştirme amacıyla, bağımsızlık ve egemenlik ilkeleri çerçevesinde farklı alanlarda çoğunlukla iki veya çok taraflı sözleşmelere dayanarak farklı yöntemlerle

---

[225] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi...", s. 1233.
[226] Xinbao, "Establishing Common International Rules", s. 126.
[227] Cerezo/Lopez/Patel, "International Cooperation to Fight Transnational Cybercrime", s 13.
[228] Xinbao, "Establishing Common International Rules To Strengthen The Co-Operatıon Of Cyber Informatıon Security", s. 122; Brian M. Mazanec, "Why International Order in Cyberspace Is Not Inevitable", **Strategic Studies Quarterly**, Summer, 2015, s. 79.
[229] James Forsyth/Billy Pope, "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace", **Strategic Studies Quarterly**, Winter, 2014, s. 124.

yardımlaşmalarını ifade eder[230]. Yukarıda siber suçlarla mücadelenin zorluklarını ve sorunları anlatırken yer yer belirtmiş olmakla birlikte, siber suçlarda adli takibi ve etkin bir suçla mücadele zemini sunacak bir uluslararası işbirliğinin sahip olması gereken unsurları ve özellikleri tespit etmekte ve bir arada saymakta fayda görüyoruz.

1) Mevcut işbirliği mekanizmaları klasik anlayışı yansıttıkları ve siber suçluluk fenomenine cevap veremedikleri için klasik işbirliği mekanizmaları ve anlayışı terk edilerek siber suçlara özgü bir işbirliği anlayışı ve mekanizması geliştirilmelidir[231].

2) Uluslararası işbirliği iki taraflı veya bölgesel girişimler şeklinde parçalı bir yapıda değil; olabildiğince geniş bir kapsamda ve mümkünse global olmalıdır. Siber suçlara açık kapı bırakılmaması adına girişimlerin kuşatıcı ve global olması önemli bir unsurdur. Bu ihtiyaç nedeniyle siber suçlarla mücadelenin bir dünya polisi ve dünya siber suçlar mahkemesi eliyle yürütülmesi önerileri ciddiyetle ele alınmalıdır[232].

3) İşbirliğinin tarafı olan devletlerin ulusal mevzuatları siber suçlarla mücadeleye uygun zemin sunacak şekilde düzenlenmeli ve birbirleriyle uyumlaştırılmalı, daha güzel bir ifadeyle ahenkleştirilmelidir. Bağlayıcı uluslararası sözleşmeler, model siber suç yasası ya da kategorik listelerle devletlerin ulusal mevzuatlarında bulunması gereken maddi ve usuli hükümleri empoze etmelidirler[233].

4) Adli yardımlaşma uluslararası işbirliğinin yalnızca bir boyutudur. Siber suçların adli takibinin zorluğu karşısında suçun önlenmesine ilişkin idari ve polisiye tedbirler siber güvenliğin sağlanabilmesi adına daha çok umut vaat etmektedir[234]. Adli işbirliğinin yanı sıra polisiye ve idari işbirliği de sağlanmalı, bu üç alan bir arada ele alınmalı ve koordine edilmelidir[235].

5) İşbirliği mekanizmaları hızlı ve pratik bir şekilde işleyebilmeli devletler bunun için uygun teknik ve yapısal donanımı sağlamalı, yeterli sayıda ve nitelikte personel istihdam etmelidirler. Ulusal makamların birbirleriyle vakit

---

[230] Georgeta Modiga, "Importance And Necessity of International Judicial Cooperatıon in Criminal Matters", **International Journal of Juridical Sciences**, sy.1 , 2014, s.89.
[231] Velasco, "Cybercrime Jurisdiction: past, present and future".
[232] Cade, "An Adaptive Approach For An Evolving Crime…", s.1175.
[233] Xinbao, "Establishing Common International", s. 128; Broadhurst, "Developments in the global law enforcement of cyber-crime", s. 412.
[234] "Comprehensive study of the problem of cybercrime", s. 11.
[235] Modiga, "Importance And Necessity of International Judicial Cooperatıon in Criminal Matters", s. 103.

kaybetmeden irtibat kurmasını sağlayacak güvenli iletişim kanalları belirlenmeli, yerel saat farkı gibi özel durumlar da dikkate alınarak yardımlaşma taleplerinin her an ulaştırılabilir ve yerine getirilebilir olması sağlanmalıdır[236].

6) Devletlerin aynı finansal ve teknolojik imkanlara sahip olmamasının sonucu olarak siber suçlarla mücadele noktasında eşit düzeyde bilgi ve donanıma sahip olmamaları söz konudur. İşbirliğinin önemli bir parçası da teknoloji ve yöntem bilgisi (know-how) paylaşımı olmalıdır. Siber alemin sürekli gelişen yapısı göz önüne alınarak düzenli bilgi paylaşım mekanizmaları tesis edilmelidir.

7) Siber suçlulukla mücadelede rol alan personelin bilgi ve tecrübe eksikliği sorununu aşmak için düzenli meslek içi eğitim hakim ve savcılar başta olmak üzere adli ve idari personelin hem siber suçların teknik özellikleri hem de işbirliği hukuku konusunda eğitilmesi de önem arz etmektedir[237].

8) Teknolojinin sınırları belirlenemeyen ve dağınık yapısı karşısında sadece kamu olanaklarıyla suçla mücadele edilmesi yeterli değildir. Bireysel özgürlükler ve güvenlik kaygılarının dengelenmesi zorunluluğu da kamu olanaklarıyla yürütülen mücadeleyi sınırlamaktadır. Bu durumda siber suçlarla etkin mücadele klasik güvenlik politikalarının terk edilerek "dağıtılmış güvenlik" (distributed security) anlayışı benimsenmelidir[238]. Gerek sivil toplum yoluyla yürütülecek mücadele ile[239], gerekse kullanıcıların yeterli bilinç ve korunma mekanizmalarına sahip olması sağlanarak[240] sivil unsurlar da siber suçlarla mücadeleye dahil edilmelidir[241].

---

[236] Verdelho, "The Effectiveness of International Cooperation Against Cybercrime", s. 37.

[237] "The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 27 Şubat 2013, s. 9.

[238] Susan Brenner, "Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model", **Journal of International Commercial Law and Technology**, sy. 2/2, 2007, 60.

[239] Siber suçlarla mücadele eden uluslararası sivil kuruluşlara Norse, National Cyber-Forensics & Training Alliance, London Action Plan ve European Financial Coalition gibi sivil toplum kuruluşları ve Norton, FireEye, AlienVault, AVG Technologies, RSA, IBM ve Microsoft gibi ticari kuruluşlar örnek gösterilebilir. Ayrıntılı bilgi için http://www.itbusinessedge.com/slideshows/top-25-cybersecurity-companies-to-watch-in-2015-11.html.

[240] Bu konuda EUROJUST bünyesinde faaliyet gösteren Avrupa Siber Suç Merkezi'nin (European Cybercrime Center), ABD'de Siber Suç Şikayet Merkezi'nin (Cyber Crime Complaint Center), İngiltere'de Ulusal Dolandırıcılık ve Siber Suç İhbar Ağının (National Fraud and Cybercrime Reporting Center) ve Avustralya'da Online Siber Suç İhbar Merkezi'nin (ACORN) internet üzerinden herkesin erişimine açık oalrak sundukları siber suç ihbar etme olanakları önemli örneklerdir. http://www.actionfraud.police.uk/reporting-fraud, http://www.acorn.gov.au/, http://www.ic3.gov/default.aspx, https://www.europol.europa.eu/content/report-cybercrime-online.

[241] Brenner, "Toward a Criminal Law for Cyberspace…", s. 106; Broadhurst, "Developments in the global law enforcement of cyber-crime", s. 412.

Adli makamların siber alemde rol alan çeşitli kamu ve özel aktörlerle mümkün olan en geniş ölçüde işbirliği yaparak, hem kendilerinin hem de diğer aktörlerin siber suçlar ve elektronik deliller konusunda farkındalık, bilgi ve donanımlarını güçlendirerek ve bu sayede siber suç ve elektronik delil sorunlarıyla baş etmeye çalışmasına "kapasite inşası" (capacity building) sistemi adı verilmektedir. Siber suçlara karşı işbirliğinde kapasite inşası anlayışının benimsenmesi gerekmektedir[242].

9) Suçla mücadelede ve suçların adli takibinde bir yandan toplumsal güvenlik kaygıları gözetilirken diğer yandan bireysel haklar ve özgürlüklerin gözetilmesi gerekir. Siber suçlar bakımından bu dengeyi kurmak ve korumak özellikle zordur. Zira siber alemin özgürlükçü yapısı, ifade özgürlüğü, haber alma özgürlüğü, girişimcilik hürriyeti başta olmak üzere birçok özgürlük ve hakkın icra edilmesi bakımından ayrı bir öneme sahiptir[243]. Bunun yanı sıra kişisel ve ticari veriler çoğunlukla bilişim araçlarında tutulmaktadır. Bu durumda siber suçlarla mücadelenin ve bu alanda uluslar arası işbirliğinin bireysel hak ve özgürlükleri gözeterek özellikle kişisel verilerin korunması noktasında gerekli yasal ve yapısal güvenceler sağlanacak şekilde yürütülmesi olmazsa olmaz bir şarttır[244].

10) Siber suçluluğun kendini yenileyen yapısı karşısında işbirliği araç ve mekanizmalarının da yenilenmesi, güncellemeye elverişli olması gerekir. Bu kapsamda işbirliği sözleşmeleri kolay tadil hükümleri içermeli, gerekli güncellemeleri tespit etmek adına izleme komisyonları oluşturulmalıdır. Siber güvenlik ve siber suçlulukla mücadelenin devletlerin dış politikaların düzenli bir maddesi haline gelmesi ve "siber diplomasi" (cyber-diplomacy) denilen bu gündeme önem verilmesi gerekir[245].

3. İşbirliğini Tesis Etmeye Yönelik Uluslararası Girişimler

Yukarıda anlatmaya çalıştığımız veriler ışığında, uluslararası işbirliğinin kaçınılmaz olması nedeniyle, günümüzde siber suçlulukla mücadelede işbirliğini

---

[242] "Capacity Building Programs on Cybercrime", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 1 Kasım 2013, s. 5.

[243] Dawn C. Nunziato, **Net Neutrality and Free Speech in The Internet Age**, California: Stanford Law Books, 2009, s. 153.

[244] Eyal Benvenisti/George W. Downs, "Court Cooperation, Executive Accountability and Global Governance", **Nyuj Int'L L. & Pol.**, sy, 51, 2009, s. 933; Broadhurst, "Developments in the global law enforcement of cyber-crime", s. 415.

[245] Dana Danca, "Cyber Diplomacy - A New Component of Foreign Policy", **Journal of Law and Administrative Sciences**, sy. 3, 2015, s. 92.

sağlamaya yönelik uluslararası kuruluşlar ve çalışmalar olduğu gibi, çok ciddi hukuksal düzenlemeler de bulunmaktadır[246].Çalışmamızın ana konusunu teşkil eden ve ikinci bölümde ayrıntılı olarak inceleyeceğimiz Avrupa Konseyi Siber Suçlar Sözleşmesi dışındaki uluslararası girişimlerin başlıcalarını özet halinde aktarmaya çalışacağız.

a) Birleşmiş Milletler

Siber suçluluk 1980'li yılların ortalarından itibaren Birleşmiş Milletler'in gündemine girmiştir. Bu yıllarda Birleşmiş Milletler bünyesinde gerçekleşen Suçların Önlenmesi ve Suçluların Tretmanı Kongrelerinde siber suçla mücadelede çözüm arayışları gündeme gelmiştir[247]. BM Genel Kurulu'nun 45/121 (1990) sayılı Kararı siber suç mevzuatına ilişkindir[248]. Bu karar doğrultusunda BM tarafından 1994 yılında siber suçların önlenmesi ve adli takibi konusunda bir elkitabı hazırlanmıştır. 2000 yılında, BM Genel Kurulu'nun 55/63 (2000) sayılı Kararı ile, bilişim teknolojilerinin kötüye kullanımı ve bunlar aracılığıyla suç işlenmesine karşı mücadele konusu ele alınmıştır[249]. 2002 yılında alınan bir başka Genel Kurul Kararı (56/121 (2002)) da aynı konuda benzer ve daha ayrıntılı içeriktedir[250]. Takip eden iki yılda alınan iki Genel Kurul Kararında da (57/239 (2003) ve 58/199 (2004) siber güvenliğin ve uluslararası işbirliğinin önemi vurgulanmıştır[251]. Daha sonraki yıllarda da siber güvenlik ve siber suçlar çeşitli Genel Kurul kararlarına konu olmuştur[252]. Bunların yanı sıra 2011 yılında BM nezdinde, Siber Suçlara Dair Hükümetlerarası Uzmanlar Grubu da kurulmuştur, bu grup düzenli toplantılar yapmakta ve raporlar yayınlamaktadır.

Birleşmiş Milletler bünyesinde gerçekleştirilen bu girişimler global girişimler olması itibariyle önemli olmakla birlikte, gerek bahsi geçen genel kurul kararlarının

---

[246] Dülger, **Bilişim Suçları**, s. 186.
[247] Hasan Sınar, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", **Prof. Dr. Çetin Özek Armağanı**, İstanbul, 2004, s. 767.
[248] A/RES/45/121 (14.12.1990).
[249] A/RES/55/63.
[250] A/RES/56/121.
[251] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s.1239.
[252] Örneğin 60/177 (2006) sayılı Karar ve 64/211 (2010) sayılı Karar.

gerekse Uzmanlar Grupu raporlarının tavsiye niteliğinde olup, bağlayıcı olmaması nedeniyle umulan başarıyı sağlayamamaktadır[253].

b) Avrupa Birliği

Avrupa Birliği'nde siber suçlara yönelik anılması gereken ilk metin Konsey'in 2005 tarihli "Bilişim sistemleri aleyhinde saldırılara dair Avrupa Birliği Konseyi Çerçeve Kararı"dır[254]. Karar ile temel olarak üye devletlerin maddi ceza mevzuatlarının iyileştirilmesi amaçlanmıştır. Bu karar AB içindeki siber suçlulukla mücadele konusundaki ilk ciddi girişimdir[255]. Ancak Karar, önerdiği suç tipleri ve tanımların muğlak ve yoruma açık olduğu ve bu surette mevzuatların uyumlaştırılması noktasında eksik kaldığı gerekçesiyle eleştirilmiş[256], Avrupa Birliği Komisyonu tarafından raporlaştırılan bu eleştiriler doğrultusunda 2007 yılında AB'nin siber suçlulukla mücadele politikasını daha net ortaya koyacak şekilde revize edilmiştir[257].

2009 yılında yürürlüğe giren Lizbon Antlaşması'nın m.82-86 hükümleriyle AB'de, üye devletlerin maddi ve usuli ceza hukuku hükümlerini uyumlulaştırma aşamasına geçilmiştir. Anlaşmanın 83. maddesiyle AB'ye, siber suçlar da dahil pek çok sınır aşan suç tipi bakımından maddi hukuka ve usul hukukuna ilişkin asgari standartları tespit eden kurallar öngörme yetkisi tanınmıştır. Bu itibarla, artık siber suçlara ilişkin mevzuatın geliştirilmesi konusunda AB'nin hukuken bağlayıcı tasarruflarda bulunma yetkisi bulunmakta ve siber suçlar bakımından AB ile üye devletler arasında "paylaşılmış yetki" söz konusu olmaktadır[258].

2013 yılında kabul edilen "Bilişim Sistemleri Aleyhinde Saldırılara Dair Direktif", 2005 tarihli Bilişim Sistemleri Aleyhinde Saldırılara Dair Avrupa Birliği Konseyi Çerçeve Kararı'nın yerini almıştır[259]. Direktif ile finansal siber suçlar, hukuka aykırı içerikler, elektronik delillerin toplanması, muhafazası ve

---

[253] Broadhurst, "Developments in the global law enforcement of cyber-crime", s. 417.
[254] Konsey Çerçeve Kararı 2005/222/JHA, 24 Şuabt 2005.
[255] Elaine Fahey, "The EU ' s Cybercrime and Cyber-Security Rulemaking : Mapping the Internal and External Dimensions of EU Security", **European Journal of Risk Regulation**, sy.1, 2014, s. 51.
[256] Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking", s. 1239.
[257] Avrupa Parlamentosu için Komisyon Raporu, The Council and the Committee of the Regions—Towards a general policy on the fight against cyber crime (COM(2007) 267 final).
[258] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s.1239.
[259] Avrupa Parlamentosu ve Konsey Direktifi, 2013/40/EU, 12 Ağustos 2013.

değerlendirilmesi konularında, detaylı yetki kuralları da içeren kapsamlı bir AB siber suç mevzuatı oluşturulmak istenmiştir[260]. Direktifin öne çıkan hükümleri bilişim sistemlerine izinsiz erişim, bilişim sistemlerine müdahale ve verilere müdahale suçlarının çok ağır bir şekilde cezalandırılması[261] ve yeni suç işleme yöntemlerine karşı özel bir strateji geliştirilmesine önem vermesidir[262]. Direktifin öne çıkan bir başka yönü ise yetkiye ilişkin hükümleridir. Direktif uyarınca kısmen de olsa sınırları dışında işlenmiş bir suç üzerinde yetki iddiasında bulunacak bir üye devletin Komisyon'u bilgilendirme zorunluluğu bulunmaktadır. Nevi şahsına münhasır bir ulus üstü kuruluş olan AB bünyesinde karşımıza çıkan "paylaşılmış yetki" kavramı siber suçlarda yaşanan yetki sorunlarına yeni bir boyut getirse de, Direktif'in bu hükmü olumlu yetki uyuşmazlıkları bakımından dikkate alınması gereken değerli bir adımdır.

Avrupa (Birliği) Polis Ofisi EUROPOL tarafından kurulmuş olan Yüksek Teknolojili Suçlar Merkezi (High Tech Crime Centre) Avrupa çapındaki sınır aşan siber suçların soruşturulmasında koordinasyonu sağlamayı amaçlamaktadır. Bu doğrultuda 2010 yılında EUROPOL bünyesinde, Avrupa Komisyonu, EUROJUST ve AB ülkelerinin siber suçlulukla mücadele birimlerinin başındaki kişilerden oluşan bir platform olan Avrupa Siber Suç Timi (European Cybercrime Task Force) kurulmuştur. Platformun görevi siber suçlulukla mücadelede, AB içinde uyumlu bir yaklaşımın geliştirilmesinde ve teşvikinde yardımcı olmak ve suç işlemekte siber teknolojinin kullanımından kaynaklanan sorunlara cevap bulmaktır. AB'de siber suçlulukla mücadelede en önemli "altyapısal" unsur 2013 yılında kurulan Avrupa Siber Suç Merkezi'dir (European Cybercrime Center). EUROPOL bünyesinde Lahey'de kurulan Merkez'in, siber suç ihbarına ortak bir standart getirmeyi, polis, adli makamlar ve diğer aktörler arasında bilgi paylaşım mekanizmalarını geliştirmeyi ve bu yolla siber suçlulukla mücadelede AB'nin odak noktası olması amaçlanmaktadır[263].

c) G8 Grubu Ülkeleri

---

[260] Fahey, "The EU ' s Cybercrime and Cyber-Security Rulemaking", s. 1240.
[261] Bu suçların iki yıldan beş yıla kadar hapis cezasıyla cezalandırılması öngörülmektedir.
[262] Özellikle botnet saldırı türleri direktifin özel strateji geliştirilmesine önem verilmektedir. Fahey, "The EU ' s Cybercrime and Cyber-Security", s. 1240.
[263] Fahey, "The EU ' s Cybercrime and Cyber-Security Rulemaking", s. 1240.

Gayri safi milli hâsılaları en 8 büyük devletten (ABD, Almanya, Fransa, İngiltere, İtalya, Japonya, Kanada ve Rusya'dan) oluşan G-8 (Group of Eight) nezdinde, 1997 yılında Yüksek Teknolojili Suçlara Dair Alt Komite (High-Tech Crime Subgroup) kurularak siber suçlarla mücadele konusu ele alınmıştır. Komite'nin çalışmalarını takiben, G8 devletlerinin İçişleri ve Adalet Bakanları, yüksek teknolojili suçlarla mücadele etmek için birtakım temel ilkeleri ve on hususdan oluşan bir eylem planını kabul etmişlerdir[264].

G8 bünyesinde farklı zamanlarda yapılan çeşitli çalışmalarda, dijital "suç sığınaklarının" yok edilmesinin önemi, siber suçlarla mücadelede kullanılabilecek usul hukuku tedbirleri, internetin suç amacıyla kullanılmasını önlemek için global bir kapasite inşa programının gerekliliği, siber suçlarla mücadelede etkili karşı-önlemlerin geliştirilmesi, internetin terör amacıyla kullanılması meselesi gibi konularında tespitler ve öneriler ortaya konulmuştur[265].

G8 girişimlerinin en önemlisi 2004 yılında kararlaştırılan siber suçlarla mücadelede İrtibat Noktaları Ağı'dır (Contact Points Network). Polis ve adli makamların haftanın yedi günü yirmi dört saat her an irtibata geçebilmeleri amacıyla kurulan İrtibat Noktaları Ağı, Avrupa Siber Suçlar Sözleşmesi tarafından da örnek alınmıştır. Çalışmamızın ikinci kısmında bu konudan ayrıntılı olarak bahsedeceğiz.

d) Ekonomik İşbirliği ve Kalkınma Örgütü

Ekonomik İşbirliği ve Kalkınma Örgütü OECD, üye devletlerin siber suçlarla mücadelede konusunda politika geliştirmelerinde yol göstermeyi amaçlayan çalışmalar yapmaktadır. Mali Görev Gücü (Financial Action Task Force)[266] tarafından yaplan çok sayıda çalışmadan en önemlisi; Görev Gücü tarafından hazırlanan ve 2002 yılında OECD Konseyi tarafından kabul edilen "Bilgi Sistemleri ve Ağlarının Güvenliği İçin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" adlı belgedir[267]. 11 Eylül saldırılarından sonra yükselen siber terörizm endişeleri

---

[264] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s.1240.
[265] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s.1241.
[266] Mali Görev Gücünün ortaya çıkışı, görevleri ve yapısı hakkında ayrıntılı bilgi için bkz: Murat Volkan Dülger, **Suçtan Kaynaklanan Mal Varlığı Değerlerinin Aklanmasına İlişkin Suçlar ve Yaptırımlar**, Ankara, Seçkin Yayıncılık, 2011, s. 121 vd.
[267] Belgenin tam metni için: (erişim: 10.07.2015), www.oecd.org/EN/document/0,EN-document-29-nodirectorate-no-12-33186-29,00.html.

konusunda tavsiyelerden oluşan belge bağlayıcı olmamakla birlikte, siber alemin güvenliğine ilişkin konularda önemli bir mutabakatı yansıtmaktadır[268].

e) INTERPOL

Uluslararası Polis Teşkilatı INTERPOL, üye teşkilatları arasında koordinasyonu sağlamakta, bunlara teknik ve pratik destek sunmakta, ayrıca polislerin siber suçlulukla mücadelenin gerektirdiği özel uzmanlık bilgisine sahip olması ihtiyacı üzerinde durarak, bu ihtiyacı karşılamak adına uluslararası eğitim programları ve uygulamacılara yönelik pratik bilgilerle rehberlik sunan el kitapları hazırlamaktadır[269].

Siber suçluluğun teknik boyutlarının anlaşılması, mücadele yöntemlerinin teknik adaptasyonunun sağlanması amacıyla Singapur'da INTERPOL Global Yenilik Kompleksi (Global Innovation Complex) IGIC kurulmuştur. Üye teşkilatlara gerekli uzmanlık bilgisinin aktarılması, gerekli eğitimlerin verilmesi ve uyumlulaşmanın sağlanması INTERPOL Dijital Suç Merkezi (Digital Crime Center) eliyle yürütülmektedir. Siber Toplanma Merkezi (Cyber Fusion Center) zararlı internet faaliyetlerinin gerçek zamanlı görüntülenmesi ve yorumlanması, istihbarat paylaşımı gibi bir çok noktada üye teşkilatlara önemli bir yardım hizmeti sunmaktadır. Adli Bilişim Laboratuarı (Digital Forensic Laboratory) üye teşkilatlara pratik adli bilişim hizmeti sunmanın yanı sıra, yeterli seviyede yerel adli bilişim laboratuarlarının kurulması için de teknik destek ve eğitim sunmaktadır.

Avrupa-Asya, Amerika, Afrika, Ortadoğu-Kuzey Afrika Çalışma Grupları, bölgesel polis örgütleriyle siber suçlara özgü işbirliği yürütmektedir.

Siber suçlarla mücadelede uluslararası işbirliğini tesis etmeye yönelik Asya Pasifik Ekonomi Konseyi (APEC), Güney Doğu Asya Uluslar Birliği (ASEAN), Güney Doğu Asya Ülkeleri Polis Müdürleri Derneği (ASEANAPOL) gibi daha birçok kuruluş tarafından gerçekleştirilen girişimler mevcut olmakla birlikte çalışmamızı sınırlı tutabilmek adına bu girişimlerin ayrıntısına yer vermiyoruz[270].

---

[268] Broadhurst, "Developments in the global law enforcement of cyber-crime", s. 417.
[269] Çalışmaların ayrıntıları için bkz. http://www.interpol.int/Crime-areas/Cybercrime/Activities.
[270] Bu girişimler hakkında ayrıntılı bilgi için bkz. Gercke, "Understanding Cybercrime".

İkinci Bölüm
AVRUPA SİBER SUÇLAR SÖZLEŞMESİ

Avrupa Siber Suçlar Sözleşmesi (ETS 180) Avrupa Konseyi bünyesinde, üye ve gözlemci devletler tarafından hazırlanmıştır. Sözleşme, 2001 yılında imzalanmış olup, siber suçlarla mücadele alanındaki ilk bağlayıcı uluslararası düzenlemedir. Sözleşme, hem ilk olması hem de kapsamlı içeriği itibariyle alanındaki en önemli uluslararası hukuki metin olarak görülmektedir[271].

Sözleşme, taraf devletlere siber suçlarla mücadele konusunda ulusal düzeyde uymaları gereken bir dizi yükümlülük getirmekte ve tarafların siber suçlara karşı işbirliği içinde mücadele edebilmelerini sağlamak amacıyla uluslararası adli işbirliğini düzenlemektedir. Ulusal düzeyde alınması öngörülen önlemlerle taraf devletlerin ulusal mevzuatlarının siber suçlarla mücadele edebilecek yeterli seviyeye getirilmesi ve uyumlulaştırılması amaçlanmaktadır. Sözleşme'nin en dikkat çeken fonksiyonu ise siber suçlarla mücadele özelinde kurmaya çalıştığı uluslararası adli işbirliği rejimidir[272]. Zira her ne kadar ulusal mevzuatlar yeterli ve uyumlu hale getirilse de, global siber suç sorunuyla etkin ve işbirliği içinde mücadele edilebilmesi için adli işbirliğinin somut bir düzenleme ve mekanizma çerçevesinde yürütülmesi gerekir.

Uluslararası adli işbirliği, temel olarak Sözleşme'de yer alan adli yardımlaşma hükümleri aracılığıyla sağlanmakla birlikte; öngörülen adli yardımlaşma hükümleri maddi hukuka ve usul hukukuna ilişkin önlemlerden bağımsız değildir. Zira bu

---

[271] Bu yöndeki çok sayıdaki görüş arasından bkz: Dülger, **Bilişim Suçları**, s. 193; Serdar Havuz, , "Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği", Yüksek Lisans Tezi, Harp Akademileri Stratejik Araştırmalar Enstitüsü Müdürlüğü, 2007, s. 192; Serap Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", **İÜHFM**, sy. 59, 2001, s. 155; Sınar, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 785; Micheal Vatis, "The Council of Europe 's Convention on Cybercrime", **Berkeley Technology Law Journal**, sy. 18, 2014, s. 212; Gercke, "Understanding Cybercrime" s. 200; Amalie Weber, "The Council of Europe Convention on Cybercrime", **Berkeley Technology Law Journal,** , sy. 18, 2014, s. 441; Keyser, "The Council of Europe Convention on Cybercrime"s. 325.

[272] Calderoni, "The European legal framework on cybercrime", s. 346.

önlemler, ulusal mevzuatları siber suçlarla mücadelede yeterli bir seviyeye çekmeyi ve birbirleriyle uyumlulaştırmayı, bu sayede de etkin bir uluslararası adli işbirliği sistemine uygun alt yapıyı sağlamayı amaçlamaktadır. Bu nedenle Sözleşme'nin adli işbirliği konusunda önerdiği sistemin incelenmesinden önce, bu bölümde genel olarak Sözleşme'nin yapısını, ulusal düzeyde alınmasını öngördüğü maddi ceza hukukuna ve usul hukukuna ilişkin önlemleri inceleyeceğiz.

A. Avrupa Konseyi Bünyesinde Siber Suçlarla Mücadele ve Sözleşmenin Hazırlanış Süreci

Avrupa Konseyi bünyesinde siber suçlar konusu ilk olarak 1976 yılında düzenlenen "Ekononomik Suçların Kriminolojik Yönü" başlıklı konferansta ele alınmıştır[273]. Bu yıllardaki girişimler daha ziyade sorunu anlamaya ve isimlendirmeye yönelik araştırma ve tartışma faaliyetleridir. 1980'li yıllardan itibaren ise siber suçlarla ilgili düzenleme yapma gerekliliği hissedilmiş ve bu konuda harekete geçilmiştir[274]. CDPC bünyesinde 1985 yılında kurulan bir uzmanlar komitesi bu yıldan itibaren siber suçların hukuki yönünü tartışmak üzere düzenli olarak toplanmış ve bu toplantıların sonucunda bilgisayar bağlantılı bazı eylemlerin suç haline getirilmesini öneren 1989 tarihli R (89) 9 nolu Tavsiye Karar kabul edilmiştir. Bu Tavsiye Karar'da OECD'nin 1986 tarihli bilişim suçlarıyla ilgili raporu referans alınarak burada belirlenen ihlallerin üye ülkelerde suç tipi olarak kabul edilmesi önerilmiş ve ayrıca ceza hukukuna ve bilişim suçlarına ilişkin bazı ilkelere ve OECD'nin raporunda bulunmayan bazı ihlal türlerine de yer verilmiştir[275].

1995 yılında R (95) 13 nolu tavsiye karar kabul edilmiş, Tavsiye Kararı'nda siber suçların soruşturmasına ilişkin arama-el koyma, teknik takip, soruşturma makamlarıyla işbirliği mecburiyeti, elektronik delil, kripto kullanımı, inceleme, eğitim ve uluslararası işbirliği konuları ele alınmıştır.

Bilişim suçlarının arz ettiği tehlikenin ciddiyeti ve global niteliğinin daha net anlaşıldığı 1990'lı yılların sonlarına doğru tavsiye kararlarının yerine sözleşme gibi yükümlülük getiren bağlayıcı bir hukuki araca başvurulması fikri gündeme

---

[273] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s 136.
[274] Dülger, **Bilişim Suçları**, s. 192.
[275] Dülger, **Bilişim Suçları**, s. 192.

gelmiştir[276].R (89) 9 nolu Tavsiye Karar'a Ek Rapor ve R (95) 13 nolu Tavsiye Kararı'nda ifade edilen bu fikir, CDPC'nin önerisi üzerine Avrupa Konseyi Bakanlar Kurulu tarafından somutlaştırılmış ve 1997 yılında "Siber Alemde İşlenen Suçlar Uzmanları Komitesi (Commitee of Experts on Crime in Cyberspace)" (PC-CY) kurulmuştur. PC-CY Komitesinin görevi; özellikle internet gibi telekomünikasyon ağlarının kullanımı yoluyla işlenen suçları, siber alem öznelerinin sorumlulukları konusunda gerekli ceza hukuku konuları, siber alemde geleneksel ceza muhakemesi tedbirlerinin uygulanabilirliği, siber suçlara özgü yargı yetkisi sorunlarının çözülmesi ve siber suçlarla mücadelede uluslararası işbirliği konularında araştırma ve incelemeler yapmak ve bu doğrultuda bir uluslararası sözleşme taslağı hazırlamak olarak belirlenmiştir[277].

4 Şubat 1997'de çalışmalarına başlayan PC-CY Komitesi, 2000 yılı sonunda çalışmalarını tamamlamıştır. 19 Eylül 2001'de Bakan Vekilleri Komitesi tarafından onaylanan sözleşme metni, 8 Kasım 2001'de Dış İşleri Bakanlarından oluşan Bakanlar Kurulu tarafından resmen kabul edilmiştir. Sözleşme, 23 Kasım 2001'de Macaristan'ın başkenti Budapeşte'de imzaya açılmıştır. Bu nedenle öğretide sıklıkla Budapeşte Sözleşmesi ismiyle de anılmaktadır. Sözleşme, imzaya açılmasından itibaren bir yıl içerisinde yirmi dokuz Konsey üyesi ve hazırlık aşamasına katkıda bulunan dört gözlemci devlet (ABD, Kanada, Japonya ve Güney Afrika Cumhuriyeti) tarafından imzalanmış olmakla birlikte, sözleşmenin yürürlüğe girmesi için, en az üçü konsey üyesi olmak üzere beş imzacı devlet tarafından ulusal prosedürleri uyarınca yürürlüğe konması beklenmiştir[278]. Sözleşme 1 Temmuz 2004'te yürürlüğe girmiştir. Temmuz 2015 itibariyle 53 devlet sözleşmeyi imzalamış, bunlardan 45'i sözleşmeyi yürürlüğe sokmuştur[279].

Türkiye, 10 Kasım 2010 tarihinde imzaladığı sözleşmeyi nihayet 22 Nisan 2014 tarihinde TBMM'de uygun bularak kabul etmiştir. 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun'un 28988 nolu Resmi Gazete'de yayımlanması üzerine, Sözleşme Türkiye bakımından

---

[276] Schjolber, "Harmonizing National Legal Approaches on Cybercrime", s. 9.

[277] Avrupa Siber Suçlar Sözleşmesi Açıklayıcı Rapor, (erişim: 17.07.2015), http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[278] Sözleşme m. 36; Ayrıca bkz: Shannon Hopkins, "Cybercrime Convention: A Positive Beginning" to a Long Road Ahead", **Journal of High Technology Law**, sy. 2, 2003, s. 107.

[279] Sözleşmeye taraf olan devletlerin tam listesi ve imza, uygun bulma ve yürürlüğe koyma durumları hakkında güncel bilgiler için bkz. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=20/02/2015&CL=ENG.

02.05.2014 tarihinde yürürlüğe girmiştir. Sözleşmenin Türkçe'ye resmi tercümesi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde yapılmış ve Sözleşme bu ad altında uygun bulunmuş olmakla birlikte, biz yukarıda Giriş kısmında da belirttiğimiz üzere "cybercrime" kavramın doğru çevirisinin "siber suç" şeklinde olması gerektiğini ve "siber suç" kavramının "sanal ortamda işlenen suçlar" kavramına göre daha geniş kapsamlı üst bir kavram olduğunu düşünüyor, dolayısıyla doktrinde de yer etmiş olduğu şekilde "Avrupa Siber Suçlar Sözleşmesi" ifadesini tercih ediyoruz. Nitekim Avrupa Konseyi tarafından da Sözleşme'nin adının "Avrupa Siber Suçlar Sözleşmesi" şeklindeki çevirisi benimsendiğini görüyoruz[280].

Sözleşme'nin verimli ve etkin bir şekilde uygulanmasını sağlamak amacıyla 2006 yılında Siber Suçlar Sözleşmesi Komitesi (Cybercrime Convention Committee) T-CY kurulmuştur. T-CY Komitesinin amacı, Sözleşme'nin "Taraflar Arasında İstişareler" başlıklı 46. maddesinde belirtilen istişare mekanizmasını sağlamaktır. Komite'de taraf devletlerin temsilcilerinin yanı sıra Avrupa Birliği, Afrika Birliği, Avrupa Birliği Bilgi ve Ağ Güvenliği Ajansı ENISA, EUROPOL, INTERPOL, Uluslararası Telekomünikasyon Birliği, OECD, Amerikan Devletleri Örgütü, Avrupa Güvenlik ve İş Birliği Örgütü OSCE ve Birleşmiş Milletler Uyuşturucu ve Suç Ofisi UNODC'un temsilcileri de gözlemci sıfatıyla yer almaktadır. Komitenin temel misyonu sözleşmenin yorumlanmasına ve uygulamasına ilişkin mevcut ve olası sorunların çözülmesidir. Bunun dışında görev alanları arasında; taraf devletlerin Sözleşme'ye ilişkin imza, uygun bulma, yürürlüğe sokma, çekince koyma, beyanda bulunma vb. faaliyetlerinin diğer taraf devletlere duyurulması, siber suçlara ve elektronik ortamda delil toplanmasına ilişkin hukuki, siyasi ve teknolojik gelişmeler konularında bilgi paylaşımında bulunulması, taraf devletlerin yükümlülüklerini yerine getirip getirmediklerinin ve performanslarının denetlenmesi, kapasite inşası programların teşvik edilmesi, spesifik sorunlar için alt çalışma grupları kurulması, başka ulus üstü organizasyonlarla iletişimin sağlanması, gerektiği taktirde Sözleşme'nin başka belgelerle desteklenmesi veya değiştirilmesi sayılabilir[281]. T-CY

---

[280] Sözleşmenin Avrupa Konseyi'nin resmi internet sitesinde yer alan Türkçe çevirisi için bkz. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS%20185%20turkish.pdf. Ayrıca sözleşmenin Türkçe'ye bir diğer çevirisi "Avrupa Konseyi Siber Suçlulk Sözleşmesi" şeklinde yapılmıştır. Sözleşmenin bu şekildeki özgün çevirisi için bkz. Emine Eylem Aksoy,. "Siber Suçluluğa Dair Sözleşme",**Prof. Dr. Kemal Oğuzman'a Armağan**, 2002, 869-896.

[281] T-CY Usül Kuralları, T-CY (2013) 25 rev, (erişim: 17.07.2015), http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)25%20rules_v14.pdf.

Komitesi Avrupa Konseyi'nin Strasbourg'daki yerleşkesinde düzenli olarak toplanmakta, hem anlık bilgi paylaşımı için istişare zemini sunmakta hem de bu istişarelerde varılan sonuçları raporlamaktadır. Komite, toplantı tutanaklarının yanı sıra; spesifik raporlar, rehber kitapçıklar ve periyodik ülke değerlendirme raporları hazırlayarak yayınlamaktadır.

Sözleşme'nin uygulanması noktasında bir diğer önemli kurum Romanya Hükümeti'nin teklifi üzerine 2013 yılında Bükreş'te kurulan ve Nisan 2014'te faaliyete başlayan Avrupa Konseyi Siber Suç Program Ofisi (The Cybercrime Programme Office of Council of Europa) C-PROC'dur. C-PROC, siber suçlar ve elektronik ortamda delil toplaması konularında ortaya çıkan sorunlar karşısında devletlerin ceza adaleti kapasitelerinin Sözleşme standartları çerçevesinde güçlendirilmesini amaçlamaktadır. C-PROC, kapasite inşası işleviyle T-CY Komitesi'nin Sözleşme'nin uygulanması yönündeki çalışmalarını tamamlamaktadır[282]. C-PROC hedeflerini çoğunlukla sivil kapasite inşası projelerini destekleyerek gerçekleştirmektedir. "Action Against Economic Crime", "Octopus" ve "GLACY Global Action on Cybercrime" projeleri bunlara örnek olarak gösterilebilir[283].

B. Sözleşmenin Amaçları ve İlkeleri

Sözleşme'nin Giriş kısmında sözleşmenin amacı şu şekilde ifade edilmektedir: *"Bu sözleşme bilişim sistemlerinin ağlarının ve verilerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine yönelen zarar verici eylemleri önlemenin yanı sıra, bu sistem, ağ ve verilerin kötüye kullanılmasını da önlemek üzere, sözleşmede belirtildiği üzere, bu eylemlerin suç olarak tanımlanmasını sağlamak ve bu suçlara karşı etkin bir şekilde mücadele edebilmek için gerekli yetkileri benimsemek suretiyle, bu eylemlerin gerek ulusal gerekse ulus üstü düzlemde ortaya çıkartılması, soruşturulması ve kovuşturulmasını kolaylaştırmak ve hızlı ve güvenilir bir uluslararası işbirliğinin gerçekleştirilmesi amacıyla düzenlemeler öngörmektedir."*

---

[282] "About C-PROC", (erişim: 17.07.2015), http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/C-PROC/cPROC_about_ENG_v3.pdf.

[283] Adı geçen projeler hakkında ayrıntılı bilgi için bkz. http://www.coe.int/en/web/cybercrime/capacity-building-programmes.

Sözleşme'yle birlikte Bakanlar Kurulu tarafından kabul edilen ve resmiyet kazanan Avrupa Siber Suçlar Sözleşmesi Açıklayıcı Raporu, sözleşmenin analizi ve yorumlanması açısından en önemli kaynaktır. Rapor, tarafların Sözleşme'yi kaleme alma sürecindeki hedef ve amaçlarını anlama ve sözleşme hükümlerinin arkasındaki gerçek iradeyi inceleme şansı sunmaktadır[284]. Bağlayıcılığı olan yasama yorumu niteliğinde olmasa da, Sözleşme hükümlerinin yorumlanmasında referans alınması gereken birincil kaynak Açıklayıcı Rapordur[285].

Açıklayıcı Rapor doğrultusunda Sözleşme'nin başlıca üç amacı olduğu söylenebilir[286]: 1) Bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını mümkün kılmak; 2) Siber suçların soruşturulması açısından, siber aleme uygun düşen ortak usul kurallarını tanımlayarak, devletler arasındaki muhakeme kurallarının yeknesaklaştırılmasını mümkün kılmak; 3) Hem geleneksel hem de yeni türden uluslararası işbirliği yöntemlerini belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını mümkün kılmak.

Bu itibarla Sözleşme'nin amaçlarının son derece isabetli olarak belirlenmiş olduğunu belirtmek gerekir. Sözleşme'nin sayılan amaçlara ne ölçüde hizmet edebildiği, sözleşmenin maddi, usuli ve adli yardımlaşmaya ilişkin hükümleri ayrıntılı bir şekilde ele alınarak ve uygulamadaki başarısı değerlendirilerek anlaşılabilir; aşağıda Sözleşme'nin içeriğini ayrıntılı olarak inceleyeceğiz.

Modern suç politikasının ana ilkeleriyle paralel bir Avrupa siber suç politikasının ana ilkelerinin ortaya koyma amacında olan Sözleşme'nin benimsemiş olduğu temel ilkeler ise şu şekilde sıralanabilir[287]:

1) Siber suçlarla mücadele sürekli ve güncellenen bir ortak mücadele politikası gerektirmektedir[288].

2) Siber suçlara karşı etkin bir mücadele ancak artırılmış, hızlı ve iyi işleyen bir uluslararası işbirliği sayesinde mümkün olabilir[289].

3) Devletlerle özel sektör arasında işbirliği sağlanması ve bilişim teknolojilerinin kullanımı ve geliştirilmesine ilişkin meşru çıkarların korunması gereklidir[290].

---

[284] Miquelon, "The Convention on Cybercrime", s. 330.
[285] Açıklayıcı Rapor, par. II.
[286] Açıklayıcı Rapor, par. 16.
[287] Dülger, **Bilişim Suçları**, s. 193.
[288] Açıklayıcı Rapor, par. 6.
[289] Açıklayıcı Rapor, par. 16.

4) Siber suçlarla ilgili ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce ve ifade özgürlüğü olmak üzere tüm temel hak ve özgürlükler korunmalıdır[291].

5) Suç olarak tanımlanacak fiillerin hukuka uygun meşru fillerden ayırt edilebilmesini ve hukuk güvenliğini sağlayabilmek adına siber suçlar mutlaka kasten işlenebilen ve hukuka aykırı fiiller olmalıdır[292].

6) Siber alemde yürütülen soruşturmalarda kişisel verilerin korunmasına azami özen gösterilmelidir[293].

Bu ilkelere, be şekilde formüle edilmeseler de, Sözleşme'nin Giriş kısmında da yer verilmiştir.

C. Sözleşmenin Yapısı ve İçeriği

1. Genel Olarak

Avrupa Siber Suç Sözleşmesi, dört bölüm ve kırk sekiz maddeden oluşmaktadır, bunlar sırasıyla (I) Terimler; (II) Ulusal düzeyde alınacak önlemler - maddi hukuk ve usul hukuku; (III) Uluslararası işbirliği ve (IV) Diğer hükümlerdir.

Sözleşme'nin 1. maddesinden ibaret olan "Terimler" başlıklı Birinci Bölümde, Sözleşme'de kullanılan dört ana terime ilişkin tanımlar yer almaktadır. Bunlar; bilişim sistemi, bilişim verisi, hizmet sağlayıcı ve trafik verisi terimleridir[294]. Uygulama ve öğretide yeknesak tanımları bulunmayan bu kavramların Sözleşme

---

[290] Açıklayıcı Rapor, par. 5.

[291] Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında " Avrupa Siber Suç Politikasının Ana İlkeleri", **İÜHFM**, sy. 59, 2001, s. 6.

[292] İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", s. 8; Açıklayıcı Rapor, par. 38, 39.

[293] Açıklayıcı Rapor, par. 5.

[294] Sözleşme'nin 1. maddesinde bu terimlerin tanımları şu şekilde yapılmıştır: *"Bilişim sistemi terimi; bir veya birden fazlası bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder. Bilişim verisi terimi; bilişim sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların bilginin veya kavramların bir bilişim sisteminde işlemeye uygun haldeki her türlü temsilini ifade eder. Hizmet sağlayıcı terimi; hizmetini sağlayanlara bir bilişim sistemi aracılığıyla iletişim kuram olanağı sağlayan her türlü kamu veya özel sektör kişisini ve böylesi iletişim ve hizmetlerin kullanıcıları adına bilişim verilerini işleyen veya depolayan diğer her türlü tüzel kişiyi ifade eder. Trafik verisi; bir bilişim sistemi aracılığıyla gerçekleşen iletişimle ilgili olan, iletişim zincirinin bir halkası olan bir bilişim sistemi tarafından üretilmiş, iletişimin başlangıç noktasını, hedefe varış noktasını, izlediği yolu, saatini, tarihini, boyutunu, süresini, iletişim kullanılan hizmetin temel türünü gösteren her türlü bilişim verisini ifade eder."*

kapsamında nasıl anlaşılması gerektiğini göstermesi bakımından yer verilen bu tanımlar, taraf devletler bakından ulusal mevzuata aktarma yükümlülüğü içermeyip yol gösterici niteliktedir[295].

"Ulusal Düzeyde Alınacak Önlemler" başlıklı İkinci Bölümde; öncelikle maddi ceza hukuku bağlamında birtakım suç tiplerine (m. 2-12), ardından da ceza muhakemesi hukuku bağlamında birtakım usuli tedbirlere ve yargı yetkisi meselesine dair bazı genel ilkelere (m. 13-22) yer verilmektedir. Sözleşme'nin bu bölümünde yer verilen suç tipleri ve muhakeme tedbirlerini bire bir kopyalayarak ulusal mevzuata uyarlama zorunluluğu bulunmamaktadır[296].

Sözleşme, ulusal düzeyde alınacak önlemler noktasında minimum bir standart belirlemekte, taraf devletlerin bu standardı sağlamak koşuluyla bu suç tiplerini ve usuli yetkileri farklı bir formülasyonla düzenlemelerine veya başkaca siber eylemleri suç haline getirmelerine ve gerekli görülen farklı muhakeme tedbirlerini benimsemelerine imkan tanımaktadır[297]. Sözleşmenin öngördüğü suç tiplerinin ve usuli yetkilerin yapısal unsurlarını kesin bir şekilde belirleyip taraf devletlere empoze etmemesinde, gelecekte ortaya çıkabilecek yeni suç işleme şekillerini de kapsayabilecek bir üslup benimseme kaygısı da rol oynamaktadır[298]. Taraf devletlerin öngörülen maddi ve usuli önlemeleri ulusal mevzuatlarına ne şekilde uyarlayacakları konusunda Açıklayıcı Rapor bazı yol gösterici ilkeler içerse de, bu ilkeler son derece soyut ve yetersiz kalmaktadır. Sözleşme'nin ulusal düzeyde alınacak önlemler konusundaki bu esnek tutumu ve ilgili önlemleri yeterince detaylı olarak düzenlememesi ulusal mevzuatların yeterli ve uyumlu olası amacı bakımından önemli bir eksiklik olarak değerlendirilmektedir[299].

Çalışmamızın konusunu oluşturan "Uluslararası İşbirliği" başlıklı Üçüncü Bölümde (m. 23-35), adli işbirliğinin yukarıda anılan usuli yetkilerin kullanımı bakımından adli yardımlaşmanın çerçevesi çizilmektedir. Sözleşme, adli işbirliğine dair mevcut diğer antlaşmaların yerini almayı değil; onları tamamlamayı amaçlamaktadır. Adli işbirliğine ilişkin diğer antlaşmalarla kurulu mevcut işbirliği rejimi kapsamında uygulanmayı hedefleyen Sözleşme, bunun yanı sıra ilgili devletler

---

[295] Açıklayıcı Rapor, par. 22.
[296] Açıklayıcı Rapor, par. 34.
[297] Açıklayıcı raporda, tarafların hazırlık sürecinde üzerinde anlaşamadığı "alan adı istismarı"(cybersquatting) gibi Sözleşmede yer almayan bazı fiillerin suç haline getirilmesi tavsiye edilmektedir. Açıklayıcı Rapor, par. 42.
[298] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi, s. 1244; Açıklayıcı Rapor, par. 36.
[299] Hopkins, "Cybercrime Convention: A Positive Beginning", s.110.

arasında bir antlaşma hükmünün bulunmaması durumunda uygulanacak ilke ve kuralları da belirlemektedir. Böylelikle, taraf devletler bakımından uluslararası adli işbirliğine yönelik tüm çok taraflı ve ikili antlaşmalar geçerliliği sürdürmekte ve uygulanmakta, Sözleşme ise ikincil nitelikte ya da diğer bir deyişle yedek bir adli yardımlaşa rejimi sunmaktadır. İkinci Bölümün İkinci Kısmında ulusal düzeyde alınması gereken usuli önlemlerin adli yardımlaşma hukukundaki yansımaları olan bazı özel düzenlemeler getirilmiştir. Taraf devletler, İkinci Bölümde yer alan usuli yetkilere mevzuatlarında yer vermenin yanı sıra, Üçüncü Bölüm uyarınca sınır aşan siber suçların yabancı devletlerce soruşturulmasında da bu yetkileri onların istifadesine sunmuş olacaktır[300].

"Son Hükümler" başlıklı Dördüncü Bölümde ise (m. 36-48), imza ve yürürlüğe giriş, sözleşmeye taraf olma, yer bakımından uygulama sınırlaması, sözleşmenin etkileri, beyanlar, federal devletlerin durumu, çekince rejimi, değişiklikler, uyuşmazlıkların çözümü, taraflar arasındaki istişareler, sözleşmeden ayrılma ve bildirimler gibi Sözleşme'nin uygulanmasına dair bir takım usuli ve teknik hükümler yer almaktadır.

Aşağıda Sözleşme'nin maddi ceza hukukuna ve usul hukukuna ilişkin olarak ulusal düzeyde alınmasını öngördüğü hükümleri inceleyecek ve özet olarak Türk mevzuatının Sözleşme karşısındaki durumunu belirleyeceğiz.

2. Maddi Ceza Hukukuna İlişkin Hükümler

Önce dört farklı kategoride gruplanan dokuz suç tipi tanımlanmakta, sonra ilave yükümlülük ve yaptırımlar belirtilmektedir. Sözleşmede yer alan suç kategorileri şunlardır: (1) Bilişim veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar (yasadışı erişim, yasadışı araya girme, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı), (2) Bilişim sistemleri aracılığıyla işlenen sahtecilik ve dolandırıcılık suçları (bilişim sistemleriyle bağlantılı sahtecilik ve bilişim sistemleriyle bağlantılı dolandırıcılık), (3) İçeriğe ilişkin suçlar (çocuk pornografisine ilişkin materyale sahip olmak ve

[300] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1244.

uluslararası düzeyde dağıtımını sağlamak), (4)Fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımı

a) Bilişim veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar

İlk suç tipi yasadışı erişim olup, 2. maddede düzenlenmiştir. Yasadışı erişim terimi bilişim sistem ve verilerinin güvenliğine, yani gizlilik, bütünlük, kullanıma açıklığına yönelik tehlikeli tehdit ve saldırılar şeklindeki eylemleri ifade etmektedir[301]. Bu madde uyarınca bilişim sistemlerine veya bu sistemlerin bir parça veya kısmına kasten ve hukuka aykırı olarak erişim sağlamak fiili suç haline getirilmelidir. Madde metninde öngörüldüğü şekliyle sadece izinsiz girme yani "hacking", "cracking" ya da "computer trespass" gibi eylemler ilke olarak başlı başına suç sayılabilir. Bu halde "haksız" her türlü erişim, yöntem ve saik ayrımı olmaksızın bu suçu oluşturacaktır. Ancak; taraflar suçun oluşmasını söz konusu bilişim sistemindeki güvenlik önlemlerinin ihlal edilmesi, suçun bilişim verilerinin elde edilmesi amacı ile ya da bir başka suçun işlenmesi amacı ile işlenmiş olması veya suçun uzaktaki başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişki olarak işlenmiş olması gibi şartlara bağlı da tutabilirler[302].

Yasadışı erişim suçunun Türk mevzuatındaki karşılığı Türk Ceza Kanunu'nun *"Bilişim sistemine girme"* başlıklı 243. maddesidir. TKC m. 243 hükmü *"bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak"* girme ve orada kalmaya devam etme fiilini suç olarak tanımlamaktadır. Buna göre Türk kanun koyucu yasadışı erişim eylemlerini belirli bir araç ve saik koşulu aramaksızın suç saymakla birlikte, sözleşmenin öngörmediği bir sınırlama getirmiş, bilişim sistemine girdikten sonra "kalmaya devam etme" koşulu getirerek Sözleşme'yle uyumsuz bir düzenlemeye gitmiştir[303]. Bu uyumsuzluk TCK'nın 243. maddesindeki *" giren ve*

---

[301] Açıklayıcı Rapor, par. 44.

[302] Türkiye, ulusal mevzuatında bu yönde bir hüküm olmamasına rağmen Sözleşmeyi imzalarken 2. maddeye çekince koymuş ve *"suçun oluşmasını söz konusu bilişim sistemindeki güvenlik önlemlerinin ihlal edilmesi, bilişim verilerinin elde edilmesi amacı, bir başka suçun işlenmesi amacı, suçun uzaktaki başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişki olarak işlenmiş olması"* şartlarına bağlı tutabileceğini beyan etmiştir.

[303] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Üçüncü Baskı, Ankara: Seçkin, 2011, s. 182.

kalmaya devam eden" ifadesi *"giren veya kalmaya devam eden"* şeklinde değiştirilerek giderilebilir[304].

Sözleşme'nin "Yasadışı araya girme" aşlığını taşıyan 3. maddesi uyarınca kamuya açık olmayan bilişim verilerinin, bir bilişim sisteminden bir başka bilişim sistemine veya bilişim sisteminin kendi içerisinde elektromanyetik dalgalar da dahil olmak üzere herhangi bir şekilde gerçekleşen iletimi sürecine teknik yöntemlerle araya girerek kasten ve hukuka aykırı olarak müdahil olma fiili suç olarak düzenlenmelidir. Burada kural olarak bilişim sistemlerine girilmesinden ve verilere müdahale edilmesinden bağımsız olarak, tek başına veri iletim süreçlerine dahil olunması suç haline getirilmektedir. Dolayısıyla kaynak veya hedef sisteme erişim sağlamadan, yalnızca veri iletim sürecini izleme ve iletilen veri içeriğini tespit etme şeklideki fiiller de bu suçu oluşturacaktır. Özellikle manyetik dalgaların izlenmesi ve veri iletiminin yolu kesilmeksizin ve verilere müdahale edilmeksizin veri içeriğinin tespit edilmesi mümkün olduğu için madde salt araya girme fiilinin suç olmasını önermektedir[305]. Ancak, taraflar suçun oluşmasını söz konusu bilişim sistemindeki güvenlik önlemlerinin ihlal edilmesi, bilişim verilerinin elde edilmesi amacı, bir başka suçun işlenmesi amacı, suçun uzaktaki başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişki olarak işlenmiş olması gibi şartlara bağlı da tutabilirler.

Maddede yer alan "*kamuya açık olmayan veri*" ifadesi, herkesin kullanımına açık veri paylaşım platformlarında iletilmekte olan ve radyo yayınları gibi üçüncü kişilerin erişimine açık verilerin izlenmesi fiillerini kapsam dışında tutmayı amaçlamaktadır. Aslında bu durumlarda verileri ileten kişilerin açık veya zımni rızası bulunmakta dolayısıyla hukuka uygunluk sebebi bulunması itibariyle zaten suç oluşmamaktadır. Ancak Sözleşme özellikle rızanın açık olmaması durumunda ortaya

---

[304] Türkiye'nin Avrupa Siber Suçlar Sözleşme'sini imzalayarak yüklenmiş sorumlulukları yerine getirmesi ve bu anlamda en önemli adım olarak Türk ceza mevzuatının Sözleşmesi'yle uyumlu hale getirilmesi amacıyla Adalet Bakanlığı bünyesinde bir komisyon kurularak 2014 Kasım-Aralık aylarında bazı çalışmalar yapılmıştır. Bu çalışmalarda mevzuatımızın Sözleşme'yle tam olarak uyumunu sağlayacak ölçüde değişiklik önerileri üzerinde uzlaşılamamış olmakla birlikte bazı temel noktalarda atılması gereken adımlar belirlenmiştir. Bilişim mevzuatında yapılması kararlaştırılan bu değişikliklere "Ceza Muhakemesinde İş Yükünün Azaltılması Amacıyla Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı"nda yer verilmiştir. Tasarı, 2015 Haziran itibariyle henüz Adalet Bakanlığı'ndadır. Tasarı'da TCK m. 243 hükmündeki "*ve*" ibaresinin "*veya*" olarak değiştirilmesi ve "*sisteme girmeksizin verilerin izlenmesi halinde*" de suçun oluşacağı öngörülmektedir. Tasarı'nın yasalaşması halinde yasadışı erişim suçu bakımından Türk mevzuatının sözleşmeyle tam olarak uyumlu hale geleceği söylenebilir.

[305] Açıklayıcı Rapor, par. 57.

çıkabilecek sorunları ve bu yolla meydana gelebilecek belirsizliği gidermek adına bu hukuka uygunluk sebebinin bulunmamasını suçun unsuru haline getirmiştir.

Yasadışı araya girme suçuyla veri iletişiminin gizliliği hakkının korunması amaçlanmaktadır. Bu suç adeta, kişiler arasındaki sözlü telefon görüşmelerinin geleneksel yöntemlerle dinlenmesi ve kaydedilmesi yoluyla iletişimin gizliliğinin ihlal edilmesi suçunu temsil etmektedir. Ancak burada dikkat edilmesi gereken husus yasadışı araya girme suçunun konusunu oluşturan iletişim; iki insan arasındaki haberleşme değil, iki bilişim sistemi arasında iletilen her türlü anlamlı elektronik veriyi ifade etmektedir. Söz gelimi iki kişi arasındaki cep telefonu mesajlaşmalarına ilişkin veriler iletişim olduğu gibi, bir cep telefonu cihazının program güncellemesine ilişkin olarak internet bağlantısı üzerinden aldığı, kullanıcıların talimatı dahi olmaksızın gerçekleşen, teknik fonksiyonları dışında anlam ifade etmeyen veriler de iletişimdir[306].

Türk mevzuatında yasadışı araya girme suçunu tam olarak karşılayan bir hüküm yoktur. TCK'nın 244. maddesinde, bilişim verilerine yönelik bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek şeklindeki müdahaleler suç sayılmakla birlikte bunlar bilişim verilerinin iletim sürecinde araya girerek elde edilmesini ifade etmemektedir. Kanun koyucu, bilişim verilerinin okunmasının bilişim sistemine erişilmesi koşuluna bağlı olduğu varsayımıyla hareket etmiş ve bilişim verilerinin gizliliği şeklindeki hukuki menfaatin korunması için TCK m. 243 "bilişim sistemine girme" suçunu yeterli görmüş görünmektedir[307]. Verilere erişim büyük ölçüde bilişim sistemine erişmek suretiyle gerçekleşse de yeni teknolojiler sisteme ve verilere müdahale etmeksizin verilerin okunmasını olanaklı kılarak kanun koyucunun varsayımını yanlışlamıştır[308].

Tasarı'da TCK'nın 243. maddesine "sisteme girmeksizin verilerin izlenmesi halinde de bu fıkraya göre ceza verilir" hükmü eklenerek bu maddeyle yasadışı araya girme suçunun da karşılanması amaçlanmaktadır. Madde metnine eklenen bu ifade ile verilerin izlenmesine yönelik her türlü eylem hiçbir sınırlama getirilmeksizin suç

---

[306] Açıklayıcı Rapor, par. 51.

[307] 243. maddenin oluşması için sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Ancak madde gerekçesinde suça konu bilişim istemlerinin içerisindeki verilerin vurgulandığı görülmektedir. Türk Ceza Kanunu Madde Gerekçeleri, m. 243.

[308] Açıklayıcı Rapor, par. 53.

sayılmaktadır. Böylelikle bilişim verileri ister bilişim sistemine erişilerek, ister bilişim sistemine müdahale edilmeksizin herhangi bir yöntemle hukuka aykırı olarak araya girmek suretiyle izlendiği takdirde, bu fiil 243. madde uyarınca suç teşkil edecektir. Dolayısıyla Tasarı bu haliyle kanunlaşırsa yasadışı araya girme suçu bakımından mevzuatımızın Sözleşme'yle uyumluluğu sağlanmış olacaktır.

Sözleşme'nin 4. maddesinde verilere müdahale suçu düzenlenmektedir.Bu madde uyarınca taraf devletler bilişim verilerinin tahrip edilmesi, silinmesi, bozulması, değiştirilmesi ya da erişilemez kılınması eylemlerini suç haline getirmelidir. Bu maddenin amacı bilişim verilerini de, fiziksel nesneler gibi, kasıtlı hasar verme girişimlerine karşı koruma altına almaktır[309].

Burada koruma altına alınan hukuki menfaat, depolanmış verilerin bütünlüğü, uygun biçimde çalışmaları ve kullanımıdır[310]. Kural olarak bu suçun oluşması için müdahale edilen verilerin nicelik veya nitelik olarak belirli bir değere sahip olması şartı yoktur; ekonomik ve manevi değerinden bağımsız olarak herhangi bir bilişim verisine yönelik müdahale bu suçu oluşturmaya elverişlidir. Ancak maddenin ikinci fıkrasında taraf devletlere suçun oluşmasını ciddi bir zararın meydana gelmesi şartına bağlama seçeneği sunulmuştur. "Ciddi zarar" kavramından ne anlaşılması gerektiği ise tamamıyla ulusal mevzuatlara bırakılmıştır[311].

Verilere müdahale suçunun Türk mevzuatındaki karşılığı TCK m. 244/2 hükmüdür. Bu hüküm uyarınca "*bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır*." TCK m. 244/2 hükmü Sözleşme'nin 4. maddesinde öngörülen tüm hareketleri seçimlik hareketler olarak saymakta ve verilere müdahale suçunu bire bir karşılamaktadır. TCK m. 244/2 hükmü, herhangi bir zarar verme koşulu aramaksızın başlı başına verileri müdahale edilmesi fiilini suç haline getirmekle birlikte, TCK m. 244/4 hükmünde failinin çıkar sağlaması hali ayrı bir suç olarak düzenlemiştir. Adı geçen hüküm uyarınca failin verilere müdahale etmek suretiyle "*kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde*" daha ağır cezayla cezalandırılması öngörülmektedir.

---

[309] Açıklayıcı Rapor, par. 60.
[310] Açıklayıcı Rapor, par. 60.
[311] Açıklayıcı Rapor, par. 64.

Sözleşme'nin 5. maddesi sisteme müdahale suçuna ilişkindir. Bu madde, sisteme veri göndermek veya yerleştirmek veya var olan verilere müdahale etmek suretiyle bir bilişim sisteminin işleyişinin ciddi olarak engellenmesi fiillerinin suç haline getirilmesini düzenlemektedir. "Sabotaj"[312] olarak da isimlendirilen "engelleme" terimi; bir bilişim sisteminin uygun işleyişine teknik yöntemlerle müdahale eden fiilleri ifade etmektedir[313].

Bu suçla korunmak istenen hukuki menfaat bilişim sistemi kullanıcılarının bu sistemleri uygun biçimde işletme ve kullanma haklarıdır. Bilişim sistemlerinin işleyişinin engellenmesinin ne anlama geleceği konusu yoruma açıktır zira Sözleşme metni her tür işleyiş biçiminin koruma altına alınmasını sağlamak için esnek bir dille kaleme alınmıştır[314]. Engelleme fiili yöntem itibariyle sınırlandırılmamakla birlikte, suçun oluşması için engellemenin "ciddi ölçüde" olması şartı aranmıştır. Açıklayıcı rapora göre, "*verilerin belli bir sisteme, sahibinin ya da işletmecisinin sistemi kullanma ya da diğer sistemlerle iletişim kurma yeteneği üzerinde önemli ölçüde zararlı bir etkisi olan bir biçim, hacim ya da sıklıkta gönderilmesi "ciddi ölçüde" olarak*" değerlendirilmektedirler[315]. Bu tanım yol gösterici nitelikte olup, taraf devletler engellemenin "ciddi ölçüde" sayılması için hangi ölçütlerin kullanılacağına kendileri karar verecektir[316].

Sisteme müdahale suçunun Türk mevzuatındaki karşılığı TCK'nın m. 244/1 ve 244/2 hükümleridir. 244. maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engellemek veya bozmak suç olarak tanımlanmıştır. İkinci fıkrada ise yukarıda bahsettiğimiz üzere sistemin engellenmesi koşulundan bağımsız olarak sistemde yer alan verilere müdahale filleri suç olarak tanımlanmaktadır. Hiçbiri Sözleşme'nin 5. maddesinin bire bir karşılığı olmayan bu hükümlerden, TCK 244/1 hükmü yöntem ayrımı yapmaksızın bilişim sistemlerine yönelik her türlü müdahale fiilini suç haline getirerek, sisteme müdahale suçunu kapsamakta ve bundan daha geniş bir kapsam getirmektedir. Sözleşme uyarınca bilişim sistemlerinin teknik olmayan yollarla, örneğin yakarak, kırarak vb fiziki yöntemlerle zarar vermek suretiyle engellenmesi fiilleri sisteme müdahale suçunu oluşturmamaktadır. Oysa TCK 244/1 hükmü, serbest hareketli bir suç düzenleyerek bilişim sistemlerine yönelik müdahalenin

[312] R (89) 9 sayılı Tavsiye Kararı'nda bu fiillerden bilgisayar sabotajı olarak söz edilmektedir.
[313] Açıklayıcı Rapor, par. 66.
[314] Açıklayıcı Rapor, par. 65.
[315] Açıklayıcı Rapor, par. 67.
[316] Havuz, . "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 149.

yöntemi ne olursa olsun, kasıtlı ve hukuka aykırı olarak bilişim sisteminin işleyişinin engellenmesi neticesine sebebiyet verilmesi halinde suçun oluşacağını öngörmektedir. Yani Türk mevzuatı, sisteme müdahale suçu bakımından Sözleşmenin getirdiği minimum standardı sağlamakta ve sözleşmede öngörülenin ötesinde bir koruma getirmektedir. Bu itibarla bu konuda Türk mevzuatın Sözleşmeye uyumlu olduğu söylenebilir.

Cihazların kötüye kullanımını düzenleyen 6. madde, Sözleşme'nin maddi ceza hukukuna ilişkin hükümleri arasında en dikkat çekici olanıdır[317]. Bu maddede, Sözleşmenin 2 ilâ 5. maddelerinde düzenlenen suçları işlemek üzere kasıtlı olarak tasarlanmış cihazları veya bilgisayar programlarını ya da bir bilişim sisteminin tamamına veya bir kısmına erişimi mümkün kılan şifre, erişim kodu ve benzer verilerin, bahsi geçen suçları işlemek amacıyla üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi veya başka bir şekilde erişilebilir hale getirilmesi bağımsız bir suç olarak tanımlanmaktadır. Diğer bir ifadeyle, sayılan suçlara yönelik belirli hazırlık hareketleri bağımsız bir suç olarak tanımlanmaktadır.

Bir suçun işlenmesi sürecinde, suç işleme kararına varılmasından sonra, ancak suçun icrasına başlanmadan önce hazırlık hareketleri gerçekleştirilmektedir[318]. Başka bir anlatımla failin suçun kanuni tanımında yer alan unsurların veya nitelikli hallerin doğrudan doğruya gerçekleştirilmesi olarak ifade edilen icra hareketlerine başlamadan önce gerçekleştirdiği eylemlere hazırlık hareketleri denmektedir[319]. Ceza hukukunda kural olarak hazırlık hareketlerinin cezalandırılmaması tercih edilmekte, yalnızca hazırlık hareketlerini gerçekleştiren ve icra hareketlerine her ne sebeple olursa olsun başlamamış olan kişi teşebbüsten dahi sorumlu tutulmamaktadır[320]. Hazırlık hareketlerinin cezalandırılmamasının sebeplerinin başında öncelikle ceza hukukunun son çare olması ilkesi ve kişilere mümkün olduğunca geniş bir özgürlük alanı tanıma düşüncesi gelmektedir[321]. Diğer yandan hazırlık hareketleri aşamasında failin hareketleri korunan hukuki menfaat bakımından doğrudan ve ciddi bir tehlike oluşturmamaktadır. Kaldı ki bu aşamada failin suça yönelik iradesini yani suç işleme kastını tespit etmek de oldukça güçtür[322]. Bununla birlikte bazı suçlar bakımından

---

[317] Erik Wennerstrom, "A Decade of European Legal Developments", **Scandinavian Studies Journal**, sy. 47, 2004, s. 453.
[318] Koca/Üzülmez, **Ceza Hukuku Genel Hükümler**, s. 393.
[319] Artuk/Gökçen/Yenidünya, **Ceza Hukuk Genel Hükümler**, s. 570.
[320] Koca/Üzülmez, **Ceza Hukuku Genel Hükümler**, s. 393.
[321] Artuk/Gökçen/Yenidünya, **Ceza Hukuk Genel Hükümler**, s. 561.
[322] Koca/Üzülmez, **Ceza Hukuku Genel Hükümler**, s. 393.

suçun ancak hazırlık hareketlerinin cezalandırılması halinde önlenebileceği ve hazırlık hareketlerinin suç işleme kastını yeterli şekilde ortaya koyduğu düşüncesiyle hazırlık hareketleri müstakil olarak suç olarak tanımlanabilmektedir[323]. Ancak yukarıda saydığımız gerekçelerle hazırlık hareketlerinin suç sayılması, çok iyi formüle edilmesi ve istisna olarak başvurulması gereken bir uygulamadır[324].

Siber suçların ve özellikle bilişim veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçların bazı özellikleri Sözleşme'yi kaleme alanları bu suçlar bakımında hazırlık hareketlerini suç haline getirmeye itmiştir[325]. Bu sebepler kısaca şu şekilde sayılabilir: Bu suçların icra hareketleri çok kısa bir süre içerisinde gerçekleşmekte ve bu aşamada suçların önlenmesi veya tespiti mümkün olmamakta veya çok güç olmaktadır. Bu suçlar çoğunlukla bu işi meslek edinmiş "hacker" adı verilen kişiler tarafından işlenmekte ve bu kişiler suç işlemek için özel olarak tasarlanmış veya dönüştürülmüş cihazlar ya da zararlı yazılımlar kullanmaktadır. İcra hareketleri başlamadan önce müdahale edilmesi halinde çoğunlukla henüz dolaşıma girmemiş, bir bilişim sisteminde depolanmış durumda olan veriler söz konusu olduğu için fiziksel olarak yapılacak müdahalelerle suç önlenebilir ve deliller elde edilebilir. Bunlar ve benzeri gerekçelerle hazırlık hareketleri aşamasında müdahale edilmediği takdirde müdahale şansının güçleşeceği veya geri döndürülemez bir şekilde zarar meydana gelmiş olduğu için anlamsız kalacağı gerekçesiyle bilişim veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar bakımından 6. maddede sayılan hazırlık hareketlerinin gerçekleştirilmesinin suç haline getirilmesi yoluna gidilmiştir.

Siber suçların işlenmesi çoğunlukla meşru kullanım amacıyla üretilmiş cihazlardan ziyade suç işlemek için üretilmiş ya da başkalaştırılmış araçlarla

---

[323] Örneğin Türk Ceza Kanunu'nda suç işlemek için örgüt kurma, suç için anlaşma, çocuğu fuhşa teşvik etme suçları bakımından esasında hazırlık hareketi niteliğinde olan filler bağımsız suç olarak düzenlenmiştir: TCK'nın "*Suç işlemek amacıyla örgüt kurma başlıklı*" 220. maddesinde *"Kanunun suç saydığı fiilleri işlemek amacıyla örgüt kuranlar veya yönetenler, örgütün yapısı, sahip bulunduğu üye sayısı ile araç ve gereç bakımından amaç suçları işlemeye elverişli olması halinde, iki yıldan altı yıla kadar hapis cezası ile cezalandırılır"* denmekle tüm suçlar bakımından örgüt kurma şeklindeki hazırlık hareketleri müstakil olarak suç olarak tanımlanmaktadır.

TCK'nın "*Suç için anlaşma*" başlıklı 316. maddesinde "*bu kısmın dördüncü ve beşinci bölümlerinde yer alan suçlardan herhangi birini elverişli vasıtalarla işlemek üzere iki veya daha fazla kişi, maddi olgularla belirlenen bir biçimde anlaşırlarsa, suçların ağırlık derecesine göre üç yıldan on iki yıla kadar hapis cezası verilir*" demekle sayılan suçlar bakımından hazırlık hareketleri suç haline getirilmektedir.

"*Fuhuş*" başlıklı 227. maddenin birinci fıkrasının son cümlesinde ise doğrudan "b*u suçun işlenişine yönelik hazırlık hareketleri de tamamlanmış suç gibi cezalandırılır*" ifadesi yer almaktadır.

[324] Artuk/Gökçen/Yenidünya, **Ceza Hukuk Genel Hükümler**, s. 562.

[325] Açıklayıcı Rapor, par. 71.

gerçekleşmektedir[326]. Sözleşmeyi kaleme alanlar, cihazların münhasıran ya da spesifik olarak suç işlemek üzere tasarımlanmış cihazlarla sınırlı tutulması ve dolayısıyla çift kullanımlı cihazların kapsam dışı bırakılması konusunu ayrıntılı olarak tartışmışlardır. Bunun aşırı dar bir kapsam olacağı düşünülmüştür. Bu yaklaşım, hükmü pratikte uygulanamaz ya da sadece nadir durumlarda uygulanabilir hale getirerek ceza soruşturmalarında delil elde etme açısından üstesinden gelinemeyecek güçlüklere yol açabilecek bir seçenek olarak değerlendirilmiştir. Alternatif olarak, yasal olarak üretilmiş ve dağıtılmış bile olsa bütün cihazları kapsam dahiline alınması görüşü de tartışılmış ancak bu görüş de reddedilmiştir. Sözleşme, makul bir uzlaşma noktası olarak, suçun kapsamını cihazların "öncelikli olarak" suç işlemek için tasarlanmış ya da dönüştürülmüş olmasıyla sınırlı tutmuştur. Tek başına bu ifade, hem meşru kullanıma hem de suç işlemeye elverişli olan cihazları kapsam dışı bırakmaktadır[327]. Her halükarda, suçun oluşmasında esas olarak manevi unsur, yani sayılan suçları işlemeyi amaçlamak şeklindeki kastın varlığı belirleyici olacaktır.

Türk ceza hukukunda bilişim sistemlerine ve verilerine yönelik suçları işlemek amacıyla cihazların kötüye kullanımını düzenleyen bir suç tipi bulunmamaktadır. Yalnızca Fikir ve Sanat Eserleri Kanunu'nun 72. maddesinde bilgisayar programlarını lisanssız kullanımını mümkün kılan "crack dosyası" benzeri program ve cihazların bulundurulması suç olarak tanımlanmaktadır, ancak bu suç tipinin kapsamı bilgisayar programlarının fikri mülkiyet hakları çerçevesinde korunmasıyla sınırlıdır[328].

Türk hukukunda ilke olarak hazırlık hareketleri cezalandırılmamaktadır. Teşebbüsü düzenleyen TCK m. 35 hükmünde dahi kişinin "*işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlaması*" koşulu aranmaktadır. Bu itibarla mevcut mevzuatımızda müstakil bir suç tipi olmaksızın cihazların kötüye kullanımının cezalandırılması mümkün değildir[329].

---

[326] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 151.

[327] Açıklayıcı Rapor, par. 73.

[328] FSEK'in "*Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketler*" başlıklı 72. maddesi şu şekildedir: *"Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır."*

[329] Tasarı'da ise TCK'ya 245. maddeden sonra gelmek üzere "*Yasak cihaz veya programlar*" başlıklı 245/A maddesinin eklenmesi ve bu alandaki eksikliğin giderilmesi öngörülmektedir. Söz konusu madde, Sözleşme'yle bire bir uyumlu olacak şekilde kaleme alınmıştır. Tasarı'da yer aldığı

b) Bilişim Sistemleri Aracılığıyla İşlenen Sahtecilik ve Dolandırıcılık Suçları

Sözleşme'nin 7. maddesi uyarınca, sahtecilik oluşturması amacıyla bilişim verilerine tek başına anlam ifade edip edilmediğine bakılmaksızın veri ilave etme, var olan verileri değiştirme, silme veya erişilemez kılma yoluyla orijinal verilerden farklı veriler meydana getirme fiillerinin suç haline getirilmesi gerekmektedir. Hukuki işlemlerde kullanılabilen ve hukuki etkiler doğurabilen her türlü özel ya da resmi belgenin tamamı veya bir kısmının eşdeğeri olan bilişim verilerinin maddede sayılan seçimlik hareketler aracılığıyla hukuki açıdan orijinalmiş gibi değerlendirilmesi amacıyla başkalaştırılması fiilleri bu suçu oluşturmaktadır[330].

Bu madde ile hukuki ilişkiler açısından önemli olabilecek elektronik verilerin güvenliği ve güvenilirliği koruma altına alınmakta ve yazılı belgeler hakkında işlenen sahtecilik suçuna paralel bir suç tipi getirilmektedir. Geleneksel sahtecilik suçları genellikle bir belgedeki ifadelerin ya da beyanların görsel olarak okunabilirliğini şart koşmaktadır. Bunun yanı sıra hem belge kavramının hem de sahtecilik kavramının içeriği bakımından mevzuatların çok farklı yaklaşımlar sergilemesi itibariyle geleneksel belgede sahtecilik suçları elektronik verilere uygulanamayabilmektedir[331]. Örneğin Türk hukuku bakımından elektronik imza ile imzalanmamış elektronik belgeler, belgede sahtecilik suçunun konusunu oluşturamazlar. Oysa delil teşkil eden bu tür verilerin manipülasyonu, üçüncü kişilerin yanlış yönlendirilmesine neden olabilir, başkalaştırılmış bu veriler hukuki süreçlerde delil olarak kullanılabilir ve bu şekilde geleneksel sahtecilikle aynı ciddiyette sonuçlara yol açabilir. Bilişim sistemleriyle bağlantılı sahtecilik suçuyla bu boşlukların doldurulması amaçlanmaktadır[332].

şekliyle 245/a hükmünün şu şekilde olması planlanmaktadır: "*Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için münhasıran tasarlanması veya uyarlanması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.*"

[330] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 152.
[331] Açıklayıcı Rapor, par. 82.
[332] Açıklayıcı Rapor, par. 81.

7. maddede, bilişim sistemleriyle bağlantılı sahtecilik suçunu oluşturacağı öngörülen hareketler, 4. maddede düzenlenen verilere müdahale suçunu oluşturan hareketlerin aynısıdır. Bu noktada iki suç tipinin ayırt edilmesinde manevi unsur belirleyici olacaktır. Bilişim verilerinin tahrip edilmesi, silinmesi, bozulması, değiştirilmesi ya da erişilemez kılınması hareketleri sahtecilik saikiyle yapıldığında bilişim sistemleriyle bağlantılı sahtecilik suçu, başka saiklerle yapıldığında verilere müdahale suçunun oluşumuna sebebiyet verecektir[333]. Bu noktada zaten 4. madde kapsamında cezalandırılan hareketlerin sahtecilik saikiyle yapılması halinde ayrı bir suça sebebiyet vermesi ve Taraf devletlerin verilere müdahale suçunun yanı sıra, ayrıca bilişim sistemleriyle bağlantılı sahtecilik suçuna yer vermeleri zorunluluğunun gerekliliği tartışma konusu yapılabilir.

Kanaatimizce bilişim sistemleriyle bağlantılı sahtecilik fiilinin ayrı bir suç olarak tanımlanması üç noktada önem arz etmektedir: Birincisi; suçların hukuki değerlerinde maddi unsurları kadar manevi unsurları da önemlidir. Görünüşte benzer olan iki hareketin manevi unsurları itibariyle farklı suçları oluşturması ve buna bağlı olarak farklı yaptırım ve hukuki sonuçlara bağlanması ceza hukukunun amaçları bakımından daha doğrudur. İkincisi; sözleşmeye taraf devletler verilere müdahale suçunu, müdahalenin belirli bir niteliksel veya niceliksel zarara yol açması koşuluna bağlı tutabilirler. Ciddi zarar kavramının içeriği Sözleşme tarafından tanımlanmamış olmakla, verilere müdahale suçunu oluşturmayacak bir fiilin bilişim sistemleriyle bağlantılı sahtecilik suçunu oluşturması muhtemeldir. Üçüncüsü; Sözleşme'nin öngördüğü suç tipleri ulusal düzeyde gerekli önlemlerin alınması yanı sıra farklı devletlerin ulusal mevzuatlarının uyumlulaştırılarak adli yardımlaşma söz konusu olduğunda karşılıklı cezalandırılabilirlik koşulunun sağlanması ve muhatap devletlerin ceza adalet sistemi aktörlerinin benzer tutum içinde olabilmelerini amaçlamaktadır[334]. Taraf devletlerin ulusal mevzuatlarında kavramların içeriğini ve suçların unsurlarını kendi sistemleri uyarınca doldurmaları karşısında Sözleşme'nin suçları ayrıntılı olarak düzenleyip müstakil ve bağımsız suçlar olarak tanımlaması yerinde bir tutum olarak görülmelidir.

Türk mevzuatında doğrudan bilişim sistemleri aracılığıyla sahteciliği suç haline getiren bir hüküm yoktur. Bununla birlikte 5070 sayılı Elektronik İmza Kanunu'nun 5. maddesinde yer alan "*güvenli elektronik imza, elle atılan imza ile aynı hukukî*

[333] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 153.
[334] Açıklayıcı Rapor, par. 20, 35.

sonucu doğurur" şeklindeki ve 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 205. maddesinde yer alan "*usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir*" şeklindeki ifadeler gereğince elektronik imzalı belgelere ilişkin bilişim verilerinde yapılan tahrifat eylemleri TCK m. 204-212 hükümlerinde düzenlenen sahtecilik suçlarını oluşturmaya elverişlidir[335]. Ayrıca Elektronik İmza Kanunu'nun 16. maddesinde "elektronik imza oluşturma verilerinin izinsiz kullanımı suçu", 17. maddesinde ise "elektronik sertifikalarda sahtekarlık suçu" düzenlenmiştir[336]. Diğer yandan TCK m. 244/2 hükmü başka bir koşula bağlamaksızın sırf verilere müdahale edilmesini suç sayarak bilişim sistemleri aracılığıyla dolandırıcılık fiillerinin cezasız kalmasını engellemektedir. Ancak bu maddelerde bilişim sistemleriyle bağlantılı dolandırıcılığı müstakil olarak suç haline getiren bir hükmün bulunmaması itibariyle, bu maddeler Türkiye'nin sözleşmesel yükümlülüğünü yerine getirmemektedir[337].

Sözleşme'nin "Bilişim Sistemleriyle Bağlantılı Dolandırıcılık" başlıklı 8. maddesinde, dolandırıcılık yoluyla kendine veya üçüncü bir kişiye maddi menfaat sağlamak amacıyla, bilişim verilerine herhangi bir şekilde veri ekleme, var olan verileri değiştirme, silme veya erişilmez kılma veyahut da bilişim sistemine herhangi bir teknik yöntemle müdahale etme fiilleriyle bir başkasının maddi zararına yol açılmasının suç olarak düzenlenmesi öngörülmektedir.

Bilişim teknolojilerinin gelişmesi ve yaygınlaşmasıyla birlikte kredi kartı dolandırıcılıkları başta olmak üzere kişilerin malvarlıklarını hedef alan suçları işleme fırsatları artmıştır. Bilişim sistemlerinde bulunan, gerçek malvarlığı değerlerini temsil eden verilerin geleneksel mal varlığına karşı suçlarının hedefi haline geldiği görülmektedir. Bu maddenin amacı veri işleme süreçlerinde kişilerin malvarlığı değerlerini hedef alınarak yapılan manipülasyonları suç olarak tanımlamaktır[338].

---

[335] Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 582.

[336] Bu suç tipleri hakkında ayrıntılı bilgi için bkz. Dülger, **Bilişim Suçları**, s.706- 718.

[337] Türkiye, Sözleşmeyi imzalarken 7. maddeye çekince koymuş ve suçun "dolandırıcılık veya benzeri hileli davranışlar kastı" şartına bağlı olacağını beyan etmiştir. Ancak ne mevcut mevzuatta ne de Tasarı'da bu yönde bir hüküm bulunmamaktadır. Ayrıca Tasarı'da TCK'nın 244. maddesine "*ikinci ve üçüncü fıkralarda tanımlanan fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca belgede sahtecilik suçlarına ilişkin hükümler uygulanır*" şeklinde 5. bir fıkra eklenerek bu sorunun çözülmesi amaçlanmaktadır. Böylelikle sahtecilik saikiyle gerçekleştirilen bilişim sistemlerine veya bilişim verilerine müdahale eylemleri, belgede sahtecilik suçlarını oluşturacaktır.

[338] Açıklayıcı Rapor, par. 86.

TCK m. 158/1-f hükmü dolandırıcılık suçunun "bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesini suçun nitelikli hali olarak düzenlemektedir. Maddenin düzenlemesi bilişim sistemleriyle bağlantılı olarak yapılabilecek her türlü hareketi içerecek ölçüde esnek bir şekilde yapılmıştır. Bu surette Sözleşme'nin suçu oluşturacak seçimlik hareketleri tek tek sayarak ulaşmaya çalıştığı her türlü veri manipülasyonunu kapsama amacı sağlanmış olmaktadır[339]. Ayrıca TCK'nın 245. maddesinde bilişim sistemlerinin parçası olan banka veya kredi kartlarının kötüye kullanılması ayrı bir suç olarak düzenlenmektedir[340].

Türk mevzuatı bakımından TCK m. 158/1-f ve m. 245 hükümleriyle, bu konuda Sözleşme'de öngörülen standardın üzerinde bir koruma getirilmiş olduğu rahatlıkla söylenebilir.

c) İçeriğe İlişkin Suçlar

İçeriğe ilişin suçlar ortak bir değer yargısının korunmasını ifade ettiği için, farklı hukuk sistemleri bu suçlar bakımından özellikle uyum direnci göstermektedir[341]. Bu nedenle Sözleşmenin hazırlık aşamasında taraflar içerikle bağlantılı suç olarak yalnızca çocuk pornografisiyle bağlantılı suçlar üzerinde anlaşabilmiştir[342]. İnternet ve diğer bilişim sistemleri aracılığıyla yayılan ırkçı söylemlerin de bu başlık altında suç olarak düzenlenmesi tartışılmış, ancak bu şekilde bir suç tipi üzerinde uzlaşı sağlanamaması üzerine bu suç tipi sözleşmeye dahil edilmemiş, Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol hazırlanmıştır. Adı geçen protokolü aşağıda ayrıca inceleyeceğiz.

---

[339] Açıklayıcı Rapor, par. 87.

[340] Buna göre; "*Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır. Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adlî para cezası ile cezalandırılır. Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.*"

[341] **Rosenzweig**, "The Internatıonal Governance Framework For Cybersecurity", s. 418.

[342] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 156.

Çocuk pornografisiyle bağlantılı suçların düzenlendiği 9. maddede, çocuk pornografisine ilişkin materyallerin bilişim sistemleri üzerinden dağıtmak amacıyla üretilmesi, bir bilişim sistemi üzerinden sunulması veya erişilebilir hale getirilmesi, dağıtılması ya da yayılması, bir bilişim sitemi aracılığıyla temin edilmesi, bir bilişim sistemi ya da veri depolama cihazında tutulması eylemlerinin suç olarak düzenlenmesi öngörülmektedir. Madde metininde çocuk pornografisine ilişkin materyaller; reşit ya da reşit görünümünde olmayan bir kişinin katılımıyla gerçekleşen müstehcen eylemlere ilişkin görüntüleri ya da reşit olmayan bir kişinin gerçekleştirdiği cinsel içerikli eylemleri betimleyen gerçekçi yapay görüntüleri içeren her türlü pornografik malzeme olarak tanımlanmaktadır.

Madde, reşit olamayan teriminin 18 yaşın altındaki bütün kişileri ifade ettiğini belirtmiş, bununla birlikte taraf devletlere bu yaş sınırını 17 veya 16 olarak belirleme opsiyonunu tanımıştır. Yine taraflara çocuk pornografisine ilişkin materyalleri kendisi için temin etmek ve bilişim sisteminde bulundurmak hareketleri bakımından ve reşit olup da reşit görünümünde olmayan kişilere ilişkin müstehcen görüntüler ve çocukları cinsel eylemler gerçekleştirirken tasvir eden gerçekçi yapay görüntüler bakımından çekince koyma hakkı tanınmıştır. Çocuk pornografisi gibi hassas bir konuda bile bu kadar istisna tanınması içerik bağlantılı suçlar bakımından uzlaşı zemini bulmanın ne kadar zor olduğunun açık bir göstergesidir.

"Müstehcen" ifadesinden ne anlaşılması gerektiği madde metninde tanımlanmamış, bu husus ulusal mevzuatların belirleyeceği standartlara bırakılmıştır[343]. Zira müstehcenlik tabirine yüklenecek anlam kültürel değerlerle yakından ilişkilidir[344] ve muhtemelen farklı kültürel alt yapılara sahip olan taraf devletler ortak bir tanım üzerinde anlaşamamışlardır. Ancak açıklayıcı rapor bazı müstehcen eylem kalıplarını saymakta ve müstehcenlik deyiminin bunları mutlaka içermesi gerektiğini belirtmektedir[345].

---

[343] Açıklayıcı Rapor, par. 99.

[344] Dülger, **Bilişim Suçları**, s. 888.

[345] "*Cinsel anlamda müstehcen eylem, gerçek ya da simülasyon olarak en az şunları içine almaktadır: a) cinsel organ-cinsel organ, oral-cinsel organ, anal-cinsel organ veya oral-anal olmak üzere, reşit olmayan kişiler arasındaki, bir yetişkin ve bir reşit olmayan kişi arasındaki, aynı ya da farklı cinsiyetler arasındaki cinsel ilişki; b) hayvanlarla cinsel ilişki; c) mastürbasyon; d) cinsel anlamda sadistik ya da mazoşistik kötü muamele; ya da e) reşit olmayan bir kişinin cinsel organlarının ya da cinsel bölgesinin şehvet uyandırıcı biçimde teşhiri. Fiilin gerçek ya da simülasyon olması önemli değildir.*" Açıklayıcı Rapor, par. 100.

Çocuk pornografisi içerikli verilerin üretimi, dağıtımı, edinilmesi ve bulundurulması eylemlerinin Sözleşme ile ayrıntılı olarak tarif edilmesi ve bu eylemlerin sanal dahi olsa her türlü gerçekleştirilme şeklinin suç olarak düzenlenmesi Sözleşme'nin en önemli düzenlemelerinden birisidir[346]. Bu düzenlemenin yapılmasının nedeni ise, internetin içeriklerin zahmetsiz ve risksiz bir şekilde yayılması için uygun bir zemin oluşturmasına bağlı olarak çocuk pornografisine ilişkin materyallerin git gide yayılması ve her geçen gün daha çok artmasıdır[347].

Sözleşme, gitgide önemini arttıran bu konuda yukarıda açıklanan tabloyu dikkate alarak konuya ilişkin ayrıntılı bir düzenleme getirmiştir. 9. maddenin metni ve açıklayıcı metinden, git gide yaygınlaşan çocuk pornografisiyle mücadele için, öncelikle bu verilerin üretiminin ve dağıtımının önlenmesinin hedeflendiği anlaşılmaktadır[348]. Zaten üretiminden bulundurmaya kadar zincirin bütün parçalarının failleri için ceza sorumluluğu getirilmesi, çocuk pornografisi üretimini azaltmanın etkin bir yolu olarak gösterilmektedir[349]. Bu itibarla Sözleşme başta Birleşmiş Milletler Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili İhtiyari Protokol olmak üzere diğer uluslararası metinlerin benimsediği ilkelerle de uyumludur[350]. Ancak yukarıda belirttiğimiz gibi 9. maddenin çekincelere imkan tanıyarak çok geniş bir istisna alanı yaratması maddenin öngördüğü korumanın gücünü kırmaktadır.

Türk ceza mevzuatında bilişim sistemleriyle ilişki olarak işlenen çocuk pornografisi suçlarına yönelik özel bir düzenleme bulunmamaktadır. TCK'nın "*Müstehcenlik*" başlıklı 226. maddesinde hem çocuklara müstehcen materyallerin verilmesi, okunması, izletilmesi gibi fiiller hem de bu materyallerin üretimi, ülkeye sokulması, çoğaltılması, nakledilmesi, depolanması, ihraç edilmesi, bulundurulması ve başkalarının kullanımına sunulması fiilleri suç olarak düzenlenmektedir.

TCK m. 226 hükmü çok kapsamlı ve kuşatıcı bir düzenleme görüntüsü verse de hangi görüntülerin müstehcen sayılacağının net bir şekilde belirtilmemesi önemli

---

[346] Murat Volkan Dülger, "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", **İstanbul Barosu Dergisi,** sy.4, 2004, s. 1485-1486.

[347] Çocuk pornografisine ilişkin ayrıntılı bilgi ve karşılaştırmalı hukukta bu alanda yapılan düzenlemeler için bkz: Cengiz Analay/Recep Gülşen, "Bilişim Suçu Olarak Pornografi" (Erişim: 20.07.2015) http://turk.internet.com/haber/yazigoster.php3?yaziid=11007.

[348] Dülger, Bilişim Suçları, s. 196.

[349] Açıklayıcı Rapor, par. 93.

[350] Açıklayıcı Rapor, par. 92.

bir eksikliktir. Madde metninin bu konudaki muğlak tutumu, bir yandan içeriği kişiden kişiye değişen bu kavramın kötüye kullanılmasına yol açabilecek nitelikte olmasının yanı sıra[351], diğer yandan bazı cezalandırılması gereken fiillerin cezasız kalması sonucunu doğurabilecek niteliktedir. Örneğin Sözleşme uyarınca müstehcen sayılan çocukları cinsel eylemler içinde tasvir eden gerçekçi yapay görüntülerin, yani animasyon çizgi film benzeri materyallerin TCK m. 226 uyarınca cezalandırılabilirliği oldukça tartışmalıdır[352]. Bu konudaki belirsizliği gidermek amacıyla Tasarı'da TCK'nın 226. maddesinin üçüncü fıkrasına "çocukları" ibaresinden sonra gelmek üzere "temsili çocuk görüntü ve seslerini veya çocuk gibi görünen kişileri" ibaresi eklenmesi önerilmektedir.

TCK m. 226 hükmü her türlü müstehcen içeriğin basın yayın yoluyla yayılmasını suç haline getirmekle birlikte, suçun internet ve diğer bilişim sistemleri aracılığıyla işlenmesine yönelik herhangi bir düzenleme içermemektedir. Uygulamada gerek ulusal düzeyde gerek uluslararası düzeyde çocuk pornografisine karşı başta internet olmak üzere her platformda çok sert bir şekilde mücadele edilmekle birlikte, mevzuatın bilişim sistemleri özelinde sessiz kalması ciddi bir boşluk oluşturmaktadır En azından suçun bilişim sistemleri aracılığıyla işlenmesi nitelikli hal haline getirilmelidir[353]. Maalesef henüz bu konudaki eksikliği gidermeye yönelik somutlaşmış bir girişim bulunmamaktadır.

d) Fikri Mülkiyet Haklarının İhlali ve Uluslararası Düzeyde Dağıtımı

Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar Sözleşme2nin 10. maddesinde düzenlenmektedir. Bu madde, fikri mülkiyet haklarına yönelik somut bir suç tanımı getirmemekte, bu alandaki öne çıkan uluslararası metinlere atıf yaparak, bu metinlerce korunan telif haklarının ve ahlaki yükümlülükler saklı kalmak üzere diğer hakların ticari ölçekte ve bilişim sistemleri aracılığıyla ihlal edilmesinin önüne geçilebilmesi için gerekli olabilecek suç tiplerinin oluşturulmasını şart koşmaktadır. Madde'nin gönderme yaptığı uluslararası metinler şunlardır: Edebiyat

[351] Dülger, **Bilişim Suçları**, s. 889.
[352] Dülger, "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisi", s. 488; Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 159.
[353] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 159.

ve Sanat Eserlerinin Korunmasına İlişkin Bern Sözleşmesi'ni tadil eden 24 Temmuz 1971 tarihli Paris Anlaşması, Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması, Dünya Fikri Mülkiyet Örgütü WIPO Telif Hakları Anlaşması, İcracı Sanatçılar, Fonogram Yapımcıları ve Yayın Kuruluşlarının Korunması Hakkında Uluslararası Anlaşma (Roma Sözleşmesi), WIPO İcracı Sanatçılar ve Fonogramlar Anlaşması.

10. maddenin taraflara getirdiği yükümlülük oldukça esnek ve belirsizdir. Öncelikle oluşturulacak suç tipinin konusunu teşkil edecek haklar, *"ahlaki haklar hariç olmak üzere, tanınan her türlü haklar ve bağlantılı haklar"* gibi son derece belirsiz bir ifadeyle tanımlanmıştır. Sonrasında suç tipinin yapısal unsurlarına ilişkin de hiçbir öneri getirilmemiş, taraf devletlerin yükümlülüğü anılan hakların *"suç olarak tanımlanması gerekli olabilecek yasal düzenlemeler"* şeklide belirtilmiştir. Bu itibarla bu madde uyarınca tarafların anılan uluslararası metinlerdeki başta telif hakları olmak üzere ahlaki haklar hariç tüm haklar bakımından ihlal eylemlerini suç haline getirme yükümlülükleri bulunmaktadır. Sözleşme çerçevesinde suç olarak tanımlama zorunluluğu maddede açıkça belirtilen metinlerle korunan haklar bakımından geçerli olup, bunlar dışındaki fikri mülkiyet ihlallerini kapsamamaktadır. Dolayısıyla patent ya da ticari marka haklarına yönelik ihlaller bu maddenin kapsamı dışındadır[354]. Tarafların sözleşmenin kaleme alınması aşamasında bu konularda uzlaşamadıkları anlaşılmaktadır. Nitekim maddenin tamamı için taraflara çekince koyma hakkı tanınmıştır.

Türkiye, Sözleşme'de atıf yapılan tüm uluslararası metinleri imzalamış ve onaylayarak yürürlüğe koymuştur[355]. Bu metinlerde öngörülen fikri mülkiyet hakları 5846 sayılı Fikir ve Sanat Eserleri Kanunu'yla koruma altına alınmış ve FSEK'in 71. maddesinde "*bu kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek*" gerçekleştirilen belirli eylemler sayılmış ve suç olarak tanımlanmıştır[356]. FSEK'in 2. maddesi uyarınca bilişim

---

[354] Açıklayıcı Rapor, par. 109.

[355] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 167.

[356] FSEK'in "*Manevi, mali veya bağlantılı haklara tecavüz*" başlıklı 71. maddesi şu şekildedir: *Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:*

1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

yazılımları eser kabul edilmekte ve dolayısıyla kanundaki korumaların kapsamına girmektedir. Ayrıca "Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri" başlıklı 72. maddede bilişim yazılımlarına yönelik lisanssız kullanımları önlemek amacıyla geliştirilmiş koruyucu mekanizmaları bertaraf etmeye yönelik tasarlanmış program ve cihazların üretilmesi, satılması ve kişisel kullanım amacı dışında elde bulundurulması bağımsız bir suç olarak düzenlenmiştir. Bilişim programlarının eser olarak kabul edilmesi ve özellikle bu programlara yönelik telif hakkı ihlallerini önlemek amacıyla 72. maddedeki suçun düzenlenmiş olması itibariyle Türk mevzuatının, fikri mülkiyet hakkı ihlalleri ve bilişim teknolojileri arasındaki yakın ilişkiyi dikkate alan ve uluslararası standartlara uygun bir koruma getirmiş olduğu savunulmaktadır[357].

Türk mevzuatının fikri mülkiyet haklarının korunması bakımında yeterli bir koruma rejimi getirdiği ve FSEK'in 71 ve 72. maddelerinde bu alandaki suç fiillerinin kapsamlı bir şekilde tanımlanmış olduğu görüşüne katılmakla birlikte, mevzuatta fikri mülkiyet hakkı ihlallerinin bilişim sistemleri aracılığıyla işlenmesine yönelik nitelikli hal vb. herhangi bir hüküm bulunmamasını Sözleşme'yle uyumluluk açısından bir eksiklik olarak değerlendiriyoruz.

---

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir."

[357] Dülger, **Bilişim Suçları**, s. 682.

e) İlave Yükümlülükler ve Yaptırımlar

Bu bölümde, sözleşmede öngörülen suçlar bakımından teşebbüs, iştirak (m. 11), tüzel kişilerin sorumluluğu (m. 12) ve yaptırım (m. 13) konuları düzenlenmektedir. Bu maddelerle taraf devletlerin mevzuatlarında sayılan suçlar bakımından teşebbüs ve iştirakin cezalandırılabilir olması, tüzel kişilerin cezai sorumluluğunun olması ve caydırıcı yaptırımların getirilmesi öngörülmektedir.

Ülkelerin ceza hukuku mevzuatları sistematik itibariyle ciddi farklılıklar gösterebilmektedir. Kıta Avrupası hukuk sistemine dahil olan ülkelerde çoğunlukla teşebbüs, iştirak ve tüzel kişilerin sorumluluğu konuları tüm suçları kapsayan genel hükümler içinde düzenlenirken, Anglo-Sakson hukuk sistemini benimseyen ülkelerde bu konuların genel hükümlerle değil, her bir suç tipi için ayrı ayrı düzenlenmesi uygulaması yaygındır. Sözleşme, ceza hukuku mevzuatlarındaki bu sistematik farklılığını göz önünde tutarak teşebbüs, iştirak ve tüzel kişilerin ceza sorumluluğu konularını özel olarak düzenlemiştir.

Kıta Avrupası sistemine dahil olan Türk hukukunda, teşebbüs (m. 35), iştirak (m. 37-39) ve tüzel kişilerin sorumluluğu (m. 20, 60) konuları TCK'nın genel hükümler kısmında düzenlenmiş olmakla, siber suçlar da dahil, şartlarını sağlayan tüm suçlar bakımından uygulanmaktadır. Bu itibarla Türk hukuku sözleşmenin ilave yükümlülükler bahsinde öngörmüş olduğu koşulları tam olarak sağlamaktadır.

3. Usul Hukukuna İlişkin Hükümler

Bu kısımda önce "Genel Hükümler" başlığı altında usul hukukuna ilişkin genel ilke ve esaslar belirtilmekte, sonrasında "Depolanmış Verilerin Süratli Şekilde Korunması", "Üretim Emri", "Depolanmış Veriler Hakkında Arama ve El Koyma", "Bilişim Verilerinin Gerçek Zamanlı Toplanması" ve "Yargılama Yetkisi" başlıkları altında ulusal mevzuatlarda yer verilmesi gereken usuli yetkiler ayrıntılı bir şekilde düzenlenmektedir.

a) Genel Hükümler

Sözleşmenin 14. ve 15. maddeleri, usul hukukuna ilişkin olarak öngörülen yetki ve tedbirlerin kapsamını ve koşullarını düzenlemektedir. Usul hükümlerinin kapsamına ilişkin 14. madde, kapsama ilişkin olarak önce; "*taraflardan her biri, somut bir soruşturma veya kovuşturmada başvurulmak üzere bu kısımda ele alınan yetki ve usulleri belirlemek için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri alır*" şeklinde ilkesel bir hüküm getirmekte, sonrasında usul hükümlerinin kapsamını daha somut olarak belirlemektedir.

Sözleşme'de düzenlenen usule ilişkin yetki ve tedbirler; *"a. Sözleşmenin 2-11. maddelerinde düzenlenen suç tipleri, b. Bir bilişim sistemi aracılığıyla işlenen diğer suçlar, c. Herhangi bir suçun elektronik ortamda bulunan delilleri"* hakkında uygulanacaktır.

Sözleşmeyi kaleme alanlar, Sözleşme'nin olabildiğince esnek ve yeni suçluluk tiplerine karşı doğabilecek ihtiyaçlara da cevap verebilecek nitelikte olmasını ilke edinmiş[358] ve siber alemin öngörülemeyen ve kuşatılamayan yapısı karşısında Sözleşme'yi kendisiyle dahi sınırlamamayı tercih etmişlerdir[359]. Bunun bir yansıması olarak usul hükümleri sözleşmenin düzenlediği suç tipleriyle sınırlı tutulmamış, usule ilişkin yetki ve tedbirlerin tüm bilişim suçları, hatta delilleri elektronik ortamda bulunan tüm suçlar için uygulanması benimsenmiştir.

Sözleşme usul hükümlerinin kapsamını oldukça geniş tutmakla birlikte, bu uygulama kapsamının iki istisnası vardır: Birincisi, taraflara, 20. maddedeki trafik verilerinin gerçek zamanlı olarak toplanması ve 21. maddedeki içerik verilerinin takibi tedbirlerinin ulusal mevzuatça belirlenecek bir dizi ciddi suçla sınırlı tutma hakkı tanınmıştır. Çoğu ülke, içerik verilerinin takip edilmesi tedbirinin özel yaşama önemli ölçüde müdahale niteliğini göz önüne alarak bu tedbiri bir dizi ciddi suçla sınırlı tutmuştur. Yine bazı ülkeler trafik verilerinin toplanmasını gizlilik ve özel yaşama müdahale açısından içerik verilerinin toplanmasıyla eşdeğer görmekte ve bu tedbirin de belirli ciddi suçlarla sınırlı tutulmasını tercih etmektedir[360]. Usul hükümlerinin kapsamına yönelik ikinci istisna da 20. ve 21. maddelerde düzenlenen tedbirlere yöneliktir. Taraflara, sözleşmeyi imzaladıkları tarihte ulusal

[358] Açıklayıcı Rapor, par. 16.
[359] Weismann, "A Decade of European Legal Developments", s. 344.
[360] Açıklayıcı Rapor, par. 143.

mevzuatlarında mevcut olan sınırlamalar yüzünden, belirli bir kullanıcı grubunun menfaatine işletilen, kamuya açık iletişim ağlarını kullanmayan ve diğer bilişim sistemleriyle bağlantılı olmayan bilişim sistemlerindeki iletişime müdahale edemeyen ülkelerin, 20. ve 21. maddelerdeki tedbirleri bu iletişimler bakımından saklı tutmalarına izin verilmektedir[361].

Sözleşme, siber suçlarla etkin bir şekilde mücadele edilebilmesi adına, önerdiği usul hükümlerinin "*en geniş şekilde*" uygulanmasını öngörürken[362], temel haklar ve özgürlükler bakımından ciddi bir müdahale niteliğinde olan bu yetki ve tedbirlerin uygulaması konusunda bir takım temel ilke ve koşullar getirmektedir. Sözleşmede yer alan yetki ve tedbirlerin tesis edilmesi, gerçekleştirilmesi ve uygulaması konularının ayrıntı ve usulleri kural olarak taraf devletlerin ulusal mevzuatlarına ve ulusal organlarına bırakılmıştır[363]. Ancak Sözleşmenin 15. maddesi bu süreçlerde ulusal düzeyde dikkate alınması gereken genel koşulları sıralamaktadır:

Öncelikle, taraf devletler söz konusu usuli yetki ve tedbirler hakkında insan hak ve özgürlükleri için yeterli koruma mekanizmalarını sağlamak zorundadırlar[364]. Bu anlamada taraf devletlerin dikkate almak zorunda oldukları bazı ortak standartlar ya da minimum önlemler mevcuttur. Bunlar, taraf devletlerin başta Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi ve Birleşmiş Milletler Medeni ve Siyasi Haklar Sözleşmesi olmak üzere uluslararası insan hakları araçları çerçevesinde üstlendikleri yükümlülükleri[365] ve her bir taraf devletin iç hukuku uyarınca benimsemiş olduğu standartları ve minimum önlemleri içermektedir.

---

[361] Bu ikinci grup istisnanın içeriği şu şekilde belirlenmelidir:*""Belirli bir kullanıcı grubu" terimiyle, örneğin şirketleri tarafından bir bilişim ağı aracılığıyla kendi aralarında iletişim kurmaları sağlanan çalışanlar gibi hizmet sağlayıcıyla bağlantıları açısından sınırlı bir grup kullanıcı kastedilmektedir. "Diğer bilişim sistemleriyle bağlantılı olmayan" terimi, Madde 20 ya da 21 çerçevesinde bir talimatın çıkarıldığı tarihte, kendisine iletişimler iletilen bir sistemin başka bir bilişim ağıyla fiziksel ya da mantıksal bir bağlantısı olmaması anlamındadır. "Kamuya açık iletişim ağlarını kullanmayan" terimi, kullanımın kullanıcıların bilgisi dahilinde olup olmamasından bağımsız olarak, internet dahil kamuya açık bilişim ağlarını, kamuya açık telefon ağlarını ve diğer kamuya açık telekomünikasyon imkanlarını kullanan sistemleri hariç bırakmaktadır".*Açıklayıcı Rapor, par. 144.

[362] Sözleşmenin 14. maddesinin son paragrafı, usul hükümlerinin kapsamının istisnaları konusunda taraflara çekince hakkı tanırken dahi, tarafları usul hükümlerinin"*en geniş şekilde*" uygulanmasını gözetmeye davet etmektedir.

[363] Zira "*taraf olan ülkelerin çok farklı hukuk sistemlerine ve kültürlerine sahip olmasından dolayı, her bir yetki ve usul için geçerli olabilecek şart ve önlemleri ayrıntılarıyla açıklamak mümkün değildir*". Açıklayıcı Rapor, par. 145.

[364] Weismann, "A Decade of European Legal Developments", s. 344.

[365] Bu konuda dikkate alınması gereken uluslararası metinler arasında Avrupa Konseyi İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi'nin 1, 4, 6, 7 ve 12. ek Protokolleri (ETS N° 005 (4), 009, 046, 114, 117 ve 177), 1969 Amerika İnsan Hakları Sözleşmesi ve 1981 Afrika İnsanların ve Halkların Hakları Sözleşmesi sayılabilir.

Sözleşmede usul hükümlerine yönelik ikinci prensip; uygulanacak yetki ve önlemlerin, niteliklerine uygun olarak, uygulama, kapsam ve süre anlamında gerekli kısıtlamalar için gerekçeler içermesini ve adli ya da başka nitelikte bağımsız denetime ve gözetime tabi olmasıdır. Ayrıca ulusal mevzuatlar, bağlayıcı uluslararası yükümlülükleri ve yerleşik ulusal ilkeleri uygularken, niteliği açısından hangi yetki ve usullerin özel şart ve önlemleri uygulamayı gerektirecek kadar özel hayata müdahale edici olduğuna karar vermek zorundadır[366].

Sözleşme uyarınca taraflar, söz konusu usul hükümlerini ulusal mevzuatlarına uyarlarken ve uygularken orantılılık ilkesinin tesis etmek[367], kamu yararı özellikle de adaletin sağlıklı şekilde yürütülmesini göz önünde bulundurmak[368] ve bu hükümlerin uygulamasının üçüncü kişilerin hak, sorumluluk ve menfaatleri üzerindeki etkilerini dikkate almak zorundadırlar[369].

b) Depolanmış Verilerin Süratli Şekilde Korunması

Bilişim verilerinin "geçiciliğinden ve uçuculuğundan"[370] dolayı veriler kolaylıkla manipülasyon ve değiştirmeye maruz kalabilir. Özensiz işleme ve saklama uygulamaları, delilleri yok etmeye yönelik kasıtlı silme veya başkalaştırma eylemleri ya da artık tutulması gerekmeyen verilerin rutin olarak silinmesi sonucunda bir suçla ilgili değerli deliller kolaylıkla yok olabilir[371]. Siber alemdeki verilerin uçuculuğu ve elektronik ortamda delil elde etme süreçlerinin hızlı hareket etmeyi mecbur kılması karşısında ceza muhakemesi hukukunun fiziksel aleme göre tasarlanmış geleneksel

---

[366] Açıklayıcı Rapor, par. 147.

[367] *"Orantılılık her bir Taraf Ülke tarafından ulusal mevzuatındaki ilgili ilkeler uyarınca uygulanacaktır. Avrupa ülkeleri için bu, yetki ve usullerin suçun niteliği ve koşulları açısından orantılı olmasını öngören 1950 Avrupa Konseyi İnsan Haklarının ve Temel Özgürlüklerin Korunması Sözleşmesi, ulusal mevzuat ve hukuk sistemleri çerçevesinde belirlenecektir. Diğer ülkeler ulusal mevzuatlarındaki, muhakeme tedbirlerinin aşırı kapsamlı olması üzerine sınırlamalar ve arama ve el koymalar için makul şüphe aranması şartları gibi ilkeleri uygulayacaktır. Ayrıca, 21. maddedeki müdahale önlemleriyle ilgili zorunlulukların ulusal mevzuatın belirlediği bir dizi ciddi suçla ilişkili olması konusundaki açık sınırlama, orantılılık ilkesinin uygulanması için açık bir örnektir"*. Açıklayıcı Rapor, par. 146.

[368] *"Örneğin kamu güvenliği, kamu sağlığı ve kurbanların menfaatleri ve özel yaşama saygı da dahil olmak üzere diğer menfaatler.."*. Açıklayıcı Rapor, par. 148.

[369] Usul hükümlerinin üçüncü kişilerin hak ve sorumluluklarına etkisi noktasında özellikle servis sağlayıcılar bakımından getirilen yükümlülüklerin sınırlarının hassas bir şekilde belirlenmesi gerekmektedir.Açıklayıcı Rapor, par. 148.

[370] Geçicilik; veri depolama cihazların sınırlı kapasitede olması dolayısıylaverilerin belirli bir süre sonra silinmek üzere tutulmasını ve uçuculuk ise verilerin iradi veya gayri irade nedenlerle geri döndürülemez olarak erişilemez hale gelmesini ifade etmektedir.

[371] Açıklayıcı Rapor, par. 155.

delil elde etme yöntemleri yavaş ve hantal kalmıştır[372]. Diğer yandan, delil elde etme süreçlerinin yavaşlığının bir sebebi de başvurulan tedbirin gerekliliği, orantılılığı ve genel olarak hukuka uygunluğunun denetlenmesine ilişkin prosedürlerdir[373]. Şüpheli, yani henüz suçluluğu ispatlanmamış dolayısıyla karine olarak masum bir kişiye ait bilişim sistemlerinde uygulanacak muhakeme tedbirlerinin hem karar hem de icra süreçleri dikkatli bir şekilde sürdürülmelidir. Kaldı ki söz konusu tedbirin muhatabı şüpheli dışında mağdur vb. üçüncü kişiler de olabilir. Dolayısıyla teknik engeller aşılsa bile muhakeme tedbirlerine usulünce karar verilmesi ve uygulanması için elektronik ortamdaki delillerin bütünlüğünü tehlikeye sokabilecek uzunlukta böyle bir sürecin geçirilmesinin zorunlu olduğu söylenebilir[374]. Bu durumda yasa koyucu ve uygulamacı, elektronik ortamda delil elde etme süreçleri bakımından bir yanda suç verilerin uçuculuğu diğer yanda hak ve özgürlüklere saygı arasında ciddi bir ikilemle karşı karşıyadır.

Sözleşme'nin bu durum karşısında ürettiği çözüm; delil niteliği taşıması muhtemel verilerin, daha sonra usulünce uygulanacak tedbirleri olanaklı kılmak üzere hızlı bir şekilde korunmasıdır[375]. Soruşturma makamları depolanmış durumda olan ve suç delili olduğundan şüphelendikleri verilere herhangi bir şekilde müdahale etmeksizin, talimat vermek suretiyle, verilerin, bunları elinde bulunduran kişi tarafından korumasını sağlayacaktır[376]. Böylelikle veriler zaten bulunmakta oldukları yerde bulunmaya devam edecek ve esasında hiçbir erişim/müdahale gerçekleştirilmemiş olmakla önemli bir hak ihlali gerçekleşmemiş olacak, aynı zamanda ileride usulünce gerçekleştirilecek soruşturma işlemleri için verilerin bütünlüğü muhafaza edilmiş olacaktır[377].

Elektronik ortamda delil elde etme süreçleri bakımından yaşanan sorunlara çözüm üretmesi bakımından depolanmış verilerin süratli şekilde korunması tedbirleri

---

[372] Peter Grabosky, "Requirements of Prosecution Services to Deal With Cyber Crime", **Crime Law Soc Change**, sy. 47, 2007, s. 201.

[373] Örneğin Türk hukuku bakımından; CMK m. 134 uyarınca bilişim sistemleri hakkında arama el koyma tedbirine başvurulabilmesi için; "*bir suç dolayısıyla yapılan soruşturma*" mevcut olmalı, "*somut delillere dayanan kuvvetli şüphe sebepleri*" mevcut olmalı, "*başka surette delil elde etme imkânı bulunmamalı*" ve bu koşulların varlığı Cumhuriyet savcısının istemi üzerine karar verecek olan hâkim tarafından incelenmelidir. Bu süreçler en iyi ihtimalle birkaç saat almaktadır.

[374] Dülger, **Bilişim Suçları**, s. 778.

[375] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 161.

[376] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 169.

[377] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 162.

Sözleşme'nin en dikkate değer usul hükümleridir[378]. Depolanmış verilerin korunmasına ilişkin 16. ve 17. maddelerde düzenlenen ulusal düzeyde uygulanacak tedbirlerin, 29. ve 30. maddelerde düzenlenen uluslararası adli yardımlaşma bakımından karşılıklarının düzenlenmiş olması da siber suçlulukla mücadele adına çok ciddi bir adımdır. Bu itibarla Sözleşme'nin oluşturmaya çalıştığı siber suçla mücadele sisteminin etkin yürümesi için, pek çok hukuk sisteminin aşina olmadığı depolanmış verilerin süratli bir şekilde korunmasına yönelik tedbirler ulusal düzeyde doğru bir şekilde tesis edilmeli ve uygulanmalı, buna paralel olarak uluslararası düzeyde de bu tedbirler aracılığıyla etkin bir yardımlaşma sağlanmalıdır[379].

Sözleşme'nin 16. maddesi depolanmış verilerin süratli şekilde korunmasına ilişkindir. Bu madde uyarınca, adli makamların, yürütülen bir soruşturma veya kovuşturmada ihtiyaç duyulan verilerin korunması için verileri elinde bulunduran gerçek ya da tüzel kişilere verileri koruması talimatı verme yetkisine sahip olması öngörülmektedir. Trafik verileri ve içerik verileri dahil olmak üzere delil niteliğinde olduğu düşünülen her türlü veriyi elinde bulunduran, servis sağlayıcılar başta olmak üzere tüm gerçek veya tüzel kişiler hakkında depolanmış verileri doksan güne kadar muhafaza etme talimatı verilmesine ve talimatı alan kişinin bu süre boyunca belirtilen verileri korumaya ve bütünlüğünü sürdürmeye mecbur tutulmasına olanak sağlayacak yasama tedbirleri ve diğer tedbirler alınmalıdır.

Bu tedbir bakımından dikkat edilmesi gereken ilk husus koruma altına alınan veriler hakkında adli makamların hiçbir müdahalesinin söz konusu olmaması ve verilere dair hiçbir bilginin adli makamlara ifşa edilmemesidir. Veriler yalnızca ileride başvurulması muhtemel tedbirleri mümkün kılmak için koruma altına alınmaktadır. Burada talimat verilen kişi, verileri korumakla yükümlü kılınmaktadır. Bu yükümlülüğün yerine getirilmesinin ne surette sağlanacağı ve ihlalinin yaptırımının ne olacağı konularına yönelik bir düzenleme getirilmemekte, bu hususlar taraf devletlerin ulusal mevzuatlarına bırakılmaktadır.

Bu tedbir bakımından dikkat edilmesi gereken bir diğer husus, tedbirin konusunun yalnızca depolanmış durumda olan veriler olması, tedbirin verileri tutma zorunluluğunu içermemesidir. Yani bu tedbir somut bir soruşturma ya da

---

[378] Daniele Cangemi, "Procedural Law Provisions of the Council of Europe Convention on Cybercrime**", International Review of Law of Computer and Technology**, sy, 18/2, 2004, s. 168.

[379] Açıklayıcı Rapor, par. 155.

kovuşturmada ihtiyaç duyulabilecek "belirli ve halihazırda bir bilişim sisteminde depolanmış durumda olan" verilerin korunmasından ibarettir[380].

Sözleşme, verilerin korunması talimatının azami doksan güne kadar verileri koruma yükümlülüğü getireceğini söyleyerek, taraf devletlere talimatın azami süresini daha kısa bir süreyle sınırlı tutma şansı tanımıştır. Ancak bu süre her halükarda söz konusu veriler hakkında ileride başvurulması planlanan tedbirleri mümkün kılacak şekilde belirlenmelidir. Bunun yanı sıra tarafların azami sürenin sonunda talimatın yenilenebilmesine olanak sağlaması da mümkündür.

Korumanın ne şekilde gerçekleştirileceği sözleşme tarafından ayrıntılı olarak düzenlenmemiştir. Koruma talimatını alan kişinin yalnızca verilerin bütünlüğüne müdahale etmeme şeklinde pasif bir sorumluluk altına mı, yoksa verilerin bütünlüğünün uzaktan erişim vb. yollarla üçüncü kişiler tarafından gerçekleştirilebilecek müdahalelere karşı alınması şeklinde aktif bir sorumluluk altına mı sokulacağı, verilerin korunması talimatının verilere üçüncü kişilerin erişiminin engellenmesi şeklindeki dondurma önlemini de kapsayıp kapsamayacağı hususlarında tercih taraf devletlere bırakılmıştır[381].

16. maddenin 3. fıkrasında depolanmış verilerin korunması talimatını alan kişiler bakımından sır tutma yükümlülüğü getirilmektedir[382]. Bu yükümlülüğün amacı yürütülen soruşturma ya da kovuşturmanın gizliliğinin sağlanmasıdır.

Depolanmış verilerin süratli şekilde korunması, Sözleşme'nin en önemli ve siber suç soruşturmalarının etkili olması bakımından en öne çıkan düzenlemesi olmasına rağmen, taraf devletlerin bu tedbiri iç hukuklarına aktarırken farklı yorumlara yöneldikleri ve uygulanması noktasında gönülsüz oldukları görülmektedir[383]. Zaten Sözleşme'nin hazırlık sürecinde de depolanmış verilerin süratli şekilde korunması konusunda yoğun tartışmalar yaşanmış ve uzlaşı sağlanamaması nedeniyle bu tedbirin daha ayrıntılı ve daha net bir şekilde düzenlenmesi mümkün olamamıştır[384].

Taraf devletlerin büyük bir kısmı, ulusal mevzuat uyarınca trafik verilerinin servis sağlayıcılar tarafından tutulması şeklindeki zorunluluğun sözleşmenin 16.

---

[380] Açıklayıcı Rapor, par. 152.
[381] Açıklayıcı Rapor, par. 159.
[382] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 164.
[383] "Implementation of the preservation provisions of the Budapest Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 25 Ocak 2013, s. 10.
[384] Açıklayıcı Rapor, par. 160.

maddesinde öngörülen depolanmış verilerin süratli bir şekilde korunması tedbirini karşıladığını düşünmekte ve mevzuatlarında talimat verme şeklinde ayrı bir tedbire yer vermemektedir[385]. Sözleşme'nin öngördüğü şekilde koruma talimatı verme tedbirini benimseyen on dört ülkede de, talimat tedbirine sıklıkla başvurulan ABD hariç, bu tedbirin uygulamasının çok istisnai bir durum olduğu, bunun yerine veriler hakkında arama - el koyma tedbirine başvurulduğu görülmektedir[386].

Sözleşme'nin gerekçesinde özellikle vurgulanmış olmasına rağmen taraflar Sözleşme'yi iç hukuklarına uyarlarken ve uygularken "veri koruma" ve "veri tutma" kavramlarını birbirine karıştırmaktadırlar. Açıklayıcı rapor uyarınca; "veri koruma, hâlihazırda depolanmış durumda olan verilerin saklanmaya devam edilmesi, mevcut nitelik ya da durumunun değişmesine ya da bozulmasına neden olabilecek etkenlerden korunması anlamındadır. Veri tutma ise, hâlihazırda üretilmekte olan verilerin gelecek için yedeklenmesi ve saklanması anlamına gelir"[387]. Veri tutma, servis sağlayıcıların herhangi bir ayrım yapmaksızın idari bir tedbir olarak trafik verilerinin kaydını tutması iken; veri koruma, herhangi bir gerçek ya da tüzel kişinin elinde mevcut bulunan her türlü verinin saklanmasıdır. Veri koruma, servis sağlayıcıların veri tutma vesilesiyle ellerinde bulundurdukları trafik verilerini de kapsamakla birlikte, herhangi bir kurumun veya kişinin elinde bulunan, içerik verileri dahil her türlü bilişim verisi bakımından da söz konusu olabilir. Diğer yandan veri tutma idari bir tedbir olarak, herhangi bir suç şüphesi olmaksızın sunulan servisten faydalanan herkes hakkında uygulanmakta, usulünce başvurulan bir tedbir olmadıkça adli makamlara verilmemekte ve azami bir sürenin sonunda veri koruma ilkeleri kapsamında zorunlu olarak yok edilmektedir. Şüphesiz veri tutma kapsamında tutulmuş veriler, arama - el koyma gibi muhakeme tedbirlerinin konusunu oluşturabilirler. Ancak burada ikinci muhakeme işleminin olduğu ve bu muhakeme işleminin depolanmış verilerin korumasına göre çok daha fazla süre ve garantörsel prosedür gerektiren üretim emri veya arama el koyma tedbiri olacağı, bu tedbirlerin Sözleşme'nin 18. ve 19. maddelerinde düzenlenen ayrı tedbirler olduğu unutulmamalıdır. Yani tutulmuş verilerin başkaca muhakeme tedbirlerine konu

---

[385] Özellikle Avrupa Birliği ülkelerinde 2006 tarihli Veri Tutma Direktifi uyarınca servis sağlayıcıların trafik verilerini belirli bir süre için tutmak ve belirli ciddi suçlarla ilgili soruşturma ve kovuşturmalar çerçevesinde talep edilmesi durumunda adli makamlara teslim etmek zorundadır. Ancak bilişim sistemlerine karşı ve bu sistemler aracılığıyla işlenen suçlar bu suç listesinde yer almamaktadır. "Implementation of the preservation provisions", s. 9.

[386] "Implementation of the preservation provisions", s. 9.

[387] Açıklayıcı Rapor, par. 151.

olabilmesi, depolanmış verilerin süratli şekilde korunması tedbirini kesinlikle karşılamamaktadır.

Servis sağlayıcı tarafından düzenli olarak tutulan veriler, veri koruma tedbirinin de konusunu teşkil edebilir. Örneğin tuttuğu trafik verilerini altı ay boyunca saklama ve bu sürenin sonunda yok etme yükümlülüğü bulunan bir servis sağlayıcıya altı aylık sürenin bitmesine kısa bir süre kala koruma talimatı verilerek verilerin yok edilmesi önlenebilir. Bu itibarla, veri tutulması, veri koruma tedbirine başvurulması için elverişli zemin sunan önemli bir idari tedbir olarak değerlendirilebilir. Ancak Sözleşme'nin 16. maddesinde düzenlenen ve tarafların benimsemek ve uygulamak zorunda oldukları ceza muhakemesi tedbiri, veri tutma zorunluluğu şeklindeki idari tedbir ile karşılanmamaktadır. Nitekim usul hukukuna yönelik düzenlemeler hakkında genel düzenlemeler getiren 14. maddede açıkça bu kısımdaki tüm tedbirlerin "somut soruşturma ve kovuşturmalarda uygulanacak" ceza muhakemesi tedbirleri olduğu vurgulanmıştır[388]. Servis sağlayıcılar hakkında pek çok taraf devlette zaten uygulanmakta olan veri tutma zorunluluğu Sözleşme'nin hazırlanması sürecinde ayrıca tartışılmış, ancak idari bir önlem olması nedeniyle bu konuda herhangi bir hükme yer verilmemiştir[389].

Depolanmış verilerin süratli şekilde korunması tedbiri yerine, servis sağlayıcılar tarafından tutulan verilerinin üretim emri ya da arama - el koyma tedbirleri aracılığıyla elde edilmesi, Sözleşme metninin açık olarak getirdiği yükümlülüğü karşılamamasının yanı sıra pratik anlamda da ciddi bir eksikliğe yol açmaktadır. Bu şekildeki yorumu benimseyen devletler, delil olarak kullanılacak verilerin trafik verisi olduğu varsayımıyla hareket etmektedirler. Oysa koruması gereken veri bir veri saklama merkezinin (data center) elinde bulunan abone bilgileri veya içerik verileri, bir gerçek kişinin bilişim sisteminde bulunan içerik verileri olabilir. Örneğin; bir yer sağlayıcının zemin sunduğu pornografik materyallere ilişkin, zararlı yazılım mağduru bir kişinin bilgisayarındaki iletişimin trafiğine veya içeriğine ilişkin verilerin süratli bir şekilde korunması gerekebilir. Unutulmaması gereken bir diğer husus bu muhakeme tedbirinin yalnızca siber suçlar hakkında değil, delilleri elektronik ortamda bulunan tüm suçlar hakkında uygulanabilecek olmasıdır. Dolayısıyla bir gerçek ya da tüzel kişiye ait kamera cihazında kayıtlı bulunan bir cinayet soruşturmasına ilişkin görüntülere ait veriler ya da bir bankanın bilişim

[388] Açıklayıcı Rapor, par. 152.
[389] Açıklayıcı Rapor, par. 135.

sisteminde malvarlığına karşı suçlara, ekonomik suçlara veya vergi suçlarına ilişkin delil olabilecek veriler de bu tedbirin konusunu teşkil edebilir. Bunlar ve çoğaltılabilecek daha pek çok gerçekçi senaryoda tutulmuş trafik verilerinin üretim emri ya da arama el koyma marifetiyle elde edilmesinin bir anlam ifade etmeyeceği açıktır.

Türk hukukunda koruma talimatı verme şeklinde bir muhakeme tedbiri yoktur. Delil olabilecek depolanmış veriler, trafik verisi ise; 5651 sayılı Kanun uyarınca servis sağlayıcıların zorunlu olarak tuttukları bu veriler genel soruşturma işlemi niteliğinde bir taleple servis sağlayıcılardan edinilmekte, içerik verisi ise; CMK m. 134 uyarınca alınan karar ile arama el koyma tedbirine başvurulmaktadır[390]. Sözleşme'yle uyumluluğun sağlanması amacıyla hazırlanan Yasa Tasarısı'nda da depolanmış verilerin süratli şekilde korunmasına yönelik herhangi bir hüküm bulunmaması karşısında Türkiye'nin de bu konuda servis sağlayıcıların idari bir tedbir olarak veri tutmasını yeterli gören ülkeler grubuna dahil olduğu anlaşılmaktadır.

Kanaatimizce hem Sözleşme'ye taraf olmakla üstlenilen yükümlülüğün yerine getirilmesi hem de başta siber suçlar olmak üzere her türlü elektronik delil elde etme süreçlerinde yaşanan sorunların aşılması için Türk kanun koyucunun, Sözleşme'de öngörüldüğü gibi koruma talimatı verme şeklinde bir tedbiri benimsemesi yerinde olacaktır.

Sözleşme'nin 17. maddede ise trafik verilerinin süratli şekilde korunması ve kısmen açıklanması ele alınmaktadır. Bu maddede, 16. maddede öngörülen genel koruma tedbirinin özel bir görünümü olan trafik verilerinin korunması ayrı olarak düzenlenmekte ve iletişime dahil olan birden fazla servis sağlayıcının mevcut olması durumunda diğer servis sağlayıcıları da soruşturmaya dahil edebilmek adına bazı trafik verilerinin kısmen ve süratli bir şekilde açıklanması öngörülmektedir[391].

17. maddedeki trafik verilerinin korunmasına yönelik düzenleme, depolanmış verilerin korunmasına ilişkin 16. maddede "trafik verileri de dahil olmak üzere" ifadesi açıkça yer aldığı için ilk bakışta gereksiz bir tekrar gibi durmaktadır. Sözleşmeyi kaleme alanlar, trafik verilerinin korunmasının önemini özellikle vurgulama amacının dışında, trafik verilerinin, ilgili bütün servis sağlayıcılar

[390] Dülger, **Bilişim Suçları**, s. 731.
[391] Açıklayıcı Rapor, par. 165.

tarafından süratli bir şekilde korunması amacıyla trafik verilerinin korunmasını ayrıca düzenlemişlerdir[392]. Bunun ne surette sağlanacağı ise maddede ayrıntılı olarak belirtilmemekte, yalnızca iletişime bir veya birden fazla servis sağlayıcı dahil olduğuna bakılmaksızın trafik verilerinin korunması için gerekli yasal önlemlerin alınması" gerektiği belirtilmektedir. Bu halde hukuk sistemi ve usul ekonomisiyle tutarlı bir yol belirlemek ulusal mevzuatlara bırakılmıştır[393]. Yetkili merciler için hızlı bir biçimde korumayı sağlamanın bir yolu her bir servis sağlayıcıya ayrı bir koruma talimatı tebliğ etmektir. Ancak, ayrı ayrı bir dizi talimatın hazırlanması gereksiz zaman kaybına yol açabilir. Tercih edilen alternatif yöntem, kapsamı spesifik iletişimin iletimine katıldıkları saptanan bütün hizmet sağlayıcılar için geçerli olacak tek bir talimatı yeterli görmektir[394].

Kural olarak depolanmış verilerin süratli şekilde korunması tedbirinde veriler yalnızca korunmakta, adli makamlara ifşa edilmemektedir. Ancak 17. madde trafik verileri bakımından kısmi bir istisna getirmektedir. Yöneltilen koruma talimatı, birden fazla servis sağlayıcı aracılığıyla gerçekleşen iletişimlere ilişkin olduğunda, trafik verilerinin adli makamların iletişimin takip ettiği yolu ve kullandığı servis sağlayıcıları tespit etmesini mümkün kılacak ölçüde açıklanması öngörülmektedir. Siber alemde coğrafi mesafelerin ve sınırların sembolik anlamın ötesinde engel teşkil etmemesi karşısında pek çok iletişim farklı coğrafyalar üzerinden ve farklı yolları takip ederek gerçekleşmektedir[395]. Bu halde ileride usulünce elde edilecek trafik verilerinin etkili bir şekilde korunması için iletişimin kullandığı yolun ve ilgili servis sağlayıcıların hızlı bir şekilde tespit edilmesi hayati önem taşımaktadır. Sözleşme bu ihtiyaca binaen trafik verilerinin hızlı bir şekilde açıklanmasını mümkün kılmıştır. Bu uygulama, özellikle uluslararası adli yardımlaşma bakımından yansıması olan 30. maddedeki düzenlemeyle birlikte siber suç soruşturmalarında yaşanan pek çok sorunu bertaraf etme kabiliyetine sahiptir.

Sözleşme'ye taraf devletlerin 16. maddeye paralel olarak, 17. maddeyi de iç hukuklarına uyarlama ve uygulama konusunda farklı yorumları benimsedikleri ve gönülsüz oldukları görülmektedir[396]. Trafik verilerinin korunması ve kısmi olarak açıklanması tedbirini iç hukuklarına uyarlayan dokuz taraf devletten yalnızca bir kaçı

[392] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 166.
[393] Açıklayıcı Rapor, par. 168.
[394] Açıklayıcı Rapor, par. 168.
[395] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 166.
[396] Implementation of the preservation provisions", s. 51.

uygulamada bu tedbire başvurmaktadır[397]. Diğer taraf devletler servis sağlayıcıların rutin veri tutma zorunluluklarını yeterli görmektedir.

Biz yukarıda 16. maddeye ilişkin olarak yaptığımız açıklamalara ek olarak; özellikle birden fazla servis sağlayıcının hizmet verdiği iletişimlerde eş zamanlı olarak korumanın sağlanabilmesi ve sınır aşan iletişimler bakımından 30. maddenin uygulanabilmesi noktalarında servis sağlayıcıların veri tutmalarının yeterli olmadığı, taraf devletlerin maddede öngörüldüğü şekilde bir muhakeme tedbirini benimsemelerinin ve uygulamalarının gerekli olduğu kanaatindeyiz.

Türk hukukunda trafik verilerinin tutulması 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca servis sağlayıcılar tarafından sağlanmaktadır. 5651 sayılı Kanun'un erişim sağlayıcıların yükümlülüklerini düzenleyen 6. maddesi uyarınca erişim sağlayıcılar; "Sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla" yükümlüdür. Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik'in 15. maddesinde bu süre 1 yıl olarak belirlenmiştir. Tutulan trafik verilerinin adli makamlarca elde edilmesine ilişkin özel bir düzenleme bulunmamaktadır. Bundan dolayı mahkemeler ve savcılıklar genel soruşturma işlemleri kapsamında herhangi bir hakim ya da mahkeme kararı olmaksızın trafik verilerini ilgili kurumlardan doğrudan istemekte ve temin etmektedirler[398].

---

[397] Bu devletlerin listesi, 17. maddeyi iç hukuklarına uyarlama şekilleri ve uygulama karneleri için bkz. "Implementation of the preservation provisions", s. 52 vd.

[398] 2014 yılında, trafik verilerinin "*ancak bir suç soruşturması kapsamında mahkemelerce talep edilmesi halinde"* verilmesi yönünde 5651 sayılı yasanın 3. maddesine hüküm eklenmiş, ancak söz konusu hüküm Anayasa Mahkemesi tarafından iptal edilmiştir. Şu halde: "*AYM'nin iptal kararından sonra bu konuda bir yasal boşluk oluşmuştur. Zira iptal üzerine değişiklikten önceki düzenlemenin ihya olması yani yeniden yürürlük kazanması mümkün değildir… Bu durumda mahkemelerin ve savcılıkların yargılamaya veya soruşturmaya ilişkin taleplerinin herkes tarafından karşılanması yasal bir zorunluluk olduğundan artık mahkemelerin ve savcılıkların bu bilgileri ilgili kurumlardan bir hakim ya da mahkeme kararı olmaksızın doğrudan istemeleri mümkündür. Kovuşturma ya da soruşturma aşamasında mahkemelerin ya da hakimlerin bir kararla bunları istemesinde bir sorun bulunmamakla beraber, soruşturma aşamasında kolluk güçlerinin ya da savcılık makamının bir hakim kararı olmaksızın bu önemli verilere ulaşması sorun yaratabilecek niteliktedir. Sorunun çözümü AYM'nin iptal kararındaki gerekçeleri de dikkate alınarak en kısa zamanda yapılacak bir düzenleme ile söz konusu boşluğun giderilmesidir.*" Dülger, **Bilişim Suçları**, s. 731, 732.

c) Üretim Talimatı

Sözleşme'nin 18. maddesinde, adli makamlara, gerçek ya da tüzel kişileri zilyetliği ya da kontrolünde bulunan depolanmış durumdaki bilişim verilerini teslim etmeye ve hizmet sağlayıcıları zilyetliği ya da kontrolünde bulunan hizmetlere ilişkin abone bilgilerini vermeye zorlama olanağı getirilmektedir. Diğer bir ifadeyle kişilerin ellerinde bulunan ya da erişim olanakları bulunan her türlü veriyi adli makamlara teslim etmesi zorunluluğu olarak da ifade edebileceğimiz bu tedbire üretim talimatı adı verilmektedir.

Üretim talimatının konusu, somut bir soruşturma ya da kovuşturmada delil olarak kullanılabilecek, depolanmış durumdaki mevcut verilerdir. Söz konusu veriler talimatın muhatabı gerçek ya da tüzel kişinin ya elinde olmalı, yani ona ait veya onun kullandığı bir bilişim sisteminde depolanmış olmalı ya da bu kişinin söz konusu verilere erişim olanağı bulunmalıdır. Erişim olanağından kastedilen, kişinin fiziken kendi zilyetliğindeki bir bilişim sisteminde depolanmış olmayan verilere uzaktan erişim sağlayabilmesi olanağıdır. Burada, erişim tabirinden fiili olarak erişme olanağı değil, yasal ve meşru bir hak çerçevesinde erişme yetkisi anlaşılmalıdır[399].

Üretim talimatı, adli makamlara birçok durumda, özellikle daha müdahaleci ya da külfetli önlemler yerine kullanabilecek daha esnek bir önlem sağlamaktadır. Ülkelerin üçüncü şahıslarla ilgili, verilerin aranması ve el konulması gibi, "sistematik cebri önlemler" uygulamak yerine ulusal mevzuatları çerçevesinde, soruşturmalarla ilgili bilgileri temin etmek için daha az müdahaleci olan bu şekildeki tedbirlere başvurması özgürlük/güvenlik dengesinin sağlanması anlamında daha tercih edilebilir bir uygulamadır[400].

Servis sağlayıcıların ellerinde bulunan abone bilgileri bakımından üretim talimatı özel olarak vurgulanmıştır. Abone bilgileri temel olarak, abonelere ilişkin bilişim verisi şeklinde tutulan trafik ve içerik verileri hariç her türlü bilgiyi ifade etmektedir[401]. Madde'nin 3. fıkrasında abone bilgileri ayrıntılı olarak tanımlanmıştır. Buna göre: "*kullanılan iletişim türünün, teknik ayrıntıların, hizmet süresinin, hizmet*

[399] Açıklayıcı Rapor, par. 173.
[400] Açıklayıcı Rapor, par. 171.
[401] "Rules on Obtaining Subscriber Information, Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3 Kasım 2014, s. 3.

sözleşmesi bağlamında erişilebilir abone kimlik bilgilerinin, posta ve coğrafi adresinin telefon veya diğer erişim numarasının, fatura ve ödeme bilgilerinin, hizmet sözleşmesi çerçevesinde iletişim teçhizatının kurulduğu yere ilişkin diğer bilgilerin belirlenmesini sağlayabilecek herhangi bir bilgiyi ifade eder". Abone bilgilerine genellikle teknik olarak adresi tespit edilen, ancak faili anonim kalan eylemlerin gerçek kişi faillerinin ortaya çıkarılması amacıyla ihtiyaç duyulur[402].

Sözleşme üretim talimatının ne surette gerçekleşeceği ve talimatın zorlayıcılığının nasıl sağlanacağı konusunu taraf devletlerin ulusal mevzuatlarına bırakmaktadır. Sözleşme'nin şart koştuğu husus genel olarak, kişilerin söz konusu talimatı yerine getirmeye zorlanmasıdır[403].

Türk hukukunda talimat verme şeklinde bir muhakeme tedbirinin mevcut olmadığını yukarıda belirtmiştik. Yürütülen bir soruşturma ya da kovuşturma kapsamında ispat aracı olarak yararlı görülen bilgi ve eşyalar bunları elinde bulunduran kişilerden talep edilebilir. Kamu kuruluşları ve kamu görevlileri bakımından CMK m. 161/4 hükmü uyarınca hakim ya da savcının bu yöndeki taleplerini yerine getirme zorunluluğu olmakla birlikte, özel hukuk kişileri bakımından söz konusu talepleri yerine getirmeye zorlayacak herhangi bir zorunluluk yoktur. Adli makamlarca talep edilen bilgi ve eşyaları teslim etmeyen kişiler bakımından tek caydırıcı etken, talebi yerine getirmemesi halinde hakkında uygulanacak arama kararına maruz kalma tehdididir. Bilişim sistemlerinde depolanmış veriler hakkında arama el koyma tedbirini ayrıca düzenlemiş olan Sözleşme'nin, "talimatı yerine getirmeye zorlamak" tan kastının bu olmadığı aşikardır.

Sözleşme, öngördüğü muhakeme tedbirlerini kronolojiye ve şüphenin seviyesine göre bir sıralamaya göre düzenlemiştir. Buna göre, şüphenin henüz başlangıç seviyesinde olduğu ve zaman kaybedilmeden hareket edilmesi gereken ilk aşamada, daha fazla araştırma yapmak ve gerekli prosedürleri sağlamak üzere depolanmış verilerin süratli şekilde korunması tedbiri uygulanmalı, söz konusu verilerin suç delili olduğu noktasında belirli bir ölçüde kanaat oluşması halinde verileri elinde bulunduran kişiye verileri teslim etmesi talimatı verilmeli, şüphenin makul seviyeye ulaşmasından ve üretim talimatının yerine getirilmemesinden sonra ise arama el koyma tedbirine başvurulmalıdır. Böylelikle her aşamanın koşullarıyla

[402] Açıklayıcı Rapor, par. 178.
[403] Açıklayıcı Rapor, par. 180.

orantılı olarak minimum müdahale ile maksimum koruma sağlanmış olacaktır. Bu sıralama her olayda aynı şekilde uygulanamayacak olmakla birlikte, düzenlenen tedbirlerin niteliğinin ve öneminin anlaşılması bakımından akılda tutulmalıdır.

Arama - el koyma tedbirinin kişi hak ve özgürlüklerine ciddi bir müdahale niteliğinde olması karşısında, üretim talimatı tedbiriyle bu ölçüde bir müdahale gerçekleştirilmeksizin deliller elde edilebilir. Modern ceza muhakemesi hukukunun, kişilerin kendileri aleyhinde delil üretmeye zorlanamamaları şeklindeki *nemo tenetur* ilkesi uyarınca zaten yalnızca üçüncü kişiler hakkında uygulanabilecek bu tedbir ile soruşturulan suç ile belki de hiç alakası olmayan kişilerin gereksiz yere arama - el koyma gibi ağır bir koruma tedbirine maruz kalmasının önüne de geçilmiş olacaktır. Arama - el koyma tedbirinin ağır müdahale içeren yapısından kurtulmak suretiyle, CMK uyarınca bilişim sistemlerinde arama - el koyma tedbirine başvurmak için şart koşulan; "başka surette delil elde etme imkânının bulunmaması" gibi ağır ve elektronik ortamda delil elde etmeyi aşırı zorlaştıran koşullar aranmaksızın, daha basit şartlarla depolanmış verilerin elde edilmesi mümkün olacaktır.

Henüz bu yönde bir çalışması olmayan Türk kanun koyucunun ceza muhakemesi hukukuna bilişim verileri hakkında üretim talimatı tedbirini getirmesinin gerekli olduğu kanaatindeyiz.

d) Depolanmış Veriler Hakkında Arama - El Koyma

19. maddede, bilişim sistemlerinde ve bilişim verilerinin depolanmış olabileceği depolama aygıtlarında arama yapılması veya benzer şekilde erişim yapılmasının ve bu surette erişilen verilere el konulması veya benzer şekilde muhafaza altına alınmasının mümkün olması, yani depolanmış veriler hakkında arama - el koyma tedbiri düzenlenmektedir[404].

Bu tedbir, geleneksel arama - el koyma tedbirinin bilişim verilerine uyarlanmış halidir. Madde metninde arama - el koyma ifadelerinden sonra "veya benzeri yöntemlerle" ifadesine yer verilmesi, bilişim verileri hakkında gerçekleşen arama - el koyma işleminin teknik anlamda fiziksel arama - el koymadan farklı olduğu düşüncesinden ve taraf devletlerin bazılarının ulusal mevzuatlarında bu eylemleri

[404] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 169.

farklı şekilde isimlendirmeleri karşısında Sözleşme'yi kaleme alanların terim birliği sağlayamamasından kaynaklanmaktadır[405].

Geleneksel arama - el koyma tedbirinin maddi varlığı olan eşyalar dikkate alınarak düzenlenmiş olması, hatta bazı ülkelerin mevzuatında bu tedbirin yalnızca maddi varlığı olan eşyalar hakkında uygulanabilmesi karşısında, Sözleşme bilişim verilerine özel ayrı bir arama - el koyma tedbirinin getirilmesini zorunlu tutmaktadır. Bilişim verileri hakkında arama - el koyma tedbirinin, klasik arama el koyma tedbiri için evrensel olarak aranan makul şüphenin varlığının yanı sıra, elektronik ortamda delil elde etme süreçlerinin özellikleri dolayısıyla bazı özel koşullar içermesi gerekmektedir[406]. Sözleşme'nin bu anlamda şart koştuğu koşullar; el konulan verilerin bir kopyasını oluşturmaya ve bu kopyayı saklamaya, ilgili verilerin bütünlüğünü sağlamaya ve gerekmesi halinde erişim sağlanan bilişim sistemindeki verilerin üçüncü kişilerce erişilemez hale getirilmesine ilişkin yetkilerin sağlanmasıdır[407].

19. maddenin ikinci fıkrasında bilişim verileri hakkında gerçekleştirilecek arama - el koyma tedbirlerine özel çok önemli düzenleme getirilmektedir[408]. Soruşturmayı yürüten makamların, gerekli verilerin başka bir bilişim sisteminde olduğu konusunda makul şüpheye sahip oldukları durumlarda, aramayı bu bilişim sistemini ya da onun bir parçasını içine alacak şekilde genişletmelerine izin verilmektedir. Madde metninde aramanın genişletilmesine nasıl izin verileceği ve bunun nasıl gerçekleştirileceği belirtilmemektedir. Bu hususlar ulusal mevzuatlara bırakılmıştır. Ancak her halükarda aranacak veriler ilk bilgisayar sisteminden yasal olarak erişilebilir durumda olmalıdır[409]. Dikkat edilmesi gereken bir diğer husus erişilecek ikinci bilişim sisteminin fiziken ulusal sınırlar içinde bulunmasıdır. Bu madde devletlerin olağan adli yardımlaşma yollarından geçmeksizin başka bir devletin sınırları içinde bulunan verileri aramasına ve bunlara el koymasına imkân tanıyan sınır ötesi arama ve el koyma konusunu kapsamamaktadır[410]. Bu konuya, aşağıda, uluslararası adli işbirliğiyle ilgili bölümde ayrıca değineceğiz.

---

[405] "Arama ve el koyma" ifadesinin yerine "erişim ve kopyalama" ifadesinin kullanılması da önerilmiştir. Açıklayıcı Rapor, par. 134.
[406] Açıklayıcı Rapor, par. 187.
[407] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 177.
[408] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 170.
[409] Açıklayıcı Rapor, par. 194.
[410] Açıklayıcı Rapor, par. 195.

Türk hukukunda, bilişim verileri hakkında arama ve el koyma tedbiri CMK'nın "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*" başlıklı 134. maddesinde düzenlenmektedir[411].

CMK m. 134 ifadesi, Sözleşmenin öngördüğü standartları büyük ölçüde sağlamakla birlikte, aramanın genişletilmesi konusunda herhangi bir hüküm içermemesi önemli bir eksikliktir. CMK m. 134 hükmündeki bu ve başkaca eksiklikler genellikle uygulamacılar tarafından fiili olarak giderilmekle birlikte, bu tedbir aracılığıyla elde edilen delillerin hukuka uygunluğu ve dolayısıyla kabul edilebilirliği konusunda soru işaretlerine ve sorunlara yol açmamak adına bu eksikliklerin bir an önce giderilmesi yerinde olacaktır[412].

e) Bilişim Verilerinin Gerçek Zamanlı Toplanması

Sözleşme'nin 16-19. maddelerinde düzenlenen muhakeme tedbirleri, depolanmış durumda bulunan bilişim verileri hakkında uygulanacak tedbirlerdir. Bu tedbirlerin muhatabı olan gerçek veya tüzel kişiler tarafından depolanmış olmayan geçmiş tarihli verilerin bu tedbirlerin konusunu oluşturması zaten mümkün olmadığı gibi, gerçek zamanlı olarak veya ileriye yönelik olarak verilerin kaydedilmesi de bu tedbirlerin konusunu oluşturamaz[413]. Bilişim sistemleri içerisinde ya da farklı bilişim sistemleri arasında iletilmekte olan verilerin gerçek zamanlı olarak toplanması

---

[411] CMK m. 134 hükmü şu şekildedir: *"(1)Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır."

[412] Dülger, **Bilişim Suçları**, s. 730.

[413] Cangemi, "Procedural Law Provisions of the Council of Europe Convention on Cybercrime", s. 167.

Sözleşme'nin 20. ve 21. maddelerinde düzenlenmiştir. Bu tedbirler klasik iletişimin takibi tedbirlerinin bilişim verilerinin özellikleri dikkate alınarak uyarlanmış birer versiyonudur[414].

"Trafik verilerinin gerçek zamanlı toplanması" başlıklı 20. maddede, devlet tarafından başvurulacak teknik yöntemlerle ve servis sağlayıcıların mevcut teknik imkanları çerçevesinde trafik verilerinin gerçek zamanlı olarak toplanmasının ve kaydedilmesinin mümkün olması öngörülmektedir[415]. Somut bir soruşturma ya da kovuşturmada belirlenen cihazların, teknik araçlarla takip edilmesi ve bunlara ait trafik bilgilerinin eş zamanlı olarak kopyalanmasını düzenleyen madde bu kapsamda başvurulacak teknik yöntemlerin neler olacağı konusunda bir açıklama getirmemektedir[416].

Maddede servis sağlayıcılar bakımından getirilen sorumluluk konusunda bir istisna öngörülmüştür; taraflara iç hukukta yerleşmiş ilkeler uyarınca servis sağlayıcıları bu sorumluluktan muaf tutma hakkı tanınmıştır. Yani taraf devletler, servis sağlayıcılara bu şekilde bir yükümlülük getirebildiği hallerde bunlarla birlikte, getiremediği hallerde müstakil olarak bu tedbiri uygulamak ve teknik önlemleri almak zorundadır. Servis sağlayıcıların yükümlü sayılacağı durumda da bu yükümlülük, ancak servis sağlayıcının mevcut teknik imkanları dahilinde söz konusu olacaktır. Maddede servis sağlayıcılara toplama, kaydetme, işbirliği ya da yardım konusunda teknik yeterliliğe sahip olma yükümlülüğü getirilmemektedir. Servis sağlayıcıların yeni teçhizat edinmeleri ya da geliştirmeleri, uzman desteği sağlamaları ya da sistemlerinin yapılandırmasını yenilemek için masraflı girişimlerde bulunmaları şart koşulmamaktadır. Yalnızca, sistemleri ve personelleri hâlihazırda böyle bir toplama, kaydetme, işbirliği ya da yardımı sağlayacak teknik yeterliliğe sahipse bu yeterliliği kullanmaları için gerekli önlemleri almaya zorlanmaları şart koşulmaktadır[417].

Klasik telekomünikasyon araçlarına, örneğin telefon konuşmalarına ilişkin trafik verilerinin toplanması, her zaman etkili ve yararlı bir soruşturma aracı

---

[414] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 183.

[415] Sözleşme'nin 1. maddesi uyarınca "*trafik verisi; bir bilişim sistemi aracılığıyla gerçekleşen iletişimle ilgili olan, iletişim zincirinin bir halkası olan bir bilişim sistemi tarafından üretilmiş, iletişimin başlangıç noktasını, hedefe varış noktasını, izlediği yolu, saatini, tarihini, boyutunu, süresini, iletişim kullanılan hizmetin temel türünü gösteren her türlü bilişim verisini ifade eder.*"

[416] Açıklayıcı Rapor, par. 220.

[417] Açıklayıcı Rapor, par. 221.

olmuştur[418]. Bu klasik araçlar söz konusu olduğunda trafik verilerinin ait olduğu iletişimler gerçek anlamda iletişim niteliğindedir, yani iki gerçek kişi arasındaki haberleşme eylemlerinden oluşmaktadır. Bilişim sistemleri söz konusu olduğunda ise geleneksel iletişimlerden farklı olarak, bilişim sistemleri arasında gerçekleşen her türlü etkileşim, iletişim sayılmaktadır. Bilişim teknolojileri veri işleme ve veri alış verişi sistemi üzerine kuruludur. Birden fazla bilişim sistemi birbirine bağlandığında mutlaka aralarında veri alış verişinden oluşan bir iletişim meydana gelmektedir. Yani iki bilişim sistemi arasındaki e-posta, mesajlaşma vb. haberleşmeye ilişkin veri iletimleri iletişim olduğu gibi, iki kişi arasındaki haberleşme niteliğinde olmayan etkileşimler de iletişimdir. Örneğin bir bilişim sisteminin bir başka bilişim sistemine erişim sağlaması, daha somut bir ifadeyle bir bilgisayar aracılığıyla bir internet sitesine girilmesi de iletişimdir ve bu iletişime dahil olan bilişim sistemlerinin IP adresleri üzerinden trafik verilerinin toplanması da bu tedbirin kapsamına girmektedir. Sözleşme, iletişim kavramının içeriğine yönelik bu özellikten dolayı bilişim sistemleri aracılığıyla gerçekleşen iletişimlere ait trafik verilerinin özel olarak düzenlenmesini zorunlu tutmaktadır[419].

Trafik verilerinin gerçek zamanlı olarak toplanması tedbiri sayesinde şüphelinin iletişimlerinin saat, tarih, kaynak ve varış noktasıyla mağdurların sistemlerine izinsiz girildiği tarih arasında bağlantı kurulabilir, diğer mağdurlar teşhis edilebilir ya da suç ortakları arasındaki bağlantılar ortaya çıkarılabilir[420]. İçerik verilerinin, yani iletişimi oluşturan verilerin içeriğinin takip edilmesi kadar külfetli olmayan ve hak ve özgürlüklere müdahale niteliği daha az olan bu tedbirden, başta bilişim veri veya sistemlerinin gizliliği ve bütünlüğüne yönelik suçlar ve içerik bağlantılı suçlar olmak üzere pek çok siber suç soruşturma veya kovuşturmasında faydalanılabilir[421].

Türk hukukunun trafik verilerinin gerçek zamanlı olarak toplanması bakımından değerlendirmesini aşağıda içerik verilerinin takibi tedbiriyle bir arada yapacağız.

---

[418] Açıklayıcı Rapor, par. 217.
[419] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 173.
[420] Açıklayıcı Rapor, par. 218.
[421] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 174.

İçerik verilerinin takibi ise Sözleşme'nin 21. maddesinde düzenlenmektedir. Bu maddede, devlet tarafından başvurulacak teknik yöntemlerle ve servis sağlayıcıların mevcut teknik imkânları çerçevesinde bilişim sistemleri aracılığıyla gerçekleşen iletişimlere ait içerik verilerinin gerçek zamanlı olarak toplanmasının ve kaydedilmesinin mümkün olması öngörülmektedir. İçerik verileri, bilişim sistemleri arasındaki veri alış verişinde gönderilen ve alınan verilerin kendisini ifade etmektedir. Bu tedbir uyarınca, somut bir soruşturma ya da kovuşturmada belirlenen bilişim sistemlerinin gerçekleştirmiş olduğu iletişimlerde gönderdikleri ya da aldıkları verilerin görülebilmesinin ve kopyalanmasının mümkün olması amaçlanmaktadır.

İçerik verilerinin takibinin teknik olarak nasıl gerçekleştirileceği konusunda trafik verilerinin gerçek zamanlı olarak korunması tedbirinde olduğu gibi sessiz kalan Sözleşme, servis sağlayıcıların yükümlülükleri konusunda da bu tedbire paralel bir düzenleme getirmektedir. Zaten temel mantığı aynı olan bu iki tedbirin düzenlenmesinde yer verilen unsurlar ve ifadeler büyük ölçüde aynıdır[422].

İçerik verilerinin takip edilmesi tedbiri, telefon görüşmelerinin dinlenmesi ve kayda alınması tedbirinin bilişim sistemlerinin iletişimlerine uyarlanmış halidir denilebilir. Ancak yukarıda belirttiğimiz gibi bilişim sistemleri bakımından iletişim, iki gerçek kişi arasındaki haberleşmeyle sınırlı olmayıp, gönderilen ve alınan her türlü veriyi ifade etmektedir[423]. Bu kapsamda söz gelimi bir internet sitesinde yayına sunulmuş olan bir video görüntüsünü temsil eden veriler de içerik verisidir ve bu tedbirin konusunu oluşturabilir.

İçerik verilerinin takip edilmesi tedbiri, uygulanması teknik anlamda zor ve bir o kadar da külfetli bir tedbirdir[424]. Ancak bu tedbir bakımından asıl öne çıkan durum, tedbirin hak ve özgürlüklere aşırı ölçüde müdahale içermesidir[425]. Bu nedenle Sözleşme'de bu tedbirin tüm suçlar için değil, belirli ciddi suçlar bakımından uygulanması öngörülmüştür. Bu suçların hangi suçlar olacağı ise ulusal mevzuatlara bırakılmıştır. Suç tipi sınırlamasının yanı sıra, içerik verilerinin takibine, trafik verilerinin toplanması tedbirinin yetersiz kalması durumunda başvurulmalıdır. Bu

---

[422] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 185.

[423] Sözleşme'de içerik verilerine ilişkin bir tanım yer almamakla birlikte, Açıklayıcı Rapor'da şu şekilde tanımlanmaktadır: "*İçerik verileri" iletişimin iletişim içeriği, yani iletişimin anlamı ya da niyeti, ya da iletişim yoluyla iletilen mesaj ya da bilgi anlamındadır. Trafik verileri dışında iletişime ait olarak iletilen her şey içerik verisidir*". Açıklayıcı Rapor, par.229.

[424] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 186.

[425] Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 174.

durum sözleşmede açıkça zikredilmemekle birlikte, usul hukukuna ilişkin genel hükümler getiren 15. maddenin benimsediği orantılılık ilkesi bunu gerektirir.

Türk hukukunda, bilişim verilerine ait trafik veya içerik verilerinin gerçek zamanlı olarak takip edilmesini düzenleyen özel bir hüküm bulunmamaktadır. Ancak, CMK'nın telekomünikasyon yoluyla yapılan iletişimin denetlenmesini düzenleyen "*İletişimin tespiti, dinlenmesi ve kayda alınması*" başlıklı 135. maddesinde, telekomünikasyon yoluyla yapılan iletişimin tespit edilmesi, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi düzenlenmektedir. Bazı yazarlar bilişim sistemleri arasındaki iletişimlerin de telekomünikasyon yoluyla yapılan iletişim olduğunu ve dolayısıyla CMK'nın 135. maddesinde düzenlenen bu tedbirin kapsamına girdiğini savunmaktadır[426]. Oysa CMK'nın 135. maddesinde düzenlenen tedbir kişiler arasındaki haberleşme niteliğindeki iletişimleri konu almaktadır. Hem madde metnine, hem de ikincil mevzuata açıkça yansımış olan bu durum, öğreti tarafından da benimsenmiş ve 135. maddedeki tedbirin konusunun kişiler arasındaki haberleşme faaliyetleri olduğu vurgulanmıştır[427]. Oysa bilişim sistemlerindeki iletişimlerde esas olan kişiler değil, iletişimin tarafı olan bilişim sistemleridir. Bu itibarla CMK'nın 135. maddesi yalnıza e-posta, mesajlaşma gibi kişiler arasındaki haberleşme faaliyetlerine ilişkin bilişim verilerine uygulanabilir nitelikte olup, bilişim sistemleri arasında gönderilip alınan diğer verileri kapsamamaktadır.

CMK m. 135'teki iletişimin denetlenmesi tedbirinin bilişim sistemleri arasındaki her türlü iletişime dair verileri kapsayacağı görüşü teorik olarak kabul edilse dahi, tedbirin bilişim verileri hakkında uygulamasını mümkün kılacak ikincil mevzuatın bulunmaması karşısında bu görüş pratik bir anlam ifade etmemektedir. Gerçekten de "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla

---

[426] Bu yönde görüşler için bkz: Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 186; Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 176.

[427] Maddede ve ikincil mevzuatta geçen "dinlenmesi" ve "şüpheli veya sanığın" ifadeleri bu durumu ortaya koymaktadır. Ayrıca Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelikte iletişimin dinlenmesi ve kayda alınması: *"telekomünikasyon yoluyla gerçekleştirilmekte olan **konuşmaların** dinlenmesi ve kayda alınması ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri"* olarak tanımlanmıştır. CMK m. 135'teki tedbirin içeriği ve kapsamı konusunda benzer yaklaşım için bkz. Veli Özer Özbek/Mehmet Nihat Kanbur/ Koray Doğan/Pınar Bacaksız/İlker Tepe, **Ceza Muhakemesi Hukuku**, 6. Baskı, Ankara: Seçkin, 2014, s. 441 vd.; Nur Centel/Hamide Zafer, **Ceza Muhakemesi Hukuku**, 11. Baskı, İstanbul: Beta, 2014, s. 417 vd.; Yenisey/Nuhoğlu, **Ceza Muhakemesi Hukuku Ders Kitabı**, s. 609 vd.; Hakan Hakeri/Yener Ünver, **Ceza Muhakemesi Hukuku**, 5. Baskı, Ankara: Adalet, 2012, s. 414.

Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik" de bütünüyle gerçek kişiler arasındaki haberleşme niteliğindeki iletişimlerin takip edilmesini esas alarak hazırlanmış ve bilişim verilerinin takip edilmesine yönelik hiçbir hükme yer verilmemiştir. Özellikle Yönetmelik'in "Tedbirin Kapsamı" başlıklı 7. Maddesinde, tedbire konu olacak iletişimlerin şüpheli ya da sanığın haberleşmeleri olduğu belirtilmiş olması karşısında bu tedbirin bilişim sistemlerinin iletişimlerine uygulanması bakımından yasal belirsizliğin yanı sıra ciddi bir alt yapı eksikliği olduğu ortadadır[428].

Uygulamada da CMK'nın 135. maddesinin bilişim verileri hakkında uygulanmasının örneği yoktur Zaten bilişim alanında suçlar, iletişimin dinlenmesi, kayda alınması ve sinyal verilerinin değerlendirilmesi bakımından belirlenmiş katalog suçlar arasında yer almamaktadır. Diğer suçlar bakımından da zaten ikincil mevzuat ve yapılanma anlamında uygun zemin bulunmadığı için, bilişim verileri hakkında bu maddenin uygulanması söz konusu olmamaktadır[429].

Adli makamların, servis sağlayıcılar tarafından 5651 sayılı Kanun uyarınca zorunlu olarak tutulan ve istem üzerine Başbakanlık Telekomünikasyon İletişim Başkanlığı'na verilen trafik verilerini özel olarak bir tedbire başvurmadan elde edebildiklerini yukarıda belirtmiştik. Uygulamada trafik verileri bakımından özel bir tedbire başvurmaya gerek duymadan, kolaylıkla bilgi edinilebilen bu yöntem yeterli

---

[428] Adı geçen yönetmeliğin *"Tedbirin Kapsamı"* başlıklı 7. maddesi şu şekildedir:

"(1) İletişimin tespiti, dinlenmesi, kayda alınması veya sinyal bilgilerinin değerlendirilmesi tedbirine şüpheli veya sanık bakımından karar verilir.

(2) Birinci fıkrada sayılan tedbirler, hakkında tedbir uygulanacak kişinin üzerine kayıtlı veya kullanmakta olduğu iletişim araçlarının tümü hakkında uygulanabilir. Hakkında karar verilen kişi ile iletişim araç sahibinin farklı kişiler olması hâlinde bu durum talep ve kararda açıkça belirtilir.

(3) İletişimin tespiti, dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi kararı kişilerin yurt dışı bağlantılı iletişimini de kapsar.

(4) Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar Cumhuriyet savcısının huzurunda derhâl imha edilir ve bu husus bir tutanağa bağlanır. Ceza Muhakemesi Kanununun 135 inci maddesinde belirtilen yasal şartlar varsa, suç işleme şüphesi altındaki tanıklıktan çekinme hakkı olan şahıslar hakkında da hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla bu tedbire başvurulabilir.

(5) Şüpheli veya sanığa yüklenen suç dolayısıyla suç şüphelisi olmayan müdafiin bürosu, konutu ve yerleşim yerindeki telekomünikasyon araçları hakkında, Ceza Muhakemesi Kanununun 135 inci madde hükmü uygulanamaz.

(6) Dinleme ve kayda alma kararının yerine getirilmesi sırasında şüphelinin başka bir iletişim aracını kullandığı belirlendiğinde buna ilişkin verilecek karar ya da kararların süresi önceki tedbir kararında verilen sürenin bitiş tarihini geçemez."

[429] Bu konuda uygulamaya ilişkin bilgiler, İstanbul Cumhuriyet Başsavcılığı Bilişim Suçları Bürosu'nda görev yapan Cumhuriyet Savcısı Hasan Basri Zamanis'ten şifahi olarak edinilen verilere dayanmaktadır.

görülmektedir. Oysa şüpheli tarafından iletişimin izinin kaybettirilmesine yönelik önlemler alındığı durumlarda trafik verilerinin geçmişe doğru takip edilmesi çok zor hatta imkânsız olabilmektedir. Trafik verilerinin uygun teknik imkânlarla gerçek zamanlı olarak toplanması halinde bu sorun kısmen de olsa aşılabilir. Ayrıca idari bir tedbir olarak tutulan trafik verilerinin özel bir koruma tedbirine başvurmadan, doğrudan elde edilmesi doğru bir uygulama değildir. Kişilerin özel hayatının ve haberleşme özgürlüğünün ihlal edilmesi suretiyle açıkça temel haklara müdahale niteliğinde olan trafik verilerinin edinilmesi işlemi mutlaka bir koruma tedbiri çerçevesinde gerçekleşmedir[430]. Aksi hal, yani mevcut durum hem temel insan hakları metinlerinde hem Anayasa'da yer bulan temel hak ve özgürlüklerin ancak yasayla düzenlenen ve hakim kararıyla uygulanan önlemlerle kısıtlanabilmesi ilkesine aykırıdır.

Diğer yandan yasal soruşturma ve kovuşturma işlemleri kapsamında uygulan(a)masa da, polis ve istihbarat birimlerinin bilişim verilerinin gerçek zamanlı olarak takip edilmesi için gerekli teknik alt yapıya sahip olduğu ve fiilen bu yöntemlere başvurduğu bilinmektedir[431]. Demokratik bir hukuk devletinde tümüyle kabul edilemez olan bu yöntemle elde edilen verilerin ceza muhakemesi bakımından hukuka aykırı delil niteliğinde olduğu ve dikkate alınmayacağı da muhakkaktır. Bilişim verilerinin gerçek zamanlı olarak takip edilmesi konusunda yeterli yasal zeminin mevcut olmaması bir yandan ceza muhakemesi süreçlerinde bu delillerin elde edilerek kullanılmasını önlemekte diğer yandan da fiilen uygulanan bu tür işlemlerin tümüyle hukuk dışı kalarak denetlenebilir olmamasına yol açmaktadır.

Türk ceza muhakemesi hukukunda bu sorunların çözülmesi için, hem trafik verilerinin geçmişe dönük olarak ve gerçek zamanlı olarak tespit edilmesi hem de içerik verilerinin gerçek zamanlı olarak takibinin mevzuat tarafından ayrıntılı ve net bir şekilde koruma tedbiri olarak düzenlenmesi şarttır. Bu düzenleme CMK'nın 135. maddesinde yapılacak değişiklik veya eklemelerle yapılabileceği gibi bağımsız bir madde altında da yapılabilir[432]. Ayrıca mutlaka ilgili ikincil mevzuatla bu tedbirlerin

---

[430] Centel/Zafer, **Ceza Muhakemesi Hukuku**, s. 319.

[431] *"...TİB'de başlatılan incelemede 300 trilyon belgeye sığan kapasitede dinleme yapıldığı ortaya çıktı ama dosyalara ulaşılamadı; kablo sistemi bile çözülemedi. TİB yetkililerinin tavsiyesi vahim: Binanın gömülmesi gerekir"*. "Milyarlarca saatlik dinleme gömülecek", Milliyet Gazetesi, (erişim: 27.08.2015), http://www.milliyet.com.tr/milyarlarca-saatlik-dinleme-gundem-1989484/.

[432] Sözleşemeye taraf devletlerde her iki yönde de uygulamaya rastlanmaktadır. Ayrıntılı bilgi için Avrupa Konseyi'nin resmi internet sitesinde yer alan karşılaştırma tablolarına bkz. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp.

uygulanmasına ilişkin teknik ayrıntılar düzenlenmeli ve olası kötüye kullanım ve hak ihlallerinin önüne geçmek adına gerekli güvence ve denetim mekanizmaları tesis edilmelidir.

Sözleşmenin düzenlediği usuli tedbir ve yöntemler konusunda yalnızca minimum güvenlik standardını getirmekle kalmadığını, aynı zamanda 15. madde uyarınca bu tedbir ve yetkilerin uluslararası metinlerde ve iç hukukta benimsenen temel ilkelere uygun olarak tesis edilmesi ve uygulanmasını zorunlu tuttuğunu yukarıda belirtmiştik. Türkiye, hem Sözleşme'nin öngördüğü minimum güvenlik standardını sağlamak hem de hak ve özgürlüklerin sınırlandırılması konusunda temel uluslararası metinlere taraf olmakla yüklendiği ve de Sözleşme'nin ısrarcı atfıyla özellikle gündeme gelen standartları sağlamak adına bilişim verilerinin gerçek zamanlı toplanması konusunda yasal önlemleri gecikmeksizin almalıdır.

f) Yargılama Yetkisi

Sözleşme'nin 22. maddesinde taraf devletlerin, 2-11. maddelerde düzenlenen suçlar üzerinde yargı yetkisi tesis ederken uymak zorunda oldukları bir dizi ölçüt sayılmıştır. Esasında yetkinin maddi ceza hukukuna mı, ceza muhakemesi hukukuna mı ilişkin olduğu sorusunun net bir cevabı yoktur[433]. Sözleşme, yetki konusunu ceza muhakemesiyle daha yakından ilişkili görerek usul hukukuna ilişkin hükümler arasında düzenlemiştir.

Sözleşme, kural olarak ülkesellik (mülkilik) prensibini benimsemektedir. Buna göre taraf devletler, kendi ulusal sınırları içerisinde, bayraklarını taşıyan gemilerde ve kendi ülkelerine kayıtlı uçaklarda işlenen suçlar bakımından yetkili olacaklardır. Sözleşme ülkesellik ilkesinin istisnası olarak faile göre şahsilik ilkesini öngörerek, vatandaşın yurt dışında suç işlemesi halinde de, fiilin suçun işlendiği yerde cezalandırılabilir olması koşuluyla ilgili taraf devletin de yetkili olacağını düzenlemiştir.

---

[433] Leronzo Picotti, "National Legistlation Implementing the Convention on Cybercrime- Comperative Anlaysis and Good Practices", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Tartışma Raporu, 28 Ağustos 2008, s. 56.

Görüldüğü üzere, Sözleşme, yetki konusunda yaygın pratiği ilke olarak dillendirmenin ötesinde özel bir düzenleme içermemektedir[434]. Suçun nerede işlenmiş sayılacağı şeklindeki, siber suçlar bakımından karmaşık yetki sorunlarının fitilini ateşleyen en temel sorunu göremezden gelen Sözleşme, ilkesel bir yaklaşımla olumsuz yetki uyuşmazlıklarının önüne geçmeyi ve siber suçların takipsiz kalmasını önlemeyi amaçlamaktadır. Olumlu yetki uyuşmazlıkları karşısında sözleşmenin öngördüğü çözüm ise tarafların istişare etmeleridir. 22. maddenin son paragrafında yer alan tarafların istişare etmeleri önerisi bir çözüm niteliğinde olmayıp, Sözleşme'nin bu konuda sessiz kalması itibariyle tarafların zaten mecbur kaldıkları durumun ifadesinden ibarettir.

Sözleşme, 22. maddenin 4. bendinde öngörülen yetki halleri dışında ulusal mevzuatın devleti yetkili kıldığı hallerin dışlanmayacağını belirterek, adeta açıkça tek kaygısının olumsuz yetki uyuşmazlıkların önüne geçme olduğunu ve olumlu yetki uyuşmazlıklarını sorun olarak görmediğini itiraf etmektedir. Aslında Sözleşme'nin yetki konusundaki bu tutumu, siber suçların cezasız kalmaması amacıyla çelişmektedir. Zira birden fazla devletin kendini yetkili saydığı durumlarda tarafların diğerinin soruşturma yapacağı düşüncesiyle soruşturma yapmaktan kaçınması muhtemeldir[435].

Bu nedenle kanaatimizce yetki mümkün olduğunca tek bir devlete ait olacak şekilde düzenlenmeli, olumsuz uyuşmalıklar kadar olumlu uyuşmazlıklar da minimize edilmeye çalışılmalıydı. Sınır aşan siber suçların soruşturulmasında hem ulusal adli makamların ulusal düzlemde yapacakları işlemler bakımından hem de adli yardımlaşmanın doğru ülkenin adli makamlarına yöneltilebilmesi bakımından son derece kritik bir öneme sahip olan yetki konusunda Sözleşme'nin, net olmayan ve yetki sorunlarını çözmekten uzak bu tavrı önemli bir eksikliktir[436].

Türk hukukunda yetki, Ceza Kanunu'nun "*Yer bakımından uygulama*" başlıklı 8. maddesinde düzenlenmiştir[437]. Buna göre: *"Türkiye'de işlenen suçlar hakkında*

---

[434] Suçun işlendiği yer konusunda Açıklayıcı Rapor'da bir öneri getirilmektedir. Buna göre: hedef bilişim sisteminin bulunduğu yer suçun işlendiği yer kabul edilebilir (Açıklayıcı Rapor, par. 233). Açıklayıcı raporun bağlayıcılığın olmaması dolayısıyla bu kabulün taraflara, yetki sorunu yaşandığı taktirde yürütecekleri istişarelerde yol göstermenin dışında bir anlamı yoktur.

[435] Yenisey/Nuhoğlu, **Ceza Muhakemesi Hukuku Ders Kitabı**, s. 253.

[436] Podgor, "International Computer Fraud", s. 301.

[437] Burada yetkiden kastedilen yabancılık unsuru içeren suçlarda Türk mahkemelerinin yetkili olması durumudur. Bunun dışında Ceza Muhakemesi Kanunu'nun 12-21. maddelerinde düzenlenen yetki, Türkiye içinde hangi yer mahkemelerinin davaya bakacağına ilişkin olup, sınır aşan suçlarda Türk mahkemelerinin yetkili olup olmadığı hususunu düzenlememektedir.

Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır. Suç; a) Türk kara ve hava sahaları ile Türk karasularında, b) Açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla, c) Türk deniz ve hava savaş araçlarında veya bu araçlarla, d) Türkiye'nin kıt'a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı, işlendiğinde Türkiye'de işlenmiş sayılır". Ülkesellik prensibini benimseyen TCK m. 8 hükmü ve yabancılık unsuru içeren suçlara ilişkin TCK'nın 9-13. maddeleri Sözleşme'nin yetki hükümleriyle bire bir uyumludur[438].

D. Sözleşme'nin Genel Değerlendirmesi ve Sözleşmeye Yönelik Eleştiriler

Avrupa Siber Suçlar Sözleşmesi siber suç yasalarının reformunu uluslararası düzleme çeken çok yönlü bir girişimdir[439]. Sözleşme, siber suçlarla mücadele konusundaki mevcut uluslararası girişimler arasında içerik ve katılım anlamında en kapsamlı olan metindir[440]. Sözleşme'yi bu alanda eşsiz yapan şey ise, çok taraflı bir uluslararası sözleşme olarak taraf devletlere bağlayıcı yükümlülükler getirmesidir[441]. Giderek daha da birbirine bağımlı hale gelen ve siber güvenlik anlamında büyük risklerle karşı karşıya olan uluslararası toplumu bir araya getirmeye yönelik ilk bağlayıcı hukuki metin olan Sözleşme'nin geç kalmış bir girişim olduğu bile söylenebilir[442].

Birinci bölümde ayrıntılı olarak ortaya koyduğumuz üzere, farklı hukuk sistemleri bir arada uygulanma ve işbirliği içinde hareket etmeye karşı uyum direnci geliştirmektedir. Devletlerin diplomatik anlamda iyi niyetle ve çözüm odaklı hareket etmeleri uyum direncini aşma konusunda bir ölçüde çözüm sunabilse de mevzuatlardaki farklılıklar çoğu zaman işbirliğini imkânsız kılmaktadır. Bu yönüyle

[438] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi" s. 192.
[439] Herlihy, "The Cybercrime Convention: A Pioneering Text", s. 175.
[440] Vatis, "The Council of Europe 's Convention on Cybercrime", s. 220.
[441] Keyser, "The Council of Europe Convention on Cybercrime", s. 296.
[442] Keyser, "The Council of Europe Convention on Cybercrime", s. 297.

ulusal mevzuatları uyumlulaştırma girişimi, Sözleşme'yi değerli kılan yönlerin başında gelmektedir[443].

Sözleşme, pek çok özelliği ile siber suçlarla mücadelede yaşanan sorunlara çözüm sunmaya elverişli bir aday görünümündedir. Bu özelliklerinin başında; siber suçlarla mücadele konusunda imzalandığı tarihe kadar oluşmuş birikimi dikkate alması, alanda faaliyet gösteren diğer uluslararası kurumlarla irtibatı sürdürmeye yönelik sistemler içermesi, siber alemin değişken yapısını ilkesel olarak kabul etmiş olması, taraf devletler arasında iletişimin ve istişarelerin sağlıklı olarak sürdürülmesine yönelik iletişim mekanizmaları kurması ve Sözleşme'nin yaşayan bir metin olabilmesi yönünde çalışmalar yürüten T-CY yani Avrupa Siber Suçlar Sözleşmesi Komitesi'nin varlığı sayılabilir.

Avrupa Siber Suçlar Sözleşme'sinin siber suçlarla mücadele alanında en önemli uluslararası metin olduğu öğretide ağız birliği ile dillendirilmektedir[444]. Sözleşme'nin önemi, öğretinin yanı sıra başta uluslararası siyasi örgütler olmak üzere pek çok platformda tasdik edilmektedir. Birleşmiş Milletler Uyuşturucu ve Suç Ofisi UNODC tarafından Sözleşme'nin önemi vurgulanmakta ve dikkatle incelenmesi gerektiği belirtilmektedir[445]. Yine UNODC, Sözleşme'ye katılım konusunda dünya devletlerinin çekimserliğini eleştirmekte ve katılımları teşvik etmektedir. Avrupa Birliği de Sözleşme'nin önemini farklı vesilelerle vurgulamakta[446] ve üye devletleri Sözleşme'yi imzalamaya ve etkin bir şekilde uygulamaya davet etmektedir[447]. Bunun dışında Asya - Pasifik Ekonomik İşbirliği (APEC), Amerikan Devletleri Örgütü (OAS) ve Interpol başta olmak üzere pek çok uluslararası kurum Sözleşme'yi öne çıkarmakta ve desteklemektedir[448]. Siber alemde faaliyet gösteren çok sayıda sivil

---

[443] Mıquelon, "The Conventıon On Cybercrıme: A Harmonızed Implementatıon", s. 352.

[444] Bu yöndeki çok sayıdaki görüş arasından bkz: Dülger, **Bilişim Suçları**, s. 193; Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 192; Keskin, "Avrupa Konseyi Siber Suçlar Sözleşmesinde Ceza Muhakemesi", s. 155; Sınar, "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", s. 785; Vatis, "The Council of Europe Convention on Cybercrime", s. 2012; Gercke, "Understanding Cybercrime" s. 200; Weber, "The Council of Europe Convention on Cybercrime", s. 441; Keyser, "The Council of Europe Convention on Cybercrime", s. 325.

[445] UNODC Sekreterliği, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime", (erişim: 21.08.2015), http://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf.

[446] Buono, "Gearıng Up The Fıght Agaınst Cybercrıme", s. 336.

[447] Avrupa Parlamentosu için Komisyon Raporu, "Towards a general policy on the fight against cyber crime (COM(2007)267 final)", s. 6.

[448] Vatis, "The Council of Europe Convention on Cybercrime", s. 219.

toplum örgütü ve özel kuruluş da Sözleşme'yi olumlu bir girişim olarak değerlendirmektedir[449].

Sözleşme'ye olumlu eleştirilerin yanı sıra, çok sayıda olumsuz eleştiri de yöneltilmektedir. Bunların başında Sözleşme'nin çok sayıda belirsizlik ve esneklik içermesi gelmektedir. Sözleşme'de, ulusal düzeyde alınacak önlemler düzenlenirken suç tiplerinin ve uygulanacak usuli tedbirlerin tanımı yapılmakta, ancak bunları bire bir kopyalama yükümlülüğü getirilmemektedir. Bu durumun belirsizlikleri ve dolayısıyla taraf devletlerin ulusal mevzuatlarındaki olası farklılık ve uyumsuzlukları gidermede yetersiz kaldığı düşünülmektedir[450]. Bunun yerine taraf devletlerin bire bir kopyalamak zorunda oldukları model bir siber suç yasası önerilmesinin daha etkili bir çözüm olacağı savunulmaktadır[451]. Bu yöndeki eleştirilerin somut bir yansıması olarak Birleşmiş Milletler'in telekomünikasyona ilişkin konularda yetkili birimi ITU ve Amerikan Barolar Birliği tarafından "ITU Siber Suç Mevzuat Araçları" hazırlanmıştır[452].

Sözleşme'ye belirsizlik ve esneklik kapsamında yöneltilen eleştirilerin bir diğer kaynağı çekincelere geniş ölçüde imkan veren çekince rejimidir[453]. Sözleşme'nin 44. maddesindeki düzenleme itibariyle kolay bir şekilde çekince koymanın mümkün olması sebebiyle, bazı taraf devletler ulusal mevzuatlarında gerekli önlemleri en azından Sözleşme'de öngörüldüğü şekliyle almayabilecektir[454].

Biz Sözleşme'nin belirsizliği ve esnekliği konusundaki bu eleştirilere katılmakla birlikte, Sözleşme'ye taraf olan farklı coğrafyalardan ve farklı hukuk sistemlerinden gelen devletlerin, Sözleşme'nin bu hali üzerinde dahi zorlukla ittifak edebildiğinin de hatırda tutulması gerektiğini düşünüyoruz.

Sözleşmeye yöneltilen önemli bir eleştiri de sözleşmenin yetki sorunları konusunda ilkesel önerilerin ötesinde bir çözüm getirmeyip, sorunun sürmesine imkân tanımasıdır[455].

---

[449] Vatis, "The Council of Europe Convention on Cybercrime", s. 220.
[450] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 142.
[451] Zahid Jamil,"Cybercrime Model Laws", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu,9 Kasım 2014, s. 7.
[452] ITU Siber Suç Mevzuat Araçları (ITU Toolkit), doğrudan kopyalanması öngörülen maddi ceza hukukuna ve muhakeme hukukuna yönelik model yasalar içermektedir. Bahsi geçen araçlara şu adresten erişilebilir: (erişim: 25.08.2015) http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.
[453] Weber, "The Council of Europe Convention on Cybercrime", s. 444.
[454] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1245.
[455] Podgor, "International Computer Fraud", s. 301.

Biz de yukarıda ayrıntılı olarak açıkladığımız üzere sözleşmenin bu konuda amaçlarıyla bağdaşmayan bir tutum içinde olduğunu düşünüyoruz.

Sözleşme'nin en yoğun şekilde eleştirildiği konular arasında ulusal düzeyde başvurulması ve uluslararası adli yardımlaşmaya da konu olması öngörülen usuli tedbirlerin, hak ve özgürlükleri ihlal edici nitelikte olması gelmektedir[456]. Sözleşme'yi "otoriter" bir yapıda gören bazı düşünürler sözleşmeyi eleştirmekte ve temel hak ve özgürlükleri kısıtlayıcı, bireyin karşısında kamusal otoriteyi güçlendirici bir yapıda olduğu için Sözleşme'nin bu haliyle imzalanmaması gerektiğini belirtmektedirler[457]. Sözleşme'nin özellikle ilk zamanlarında yoğun olarak dillendirilen bu yöndeki eleştiriler – belki de taraf devletlerin Sözleşme'yi gereği gibi uygulamamalarının da etkisiyle- giderek azalmaktadır[458].

Biz bu yöndeki endişelerin dikkate alınması gerektiğini düşünmekle birlikte, Sözleşme'nin öngördüğü maddi ve usuli hükümlerin bütünüyle reddedilmesi yönündeki görüşlere katılmıyor, Sözleşme hükümlerini, siber suçlarla etkin bir şekilde mücadele edilebilmesi için gerekli araçlar olarak değerlendiriyoruz[459]. Zaten Sözleşme, öngörülen usuli tedbirlerin ne pahasına olursa olsun mutlak surette uygulanmasını şart koşmamaktadır. Aksine; 15. maddede söz konusu usuli yetki ve tedbirler hakkında insan hak ve özgürlükleri bakımından yeterli koruma mekanizmalarının sağlanması koşulu getirilmekte ve temel koruyucu insan hakları belgelerine atıf yapılmaktadır.

Sözleşme'de öngörülen usuli tedbirlerin temel hak ve özgürlüklere müdahale edici nitelikte olduğu tartışmasızdır. Bu tedbirlere yönelik koruyucu mekanizmaların yalnızca ilkesel olarak öngörülmesi ve ayrıntılı şekilde tanımlanmamış olması bir eksiklik olarak görülebilir. Ceza ve ceza muhakemesi hukukunun klasik sorunsalı olan özgürlük - güvenlik dengesi elbette ilgili mevzuat tarafından hassasiyetle gözetmeli ve ayrıntılı hükümlerle garanti altına alınmalıdır. Ancak bu sorunsalın tek başına düzenleyici işlemlerle aşılması mümkün değildir. Tamamen kazuistik bir yöntemle tüm olası senaryolar için çözüm önerileri olan bir mevzuat yapılabileceği varsayılsa dahi dahi insan üretimi böyle bir mevzuat yine de kusursuz olmayacaktır.

---

[456] Vatis, "The Council of Europe Convention on Cybercrime", s. 219.
[457] Dülger, **Bilişim Suçları**, s. 196.
[458] Vatis, "The Council of Europe Convention on Cybercrime", s. 217.
[459] Aynı yönde görüş için bkz. Dülger, **Bilişim Suçları**, s. 196.

Bu itibarla sorunun çözümü esasında uygulayıcının etik bilinci ve haklara saygısında yatmaktadır[460].

Sözleşme'nin servis sağlayıcılara çok ağır bir yükümlülük getirdiği konusunda da eleştiriler dillendirilmekle birlikte bu görüşlere katılmak mümkün değildir[461]. Birincisi, siber alemi düzenlemenin yolu kimi zaman ilgili hizmeti sunan servis sağlayıcıların işbirliğini zorunlu kılmaktadır ve bazı konularda servis sağlayıcıların yasal yükümlülük altına sokulması kaçınılmazdır. Diğer yandan, Sözleşme, alınacak usuli tedbirlerin teknik boyutunu ve uygulamaya yönelik ayrıntıları ulusal mevzuatlara bırakmakta, servis sağlayıcılara sorumluluk yüklediği durumlarda dahi istisnalar öngörmektedir. Taraf devletlerin Sözleşme gereği üstlendikleri yükümlülükleri, servis sağlayıcılara orantısız bir yükümlülük getirerek sağlamaya çalışmaları ilgili taraf devletler bakımından eleştirilebilecek bir husus olmakla birlikte; Sözleşme'nin eksikliği olarak değerlendirilemez.

Netice olarak; tüm eksik ve eleştiriye açık yanlarına rağmen Sözleşme'nin en önemli özelliği; siber suçlara karşı uluslararası toplumun ortak bir ceza siyaseti benimsemesi ve işbirliği içinde hareket etmesi adına öncü bir girişim olmasıdır[462]. Sözleşme'nin minimum standartlar öngörerek başlattığı bu girişimin başta Sözleşme'ye taraf devletler olmak üzere uluslararası sistemin aktörleri tarafından geliştirilmesi gerekmektedir.

E. Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol

Teknolojik, ticari ve ekonomik gelişmelerin dünyanın farklı toplumlarına ait bireyleri bir arada yaşamaya itmesine karşılık, ırk ve etnik köken farkına dayalı, ayrımcılık ve nefret başta olmak üzere tahammülsüzlük örnekleri de artarak

---

[460] Ahmet Ulvi Türkbağ, "Hukuk Eğitiminin Etik Boyutu", **1. Hukuk Eğitimi Kongresi**, 07-08 Kasım 2013, Akdeniz Üniversitesi Hukuk Fakültesi, Ankara: Türkiye Adalet Akademisi Yayınları, 2014, s. 69.

[461] Bu yöndeki eleştiriler için bkz. Vatis "The Council of Europe Convention on Cybercrime", s. 218; Keyser, "The Council of Europe Convention on Cybercrime", s. 325; Önok "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1246.

[462] Herlihy, "The Cybercrime Convention: A Pioneering Text", s. 176.

varlıklarını sürdürmektedir[463]. Avrupa'da, özellikle Schengen protokolünün yürürlüğe girmesi sonucu sınırların olmadığı ve dolaşım özgürlüğünün uygulandığı son yirmi yılda yabancı nüfusunda ciddi bir artış olmuş ve bunun ardından çok sayıda örgütlü ırkçı eylem ve gösteri baş göstermiştir[464]. Özellikle internetin kullanımının da yaygınlaştığı bu yıllarda bilişim sistemleri aracılığıyla yayılan ırkçı ve nefret içerikli söylem, propaganda ve tehditler ciddi bir sorun haline gelmiştir[465].

Uluslararası toplum olarak ırk ve etnik köken ayrımına dayalı ayrımcılık, nefret ve tahammülsüzlük eylemlerine karşı yürütülen mücadelede önemli adımlar atılmış ve bu çabalar Evrensel İnsan Hakları Beyannamesi (1948) ve Her Türlü Irk Ayrımcılığının Ortadan Kaldırılmasına İlişkin New York Sözleşmesi (1966) başta olmak üzere çeşitli uluslararası metinlerle de somutlaştırılmıştır. Ancak başta internet olmak üzere bilişim sistemleri üzerinden gerçekleştirilen ırkçı eylemlerin özel olarak düzenlenmesi ihtiyacı ortaya çıkmıştır[466].

Avrupa Siber Suçlar Sözleşmesi'nin hazırlanması sürecinde bilişim sistemleri aracılığıyla işlenen ırkçı eylemlerin de "içerikle bağlantılı suçlar" başlığı altında yer alması fikri tartışılmıştır. Ancak taraflar, düşünce ve ifade özgürlüğünün içeriği ve sınırları konusunda çok büyük bir sorunsal teşkil eden bu suçlar konusunda uzlaşma sağlayamamıştır. Bunun üzerine bu suçların bir ek protokolle imzaya açılması kararlaştırılmış, CDPC tarafından protokolü hazırlamak üzere, PC-CY Komitesinden ayrı bir alt komite kurulmuştur[467]. 2001 yılında kurulan Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Nefret İçerikli Eylemlerin Suç Haline Getirilmesi Konusunda Uzmanlar Komitesi PC-RX, Sözleşme'nin maddi ve usuli hükümler ve adli yardımlaşma anlamında ırkçı eylemlere de genişletmeyi amaçlayan Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline

---

[463] Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokole Açıklayıcı Rapor, par. 2.

[464] Dülger, **Bilişim Suçları**, s. 197.

[465] Örneğin 2011 yılında Norveç'te Anders Behring Breivik adlı ırkçı saldırgan tarafından bir gençlik kampında gerçekleştirilen ve 77 kişinin ölümüne, 242 kişinin ise yaralanmasına yol açan saldırılar dünya çapında infial uyandırmış, ilk zamanlar bireysel bir eylem olarak düşünülen saldırının internet üzerinden örgütlenen ırkçı bir yapılanmanın eylem planı olduğu ortaya çıkmıştır. Söz konusu yapılanmanın dünyanın farklı coğrafyalarından destekçileri olduğu ve internette yayılan "Avrupa Bağımsızlık Bildirgesi-2083" başlıklı 1516 sayfalık bir manifesto etrafında bir araya geldikleri anlaşılmıştır. Kaynak: (erişim: 21.07.2015), https://www.opendemocracy.net/simen-saetre/in-search-of-spider-in-anders-behring-breivik's-web.

[466] Ek Protokole Açıklayıcı Rapor, par. 3.

[467] Ek Protokole Açıklayıcı Rapor, par. 4, 5.

Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol'ü hazırlamıştır[468]. PC-RX Komitesi Ek Protokol hakkında bir de Açıklayıcı Rapor hazırlamıştır.

28 Ocak 2003'te Strasbourg'da imzaya açılan ve en az 5 imzacı devlet tarafından yürürlüğe sokulmasının ardından 3 Ocak 2006'da yürürlüğe giren Ek Protokol'ü Ağustos 2015 itibariyle 31 devlet imzalamış, bunlardan yalnızca 10 tanesi onaylayarak yürürlüğe sokmuştur. Sözleşmeye taraf olan ancak Avrupa Konseyi üyesi olmayan 21 devletten yalnızca Kanada Ek Protokol'ü imzalamıştır.

Toplamda 16 maddeden oluşan Ek Protokol 'de dört grup suç belirlenmiş, bunun dışında teşebbüs, iştirak gibi ek yükümlülüklere ve Ek Protokol'ün uygulamasına ilişkin hükümlere yer verilmiştir. Ek protokolde öngörülen suç tipleri şunlardır: Irkçı ve yabancı düşmanlığı içeren materyallerin bilişim sistemleri aracılığıyla yayılması (m. 3), ırkçı veya yabancı düşmanlığı motivasyonlu tehdit (m. 4), ırkçı veya yabancı düşmanlığı motivasyonlu aşağılama (m. 5), soykırım ve insanlığa karşı suçların inkarı, önemsizleştirilmesi, onaylanması veya haklı görülmesi (m. 6).

Türkiye henüz Ek Protokol'ü imzalamış değildir. Türk mevzuatında TCK'nın "*Halkı kin ve düşmanlığa tahrik ve aşağılama*" başlıklı 216. maddesinin Ek Protokol'ün 3, 4 ve 5. maddelerinde düzenlenen suç tiplerini büyük ölçüde karşıladığı söylenebilir. Ancak Türkiye'nin özellikle 6. maddede düzenlenen soykırım ve insanlığa karşı suçların inkarı, önemsizleştirilmesi, onaylanması veya haklı görülmesi suçu bakımından Ek Protokol'ü imzalamaktan kaçındığı ifade edilmektedir[469]. Uluslararası platformda Türkiye'nin sıklıkla karşısına çıkan sözde Ermeni soykırımı iddiaları dolayısıyla, Türkiye Cumhuriyeti'nin temsil eden yetkililer her platformda; soykırım iddialarının tarihçiler tarafından tartışılması gereken bir konu olduğunu ve tarihi bir olayın niteliğinin yasalar aracılığıyla aksi iddia edilemez şekilde belirlenmesinin bilimsel olmadığı gibi düşünce ve ifade özgürlüğüyle de bağdaşmayacağını savunmaktadırlar[470]. Bu nedenle Türkiye'nin yakın gelecekte Ek Protokolü imzalayacağını öngörmek oldukça güçtür.

---

[468] Ek Protokole Açıklayıcı Rapor, par. 6.

[469] Havuz, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 163.

[470] Ek Protokol uyarınca okuduğunuz bu cümle dahi suç teşkil etmelidir. Zira Ermeni soykırımı iddiaları hakkında "sözde" ifadesi kullanarak önemsizleştirici hatta inkâr edici bir üslup kullanmaktayız.

Üçüncü Bölüm
AVRUPA SİBER SUÇLAR SÖZLEŞMESİNDE ULUSLARARASI ADLİ İŞBİRLİĞİ

A. Avrupa Siber Suçlar Sözleşmesinin Öngördüğü Uluslararası Adli İşbirliği Sistemi

Avrupa Siber Suçlar Sözleşmesi'nin asıl amacı devletlerin global siber suç sorunuyla işbirliği ve uyum içinde mücadele etmelerini sağlamaktır[471]. Sözleşme'nin, taraf devletlerin ulusal düzeyde almasını öngördüğü maddi hukuka ve usul hukukuna ilişkin önlemler de esasında bu amaca yöneliktir. Bu düzenlemeler sayesinde işbirliği ve uyum içinde yürütülecek ortak mücadeleye uygun bir zemin inşa edilmesi amaçlanmaktadır. Ancak ulusal mevzuatların etkin ve uyumlu bir hale getirilmesi, siber suçlarla uluslararası düzeyde mücadele edilmesi için tek başına yeterli değildir. Bunun için, sınır aşan siber suçların soruşturma ve kovuşturmalarında farklı devletlerin adli makamlarının işbirliğini mümkün kılacak uluslararası adli işbirliği mekanizmalarının da mevcut olması ve etkin bir şekilde işlemesi şarttır.

Sözleşme'nin "Uluslararası İşbirliği" başlıklı Üçüncü Bölümünde, önce uluslararası adli işbirliğine ilişkin genel ilkeler sayılmakta, sonrasında suçluların iadesi ve adli yardımlaşma rejimi düzenlenmektedir. Konunun ayrıntılarına geçmeden önce, bu alana ilişkin kavramların kullanımında yaşanan karmaşaya değinmekte ve bu konuda görüşümüzü açıklamakta fayda görüyoruz. "Uluslararası işbirliği", "uluslararası adli işbirliği", "uluslararası adli yardımlaşma" kavramları birbirine yakın ve ilişkili kavramlar olmaları itibariyle sıklıkla karıştırılmakta ve birbirlerinin yerine kullanılabilmektedir.

Uluslararası işbirliği; bir konuda gerek devletler, gerek uluslar üstü siyasi yapılar gerekse de başta uluslararası sivil toplum örgütleri olmak üzere uluslararası

[471] Paust, "Cybercrimes and the Domestication of International Criminal Law", s. 436.

toplumu oluşturan diğer aktörlerin konu sınırlaması olmaksızın tesis ettikleri ve uyguladıkları ortak yaklaşım ve tavrı ifade eden üst bir kavramdır[472]. Siber suçlar konusunda uluslararası işbirliği; suçların adli takibi konusunda uluslararası sözleşmeler ve diğer işbirliği mekanizmalarıyla tatbik edilecek adli işbirliğini, hukuki bağlayıcılığı olmayan diplomatik faaliyetleri, özel sektörle dayanışma içinde yürütülecek toplumsal farkındalık kampanyalarını, siber güvenliğin sağlanmasına yönelik araştırma, geliştirme ve eğitim faaliyetleri ile burada kısıtlayıcı bir liste halinde sayamayacağımız siber suç olgusunun önlenmesine yönelik her türlü işbirliği faaliyetini ifade eder.

Uluslararası adli işbirliği; genel anlamda işbirliğinin bir alt dalı olup, suç sorunları konusunda yasal önlemlerin alınması, bilgi ve belge paylaşımı mekanizmalarının kurulması ve adli süreçlerin yürütülmesi konusunda somut yardımlaşma taleplerinin yerine getirilmesi, yani adli yardımlaşmanın yürütülmesi dahil suçla mücadelenin adli boyutuna ilişkin her türlü konuyu kapsamaktadır[473]. Devletlerin ceza adalet sistemleri kapsamında siber suçların tespiti, soruşturulması ve kovuşturulmasına ilişkin her türlü faaliyete ilişkin ortak girişimleri adli işbirliğinin konusunu teşkil edebilir. Bu itibarla adli işbirliğinin önleyici polisiye tedbirleri de kapsadığı unutulmamalıdır.

Uluslararası adli yardımlaşma ise; adli makamların, yabancı bir devletin adli makamlarının yetkili olduğu bir soruşturma işlemini yapma konusunda bu makamlardan işlemi kendisi adına yapmasını istemesidir[474].

Sözleşme'nin Üçüncü Bölümünün başlığı "Uluslararası İşbirliği" olmakla birlikte bu bölümde genel olarak işbirliği değil, adli işbirliği ele alınmaktadır. Uluslararası adli işbirliğine ilişkin genel ilkeleri saymakla yetinen ve suçluların iadesini özel olarak düzenleyen Sözleşme'nin asıl yoğunlaştığı konu uluslararası adli yardımlaşmadır.

---

[472] Modiga, "Importance And Necessity of International Judicial Cooperatıon in Criminal Matters", s. 98.

[473] Modiga, "Importance And Necessity of International Judicial Cooperatıon in Criminal Matters", s. 98.

[474] Robert J.Currie, "Peace And Public Order: International Mutual Legal Assistance:The Canadian Way", **Dalhousie Journal of Legal Studies**, sy. 7, 1998, s. 95.

1. Uluslararası Adli İşbirliğine İlişkin Temel İlkeler

Sözleşme'nin 23. maddesinde uluslararası adli işbirliğiyle ilgili üç genel ilke ortaya konmuştur. Maddede ilk olarak, Taraflar arasındaki uluslararası işbirliğinin "mümkün olan en geniş biçimde" gerçekleştirileceği belirtilmiştir. Bu ilke tarafların birbirlerine kapsamlı işbirliği sağlamalarını ve bilgi ve delillerin uluslararası akışının düzgün ve hızlı olmasını engelleyen faktörleri en aza indirmelerini önermektedir[475]. Oldukça soyut bir çerçeve çizmesi itibariyle doğrudan uygulanabilir olmayan ve temenniden ibaret kalan bu ilke, devamında sayılan ilkelerle daha somut bir kalıba oturtulmaktadır.

23. maddede ikinci olarak işbirliği yükümlülüğünün genel kapsamı ortaya konmuştur: İşbirliği bilişim sistemleri ve verileri ile ilgili suçlar ve herhangi bir suçun delillerinin elektronik ortamda toplanmasının söz konusu olduğu bütün durumlar için geçerli olacaktır. Sözleşme, adli işbirliğini 2-10. maddelerde düzenlenen suç tipleriyle hatta genel olarak siber suçlarla sınırlamayıp, siber alemde yürütülecek tüm soruşturmaların kapsam dahilinde olduğunu söyleyerek "mümkün olan en geniş şekilde" uygulanması ilkesini daha somut bir çerçeveye oturtmaktadır. Ancak belirli konularda taraflara farklı bir kapsam benimseme hakkı tanınmıştır. Bunlar; suçluların iadesine ilişkin 24. madde, trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşmaya ilişkin 33. madde ve içerik verilerinin takip edilmesi konusunda yardımlaşmaya ilişkin 34. maddelerde tanınmış olan istisnalardır.

Adli işbirliğine ilişkin üçüncü genel ilke; işbirliğinin hem sözleşmenin adli işbirliğine ilişkin hükümleri çerçevesinde hem de cezai meselelerde uluslararası adli işbirliğine ilişkin diğer uluslararası belgelerin, tek taraflı ya da karşılıklı antlaşmaların ve ulusal mevzuatların uygulanması yoluyla gerçekleştirileceğidir. Bu ifade ile, Sözleşme'nin Üçüncü Bölümünde yer alan adli işbirliğine, karşılıklı adli yardımlaşmaya ve suçluların iadesine ilişkin hükümlerin, taraflar arasında bu konularda mevcut uluslararası sözleşmelerin ve ulusal mevzuatın uluslararası işbirliğiyle bağlantılı ilgili hükümlerinin yerini almayacağı anlatılmaktadır[476].

---

[475] Açıklayıcı Rapor, par. 242.
[476] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi" s. 1249.

Bu temel ilke suçluların iadesine ilişkin 24. madde, adli yardımlaşmaya ilişkin genel ilkelerin sayıldığı 25. madde, kendiliğinden bilgi verme ilişkin 26. madde, uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen adli yardım taleplerine ilişkin usulleri düzenleyen 27. madde, kullanımda gizlilik ve sınırlamaya ilişkin 28. madde, depolanan veriler hakkında arama el koymaya ilişkin 31. madde, trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşmaya ilişkin 33. madde ve içerik verilerinin takip edilmesine ilişkin 34. maddelerde de bir kez daha vurgulanarak açık bir biçimde pekiştirilmiştir[477]. Sözleşme'nin adli işbirliği hükümlerinin mevcut sistemleri kaldırmaksızın, bu sistemlerle bir arada uygulanması, çok sayıda çok taraflı ve iki taraflı antlaşmayla düzenlenmiş olması itibariyle karşılıklı adli yardımlaşma uygulaması bakımından önemli sonuçlar doğurmaktadır. Bu sonuçları, ilkeye ilişkin diğer ayrıntıları ve değerlendirmelerimizi aşağıda Sözleşme'nin öngördüğü adli yardımlaşma rejimini açıklarken aktaracağız.

2. Suçluların İadesi

Suçluların iadesi, en temel adli işbirliği yöntemlerinden birisidir[478]. Bununlar birlikte, iadenin bir adli yardımlaşma yöntemi olmadığını hatırlatmakta fayda görüyoruz. İade, yargılanacak kişinin yargılama konusu fiil üzerinde yargılama yetkisine sahip olan devletin adli makamlarına teslim edilmesidir. Oysa, adli yardımlaşma, yargılama yetkisine sahip olan devletin adli makamlarının, yer itibariyle uygulama yetkisine sahip olmadıkları konularda yetkili devletin adli makamlarından söz konusu soruşturma işlemini kendileri yerine yapmalarını istemesidir[479].

Sözleşme'nin 24. maddesinde, sadece 2 ila 10. maddelerde tanımlanan ve her iki taraf devletin yasaları uyarınca bir yıl hapis ya da daha ağır bir cezayla cezalandırılabilir olan suçlar bakımından geçerli olmak üzere iade yükümlülüğü düzenlenmektedir. Bu suçlar mevcut iade anlaşmaları çerçevesinde iadeye konu olabilen suçlar olarak değerlendirilecek ve tarafların kendi aralarında gelecekte yapacakları anlaşmalara dahil edilecektir.

---

[477] Açıklayıcı Rapor, par. 244.
[478] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1250.
[479] James Cockayne, "Review: On the Cosmopolitanization of Criminal Jurisdiction", Journal of International Criminal Justice, sy. 3/2, 2005, s. 515.

Açıklayıcı Rapora göre bir yıllık sürenin tespitinde somut olayda suça verilecek ceza değil, suç için soyut normda öngörülen cezanın üst sınırı dikkate alınacaktır.[480]. Sözleşme'nin kendi öngördüğü suçlar bakından bir de ceza sınırı getirmesinin sebebi, taraf devletlerin Sözleşme'de öngörülen bazı suçları daha kısa azami hapis süreleriyle cezalandırabilme ihtimalidir. İade talebinde bulunulabilmesi için talebe dayanak oluşturacak suçun en az bir yıl hapis cezası gerektirmesi şartı, aynı yönde hüküm içeren Suçluların İadesine Dair Avrupa Sözleşmesi'yle de uyumludur.

Sözleşme bir yıllık asgari ceza sınırını mutlak bir şekilde düzenlememiştir. Maddenin 1. fıkrasının (b) bendinde Suçluların İadesine Dair Avrupa Sözleşmesi'ne ve isimleri verilmeden iadeye ilişkin diğer uluslararası mevzuata gönderme yapılmış olup, bu metinler uyarınca farklı bir asgari ceza sınırı söz konusu olduğunda bu sınırın uygulanacağı belirtilmiştir. Birçok iade anlaşması bir yıllık asgari ceza sınırını benimsemektedir[481]. Ancak bu anlaşmalarda sonradan yapılacak değişiklikler de kendiliğinden Sözleşme'nin öngördüğü asgari ceza sınırını değiştirmiş olacaktır. Bunun yanı sıra, başta Suçluların İadesine Dair Avrupa Sözleşmesi olmak üzere iade konusundaki uluslararası metinler, iadeye konu suçların asgari ceza süresi konusunda başka bir süre sınırının belirlenmesi hakkını saklı tutmaya imkan tanımaktadır. Bu kapsamda farklı bir asgari limit belirlemiş olan devletler bakımından da Sözleşme'nin öngördüğü bir yıllık süre geçerli olmayacaktır. Adli işbirliğine ilişkin pek çok konuda olduğu gibi bu konuda da Sözleşme'nin getirdiği hükümler yedek norm hükmündedir[482]. Bu durum uluslararası adli işbirliğinin taraflar arasında yürürlükte olan mevcut anlaşmalar uyarınca yürütülmesi şeklindeki genel ilkenin doğal bir sonucudur.

23. maddenin 3. fıkrası uyarınca taraflar arasında iade anlaşması bulunmadığı ya da mevcut anlaşmalar Sözleşme'de yer alan suçlarla ilgili bir talebi kapsamadığı ya da ulusal mevzuatın aradığı koşullar sağlanamadığı için iade işleminin gerçekleştirilemediği durumlarda Sözleşme'nin iade için hukuki zemin oluşturacağı düzenlenmiştir. Esasında maddenin genel düzenlemesinden anlaşılan bu husus, bir devletin ulusal ya da uluslararası mevzuat gereğince iade işlemini gerçekleştirebilmek için bu konuda "açık bir uluslararası sözleşmeye dayanmak

[480] Açıklayıcı Rapor, par. 245.
[481] Açıklayıcı Rapor, par. 246.
[482] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 178.

zorunda olması" durumunda sözleşmenin farlı şeklinde yorumlanmasından kaynaklı aksaklıkları bertaraf etmeyi amaçlamaktadır. Maddenin 4. fıkrasında ise iadeye ilişkin ulusal mevzuatın iadeye dayanak oluşturabilecek bir grup suçla sınırlı tuttuğu durumlarda, Sözleşme'de yer alan suçları bu suç grubuna dahil etme zorunluluğu getirilmiştir.

Madde'nin 5. fıkrasında, uluslararası ve ulusal mevzuatta öngörülen hüküm ve şartları yerine getirmemesi halinde iade talebinin reddedilebileceği belirtilmektedir. Yine bu durum, işbirliğinin taraflar arasında yürürlükte bulunan mevcut işbirliği rejimi çerçevesinde gerçekleştirilmesi ilkesinin yansıması ve tekrarıdır. Örneğin, Suçluların İadesine Dair Avrupa Sözleşmesi ve Ek Protokollerinde (ETS No 86 ve 98) belirtilen şartlar ve sınırlamalar bu sözleşmelerin tarafları için geçerli olacak ve iade konusu suçun siyasi nitelikli olduğuna ya da söz konusu kişinin ırkı, dini, milliyeti ya da siyasi görüşü nedeniyle iade talebine konu yapıldığına karar verildiğinde, iade talebi reddedilebilecektir[483].

Madde'nin 6. fıkrasında "aut dedere aut judicare" (iade et ya da kovuştur) ilkesine yer verilmiştir. Birçok ülkenin mevzuatı uyarınca vatandaşın iadesi mümkün olmadığı için, vatandaşı oldukları devlette bulunan suçluların, başka bir taraf devlette işlenmiş oldukları suçlar takipsiz kalabilir. 6. fıkra uyarınca, kişinin vatandaş olması gerekçesiyle iade talebi reddedildiğinde, talebi yapan devletin isteği üzerine, muhatap devlet, ilgili fiili soruşturulmak üzere ulusal adli mercilere sevk etmek zorundadır. 6. fıkranın son cümlesi uyarınca, bu soruşturma ciddiyetle ve titizlikle yürütülecek ve soruşturma sonucunda talepte bulunan devlet bilgilendirilecektir. İade talebi reddedilen devlet, fiilin ulusal makamlarca soruşturulmasını talep etmezse, talebi reddeden devlet soruşturma yapmak zorunda değildir. İade talebinin olmadığı ya da talebin başka bir gerekçeyle reddedildiği durumlarda da, ilgili devletin sınırları dışında işlenmiş suçları kendiliğinden soruşturma yükümlülüğü bulunmamaktadır[484].

Taraf devletlerin iade taleplerinin nereye yöneltileceğini bilebilmesi için, maddenin 7. fıkrasında, tarafların herhangi bir anlaşmanın olmadığı durumlarda iade ve geçici tutuklama taleplerini yapmak ya da kabul etmekle sorumlu olacak makamların isim ve adreslerini Avrupa Konseyi Genel Sekreteri'ne bildirmeleri şart koşulmuştur.

---

[483] Açıklayıcı Rapor, par. 250.
[484] Açıklayıcı Rapor, par. 252.

3. Sözleşmenin Öngördüğü Karşılıklı Adli Yardımlaşma Rejimi

Uluslararası adli yardımlaşma, ilgili devletler arasında yürürlükte bulunan ikili ya da çok taraflı sözleşmeler vasıtasıyla gerçekleştirilir. Bu sözleşmeler muhatap devleti adli yardımlaşma talebini yerine getirmeye zorlar. İki devlet arasında bu şekilde bir sözleşme bulunmaması halinde ise adli yardımlaşma, uluslararası teamül hukuku kuralları ve mütekabiliyet (karşılıklılık) ilkesi çerçevesinde yürütülür[485].

Yarımlaşma talebinde bulunacak devlet kendi iç hukuku uyarınca yetkilendirdiği makamlar eliyle ve muhatap devletle aralarındaki adli yardımlaşma anlaşması çerçevesinde belirlediği usuller uyarınca bir adli yardımlaşma talebi düzenleyerek muhatap devlete iletir. İstinabe müzekkeresi (letter rogatory) denilen bu talep, adli yardımlaşma anlaşması uyarınca gerekli koşulları sağlıyorsa muhatap devletin adli makamları tarafından yerine getirilir.

Çalışmamızın ilk kısmında ayrıntılı olarak ortaya koymaya çalıştığımız üzere mevcut adli yardımlaşma rejimleri, gerek ulusal ve uluslararası mevzuattan gerek uygulamadan kaynaklı sorunlar nedeniyle günümüzün global suç sorunlarına cevap verebilecek şekilde işlememektedir. Çoğunlukla sınır aşan nitelikte olan ve hızlı hareket etmenin hayati önem arz ettiği siber suçlara ve delilleri elektronik ortamda bulunan diğer suçlara ilişkin soruşturmalar söz konusunu olduğunda ise klasik adli yardımlaşma mekanizmaları bütünüyle etkisiz ve anlamasız kalmaktadır. Sözleşme'yi kaleme alanlar bu sorunu kısmen de olsa çözebilmek amacıyla adli yardımlaşmaya ilişkin genel ilkeler benimsemiş ve bazı özel düzenlemeler getirmiştir.

a) Adli Yardımlaşmaya İlişkin Genel İlkeler

Adli yardımlaşmaya ilişkin genel ilkeler Sözleşme'nin 25. maddesinde belirtilmiştir. Bu ilkeler büyük ölçüde 23. maddede belirtilen uluslararası adli işbirliğine ilişkin ilkelere paralel olarak düzenlenmiştir. Taraflar siber suçlara ve

[485] Kemal Şimşek, **Yabancıların Türkiye'de Yargılanması ve Uluslararası Adli Yardımlaşma**, Ankara: Adalet, 2014, s. 146.

delilleri elektronik ortamda bulunan diğer suçlara ilişkin soruşturma ve kovuşturmalarda "mümkün olan en geniş şekilde" yardımlaşacaktır. Görüldüğü üzere 23. maddede belirtildiği gibi, adli yardımlaşma konusunda işbirliği yükümlülüğü ilke olarak hem sözleşmede öngörülen suç tipleri, hem genel olarak siber suçlar, hem de delilleri elektronik ortamda bulunan her türlü suç bakımından geçerlidir. Ancak, 34 ve 35. maddelerde tarafların bu önlemlerle ilgili olarak farklı uygulama kapsamları belirlemelerine izin verilmiştir.

Sözleşmede öngörülen adli yardımlaşma hükümleri bu konudaki mevcut uluslararası ve ulusal mevzuatlar çerçevesinde yürütülecektir. Genel olarak adli işbirliği konusunda benimsenen bu ilke adli yardımlaşmaya ilişkin 25. maddede de açıkça dile getirilmektedir. Sözleşme, prensip olarak mevcut adli yardımlaşma mekanizmaları çerçevesinde uygulanacak bir sistem öngörse ve mevcut bir mekanizma olmadığında uygulanacak yedek bir sistem tesis etse de, 27 ila 35. maddelerdeki düzenlemeler bağımsız ve doğrudan uygulanabilir niteliktedir. Bu hükümlerin bir kısmı uygulanabilir mevcut bir mekanizma olmadığında devreye girecek yedek hükümlerken (27, 28), bir kısmı da özel yardımlaşma usulleri olup taraflara ilave yükümlülükler getirmektedir. Diğer bir anlatımla taraflar adli yardımlaşmayı uygulanabilir mevcut mekanizmalar çerçevesinde yürütecek; mevcut mekanizmaların yetersiz kaldığı durumlarda Sözleşme'nin sunduğu yedek mekanizmaları kullanacak; ancak her halde sözleşmenin öngördüğü özel yardımlaşma usullerini uygulayacaktır.

Sözleşme'nin mevcut yardımlaşma mekanizmalarını koruması ve bunlarla birlikte uygulanması, bu alanda yaşanan sorunların aynen devam etmesine yol açacağı endişesiyle eleştirilmekte ve bunun yerine bütünüyle yeni ve bağımsız bir adli yardımlaşma sisteminin kurulması önerilmektedir[486]. Ancak, çok taraflı bir sözleşmenin kendisinden önce imzalanmış çok sayıdaki diğer sözleşmeleri kısmen veya tamamen ilga ederek bunların yerini alması pratik anlamda yapılabilir olmadığı gibi; bu durum yazılı metinler kadar yerleşik uygulama yani teamüllerin de etkili olduğu uluslararası hukuk bakımından tercih edilesi bir seçenek de değildir. Sözleşme, adli yardımlaşma anlaşması bulunmayan hallerde uygulanacak yedek adli yardımlaşma kurallarını belirlemek suretiyle mevcut sistemin açıklarını kapatmayı amaçlamakta, mevcut sistemin hantallığını aşmak üzere de siber alemde yürütülen

[486] Weber, "The Council of Europe 's Convention on Cybercrimes", s. 442, Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1249.

soruşturmalar için özel adli yardımlaşma usulleri getirmektedir. Mevcut adli yardımlaşma rejimlerinin korunması yoluyla uygulamacıların en iyi tanıdıkları araç ve düzenlemeleri kullanmalarına izin verilmesinin daha pratik olacağı gözden kaçırılmamalıdır[487]. Sözleşme'nin öngördüğü özel usullerin eksiklikleri ve eleştiriye açık yönleri olsa da, Sözleşme'nin uluslararası adli yardımlaşma konusundaki genel sistematiği olabilecek en iyi yöntemdir denilebilir[488].

Taraf devletlerin sözleşmenin doğrudan uygulanabilir hükümlerini ne şekilde tatbik edecekleri konusunda bir açıklık yoktur. Sözleşme, "gerekli yasama tedbirleri ve diğer tedbirleri" kabul etmenin gerektiğini ifade etmekle yetinmektedir. Bazı taraf devletler bu hükümleri uygulamak için herhangi bir uygulama mevzuatına gerek duymayacaktır; çünkü ayrıntılı yardımlaşma rejimleri tesis eden uluslararası antlaşmaların hükümlerinin kendi kendine uygulanabilir nitelikte olduğu kabul edilmektedir[489]. Doğrudan uygulanabilir yardımlaşma usullerini yürütmek için taraf devletlerin, ya bu hükümleri doğrudan uygulanabilir olarak değerlendirmesi ya da bunun için gerekli olabilecek düzenlemeleri hızla yapmaları beklenmektedir[490].

Sözleşme'de adli yardımlaşma taleplerinin iletim şekline ilişkin çok önemli bir kolaylık öngörülmektedir. 25. maddenin 3. fıkrası uyarınca acil durumların söz konusu olması halinde taleplerin faks veya e-posta gibi hızlı iletişim araçları ile iletilmesinin mümkün olması öngörülmektedir. Bazı bilişim verileri kısa süreliğine saklanmakta ve sonra silinmektedir. Diğer yandan bilişim verileri son derece uçucu niteliktedir; birkaç tuşa basılarak ya da otomatik programların çalışması sonucunda bu veriler silinebilir ve böylelikle kritik önemdeki deliller erişilemez hale gelebilir. Yine bazı durumlarda, deliller hızla toplanmazsa kişilerin can ve mal güvenlikleri önemli ölçüde tehlikeye girebilir. Bu tür acil durumlarda, sadece talep değil buna verilen cevap da hızlı bir biçimde iletilmelidir. Bu nedenle 25. maddenin 3. bendinde adli taleplerin, yazılı ve mühürlü belgelerin diplomatların çantalarında ya da posta hizmetlerinde taşındığı, çok daha yavaş olan geleneksel iletimler yerine hızlı iletişim yollarıyla iletilmesi ve muhatap devletin de bu gibi durumlarda taleplere cevap vermek için hızlı yolları kullanması öngörülmektedir. Tarafların, mevcut mevzuatları halihazırda buna imkan sağlamıyorsa, gerekli düzenlemeleri yapmaları şart koşulmaktadır.

---

[487] Açıklayıcı Rapor, par. 262.
[488] Vatis, "The Council of Europe 's Convention on Cybercrime", s. 208.
[489] Açıklayıcı Rapor, par. 255.
[490] Açıklayıcı Rapor, par. 256.

Madde metninde geçen faks ve e-posta örnek olarak sayılmış olup içinde bulunulan şartlar açısından uygun olabilecek herhangi başka bir hızlı iletişim yolu da kullanılabilir. Teknoloji ilerledikçe, yardımlaşma talebi için kullanılabilecek başka hızlı iletişim yolları da geliştirilecektir[491]. Bu konudaki tek kriter, söz konusu araçların "güvenlik ve doğrulama ölçütlerini" sağlamasıdır. Güvenlik ve doğrulama ölçütüyle ilgili olarak, taraf devletler kendi aralarında iletişimlerin doğruluğunun nasıl güvence altına alınacağına ve özellikle hassas olan bir durumda "şifreleme dahil özel güvenlik korumalarına" gerek duyulup duyulmadığına karar verebilirler. Ayrıca, muhatap devletin, hızlı iletimin ardından geleneksel kanallarla resmi bir onayın gönderilmesini şart koşmasına da izin verilmektedir.

Adli yardımlaşma taleplerinin ret nedenlerinin, "aksi öngörülen" haller dışında mevcut adli yardımlaşma mevzuatına tabi olduğu düzenlenmiştir. Aksi öngörülen haller Sözleşme'nin 27. ve 29. maddelerindeki, ret nedenlerine ilişkin özel düzenlemeleri ifade etmektedir. Ayrıca, Sözleşme'de düzenlenen suçlara ilişkin taleplerin, sırf suçun mali suç olarak değerlendirilmesi gerekçesiyle reddedilemeyecektir.

Adli yardımlaşma mevzuatlarında yer alan en önemli ret nedeni olan karşılıklı cezalandırılabilirlik koşulu ise sözleşme tarafından özel olarak tanımlanmaktadır. Buna göre, talebe dayanak teşkil eden suça konu olan fiil, muhatap devletin yasaları uyarınca da suç teşkil ediyorsa, bu yasalar suçu başka bir suç kategorisine yerleştiriyor ya da suçu adlandırmak için farklı bir terminoloji kullanıyor olsa bile, karşılıklı cezalandırılabilirlik sağlanmış kabul edilecektir[492]. Sözleşme'nin karşılıklı cezalandırılabilirliği bu şekilde tanımlaması oldukça yerindedir. Zira bazı devletler karşılıklı cezalandırılabilirlik koşulunu, suça konu olan fiilin her iki ülkede de suç sayılması şeklinde (*in abstacto*) değil, fiilin talep edilen ülkede tüm koşullarıyla cezalandırılabilirlik şartlarını taşıması şeklinde (*in concreto*) veya aynı suç kategorisinde yer alması şeklinde uygulamaktadır[493]. Sözleşme, adli yardımlaşmayı en geniş ölçüde mümkün kılmak amacıyla karşılıklı cezalandırılabilirlik koşulunu en hafif düzeyde tanımlamıştır[494].

---

[491] Açıklayıcı Rapor, par. 256.
[492] Açıklayıcı Rapor, par. 259.
[493] Aldesco, "The Demıse Of Anonymıty", s. 96.
[494] Açıklayıcı Rapor, par. 259.

b) Kendiliğinden Bilgi Verme

Taraf devletlerden birinde, ulusal düzeyde yürütülen soruşturma veya kovuşturmalarda elde edilen bilgilerin, diğer taraf devletlerin Sözleşme'de düzenlenen suçlarla ilgili soruşturma başlatmasına ya da var olan soruşturmaların yürütülmesine yardımcı olabileceği hallerde ilgili devlet ya da devletlere kendiliğinden bilgi verme yükümlülüğü getirilmektedir. Sözleşmenin 26. maddesinde hükme bağlanan bu uygulama, Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El Konulmasına İlişkin Avrupa Sözleşmesi'nin 10. maddesi ve Yolsuzluğa Karşı Ceza Hukuku Sözleşmesi'nin 28. maddesi gibi geçmiş Avrupa Konseyi metinlerindeki hükümlerden türetilmiştir[495]. Bir devletin belli bir siber suç soruşturma ya da kovuşturmasında başka bir devlete yardımcı olabileceğine inandığı değerli bilgilere sahip olduğu ve soruşturma ya da takibatı yürüten ülkenin bunun varlığını bilmediği durumlar sıklıkla yaşanmaktadır[496]. Bu gibi durumlarda, ilgili devletin yardımlaşma talebinde bulunması mümkün değildir. Bazı ülkelerin ulusal mevzuatları uyarınca, talep olmaksızın yardım sağlanması için kesin bir yetkilendirme gerekmektedir. Bu nedenle Sözleşme'nin bu hükmü oldukça önemlidir.

Taraf devletlerin, hassas bilgiler söz konusu olduğunda, bilgilerin gizli tutulmasını ya da bilginin kullanımıyla ilgili başka şartları isteme hakkı vardır. Bilginin ifşa edilmesi durumunda, bilgiyi veren devletin çıkarlarının tehlikeye gireceği, örneğin bilgi toplama yönteminin niteliğinin ya da bir suç grubu ile ilgili soruşturma yürütüldüğünün gizlenmesine ihtiyaç duyulduğu durumlarda hassas bilgilerin varlığından söz edilebilir[497]. Bilgi veren devlet tarafından aranan bir şarta uyulmasının önünde, bilgi verilen devlet bakımından hukuki ya da fiili engeller varsa, örneğin; bilginin kamuya açık bir duruşmada delil olarak kullanılması gerekliliğinden ötürü gizlilik şartına uyulamayacaksa, bilgi verilen devlet, bilgi veren devlete bunu bildirecektir. Bu durumda da elinde bilgiyi bulunduran devletin bilgi vermekten kaçınma seçeneği vardır.

Bilgi vermenin hangi makamlar aracılığıyla ve hangi usullere göre gerçekleşeceği konusunda yol gösterici bir hükme ne Sözleşme'de ne de Açıklayıcı

---

[495] Açıklayıcı Rapor, par. 260.
[496] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi", s. 179.
[497] Açıklayıcı Rapor, par. 261.

Rapor'da yer verilmektedir. 7/24 irtibat noktalarının, sözleşme çerçevesinde taraf devletlerin irtibatlarını sağlamak üzere genel olarak yetkilendirilmiş olmaları itibariyle bu noktada birincil olarak rol alması gerekmektedir.

c) Uluslararası Adli Yardımlaşma Anlaşmalarının Yürürlükte Olmadığı Hallerde Uygulanacak Hükümler

Avrupa Konseyi devletleri bakımından adli yardımlaşma konusunda bir çok ortak antlaşma zaten mevcuttur[498]. Buna karşılık, Sözleşme'ye, Avrupa Konseyi'ne taraf olmayan devletler de taraftır ve bunların söz konusu diğer adli yardımlaşma sözleşmelerine taraf olması kolay ve olası değildir. Böyle durumlarda adli yardımlaşmayı mümkün kılmak amacıyla, aralarında uygulanabilir ortak bir antlaşma mevcut olmayan devletler açısından, adli yardımlaşmanın ne şekilde gerçekleşeceğine dair ilke ve esaslar Sözleşme'nin 27. maddesinde düzenlenmiştir[499]. Bu itibarla Sözleşme, aralarında özel bir antlaşma bulunmayan taraf devletler açısından, karşılıklı adli yardımlaşma antlaşması işlevi görecektir[500].

Sözleşme'nin en uzun maddesi olan 27. madde, 2 ila 10. fıkralarında, uluslararası adli yardımlaşma antlaşmalarının yokluğunda, yardımlaşmanın gerçekleştirilebilmesini sağlayacak, merkezi yetkili makamların tesisi, erteleme ya da reddetme durumlarında şartların, gerekçelerin ve usullerin yerine getirilmesi, taleplerin gizliliği ve doğrudan doğruya iletişimler gibi bir dizi konuda ayrıntılı düzenlemeler getirmektedir. Ancak maddede, uluslar arası adli yardımlaşmaya ilişkin ulusal mevzuatta düzenlenmesi gerekebilecek birçok konuyla ilgili gerekli belirlemeler yapılmamıştır. Örneğin, taleplerin şekli ve içeriği, tanık ifadelerinin talebi yapan devlet tarafından mı muhatap devlet tarafından mı alınacağı, resmi ya da ticari kayıtların sağlanması, tanıkların gözetim altında nakledilmesi ya da müsadereye ilişkin adli yardımlaşma konularının ele alındığı hiçbir hüküm yoktur[501]. Bu konular ulusal mevzuatlar ve tarafların istişareleri çerçevesinde halledilmek durumundadır.

---

[498] Örnekler için bkz. Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1253.
[499] "International Cooperation under the Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 18 Ağustos 2009, s. 5.
[500] Calderoni, "The European legal framework on cybercrime", s. 348.
[501] Açıklayıcı Rapor, par. 264.

27. maddenin 2. fıkrasında, yardım taleplerini göndermek ve cevaplamakla sorumlu yetkili merkezi makam ya da makamların belirlenmesi gereği vurgulanmış ve şart koşulmuştur. Yetkili merkezi makamların kurulması cezai konularda yardımlaşmayla ilgili modern metinlerin ortak bir özelliğidir ve siber suçlarla mücadelede olmazsa olmaz olan hızlı hareket etme noktasında çok yardımcı olan bir uygulamadır[502]. Bu tür yetkili makamlar arasında doğrudan iletişim, diplomatik kanallardan gerçekleştirilen iletişimlere göre daha hızlı ve daha etkilidir. Ayrıca, aktif bir merkezi yetkili makam, hem gelen hem de giden taleplerin titizlikle takip edilmesi, yabancı makamlara ilgili devletin mevzuatı uyarınca gerekli şartların nasıl en iyi şekilde yerine getirileceği konusunda tavsiye verilmesi ve özellikle acil ya da hassas taleplerin uygun şekilde ele alınmasını sağlamakla önemli bir işlevi yerine getirecektir[503].

Etkin bir uygulama tesis edilebilmesi amacıyla adli yardımlaşma konularında tek bir merkezi yetkili makam belirlenmesi tavsiye edilmektedir. Bir devletin taraf olduğu yardımlaşma antlaşmaları veya ulusal mevzuatı çerçevesinde adli yardımlaşma işlerinde yetkilendirilmiş mevcut merkezi makamın, bu madde kapsamında yürütülecek adli yardımlaşmalarda da merkezi yetkili makam olarak belirlenmesi en etkin yol olacaktır. Ancak, taraf devletlere yardımlaşma sistemleri çerçevesinde uygun olduğu durumlarda birden fazla merkezi yetkili makam belirleme imkanı tanınmıştır[504]. Bütün taraf devletler bu madde çerçevesinde yardımlaşma taleplerini almak ve cevaplamakla görevlendirilmiş yetkili makam ya da makamların isim ve adreslerini (e-posta ve faks numaraları dahil olmak üzere) Avrupa Konseyi Genel Sekreterliği'ne bildirmek ve güncellemek zorundadır[505].

Yardımlaşma talebinde bulunan bir devlet için çoğu zaman temel hedeflerden birisi; elde edilecek delillerin hukuka uygunluğunun sağlanması ve kabul edilebilirliğinin sağlanması ve sonuç olarak delilin mahkemede kullanılabilmesini sağlanmasıdır. 27. maddenin 3. bendinde bu durum gözetilerek, yardımlaşma yoluyla

---

[502] "The functioning of 24/7 points of contact for cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, Nisan 2009, s. 33.

[503] Açıklayıcı Rapor, par. 265.

[504] Pek çok taraf devlet farklı makamları yetkilendirmeyi tercih etmektedir. Örneğin Türkiye bakımından durum bu şekildedir. Adli yardımlaşma konularında genel yetkili makam Adalet Bakanlığı Uluslararası Hukuk ve Dış İşleri Genel Müdürlüğü iken, 27. madde kapsamında yetkili makam olarak Emniyet Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı belirlenmiştir.

[505] Bu bilgiler Avrupa Konseyi'nin resmi internet sitesinde erişime sunulmaktadır: (erişim: 20.08.2015), http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)17_Assess_report_v50adopted.pdf.

elde edilen delillerin kabul edilebilirlik koşularını sağlaması amacıyla muhatap devletin mevzuatına aykırı olmadıkça, talebin, talebi yapan devletin belirlediği usullere uygun olarak uygulanması şartı getirilmiştir. Açıklayıcı Rapor'da bu hükmün sadece teknik koşullarla ilgili olduğu, ceza muhakemesi tedbirlerin uygulanmasına ilişkin temel koşullarla ilgili olmadığı özellikle vurgulanmaktadır[506]. Yardım isteyen devletin uyulmasını istediği özel koşulların muhatap devlette mevcut olmayan koşullar olması ret sebebi oluşturmayacaktır, yalnızca söz konusu istemin muhatap devlette yasak bir usul olması halinde bu talep reddedilebilecektir. Örneğin, yardım talep eden devletin mevzuatı çerçevesinde bir tanığın ifadesinin yeminli olarak alınması bir usul şartı olabilir. Muhatap devlet, kendi ulusal yasalarında ifadelerin yeminli olarak alınması şartı olmasa da talebi yapan devletin bu yöndeki talebine uymalıdır[507].

27. maddenin 4. fıkrasında bu madde uyarınca yapılacak adli yardımlaşma taleplerine yönelik ret nedenleri düzenlenmektedir. Yardım talebi, muhatap devletin ulusal mevzuatında belirlenen devletin egemenliğine, güvenliğe, kamu düzenine ya da diğer temel çıkarlara zarar gelmesini de içeren gerekçelerle ve suçun siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olarak değerlendirildiği durumlarda reddedilebilir. Ret gerekçeleri adli işbirliğinin ve özel olarak adli yardımlaşmanın "en geniş şekilde" uygulanacağı yönündeki 23 ve 25. maddelerle uyumlu olarak dar tutulmalı ve ölçülü bir şekilde kullanılmalıdır[508].

27. maddenin 5. bendinde, bir yardımlaşma talebinde yer alan işlemlerin derhal yapılmasının devlette yürütülmekte olan soruşturma veya kovuşturmalar bakımından zararlı olacağı durumlarda, muhatap devletin talebin yerine getirilmesini ertelemesine izin verilmektedir. Yalnız burada izin verilen reddetme değil, ertelemedir. Örneğin, yardım isteyen devletin soruşturma ya da duruşmada kullanılmak amacıyla delil ya da tanık ifadesi alınmasını talep ettiği ve aynı delil ya da tanığın muhatap devlette mevcut ya da başlamak üzere olan bir soruşturma ya da kovuşturma bakımından gerekli olduğu durumlarda erteleme mümkün olacaktır[509].

Ret ve erteleme gerektiren durumlarda adli yardımlaşma mekanizmasının bütün bütün kilitlenmesini önlemek amacıyla, bu hallerde muhatap devletin bazı özel şartlarla talebi yerine getirmeyi önermesi imkanı öngörülmüştür. Bu halde şartlar

[506] Açıklayıcı Rapor, par. 267.
[507] Açıklayıcı Rapor, par. 267.
[508] Açıklayıcı Rapor, par. 268.
[509] Açıklayıcı Rapor, par. 269.

yardım isteyen devlet için uygun değilse, muhatap bunlarda değişiklik yapabilir ya da yardımı reddetme ya da erteleme hakkını kullanabilir. Muhatap devlet "mümkün olan en geniş" yardımı sağlamakla yükümlü olduğu için hem ret hem de şart ileri sürme haklarının ölçülü bir biçimde kullanılması gerekir[510].

Yardımlaşma talebi sonucunda her halükarda yardım isteyen devlete sonucun bildirilmesi zorunludur. 27. maddenin 7. bendiyle getirilen bu zorunluluk uyarınca talebin olumlu karşılanması halinde sonucu bildirme ve yardımı reddetme ya da erteleme durumunda bunun nedenlerini açıklama yükümlülüğü getirilmektedir. Ret ya da erteleme gerekçelerinin açıklanması, başka şeylerin yanı sıra, yardım isteyen devletin yardım konusu işlem konusunda muhatap devletin hangi şartları nasıl yorumladığını anlamsına yardımcı olabilir ve gelecekte yardımlaşmanın etkinliğini artırmak için bir istişare temeli oluşturabilir[511].

Acil durumlarda 27. maddenin yukarıda açıkladığımız diğer bentlerinde düzenlenen adli yardımlaşma rejimi yetersiz kalabilecektir. Bu nedenle 27. maddenin 9. bendinde acil durumlara yönelik bazı özel istisna halleri düzenlenmiştir.2. bent uyarınca kural olarak taraflar belirlenen merkezi yetkili makamlar aracılığıyla iletişim kuracaktır. Ancak, acil durumlarda, adli yardımlaşma talepleri yardım isteyen devletin hakim ve savcıları tarafından doğrudan doğruya muhatap devletin hakim ve savcılarına yöneltilebilir. Bu usulü izleyen hakim ya da savcı, muhatap devletin merkezi yetkili makamına iletilmesi amacıyla talebin bir kopyasını kendi merkezi yetkili makamına göndermelidir. Fıkranın (b) bendi uyarınca bu taleplerin INTERPOL aracılığıyla iletilmesi de mümkündür. Ayrıca fıkranın (c) bendi uyarınca kendi yetki sınırlarının dışına çıkan bir talep alan makamlar acil durumlara özel olarak ikili bir yükümlülük altındadır. İlk olarak, talebi doğru muhatap makama iletmek zorundadır. İkinci olarak, yardım isteyen devletin yetkili makamlarını bu durum konusunda bilgilendirmek zorundadır. Fıkranın (d) bendi uyarınca, muhatap devletin ilgili makamları, yardım isteyen makama, doğrudan talebin sonucunu da iletebilecektir. Son olarak (e) bendi, devletlerin acil durumlarda taleplerin daha etkin şekilde gerçekleştirilebilmesi amacıyla Avrupa Konseyi Genel Sekreterliği aracılığıyla, doğrudan iletişimlerin yalnızca merkezi yetkili makama iletilmesi gerektiğini diğer taraf devletlere bildirmesine izin vermektedir[512].

---

[510] Açıklayıcı Rapor, par. 270.
[511] Açıklayıcı Rapor, par. 271.
[512] Açıklayıcı Rapor, par. 274.

Sözleşme'nin *"Gizlilik ve Kullanımın Sınırlandırılması"* başlıklı 27. maddesinde muhatap devletin yardımlaşma talebine konu bilgi ya da malzemelerin özellikle hassas olduğu durumlarda, bunların kullanımlarının yardım talebin dayanak oluşturan soruşturma ile sınırlı tutulmasını ya da talepte bulunan adli makamlar dışında kimseye açıklanmamasını sağlayabilmesi amacıyla bilgi ve materyallerin kullanımıyla ilgili sınırlamalar getirilmiştir. Bu sınırlamalar yalnızca uluslararası adli yardımlaşma antlaşmalarının yürürlükte olmadığı hallerde uygulanmak üzere öngörülmüştür.

Bu kapsamda bir devletin bir yardımlaşma talebine cevap verirken iki tür şart ileri sürebilmesine izin verilmektedir. Birincisi, böyle bir şartın yerine getirilmemesi halinde talebe uyulmasının mümkün olmadığı durumlarda (muhatap devletin gizli bir bilgi kaynağının kimliğinin ifşa olacak olması gibi), sağlanan bilgi ve malzemelerin gizli tutulması talep edilebilir. İkincisi, bilgi ve malzemelerin sağlanması, talepte belirtilenler dışındaki soruşturma ya da kovuşturmalarda kullanılmaması şartına bağlanabilir. Bu şartın geçerli olabilmesi için, yardım isteyen devletin bilgi ve malzemeleri başka şekilde kullanmasına hiçbir şekilde müsaade edilmediğinin açıkça belirtilmesi gerekmektedir[513].

Maddenin 3. fıkrası uyarınca, yardım isteyen devletin, gizlilik veya kullanım sınırlandırması şartlarına ulusal mevzuatı ya da fiili durumlar nedeniyle uyamayacaksa, bu durumu muhatap devlete bildirmesi ve muhatap devletin söz konusu bilgiyi sağlamama seçeneğine sahip olması söz konusu olacaktır. 4. fıkrada da şartlı olarak yardım sağlanan durumlarda, yardım sağlayan devletin şartlara uyulduğunu kontrol etmek amacıyla verilen bilgi ve malzemelerin kullanım şekline ilişkin izah isteyebileceği belirtilmektedir.

4. Özel Adli Yardımlaşma Hükümleri

Bu kısımda düzenlenen özel adli yardımlaşma usulleri, sözleşmenin usul hukukuna ilişkin ulusal düzeyde alınmasını öngördüğü tedbirlerin adli yardımlaşma hukukundaki yansımalarıdır. Bu yolla bu tedbirlerin adli yardımlaşmaya konu olabilmesinin garanti edilmesi amaçlamaktadır. Bu amaçla geçici önlemlerin

[513] Açıklayıcı Rapor, par. 278.

alınmasına ilişkin ve soruşturma yetkilerine ilişkin özel adli yardımlaşma hükümleri getirilmiştir. Bunlardan geçici önlemlerin alınması konusundaki yardımlaşmalar münhasıran Sözleşme çerçevesinde gerçekleştirilecektir. Yani bu konulardaki yardımlaşma talepleri ilgili devletler arasında başkaca uygulanabilir adli yardımlaşma mevzuatı mevcut olsa dahi Sözleşme'de öngörülen usuller ile gerçekleştirilecektir. Soruşturma yetkilerine ilişkin yardımlaşmalar ise Sözleşme'nin genel ilkesel tutumuna paralel olarak; öncelikle uygulanabilir mevcut adli yardımlaşma rejimine, boşluk olması halinde Sözleşme'ye tabi olacaktır. Pratik bir anlatımla iki taraf devlet arasında verilerin süratli şekilde korunması gibi geçici önlemlerinin alınması Sözleşme çerçevesinde; daha sonra gerçekleşecek, depolanmış veriler hakkında arama el koyma tedbiri uygulanması gibi soruşturma yetkilerine ilişkin adli yardımlaşmalar ise mevcut adli yardımlaşma rejimi çerçevesinde gerçekleştirilecektir.

a) Geçici Önlemlerin Alınması Konusunda Yardımlaşma

Depolanmış verilerin süratli şekilde korunması ve trafik verilerinin süratli şekilde açıklanması konularında adli yardımlaşmalar, Sözleşme tarafından "geçici önlemler" olarak adlandırılmakta ve klasik soruşturma işlemlerinden ayrı tutulmaktadır. Bu önlemlere ilişkin adli yardımlaşma talepleri ve bu taleplerin yerine getirilmesi, taraflar arasındaki mevcut yardımlaşma rejimine göre değil, Sözleşme'ye göre yapılacaktır. Örneğin, bu konudaki talepler, mevcut adli yardımlaşma sistemi uyarınca taleplerin iletilme şekli ve iletilecekleri makam ne şekilde belirlenmiş olursa olsun, Sözleşme uyarınca belirlenmiş 7/24 iletişim noktasına, e-posta, fax vb hızlı iletişim araçlarıyla iletilecektir.

Siber suçlara ilişkin ve elektronik ortamda delil toplanmasını gerektiren soruşturmalarda hızlı hareket etme zorunluluğundan ve bunun karşısında masumiyet karinesi başta olmak üzere diğer hukuki güvencelerden kaynaklı zorlukları aşmak için Sözleşme'nin temel çözüm olarak benimsediği formül geçici koruma tedbirlerine başvurulmasıdır. Bu önlemler Sözleşme'nin siber suç soruşturmalarında yaşanan sorunların çözümünüzde kurmak istediği sistemin en önemli parçalarıdır ve hatta temelini oluşturmaktadır denilebilir. Bu nedenle Sözleşme bu önlemleri ayrı tutmakta ve bunların uygulanmasında klasik adli yardımlaşma rejiminin değil, her halükarda

bizzat Sözleşme'nin uygulanmasını öngörmektedir. Şüphesiz geçici önlemlerin hak ve özgürlüklere ciddi bir müdahale içermemesi ve ilgili verilerin, talepte bulunan devlete ancak sonradan gerçekleşecek soruşturma yetkilerine ilişkin yardımlaşma aracılığıyla verilecek olması da bu durumu mümkün kılan sebepler arasındadır.

(1) Depolanan Verilerin Süratli Şekilde Korunması

Sözleşme'nin 29. maddesinde, 16. maddede getirilen ulusal düzeydeki depolanmış verilerin süratli şekilde korunması tedbirinin uluslararası düzeydeki eşdeğeri düzenlenmektedir. Maddede, diğer bir taraf devletin sınırları içerisinde yer alan bir bilişim sisteminde depolanmış halde bulunan veriler hakkında arama el koyma veya benzer şekillerde verilere erişim sağlama konusunda adli yardım talebinde bulunmak isteyen taraf devletlerin, ilgili devletten verilerin süratli şekilde korunmasını isteyebilmesi düzenlenmektedir. Taraf devletler iç hukuklarını da bu yönde talepleri yerine getirmeye elverişli hale getirmelidir. Koruma, geleneksel bir yardımlaşmanın uygulamasından çok daha hızlı gerçekleştirilmesi düşünülen sınırlı ve geçici bir önlemdir. Daha önce de belirttiğimiz gibi bilişim verileri son derece hassas ve geçici niteliktedir. Birkaç tuşa basılarak ya da otomatik programların çalışması sonucunda veriler silinebilir, değiştirilebilir ya da taşınabilir ve böylece bir suçun delilleri yok edilebilir. Bazı bilişim verileri sadece kısa süreler için saklanıp sonra silinirler. Haftalar ya da aylar sürebilecek resmi bir yardımlaşma talebinin uygulanması sürecinde ilgili verilerin kaybolmasını önleyecek bir mekanizmaya ihtiyaç duyulmuştur[514].

Depolanmış verilerin süratli şekilde korunması önlemi, olağan yardımlaşma uygulamasından çok daha hızlı olmasının yanı sıra, aynı zamanda daha az müdahale içermektedir. Muhatap devletin ilgili makamlarının, verilere bizzat müdahale etmeleri gerekli değildir. Genellikle bir servis sağlayıcı bazen de başka bir üçüncü gerçek ya da tüzel kişi olan verileri elinde bulunduran kişinin ileriki bir aşamada verilerin soruşturma makamlarına teslim edilmesini sağlayacak sürecin gerçekleştirilmesi süresince verileri koruması yani silmemesi yeterlidir. Dolayısıyla bu usulün avantajı hem gerekli önlemlerin hızlı bir şekilde alınmasını mümkün

[514] Açıklayıcı Rapor, par. 282.

kılması hem de kişisel hak ve özgürlükler anlamında daha koruyucu nitelikte olmasıdır[515].

29. maddenin 2. fıkrasında depolanmış verilerin korunması konusunda yardımlaşma taleplerinin nasıl yapılacağı ve içeriği düzenlenmiştir. Öncelikle verilerin korunması geçici bir önlem olduğu ve talebin hızlı bir biçimde hazırlanıp iletilmesi gerektiği göz önünde bulundurularak, bilgiler özet şeklinde sunulmalı ve sadece verilerin korunmasını sağlamak için gerekli asgari bilgiyi içermelidir[516]. Talepte; korumayı isteyen makam, hakkında soruşturma ya da kovuşturma yürütülen suçun ne olduğu ve suça ilişkin özet bilgi, korunacak verilerin neler olduğu ve bunların suçla ilgisi, korunacak verileri elinde bulunduran kişinin kim olduğu ya da ilgili bilişim sisteminin yerini belirleyen herhangi bir bilgi ve korumanın gerekliliğine ilişkin açıklamalar yer almalıdır. Ayrıca ilgili verilerin daha sonra soruşturma yetkileri konusunda bir adli yardımlaşma talebine konu edileceği belirtilmelidir.

Depolanmış verilerin süratli şekilde korunması hızlı bir şekilde işlemesi gereken ve müdahale niteliği az olan bir tedbir olması itibariyle bu tedbire ilişkin ret sebepleri konusunda özel bir istisna öngörülmüştür. 29.maddenin 3. fıkrası karşılıklı cezalandırılabilirlik şartının verilerin korunması taleplerinin gerçekleştirilmesi bakımından bir şart olarak ileri sürülemeyeceğini ortaya koymaktadır. Bu istisnanın getirilmesinin en önemli nedeni karşılıklı cezalandırılabilirlik koşulunun tespit edilmesinin ciddi bir inceleme, dolayısıyla zaman gerektirmesine mukabil, depolanmış verilerin korunmasının mümkün olan en kısa süre içerisinde gerçekleştirilmesi gerekliliğidir. Örneğin, bir soruşturmanın ilk aşamalarında, verilerin korunması talebinde bulunan devlet, sınırları içinde bir bilişim sistemine izinsiz girildiğinin farkında olabilir ama fiilin niteliği ve boyutlarını tam olarak anlaması zaman alabilir. Muhatap devlet, karşılıklı cezalandırılabilirliğin kesin olarak belirlenmesi sürecinde izinsiz girişin kaynağının bulunabilmesini sağlayacak trafik verilerini korumayı geciktirirse, kritik önemdeki veriler, bu verileri sadece birkaç saat ya da gün tutan servis sağlayıcılar tarafından rutin bir işlem olarak silinecektir. Karşılıklı cezalandırılabilirlik koşulunun sağlandığı daha sonra anlaşılsa

[515] Açıklayıcı Rapor, par. 283.
[516] Açıklayıcı Rapor, par. 283.

bile, önemli trafik verileri kaybedilmiş olacak suçun failleri hiçbir zaman tespit edilemeyebilecektir[517].

Verilerin süratli şekilde korunmasına ilişkin yardımlaşma taleplerinde genel kural karşılıklı cezalandırılabilirlik koşulunun aranmaması olmakla birlikte, maddenin 4. fıkrasında hakkın sınırlı bir biçimde saklı tutulması imkanı tanınmıştır. Sözleşmede düzenlenenler dışındaki suçlarla ilgili olarak yapılan verilerin korunması talepleri söz konusu olduğunda, koruma talebini takip edecek arama el koyma, üretim emri vb. şeklindeki soruşturma yetkilerine ilişkin yardımlaşma talepleri açısından karşılıklı cezalandırılabilirlik şartını ayan bir devletin, ileride bu şartların sağlanamayacağına inanmak için gerekçelere sahip olması durumunda, verilerin korunması talebini reddetmesi mümkündür. Daha açık bir anlatımla Sözleşme'nin 2.-10. maddeleri arasında düzenlenen suçlar dışında bir suç söz konusu olduğunda, soruşturma yetkililerine ilişkin yardımlaşma taleplerinde karşılıklı cezalandırılabilirlik koşulunu arayan devletler, ileride bu koşulun sağlanamayacak olmasını verilerin süratli şekilde korunması talebi için de ret sebebi yapabileceklerdir. Böylelikle, karşılıklı cezalandırılabilirlik şartı konusundaki istisna pratikte yalnızca Sözleşme'nin 2- 10. maddelerinde düzenlenen suçlar bakımından getirilmiş olmaktadır. Taraf devletlerin bu suçları ulusal mevzuatlarında suç olarak tanımladıkları varsayımıyla, bu suçlar konusundan karşılıklı cezalandırılabilirlik zaten hiçbir zaman sorun teşkil etmeyecektir[518].

29.maddenin 4. fıkrasında yer alan karşılıklı cezalandırılabilirlik şartının ret sebebi yapılamayacağı şeklindeki düzenlemenin dışında, maddenin 5. fıkrasında nelerin ret sebebi yapılabileceği sınırlı olarak sayılmıştır. Buna göre verilerin süratli şekilde korunması talebinin muhatabı olan devlet bu talebi yalnızca, yardım talebine konu olan suçun siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olarak değerlendirilmesi veya söz konusu talebin yerine getirilmesinin egemenliğine, ulusal güvenliğine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğini düşünmesi halinde reddedebilir.

Muhatap devlet bakımından ortaya çıkması muhtemel sakıncaların yanı sıra bazı özel durumlarda talepte bulunan devlet bakımından da sakıncalar belirebilir. Örneğin, korunacak verileri tutan servis sağlayıcı ya da diğer üçüncü kişilerin bir suç

---

[517] Açıklayıcı Rapor, par. 284.

[518] Hüseyin Çeken, "Council of Europe's Convention on Cybercrime and Turkey", Marmara Üniversitesi Avrupa Topluluğu Ensitüsü, Yüksek Lisans Tezi, s. 120.

örgütü ya da bizzat şüpheli ya da sanıklar tarafından kontrol edildiği durumlarda muhatap devlet, verileri koruyacak kişinin talepte bulunan devlette yürütülen soruşturmasının gizliliğini tehdit edecek ya da başka bir biçimde bu soruşturmaya zarar verecek bir eylemde bulunabileceğini fark edebilir[519]. Maddenin 6. fıkrası bu gibi durumlarda talepte bulunan devletin, tedbirin uygulanmasından doğacak riski almak ya da üretim, arama el koyma gibi daha müdahaleci ama daha güvenli bir tedbir konusunda yardımlaşma talep etmek seçeneklerini değerlendirebilmesi için derhal bilgilendirilmesi gerektiğini belirtmektedir.

Bu madde uyarınca koruma talebine konu olan veriler, talepte bulunan devletçe soruşturma yetkileri konusunda yardımlaşma talebinde bulunulabilmesini sağlamak üzere en az altmış gün korunmak zorundadır. Ayrıca soruşturma yetkileri konusunda yardımlaşma talebi geldikten sonra, bu talep hakkında karar verilinceye kadar da ilgili veriler korunmaya devam edilmelidir. Koruma süresinin, soruşturma yetkileri konusunda yapılan yardımlaşma talebinin değerlendirilmesi süresince uzayacağı hükmü, Sözleşme'nin klasik yardımlaşma süreçlerinin hantallığı konusunda duyduğu endişenin ve bu hantallıktan kaynaklı aksaklıkları çözme noktasındaki iradenin en somut göstergelerinden birisidir

(2) Depolanan Trafik Verilerinin Süratli Şekilde Açıklanması

Sözleşme'nin 30. maddesinde, 17. maddede yer verilen ulusal düzeydeki trafik verilerinin süratli şekilde korunması ve kısmen açıklanması tedbirinin uluslararası düzeydeki eşdeğeri düzenlenmektedir. 29. madde kapsamında verilerin süratli şekilde korunması talebine konu edilen trafik verilerini koruma altına alan muhatap devlet, kendi ulusal sınırları içinde bulunan trafik verilerinden, talepte bulunan devlette ya da üçüncü bir devlette bulunan başka servis sağlayıcıların da iletişime dahil olduğunu tespit edebilir[520]. Bu tür durumlarda muhatap devlet, diğer devletteki servis sağlayıcının kimliğini ve genel olarak iletişimin izlediği yolu belirlemeye yetecek miktarda trafik verisini hızlı bir biçimde açıklamak zorundadır. Bu sayede talepte bulunan devletin, daha önce var olduklarını tespit edemediği delilleri, gerek

[519] Açıklayıcı Rapor, par. 286.
[520] Açıklayıcı Rapor, par. 290.

adli yardımlaşma yoluyla üçüncü devletlerin sınırları içinde gerek ulusal düzeydeki önlemlerle kendi sınırları içerisinde ortaya çıkarması mümkün kılınmış olacaktır.

Bu tür bilgilerin siber suç soruşturmaları bakımından çok önemli olmasından dolayı, 29. maddede olduğu gibi 30. madde bakımından da ret nedenleri sıkı bir biçimde sınırlandırılmış ve iki hal dışında yardım talebinin reddedilmesine izin verilmemiştir.30. maddenin 2. fıkrası uyarınca, muhatap devlet, trafik verilerini ifşa etmeyi ancak; ifşa eyleminin egemenliğine, ulusal güvenliğine, kamu düzenine ya da diğer temel çıkarlarına zarar verici olduğu veya suçun siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olduğunu düşündüğü durumlarda reddedebilir.

Uygulamada, geçici önlemlerin alınması konusunda adli yardımlaşmanın oldukça az sayıda devlet tarafından başvurulan, istisnai bir yöntem olduğu görülmektedir[521]. Verilerin süratli şekilde korunmasına yönelik tedbirlere ulusal düzeyde doğru ve etkin şekilde yer verilmemesinin doğal bir sonucu olarak bu konularda adli yardımlaşma sağlanması da mümkün olmamaktadır. Verilerin süratli şekilde koruması konusunda muhakeme tedbirlerinin tesis edilmemiş olmasına paralel olarak çok az sayıda taraf devlet geçici önlemlerin alınması konusunda uluslararası adli yardımlaşmaya yönelik özel düzenlemeler getirmiştir[522]. Sözleşme'nin bu konudaki hükümleri doğrudan uygulanabilir nitelikte olmakla ve bu konularda adli yardımlaşma sağlanması için gerekli hukuki zemini sunmakla birlikte, ulusal mevzuatlarda konunun ele alınmaması devletlerin bu konudaki isteksizliklerini ortaya koymaktadır. Nitekim Sözleşme'nin ilk on yılında birkaç istisnai örnek dışında geçici önlemlerin alınması konusunda adli yardımlaşmanın uygulanmadığı görülmektedir[523].

Ulusal düzeyde verilerin süratli şekilde korunmasını mümkün kılacak yasal önlemlerin alınmamış olması, adli yardımlaşmaya ilişkin prosedürlerin net bir şekilde tanımlanmamış olması ve uygulama makamlarının alışık olmadığı bir yöntem olması itibariyle geçici önlemlerin alınması konusunda uluslararası adli yardımlaşma uygulaması oldukça sınırlı olmakla birlikte[524], polisiye işbirliği konusunda bu

[521] "Implementation of the preservation provisions of the Budapest Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 5 Kasım 2013, s. 13.
[522] 2015 yılı itibariyle yalnızca Portekiz, Romanya ve Moldova geçici önlemlerin alınması konusunda adli yardımlaşmaya yönelik özel düzenlemeler yapmıştır.
[523] "Implementation of the preservation provisions of the Budapest Convention on Cybercrime", s. 13.
[524] "Implementation of the preservation provisions of the Budapest Convention on Cybercrime", s. 17.

tedbirlere benzer yardımlaşma pratiğinin oldukça yaygın olduğu görülmektedir[525]. Özellikle polisin trafik verilerine erişmek için özel bir tedbire başvurmaya ihtiyaç duymadığı, doğrudan doğruya servis sağlayıcılardan ya da başka bir kanalla verileri elde edebildiği devletlerde polisiye işbirliği anlamında geçici önlemlerin alınması konusunda yardımlaşma oldukça sık başvurulan ve etkin bir uygulamadır[526].

b) Soruşturma Yetkileri Konusunda Adli Yardımlaşma

Sözleşmenin bu kısımda düzenlediği depolanmış veriler hakkında arama el koyma, depolanmış verilere sınır ötesi erişim, bilişim verilerinin gerçek zamanlı olarak toplanması konularına ilişkin adli yardımlaşma hükümleri soruşturma yetkilerine ilişkin olup, bunlar taraf devletlerin mevcut adli yardımlaşma sitemleri çerçevesinde gerçekleştirilecektir. Ancak, taraflar arasındaki mevcut sistem bu konularda adli yardımlaşmanın sağlanmasına olanak tanımıyorsa Sözleşme hükümleri devreye girecek ve söz konusu yardımlaşmalar için hukuki zemin sunulmuş olacaktır. Yani Sözleşme, soruşturma yetkilerine ilişkin yardımlaşma konusunda yedek normlar getirerek bu konularda adli yardımlaşmanın her halde mümkün olmasını amaçlamaktadır.

(1) Depolanmış Veriler Hakkında Arama El Koyma

Sözleşme'nin 31. maddesinde, 19. maddede ulusal düzeyde alınması öngörülen depolanmış veriler hakkında arama ve el koyma tedbirinin uluslararası adli yardımlaşma hukukundaki karşılığı düzenlenmiştir. Buna göre taraf devletler, ulusal düzeydeki amaçlar için olduğu gibi, başka bir taraf devletin talebi üzerine kendi ulusal sınırları içindeki bir bilişim sistemi aracılığıyla saklanan, trafik verileri de dahil olmak üzere, verileri arama ya da bunlara benzer şekilde erişme, el koyma ya

[525] Taraf devletlerin Sözleşme'de öngörülen geçici önlemlerin alınması konusunda adli yardımlaşma hükümleri yerine, bu konularda polisiye işbirliğine başvurmaları konusunda ayrıntılı bilgi için bkz. "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3 Kasım 2014, s. 21-33.

[526] "Implementation of the preservation provisions of the Budapest Convention on Cybercrime", s. 33.

da bunları benzer şekilde güven altına alma ve ifşa etme yeterliliğine sahip olmalıdır[527].

31. maddenin 3. fıkrasında, ilgili verilerin kaybolma ya da değiştirilmeye açık olduğuna inanmak için gerekçelerin mevcut olması ya da taraflar arasındaki mevcut adli yardımlaşma siteminin gerektirmesi durumlarında depolanmış veriler hakkında arama el koyma taleplerine hızlı bir şekilde cevap verileceği öngörülmüştür. Sözleşme'nin bu hükmü esasında yaptırımı olmayan bir temenni ve hatırlatma niteliğindedir. Zira tarafların hangi hallerde bu talepleri hızlı şekilde cevaplamaları gerektiği, bu konuda bir süre sınırı olup olmadığı konularında ne Sözleşme ne de açıklayıcı rapor yol göstermektedir. Diğer yandan mevcut adli yardımlaşma sisteminin hızlı hareket edilmesini gerektirdiği durumlarda taraflar zaten ilgili hukuki metinler uyarınca hızlı hareket etme sorumluluğu altında olacaktır.

Taraf devletlerce ulusal düzeyde en sık başvurulan tedbir olan depolanmış veriler hakkında arama el koyma tedbiri, buna paralel olarak adli yardımlaşma taleplerine de en sık konu olan tedbir türüdür[528]. Özellikle trafik verileri, sıklıkla yardımlaşma taleplerine konu olmaktadır. Ancak, ulusal düzeyde trafik verilerini herhangi bir özel muhakeme tedbirine başvurmadan elde etme yetkisine sahip olan soruşturma makamları, yabancı devletlerden gelen talepleri de aynı şekilde karşılamakta, talep edilen veriyi özel bir tedbire başvurmaksızın vermektedir[529].

(2) Depolanmış Verilere Sınır Ötesi Erişim

Depolanmış verilere sınır ötesi erişim, taraf devletlerin, sınır ötesindeki verilere, ilgili devletin makamlarına hiçbir şekilde başvuru ya da bilgi verme söz konusu olmaksızın doğrudan doğruya erişim sağlayabilmelerini ifade etmektedir. Sözleşme'nin 32. maddesinde iki durumda depolanmış verilere uzaktan sınır ötesi erişimin mümkün olduğu düzenlenmiştir. İlk olarak, erişilen verilerin kamuya açık olduğu, yani herhangi bir kullanıcının özel bir izin ya da yetkiye ihtiyaç olmaksızın erişebileceği verilere sınır ötesinden erişim sağlanabilir. Siber alemde verilerin fiziksel olarak depolanmış oldukları yerden bağımsız olarak farklı coğrafyalardan

[527] Açıklayıcı Rapor, par. 292.
[528] "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 5.
[529] "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 12.

erişilebilir olması karşısında, herkesçe girilebilen internet siteleri veya özel bir yetki gerekmeksizin herkesin ilgili verilere erişim sağlayabileceği veri paylaşım programları aracılığıyla sınır ötesindeki verilere erişilmesi cebir içermeyen ve hak ve özgürlüklere müdahale içermeyen bir delil elde etme yöntemi olması itibariyle, bu konuda sınır ötesi erişimin mümkün olması öngörülmüştür. Zaten kamuya açık olan bu verilerin yabancı bir devletin soruşturma makamlarının erişiminim yasaklanması fiilen mümkün değildir ve Sözleşme bu hükümle aslında yalnızca, bu şekilde elde edilen verilerin, verilerin bulunduğu devletin egemenlik haklarının ihlali olmadığını tespit etmektedir.

Sınır ötesi uzaktan erişime izin verilen ikinci durum, bir devletin verilere erişim ve ifşa etme hakkına sahip olan kişinin yasal ve gönüllü onayını alarak kendi sınırları içerisindeki bir bilişim sistemi aracılığıyla sınır ötesi verilere erişim sağlaması halidir. Verileri ifşa etmek için "yasalar uyarınca yetkili" kişinin kim olduğu, koşullara, kişinin niteliğine ve somut olaya uygulanacak yasal hükümlere bağlı olarak farklılık gösterebilir. Sözleşme ve Açıklayıcı Rapor yetkili kişinin neye göre belirleneceği ve bu kişinin rızasının hangi hallerde yasal ve gönüllü olarak alınmış sayılacağı konularında yol göstermemektedir. Örneğin, A devletindeki bir kişinin, üçüncü kişilerle yazışmalarına ilişkin, e-posta hizmetinden faydalandığı B devletindeki bir servis sağlayıcının veri hangarlarında depolanmış veriler hakkında kim ya da kimler yetki sahibi kabul edilecektir? E-posta adresi sahibi kişi, üçüncü kişilerle yazışmalarını ifşa etme yetkisine sahip midir? Ya da e-posta hizmeti sunan servis sağlayıcı, muhatap olduğu bir üretim talimatı karşısında zaten elinde bulunan bu verileri ifşa etme konusuna yetkili sayılacak mıdır? Bu son ihtimalde üretim talimatı üzerine verileri ifşa eden kişinin rızasının yasal olduğu tartışmasızdır, ancak bu şekilde verilen rıza gönüllü müdür? Sözleşme bu sorulara cevap verecek hükümler getirmemektedir.

Sözleşme'nin 32. maddesinin sınır ötesi erişim konusunda taraf devletlere herhangi bir yükümlülük getirmediği, yalnızca sınır ötesi erişim sağlanması halinde taraf devletler arasında çıkması muhtemel uyuşmazlıkları gidermek adına sayılan hallerde sınır ötesi erişimin meşru görülmesini öngördüğü görülmektedir[530]. Diğer bir anlatımla, ulusal mevzuatı uyarınca, ulusal soruşturma makamlarının sınır ötesi erişimle delil elde etme yetkisine sahip olduğu devletler bu eylemlerinden dolayı, verilerin bulunduğu devletlere karşı herhangi bir sorumluluk altına girmeyecektir.

[530] Brenner, Law,, s. 91

Bunun yanında, ulusal mevzuatı sınır ötesi erişime imkan tanımayan devletler bu yönde bir düzenlemeye gitme yükümlülüğü altına sokulmamaktadır.

Taraf devletlerin, adli yardımlaşmaya başvurmaksızın başka bir taraf devletin ulusal sınırları içerisinde depolanmış halde bulunan bilişim verilerine erişmelerine izin verilebileceği konusu Sözleşme'nin hazırlanması sürecinde taraflarca ayrıntılı bir biçimde tartışılmıştır[531]. Ülkelerin tek taraflı olarak verilere erişmelerinin kabul edilebilir olduğu ve olmadığı durumlar ayrıntılı bir biçimde ele alınmıştır. Sonuçta Sözleşme'yi kaleme alanlar bu alanı düzenleyen kapsamlı, hukuki açıdan bağlayıcı bir rejim hazırlamanın henüz mümkün olmadığına karar vermişlerdir[532]. Bu durum, bu konuda birçok devletin deneyim sahibi olmamasından ve tüm somut senaryolara uygun çözüm sunacak soyut genel kurallar formüle etmenin güçlüğünden kaynaklanmaktadır.

Sonuç olarak Sözleşme'yi kaleme alanlar, 32. maddede herkesin üzerinde anlaştığı sınırlı durumların belirtilmesiyle yetinilmesine karar vermişlerdir. Bu konuda daha fazla deneyime sahip olunduğu ve bu deneyimler ışığında daha fazla tartışmanın yapıldığı bir zamana kadar diğer durumların düzenlenmemesi kararlaştırılmıştır[533]. Buna rağmen maddenin mevcut hali oldukça fazla eleştiri almaktadır[534]. Birçok devletin, örneğin Konsey üyesi olan Rusya'nın, Sözleşme'yi imzalamaktan kaçınması noktasındaki en önemli çekincesinin 32. madde hükmü olduğu ifade edilmektedir[535].

Siber alemde suç soruşturmalarının alışılmışın ötesinde hızlı hareket etmeyi gerektirmesi ve siber alemde yer alan aktörlerin başta internet olmak üzere bilişim ağlarıyla birbiriyle bağlantı içinde olması karşısında, soruşturma makamları sınır ötesi verilere doğruda erişim sağlayarak delil elde etme eğilimindedirler. Yalnızca kamuya açık veriler hakkında veya erişim yetkisine sahip kişinin rızası alınarak gerçekleştirilen erişimler değil, belirli özel yazılımlar aracılığıyla kamuya açık olmayan verilere cebren erişim de söz konusu olmaktadır. Başta ABD olmak üzere

---

[531] Açıklayıcı Rapor, par. 293.
[532] Açıklayıcı Rapor, par. 293.
[533] Açıklayıcı Rapor, par. 294.
[534] Bu yöndeki eleştirler için bkz. Goldsmith, "Internet and Legitimacy of Remote Cross-Border Searches", s. 117.
[535] Vatis, "The Council of Europe 's Convention on Cybercrimes", s. 218.

bir çok devlette sınır ötesi verilere uzaktan erişim siber alemde yürütülen soruşturmalar bakımından oldukça önemli ve sıklıkla başvurulan bir araçtır[536].

Taraf devletlerin ulusal mevzuatlarının sınır ötesi erişim konusundaki yaklaşımları oldukça çeşitli ve farklıdır; sınır ötesi erişim bazı devletlerde bütünüyle hukuka uygun, bazı devletlerde belirli koşullarda hukuka uygun, bazı devletler de ise bütünüyle hukuka aykırıdır[537]. Türkiye'nin de dahil olduğu önemli bir grup devlette ise konuda mevzuatta açık bir hüküm veya benimsemiş bir içtihat bulunmamaktadır[538]. Bu durumda soruşturmayı yürüten devlet bakımından yasal soruşturma faaliyeti niteliğinde olan bir eylem, verilerin bulunduğu devlet bakımından suç oluşturabilmektedir[539].

Sözleşme mevcut haliyle ulusal hukukların bu konudaki yaklaşım farklılıklarından kaynaklı sorunlara çözüm sunacak kapsamlı bir düzenleme getirmemektedir. Ancak, T- CY komitesi uzaktan sınır ötesi erişim konusunda çalışmalarını sürdürmektedir. Bu kapsamda siber alemde yetki sorunlarını ve sınır ötesi verilere uzaktan erişime ilişkin sorunları incelemek ve çözüm önerileri geliştirmek amacıyla 2011 yılında T- CY bünyesinde Sınır Ötesi Erişim ve Yetki Hakkında Alt Çalışma Grubu kurulmuştur[540]. Alt Çalışma Grubu, çok sayıda toplantı düzenleyerek çalışmalarını 2013 yılında kapsamlı bir rapor şeklinde T-CY Genel Kurulu'na sunmuştur. Söz konusu raporda adli işbirliği mekanizmaların geliştirilmesi yönünde temennilerin yanı sıra, bir ek protokol hazırlanarak uzaktan sınır ötesi erişim konusunun daha ayrıntılı bir şekilde düzenlenmesi ve yaptırım altına alınması önerisine yer verilmiştir. Söz konusu rapor doğrultusunda yürütülen ek protokol çalışmaları, Verilere Sınır Ötesi Erişim Hakkında Avrupa Siber Suçlar Sözleşmesi'ne Ek Protokol Taslağı olarak somutlaşmış ve Taslak, Nisan 2013'te T-CY Genel Kurulu'na sunulmuştur.

Verilere Sınır Ötesi Erişim Hakkında Avrupa Siber Suçlar Sözleşmesi'ne Ek Protokol Taslağı, sorunların çözümüne yönelik uzlaşılmış tek bir çözüm önermemekte, dört farklı seçenek sunmaktadır. Birinci seçenek, sınır ötesindeki

---

[536] Brenner, "Law, Dissonnance and Remote Computer Searches", s. 66.
[537] Brenner, "Law, Dissonnance and Remote Computer Searches", s. 91.
[538] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1259.
[539] Bu konuda Birinci Bölüm'de "Siber Alemde Yetki Sorunları" başlığı altında ayrıntılı olarak incelediğimiz "Invita" olayı önemli bir örnektir.
[540] "Preparation by the T-CY of a draft Additional Protocol to the Convention on Cybercrime (ETS 185) regarding transborder access to data" Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 16 Mayıs 2013, s. 2.

verilere ilgilinin rızası ile erişim sağlanmasının herhangi bir kısıtlama olmaksızın kabul edilmesidir[541]. İkinci seçenek, gönüllü rıza olmasa dahi, yasal olarak elde edilen erişim olanaklarıyla, örneğin hukuka uygun olarak uygulanmış bir arama tedbiri çerçevesinde elde edilen şifre aracılığıyla, gerçekleştirilen sınır ötesi erişimlerin kabul edilebilir olmasıdır[542]. Üçüncü seçenek, sınır ötesi erişimin zorunlu hallerde veya soruşturma yetkililerinin iyi niyetle hareket ettiği hallerde kabule edilebilir olması şeklinde bir istisna öngörülmesidir[543]. Dördüncü seçenek ise, 19. maddenin 3. fıkrası uyarınca ulusal sınırlar içerisinde yer alan bilişim sistemleri hakkında yapılan arama el koymalar bakımından geçerli olan, bir bilişim sistemindeki veriler hakkında icra edilen bir arama el koyma tedbirinin diğer bilişim sistemlerine genişletilmesinin, sınır ötesi veriler hakkında da uygulanmasıdır[544]. Taslak'ta bu seçeneklerden bir ya da birkaçının kabul edilmesi önerilmektedir[545]. Sınır ötesi erişim konusunda Taslak'ta yer alan bu öneriler üzerinde veya başka bir çözüm yolu üzerinde henüz uzlaşma sağlanamamış olup, Alt Çalışma Grubu çalışmalarını sürdürmektedir[546]. Bu çalışmaların 2015 yılı sonunda tamamlanması öngörülmüştür. Bu süre sonunda Ek Protokol hazırlanıp imzaya açılsa dahi Sözleşme'ye taraf devletlerin büyük kısmının Ek Protokol'ü imzalamaktan kaçınacağı düşünülmektedir[547].

(3) Bilişim Verilerinin Gerçek Zamanlı Olarak Toplanması

Ulusal düzeyde alınması öngörülen bilişim verilerinin gerçek zamanlı olarak toplanması tedbirlerinin uluslararası adli yardımlaşama hukukundaki karşılığı olarak

---

[541] "(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Sınır Ötesi Erişim ve Yetki Hakkında Alt Çalışma Grubu Önerisi, 9 Nisan 2013, s. 4

[542] "(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data", s. 5.

[543] "(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data", s.5.

[544] "(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data", s. 6.

[545] "(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data", s. 6.

[546] "Transborder access to data and jurisdiction:Options for further action by the T-CY", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3. Ekim 2014, s. 5.

[547] "Preparation by the T-CY of a draft Additional Protocol to the Convention on Cybercrime (ETS 185) regarding transborder access to data", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 16 Mayıs 2013, s.2.

Sözleşme'nin 33. ve 34. maddelerinde bilişim verilerinin gerçek zamanlı olarak toplanması konusunda adli yardımlaşma hükümleri getirilmiştir.

33. maddede trafik verilerinin gerçek zamanlı olarak toplanması konusunda adli yardımlaşma düzenlenmektedir. Taraf devletler, trafik verilerinin gerçek zamanlı olarak toplanması konusundaki yardım taleplerini yerine getirme yükümlülüğü altına sokulmakla birlikte, taleplerin ne şekilde yerine getirileceği konusunda bir hükme yer verilmemiştir. Yalnızca, devletlerin, uygulanan adli yardımlaşma sistemi ve iç hukukları uyarınca talepleri yerine getirecekleri belirtilmekle yetinilmiştir.

Birçok siber suç olayının soruşturulabilmesi trafik verilerinin tespit edilebilmesine bağlıdır. Bu nedenle pek çok taraf devlet, servis sağlayıcılara trafik verilerini belirli bir süre için tutma yükümlülüğü getirmektedir. Siber alemde yürütülen soruşturmaların genellikle ilk ve en önemli adımı, servis sağlayıcı ya da belirlenmiş bir merkezi yetkili makamdan tutulmuş verilerin istenmesidir. Ancak failler, bazı özel programları kullanarak verilerin takip ettiği yolu takip edilemez kılabilmektedir. Bu durumda trafik verilerinin gerekçe zamanlı olarak toplanması iletişimin takip ettiği yolu saptayabilmenin tek yolu olmaktadır. Diğer yandan soruşturulan iletişimin farklı devletlerde bulunan farklı servis sağlayıcılar aracılığıyla gerçekleşmesi halinde, farklı yasal yükümlülüklere tabi olan servis sağlayıcıların trafik verilerini farklı süreler için tutmaları dolayısıyla, iletişim geriye doğru kaynağına kadar takip edilemeyebilir. Bu nedenle, farklı devletlerdeki servis sağlayıcıların dahil olduğu iletişimlerde trafik verilerinin gerçek zamanlı toplanması özellikle önem arz etmektedir. Sözleşme bu ihtiyacın farkında olarak 33.maddede taraf devletlere trafik verilerini gerçek zamanlı olarak toplanması konusunda adli yardımlaşma sağlama yükümlülüğü getirmiştir.

33. maddede trafik verilerinin gerçek zamanlı olarak toplanması konusunda gerçekleştirilecek yardımlaşma düzenlenirken, ulusal düzeydeki karşılığı olan muhakeme tedbirine ve mevcut adli yardımlaşma sistemlerine atıf yapılmakla yetinilmiş ve ayrıntılı özel hükümler getirilmemiştir. Yalnızca maddenin 2. fıkrasında bu konuda yardımlaşmanın kapsamını mümkün olduğunca geniş tutmak amacıyla getirilmiş bir şart yer almaktadır[548]. Buna göre "en azından" ulusal düzeyde bu tedbire başvurulabilecek suçlar bakımından adli yardımlaşma sağlanmak zorundadır. Diğer bir değişle uygulanan mevcut adli yardımlaşma antlaşması trafik

[548] Açıklayıcı Rapor, par. 295.

verilerinin gerçek zamanlı toplanması tedbiri bakımından daha dar bir kapsam öngörüyor olsa bile, taraf devletler ulusal düzeyde bu tedbire başvurulmasına olanak tanıdıkları suçlar bakımından adli yardım sağlamak zorundadırlar[549].

Uygulamada trafik verilerinin gerçek zamanlı olarak toplanması çok sık başvurulan bir yardımlaşma aracı değildir[550]. Bununla birlikte ulusal mevzuatları elverişli olan taraf devletler arasında bu konuda geniş kapsamlı bir yardım sağlanmakta olduğu görülmektedir[551]; çünkü bu tür bir toplama hem içerik verilerine müdahaleden hem de arama ve el koymadan daha az müdahaleci bir önlem olarak değerlendirilmektedir[552].

İçerik verilerinin takip edilmesi konusunda yardımlaşma 34. maddede düzenlenmiş olup, bu konuda da madde metni oldukça kısa tutulmuş, mevcut adli yardımlaşma mekanizmalarına atıf yapılmakla yetinilmiş ve özel düzenlemeler getirilmemiştir. Sözleşme'nin bu konuda geniş kapsamlı bir uygulamayı teşvik edecek ayrıntılı düzenlemeler getirmemesinin en önemli nedeni, içerik verilerinin takip edilmesi tedbirinin özel hayata müdahale edici nitelikte olmasıdır[553]. Bu itibarla devletlerin mevcut adli yardımlaşma mekanizmaları uyarınca içerik verilerinin takibi konusunda yardımlaşma sağlama yükümlülüklerine ilave bir yükümlülük getirilmemiştir. Dolayısıyla bu konuda yardımlaşma, taraflar arasındaki geçerli antlaşmalar ve iç hukuklarının izin verdiği ölçüde sağlanacaktır. Sözleşme'nin bu konudaki esnek tutumuna paralel olarak, T-CY'nin de Sözleşme'nin uygulanmasına ilişkin değerlendirme raporlarında içerik verilerinin takip edilmesi tedbirine yer verilmediği görülmektedir.

5. 7/24 İletişim Ağı

Sözleşme'nin tesis etmeye çalıştığı adli işbirliği rejimi, büyük ölçüde mevcut sistemlerin uygulanması, ancak mevcut sistemlerin yetersiz veya hantal kaldığı durumlarda Sözleşme düzenlemelerinin devreye girerek sistemdeki sorun ve tıkanıklığı bertaraf edilmesi üzerine kuruludur. Sözleşme'nin bu anlamda

[549] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1259.
[550] "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 79.
[551] "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 83.
[552] Açıklayıcı Rapor, par. 295.
[553] Açıklayıcı Rapor, par. 296.

benimsediği en önemli araç, taraf devletlerde 7 gün 24 saat erişilebilen irtibat noktaları kurulması ve bu irtibat noktaları vasıtasıyla sürekli ve hızlı bir iletişim ağı kurulmasıdır.

Yukarıda farklı yerlerde belirttiğimiz üzere, siber suçlarla etkin biçimde mücadele etmek ve elektronik ortamda delillerin toplanması çok çabuk hareket etmeyi gerektirmektedir. Oysa mevcut polisiye işbirliği ve adli yardımlaşma biçimleri siber alemin gerektirdiği ölçüde hızlı hareket etmeyi mümkün kılacak şekilde tasarlanmamıştır. Bilişim çağının gereklerine cevap verebilmek adına bu işbirliği mekanizmalarına yeni kanalların eklenmesi ihtiyacı doğmuştur. Bu kapsamda G8 grubu ülkelerin iletişim ağı projesi örnek alınmış ve taraf devletlerin belirleyeceği irtibat noktalarından oluşan bir irtibat ağı öngörülmüştür.

Sözleşme'nin 35. maddesi ile taraf devletlere, 7 gün 24 saat ulaşılabilen irtibat noktaları belirleme sorumluluğu getirilmektedir. Buna göre belirlenecek irtibat noktalarının temel görevi siber suçlara ilişkin ve genel olarak siber alemde yürütülen soruşturma ve kovuşturmalarda hızlı ve etkili yardımlaşmayı sağlamaktır. Bu soyut ve genel görev tanımının belirli ölçüde somutlaştırılması adına 35. maddede irtibat noktalarının özellikle yerine getirmesi gereken görevler sayılmıştır. İrtibat noktaları, Sözleşme'de öngörülen geçici önlemlerin alınması konusunda adli yardımlaşma taleplerini almak ve iletmekle sorumludur. Niteliği gereği, haftanın 7 günü ve günün 24 saati ne zaman ihtiyaç duyulursa derhal ve hızlı bir şekilde gerçekleştirilmesi gereken bu konulardaki yardımlaşmaların başka kanallarla değil, 7/24 irtibat noktaları aracılığıyla gerçekleştirilmesi öngörülmüştür.

İrtibat noktalarının bir diğer görevi, doğrudan yerine getirmeyeceği işlevlerin hızlı bir biçimde gerçekleştirilmesini kolaylaştırmaktır[554]. Mevcut adli yardımlaşma sistemi uyarınca yardımlaşma taleplerinin başka bir makama iletileceği öngörüldüğü durumlarda dahi, bu kanalla gerçekleşecek iletişimin yeterince hızlı ve etkili olmayacağı düşünüldüğünde 7/24 irtibat noktalarının iletişimin hızlı ve etkili bir şekilde sağlanması konusunda etkin rol oynaması amaçlanmaktadır.

İrtibat noktalarının, resmi adli yardımlaşma talebi kendisi üzerinden gerçekleştirilip gerçekleştirilmeyeceğine bakılmaksızın, siber alemde yürütülen her türlü soruşturma ve kovuşturmada delil toplanması ve şüphelilerin yerinin tespitini kolaylaştıracak hukuki bilgileri vermesi ve bu işlemlerin yerine getirilmesini

[554] Açıklayıcı Rapor, par. 298.

kolaylaştırması öngörülmektedir. Diğer bir deyişle, irtibat noktaları diğer taraf devletlerin adli yardımlaşma talebinde bulunabilmesi için ulusal mevzuata ve uygulamaya ilişkin gerekli hukuki bilgileri sağlamak, bunun yanı sıra soruşturma işlemlerini kolaylaştıracak her türlü desteği sağlamakla görevlidir[555]. Bu kapsamda özellikle ön alan soruşturmaları noktasında olmak üzere polisiye işbirliğini sağlamak da irtibat noktalarının görev alanına girmektedir[556].

İrtibat noktaları en önemli fonksiyonları olan sürekli ve hızlı iletişim sağlanması doğrultusunda gerekli iletişim araçlarına sahip olmalıdır. Sözleşme'de, irtibat noktaları arasında iletişimin hangi araçlarla yapılacağı konusunda herhangi bir belirleme veya kısıtlama yoktur. Sözleşme'nin bu noktada öngördüğü standart "hızlı bir iletişime olanak sağlayacak yeterliliğe" sahip olunmasıdır. İletişim ağının düzgün işleyebilmesi için öncelikle telefon, faks ve bilgisayar teçhizatı temel önemdedir ve bunların yanı sıra teknoloji geliştikçe diğer iletişim biçimlerinin de sistemin parçası halinde getirilmesi gereklidir[557].

İrtibat noktaları arasında iletişimin hangi dilde gerçekleşeceği konusunda da herhangi bir düzenleme getirilmemiştir. Buna göre taraf devletler irtibat noktalarının hangi dil ya da dillerde faaliyet göstereceğini belirleme noktasında serbest bırakılmışlardır. Uygulamada devletler çoğunlukla irtibat noktalarının kendi resmi dillerinde ve İngilizce olarak faaliyet göstermesini öngörmekle birlikte, resmi adli yardımlaşma talepleri bakımından çoğunlukla talebin devletin resmi anadilinde yapılması şartı aranmaktadır. Kanaatimizce, 7/24 irtibat noktaları hakkında, belirlenecek ortak bir veya birkaç dilde her türlü yardım talebini alma ve cevaplama zorunluluğu getirilmesi, irtibat noktalarının iletişimleri hızlı bir şekilde gerçekleştirme misyonuyla daha uyumlu olurdu. Bu yönde getirilecek zorunluluğa paralel olarak, irtibat noktalarında görev yapacak personelin ilgi yabancı dillere hakim olması zorunluluğu da getirilerek daha hızlı ve etkin bir iletişim ağı sağlanabilirdi. Zira adli yardımlaşma taleplerinin muhatap devletin resmi anadilinde yapılması zorunluluğu, taleplerin tercümesi esnasında zaman kayıplarına yol açmaktadır[558]. Diğer yandan pek çok farklı dil arasında tercüme yapılmasındansa, yalnızca belirlenmiş ortak iletişim diline tercüme yapılması, farklı diller arasındaki

[555] Açıklayıcı Rapor, par. 299.
[556] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1261.
[557] Gercke, "Understanding Cybercrime", s. 473.
[558] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1261.

tercümelerde yaşanan tercüme hatalarını ve buna bağlı iletişim sorunlarını minimize edecektir.

İrtibat noktalarına yüklenen bir diğer görev, teknik danışmanlık ve öneri sağlanmasıdır. Siber suç soruşturmalarının ve elektronik ortamda delil elde etme süreçlerinin uzmanlık gerektirmesi ve bu alanlarda teknolojin sürekli olarak gelişmesi dolayısıyla adli makamlar düzenli olarak teknik danışmanlık ve öneriye ihtiyaç duymaktadır. İrtibat noktalarının bu ihtiyaca belirli ölçüde cevap vermesi amaçlanmaktadır[559]. Buna göre irtibat noktaları belirlenirken veya kurulurken teknik konularda danışmanlık ve öneri getirebilecek yeterliliğe sahip olmasının gözetilmesi gerekmektedir.

İrtibat noktasının idari yapı dahilinde nasıl konumlandırılacağı, taraf devletlerin seçimine bırakılmıştır. İrtibat noktası olarak, halihazırda genel olarak uluslararası adli işbirliği konularında yetkilendirilmiş merkezi makam belirlenebileceği gibi, emniyet veya diğer birimler içerisinde belirlenecek bir başka makam da belirlenebilir. Bu bakımdan, irtibat noktasının bizzat kendisi adli yardım talebini yerine getirmek zorunda değildir[560]. Her durumda, irtibat noktası, hem siber saldırıları durdurmak ve izini tespit etmek açısından teknik yardım sunacak hem de bazı uluslararası adli yardımlaşma işlevlerini yerine getirecektir[561]. Halihazırda adli işbirliği konusunda yetkilendirilmiş merkezi makamın irtibat noktası olarak belirlenmesi, tekillik sağlaması itibariyle daha tercih edilir bir yöntem olmakla birlikte, teknik konularda bu makamın yetersiz kalabileceği düşüncesiyle başka bir makamın belirlenmesine imkan tanınmıştır[562].Uygulamada, genellikle polisin irtibat noktası olarak belirlendiği gözlemlenmektedir[563]. Bununla birlikte, adalet bakanlıkları, diğer bakanlıklar, istihbarat birimleri, savcılık makamları ya da ayrı bir uzmanlar komitesi gibi çok farklı makamların irtibat noktası olarak belirlenmesine ilişkin örnekler de mevcuttur[564].

---

[559] Havuz, "Avrupa Konseyi Siber Suçlar Sözleşmesi"s. 205.
[560] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1260.
[561] Açıklayıcı Rapor, par. 300.
[562] Peter Csonka, "The Council of Europe's Convention on Cyber-Crime and Other European Initiatives", **Revue İnternationale De Droit Pénal**, sy. 77, 2006, s. 496.
[563] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1261.
[564] Taraf devletlerce irtibat noktası olarak farklı makamların belirlenmesine a) emniyet teşkilatı ya da içindeki bir birimi belirleyen (Türkiye, Arnavutluk, Ermenistan, Danimarka, Estonya, Almanya, Macaristan, İzlanda, Letonya, Litvanya, Slovakya), b) Adalet Bakanlığı'nı belirleyen (Kıbrıs R.K.), c) başka bir Bakanlığı belirleyen (Azerbaycan: Ulusal Güvenlik Bakanlığı, Bulgaristan: İçişleri Bakanlığına bağlı özel bir birim, Moldova: İçişleri Bakanlığı'na bağlı özel bir birim, Slovenya), d) İstihbarat Birimi'ni tayin eden (Finlandiya), e) ayrı bir uzman birimi tayin eden

7/24 iletişim ağı Sözleşme'nin öngördüğü adli işbirliği hükümleri içerisinde en etkili araç olarak görülmektedir[565]. Sözleşeme bu iletişim ağını mümkün olduğunca en geniş kapsamda etkin kılarak hem mevcut adli işbirliği sistemlerindeki aksaklıkları büyük ölçüde gidermeyi, hem de Sözleşme'de özel olarak düzenlenen adli yardımlaşma araçlarının etkin bir şekilde uygulanmasını amaçlamaktadır. Ancak uygulamada 7/24 iletişim ağı öngörüldüğü şekilde etkin işlememektedir[566]. Bu durumun başlıca nedenleri irtibat noktalarının idari yapılanmadaki yerleri ve diğer kurumlarla ne şekilde irtibat içinde olacakları konularındaki belirsizlikler, irtibat noktalarının iletişim dili olarak ortak bir dilin belirlenmiş olmaması ve istihdam edilen personelin gerekli eğitimlere tabi tutulmaması gelmektedir[567]. T-CY, 7/24 iletişim ağının etkinliğinin artırılması ve mümkün olan en geniş kapsamda uygulanması için çalışmalarını sürdürmekte ve iletişim ağına katılmak için, Sözleşme'ye taraf olmanın gerekmediğini hatırlatmaktadır[568].

B. Türk Hukukunda Uluslarası Adli İşbirliği Ve Sözleşmenin İlgili Hükümlerinin Türkiye Bakımından Uygulanması

Türk hukukunda genel olarak uluslararası adli işbirliği ve özel olarak uluslararası adli yardımlaşma, bu alanda imzalanarak kabul edilmiş çok taraflı ve iki taraflı uluslararası antlaşmalar çerçevesinde, uygulanabilir bir uluslararası antlaşmanın bulunmadığı hallerde ise karşılıklılık esasına göre yürütülmektedir[569]. Türk kanun koyucu Almanya, Avusturya, İsviçre gibi bazı devletlerin benimsediği şekilde adli işbirliğinin çeşitli yönlerini düzenleyen bağımsız bir kanunu yürürlüğe koymayı tercih etmemiştir[570].

Yurtdışında gerçekleştirilmesi gereken muhakeme işlemleri konusunda, diğer bir deyişle yabancı makamlardan adli yardımlaşma talep edilirken Türk

---

(Fransa, Norveç, Romanya: Yüksek Mahkeme'ye bağlı özel bir birim), f) Savcılık Makamı'nı tayin eden (İtalya: Roma Başsavcısı, Hollanda, Sırbistan, Makedonya (Eski Yugoslav Cumhuriyeti) örnek olarak gösterilebilir.

565 Vatis, "The Council of Europe 's Convention on Cybercrime", s. 214; Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1260.

566 "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 88..

567 "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 91.

568 "Report of the 2nd Meeting of the Cybercrime Convention Committee", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, Mart 2007, s. 5.

569 Şimşek, **Yabancıların Türkiye'de Yargılanması**, s. 91.

570 Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1247.

makamlarının nasıl hareket etmesi gerektiği veya yurtdışından gelen adli yardımlaşma taleplerini karşılarken Türk ulusal makamlarının takip etmesi gereken usul noktasında da yasal bir düzenleme mevcut değildir. Bu bakımdan, genel olarak uygulanabilir ortak bir çerçeve yoktur[571]. Farklı işbirliği türleri, dayanak alınan çok taraflı ya da iki-taraflı uluslararası antlaşmalarda yer alan hüküm ve usullere tabi olmaktadır. Adli işbirliğine ilişkin genel olarak uygulanabilir yasal düzenleme bulunmamakla birlikte, Anayasa'nın 38. maddesinde ve 5237 sayılı Türk Ceza Kanunu'nun 18. maddesinde geri vermeyle ilgili hükümler yer almaktadır.

Avrupa Siber Suçlar Sözleşmesi'nin adli işbirliği konusunda mevcut işbirliği mekanizmalarını korumayı ve öncelikli olarak bu mekanizmalar aracılığıyla uygulanmayı tercih etmesi dolayısıyla Türkiye bakımından adli işbirliğinin hukuki dayanağını teşkil eden ulusal mevzuatı ve uluslararası antlaşmaları kısaca incelemekte fayda görüyoruz.

1. Türk Hukukunda Uluslararası Adli İşbirliğinin Hukuki Dayanakları

a) Anayasal İlkeler

Belirttiğimiz üzere, Türk hukukunda adli işbirliği bu alandaki uluslararası antlaşmalar çerçevesinde uygulanmaktadır. Uluslararası antlaşmaların Türk hukuku bakımından yürürlüğe girmesi ve uygulanmasına ilişkin esaslar Anayasa'nın 90. maddesinde düzenlenmektedir.

Anayasa'nın 90. maddesi uyarınca Türkiye Cumhuriyeti adına yabancı devletlerle ve uluslararası kuruluşlarla yapılan antlaşmaların onaylanması, Türkiye Büyük Millet Meclisinin onaylamayı bir kanunla uygun bulmasına bağlıdır. Maddede, farklı nitelikteki uluslararası antlaşmaların yürürlüğe girmesi bakımından farklı seçenekler öngörülmüş olmakla birlikte uluslararası adli işbirliği konusundaki uluslararası antlaşmaların yürürlüğe girmesi TBMM tarafından uygun bulma kanunuyla kabul edilmesine bağlıdır[572].

---

[571] Durmuş Tezcan/Mustafa Ruhan Erdem/Murat Önok, **Uluslararası Ceza Hukuku**, 2. Baskı, Ankara: Seçkin, 2014, s. 181.

[572] Anayasa'nın 90. maddesinin 2. ve 3. fıkralarında ekonomik, ticari veya teknik ilişkileri düzenleyen ve süresi bir yılı aşmayan antlaşmalar, yürürlükte olan bir uluslararası antlaşmaya dayanan

Uluslararası antlaşmaların Türk hukukundaki etkisi, Anayasa'nın 90. maddesinin son fıkrasına dayanmaktadır. Buna göre "*usulüne göre yürürlüğe konulmuş milletlerarası antlaşmalar kanun hükmündedir*". Bu hüküm sayesinde Türkiye Cumhuriyeti adına imzalanmış adli işbirliği antlaşmaları uygun bulunmaları üzerine doğrudan doğruya uygulanma kabiliyeti kazanmaktadır. Türkiye'nin imzalamış olduğu adli işbirliğini düzenleyen diğer uluslararası antlaşmaların yanı sıra, Avrupa Siber Suçlar Sözleşmesi de 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun'un 28988 nolu Resmi Gazete'de yayımlanması üzerine 02.05.2014 tarihi itibariyle yürürlüğe girmiştir. Bu tarih itibariyle Sözleşme Türk hukukunun bir parçası haline gelmiş olup doğrudan doğruya uygulanabilir niteliktedir. Türk makamlarınca siber alemde yürütülen soruşturmalarla ilgili olarak gerçekleştirilecek adli yardımlaşmalarda, Sözleşme'nin doğrudan doğruya uygulanacağını öngördüğü özel adli yardımlaşma biçimleri ve başka bir antlaşama bulunmaması halinde, Sözleşme'nin bu durumlar için öngördüğü yedek normlar başkaca bir hukuki dayanağa ihtiyaç duymaksızın uygulanabilir[573].

Sözleşme'nin Türk hukukundaki yerinin belirlenmesi konusunda da Anayasa'nın 90. maddesi yol gösterici niteliktedir. Maddenin son fıkrasında usulünce kabul edilmiş uluslararası antlaşmaların "*kanun hükmünde olduğu*" belirtilmekle birlikte, devamında "*bunlar hakkında Anayasaya aykırılık iddiası ile Anayasa Mahkemesine başvurulamaz*" denilmektedir. Uluslararası antlaşmaların kanunlarla eşdeğer olduğu yönündeki birinci cümleye karşın, ikinci cümleden uluslararası antlaşmaların kanunlardan üstün olduğu anlamı çıkmaktadır. Maddenin açık olmayan bu ifadeleri karşısında uluslararası antlaşmaların Türk hukukundaki hiyerarşik yeri konusunda doktrinde farklı görüşler ortaya konmuştur[574]. Biz, uluslararası

---

uygulama antlaşmaları ve kanunun verdiği yetkiye dayanılarak yapılan ekonomik, ticari, teknik veya idari konulardaki antlaşmalar bakımından farklı seçenekler benimsenmiştir: *"Ekonomik, ticari veya teknik ilişkileri düzenleyen ve süresi bir yılı aşmayan andlaşmalar, Devlet Maliyesi bakımından bir yüklenme getirmemek, kişi hallerine ve Türklerin yabancı memleketlerdeki mülkiyet haklarına dokunmamak şartıyla, yayımlanma ile yürürlüğe konabilir. Bu takdirde bu andlaşmalar, yayımlarından başlayarak iki ay içinde Türkiye Büyük Millet Meclisinin bilgisine sunulur.*
Milletlerarası bir andlaşmaya dayanan uygulama andlaşmaları ile kanunun verdiği yetkiye dayanılarak yapılan ekonomik, ticari, teknik veya idari andlaşmaların Türkiye Büyük Millet Meclisince uygun bulunması zorunluğu yoktur; ancak, bu fıkraya göre yapılan ekonomik, ticari veya özel kişilerin haklarını ilgilendiren andlaşmalar, yayımlanmadan yürürlüğe konulamaz."

[573] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1248.

[574] Bu konuda ileri sürülen görüşler için bkz. Hasan Tunç, "Milletlerarası Sözleşmelerin Türk İç Hukukuna Etkisi Ve Avrupa İnsan Hakları Mahkemesinin Türkiye İle İlgili Örnek Karar

antlaşmaların kanun hükmünde olduğu şeklindeki açık hüküm ve Anayasa'nın hiçbir yerinde uluslararası antlaşmaların kanunlardan üstün olduğunu belirten bir hüküm bulunmaması karşısında, bu antlaşmaların Anayasa Yargısından bağışık tutulmalarının tek başına kanunlardan üstün tutulma anlamına gelmeyeceğini, Türkiye Cumhuriyeti Devleti'nin bir uluslararası anlaşmayı imzalayarak uluslararası hukuk uyarınca üstelenmiş olduğu yükümlülükler uyarınca bu şekilde bir bağışıklık getirildiğini düşünüyoruz[575].

Anayasa'nın 90. maddesinin son cümlesinde temel hak ve özgürlüklere ilişkin milletlerarası antlaşmaların kanunlar karşısındaki konumu konusunda özel bir düzenleme getirilmiştir. Buna göre temel hak ve özgürlüklere ilişkin uluslararası antlaşmaların kanunlarla farklı hükümler içermesi durumunda milletlerarası antlaşma hükümleri esas alınır. Avrupa Siber Suçlar Sözleşme'si temel hak ve özgürlüklere ve bu konudaki uluslararası metinlere sıklıkla atıf yapmakla birlikte, temel hak ve özgürlüklere ilişkin uluslararası antlaşma niteliğinde değildir. Netice olarak Sözleşme, kanunlara eş değer niteliktedir. Bunun sonucu olarak Sözleşme'yle aykırılık içerisinde olan kanun hükümleri Sözleşme'nin yürürlüğe girmesi ile kendiliğinden hükümsüz hale gelmemektedir. Çalışmamızın İkinci Bölümünde ortaya koyduğumuz Türk ceza mevzuatının Sözleşme'yle uyum içinde olmayan hükümlerinin Sözleşme'yle uyumluluk sağlanacak şekilde yeniden düzenlenmesi Türkiye'nin uluslararası hukuk uyarınca üstlenmiş olduğu bir sorumluluk olup, bu düzenleme, TBMM tarafından gerekli kanunların yapılması yoluyla gerçekleşecektir.

Uluslararası adli işbirliği konusunda Anayasa'nın temel rolü bu konudaki uluslararası antlaşmaların doğrudan uygulanabilirliğine zemin sağlamak olmakla birlikte, "Suç ve cezalara ilişkin esaslar" başlıklı 38. maddede suçluların iadesine yönelik dar kapsamlı bir ilkeye yer verilmektedir. 38. maddenin son fıkrası uyarınca, Uluslararası Ceza Divanına taraf olmanın gerektirdiği yükümlülükler hariç olmak üzere, vatandaş, suç sebebiyle yabancı bir ülkeye verilemez.

İncelemesi", (Anayasa Mahkemesi'nin 38. Kuruluş Yıldönümü Nedeniyle Düzenlenen Sempozyumda Sunulan Bildiri), Anayasa Yargısı, sy. 17, 2000, s. 175 vd.

[575] Aynı yönde görüş için bkz. Necmi Yüzbaşıoğlu, **Türk Anayasa Yargısında Anayasallık Bloku**, İstanbul: İÜHF Yayınları, 1993, s. 52 vd.

b) Uluslararası Antlaşmalar

Ceza hukuku alanında adli yardımlaşma konusunda Türkiye'nin taraf olduğu birçok uluslararası antlaşma bulunmaktadır[576]. Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi (CİKAYAS), Suçluların İadesine Dair Avrupa Sözleşmesi, Hükümlülerin Nakline Dair Avrupa Sözleşmesi, Ceza Yargılarının Milletlerarası değeri Konusunda Avrupa Sözleşmesi, Ceza Kovuşturmalarının Aktarılması Konusunda Avrupa Sözleşmesi, Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El Konulmasına İlişkin Sözleşme örnek olarak verilebilir.

Avrupa Konseyi bünyesinde hazırlanıp 1959 ılına yürürlüğe giren CİYAKAS, Avrupa genelinde uluslararası adli yardımlaşmaların yürütülmesinde merkezi öneme sahiptir. Avrupa Konseyi'ne üye 47 devletin tamamı bu sözleşmeyi imzalamış ve uygun bulmuştur. Sözleşme'de ceza hukukunda karşılıklı yardımlaşma konusunda çok sayıda ilke ve usul ortaya konulmuştur. Sözleşme'nin uluslararası adli yardımlaşma konusunda benimsediği temel ilke karşılıklı cezalandırılabilirlik ilkesidir[577]. Bununla birlikte Sözleşme'nin en dikkat çeken ilkesi, basit suçlar söz konusu olduğunda, karşılıklı cezalandırılabilirlik koşulu aranmaksızın adli yardımlaşmanın sağlanacağının öngörülmesidir[578].

CİYAKAS, taraf devletler arasında genel olarak her türlü suç bakımından ve her türlü soruşturma işlemleri hakkında adli yardımlaşmanın mümkün olmasını amaçlamaktadır[579]. Bu genel kuralın istisnası olarak askeri suçlar kapsam dışında tutulmuş, siyasi ve mali suçlar bakımından da adli yardımlaşma sağlanması taraf devletlerin takdirine bırakılmıştır.

Konu ve taraf devletler anlamında çok geniş bir kapsamda uygulanan CİYAKAS, Avrupa Siber Suçlar Sözleşme'sinin adli yardımlaşma hükümlerinin uygulanmasında da büyük öneme sahiptir. Avrupa Konseyi üyesi devletler arasında Siber Suçlar Sözleşmesi uyarınca gerçekleştirilecek yardımlaşmalar, Sözleşme'nin

---

[576] Şimşek, "Uluslararası Adli Yardımlaşma", s. 146.
[577] Gürol, "Uluslararası Ceza Hukukunda Adli Yardımlaşma", 1720.
[578] Şimşek, **Yabancıların Türkiye'de Yargılanması**, s. 95.
[579] Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi Açıklayıcı Raporu, par. 8.

doğrudan uygulanacağı öngörülen hükümleri hariç olmak üzere CİYAKAS'ta öngörülen ilke ve usuller çerçevesinde gerçekleştirilecektir.

Adli yardımlaşma konusunda yukarıda saydığımız çok taraflı antlaşmalar dışında Türkiye'nin imzalamış olduğu 44 adet iki taraflı uluslararası antlaşma bulunmaktadır[580]. Bu anlaşmaların çoğunluğu içerik itibariyle birebir CİYAKAS hükümlerini yansıtmaktadır[581].

Ayrıca, Türkiye'nin taraf olduğu ceza alanındaki çok sayıda çok taraflı uluslararası antlaşma, ortak bir suçla mücadele siyaseti benimsenmesi, mevzuatların uyumlulaştırılması, adli ve polisiye yardımlaşmanın mümkün olması ve etkinliğinin sağlanması, teknik destek ve bilgi paylaşımı gibi çeşitli konularda adli işbirliğine ilişkin hükümler içermektedir[582].

c) Kanunlarda Yer Alan Hükümler

---

[580] Türkiye'nin karşılıklı adli yardımlaşma antlaşması imzalamış olduğu devletler şunlardır: Amerika Birleşik Devletleri, Almanya, Arnavutluk, Avustralya, Avusturya, Azerbaycan, Bosna Hersek, Bulgaristan, Cezayir, Çek Cumhuriyeti, Çin, Fas Krallığı, Gürcistan, Hırvatistan, Hindistan, Irak, İngiltere, İran, İsviçre, İtalya, Kuzey Kıbrıs Türk Cumhuriyeti, Kanada, Kazakistan, Karadağ, Kırgızistan, Kuveyt, Libya, Litvanya, Lübnan, Macaristan, Makedonya, Mısır, Moğolistan, Moldova, Özbekistan, Pakistan, Polonya, Romanya, Sırbistan, Slovakya, Slovenya, Suriye, Suudi Arabistan, Tacikistan, Tunus, Türkmenistan, Ukrayna, Umman, Ürdün.

[581] Bilal Çalışkan, "Sınıraşan Örgütlü Suçlarla Uluslararası Mücadelede Adli Yardımlaşma", **Adalet Akademisi Dergisi**, 2008, s. 14.

[582] Bu antlaşmalara örnek olarak; Terörizmin Önlenmesine Dair Avrupa Sözleşmesi, Terörizmin Önlenmesine Dair Avrupa Konseyi Sözleşmesi, Kültür Varlıklarının Kanunsuz İthal, İhraç ve Mülkiyet Transferinin Önlenmesi ve Yasaklanması İçin Alınacak Tedbirlerle İlgili Birleşmiş Milletler Sözleşmesi, Uyuşturucu ve Psikotrop Maddeler Kaçakçılığına Karşı Birleşmiş Milletler Sözleşmesi (Viyana Sözleşmesi), Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesi (Palermo Sözleşmesi), Sınıraşan Örgütlü Suçlara Karşı BM Sözleşmesine Ek İnsan Ticaretinin, Özellikle Kadın ve Çocuk Ticaretinin Önlenmesine, Durdurulmasına ve Cezalandırılmasına İlişkin Protokol, Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek, Ateşli Silahlar, Parçaları ve Aksamları ile Mühimmatının Yasa Dışı Üretimine ve Kaçakçılığına Karşı Protokol, Birleşmiş Milletler Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme, Suçtan Elde Edilen Gelirlerin Aklanması, Aranması, Zapt Edilmesi ve Müsaderesine İlişkin Avrupa Konseyi Sözleşmesi, Uluslararası Ticari İşlemlerde Yabancı Kamu Görevlilerine Verilen Rüşvetin Önlenmesi Sözleşmesi, Yolsuzluğa Karşı Ceza Sözleşmesi, Birleşmiş Milletler Yolsuzlukla Mücadele (Mérida) Sözleşmesi, Nükleer Maddelerin Fiziksel Korunmasına Dair Birleşmiş Milletler Sözleşmesi, Deniz Seyir Güvenliğine Karşı Yasa Dışı Eylemlerin Önlenmesine Dair Birleşmiş Milletler Sözleşmesi, Rehine Alınmasına Karşı Uluslararası Birleşmiş Milletler Sözleşmesi, Diplomasi Ajanları Dahil Olmak Üzere Uluslararası Korunan Kişilere Karşı İşlenen Suçların Önlenmesi ve Cezalandırılmasına Dair Birleşmiş Milletler Sözleşmesi, Uluslararası Sivil Havacılığın Güvenliğine Karşı Kanun Dışı Eylemlerin Önlenmesine İlişkin Birleşmiş Milletler Sözleşmesi, Uçakların Yasa Dışı Yollarla Ele Geçirilmesinin Önlenmesi Hakkında Birleşmiş Milletler Sözleşmesi sayılabilir. **Çalışkan**, "Sınıraşan Örgütlü Suçlarla Uluslararası Mücadelede Adli Yardımlaşma", s. 5-17.

Türk mevzuatında, çeşitli kanunlarda uluslararası adli işbirliğine ilişkin hükümler bulunmaktadır. Bu kapsamda anılması gereken ilk kanun, 3002 sayılı Türk Vatandaşları Hakkında Yabancı Ülke Mahkemelerinden ve Yabancılar Hakkında Türk Mahkemelerinden Verilen Ceza Mahkumiyetlerinin İnfazına Dair Kanun'dur. Bu kanunda, Türk vatandaşları hakkında yabancı devlet mahkemelerinden verilen ceza mahkumiyetlerinin Türkiye'de, yabancılar hakkında Türk mahkemelerinden verilen ceza mahkumiyetlerinin de hükümlünün vatandaşı olduğu devlette yerine getirilmesine dair usul ve esaslar düzenlenmiştir[583].

Türk Ceza Kanunu'nun "Geri verme" başlıklı 18. maddesinde suçluların iadesine ilişkin ayrıntılı düzenlemeler getirilmiştir. Esasında geri vermeye ilişkin koşullar, Türkiye'nin çeşitli devletlerle imzalamış bulunduğu iki taraflı sözleşmeler ile Suçluların İadesine Dair Avrupa Sözleşmesinde belirlenmiştir. Ancak, buna rağmen geri vermeye ilişkin asgari şartların, iç hukuk düzenlemesi olan kanunla belirlenmesi, uygulamada tekilliği sağlama açısından önem taşıdığı düşünülmüştür[584]. Zira iki taraflı antlaşmalarda genellikle geri verme taleplerinin hangi usul ve esaslara göre yerine getirileceği düzenlenmemekte, taraf devletlerin iç hukukuna bırakılmaktadır. Oysa kişi özgürlüğünün kısıtlanması sonucunu doğuran geri vermenin usul ve esasına ilişkin asgari şartların kanunla belirlenmesine ihtiyaç vardır[585].

TCK'nın 18. maddesindeki düzenlemenin genel olarak Suçluların İadesine Dair Avrupa Sözleşmesi'nin benimsediği ilkeleri yansıttığı ve Sözleşmeyle bire bir uyumlu olduğu görülmektedir[586]. Ayrıca Anayasa'da hüküm altına alındığı üzere, kural olarak vatandaşların iade edilmeyeceği ilkesine yer verilmiştir.

---

[583] Ahmet Ulutaş/Ömer Serdar Atabey, **Ceza Alanında Uluslararası Adli İşbirliği Hukuku**, Ankara: Adalet, 2011, s. 207.

[584] Ulutaş/Atabey, **Ceza Alanında Uluslararası Adli İşbirliği Hukuku** s. 205.

[585] Artuk/Gökçen/Yenidünya, **Ceza Hukuku Genel Hükümler**, s. 1002.

[586] TCK'nın geri verme başlıklı 18. maddesi şu şekildedir: *(1) Yabancı bir ülkede işlenen veya işlendiği iddia edilen bir suç nedeniyle hakkında ceza soruşturması ya da kovuşturması başlatılan veya mahkûmiyet kararı verilmiş olan bir yabancı, talep üzerine, soruşturma ya da kovuşturmanın yapılabilmesi veya hükmedilen cezanın infazı amacıyla geri verilebilir. Ancak, geri verme talebine esas teşkil eden fiil;(1)*

a) Türk kanunlarına göre suç değilse,

b) Düşünce suçu veya siyasi ya da askerî suç niteliğinde ise,

c) Türkiye Devletinin güvenliğine karşı, Türkiye Devletinin veya bir Türk vatandaşının ya da Türk kanunlarına göre kurulmuş bir tüzel kişinin zararına işlenmişse,

d) Türkiye'nin yargılama yetkisine giren bir suç ise,

e) Zamanaşımına veya affa uğramış ise,

Geri verme talebi kabul edilmez.

d) Türk Uluslararası Adli İşbirliği Kanun Tasarısı

Türk hukukunda genel olarak adli işbirliğine yönelik bağımsız bir kanun bulunmadığını yukarıda belirtmiştik. Ancak bu durum adli işbirliği ve özellikle uluslararası adli yardımlaşma süreçlerinde belirsizliklere yol açmakta ve sitemin işlerliğini olumsuz yönde etkilemektedir[587]. Bu nedenle genel olarak adli işbirliği ve özel olarak adli yardımlaşmayı düzenleyen genel bir kanunla ilgili usul ve esasların belirlenmesi gerekliliği doktrinde uzun süredir dillendirilmektedir[588].

Türk ceza adalet sisteminde Avrupa Birliği standartlarının yakalanarak Avrupa İnsan Hakları Sözleşmesi'nin etkin bir şekilde uygulanması, uluslararası adlî işbirliğinin güçlendirilmesi ve yargılama sürelerini kısaltarak ceza adaletini daha etkin şekilde sağlanması amaçlarıyla 12 Mart 2012 tarihinde başlatılan Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Projesi kapsamında bir "Türk Uluslararası Adli İşbirliği Kanun Tasarısı" hazırlanması yönünde çalışmalar yürütülmektedir. Bu kapsamda Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü ve Uluslararası Hukuk ve Dışişleri Genel Müdürlüğü'nce çok sayıda çalıştay organize edilmiş, ulusal mevzuatlarında adli işbirliği kanunlarına yer veren 11 devletin

---

(2) Uluslararası Ceza Divanına taraf olmanın gerektirdiği yükümlülükler hariç olmak üzere, vatandaş suç sebebiyle yabancı bir ülkeye verilemez.

(3) Kişinin, talep eden devlete geri verilmesi halinde ırkı, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasi görüşleri nedeniyle soruşturulacağına ya da kovuşturulacağına veya cezalandırılacağına ya da işkence ve kötü muameleye maruz kalacağına dair kuvvetli şüphe sebepleri varsa, talep kabul edilmez.(1)

(4) Kişinin bulunduğu yer ağır ceza mahkemesi, geri verme talebi hakkında bu madde ve Türkiye'nin taraf olduğu ilgili uluslararası sözleşme hükümlerine göre karar verir. Bu karara karşı temyiz yoluna başvurulabilir.

(5) Mahkeme geri verme talebinin kabul edilebilir olduğuna karar verirse, bu kararın yerine getirilip getirilmemesi Bakanlar Kurulunun takdirine bağlıdır.

(6) Geri verilmesi istenen kişi hakkında koruma tedbirlerine başvurulmasına, Türkiye'nin taraf olduğu ilgili uluslararası sözleşme hükümlerine göre karar verilebilir.

(7) Geri verme talebinin kabul edilebilir olduğuna karar verilmesi halinde, ayrıca Ceza Muhakemesi Kanunu hükümlerine göre tutuklama kararı verilebilir veya diğer koruma tedbirlerine başvurulabilir.(1)

(8) Geri verme halinde, kişi ancak geri verme kararına dayanak teşkil eden suçlardan dolayı yargılanabilir veya mahkûm olduğu ceza infaz edilebilir."

[587] Şimşek, "Uluslararası Adli Yardımlaşma", s. 159.

[588] Bu yönde görüşler için bkz. Feridun Yenisey, "Milletlerarası Ceza Hukukunda Yeni Gelişmeler", **70. Yılında Türk Ceza Kanunu - Genel Hükümler**, İstanbul, 1998, s. 52; Tezcan/Erdem/ Önok, **Uluslararası Ceza Hukuku**, s. 181; Fatih Selami Mahmutoğlu, Suçluların Geri Verilmesi, **70. Yılında Türk Ceza Kanunu - Genel Hükümler**, İstanbul, 1998, s. 66; Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1247.

mevzuatları incelenmiş ve bu devletlerin ilgili birimlerine çalışma ziyaretleri düzenlenmiştir[589].

Türk Uluslararası Adli İşbirliği Kanununda genel olarak ceza alanında uluslararası adli yardımlaşmaya ilişkin modern yaklaşımları yansıtan ilke ve esaslara yer verilmesi ve özel olarak "Adli Yardım Taleplerinin Hazırlaması", , "Siber Suçlar ve Adli Yardımlaşma", "Suçluların İadesi", "Kovuşturma ve İnfaz Devri", "Hükümlü Nakli", "Yolsuzluk Alanında Uluslararası Düzenlemeler ve Adli İşbirliği", "Terörizmin Finansmanı, Mali Eylem Görev Gücü ve Adli İşbirliği" ile "Örgütlü Suçlarda ve Uyuşturucu Suçlarında El Koyma, Müsadere ve Adli İşbirliği" konularının düzenlenmesi planlanmaktadır[590].

2. Türkiye'de Siber Suçlarda Adli İşbirliği Uygulaması

Türk hukukunda uluslararası adli iş birliği ve adli yardımlaşma konularında yetkili merkezi makam Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'dür (UHDİGM). 2992 sayılı Adalet Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'un 13/A maddesine göre, "*hukuki ve cezai konularda uluslararası adli yardımlaşma; tebligat, istinabe, suçluların iadesi, hükümlülerin transferi, kovuşturmaların aktarılması işlemlerini yapmak*", konularında UHDİGM yetkili ve görevlidir.

Türkiye, Sözleşme'nin 27. maddesi çerçevesinde uygulanabilir başkaca adli yardımlaşma antlaşması bulunmadığı hallerde yardımlaşma taleplerini almak ve cevaplamakla görevlendirilmiş yetkili makam olarak da UHDİGM'i belirlemiş ve bu durumu Avrupa Konseyi Genel Sekreterliği'ne beyan etmiştir. Aynı şekilde 24. madde öngörülen süratli iletişim noktası olarak da UHDİGM belirlenmiştir.

UHDİGM, halihazırda adli işbirliği konusunda ilke ve usulleri düzenleyen bir kanuni düzenleme bulunmaması karşısında ceza işlerinde uluslar arası işbirliğinde adli makamların dikkat etmesi gerek hususlarda açıklama ve tavsiyelerde bulunan genelgeler yayımlamakta bu surette uygulama birliğini sağlamaya çalışmaktadır. Bu

---

[589] Türk Uluslararası Adli İşbirliği Kanun Tasarısı çalışmaları hakkında ayrıntılı bilgi için bkz. http://www.uhdigm.adalet.gov.tr/projeler/adliyardimlasmaevrak.html.

[590] Yargı Reformu Stratejisi, Adalet Bakanlığı, Nisan 2015, s. 67.

konuda, 01.03.2008 tarihli ve 69/1 sayılı "Cezai İşlere İlişkin Uluslararası İşbirliğinde Adli Makamlarımızca Dikkat Edilmesi Gereken Hususlar"a dair ve 01.03.2008 tarihli ve 66/1 sayılı "Adli Yardım Taleplerinin İletilmesine İlişkin Avrupa Sözleşmesinin Uygulanması" hakkındaki genelgeler uygulamayı şekillendirmeleri itibariyle önemlidirler[591]. Bu genelgeler adli işbirliğine ilişkin başta CİYAKAS olmak üzere uluslararası antlaşmalarca benimsenmiş ilkelerin uygulamacılar açısından pratikte ne şekilde anlam ifade edeceği konusunda genel yol gösterici açıklamalar getirmektedir[592]. Bunun yanı sıra suçluların iadesi, tebligat, adli yardımlaşma taleplerinin hazırlanması, gelen taleplerin yerine getirilmesi konularında takip edilmesi gereken prosedürler ayrıntılı olarak açıklanmakta ve belirli suç tipleri, belirli yardımlaşma türleri ve belirli devletler bakımından adli yardımlaşmaların arz ettiği özellikler ortaya konulmaktadır.

UHDİGM tarafından hazırlanan genelgelerde siber suçlarla ilgili adli yardımlaşmaya ilişkin herhangi bir açıklama bulunmamaktadır. Bahsi geçen genelgelerin Sözleşme'nin Türkiye tarafından imzalanmasında önce hazırlanmış olması itibariyle bu durum normal karşılanabilir. Siber suçlarla ilgili adli yardımlaşmalar konusunda yol gösterici açıklamalar UHDİGM'in resmi internet sitesinde yer almaktadır. Burada, belirli devletler ve yaygın olarak kullanılan bazı servis sağlayıcılar özelinde trafik bilgilerinin ne şekilde elde edileceği vb. konularda pratik açıklamalar yer almaktadır. Ancak ilginç bir şekilde Siber Suçlar Sözleşme'si çerçevesinde adli yardımlaşmaya ilişkin herhangi bir açıklama bulunmamaktadır. Bu durum Türkiye'nin Sözleşme'yi uygulama iradesi noktasında olumsuz bir göstergedir. Uluslararası sözleşmelerin ulusal makamlarca dikkate alınması bu konuda merkezi makamların gerekli alt yapıyı sağlamasına ve teşviklerine bağlıdır. Bu itibarla UHDİGM'in hızlı bir şekilde hem bir genelge yayınlamak hem de resmi internet sitesinde gerekli pratik bilgileri sunmak suretiyle Sözleşme'nin adli işbirliği hükümlerinin Türkiye bakımından uygulanmasında takip edilmesi gereken usullere ve dikkat edilmesi gereken hususlara açıklık getirmesi gerektiği kanaatindeyiz.

Türkiye'nin, Sözleşme'nin 35. maddesi uyarınca belirlediği 7/24 irtibat noktası Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'dır. Sözleşme'nin Türkiye tarafından imzalanmasından sonra kurulan Daire, henüz tam olarak kurulumunu tamamlamamış ve Daire'nin faaliyetleri planlanan etkinliğe

[591] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1248.
[592] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi", s. 1248.

ulaşmamıştır[593]. Bununla birlikte Sözleşme'nin Türkiye bakımından yürürlüğe girmesiyle birlikte resmen 7/24 irtibat noktası niteliği kazanan Daire, Türikiye'nin Avrupa Konseyi Genel Sekreterliği'ne beyan ettiği irtibat bilgileri doğrultusunda iletişim ağının bir parçası olarak faaliyet göstermektedir[594].

Siber Suçlarla Mücadele Daire Başkanlığı'nın 7/24 irtibat noktası olarak görevlerini hangi esaslara göre yerine getireceği, mahkemeler, savcılıklar, diğer emniyet birimleri ve diğer kurumlarla irtibat ve ilişkisinin hangi usuller çerçevesinde sağlanacağı, adli işbirliği konusunda merkezi yetkili makam olan UHDİGM ile nasıl bir ilişki içinde olacağı konularında herhangi bir düzenleme bulunmamaktadır ve bu önemli bir eksikliktir. T- CY'nin raporlarına yansıdığı şekliyle bu durum 7/24 irtibat noktalarının istenilen seviyede işler durumda olmamasının en önemli sebebidir[595].

7/24 irtibat noktasının, UHDİGM olarak değiştirilmesi yönünde girişimler bulunmaktadır[596]. Kanaatimizce UHDİGM'in irtibat noktası olarak belirlenmesi adli işbirliğinde tekillik sağlayacak, hem gereksiz bürokrasi ve zaman kaybını ortadan kaldıracak hem de yürütülen faaliyetler kapsamında edilen tecrübe ve birikimlerin tek elde toplanması sayesinde daha verimli işbirliği uygulamalarına zemin hazırlayacaktır.

Son olarak belirtmek gerekir ki; Sözleşme'nin gerekliklerinin tam olarak yerine getirilmemiş olması ve yapısal eksikliklere rağmen, siber suçlarla mücadelede Türk uygulamasının, uygulamacıların istekli ve çözüm odaklı yaklaşımları sayesinde genel olarak iyi bir durumda olduğu söylenebilir[597].

---

[593] *"Bilişim teknolojileri kullanılarak işlenen suçların soruşturulması ve dijital delillerin incelenmesi için destek veren görevli daire başkanlıklarının ve taşra teşkilatındaki birimlerin dağınık yapısının tek bir çatı altında toplanması, mükerrer yatırımların önüne geçilmesi, siber suçlarla mücadelenin etkin ve verimli olarak yürütülmesini sağlamak amacıyla 2011/2025 sayılı Bakanlar Kurulu Kararı ile Emniyet Genel Müdürlüğü bünyesinde Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. 28/02/2013 tarih ve B.05.1.EGM.0.65.35539/31772 sayılı Bakanlık Oluruna istinaden Bilişim Suçlarıyla Mücadele Daire Başkanlığının ismi Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir Siber Suçlarla Mücadele İl Şube Müdürlüklerinin kurulumunun tamamlanmasına yönelik çalışmalarına hızla devam edilmektedir"*. (erişim: 11.09.2015), http://www.egm.gov.tr/sayfalar/sibersuclarlamucadeledairebaskanligi.aspx.

[594] Türkiye 7/24 irtibat noktasını ve iletişim bilgilerini şu şekilde beyan etmiştir: Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı, Kızılırmak Mah. Anadolu Bulvarı 2185. Sokak No: 14, 06520, Söğütözü- Çankaya/Ankara, Tel: 00903122869300 Faks: 00903122869206, FCT: 0090505318009, E-Posta: siber@egm.gov.tr.

[595] "The mutual legal assistance provisions of the Budapest Convention on Cybercrime", s. 123.

[596] Dülger, Bilişim Suçları, s. 204.

[597] Önok, "Avrupa Konseyi Siber Suç Sözleşmesi",.s 1248; Murat Volkan Dülger/Gözde Modoğlu, Bilişim Suçlar, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi, Türk Ceza Adalet Sisteminin Etkinliğin Geliştirilmesi Avrupa Birliği /Avrupa Konseyi Ortak Programı, 2015, s. 163.

SONUÇ

İnternet başta olmak üzere bilişim teknolojileri hayatın hemen her alanının vazgeçilmez bir parçası haline gelmiştir. Neredeyse içinde yaşadığımız fiziki alem kadar bağımlı olduğumuz siber alem, sunduğu olanakların yanında bazı riskleri de beraberinde getirmektedir. Bu riskler arasında en tehlikeli grubu, bilişim sistemleri aracılığıyla ya da bu sistemlere kaşı işlenen suçlar oluşturmaktadır. Siber suç adını verdiğimiz bu nispeten yeni suçluluk türü, bilişim teknolojilerinin gelişim hızına paralel olarak, hem sayıca hem nitelik itibariyle sürekli artmakta ve önemli bir güvenlik sorunu teşkil etmektedir.

Siber suçların, teknik özellikleri dolayısıyla bu suçların soruşturulmasında geleneksel araçlar ve yaklaşımlar yetersiz kalmaktadır. Bu teknik özelliklerden öne çıkanlar; siber alemde olguların ve işlemlerin fiziksel karşılığının bulunmaması, işlemlerin alışılmadık ölçüde hızlı gerçekleşmesi, buna bağlı olarak birim zamanda gerçekleşen işlem sayısının fazlalığı, suç faillerinin anonim kalma şansı ve en önemlisi siber alemin sınır tanımayan bir yapıda olmasıdır. Siber suçlarla mücadelenin başarılı olabilmesi için, bu teknik özelliklerin farkında olarak yürütülmesi gerekmektedir. Bu kapsamda ulusal mevzuatların yeterli bir şekilde koruma sağlaması atılması gereken ilk adımdır. Ancak siber suçlarla mücadele edilmesi için asıl önemli adım, uluslararası işbirliğinin sağlanmasıdır. Siber suçlar, sınır aşan yapıları itibariyle global bir tehdit oluşturmaktadır. Bu tehdide verilecek cevap da global olmalıdır. Aksi halde farklı devletler tarafından ulusal düzeyde birbirinden bağımsız olarak yürütülen mücadele etkisiz ve anlamsız kalacaktır.

Uluslararası toplumu oluşturan devletlerin ve ulusüstü yapıların siber suçlara karşı yürüteceği global mücadele -yani adli işbirliği- en azından şu üç unsuru içermelidir: Birincisi, tüm devletlerin ulusal mevzuatlarının belirli bir minimum yeterliliğe sahip olması sağlanmalıdır. Çünkü, siber suçlar siyasi ve coğrafi sınırlardan etkilenmemekte; dünyanın herhangi bir yerinde bir devletin ulusal mevzuatı itibariyle gerekli önlemleri almamış olan ve siber suçlarla gereğince mücadele etmeyen devletler, siber suçlular için bir suç cenneti ve sığınma limanı oluşturmakta; bu durumdan doğan riskler tüm uluslararası toplumu etkilemektedir.

İkinci olarak, siber suçlar konusunda teknik yardımlaşma ve bilgi paylaşımı sağlanmalıdır. Üçüncüsü farklı devletlerin sınırları içerisindeki unsurların dahil olduğu siber soruşturmalarının etkin bir şekilde yürüyebilmesi için adli yardımlaşma mekanizmaları tesis edilmeli, en geniş kapsamda ve en etkili şekilde yardımlaşma sağlanmalıdır.

Siber suçlarla mücadelenin en önemli ve kaçılmaz unsurunun uluslararası adli işbirliği olduğu konusunda görüş birliği olmasına rağmen, uygulamada hem ulusal mevzuatlardan hem uluslararası hukuktan kaynaklı nedenlerle hem de farklı hukuk sistemlerinin doğaları gereği uyum direnci göstermeleri dolayısıyla istenilen düzeyde adli işbirliği sağlanamamaktadır. Özellikle adli yardımlaşma konusunda, alışılagelmiş klasik ve hantal yöntemler siber suçlara ilişkin yardımlaşma ihtiyaçlarına cevap verememektedir. Adli işbirliği sağlanması noktasındaki mutlak ihtiyaç ve bunun karşısında hukuki ve yapısal eksiklikler dolayısıyla istenilen işbirliğinin sağlanamaması karşısında pek çok ulus üstü siyasi veya sivil örgüt, siber suçlara karşı işbirliğini kurmaya ve geliştirmeye yönelik girişimlerde bulunmuştur. Bu girişimlerden en önemlisi Avrupa Konseyi Siber Suçlar Sözleşmesi'dir.

Avrupa Siber Suçlar Sözleşmesi üç temel amacı gerçekleştirmek üzere kabul edilmiştir: 1) Bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmak; 2) Siber suçların soruşturulması açısından, siber aleme uygun düşen ortak usul kurallarını tanımlayarak, devletler arasındaki muhakeme kurallarının yeknesaklaştırılmak; 3) Hem geleneksel hem de yeni türden uluslararası işbirliği yöntemleri belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını temin etmek. Esasında Sözleşme'nin bir tek amacı olduğu söylenebilir: Siber suçlarla mücadelede etkin adli işbirliğini sağlamak.

Sözleşme'nin adli işbirliğini sağlama noktasındaki önceliği, ulusal mevzuatların yeterli hale getirilmesi ve uyumlulaştırılmasıdır. Zira kendileri yeterli olamayan hukuk sistemlerinin, işbirliği içinde olmaları da mümkün ve anlamlı olmayacaktır. Ayrıca suçluların iadesi, adli yardımlaşma gibi en önemli adli işbirliği araçlarının gerçekleştirilmesi ulusal mevzuatların yeterli ve uyumlu olmasına bağlıdır. Bu itibarla Sözleşme'nin ulusal mevzuatlara yönelik getirdiği yükümlülükler adli işbirliğine yönelik hazırlık hareketleri değil, bizatihi Sözleşme'nin kurmaya çalıştığı adli işbirliği rejiminin kendisidir. Zaten Sözleşme, adli işbirliği konusunda yeni bir düzen getirmemekte, mevcut işbirliği

mekanizmalarının sürdürülmesini ve siber suçlarla mücadele konusunda etkin bir şekilde işletilmesini öngörmektedir. Sözleşme'nin, uygulanabilir işbirliği aracı bulunmayan ve mevcut işbirliği mekanizmalarının yeterli gelmediği hallere yönelik öngördüğü az sayıdaki hüküm dışında adli işbirliğini ayrıntılı olarak düzenlemediği, genel ilkeleri dillendirmekle yetindiği görülmektedir. Bu halde Sözleşme'nin adli işbirliği konusunda asıl önem arz eden kısmının ulusal mevzuatlara yönelik getirdiği önlemler olduğu söylenebilir.

Sözleşme'de ulusal mevzuatlarda suç olarak tanımlanması gerektiği belirtilen 9 suç tipi, taraf devletlerde bu suçların cezasız kalmamasını sağlayacaktır. Bunun yanında adli yardımlaşma ihtiyacı söz konusu olduğunda, geleneksel olarak aranan karşılıklı cezalandırılabilirlik şartının sağlanması ve yardımlaşmanın mümkün olması önemli bir kazanımdır. Bu nedenle devletlerin iç hukuklarında Sözleşme'de yer alan suç tiplerine, öngörüldüğü şekilde yer vermeleri, sağlanmak istenen adli yardımlaşma ve genel olarak adli işbirliği sisteminin önemli bir parçasıdır. Taraf devletlerin ulusal ceza mevzuatlarının büyük ölçüde Sözleşme'deki suç tipleriyle uyum içinde olduğu görülmektedir ve bu Sözleşme'nin önemli bir başarısıdır.

Sözleşme'de öngörülen usuli tedbirler, siber suç soruşturmalarında yaşanan sorunlara çözüm sunulması amacıyla geliştirilmiş olup, hem siber suç soruşturmalarını hem de delilleri elektronik ortamda bulunan tüm suçlara ilişkin soruşturmaları kapsamaktadır. Bu usuli tedbirlerin doğru bir şekilde benimsenmesi ve uygulanması siber alemde yürütülen suç soruşturmaları bakımından vazgeçilmez önemdedir. Özellikle, siber alemin yapısı dikkate alınarak, klasik muhakeme tedbirlerinden farklı bir yaklaşımla düzenlenmiş olan depolanmış verilerin süratli şekilde korunmasına ilişkin tedbirler, hem güvenlik hem de hak ve özgürlükler noktasında koruma sağlayan etkili çözüm araçlarıdır. Ancak taraf devletlerin çoğunluğun bu yeni tür muhakeme tedbirlerini doğru şekilde yorumlamadıkları ve ulusal mevzuatlarında bu tedbirlere yer vermedikleri görülmektedir. Taraf devletlerin bu noktada sözleşmesel yükümlülüklerini yerine getirmemeleri ve bu tedbirleri kabul eden az sayıdaki devlette de uygulamasının çok nadir olması Sözleşme'nin kurmaya çalıştığı işbirliği rejiminin en büyük başarısızlığıdır.

Türkiye'nin, Sözleşme'nin düzenlediği suç tiplerini benimsemek ve mevzuatını buna göre uyumlulaştırmak noktasında yeterli bir görüntü sergilediği söylenebilir. Ancak, öngörülen muhakeme tedbirleri noktasında tam aksine bir tablo söz

konusudur. Türkiye, Sözleşme'de düzenlenen muhakeme tedbirlerinin neredeyse hiçbirini tam olarak benimsemiş olmadığı gibi, ülkemizde bu yönde bir kanun çalışması da mevcut değildir. Kanaatimizce acilen bu konuda gerekli düzenlemelerin yapılması gerekmektedir.

Sözleşme, ulusal mevzuatların yeterli ve uyumlu hale getirilmesi dışında doğrudan doğruya adli işbirliği ve yardımlaşmaya ilişkin hükümler de içermektedir. Sözleşme bağımsız bir adli işbirliği sistemi getirmek yerine, mevcut sistemlerin uygulanmasını tercih etmiştir. Bunun yanı sıra, uygulanabilir bir adli yardımlaşma zemini – uluslararası sözleşme veya iç hukuk normu- bulunmadığı durumlarda uygulanacak rejimi belirlemek üzere yedek normlar konulmuştur. Sözleşme'de bunun dışında bazı özel yardımlaşma usulleri düzenlenmiş olup, aslında bunlar ulusal düzeyde tesis edilmesi gereken muhakeme tedbirlerinin, uluslararası adli yardımlaşma hukukundaki yansımalarından ibarettir. Bu tedbirler, ulusal düzeyde doğru bir şekilde tesis edilmiş olmaları halinde, konu sınırlaması getirmeyen mevcut adli yardımlaşma sözleşmeleri çerçevesinde zaten uygulanabilecektir. Sözleşme yalnızca, uluslararası ya da ulusal mevzuatın herhangi bir hükmünün söz konusu adli yardımlaşma yollarını yasaklaması ihtimaline binaen, garantör hükümler getirmektedir.

Sözleşme, adli yardımlaşma konusunda benimsediği ikincil nitelikte olma ilkesi dolayısıyla, uygulamada beklenen şekilde bir işlerlik sağlayamamaktadır. Özellikle depolanmış verilerin korunması konusunda adli yardımlaşma uygulaması yok denecek kadar azdır. Bu sorunun çözümü öncelikli olarak ulusal düzeyde bu tedbirlerin tesis edilmesi ve uygulanmasıdır.

Sözleşme'nin adli işbirliği noktasında getirdiği en önemli düzenleme 7/24 iletişim ağıdır. Taraf devletlerin Sözleşme'yle ilgili her konuda teknik ve hukuki bilgi paylaşımı sağlaması ve bazı durumlarda adli yardımlaşma işlemlerinin gerçekleştirilmesiyle görevli 7 gün 24 saat ulaşılabilir durumda olan irtibat noktaları belirlemeleri yükümlülüğü, siber suçlar bakımında oldukça yerinde bir uygulamadır. Türkiye, 7/24 irtibat noktası olarak Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'nı belirlemiştir. Daire, istenilen düzeyde olmasa da, özellikle polisiye işbirliği noktasında irtibat noktası olarak görevini yerine getirmektedir.

Türkiye, Sözleşme'nin usul hukukuna ilişkin alınmasını şart koştuğu önlemleri almamış olmakla, bu konularda adli yardımlaşma da gerçekleştirememektedir. Dolayısıyla ülkemizin bu konudaki eksikliği yalnızca ulusal düzeydeki uygulamayı değil, adli yardımlaşmayı da olumsuz etkilemektedir. Bu konuda ceza muhakemesi hukukunda gerekli değişiklikler yapıldığında, kanun hükmünde olması itibariyle doğrudan uygulanabilir nitelikte olan Sözleşme'nin adli yardımlaşma hükümleri, gerekli hukuki zemini sunacak ve bu konularda adli yardımlaşma sağlanabilecektir. Adli işbirliği ve özel olarak adli yardımlaşma konularında olumlu bir tutum içinde olduğu değerlendirilen Türkiye'nin, Sözleşme'yle uyumluluğu sağlamak adına gerekli hukuki ve yapısal düzenlemeleri yapması gereklidir.

KAYNAKÇA

Aksoy, Emine Eylem. "Siber Suçluluğa Dair Sözleşme", **Prof. Dr. Kemal Oğuzman'a Armağan**, 2002, 869-896.

Aldesco, Albert. "The Demıse Of Anonymıty: A Constıtutıonal Challenge To The Conventıon On Cybercrıme", **Loyola of Los Angeles Entertainment Law Review**, sy. 23, 2003, 81-123.

Analay, Cengiz/Gülşen, Recep. "Bilişim Suçu Olarak Pornografi" (Erişim: 20.07.2015) http://turk.internet.com/haber/yazigoster.php3?yaziid=11007.

Artuk, Mehmet Emin/Gökçen, Ahmet/Yenidünya, Caner. **Ceza Hukuku Genel Hükümler**, 8. Baskı, Ankara: Adalet, 2014.

Artuk, Mehmet Emin/Gökçen, Ahmet/Yenidünya, Caner. **Ceza Hukuku Özel Hükümler**, 13. Baskı, Ankara: Adalet, 2013.

Avrupa Parlamentosu için Komisyon Raporu, "Towards a general policy on the fight against cyber crime (COM(2007)267 final).

Avrupa Siber Suçlar Sözleşmesi Açıklayıcı Rapor, (erişim: 17.07.2015), http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

Benvenisti, Eyal/Downs, George W. "Court Cooperation, Executive Accountability and Global Governance", **Nyuj Int'L L. & Pol.**, sy, 51, 2009, 931-958.

Biddle, Peter/England, Paul/Peinado, Marcus/Willman, Bryan. "The Darknet and the Future of Content Distribution", **Microsoft Corporation Yayınları**, (erişim: 04.07.2015), http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokole Açıklayıcı Rapor.

Bonicci, Jeanne Pia Mifsud. **Self Regulation in Cyberspace**, Leiden: Asser Press, 2008.

Brenner, Susan. "Approaches to Cybercrime Jurisdiction", **Journal of High Technology Law**, sy. 4, 2004, 1-50.

Brenner, Susan. "Law, Dissonance, And Remote Computer Searches", **North Carolina Journal of Law & Technology**, sy 14, 2012, 43-92.

Brenner, Susan. "Private-Public Sector Cooperation in Combating Cybercrime: In Search of a Model", **Journal of International Commercial Law and Technology**, sy. 2/2, 2007, 58-67.

Brenner, Susan. "Toward a Criminal Law for Cyberspace: Distributed Security", **Boston University Journal of Science & Technology Law**, sy. 10, 2004, 1-104.

Brenner, Susan. "Transnatioanl Investigation of Cybercrime", **Cybercrime and The Law: Challenges, Issiues and Outcomes**, New Jamsphire: University Press of New England, 2012, 170-188.

Brenner, Susan/Schwerha, Joseph J. "Transnational Evidence Gathering And Local Prosecution of International Cybercrime", **Journal of Computer & Informatıon Law**, sy. 20, 2002, 347-396.

Buono, Laviero. "Gearing Up The Fight Against Cybercrime in The European Union: A New Set Of Rules And The Establishment Of The European Cybercrime Centre (Ec3)", **New Journal of European Criminal Law**, sy 3., 2012, 332-343.

Cade, Nicholas W. "An Adaptive Approach For An Evolving Crime: The Case For An International Cyber Court And Penal Code", **Brook. J. Int'l L**., sy 37, 2011, 1139-1175.

Calderoni, Francesco. "The European legal framework on cybercrime: striving for an effective implementation", **Crime Law Soc Change**, 2010, 339- 355.

Cangemi, Daniele. "Procedural Law Provisions of the Council of Europe Convention on Cybercrime**", International Review of Law of Computer and Technology**, sy, 18/2, 2004.

"Capacity Building Programs on Cybercrime", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 1 Kasım 2013.

Cardozo, Nate. "What Were They Thinking? Microsoft Seizes, Returns Majority of No-IP.com's Business", **Electronic Frontier Foundation** (Erişim: 10.07.2015), http://www.eff.org/deeplinks/2014/07/microsoft-and-noip-what-were-they-thinking.

Centel, Nur / Zafer, Hamide. **Ceza Muhakemesi Hukuku**, 11. Baskı, İstanbul: Beta, 2014.

Cerezo, Ana I./Lopez, Javier/Patel, Ahmed. "International Cooperation to Fight Transnational Cybercrime", **2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA,** 2007, 13-27.

Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi Açıklayıcı Raporu.

Chertoff, Michael / Simon, Tobby. "The Impact of the Dark Web on Internet Governance and Cyber Security", **Global Commission on Internet Governance**, Centre for International Governance Innovation and the Royal Institute for International Affairs, (erişim: 04.07.2015), https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf.

Clayton, Richard/Moore, Tyler/Christin, Nicolas. Concentrating Correctly on Cybercrime Concentration, Proceedings of the **Forteenth Workshop on the Economics of Information Security**, Delft, 2015.

Conway, Gerard. The Council of Europe as a Normative Backdrop to Potential European Integration in the Sphere of Criminal Law, **The Denning Law Journal**, sy. 19, 2007, 123-148.

Csonka, Peter. "The Council of Europe's Convention on Cyber-Crime and Other European Initiatives", **Revue İnternationale De Droit Pénal**, sy. 77, 2006, 473-501.

Currie, Robert J. "Peace And Public Order: International Mutual Legal Assistance:The Canadian Way", **Dalhousie Journal of Legal Studies**, sy. 7, 1998, 91-124.

Çeken Hüseyin, "Council of Europe's Convention on Cybercrime and Turkey", Marmara Üniversitesi Avrupa Topluluğu Ensitüsü, Yüksek Lisans Tezi.

Danca, Dana. "Cyber Diplomacy - A New Component of Foreign Policy", **Journal of Law and Administrative Sciences**, sy. 3, 2015, 91-97.

Demibaş, Timur. Ceza Hukuku Genel Hükümler, 10. Baskı, Ankara: Seçkin, 2014.

Dülger, Murat Volkan. "Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler", **İstanbul Barosu Dergisi,** sy.4, 2004, s. 1485-1486.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku,** 5. Baskı, Ankara: Seçkin, 2014.

Dülger, Murat Volkan. **Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)**, Ankara, Seçkin, 2014.

Dülger, Murat Volkan. **Suçtan Kaynaklanan Mal Varlığı Değerlerinin Aklanmasına İlişkin Suçlar ve Yaptırımlar**, Ankara, Seçkin Yayıncılık, 2011.

Elholm, Thomas. "Does EU Criminal Cooperation Necessarily Mean Increased Repression?",**European Journal of Crime**, Criminal Law and Criminal Justice, sy. 17, 2009, 191-226.

European Evidence Warrant, Summaries of European Union Legistlation, (erişim 01.08.2015), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:jl0015.

Fahey, Elaine. "The EU's Cybercrime and Cyber-Security Rulemaking : Mapping the Internal and External Dimensions of EU Security", **European Journal of Risk Regulation**, sy.1, 2014, 46-60.

Filazi, İbrahim. "İnternetin Yeraltı Dünyası: DeepWeb", (erişim: 04.07.2015), http://www.ifilazi.net/deepweb.html.

Foggetti, Nadina. Transnational Cyber Crime, Differences Between National Laws and Development of European Legislation: by Repression?", **Masaryk University Journal of Law and Technology,** sy. 2, 2008, 31-45.

Forsyth, James/Pope, Billy "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace", **Strategic Studies Quarterly**, Winter, 2014.

Goldsmith, Jack. "The Internet and the Legitimacy of Cross-Border Searches", **Chicago Public Law and Legal Theory**, (erişim: 07.07.2015)http://www.law.uchicago.edu/academics/publiclaw/resources/16.JG.Internet.pdf.

Goodman, Marc / Brenner, Susan. "Emerging Consensus on Criminal Conduct in Cyberspace", **International Journal of Law and Information Technology**, sy. 10/2, 2002.

Grabosky, Peter. "Requirements of Prosecution Services to Deal With Cyber Crime", **Crime Law Soc Change**, sy. 47, 2007, 201-223.

Gürol, Candaş. "Uluslararası Ceza Hukukunda Adli Yardımlaşma", **İstanbul Barosu Dergisi**, sy. 84/3, 2010, 1685-1721.

Hallevy, Gabriel. "The Criminal Liability of Artificial Intelligence Entities", **Social Sicence Research Network**, (erişim: 06.07.2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1564096 .

Hallevy, Gabriel. "Criminal Liability of Artificial Intelligence Entities - From Science Fiction to Legal Social Control", **Akron Intellectual Property Journal**, sy 4, 2010.

Hamano, Masaki. Comparative Study in the Apporach to Jurisdiction in Cyberspace, (erişim 03.07.2015), http://www.oocities.org/siliconvalley/bay/6201/.

Havuz, Serdar. "Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği", Yüksek Lisans Tezi, Harp Akademileri Stratejik Araştırmalar Enstitüsü Müdürlüğü, 2007.

Henkoğlu, Türkay. **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, İstanbul: Pusula Yayıncılık, 2011.

Hiller, Janine S. "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets", **Santa Clara High Technology Law Journal**, sy 31, 2015, 162-214.

Hopkins, Shannon L. "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", **Journal of High Technology Law**, sy. 2, 2003, 101-122.

"How FBI brought down cyber-underworld site Silk Road", USA Today, (erişim: 04.07.2015), http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

"Implementation of the preservation provisions of the Budapest Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 25 Ocak 2013.

"International Cooperation under the Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 18 Ağustos 2009.

İçel, Kayıhan. "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında " Avrupa Siber Suç Politikasının Ana İlkeleri", **İÜHFM**, sy. 59, 2001.

Jamet, Denis L. "What Do Internet Metaphors Reveal About The Perception Of The Internet?", s. 19 (erişim: 12.06.2015), http://www.metaphorik.de/sites/www.metaphorik. de-/files/ journal-pdf/18_2010_jamet.pdf.

Jamil, Zahid. "Cybercrime Model Laws", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu,9 Kasım 2014.

Kadir, Rizgar Mohammed. "The Scope and the Nature of Computer Crimes Statutes -A Critical Comparative Study", **German Law Journal**, sy. 11/6, 2010, 639-632.

Karagülmez, Ali. **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Üçüncü Baskı, Ankara: Seçkin, 2011.

Kaspersen, Henrique. "Cybercirme and Internet Jurisdiction", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 5 Mart 2009.

Kaya, Mehmet Bedii, **Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi**, İstanbul: On İki Levha, Şubat 2010.

Keyser, Mike. "The Council of Europe Convention on Cybercrime", **Journal of Transnational Law and Policy**, sy. 12, 2003, 287-326.

Klimek, Libor. "Combating Attacks Against Information Systems", **Masaryk University Journal of Law and Technology**, sy.6, 2012, 87-99.

Klosek, Jacqueline. "The Development of International Police Cooperation within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof", **American University International Law Review**, sy. 14/3, 1999, 599-656.

Koca, Mahmut. "Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları", **Prof. Dr. Ali Güzel'e Armağan**, C. II, İstanbul, 2010, 1651-1660.

Koca, Mahmut/Üzülmez, İlhan. **Türk Ceza Hukuku Genel Hükümler**,7. Baskı, Ankara: Seçkin, 2014.

Kocasakal, Ümit. **Avrupa Birliği Ceza Hukuku'nun Esasları**, İstanbul: Vedat Kitapçılık, 2004.

Lewis, Brian C. "Preventıon Of Computer Crıme Amıdst Internatıonal Anarchy", **Amerıcan Crımınal Law Revıew**, sy. 41, 2015, 1353-1372.

Mahmutoğlu, Fatih S. "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, sy.1/2, 2001.

Mahmutoğlu, Fatih Selami. Suçluların Geri Verilmesi, **70. Yılında Türk Ceza Kanunu - Genel Hükümler**, İstanbul, 1998, s. 66

Malmir, Mahmoud/Neshastehriz, Sohrab. "Identify the Characteristics of Cyber Space Facilitator in Relation to Committing a Crime", **Int. J. Rev. Life. Sci.,** sy. 5/3, 183-191.

Mason, Stephen. **International Electronıc Evidence**, London: British Institute of International and Comparative Law, 2008.

Mazanec, Brian M. "Why International Order in Cyberspace Is Not Inevitable", **Strategic Studies Quarterly**, Summer, 2015.

Memiş, Pınar. "İnternet ve Ceza Hukuku: Fransa Örneği",**Prof. Dr. Çetin Özek Armağanı,** 2004, 597-609.

Memiş Kartal, Pınar. "Evidence and Proof of Cybercrime in Turkish Law", **Kazancı Hakemli Hukuk Dergisi**, sy.93-94, 2012, 109-116.

Memiş, Tekin. "İnternet Ortamında Haksız Rekabet Halleri ve Türk Hukuku", **İnternet ve Hukuk**, Der: Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004.

Mıquelon, Mırıam F. "The Conventıon On Cybercrıme: A Harmonızed Implementatıon Of International Penal Law :What Prospects For Procedural Due Process?", **Journal Of Computer & Informatıon Law**, sy 23, 2005, 329-362.

"Milyarlarca saatlik dinleme gömülecek", Milliyet Gazetesi, (erişim: 27.08.2015), http://www.milliyet.com.tr/milyarlarca-saatlik-dinleme-gundem-1989484/.

Modiga, Georgeta. "Importance And Necessity of International Judicial Cooperatıon in Criminal Matters", **International Journal of Juridical Sciences**, sy.1 , 2014, 98-103.

Murray, Andrew. **Information Technology Law: The Law and Society**, 2. Baskı, London: Oxford, 2013.

Nunziato, Dawn C. **Net Neutrality and Free Speech in The Internet Age**, California: Stanford Law Books, 2009.

Odlyzko, Andrew. "The Internet and other networks: utilization rates and their implications", **Information Economics and Policy**, sy. 12/4, 2000, 341-365.

Olteanu, Andreea Verte. "Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime", **Journal Of Eastern-European Criminal Law**, sy. 1, 2014, 84-96.

Öktem, Niyazi/Türkbağ, Ahmet Ulvi. **Felsefe, Sosyoloji, Hukuk ve Devlet**, İstanbul: Der Yayınları, 2011.

Önok, Murat. "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Prof.Dr. Nur Centel'e Armağan, MÜHFHAD,** sy. 19/2, 1229-1269.

Özbek, Mücahid. "The Impacts of European Cybercrime Convention on Turkish Criminal Law", **GSI Articletter Law Review**, s. 13, 2015, s. 68-79.

Özbek, Veli Özer. "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, sy. 4/1, 2002, 101-158.

Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker. **Ceza Muhakemesi Hukuku,** , 6. Baskı, Ankara: Seçkin, 2014.

Pagallo, Ugo. **The Laws of Robots: Crimes, Contracts, and Torts**, London: Springer, 2013.

Paust, Jordan. "Cybercrimes and the Domestication of International Criminal Law", **Santa Clara Journal of International Law**, sy. 5/2, 2007, 432-444.

Pazarcı, Hüseyin. **Uluslararası Hukuk**, Ankara: Turan Kitabevi, Haziran 2014.

Peta, Cezar. "Community and National Structures for Police and Judicial Cooperation", **Public Security Studies**, sy. 3, 2014, 267-275.

Picotti, Leronzo. "National Legistlation Implementing the Convention on Cybercrime- Comperative Anlaysis and Good Practices", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Tartışma Raporu, 28 Ağustos 2008.

Podgor, Ellen. "International Computer Fraud: A Paradigm For Limiting National Jurisdiction", **University of California Davis Law Review**, s. 35, 2012, 267-317.

Pradillo, Ortiz. "Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain", **European journal of Crime**, sy, 19, 2012, 363-395.

"Preparation by the T-CY of a draft Additional Protocol to the Convention on Cybercrime (ETS 185) regarding transborder access to data", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 16 Mayıs 2013.

Renda, Andrea. "Cybersecurity and Internet Governance", **Council on Foreign Relations**. (Erişim: 03.05.2013), http://www.cfr.org/cybersecurity/cybersecurity-internet-governance/p30621.

Reno, Janet. United States Attorney General, Keynote Address at the Meeting of the G8 Senior Experts' Group on Transnational Organized Crime, (erişim 11.07.2015), http://www.usdoj.gov/criminal/cybercrime/agfranc.htm.

Roderic Broadhurst, "Developments in the global law enforcement of cyber-crime", **Policing: An International Journal of Police Strategies & Management**, sy. 29/3, 2006, 408-433.

Rosenzweig, Paul. "The Internatıonal Governance Framework For Cybersecurity", **Canada-Unıted States Law Journal**, sy. 37, 2012, 405-432.

"Rules on Obtaining Subscriber Information", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3 Kasım 2014.

Schjolberg, Stein. "Harmonizing National Legal Approaches On Cybercrime", **WSIS Thematic Meeting on Cybersecurity**, International Telecomunication Union, 1 Temmuz 2005, (erişim: 17.08.2015), http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

Schjolberg, Stein. **The History of Cybercrime**, Norderstedt: Cybercrime Research Instıtute GmBh, 2014.

Seitz, Nicolai. "Transborder Search: A New Perspective in Law Enforcement", **Yale Law School**, (erişim: 07.07.2015), http://islandia.law.yale.edu/isp/digital%20cops/papers/Seitz_Nicolai.pdf.

Shah, Monica R. "The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace", **Columbia Law Review**, sy. 105, 2015.

Sınar, Hasan. "Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme", **Prof. Dr. Çetin Özek Armağanı**, İstanbul, 2004.

Sınar, Hasan. "New Perspectives on Computer Forensics", **MHB Prof. Dr. Gülören Tekinalp'a Armağan,** 2003.

Sınar, Hasan. **İnternet ve Ceza Hukuku**, İstanbul, 2001.

Sieber, Ulrich. **İnternetteki Suçlar ve Suçun İnternette Takibi**, Ankara: Seçkin, 2014.

Singh, Mrinalini/Singh, Shivam. "Cyber Crime Convention And Trans Border Crımınality", **Masaryk University Journal of Law and Technology**, sy 1., 2007, 53-66.

Sparrow, Andrew. The **Law of Virtual Worldsand Internet Social Networks**, Burlington: Gower, 2010.

Stahl, William M. "The Uncharted Waters Of Cyberspace: Applying The Principles of International Maritime Law To The Problem Of Cybersecurity", **Ga. J. Int'l & Comp. Law Review**, sy. 40, 247-273.

Stein, Sibyl. "Combating Crime in the European Union: The Development of EU Policy after the Convention", **European Journal of Crime, Criminal Law and Criminal Justice**, sy 12/4, 2004, 334-347.

Sulek, David/Moran, Ned. "What Analogies Can Tell Us About the Future of Cybersecurity", **Nato Siber Savunma İşbirliği ve İstihbarat Merkezi, ccdoe.org**, (erişim: 12.06.2015, https://ccdcoe.org/sites/default/files/multimedia/pdf/ 08_SULEK_-What%20Cyber%20Analogies%20Can%20Tell%20Us.pdf).

Şimşek, Kemal. "Uluslararası Adli Yardımlaşma Konusunda Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri Üzerine", **Adalet Dergisi**, sy. 45, 2013, 145-160.

Taşkın, Cankat. "Bilişim Hukuku Uluslararası Uyuşmazlıklar**", Türkiye Barolar Birliği Dergisi**, sy. 85, 2009, 332-372.

Tehrani, Pardis Moslemzadeh/Manap, Nazura Abdul. "A Rational Jurisdiction For Cyber Terrorism", **Computer Law and Security Review**, sy, 29/6, 2013, 207-215.

Tezcan, Durmuş/Erdem, Mustafa Ruhan/Önok, Murat. **Uluslararası Ceza Hukuku**, 2. Baskı, Ankara: Seçkin, 2014.

"The cybercrime legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 27 Şubat 2013.

"The mutual legal assistance provisions of the Budapest Convention on Cybercrime", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3 Kasım 2014.

Thompson, Mary. "Distributed Security Architecture", **Journal Of Computer & Informatıon Law**, sy. 23, 2001.

"Transborder access to data and jurisdiction:Options for further action by the T-CY", Avrupa Konseyi Siber Suçlar Sözleşmesi Komisyonu Değerlendirme Raporu, 3. Ekim 2014.

Tunç, Hasan "Milletlerarası Sözleşmelerin Türk İç Hukukuna Etkisi Ve Avrupa İnsan Hakları Mahkemesinin Türkiye İle İlgili Örnek Karar İncelemesi", (Anayasa Mahkemesi'nin 38. Kuruluş Yıldönümü Nedeniyle Düzenlenen Sempozyumda Sunulan Bildiri), Anayasa Yargısı, sy. 17, 2000.

Türkbağ, Ahmet Ulvi. "Hukuk Eğitiminin Etik Boyutu", **1. Hukuk Eğitimi Kongresi**, 07-08 Kasım 2013, Akdeniz Üniversitesi Hukuk Fakültesi, Ankara: Türkiye Adalet Akademisi Yayınları, 2014.

Ulutaş, Ahmet/Atabey, Ömer Serdar. **Ceza Alanında Uluslararası Adli İşbirliği Hukuku**, Ankara: Adalet, 2011.

UNODC Sekreterliği, "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime", (erişim: 21.08.2015), http://www.unodc.org/documents/crime-congress/12th-CrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf.

UNODC Uzmanlar Grubu Raporu, "Comprehensive Study Of The Problem Of Cybercrime And Responses To İt By Member States, The International Community and The Private Sector", Viyana, 2013.

Vatis, Micheal. "The Council of Europe 's Convention on Cybercrime", **Berkeley Technology Law Journal**, sy. 18, 2014, 207-223.

Velasco, Cristos. "Cybercrime jurisdiction: past, present and future", **ERA Forum**, Springer, 2015, DOI 10.1007/s12027-015-0379-y.

Verdelho, Pedro. "The Effectiveness of International Cooperation Against Cybercrime: Examples of Good Practice", Avrupa Konseyi, Veri Koruma ve Siber Suç Dairesi, Global Project on Cybercrime Raporu, 12 Mart 2008.

Walden,Ian. "Harmonising Computer Crime Laws in Europe", **European Journal of Crime**, Criminal Law and Criminal Justice, sy. 12/4, 2004, 321-336.

Weber, Amalie. "The Council of Europe Convention on Cybercrime", **Berkeley Technology Law Journal,** , sy. 18, 2014, 425-446.

Weil, Prosper. "Le droit international en quête de son identité", **Recueil des Cours de l'Academie de Droit International**, sayı 237, 1992.

Welcome To The Deep Web: The Internet's Dark And Scary Underbelly, Worldcrunch, (erişim: 06.05.2015), http://www.worldcrunch.com/tech-science/welcome-to-the-deep-web-the-internet-039-s-dark-and-scary-underbelly/invisible-internet-tor-onion-network/c4s10150/.

Wennerstrom, Erik. "A Decade of European Legal Developments", **Scandinavian Studies Journal**, sy. 47, 2004, 452-460.

"WikiLeaks:Tor", (erişim: 06.05.2015), https://wikileaks.org/wiki/WikiLeaks:Tor.

Xinbao, Zhang. "Establishing Common International Rules To Strengthen The Co-Operatıon Of Cyber Informatıon Security", **China Legal Science**, sy. 1, 2013, 121-139.

Yenidünya Caner/Değirmenci, Olgun. **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003.

Yenisey, Feridun. "Milletlerarası Ceza Hukukunda Yeni Gelişmeler", **70. Yılında Türk Ceza Kanunu - Genel Hükümler**, İstanbul, 1998, s. 52.

Yenisey, Feridun/Nuhoğlu,Ayşe. **Ceza Muhakemesi Hukuku Ders Kitabı**, 2. Baskı, İstanbul: Bahçeşehir Üniversitesi Yayınları, Ekim 2014.

Yüzbaşıoğlu, Necmi. **Türk Anayasa Yargısında Anayasallık Bloku**, İstanbul: İÜHF Yayınları, 1993.

Zarza, Angeles Gutierrez. **Exchange of Information and Data Protection in Cross Border Criminal Proceedings in Europe**, Springer, 2015

Zavrsnik, Ales. "Cybercrime Definitıonal Challenges And Criminological Particularities", **Masaryk University Journal of Law and Technology,** sy. 2, 2008, 1-30.

ÖZGEÇMİŞ

1989 yılında Ordu'da doğan yazar, 2006 yılında Kayseri Özel Kılıçaslan Lisesi'nden mezun olmuştur. Lisans eğitimini Galatasaray Üniversitesi Hukuk Falütesi'nde gören yazar, 2012 yılında bu programdan mezun olmuştur.

Halen İstanbul Medipol Üniversitesi Hukuk Falüktesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalında Araştırma görevlisi olarak çalışan yazarın "Une Etude sur Les Principes Intangibles de La Constitution Bosnienne", "The Impacts of European Cybercrime Convention on Turkish Criminal Law" adlı yayımlanmış çalışmaları bulunmaktadır.

TEZ ONAY SAYFASI

Üniversite : TC. Galatasaray Üniversitesi

Enstitü : Sosyal Bilimler Enstitüsü
Adı Soyadı : Mücahid ÖZBEK
Tez Başlığı : Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma
Savunma Tarihi: 28.09.2015
Danışmanları : Yrd. Doç. Dr. E. Eylem AKSOY RETORNAZ
Yrd. Doç. Dr. Murat Volkan DÜLGER

JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı	İmza
Doç. Dr. Pınar MEMİŞ KARTAL	
Yrd. Doç. Dr. M. Sinan ALTUNÇ	
Yrd. Doç. Dr. Çağla TANSUĞ	
Yrd. Doç. Dr. E. Eylem AKSOY RETORNAZ	
Yrd. Doç. Dr. M. Volkan DÜLGER	

Enstitü Müdürü
Prof. Dr. M. Yaman ÖZTEK