İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

GELİŞMİŞ İŞ BİRLİĞİ VE ELEKTRONİK KANITLARIN İFŞASINA İLİŞKİN SİBER SUÇ SÖZLEŞMESİNE GETİRİLEN İKİNCİ EK PROTOKOLÜN İNCELENMESİ

Didem COŞKUN
118691010

Dr. Öğr. Üyesi Mehmet Bedii KAYA

İSTANBUL
2022

Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin Siber Suç Sözleşmesine Getirilen İkinci Ek Protokolün İncelenmesi

Analysis of the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence

Didem COŞKUN
118691010

Tez Danışmanı :	**Dr. Öğr. Üyesi Mehmet Bedii KAYA** İstanbul Bilgi Üniversitesi	(İmza) .....
Jüri Üyeleri :	**Prof. Dr. Leyla KESER BERBER** İstanbul Bilgi Üniversitesi	(İmza) .....
	Dr. Öğr. Üyesi Erkan SARITAŞ İstanbul 29 Mayıs Üniversitesi	(İmza) .....

Tezin Onaylandığı Tarih : 17 Ekim 2022
Toplam Sayfa Sayısı : 196

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler (İngilizce)
1) Siber	1) Cyber
2) Suç	2) Crime
3) Sözleşme	3) Convention
4) Protokol	4) Protocol
5) Kanıt	5) Evidence

ÖNSÖZ

Sevgili babama ve anneme armağan…

İÇİNDEKİLER

İKİNCİ BÖLÜM
GELİŞMİŞ İŞ BİRLİĞİ VE ELEKTRONİK KANITLARIN İFŞASINA İLİŞKİN İKİNCİ EK PROTOKOL

KISALTMALAR

1. Ek Protokol	**:**	Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Konseyi Siber Suç Sözleşmesi'ne Ek Protokol
2. Ek Protokol	**:**	Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin Avrupa Konseyi Siber Suç Sözleşmesi'ne İkinci Ek Protokol
AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
A.g.e.	:	Adı Geçen Eser
Bkz.	:	Bakınız
BM	:	Birleşmiş Milletler
BTK	:	Bilgi Teknolojileri Kurumu
C.	:	Cilt
CDPC	:	The European Committee on Crime Problems (Avrupa Suç Sorunları Komitesi)
EDPB	:	European Data Protection Board (Avrupa Veri Koruma Kurulu)
INTERPOL	:	The International Criminal Police Organization (Uluslararası Kriminal Polis Teşkilatı)
IP	:	Internet Protokol (İnternet Protokolü)
ISO	:	International Organization for Standardization (Uluslararası Standardizasyon Örgütü)
İÜHFM	:	İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
KVKK	:	6698 Sayılı Kişisel Verilerin Korunması Kanunu
m.	:	Madde
MÜHFHAD	:	Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi
ODTÜ	:	Orta Doğu Teknik Üniversitesi

OECD	:	Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İş Birliği Örgütü)
PACE	:	Parliamentary Assembly of the Council of Europe (Avrupa Konseyi Parlamenterler Meclisi)
s.	:	Sayfa
Sy.	:	Sayı
T-CY	:	The Cybercrime Convention Committee (Siber Suç Sözleşmesi Komitesi)

ÖZET

Bilişim teknolojilerinin sağladığı imkanlar suçun işleniş biçiminde kolaylığa ve suçun işleniş şekillerinde çeşitliliğe sebep olmakta, failler suç işlerken teknolojinin sunduğu imkanlardan yararlanabilmektedir. Yalnızca siber suçlar değil, diğer pek çok suçun soruşturulması ve kovuşturulmasında ihtiyaç duyulan veriler bilişim ortamında bulunmaktadır ve çoğunlukla bu veriler farklı ülkelerdeki hizmet sağlayıcılar veya diğer kuruluşların bünyesinde ya da kontrolünde bulunmaktadır. Bu tür verilerin kolaylıkla saklanabilmesi, yok edilebilmesi ve değiştirilebilmesi mümkündür. Bu durum karşısında adaleti tesis edebilmek için ilgili birimlerce kanıtlara ivedi bir şekilde ulaşılması gerekmektedir.

Avrupa Konseyi Siber Suç Sözleşmesi siber suçlarla mücadelede en önemli enstrümanlardan biri olarak kabul edilmektedir. Bu çalışma ile Sözleşmeye getirilen Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin İkinci Ek Protokol incelenecektir. Bu Protokol, suçlara ilişkin soruşturma ve kovuşturma süreçlerinde ihtiyaç duyulan ve farklı ülkelerde bulunan elektronik kanıtların edinilebilmesi için öngörülen gelişmiş iş birliği önlemlerini, şartları ve teminatları düzenlemekte ve pek çok yenilik getirmektedir.

Bu çalışma ile öncelikle Sözleşme hakkında bilgi verilecek, ardından Protokol ile Sözleşmeye ne tür düzenlemeler getirildiği ve bu düzenlemelerin ne tür özellikleri ihtiva ettiği incelenecek ve değerlendirilecektir.

Anahtar Kelimeler: Siber, Suç, Sözleşme, Protokol, Kanıt

ABSTRACT

Opportunities provided by information technologies cause diversity and ease in the way the crime is committed, and the perpetrators can benefit from the opportunities offered by technology while committing crimes. The data that are needed to investigate and prosecute not only cybercrimes, but also other types of crimes are stored in the cyber environment, and mostly these data are within or under the control of service providers, and other organizations in different countries. Such data can be easily hidden, destroyed, and changed. In order to establish justice under these circumstances, it is necessary to reach the evidence immediately by the relevant units.

The Council of Europe Convention on Cybercrime is considered one of the most important instruments in the fight against cybercrime. This study will examine the Second Additional Protocol on Enhanced Cooperation and Disclosure of Electronic Evidence that is brought to the Convention. This Protocol regulates the advanced cooperation measures, conditions and safeguards required for the acquisition of electronic evidence from different countries that are needed in the investigation and prosecution process, and brings many innovations.

With this study, firstly the Convention will be explained, then the Protocol will be examined and evaluated in regard to the regulations that the Protocol contains, and its contributions to the Convention.

Keywords: Cyber, Crime, Convention, Protocol, Evidence

GİRİŞ

Bilgi ve iletişim teknolojilerinin günden güne gelişmesinin ve kullanımındaki artışın pek çok kolaylaştırıcı etkisi olmasının yanında, suçların işleniş şekillerinde çeşitlenmeye ve bu araçlar kullanılarak işlenen suçlar dolayısıyla kişi ve birimlere de olumsuz etkisi bulunmaktadır. Son yıllarda bu tür suçların sayısında oldukça fazla artış yaşanmakta, çok sayıda mağduriyete sebep olunmaktadır. Bazı suçlar siber yollarla işlenebilirken, siber yollarla işlenmeyen suçlara ilişkin kanıtlar da siber alemde mevcut olabilmektedir. Suçluların ve suça ilişkin verilerin, zararın meydana geldiği ülkelerin sınırlarının dışında olması, suça ilişkin etkin soruşturma ve kovuşturmanın mümkün olabilmesi için uluslararası etkin iş birliğini zaruri hale getirmektedir. Elektronik kanıtları iletmek için sınır ötesi araçlar oluşturmanın nihai amacı, yalnızca kanıtları erişilebilir kılmak değil, aynı zamanda kanıtların mahkeme önünde güvenilirliğini ve kabul edilebilirliğini korumaktır.

Suça ilişkin soruşturma ve kovuşturmada etkin uluslararası iş birliğini sağlayan en kapsamlı enstrümanlardan biri Avrupa Konseyi Siber Suç Sözleşmesidir. Sözleşmenin eleştirilen yönleri mevcuttur, zira 2001 yılında düzenlenmiştir. Ortaya çıkan ihtiyaçların bir sonucu olarak Siber Suç Sözleşmesine Gelişmiş iş Birliği ve Elektronik Kanıtların İfşasına İlişkin İkinci Ek Protokol getirilmiştir. Sözleşmeye getirilen İkinci Ek Protokol'ün içeriği ve getirdiği yenilikler bu çalışmanın ana konusunu oluşturmaktadır. Konu doktrinsel olarak kaleme alınacak, Protokolün incelenmesine zemin oluşturmak için öncelikle Sözleşme incelenecek, ardından da literatür taraması ile Protokol incelenecektir.

Çalışma dört bölümden oluşmaktadır. İlk bölümde siber suçlarla ilgili tanımlama yapılacak, siber suçların işleniş şekilleri ve etkileri hakkında bilgi verilecektir. İkinci bölümde, Sözleşmeye neden ihtiyaç duyulduğu ve Sözleşmenin

hazırlık süreci anlatılacak, ardından maddeleri ayrıntılı olarak incelenmeden, yapısı ve Sözleşmeye ilişkin değerlendirilmeler belirtilecektir.

Üçüncü bölümde, Sözleşmeye getirilen İkinci Ek Protokol'ün hazırlanma sürecinden, hedef ve ilkelerinden, yapısı ve içeriğinden söz edilecektir. Ardından, son hükümler bölümüne yer verilmeden, Protokolde yer alan maddelerin ayrıntılı incelemesine ve maddeler incelenirken tespit edilen değerlendirmelere ve gerektiğinde Sözleşme ile kıyaslamalarına yer verilecektir. Sonuç kısmında genel bir değerlendirme yapılarak çalışma sonlandırılacaktır.

Sözleşme ve Protokol, yalnızca siber yollarla işlenen suçlar için değil, aynı zamanda herhangi surette işlenen bir suça ilişkin soruşturma ve kovuşturmada adaletin sağlanması için önemli bir enstrümandır. Protokolün oluşmasında, siber alemde var olan kanıtların ifşasının hukuka uygunluğu, uluslararası iş birliğinin güçlendirilmesi, kanıt elde etmede ve veri toplamada kişisel verilerin, temel hak ve özgürlüklerin korunması gibi motivasyonların bulunmaktadır. Çalışma hazırlanırken Protokolün oldukça kapsamlı Açıklayıcı Raporundan sıklıkla yararlanılmıştır. Protokolün bu amaçlar için ne şekilde düzenlemeler içerdiği incelenecek ve değerlendirilecek, Sözleşmenin eksik kaldığı veya eleştirildiği konulara bir yenilik getirip getirmediği incelenecektir. Daha önce Türkçe dilinde Protokol metninin bir incelemesinin bulunmaması sebebiyle, bu çalışma ile hukuk literatürüne ve uluslararası iş birliğindeki uygulamalara katkı sağlanması amaçlanmaktadır.

BİRİNCİ BÖLÜM

1. SİBER SUÇLAR VE AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

1.1. SİBER SUÇLARIN GÜNÜMÜZE ETKİSİ

Teknolojinin günden güne ilerlemesi ve gelişmesiyle birlikte bilişim teknolojileri ve internet; bireylerin, özel şirketlerin, kamunun ve ülkelerin hemen hemen her işleminin ayrılmaz bir parçası haline gelmiştir ve gün geçtikçe önemi daha da artmaktadır. Çok sayıda kişisel veri, banka ve kart bilgileri, pek çok hassas nitelikteki şahsi ya da şirket sırrı niteliğindeki bilgiler internet ortamında muhafaza edilmektedir. Sosyal aktiviteler, iletişimler, alışveriş, eğitim, bankacılık işlemleri ve devlet dairelerinde yapılan işlemler internetten gerçekleştirilmekte, bunların yanı sıra oy verme işlemleri dahi bazı ülkelerde[1] artık internet üzerinden gerçekleşmektedir. İhtiyaçların artmasıyla paralel olarak, teknolojik gelişmeler de ihtiyaçları gidermek için bu doğrultuda artmakta ve çeşitlenmektedir.

Tüm dünyanın maruz kaldığı Covid-19 pandemisi sebebiyle faaliyetlerin, eğitimlerin ve verilen hizmetlerin bilgisayar üzerinden sağlanması ve ofis çalışmalarının uzaktan çalışmaya dönüşmesi sonucunda, toplumun dijital teknolojilere, internete ve uzaktan iletişim araçlarına olan ihtiyaç ve bağımlılık çok daha yoğunlaşmıştır. Bu süreçte eğitim, iş, hizmet sektörünün ve hatta kamu idareleri ile kritik sağlık hizmetlerinin sürdürülebilmesi için uzaktan çalışmaya geçilmiş ve bulut teknolojisinden faydalanılmaya başlanmıştır. Bu durumun pek çok olumlu ve kolaylaştırıcı etkisinin varlığının yanı sıra, olumsuz etkilerinin de olduğu yadsınamaz. Ancak arka planda bu faaliyetleri çevrimiçi ortama taşımak, kötü niyetli aktörlerin

[1] International Idea, E-Voting Currently Used In Any Elections With Emb Participation?, çevrimiçi, https://www.idea.int/data-tools/question-view/742, Erişim Tarihi: 04.02.2022.

istismar edebileceği çok sayıda yeni güvenlik açığı da yaratmış[2] ve yeni siber güvenlik önlemlerinin çoğunlukla etkisiz olduğu ortaya çıkmıştır.[3] Dolandırıcılık, veri hırsızlığı, fidye yazılımı saldırıları, bilgisayar korsanlığı ve oltalama saldırılarında da artmış yaşanmıştır.[4]

Sistemler nezdinde her ne kadar güçlü teknik güvenlik önlemleri alınsa da insan faktörü bu tedbirleri önemsiz hale getirip, siber saldırılara karşı zayıflık oluşturarak büyük zararlar meydana gelmesine sebep olmaktadır. Günümüzde devlet kurumları ve büyük özel şirketler iletişimlerini e-postalar üzerinden sürdürmektedir ve bu durum, saldırganlara çok cazip bir ortam sunmaktadır. Bu saldırı yöntemlerine en uygun örneklerden biri oltalama (phishing) siber saldırılarıdır. Bu saldırılar ile kişilerin şirket e- postasına kişilerin ilgisini çeken sahte bir e- posta gönderilerek o kişinin zararlı yazılım içeren bağlantı linkine tıklaması ile saldırganlar güvenlikli sistemlere sızabilmektedir.[5]

---

[2] Delerue, François. *Covid-19 and the Cyber Pandemic: A Plea for International Law and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace*, in T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.), 2021, s.12, çevrimiçi, https://ccdcoe.org/uploads/2021/05/CyCon_2021_Delerue.pdf, Erişim Tariih: 29.05.2022.

[3] Lubin, Asaf. *The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere*. Handbook on Extraterritoriality in International Law (Austen L. Parrish and Cedric Ryngaert eds., forthcoming, 2022), s.1, çevrimiçi, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4012007, Erişim Tarihi: 16.05.2022.

[4] Noujaim, Marie Christine. *Cybersecurity in the EU: A strategic priority for 2021-2027*, A Grants Office Publication, September 2021, Volume 1, Issue 2, çevrimiçi, https://www.grantsoffice.com/Portals/0/funded/issues/FUNDEDOct2021.pdf, Erişim Tarihi 26.12.2021.

[5] 2013-2015 yılları arasında teknoloji devleri Google ve Facebook yaşamıştır Saldırganlar, Facebook ve Google'ın orijinal ağ sağlayıcılarını ve onların faturalarını taklit ederek, sahte e-postalar ile oltalama saldırısı gerçekleştirmiş ve bunun sonucunda şirketler 50 Milyon Dolar değerinde zarara uğramışlardır. Saldırganlar, Litvanya'da tutuklanmış ve Amerika Birleşik Devletleri'ne iade edilmiştir
Bkz. Check Point, The 5 Most Expensive Phishing Scams of All Time, çevrimiçi, https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/, Erişim Tarihi: 13.01.2022.

Pek çok farklı siber saldırı yöntemi ve çok çeşitli saldırı vakıaları mevcuttur.[6] 2021 yılında yaşanan siber suçlara ilişkin paylaşılan rapora[7] göre; en çok mağduriyete ve zarara sebebiyet veren siber saldırı türlerinin açık arayla başında oltalama saldırıları olmakla birlikte, diğer saldırı türleri de oldukça fazla sayıda kişiye zarar vermektedir. Bunların bazıları; ödemelerin gönderildiği ancak mal ve hizmetin hiç alınamadığı veya oldukça düşük kalitede alındığı non-delivery, izin alınmadan bir kişiye ait ad, soyad, sigorta bilgileri gibi kişisel bilgilerin çalınarak kullanmak ve mevcut hesaplarda sahtekarlık yapmak şeklinde tanımlanan kimlik hırsızlığı, şantaj, teknik destek ya da müşteri desteği olarak gösterilen dolandırıcılık teknikleri ile kredi kartı ve şirket verilerinin çalınmasıdır.[8] Suçun işlenmesini kolaylaştırmak için sosyal medyadan ve sanal para birimlerinin kullanıldığı belirtilmekte, ortaya çıkan zararlar ise çoğunlukla iş e-postlarının çalınması, verilerin çalınması, çocukların istismarı, teknoloji sistemlerinin zarar görmesi ile kişilerin maddi ve manevi zarar görmesi gibi zararlar olarak karşımıza çıkmaktadır.[9]

Yeni iletişim kanalları ve yeni teknolojik altyapılar suçluların dikkatini çekmekte ve suç fiillerine konu olmaktadır. Yeni teknolojik gelişmeler, ilk olarak halkın kullanımına sunulmaktadır. Bundan dolayı emniyet güçleri ve yargı bu alandaki

---

[6] Bu noktada, siber saldırıların failin ve mağdurun bulunduğu ülkelerden farklı yerlerde gerçekleştiği ve uluslararası iş birliğinin ne denli önemli olduğu görülmektedir. Saldırganların motivasyonları; siyasi ideolojiler, ekonomik çıkarlar, manevi tatmin ve daha pek çok şekilde değişkenlik gösterirken, saldırılar bireyleri, kurumları hatta ve hatta ülkeleri dahi mağduru edebilmektedir. Zira hassas ve önemli altyapıları, kötü amaçlı yazılımlarla etkilemek, ulus devlet bilgisayar korsanlığı faaliyetlerinin en ileri teknolojik noktasıdır ve güvenlik sistemlerini ortadan kaldırmak, rakibin kritik endüstrisine zarar vermenin bir yoludur. Bkz. Groll, Elias. Cyberattack Targets Safety System at Saudi Aramco, çevrimiçi, https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/, Erişim Tarihi: 28.01.2022.

[7] Federal Bureau of Investigation, Internet Crime Report, 2021, s.22, çevrimiçi, www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, Erişim Tarihi: 30.05.2022.

[8] Tanımlamalar için, a.g.e. s.30-32. Teknik destek ve müşteri desteği şeklinde gösterilen dolandırıcılık faaliyetlerinin ifşası ve faillerin yakalanması için faaliyet gösteren gönüllüler için bkz. çevrimiçi, https://www.youtube.com/c/Scambaiter,%20, https://www.youtube.com/c/ScammerPayback, Erişim Tarihi: 31.05.2022.

[9] Federal Bureau of Investigation, Internet Crime Report, 2021, s.23-24, çevrimiçi, www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, Erişim Tarihi: 30.05.2022.

suçluların bir adım gerisinde kalmakta, sürekli olarak suçlulara yetişebilmek için çabalamaktadırlar.[10]

Saldırılar, savunmanın her zaman bir adım ilerisindedir. Örneğin; teknolojik gelişmeler doğrultusunda 5G ağlarının ve altyapıları dünya genelinde kullanımının yaygınlaştırılması planlanmaktadır. 5G teknolojisinin çok büyük faydalar sunacak olmasına karşın; çok sayıda anten gerektirmesi ve bilgisayar yazılım sistemine bağımlılığı ile daha az merkezi nitelikte olan yapısı sebepleriyle saldırganlara sistemlerde daha fazla potansiyel açık keşfetme ve saldırıda bulunma imkânı sunmaktadır.[11] Siber suçların işleniş biçimleri çok farklılık ve esneklik göstermekte, çoğunlukla öngörülebilir olamamaktadır. Her bir teknolojik gelişme siber suçlara, suç işleme şekillerinde çeşitliliğe, suç işleme hızının artmasına ve güvenlik sorunlarına sebep olmaktadır. Adalet sistemleri ile bu sistemlerin aktörleri de bu gelişmelere karşı yeterli derecede bilgi sahibi olamamaktadır.

Araştırmalar, 2021 yılının son 6 ayında uluslararası siber saldırıların %29 oranında artış gösterdiğini ve fidye yazılımların %93 oranında arttığını ve yeni tekniklerle işlenmeye başladığını belirtmektedir.[12] Fiziksel siber saldırıların; 2023 yılı itibariyle 50 Milyar Dolar maddi zararın yanı sıra, dava ve sigorta masrafları, ödenecek tazminatlar, para cezaları ve itibar kaybı açısından kuruluşlar için maliyetler çıkartacağı öngörülmekte, 2025 yılıyla birlikte bilgi hırsızlığının ötesinde siber

[10] Gulyass, Attila. *Dark Web Investigation: edited by Babak Akhgar, Marco Gercke, Stefanos Vrochidis, and Helen Gibson, Switzerland AG, Springer Nature,* 2021, ISBN 978-3-030-55342-5, $141.67(hardback), 305 pages. Terrorism & Political Violence, 33(8), s.1807–1809.
[11] Shaping Europe's Digital Future, Cybersecurity Policies, çevrimiçi, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies, Erişim Tarihi: 27/12/2021.
[12] Check Point, Ransomware Exploits and Supply Chain Attacks Lead the Cyber Trends in the First Half of 2021, çevrimiçi, https://pages.checkpoint.com/cyber-attack-2021-trends.html, Erişim Tarihi: 27.12.2021.

saldırganların silahlandırılmış operasyonel teknoloji ile insanlara zarar verebileceği ve hatta ölümlere sebep olabileceği tahmin edilmektedir. [13]

1.1.2. Siber Suçların Yapısı

Siber suçlar veya ülkemizdeki daha yaygın kullanımıyla "bilişim suçları", doktrinde mutabık kalınan bir tanımı olmamakla birlikte, genel itibariyle, verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yahut bu sistemde bulunan verilere yönelik olarak veya bu sistemlerin araç olarak kullanılması suretiyle gerçekleştirilen haksız fiiller olarak tanımlanmaktadır.[14]

Geleneksel suçların ekonomik, teknolojik ve siyasi gelişimler sonucunda nitelik değiştirmesi neticesinde sınır aşan suçlar kavramı ortaya çıkmıştır.[15] Siber suçlar yapıları itibariyle failin bulunduğu ülkede gerçekleştirmiş olduğu hareket ile başka bir veya birçok ülkede suç teşkil eden neticeyi meydana getirebilmeye müsaittir. Siber suçlar neredeyse her zaman sınır ötesi niteliği haizdir. Bu tür suçların ülkelerin sınırlarını aşması ve suçun işlenme hızındaki artış dolayısıyla, suçla etkin mücadele için ivedi şekilde uluslararası boyutta iş birliği, ülkeler ve ülkelerin ilgili kurumlar arası veri paylaşımı ve kolektif olarak siber suçlara karşı mücadele zaruridir. Bu konu teknik, etik ve hukuki hususları içeren karmaşık bir yapıdadır. Strateji, politika ve mevzuat

---

[13] Moore, Susan. *Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans*, Press Release, çevrimiçi, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we, Erişim Tarihi: 25.11.2021.

[14] Dülger, Volkan Murat. *Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi*, s. 2; İçel, Kayıhan. *Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri',* İÜHFM, C: LIX, S.: 1-2, 2001, s.3-10; Kurt, Levent. *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Ankara, 2005, s. 49-53; Özen, Muharrem ve Baştürk, İhsan. *Bilişim-İnternet ve Ceza Hukuku*, Ankara, 2011, s. 90-91.

[15] Erdem, Merve ve Özocak, Gürkan. *Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği*, 2017, s.1.

geliştirilebilmesi ile siber suçlara karşı koruma sağlanabilmesinin yanında, etkin soruşturma ve kovuşturma tesisi için siber suçların yapısının sağlam bir şekilde anlaşılması hayati öneme sahiptir.[16]

Ülkeler, mevcut yasalarıyla veya onlardan sorumlu ceza felsefesiyle tutarsız oldukları düşündüklerinden, siber saldırılar karşısında uluslararası olarak benimsenen belirli hükümleri iç hukuklarına dahil etmeyi reddedebilirler, uluslararası düzeyde iş birliği kurmaktan dahi imtina edebilirler. Kişisel veya ülkesel çıkarlar, ülkelerin siber suçluluğa hoşgörü sağlamasına veya siber suçlularla iş birliği yapmasına dahi neden olabilir. Ülkeler vatandaşlarının, fikri mülkiyetin ve yazılımın yasa dışı kullanımından ekonomik olarak fayda sağlamalarını teşvik edebilir ya da buna göz yumabilirler. Banka gizliliği sunulmasına paralel olarak, ülkeler siber suçlular tarafından kendi ülke sınırları içinde yatırılan veya harcanan fonlardan kâr edebilirler.[17]

Bir ülkenin, kendisinin siber terörizm için bir üs olarak kullanılmasına izin verdiği durumlar da siyasi motivasyonlarla ilgili olabilir. Ayrıca iç savaş ve şiddetin, hukukun üstünlüğüne yönelik mevcut ve acilen müdahale edilmesi gereken tehditler oluşturduğu ülkelerde, siber suçların ceza kanunlarında düzenlenmesi ve ağır karşılıklı adli yardım yükümlülüklerinin iş birliğini talep eden ülke tarafından değil de talep edilen ülke tarafından faturanın ödemesini gerektirebilecek durumlarda yerine getirilmesi, o ülkelerin yasama gündeminde yer almayabilmektedir.[18] Meydana gelen kötü niyetli siber saldırı vaka sayısı ile bu saldırıların faillerini adalete teslim etmek için yürütülen ceza soruşturma ve kovuşturma sayısı arasındaki büyük fark mevcuttur, bu durum "Siber Uygulama Boşluğu" olarak ifade edilmektedir.[19]

---

[16] Gercke, Marco. *Understanding Cybercrime: Phenomena, Challenges and Legal Response. (2013). Review of Information & Communications Technology & Development in the Arab Region,* s.36-37.
[17] Allan, Gregor. 2005. *"Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative." New Zealand Law Review*, 2005, s.155.
[18] Allan, s.155-156.
[19] Lubin, s.1.

Yukarıda söz edilen tutumların yanı sıra, siber suçların verdiği zararların ciddiyetinin bilincinde olan ülkeler ve kuruluşlar iş birliği taraftarı bir tutum sergilemektedir. Geçtiğimiz yıllar içerisinde bazı uluslararası kuruluşlar siber suçlara karşı mücadeleye yoğun şekilde katkı göstermektedir.[20] Avrupa Konseyi'nin siber suçlar ile ilgili çalışmaları uluslararası çalışmalar arasında en çok dikkat çeken çalışmalardan biridir.

Avrupa Komisyonu, altyapı yatırım fonu programı kapsamında 2014-2020 dönemi için siber güvenliğe halihazırda büyük ölçüde yatırım yapmış ve 2021 yılının Ekim ayında yapılan Avrupa Konseyi toplantısında, siber güvenliğin kilit önceliklerden biri olması gerektiğini vurgulamıştır. Avrupa Komisyonu, 2022 için yayınladığı programda, e-kanıt için tartışmaların sürdüğünü ifade etmiştir.[21]

Çalışmamızın buraya kadarki kısmı, siber suçların yapısının ne şekilde değişkenlik gösterdiğini ve zararlara sebep olabildiğini, önlenebilmesi ve adaletin sağlanabilmesi için uluslararası iş birliğinin ne denli önemli olduğunu ifade etmektedir. Bu bölümden sonraki bölümde; uluslararası iş birliğinde en önemli enstrümanlardan biri olarak görülen Avrupa Konseyi Siber Suç Sözleşmesi genel hatlarıyla incelenecek, Sözleşmeye getirilen eleştirilere ve eksikliklerine yer verilecektir. Ardından bir sonraki bölümde, bu çalışmanın asıl konusu olan, siber suçların işlenişindeki artış yaşanması, daha yoğun iş birliğine ve bu süreçte elektronik kanıtlara duyulan ihtiyaç dolayısıyla Sözleşmeye Getirilen Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin Siber Suç Sözleşmesine İkinci Ek Protokolün incelemesi yapılacaktır. Siber suçların bireylere ve ülkelere olan olumsuz etkilerinin varlığının ve siber suçlarla etkin mücadelenin gerekliliğinin bilincinde olarak, bu alanda yenilik getiren Protokolün, son hükümleri haricindeki maddelerinin incelenmesinin yapılacak, amaçları ile ne şekilde

[20] Gercke, s.36-37.
[21] Malaja, Polina. *EU Policy Update - October 2021*, çevrimiçi, https://www.centr.org/news/eu-updates/october-2021.html, Erişim Tarihi: 26.12.2021

uyumlu düzenlemeler getirdiği incelenecek, Sözleşmenin eksik kaldığı veya eleştirildiği konulara bir yenilik getirip getirmediği incelenecektir.

1.2.AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

1.2.1. Siber Suçlar Alanında Neden Uluslararası Sözleşmeye İhtiyaç Duyuldu?

Siber suçlar, ilk bölümde örneklerde de bahsi geçildiği üzere, çoğunlukla suçun neticesinin gerçekleştiği ülkelerin sınırları ötesinde bulunan kişi veya kişilerin, suç niteliği taşıyan hareketleriyle gerçekleşen ve yapısı çoğunlukla sınırlar ötesi nitelikte olan suç tipleridir. Ülkelerin, soruşturma bilhassa kanıt toplama ve kovuşturma işlemlerini tam ve etkin bir şekilde gerçekleştirmesi uluslararası iş birliği olmadan oldukça zordur. Zira, bu tür suçların işlendiği araçlar ve sistemler teknik ve çok değişkenlik göstermektedir, ayrıca internetin saldırganlara belirli ölçüde anonimlik sağlaması ve bu anonimliğin ardındaki kimliklerin ortaya çıkartılmasında ileri teknik uzmanlığın gerekmesi nedeniyle de failleri tespit etmekte zorluklar yaşanmaktadır.[22] Dolayısıyla, siber suç olgusuyla mücadele etmek bakımından en önemli husus, uluslararası adli yardımlaşmadır.[23]

Siber suçlarla ilgili yargısal problemler; gerekli suç tanımının olmaması, usule ilişkin yetkilerin yokluğu ve yabancı ülkelerle uygulanabilir karşılıklı yardımlaşma hükümlerinin bulunmaması olarak üç şekilde karşımıza çıkmaktadır. Bir ülkede bulunan suçlular tarafından başka bir ülkeye zarar vermek suretiyle işlenen suçun, suçluların bulunduğu ülke mevzuatına suç sayılmaması, zarar gören mağdurların adalete erişimde engel olabilmektedir.[24] Ancak, failin bulunduğu ve zararın meydana

[22] Gercke, s.37-36.
[23] Önok, Murat. *Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği,* Prof.Dr. Nur Centel'e Armağan, MÜHFHAD, sy.19/2, s.1232-1234.
[24] 2000 yılında üretilen ve 20 yıl süren güvenlik açıklarına sebep olan "I love you virüsünün" dünya genelinde 45 milyon bilgisayarı etkilemesine, 10 milyar dolara kadar zarara sebep olmasına ve tüm bu fiili işleyen kişi olan Onel De Guzman'ın kimliğinin saptanmasına rağmen, suçu işleyen kişinin

geldiği ülkelerde yeterli suç tanımları ve araştırma yetkileri bulunsa da suçun kovuşturulması karşılıklı yardımlaşma hükümlerinin yokluğunda hiçbir anlam taşımayacaktır.[25]

Kolluk kuvvetlerini engelleyen nedir sorusu karşısında, geleneksel görüşe göre bunun cevabı, ülkelerin sınır ötesi icra yetkisi yasağıdır.[26] Uluslararası Adalet Divanı'nın Lotus-Bozkurt davasında ifade edildiği üzere, "Uluslararası hukukun, aksine izin veren bir kuralın bulunmaması halinde, bir ülkeye dayattığı ilk ve en önemli kısıtlama, başka bir ülkenin topraklarında gücünü hiçbir biçimde kullanamayacağıdır."[27]

Ülkelerin sınırlarını aşan siber suçların faillerinin, uluslararası arenada cezai sorumluluğu yoktur, bu faillerin cezai sorumluluğu ulusal hukuk düzeyinde öngörülmekte ve failler burada yaptırıma maruz kalmaktadır.[28] Zira saldırganlar birer kişidir ve fiziksel olarak bir ülkenin yargı yetkisi dahilinde bulunmaktadır. Saldırganların, siber suç niteliği taşıyan hareketleri aynı anda çok sayıda ülkedeki bilişim sistemlerini ve mağdurları etkileyen neticeyi doğurabilmekte ve bu durum aynı anda çok sayıda ülkeyi de ilgilendirebilmektedir. Bu durum ise hem suçluların yerini tespit etmekte hem de tespit edilen yerin o ülkenin sınırları dışında olması durumunda, ceza hukukundaki mülkilik ve ülkelerin egemen eşitliği ilkeleri bakımından suçların soruşturulması ve kovuşturulmasında zorluklar yaratabilmektedir. Her ne kadar etkiler

---

Filipinler'de olması ve Filipinler'in belirtilen dönemde bilgisayar marifetiyle işlenen suçlara ilişkin bir suç tanımının olmaması, bu suç fiilini gerçekleştiren failin cezasız kalmasına sebep olmuştur. Yine 2000 yılında ABD'de meydana gelen siber saldırı faillerinin Rusya'da yakalanması, ancak Rusya'nın iş birliğini reddetmesi sonucu kovuşturmanın yapılamaması ve faillerin cezasız kalması neticesiyle karşılaşılmıştır. Detaylı bilgi için bkz., çevrimiçi, https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html, Erişim Tarihi: 13.03.2022.

[25] Weber, Amalie M. *The Council of Europe's Convention on Cybercrime*, 2003, Berkeley Technology Law Journal 18, no.1: s.426-427.

[26] Lubin, s.2

[27] Bkz. S.S. Lotus Davası, Fransa-Türkiye 1927, PCIJ, çevrimiçi, http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm, Erişim Tarihi: 16.05.2022.

[28] Erdem ve Özocak, s.1-2.

uluslararası sınırları rahatlıkla geçebilse de yargı yetkisinin böyle bir imkânı yoktur. Doktrin bu nedenle bir ülkenin kolluk kuvvetlerinin tek taraflı olarak, başka bir ülkeye girmesini ve cezai soruşturmalarının bir parçası olarak bir kişiyi alıkoymasını veya belgelere el koymasını önermemektedir.[29]

Ülkelerin yetkileri sınırlarının dışına uzanamadığı için siber suçlarla mücadelede klasik yargı yetkisi anlayışı yetersiz kalmaktadır ve bu durum siber suçlarla mücadelede temel engellerden birini oluşturmaktadır. Siber dünyanın ve uluslararası hukukun temel prensipleri arasındaki bu çatışma, siber suçların uluslararası seviyede ele alınmasını gerektirmektedir.[30] Yaşanan sorunların çözümü için uluslararası iş birliği gerekmesi dolayısıyla, devletler egemenliklerinden kısmen de olsa vazgeçecektirler. Bunun ne şekilde ve ne zaman olması gerektiği devletlere başka devletler tarafından dikte edilemeyeceği için bu hususta önceden yürürlüğe sokulmuş, uluslararası ortak bir ceza politikası belirleyen uluslararası anlaşmalar varlığı gerekmektedir.[31]

Ülkeler uluslararası bir mutabakat, diğer bir ifadeyle ülkelerin izni olmaksızın, bağımsız bir şekilde başka bir ülkenin sınırları içerisinde soruşturma ve kovuşturma yapamazlar. Ülkeler arasında iş birliği ve mevzuat uyumunun mevcut olmaması, ülkelerin tek taraflı olarak uzaktan adli bilişim soruşturması yapmasına ve yargı yetkisini aşan uygulamalara başvurmaları vakıalarına ortam sağlamaktadır ve ulusal

[29] Alvarez-Machain v. US [2003] 9th Cir, 331 F 3d 604 (Lacking Extraterritorial Enforcement Under The Controlled Substances Act To Abduct The Plaintiff From Mexico), s.629, çevrimiçi, https://casetext.com/pdf-sent?slug=alvarez-machain-v-us-5, Erişim Tarihi: 29.05.2022.
[30] Allan, s.153-154.
[31] Erdoğan, Yavuz. *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri,* Legal Yayıncılık, 2018, s.24.

egemenliğe tehdit oluşturmaktadır.[32] Zarar gören ülke makamları, suçun işlendiği ülkenin birimlerine sızarak yasadışı veri elde edebilmektedir.[33]

Siber suçlar bakımından, her suçta olduğundan daha fazla ulusal düzeydeki iş birliğinin çok önemli olduğu sıklıkla dile getirilmektedir.[34] Bunun bilincinde olan ülkeler, uluslararası örgütler ve sivil toplum kuruluşları, yeknesak bir mücadeleyi mümkün kılmayı amaçlayan sayısız girişimlerde bulunmuşlardır[35] ve uluslararası sözleşmelerle kurumların ülkelerle ve ülkelerin birbirleriyle iş birliği mümkün hâle gelmiştir. Sınırlar ötesi etkisi olan bu suçlar bakımından ülkeler, uluslararası iş birliğini sağlayan genel anlaşmalar akdetmiştir.[36] Bu sözleşmeler arasında, siber suçlarla etkin mücadelede uluslararası iş birliğini ve veri paylaşımı ile ortak bir ceza politikasının oluşturulmasını sağlayan en önemli anlaşmalardan biri olarak Avrupa Konseyi bünyesinde kabul edilen 2001 tarihli Avrupa Konseyi Siber Suç Sözleşmesi kabul edilmektedir.[37]

1.2.2. Avrupa Konseyi Siber Suç Sözleşmesi'nin Hazırlık Süreci

Sözleşmenin oluşum süreci, 1996 yılının Kasım ayında Avrupa Suç Sorunları Komitesi'nin (CDPC), Avrupa Konseyi'nin siber suçlarla ilgili bir komite oluşturması gerektiği önerisiyle başlamıştır.[38] Bu tavsiyenin ardından 1997 yılında, Avrupa Konseyi bünyesinde Siber Suç Uzmanlar Komitesi'nin kurulmasıyla başlayan

[32] Erdem ve Özocak, s.2.
[33] 2000 yılında ABD ve Rusya arasında yaşanan olayda; ABD'nin banka ve kredi kartı sistemlerine siber yollarla saldıran saldırganların Rusya'da olduklarının tespit edilmesi sonucunda ABD, Rusya'nın yardımı ve izni olmaksızın, Rusya'da bulunan birimler üzerinden sistemlere sızarak takip etmiş ve delil elde etmiştir. Yaşanan olayın hukuka uygunluğu ve toplanan delillerin hukuki niteliği tartışma konusu olmuş, ulusal egemenliğe tehdit niteliği taşımıştır. Ayrıntılı bilgi için bkz. Weber, Amalie, s.428.
[34] Karagülmez, Ali. *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, 3. Baskı, Ankara, 2011.
[35] Önok, s.1232.
[36] Erdem ve Özocak, s.2.
[37] Önok, s.1232.
[38] Vatis, Michael A. *The council of Europe convention on cybercrime. In Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for US policy*, 2010, s.208.

çalışmalar ve bilişim suçlarıyla ilgili OECD raporları ve Konsey'in tavsiye kararları neticesinde, dört yıllık bir çalışmanın[39] ve yirmi yedi adet taslağın[40] sonucu olarak oluşturulan Sözleşme, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmıştır. 1 Temmuz 2004 tarihinde internet ve bilgisayar aracılığıyla işlenen suçlar bakımından oluşturulan ilk uluslararası anlaşma olarak yürürlüğe girmiştir.[41] Türkiye Cumhuriyeti, Sözleşmeyi 10 Kasım 2010 yılında imzalamış ve 29 Eylül 2014 yılında iç hukukuna dâhil etmiştir.[42]

Sözleşmeye, Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol[43] ve Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin Siber Suç Sözleşmesi'ne İkinci Ek Protokol[44] getirilmiştir. Küresel boyutta siber suçla mücadelede kolektif bir şekilde oluşturulan Sözleşme, Avrupa Konseyi üyesi olmayan ülkelere[45] de açık ve bu ülkeler[46] tarafından imzalanmış olmakla beraber, henüz dünyadaki tüm ülkelerce kabul edilmemiş olsa da siber suçlarla mücadelede en kapsamlı ve kapsayıcı uluslararası enstrüman konumundadır.[47]

---

[39] Weber, s.429.
[40] Keyser, Mike. *The Council of Europe Convention on Cybercrime. Journal of Transnational Law & Policy* 12 (2), 2003, s.296.
[41] Erdem ve Özocak, s.2.
[42] Aliusta, Cahit ve Benzer, Recep. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:4, No:2, 2018, s.35-42.
[43] Additional Protocol To The Convention On Cybercrime, Concerning The Criminalisation Of Acts Of A Racist And Xenophobic Nature Committed Through Computer Systems (ETS No.189), https://rm.coe.int/168008160f.
[44] Gelişmiş İş Birliği ve Elektronik Kanıtların Ifşasına Ilişkin Siber Suç Sözleşmesine İkinci Ek Protokolün Türkçe Çevirisi için bkz., çevrimiçi, https://rm.coe.int/turkish-2nd-ap-to-the-bc-nov-2021/1680a55b47, Erişim Tarihi: 13.02.2022.
[45] Sanal Ortamda İşlenen Suçlar Sözleşmesi, m.37.
[46] Mauritius, Peru, Senegal gibi ülkeler. Bkz., çevrimiçi, https://www.coe.int/en/web/about-us/our-member-states?desktop=true, Erişim Tarihi: 13.02.2022.
[47] Akpek, Nusret Onur. *Siber Suçlar Sözleşmesinin Getirdikleri ve Iç Hukuk Açısından Konuya Yaklaşım*. İstanbul Bilgi Üniversitesi, 2015, s.21.

Sözleşmeyi İmzalamış ve Onaylamış Olan Ülkeler Listesi

Almanya
Amerika Birleşik Devletleri
Andorra
Arnavutluk
Arjantin
Avustralya
Avusturya
Azerbaycan
Belçika
Bosna Hersek
Bulgaristan
Cape Verde
Çekya
Danimarka
Dominik Cumhuriyeti
Ermenistan
Estonya
Fas
Filipinler
Finlandiya
Fransa
Gana
Güney Kıbrıs Rum Yönetimi
Gürcistan
Hırvatistan
Hollanda
İngiltere
İspanya
İsrail
İsveç
İsviçre
İtalya
İzlanda
Japonya
Kanada
Karadağ
Kolombiya
Kosta Rika
Kuzey Makedonya
Letonya
Lihtenştayn
Litvanya
Lüksemburg
Macaristan
Malta
Moldova
Monako
Morityus
Norveç
Panama
Paraguay
Peru
Polonya
Portekiz
Romanya
San Marino
Senegal
Sırbistan
Slovakya
Slovenya
Sri Lanka
Şili
Tonga
Türkiye
Ukrayna
Yunanistan

Sözleşmeyi İmzalayan Ancak Henüz Onaylamayan Ülkeler

Benin

Brezilya

Burkina Faso

Ekvador Cumhuriyeti

Fiji Adaları

Guatemala

Güney Afrika Cumhuriyeti

İrlanda

Meksika

Nijer

Nijerya

Trinidad ve Tobago

Tunus

Vanuatu

Yeni Zelanda[48]

Avrupa Konseyi Siber Suç Sözleşmesi, 2022 yılının Haziran ayı itibariyle 66 ülke tarafından imzalanmıştır. Bu durum, 66 ülkenin iç hukuklarını Sözleşmedeki şekilde birbirleriyle uyumlu hale getirdiğini veya getirecek olduğunu ve siber suçlarla küresel şekilde mücadelede birbirleri ile iş birliğine hazır olduklarını bizlere sunmaktadır.[49] Birleşmiş Milletler (BM) üyesi toplamda 193 ülke olması[50] ve siber suçların en yoğun şekilde işlendiği Çin, Rusya ve Hindistan[51] gibi ülkelerin Sözleşmeyi

[48] The Budapest Convention and its Protocols, Who are the Parties to the Budapest Convention?, çevrimiçi, https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[2],%22105166442%22:[2]}, Erişim Tarihi: 04.02.2022.
[49] Akpek, s.26.
[50] Growth in United Nations membership, UN, çevrimiçi, https://www.un.org/en/about-us/growth-in-un-membership, Erişim Tarihi: 07.02.2022.
[51] Enigma Soft, Top 20 Countries Found to Have the Most Cybercrime, çevrimiçi, https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, Erişim Tarihi: 07.02.2022.

henüz imzalamamış olması siber suçlarla mücadelede hâlâ kat edilmesi gereken çok yol ve önümüzde uzun bir süreç olduğunu göstermektedir. Ancak, 66 ülkenin bu konuda birlik oluşturmuş olması her halükârda umut vadetmektedir, böylece pek çok suçun soruşturulması ve kovuşturulmasına imkân sağlayarak mağdurlara yardımcı olunabilmektedir.

Orijinal metni Fransızca ve İngilizce[52] olarak kaleme alınan Avrupa Konseyi Siber Suç Sözleşmesi'nin mevzuatımızdaki Türkçe çevirisi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" ismiyle yapılmıştır.[53] Literatürde; Avrupa Konseyi Siber Suç Sözleşmesi, Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Budapeşte Siber Suçlar Sözleşmesi isimleriyle de anılan işbu Sözleşme, ağırlıklı olarak "Avrupa Konseyi Siber Suç Sözleşmesi" ismiyle dile getirilmektedir ve bu çalışmada da hem bu ismiyle hem de tek başına "Sözleşme" olarak anılacaktır.

Avrupa Konseyi Siber Suç Sözleşmesi'nde "siber suç" (cybercrime) olarak tanımlanan ve bu çalışmanın temel terimlerinden biri olan işbu suç tipi, doktrinde bir uzlaşı olmamakla birlikte, Türk literatüründe "bilişim suçları, sanal ortamda işlenen suçlar, bilişim sistemleri aleyhine işlenen suçlar ve bilişim sistemleri aracılığıyla işlenen suçlar" terimleriyle karşımıza çıkmaktadır.[54] Doktrinde ve literatürde yaygın olarak "siber suç" terimi kullanılmaktadır.[55]

Gün geçtikçe gelişen teknoloji ve yenilikler, siber suçlarda yeni görünüm şekilleri ortaya çıkarmaktadır. Mevzuatın bu yenilikler karşısında uyarlanmayıp, klasik

---

[52] Details of Treaty No.185, bkz. çevrimiçi, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, Erişim Tarihi: 23.01.2022.
[53] İnsan Hakları Daire Başkanlığı, Sanal Ortamda İşlenen Suçlar Sözleşmesi, çevrimiçi, https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenen Suclar.pdf, Erişim Tarihi: 31.01.2022
[54] Önok, s.1231.
[55] Dülger, M. Volkan. *Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması,* 2019, s.147.

suç tipleri için mevcut hukuk kurallarının bilişim teknolojilerinde ortaya çıkan ve çıkacak olan suç tiplerine uygulanmaya çalışılması, failleri cezalandırmakta yetersiz kalabilmektedir. Dolayısıyla, ülkelerin mevzuatını da aynı hızla değiştirmesini, geliştirilmesini ve değişen şartlara uyarlamasını gerektirmektedir.[56]

Siber suçların tanımı mukayeseli hukukta birbiriyle aynı olmadığı gibi, halihazırdaki tanımlamalar da her zaman net değildir. Siber suçların değişiklik göstermesi ve yapısı dolayısıyla, sınırları aşan boyuttadır ve teknik şekilde takip edilmesi ile yargılama süreci oldukça zordur.[57] Ülkelerin ortak bir ceza politikası oluşturmamaları, maddi hukuk ve usul hukukundaki farklılıklar, etkili bir adli yardımlaşmayı engellemektedir ve bu sebeple siber suçlara ilişkin maddi ceza hukuku kurallarının yeknesaklaştırılması çok önemlidir.

Her ülkenin maddi ve usul ceza kanunları birbirinden farklılık göstermektedir. Bu farklılık delil toplama hususunda, toplanan delillerin hukuka aykırılığı[58] riskini doğurabilmekte ve ceza yargılamasını olumsuz etkileyebilmektedir.[59] Tekrar ifade etmek gerekir ki, ülkelerin iş birliğinde bulunabilmesi için gerekli olan iki temel şart; iki ülke arasında olan ya da iki ülkenin de tarafı bulunduğu çoklu karşılıklı bir adli yardımlaşma sözleşmesi ile yardım talep edilen ülkenin mevzubahis iş birliği talebine konu suçu kendi iç hukukunda suç kabul etmesi, diğer bir ifadeyle suçlar bakımından "karşılıklılık ilkesinin" varlığıdır.[60] Dolayısıyla, Sözleşmede de açıkça ifade olunduğu üzere "Böylesi eylemlerin suç haline getirilerek engellenmesi ve uygun mevzuatın kabul edilmesi ile söz konusu cezai suçlularla etkili biçimde mücadele edilmesine yetecek yetkilerin temin edilmesini sağlamak amacıyla, hem ulusal hem de uluslararası düzeyde tanımlanması, soruşturulması ve yargıya götürülmesinin kolaylaştırılması

[56] Önok, s.1233
[57] Erdem ve Özocak, s.2.
[58] Bkz. *Venenata arbor fructus venenosa* ilkesi.
[59] Önok, s.1235
[60] Erdem ve Özocak, s.5.

amacıyla ve uluslararası iş birliğinin geliştirilmesi suretiyle ortak bir ceza siyasetinin öncelikli olarak takip edilmesi ihtiyacı"nın bilincinde olunarak uluslararası iş birliği için bu Sözleşme kaleme alınmıştır.[61]

İleride daha fazla detaylandırılacağı üzere özetle, Sözleşme siber suçların değişen yapısına karşı koruma sağlayabilmek için, Taraf ülkelere mevzuatını uyarlamalarında bir çerçeve oluşturmaya çalışmaktadır. Ülkelerin mevzuatında gerekli düzenlemeleri yapmamaları, zarar verici suç fiillerinin ulusal mevzuatında suç olarak tanımlanmaması, delillerin hukuki niteliği sorununun yanında saldırganların istedikleri ülkeden, istedikleri konumdaki hedeflere zarar verebilme imkânları olması dolayısıyla, saldırganların o ülkeleri adeta bir suç karargâhı ya da güvenli bölge haline getirebilme riski vardır ve bu durum milletlerarası özel hukuktaki forum shopping kavramı gibi, kişinin belli bir ülkenin sağladığı esnekliği keşfedip, bundan istifade etmek için bu ülkelerden suç teşkil eden faaliyetlerini sürdürmesi şeklinde bir sonuç doğurabilecektir.[62] Ülkelerin siber saldırılarda kolektif ve birbirleriyle uyumlu bir şekilde hareket etmesi siber suçlarla mücadelede ana şarttır. Bu bakımdan, ifade olunduğu üzere "siber suçlara karşı mücadele ya küresel olacaktır ya da hiçbir anlamı olmayacaktır."[63]

1.2.3. Sözleşmenin Amacı

Gerekçe Niteliğindeki Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Rapor Taslağı'nda[64] Sözleşmenin amaçları aşağıda belirtilen üç madde olarak ifade edilmiştir;

---

[61] Sanal Ortamda İşlenen Suçlar Sözleşmesi, Giriş kısmı, paragraf 4 ve 9,.
[62] Önok, s.1236
[63] Esposito, Luca G. *The Council of Europe Convention on cyber-crime: a revolutionary instrument?,* in Broadhurst, Roderic. (Ed.), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, Hong Kong, 2004, s.412.
[64] Explanatory Report to the Convention on Cybercrime, II.The preparatory Works, Art.133, çevrimiçi, https://rm.coe.int/16800cce5b, Erişim tarihi: 18.03.2022.

1- Siber suçlar alanında ülkelerin maddi ceza ve muhakeme hukuklarının uyumlu hale getirilmesi,
2- Siber suçlar ile bilgisayar kullanılarak işlenen ya da delilleri elektronik formda olan suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usul hukuku alanında gerekli yerel yetkilerin sağlaması,
3- Bu bağlamda hızlı ve etkin nitelikte uluslararası iş birliği rejimi oluşturmak.[65]

Yukarıda sayılanlara ek olarak, açıklayıcı raporun ilerleyen bölümlerinde Sözleşmede yer alan usul hükümlerinin temel amacının, somut ceza soruşturma ve kovuşturmalarında kullanılmak amacıyla veri elde edilmesine izin verilmesini sağlamak olduğu[66] ve ortak küresel bir ceza politikası oluşturmak, toplumu bilişim suçlarına karşı korumak olduğu ifade edilmektedir.

Sözleşme hem maddi ceza hukuku hem de ceza muhakemesi hukukuna ilişkin çok sayıda hüküm içermektedir. Sözleşmede belirlenen usuller sadece bilişim sistemleri aracılığıyla işlenebilen suçlar ve bilişim suçları değil, aynı zamanda klasik suçlar için yapılan soruşturma ve kovuşturmalar sırasında bilişim sistemleri yoluyla kanıt toplanması gerektiğinde de uygulanabilecektir. [67] Diğer bir ifadeyle, delilin ilişkin olduğu suçun türünün önemi bulunmamaktadır.[68]

Sözleşmenin yapısı, yargısal olarak karşılaşılan zorlukların farkındalığını yansıtmaktadır ve giriş kısmında da asıl amacının toplumu siber suçlardan korumak

[65] Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı ve Açıklayıcı Memorandumu / Hazırlayan: Siber Suç Uzmanları Komitesi, Çevirisi: İnternet ve Hukuk Platformu, Ankara Barosu, 2008, 3.Baskı, s.79, çevrimiçi, http://www.ankarabarosu.org.tr/siteler/1940-2010/kitaplar/pdf/a/sibersuclar.pdf, Erişim Tarihi: 27.12.2021. Orijinali için bkz. çevrimiçi, https://rm.coe.int/16800cce5b, Erişim Tarihi: 27.12.2021.
[66] Erdoğan, s.1-2. Ayrıntılı bilgi için bkz. Gerekçe Niteliğindeki Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Rapor Taslağı Art.133.
[67] Erdoğan, s.2.
[68] Erdoğan, s.2.

amacıyla ortak bir ceza politikası inşa etmek olduğu ifade edilmektedir. Sözleşme siber suçlar ile ilgili kanunları ve usul mekanizmalarını uyumlaştırarak ederek başarılı bir kovuşturma imkânı sunmayı amaçlamaktadır.

Sözleşme ana ilkeler çerçevesinde, cezai sorumluluğun düzenlenmesinde göz önünde bulundurulan hususlar; başta düşünce ve ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin gereklerine uyulması, bilişim suçlarının belirlenerek ülkelerin ulusal mevzuatını uyumlaştırılması suretiyle ortak bir asgari standart sağlanması, eylemlerin hukuka aykırı olması ile kasten işlenmesi şeklindendir.[69]

1.2.4. Sözleşmenin İçeriği

Bir önceki başlıkta belirtilen amaçlar çerçevesinde oluşturulan Sözleşme; dört bölümden ve 48 maddeden oluşmaktadır. Ana hatlarıyla birinci bölümde tanımlar, ikinci bölümde maddi ceza hukuku ve usul hukuku, üçüncü bölümde uluslararası iş birliğine ilişkin düzenlemelere ve dördüncü bölümde son hükümlere yer verilmektedir.[70]

Birinci bölümde Sözleşme amaçları bakımından; bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi kavramlarının neleri ifade ettiğini tanımlar başlığında detaylandırılmıştır. Birinci bölümdeki tanımlar kısmında yer almıyor olmasına karşın, Sözleşmenin ikinci bölümünde yer alan 18. maddenin 3. fıkrasında da abone verilerinin tanımlaması yer almaktadır.

[69] İçel, Kayıhan. *Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri"*, İÜHFM, Cilt: LIX, Sayı:1-2, 2001, s.6-9, çevrimiçi, https://dergipark.org.tr/en/download/article-file/95984, Erişim Tarihi: 29.05.2022.
[70] Akpek, s.22.

Sözleşmenin ikinci bölümünde bir dizi koruma tedbiri öngörülmektedir. Koruma tedbirleri asıl olarak bir amaç değil, amaca ulaşmak için kullanılan araçlardır. Koruma tedbirlerinin zaman ve uygulama şekli bakımından sınırlı olduklarından koruma tedbirlerinin uygulanmasıyla amaçlan hususlar; kanıtların hukuka uygun şekilde ele geçirilmesinin sağlanması, kanıtların yok edilmesine, değiştirilmesine engel olunması ile yargılama neticesinde hükmün yerine getirilmesinin sağlanmasıdır. [71]

İkinci bölümde siber suçlarla mücadelede ülkelerin iç hukuklarını uyarlaması için alınması gerekli suç tanımları, ceza muhakemesi bakımında usul hukukuna ilişkin önlemler, yargı yetkisi ve genel hatlarıyla ifade edilmiş kurallar dizisi bulunmaktadır. Sözleşmeye taraf olan ülkelerin bu kısımda yer alan suç tanımlamalarına ve usule ilişkin yetkilere iç hukuklarındaki mevzuatta yer vermeleri beklenmektedir. Bir görüşe göre Sözleşme, suç tipleri ve unsurlarının belirlenmesinde esnek bir dil kullanmış ve ileride ortaya çıkabilecek suç tiplerini kapsayıcı nitelikte ifadelere yer vermektedir.[72]

Sözleşme ikinci bölümün birinci kısmında; dokuz fiili dört kategoride suç olarak düzenlemektedir. İlk kategori bilgisayar verisi ve sistemlerinin bütünlük, kullanılabilirlik ve gizliliğine ilişkin suçları düzenlemektedir. Bunlar; yasadışı erişim, yasadışı araya girme, verilere müdahale etme, sisteme müdahale ve cihazların kötüye kullanımıdır. İkinci kategori; bilgisayarlarla bağlantılı sahtecilik ve bilgisayarla bağlantılı dolandırıcılık adı altında düzenlenmiş olan bilgisayar bağlantılı suçlardır. Üçüncü kategori; çocuk pornografisiyle bağlantılı olan içerik suçlarıdır. Bu kategori ile ilgili olarak 2002 tarihli Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol getirilmiştir. Dördüncü kategori; telif hakları ihlalleri ve bunlarla bağlantılı suçları düzenlemektedir. Bu bölüm ayrıca bahsi geçen suçlara teşebbüs, azmettirme ile

[71] Erdoğan, s.98.
[72] Önok, s.1243.

suça yardım ve yataklık etmeye karşı, gerekli kanunların oluşturulması için yardımcı hükümler içermektedir.[73] Sözleşmedeki bütün suçlar bakımından ortak olan unsur, cezai sorumluluğun oluşabilmesi için suçların kast ile işlenmesidir, kastın yorumlanması Taraf ülkelere bırakılmıştır.[74]

Yine Sözleşmenin ikinci bölümünün ikinci kısmında siber suçlara özgü usul ile ilgili hususlara yer verilmektedir. Bunlar; depolanan bilgisayar verisinin süratli şekilde korunması, aranması ve el konulması, üretim emri ile trafik verisinin gerçek zamanlı toplanması, süratli şekilde korunması ve kısmen açıklanmasıdır. Bu bölümün üçüncü kısmında yargılama yetkisi ile ilgili olarak, yer bakımından uygulama ve vatandaş tarafından işlenen suçlar hakkında düzenlemeler içeren hükümler yer almaktadır.[75] Bu maddelerde belirtilen "yetkili mercilerin" adli ya da idari merci olabileceği ifade olunmaktadır.[76]

Sözleşmenin üçüncü bölümünde; Sözleşmenin en yararlı özelliklerinden biri olan uluslararası iş birliği ve adli yardımlaşmayla ilgili genel ilkeler ve özel hükümler yer almakta ve uluslararası iş birliğinde üç temel prensip sunmaktadır. Bunlar; ülkeler arasında uluslararası iş birliğinin en geniş ölçüde uygulanacağı, bu hükümlerin yalnızca suçlar bakımından değil, aynı zamanda elektronik delillerle bağlantılı delillerin toplanmasında da uygulanacağı ve bu hükümlerin daha önceden var olan uluslararası anlaşmaların hükümlerinin yerine geçmeyeceği hususlarıdır. Bununla birlikte, bu kısımda yer alan 27. maddedeki düzenlemede, ilgili ülkeler arasında uluslararası anlaşmanın yürürlükte olmadığı hallerde yapılan karşılıklı yardımlaşma taleplerine ilişkin usuller de yer almaktadır. Bu düzenleme ile aralarında özel bir anlaşma

[73] Weber, s.431.
[74] Keyser, s.299.
[75] Akpek, s.23.
[76] Erdoğan, s.3.

bulunmayan Taraf ülkeler için Sözleşme, karşılıklı adli yardım anlaşması görevini görmektedir.[77]

Belirtmek gerekir ki Sözleşme, siber suçlar bakımından özel bir adli yardımlaşma sistemi getirmesi dolayısıyla, bu hususstaki adli yardımlaşma hükümleri, genel nitelikteki adli yardımlaşma hükümleri karşısında *lex specialis* ilkesi gereği öncelikli olarak uygulanma alanı bulmaktadır.[78] Uluslararası adli yardımlaşmaya ilişkin hükümler; karşılıklı yardımlaşmaya ilişkin genel ilkeler, suçluların iadesi, uluslararası anlaşmaların yürürlükte olmadığı durumlardaki karşılıklı yardım taleplerine ilişkin usuller, geçici tedbirlere ve soruşturma yetkilerine ilişkin karşılıklı yardımlaşma ile 7/24 iletişim ağının kurulması hususlarıdır. Suçluların iadesi ile ilgili hükümler de daha önceden var olan uluslararası anlaşmalar veya ülkelerin birbirileri arasındaki alternatif anlaşmaların hükümlerinin varlığına göre değişkenlik gösterecektir.[79]

Son olarak dördüncü bölümde; Sözleşmeye taraf olma, Sözleşmeden ayrılma, koyulabilecek çekinceler, değişiklikler, Sözleşmeden ayrılma ile uyuşmazlıkların çözümü gibi Sözleşmenin uygulanması hususunda son hükümler yer almaktadır.

[77] Önok, s.1253.
[78] Erdem ve Özocak, s.3.
[79] Weber, s.433.

1.2.5. Sözleşmenin Maddelerinin İncelenmesi

1.2.5.1. Tanımlar

a) Bilgisayar Sistemi

Bilgisayar sistemi tanımı, bir program aracılığıyla otomatik veri işleyebilen herhangi bir cihaz veya birbirleri ile bağlantılı veya ilgili bir grup cihazı ifade etmektedir.

b) Bilgisayar Verisi

Bilgisayar verisi tanımı, bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her tür temsilini ifade etmektedir.

c) Hizmet Sağlayıcı

Hizmet sağlayıcı tanımı hizmetlerinden faydalananlara bir bilgisayar sistemi aracılığıyla iletişim kurma imkânı sağlayan her türlü kamu veya özel sektör tüzel kişisi ile bu hizmetlerin kullanıcıları adına bilgisayar verilerini işleyen ya da depolayan her türlü özel kişiyi ifade etmektedir.

d) Trafik Verisi

Bilgisayar sistemi aracılığıyla gerçekleşen iletişimle bağlantılı olan, iletişim zincirinin bir halkasını teşkil eden bilgisayar sistemi tarafından üretilmiş, iletişimin başlangıç ve varış noktası, izlenen yol, saat, tarih, boyutu ile süresini veya iletişimde kullanılan temel hizmetin türünü gösteren bilgisayar verisi anlamına gelmektedir.

Bilişim sistemleri aracılığıyla gerçekleştirilen eylemlerin incelenmesi ve ortaya çıkarılmasıyla ziyaret edilen internet siteleri, ziyaret saatleri, aranan kelimeler gibi delil niteliğindeki pek çok unsura erişilebilmektedir. Bu durumda yürütülmekte olan soruşturmalarda suçun faillerine ya da deliline ulaşabilmek bakımından trafik verileri hayati önem taşıyabilmektedir. Verilerin çıkış noktası ile varış noktası ve arada kullanıldığı diğer noktalar tespit edilerek failler kolaylıkla ele geçirilebilecektir.[80]

e) Abone Bilgisi

Birinci bölümdeki tanımlar kısmında yer almıyor olmasına karşın, Sözleşmenin ikinci bölümünde yer alan 18. maddenin 3. fıkrasında abone verisinin tanımlaması yapılmaktadır. Bu çalışmada Sözleşmede yer alan tanımlamalarla birlikte yer verilmesi bütünlüğü sağlamak bakımından yararlı görülmüştür.

Madde metninde yer alan tanıma göre abone bilgisi; bir hizmet sağlayıcı tarafından bilgisayar verileri biçiminde veya başka bir biçimde tutulan, trafik veya içerik verileri hariç olmak üzere, hizmet abonelerine ilişkin kullanılan iletişim hizmeti türünün, ayrıca belirlenen teknik hükümlerin ve hizmet süresinin, abone kimliğinin posta veya coğrafi adresinin, telefon, erişim numarasının, fatura ve ödeme bilgileri ile iletişim teçhizatının kurulduğu yere ilişkin diğer bilgilerin belirlenmesini sağlayabilecek herhangi bir ifade eder.

Abonelik bilgileri iletişim hizmetinin kullanımıyla doğrudan bağlantılı bilgilerle sınırlı olmayıp aynı zamanda, trafik verileri ya da içerik verileri haricinde, kullanıcının kimliğinin, posta adresi, bulunduğu yerin adresinin, telefon ve diğer erişim numaralarının, faturalama ve ödeme bilgilerinin saptanmasına yardım eden, aboneyle hizmet sağlayıcı arasındaki hizmet sözleşmesi ya da düzenlemesi esas alınarak elde

[80] Erdoğan, s.167.

edilebilen her türlü bilgiyi de içine almaktadır. Trafik verileri ya da içerik verileri dışında, iletişim teçhizatının kurulu olduğu yer ile ilgili hizmet sözleşmesi esas alınarak elde edilebilen her türlü bilgiyi de ifade etmektedir.[81]

1.2.5.2. Ulusal Düzeyde Alınacak Tedbirler

1.2.5.2.1. Maddi Ceza Hukukuna İlişkin Düzenlemeler

Sözleşmenin ikinci bölümünün birinci kısmında dört kategoride dokuz tane suç suç tanımlaması yapılmaktadır. Bu kategoriler sırasıyla; bilgisayar verisi ve sistemlerinin bütünlük, kullanılabilirlik ve gizliliğine ilişkin suçlar, bilgisayarlarla bağlantılı sahtecilik ve bilgisayarla bağlantılı dolandırıcılık adı altında düzenlenmiş olan bilgisayar bağlantılı suçlardır, çocuk pornografisiyle bağlantılı olan içerik suçları ile son olarak telif hakları ihlalleri ve bunlarla bağlantılı suçlardır.

Bu kısımda; dört kategoride düzenlenen suçlara ilişkin teşebbüs, yardım ve yataklık, kurumsal yükümlükler ile yaptırımlar ve tedbirlere ilişkin düzenlemeler de yer almaktadır. Tekrar ifade etmek isteriz ki Sözleşmedeki bütün suçlar bakımından ortak unsur, cezai sorumluluğun oluşabilmesi için suçların kast ile işlenmesidir.

a) Bilgisayar Verilerinin ve Sistemlerin Gizliliğine, Bütünlüğüne, Erişilebilirliğine Yönelik Suçlar

Bu kategori altında düzenlenen suçlar; yasadışı erişim, yasadışı araya girme, verilere müdahale etme, sisteme müdahale ve cihazların kötüye kullanımı suçlarıdır. Sözleşme Taraf ülkelerin iç hukukunun Sözleşmeyle uyumlaştırılmasını beklemektedir. Türkiye Cumhuriyeti devleti bu doğrultuda, bu suç tanımlarını 5237

[81] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.180.

Sayılı Türk Ceza Kanunu'na dahil etmiştir. Burada yer verilen suç tanımlamalarına ilişkin kısaca açıklama yapılacak, ardından mevzuatımızda hangi maddeler ile bu suçlara yer verildiği ifade olunacaktır.

Yasadışı erişim suçu 2. maddede düzenlenmektedir, bir bilgisayar sisteminin tamamı veya bir kısmına haksız olarak, diğer bir ifadeyle kişinin izinsiz bir şekilde yetkisi olmadan kasten erişmesinin suç olduğunu ifade etmektedir. Burada 'haksız' ifadesi ile kişinin saikinin suçun oluşmasında bir değişikliğe sebep olmayacağı anlaşılmaktadır.[82] Yasadışı erişim suçu, Türk mevzuatına 'bilişim sistemine girme'[83] başlığı ile dahil edilmiştir. Kanunumuz bilişim sistemine hukuka aykırı olarak girerek kalmaya devam etmeyi de suç olarak düzenlemektedir.

3. maddede yasadışı araya girme suçu, bilgisayar verilerinin, bir bilgisayar sisteminden diğer bir bilgisayar sistemine umuma kapalı olarak iletilmesi sırasında, elektromanyetik dalgalar da dahil olmak üzere, teknik yöntemler aracılığıyla araya girerek hukuka aykırı ve kasten dahil olunması olarak tanımlanmıştır. Türk Ceza Kanunu'nun 243. maddesinin 1. fıkrası "bir bilişim sistemine hukuka aykırı olarak giren veya orada kalmaya devam eden kişinin" ve aynı maddenin 4. fıkrası "bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen" kişinin cezalandırılacağını düzenleyerek Sözleşme ile uyumluluk sağlamaktadır

Sözleşmenin 4. maddesinde verilere müdahale suçu düzenlenmiştir. Buna göre, bilgisayar verilerine hukuka aykırı şekilde ve kasten zarar verilmesi, silinmesi, bozulması, değiştirilmesi ya da engellenmesi eylemleri suç teşkil etmektedir. Bir sonraki madde sisteme müdahale suçunu, sisteme veri göndermek, yerleştirmek veya

[82] Örneğin, bir kişinin hukuka aykırı bir fiili sonlandırmak amacıyla hackerlara (saldırganlara) ait bilgisayar sistemlerine girmesi de bu suça vücut verebilecektir.
[83] Bu düzenleme, 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinde yer almaktadır.

var olan verilere müdahale etmek suretiyle bilişim sisteminin işleyişinin ciddi şekilde engellenmesi eylemlerini olarak düzenlemektedir.[84] Kanunumuzda sistemi engelleme, bozma, verileri yok etme veya değiştirme başlığında, verilere müdahale suçu 244. maddesinin 2. fıkrasında, sisteme müdahale suçu 244. maddesinin 1. ve 2. fıkralarında düzenlemiştir.

Cihazların kötüye kullanılması başlıklı 6. maddede, 2 ila 5. maddelerde belirtilen suçların kullanılması amacıyla, erişim kodu, bilgisayar programı, herhangi bir veri ve cihazların üretilmesi, satışı, ithalatı, dağıtılması ve tüm bu ifadeleri kapsayıcı olarak erişilebilir hale getirilmesi suç olarak düzenlenmektedir. Dolayısıyla, önceki maddede tanımlanan suçlara yönelik belirli hazırlık hareketleri de bu madde ile bağımsız bir suç olarak tanımlanmaktadır.[85] Kanunumuzda 245. ve 246. maddelerde bu suç ile ilgili düzenlemeler bulunmaktadır.

b) Bilgisayarlarla Bağlantılı Suçlar

Var olan verilerin yeni veri girme, veri değiştirme, silme ve engelleme eylemleriyle kasten ve hukuka aykırı olarak özgünlüğünün bozulması ve bu eylemlerin özgün olan verilen hukuki olarak özgün olarak kabul edilmesi veya işlem görmesi amacıyla işlenmesi 7. maddede düzenlenmektedir. Bu suç ceza kanunumuzun 244. maddesindeki ifadeler kapsamındadır.[86]

---

[84] Özbek, Mücahit. *Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma*, Galatasaray Üniversitesi, 2015, s.72.
[85] Özbek, s.73
[86] Bkz. Ek olarak, 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 205. maddesi ile 5070 sayılı Elektronik İmza Kanunu'nun 5. maddesinde yer alan düzenlemeler doğrultusunda elektronik imza vasıtasıyla düzenlenen belgelerin senet hükmünde olduğuna hükmedilmiştir, bu doğrultuda belgede sahtecilik, belgenin bozulması, yok edilmesi veya gizlenmesinin düzenlendiği TCK'nın 204 ila 212. maddeleri Sözleşme ile uyumludur.

Hukuka aykırı ve kasten, başkasının maddi kaybına sebebiyet verilmesini veya maddi menfaat sağlamak amacıyla hile ve sahtekarlıkla niyetiyle başka bir kişiye karşı bilgisayar sistemlerine veri girişi yapılmasını, verilerin değiştirilmesini, silinmesini, engellenmesini ve bilgisayar sistemlerine müdahalede bulunma bilgisayarla bağlantılı dolandırıcılık suçu olarak düzenlenmektedir. Ceza kanunumuzun 245. maddesinde banka veya kredi kartlarının kötüye kullanılması suçu ile 158. maddesinde bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılmasının nitelikli dolandırıcılık suçu olduğunu düzenlemektedir.

c) İçerikle Bağlantılı Suçlar

Sözleşmenin 9. maddesi çocuk pornografisi ile bağlantılı suçları düzenlemektedir. Buna göre, reşit olmayan veya reşit olmayan kişi görüntüsü olan kişilerin cinsel içerikli eylemlerde bulunması ile bu eylemin betimlenmesi çocuk pornografisi anlamına gelmektedir ve çocuk pornografisini kasten ve haksız yere bilgisayar sistemi üzerinden dağıtımını yapmak amacıyla üretmek, sunmak, erişilebilir hale getirmek, dağıtım veya iletimini yapmak, kendisi ya da bir başkası için bilgisayar sistemi üzerinden temin etmek, depolama aygıtında bulundurmak suç olarak tanımlanmaktadır. Ceza kanunumuzda müstehcenlik başlığı altında, 226. maddenin 3. fıkrasında, ilgili düzenleme yapılmıştır.

d) Telif Hakları ve Bunlarla Bağlantılı Hakların İhlaline İlişkin Suçlar

Telif hakları ve bunlarla bağlantılı hakların ihlaline ilişkin suçların düzenlendiği 10. maddede bu ihlalin kasten, ticari sonuç doğuracak surette ve bir bilgisayar sistemi aracılığıyla işlenmesinin suç teşkil edeceği düzenlenmekle beraber önceki maddelerde olduğu gibi detaylı bir tanım yapılmamış, uluslararası sözleşmelerdeki yükümlülüklere atıf yapılmıştır. 5846 sayılı Fikir ve Sanat Eserleri Kanunumuzda ilgili düzenlemeler yapılmıştır.

e) Tali Yükümlülük ve Yaptırımlar

Sözleşmenin 11.maddesinin 1. fıkrası, 2. ila 10. maddelerinde tanımlanan suçların işlenmesine kasten yardım veya yataklık edilmesi, 11. maddenin 2. fıkrasında sayılan suçların işlenmesine kasten teşebbüs eyleminde bulunulmasını düzenlemektedir. Böylece belirli suçlarda teşebbüs, iştirak ve azmettirme eylemlerinin de cezalandırılabilmesi mümkün olacaktır. Teşebbüsün düzenlendiği bu maddenin 2. fıkrasının uygulanması Taraflarca saklı tutulabilir. Sözleşmenin 12. maddesi tüzel kişilerin cezai sorumluluğunu ve son olarak 13. madde yaptırımlar ve tedbirleri düzenlemektedir.

1.2.5.2.2. Usul Hukukuna İlişkin Düzenlemeler

Bilişim teknolojileriyle işlenen suçların yapısı delillerin hızlıca kaybolmasına oldukça elverişlidir, elektronik deliller hızla tahrip edilebilir veya yok edilebilir. Bir yandan failleri tespit etmek de oldukça güçtür. Hız ve gizlilik bir soruşturmanın başarısı için hayati önemde olabilmektedir.[87] Dolayısıyla adaleti temin edebilmek için bazı usuli önlemler gereklilik arz etmektedir.[88]

Usul hukuku hükümlerine, diğer bir ifadeyle ceza soruşturmasında ve kovuşturmasında uygulanacak yetki ve usulleri belirleyecek olan tedbirlere ilişkin düzenlemelere, Sözleşmenin ikinci bölümünün ikinci kısmında 14. ila 22. maddeler arasında yer verilmiştir. Bu kısımda yer alan düzenlemeler birer koruma tedbiri olması dolayısıyla bazı özellikler ve ön şartlar gözetilerek uygulanmalıdır. Koruma tedbirleri kanunla düzenlenmiş olmalı, hükümden önce temel bir hak sınırlaması getirdiği ve dolasıyla bir araç olduğu ve geçici olarak uygulanması gerektiği unutulmamalıdır. Koruma tedbirlerinin uygulanmasındaki ön şartlar; gecikmede tehlike bulunması, haklı

[87] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.133.
[88] Akpek, s.91.

görünüş, ölçülülük ilkesi doğrultusunda orantı bulunması, bir karara dayanması ile geçmişte işlenmiş bir suçun bulunmasıdır.[89]

Sözleşmede düzenlenen koruma tedbirleri Sözleşmede öngörülen suç tiplerine, bilgisayar sistemi aracılığıyla işlenen tüm suçlarda ve elektronik olarak kanıtların toplanmasına ilişkin olarak uygulanabilecektir.[90] Birinci kısımda olduğu gibi, bu kısımda da Taraf ülkelerin usul hükümlerinin uygulanabilmesi için gerekli yasal düzenlemeyi yapmaları beklenmektedir. 14. maddenin 2. fıkrası uyarınca, trafik verilerinin gerçek zamanlı toplanmasının düzenlendiği 20. madde ile içerik verilerinin takibine ilişkin 21. maddeye Taraf ülkeler çekince koyabileceklerdir.[91]

Sözleşmenin 15. maddesi şartlar ve tedbirleri düzenlemektedir. Bu düzenlemeye göre, Avrupa İnsan Hakları Sözleşmesi, Birleşmiş Milletler Medeni ve Siyasal Haklar Sözleşmesi ile uygulanabilir diğer uluslararası insan hakları belgeleri doğrultusunda temel hak ve özgürlüklerin gerekli ölçüde ve orantılılık ilkesi doğrultusunda temel hak ve özgürlüklerin teminat altında olacağına hükmolunmuştur. Buna ek olarak Taraf ülkelerin iç hukukunda da ilgili önlemleri alması gerektiği ifade olunmaktadır. Bu tedbirler daha önce ifade olunduğu üzere, Sözleşmede öngörülen suç tiplerine, bilgisayar sistemi aracılığıyla işlenen tüm suçlarda ve elektronik olarak kanıtların toplanmasına ilişkin olarak uygulanabilecektir ve doğrudan özel hayatın gizliliğine, temel hak ve özgürlüklerle teşkil edeceğinden çok dikkatli olarak

---

[89] Erdoğan, s.99 ve s.110.

[90] Sanal Ortamda İşlenen Suçlar Sözleşmesi, 14. maddesinin 2. Fıkrası.

[91] "Türkiye Cumhuriyeti, Sözleşme'ye taraf olurken imkan verilen kapsamda çekince imkanını kullanarak, 14/3-b maddesine "3*) 42. madde ve 14. maddenin 3(b) paragrafına istinaden, Türkiye Cumhuriyeti Devleti, herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak, söz konusu sistemin belli bir kullanıcı grubunun menfaatine işletiliyor olması; halka açık iletişim şebekelerini kullanmıyor olması ve halka açıkya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması halinde, söz konusu aktarıma ilişkin olarak 20 'nci ve 21 'inci maddelerde belirtilen önlemleri uygulamama hakkını saklı tutar.*" şeklinde çekince koymuştur. Dolayısıyla belli bir kullanıcı grubunun menfaatine işletilen bilişim sistemleri ile halka açık iletişim şebekelerini kullanmayan ve halka açık ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmayan bilişim sistemleri hakkında Sözleşmenin ülkemizde uygulanması mümkün değildir." Erdoğan, s.144-145.

uygulanması gerekmektedir. Bu bölümde teknik detaya girilmeyecek olup, maddeler hukuki olarak genel hatlarıyla incelenecektir.

a) Depolanan Bilgisayar Verisinin Süratli Şekilde Korunması (Madde 16)

Bu husus Sözleşmenin 16. maddesinde düzenlenmektedir. Bilişim verilerinin kolaylıkla değiştirilip ve yok edilebilir olması, bilişim suçlarının çoğunluğunun bilişim sistemleri aracılığıyla gerçekleştirilen iletişimden kaynaklanması ile yasadışı içerik veya suça ilişkin delilleri taşıyan iletişimin de bizzat delil özelliği taşımasının depolanan verilen korunma gerekliliği sebepleri olduğu ifade edilmektedir.[92] Değiştirilmeden önce ceza soruşturması veya kovuşturmasında ihtiyaç duyulan delillerin muhafazası evleviyetle önemlidir, zira tahrip edilmiş ya da yok edilmiş veri suçla mücadele konusunda dezavantaja ve hatalara sebebiyet verebilir.

Madde metninde yer alan 'bir kişinin mülkiyeti veya denetimi altında depolanmış bulunan belli bilgisayar verileri' ifadesi servis sağlayıcılar anlamını taşımaktadır. Ayrıca maddenin 3. fıkrasında Taraf ülkelerin, veri korumasından sorumlu olan kişilerin bu işlemleri gizli tutacağını zorunlu koşması gerektiği ifade edilmektedir. Bu durum hem kişilerin belli ölçüde temel haklarını hem de soruşturmanın gizliliğini koruyabilmektedir. Zira 14. ve 15. madde gereği gerekli şartlar ve tedbirler temin edilmelidir.

16. madde 29. maddenin uluslararası iş birliği hususundaki yansımasıdır ve 29. madde vasıtasıyla uygulanabilirliği sağlanmaktadır.[93] 29. madde ile başka bir Taraf ülkenin egemenliği altındaki verilerin korunması için diğer Taraf ülkelere talepte

[92] Erdoğan, s.149.
[93] Önok, s.1256.

bulunma imkânı getirilmiştir, bu husus maddenin incelendiği ilerleyen başlıkta detaylandırılacaktır.

b) Trafik Verisinin Süratli Şekilde Korunması ve Kısmen Açıklanması (Madde 17)

Halihazırda mevcut olan ve saklanmakta yani depolanmış olarak bulunan akış halindeki trafik verilerin korunmasını ve kısmen açıklanmasını sağlayabilmek için Sözleşmenin 17. maddesi getirilmiştir.[94] Veri trafiğinin bir ya da birden çok servis sağlayıcının katılıp katılmadığı bilgisinin tespit edilerek, verilerin güvenilirliğinin belirlenmesi amacıyla akış halinde olan trafik verisinin süratli şekilde korunması ve kısmen açıklanması konusunu düzenlemektedir.[95]

Depolanmış trafik verileri, geçmiş iletişimlerin kaynağı veya varış noktasının tespiti ve dolayısıyla çocuk pornografisi ya da kötücül yazılımların dağıtılması gibi suçları işlemiş olan kişilerin tespitinde büyük önem taşımaktadır.[96] Böylece kişilerin yerlerinin ve hizmet aldıkları servis sağlayıcılar tespit edilerek iş birliği talebinin kime yöneltileceği tayin edilmektedir.[97] Bu düzenleme, faillerin çıkış noktasını bulmak ve

---

[94] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.150.
[95] Erdoğan, s.164.
[96] Nacar, Fatma Burcu. *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları*. İstanbul Atılım Üniversitesi, 2010. s.57, çevrimiçi, http://cdn.legalbank.net/pdf/e4cce3daacbc42dc8a38f00d22852f94.pdf, Erişim Tarihi: 24.09.2022. Sözleşmeye İlişkin Açıklayıcı Rapor, Art.166, "Geçmişteki iletişimlerle ilişkili saklı trafik verilerinin elde edilmesi geçmişteki bir iletişimin kaynağını ya da varış noktasını belirlemek açısından kritik önemde olabilir. Bu bilgiler, örneğin, çocuk pornografisi dağıtan, bir sahtekarlık eyleminin parçası olarak yalan beyanlar dağıtan, bilgisayar virüsleri dağıtan, bilgisayar sistemlerine yasadışı olarak erişmeye teşebbüs eden ya da bunu başaran ya da bir bilgisayar sistemine sistemdeki verilere ya da sistemin uygun biçimde işleyişine müdahale eden iletişimler ileten kişileri saptamak açısından büyük önem taşımaktadır. Ancak, bu tür verilerin uzun süreli olarak saklanması gizliliği korumak için hazırlanmış yasalarca yasaklandığı ya da piyasa güçleri tarafından teşvik edilmediği için bu veriler genellikle ancak kısa bir süre için saklanmaktadır. Dolayısıyla, bu verilerin bütünlüğünü sağlamak için koruma önlemlerinin alınması büyük önem taşımaktadır."
[97] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.167, "Çoğu zaman bir iletişimin iletilmesine birden fazla hizmet sağlayıcı katılabilir. Her bir hizmet sağlayıcı, bu iletişimin iletilmesiyle ilgili, iletişimin kendi

iletişimin başlangıcını tayin bakımından oldukça önemlidir. 17. madde, 30. maddenin uluslararası iş birliği hususundaki yansımasıdır ve 30. madde vasıtasıyla uygulanabilirliği sağlanmaktadır.

Madde 16 ve 17'deki önlemler, hizmet sağlayıcıları gibi veri saklayıcılar tarafından halihazırda toplanmış ve saklanmış verilerin korunması için geçerlidir. Bu önlemler, gelecekteki trafik verilerinin gerçek zamanlı olarak toplanması ve tutulması ya da iletişimlerin içeriğine gerçek zamanlı erişim için geçerli değildir.[98]

c) Üretim Emri (Madde 18)

Üretim talimatı bir kişi ya da hizmet sağlayıcının mülkiyetinde olan bilgisayar verileri ve abonelik bilgileriyle ilgilidir.[99] Maddenin 3. fıkrasında abone verisinin ne anlama geldiği tanımlanmaktadır, bu çalışmanın tanımlar bölümünde açıklamasına yer verilmiştir. Sözleşmenin 18. maddesinde üretim emrine konu veri, 16. ve 17. maddelerde olduğu gibi saklanmış, depo edilmiş ya da var olan verileri konu almaktadır.[100] Dolayısıyla bir önceki maddelerde olduğu gibi, depolanmamış veriler, diğer bir ifadeyle gelecekte ortaya çıkması muhtemel veriler için uygulanabilir değildir.

Bu kısımdaki yetki ve usullerde spesifik cezai soruşturma ve takibatlar amaçlandığından üretim emirleri, genellikle, belirli abonelerle ilgili tek tek vakalarda

sisteminden geçişi üzerine kendi ürettiği ve tuttuğu ya da diğer hizmet sağlayıcılardan aldığı bazı trafik verilerine sahip olabilir. Bazen trafik verileri, ya da en azından trafik verilerinin bazı türleri, ticari, güvenlikle ilgili ya da teknik amaçlarla, iletişimin iletilmesine katılan hizmet sağlayıcılar arasında paylaşılır. Böyle bir durumda, iletişimin kaynağını ve varış noktasını belirlemek için gereken kritik trafik verileri hizmet sağlayıcılardan herhangi birinin elinde bulunabilir. Ancak, çoğu zaman, hiçbir hizmet sağlayıcı iletişimin gerçek kaynağını ya da varış noktasını belirlemeye yetecek miktarda kritik trafik verisine tak başına sahip değildir. Her bir hizmet sağlayıcı bütünün bir parçasına sahiptir ve kaynak ve varış noktasını belirlemek için bu parçaların her biri incelenmelidir."

[98] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.149.

[99] A.g.e., Art.172.

[100] A.g.e., Art.170.

kullanılır. Örneğin, üretim emrinde geçen bir isim esas alınarak bağlantılı bir telefon numarası veya e-posta adresi istenebilir ya da bu bilgiler esas alınarak ilgili abonenin isim ve adresi talep edilebilir. Hizmet sağlayıcının, veri madenciliği amacıyla, abone grupları hakkında gelişigüzel miktarlarda abonelik bilgisi ifşa etmesi yönünde hukuki talimatlar çıkarma yetkisi vermemektedir.[101]

Bu düzenleme ile ceza soruşturmaları için arama ve el koyma tedbirine göre daha az müdahaleci bir yöntem geliştirilmiştir.[102] Üretim emri bazen soruşturmada hazırlayıcı bir önlem olarak kullanılıp, daha sonra arama ve el koyma ya da diğer verilere gerçek zamanlı müdahale gibi farklı önlemlere başvurulabilir.[103]

Failden başka bir kişi ya da hizmet sağlayıcının mülkiyetinde ya da kontrolünde olan verilerin teslimi için özel bir düzenleme kaleme alınmıştır.[104] Sözleşmenin 18. maddesinde yer alan "mülkiyetinde ya da kontrolünde" ifadesi ile verilerin, yalnızca talepte bulunan Taraf ülkenin sınırları içinde bir kişi ya da hizmet sağlayıcının fiziksel mülkiyetin bulunmasını değil, fiziksel mülkiyeti dışında olsa dahi talepte bulunan Taraf ülkenin sınırları dahilinde verilerini serbestçe kontrol edebildiği durumları da kapsadığı ifade edilmektedir.[105]

d) Depolanmış Bilgisayar Verisinin Aranması ve El Konulması (Madde 19)

Depolanmış bilgisayar verilerinin aranması ve el konulması konusu ile ilgili düzenleme Sözleşmenin 19. maddesinde yer almaktadır. Bilişim cihazlarında ve

[101] A.g.e., Art.182.
[102] Akpek, s.98.
[103] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.175.
[104] Erdoğan, s.175.
[105] "Örneğin, ABD'de bulunan bulut bilişim sistemine Türkiye' den ulaşılabilmesi halinde 18 'inci maddenin tatbiki mümkündür. Ancak unutulmamalıdır ki, uzakta saklanan verilere teknik erişebilirdik tek başına bu maddenin tatbiki için yeterli değildir. Erişilen verinin o kimsenin mülkiyetinde ya da kontrolünde de olması gerekmektedir." Erdoğan, s.177, 178.

araçlarında yapılacak arama ve el koyma koruma tedbirinin suçun tespit edilmesi ile başlayan, soruşturma ya da kovuşturma evresinde gündeme gelebilen ve fakat özel hayatın gizliliği ve mahremiyet kavramlarına müdahale teşkil edebileceğinden zorunlu olmadıkça başvurulmaması gereken bir koruma tedbiridir.[106] Zira yalnızca bilişim suçları değil, soruşturma ve kovuşturmasına elektronik kanıtlara ihtiyaç duyulduğunda da kullanılabilecek olması dolayısıyla Sözleşmenin uygulama kapsamı oldukça geniştir.

Maddenin 1. fıkrasındaki hükmü doğrultusunda, yetkili makamlar, bilgisayar sisteminin tamamı veya bir kısmı, sistem içerisinde depolanmış bilgisayar verileri ve bilgisayar verilerinin depolanmış olduğu cihazlar üzerinde arama yapabilecek veya bunlara erişebilecek yetkilerle donatılmışlardır. Bu yetkinin verilmesi hususunda Tarafların gerekli yasal düzenlemeleri yapmaları beklenmektedir.

Maddenin 2. fıkrasına göre, eğer suça konu veriler üzerinde arama yapılan sistem üzerinden ulaşılabilecek bir başka bilgisayar sisteminde bulunuyorsa ve bu durum yeterli gerekçelerle açıklanabiliyorsa, yetkili makamlar diğer sisteme erişebilecek veya o sistem üzerinde de arama yapabileceklerdir.[107] Bir arama prosedürüyle ilgili olarak ilgili Tarafların bilgilendirilmesinin gerekip gerekmediği konusu da tartışılmıştır.[108] 1. ve 2. fıkralardaki tedbirler bakımından uzmanlardan

---

[106] Bostancı, Ümit / Benzer, Recep. *Türk hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma / Search, Copy And Seizure On The Computers In The Turkish Legal System*, International Journal of Human Sciences, sy.12, 2015, s.1194, çevrimiçi,https://www.idealonline.com.tr/IdealOnline/pdfViewer/index.xhtml?uId=38281&ioM=Paper&preview=true&isViewer=true#pagemode=bookmarks, Erişim Tarihi: 24.09.2022.

[107] Akpek, s.99.

[108] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.204. "Bazı Taraf Ülkelerin yasaları, geleneksel aramada bildirim yapma zorunluluğu getirmemektedir. Konvansiyonun bilgisayar araması için bildirim zorunluluğu getirmesi, bu Tarafların yasalarında bir tutarsızlık yaratacaktır. Diğer taraftan, bazı Taraf Ülkeler, genellikle gizli bir önlem olması amaçlanmayan saklı verilerin aranması ile gizli bir önlem olan akış halindeki verilere müdahale arasındaki ayrımı korumak için, bildirimi önlemin temel bir özelliği olarak değerlendirebilirler. Dolayısıyla bildirim konusunu belirlemek ulusal mevzuata bırakılmaktadır. Taraflar ilgili kişilere bildirim yapmanın zorunlu olduğu bir sistem getirmeyi düşünüyorlarsa, böyle bir

destek alınabilmesi hususu 4. Fıkrada düzenlenmektedir. Buna göre arama ve el koymanın en iyi ve en hızlı şekilde nasıl yürütülebileceğiyle ilgili teknik nitelikler konusunda, bilgisayar sistemlerine ilişkin özel bir bilgiye sahip sistem yöneticilerine danışılmasının gerekebileceği kabul edilmektedir. Dolayısıyla, hüküm, icra mercilerinin bir sistem yöneticisini arama ve el koyma konusunda yardımcı olmaya, makul sınırlar içinde, zorlamasına izin vermektedir.[109]

Maddenin 3. fıkrasında el koyma veya benzer şekildeki koruma tedbiri düzenlenmektedir. Yetkili makamlar, bir bilgisayar sisteminin tamamına veya bir kısmına, bilgisayar verilerini depolama cihazına el koymaya, bunları koruma altına almaya, bilgisayar verilerinin kopyasını almaya veya bunları tutmaya, bilgisayar verilerinin bütünlüğünü korumaya, erişim sağlanan bilgisayar sistemindeki verilere erişilmez kılmaya veya o sistemden kaldırmaya yetkili olacaklardır.[110]

e) Trafik Verilerinin Gerçek Zamanlı Toplanması (Madde 20)

Bilişim ağları aracılığıyla üretilen trafik verilerinin gerçek zamanlı olarak, diğer bir ifadeyle bilişim ağları aracılığıyla halihazırda devam etmekte olan iletişimin ortaya çıkarttığı ve diğer Taraf ülkelerin sınırları içinde olan[111] trafik verilerinin toplanması hususu düzenlenmektedir. Bu soruşturma tekniği sayesinde şüphelinin iletişimlerinin

bildirimin soruşturmaya zarar verebileceği de hesaba katılmalıdır. Böyle bir risk mevcutsa, bildirimin ertelenmesi seçeneği değerlendirilmelidir."

[109] A.g.e., Art.200.

[110] Akpek, s.99.

[111] "Taraf devletler ülke sınırları içerisinde Sözleşmeyi uygulamaktadırlar. Bu durumda hizmet sağlayıcılara getirilecek bu yükümlülükte hizmet sağlayıcının taraf devletin sınırlan içerisinde olması kaydıyla mümkündür. Burada hizmet sağlayıcı şirketin genel merkezinin o taraf devlette olması şart değildir. Bu durumda hizmet sağlayıcı şirketin genel merkezinin ya da şubelerinden en azından birinin o devlette olmaması halinde bu zorunluluğu uygulamamız mümkün olamayacaktır. Bilişim ağları bakımından coğrafi sınırların öneminin kalmadığını dikkate aldığımızda, artık hizmet sağlayıcı şirketlerin kanunları daha esnek ya da vergi politikası gelişmemiş ülkelere kayacağı şüphesizdir. Bu durumda o ülkelerin suçların işlenmesi içinde birer merkez haline geleceği gözden uzak tutulmamalıdır. … Google, Youtube gibi pek çok şirketin Türkiye' de ofis açmalarının zorunlu kılınmasının yerindeliği ortaya çıkmaktadır." Erdoğan, s.260, 261.

saat, tarih, kaynak ve varış noktasıyla kurbanların sistemlerine izinsiz girildiği tarih arasında bağlantı kurulabilir, diğer kurbanlar teşhis edilebilir ya da suç ortakları arasındaki bağlantılar ortaya çıkarılabilir. Bu sebeple bilgisayar iletişimleriyle ilgili trafik verilerini toplayabilmek oldukça önemli bir tedbirdir.[112]

Trafik verilerinin içerik verilerine kıyasla, iletişimin saat, süre ve büyüklüğü, kişiler ve düşünceleri hakkında çok az kişisel bilgi sağlaması dolayısıyla daha az müdahaleci olduğu kabul edilmektedir. Ancak, ziyaret edilen web siteleri gibi iletişimin kaynağı ve varış noktasına ilişkin verilerle ilgili olarak daha güçlü bir gizlilik sorunu mevcuttur. Bu verilerin toplanması, bazı durumlarda, bir kişinin ilgileri, bağlantıları ve toplumsal konumunun bir profilini çıkarmak için yeterli olabilecektir. Bu sebeple Taraflar, 14. ve 15. maddeler uyarınca bu önlemleri uygulamak için uygun önlem ve hukuki önkoşulları tesis ederken bu değerlendirmeleri göz önünde bulundurmalıdır.[113] Zira Sözleşmenin 14. maddesinin 3. fıkrası Taraflara bu maddenin uygulanmasının belirli suçlara veya suç kategorileri ile sınırlı tutulabileceğini ilişkin çekince koyma imkânı getirmektedir.

f) İçerik Verilerinin Takibi (Madde 21)

İçerik verilerinin, iletişim içeriği, yani iletişimin anlamı, niyeti ya da iletişim yoluyla iletilen mesaj veya bilgi anlamına geldiği, trafik verileri dışında iletişime ait olarak iletilen her şey içerik verisi olduğu ifade edilmektedir.[114] Bu koruma tedbiri ile örneğin şüphelinin e-posta yoluyla yapılan yazışmaları, uygulamalar üzerinden yapılan canlı sesli ve görüntülü iletişimleri izlenip kaydedilmektedir.[115] Böylesi müdahaleci bir

[112] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.218.
[113] A.g.e., Art.227.
[114] A.g.e., Art.229
[115] Erdoğan, s.290.

tedbirin uygulanmasında temel hak ve özgürlüklerin hassasiyetle gözetilmesi gerekmektedir.

İçerik verilerinin takibi koruma tedbiri için Sözleşmede öngörülen bazı önkoşullar bulunmaktadır. Bunlar; önceden işlenmiş bir dizi ciddi suç varlığı, söz konusu verilerin halihazırda devam eden iletişime ilişkin olması, verilerin önceden belirlenmiş belirli iletişimlere ilişkin olması, ülke sınırları içerisinde iletilen gerçek zamanlı içerik veriri olması, hizmet sağlayıcıların gizlilik yükümlülüğünün yüklenmiş olması ile Sözleşmenin 14. ve 15. maddelerine uygun olarak uygulanmasıdır.[116] Sözleşmenin 14. maddesinin 3. fıkrası uyarınca bir önceki madde gibi bu maddenin de uygulanmasında Taraflara çekince imkânı tanınmıştır.

1.2.5.3. Uluslararası İş Birliğine İlişkin Düzenlemeler

1.2.5.3.1. Genel İlkeler

Sözleşmenin 23. maddesi ile uluslararası iş birliğinde gözetilecek üç genel ilke öngörülmektedir. Buna göre; Taraf ülkeler mümkün olan en geniş kapsamda iş birliğini gerçekleştireceklerdir, suçun bir bilgisayar sistemi kullanılarak işlendiği ya da bir bilgisayar sistemi kullanılarak işlenmeyen sıradan bir suçla ilgili elektronik kanıtların bulunduğu durumlarda bu bölüm hükümleri geçerlidir ve son olarak bu bölüm hükümleri çerçevesinde hem de cezai meselelerde uluslararası iş birliğine ilişkin uluslararası belgelerin, tek taraflı ya da karşılıklı sözleşmelerin ve ulusal yasaların uygulanması yoluyla gerçekleştirilecektir.[117]

Suçluların iadesine ilişkin 24. madde, 14. madde kapsamında Tarafların çekince koyma imkânı olan trafik verilerinin gerçek zamanlı olarak toplanması

[116] Erdoğan, s.292-295.
[117] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.243.

konusunda yardımlaşma ile içerikle ilgili verilere müdahale edilmesi konusunda yardımlaşma hususunun düzenlendiği 33. ve 34. maddelere ilişkin uygulamalar Tarafların benimsemedikleri kapsam doğrultusunda değerlendirilmelidir.[118]

1.2.5.3.2. Özel Hükümler

a) Depolanmış Bilgisayar Verisinin Süratli Şekilde Korunması (Madde 29)

Bu madde ile Taraf ülkelerin bir başka Tarafın egemenliğindeki verileri talep etme imkânı bulunmaktadır. Bu talepte yer alması gereken unsurlar madde metninin 2. fıkrasında tek tek sayılmaktadır.

Önemle belirtmek gerekir ki, bu talep karşısında, talepte bulunulan Taraf ülke verileri mülkiyetinde bulundurmaya devam etmekte, yalnızca verilerin ifşasının isteneceği yardımlaşma talebinin uygulanmasına kadarki müddette, verileri muhafaza etmektedir. Bu aşamada veriler herhangi bir şekilde ifşa edilmemekte veya açıklanması söz konusu olmamaktadır.[119] Talepte bulunan ülkenin verilerin aranmasına, verilere el konmasına, benzer şekillerde güvence altına alınmasına, erişim sağlanmasına ya da açıklanmasını talep etmesine yetecek kadar en az 60 gün süreyle bu koruma sağlanmalıdır.[120] Tarafların çifte suçluluğu şart koşmadığı takdirde her iki Taraf ülkede de talebe konu olayın cezai nitelik taşıması gerekmemektedir.[121]

---

[118] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.243.
[119] Erdoğan, s.161
[120] Sanal Ortamda İşlenen Suçlar Sözleşmesi, 29. maddesinin 7. fıkrası.
[121] "Türkiye Cumhuriyeti, Sözleşmeye taraf olurken 29. maddenin 4. fıkrasına "42. madde ve 29. maddenin 4. paragrafına istinaden, Türkiye Cumhuriyeti Devleti, çifte suçluluk şartının verilerin açıklandığı tarihte yerine getirilemiyor olduğuna ilişkin gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması talebini reddetme hakkını saklı tutar" şeklinde çekince koymuştur. Bu durumda Sözleşmenin 2 ila 11. maddeler arasında kalan suçlar dışındaki suçlarda, Türkiye Cumhuriyeti'nin 16. madde bakımından çifte suçluluk prensibini ileri sürebileceği anlaşılmaktadır." Erdoğan, s.162.

Korunacak verileri tutan hizmet sağlayıcının bir suç grubu ya da bizzat soruşturmanın hedefi tarafından kontrol edilmesi örneğindeki gibi verilerin koruyucusunun soruşturmanın gizliliğini tehdit edecek ya da başka bir biçimde soruşturmaya zarar verecek bir eylemde bulunması ihtimalinin varlığı halinde, Sözleşmenin 29. maddesinin 6. fıkrası uyarınca, talebi yapan taraf devletin talepte bulunulan devlet tarafından derhal bilgilendirilmesi gerekmektedir.[122]

'Yardım talebine konu olan suçun kendisinden talepte bulunulan taraf ülkece siyasi suç veya siyasi suçla bağlantılı suç olarak değerlendirilmesi veya söz konusu talebin gereğinin yerine getirilmesinin kendisinden talepte bulunulan taraf ülkece kendisinin egemenliğine, emniyetine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğinin düşünülmesi' Taraflara iş birliği talebini reddetme imkânı olarak tanınmaktadır.[123]

b) Korunan Trafik Verilerinin Süratli Şekilde Açıklanması (Madde 30)

Talepte bulunan Taraf, faili tespit etmek ve suça ilişkin delillere erişebilmek amacıyla diğer Taraftan 17. madde kapsamında trafik verilerinin muhafaza etmesini talep edebilecektir. Bu trafik verileri bir suç soruşturması veya kovuşturması ile ilgili halihazırda depolanmış belli bir kişinin mülkiyetinde ya da kontrolünde olan bir trafik verisi söz konusu olmalıdır. Sözleşmenin 17. ve 30. maddelerinin birlikte uygulanması marifetiyle korunan trafik verilerine ilişkin açıklama talep edilebilmektedir. Ancak belirtmek gerekir ki burada yapılması beklenen açıklama trafik verilerinin bütünü ya da içeriğin açıklanması değil, iletişim sırasında verilerin aktarıldığı yolun tespit edilmesi ile sınırlıdır.[124]

[122] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.288 ve Erdoğan, s.157.
[123] Sanal Ortamda İşlenen Suçlar Sözleşmesi, 29. maddesinin 5. fıkrası.
[124] Erdoğan, s.170.

Bu madde ile korunan trafik verilerinin açıklanması bakımından hızlandırılmış bir usul öngörülmektedir. Madde kapsamında iletilen talebin yerine getirilmesi sırasında talepte bulunulan Taraf, tedbir konusu iletişimin aktarılmasında, başka bir ülkedeki hizmet sağlayıcının yetkili olduğunu anlarsa, talepte bulunan Tarafa ilgili hizmet sağlayıcısının ve verilerin aktarıldığı yolun tespit edilmesi için gerekli olan ölçüde, trafik verisini en kısa sürede açıklamalıdır. Bu hükmün sebebi, verinin genellikle birçok ülkeden geçmesidir, dolayısıyla verinin muhafazası için tek bir ülkeden talepte bulunmak yeterli olmayıp zincirdeki tüm ülkeler veya sunucular bakımından harekete geçmek gerekir.[125]

Talebe ilişkin suçun talepte bulunulan Taraf ülkece siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olarak değerlendirilmesi ile talepte bulunulan ülkenin trafik verisinin açıklanmasını yerine getirmesi kendi egemenliğine, emniyetine, kamu düzenine veya diğer menfaatlerine zarar vereceğinin düşünülmesi halinde Sözleşme trafik verilerinin açıklanması zorunluluğu ortadan kaldıran bir imkân getirmektedir.

c) Depolanan Bilgisayar Verilerine Erişimde Karşılıklı Yardımlaşma (Madde 31)

Bu maddede depolanan bilgisayar verilerine erişime ilişkin karşılıklı yardımlaşma hususu düzenlenmiştir. Sözleşmenin 31. maddesinin, 19. maddede ulusal düzeyde alınması öngörülen depolanmış veriler hakkında arama ve el koyma tedbirinin uluslararası adli yardımlaşma hukukundaki karşılığı düzenlendiği ifade edilmektedir.[126]

[125] Önok, s.1257, 1258.
[126] Özbek, s.139.

Burada söz konusu husus, bazı verilerin aranması, bunlara erişilmesi, el konulması, güvence altına alınması ya da açıklanması amacıyla, bir Taraf ülkenin diğer bir Taraftan talepte bulunmasıdır.[127] Maddenin 3. fıkrası uyarınca ilgili verilerin kaybolması ya da değiştirilmesi riskine ilişkin gerekçelerin varlığı ile Sözleşmenin 23. maddesinde belirtilen belgeler, düzenlemeler ve kanunlarda süratle iş birliğinde bulunulmasının öngörülmesi durumlarında bu madde uyarınca gelen talebe cevap verilmesinde hızlandırılmış prosedür öngörülmektedir.

d) Depolanan Bilgisayar Verilerine İzin veya Sınır Ötesi Erişim Sağlamak (Madde 32)

Sözleşmenin 32. maddesinde, oldukça kapsamlı tartışmalar sonucunda bu alanı düzenleyen kapsamlı, hukuki açıdan bağlayıcı bir rejim hazırlamanın henüz mümkün olmadığına karar vermişlerdir[128] ve sadece iki durumla kısıtlı olarak bu yetki tanınmıştır. Buna göre; her bir Taraf ülke, diğer Taraf ülkenin iznini almaksızın, herkesin kullanabileceği bir kaynakta bulunan, kullanımı herkese açık bilgisayar verilerine, bu veriler nerede yer alırsa alsın, ulaşabilecektir, kamunun erişimine açık olmayan ve başka bir Taraf ülkenin sınırları dahilinde saklanan veriler söz konusuysa, bu verilerin ulusal sınırlar içinde bulunan bir bilgisayar sistemi aracılığıyla elde edilebilmesi, bu verileri açıklama yetkisine sahip olan kişinin yasal rızası koşuluna bağlanmıştır. Diğer Taraf ülkenin izni olmaksızın, tek taraflı olarak, sınır ötesinde saklanan verilere erişimi konusundaki yetkisi kısıtlıdır.[129]

[127] Önok, s.1258.
[128] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.293.
[129] Önok, s.1258.

e) Trafik Verilerinin Gerçek Zamanlı Toplanması İçin Karşılıklı Yardımlaşma (Madde 33)

Sözleşmenin 20. maddesinin uygulaması 33. madde ile gerçek zamanlı şekilde trafik verilerinin toplanmasına dair karşılıklı yardımlaşma başlığı altında düzenlenmiştir. Tüm Taraf ülkelerdeki soruşturma yürüten merciler için diğer Taraf ülkelerde bilgisayar sistemleri aracılığıyla iletilen iletişimlerle ilgili trafik verilerini gerçek zamanlı olarak elde etme yeterliliği, verilerin izini sürerek bir iletişimi kaynağına kadar izleyebilmek bakımından oldukça önemlidir ve bütün Taraf ülkeler, diğer Taraflar için trafik verilerini gerçek zamanlı olarak toplamakla yükümlüdür. [130]

Sözleşmenin 14. maddesinin 3. fıkrasında trafik verilerine ilişkin 20. maddeye çekince konulması imkânı tanınmaktadır. Tarafların bu önlemin uygulama kapsamını uluslararası iş birliğine ilişkin genel ilkelerin düzenlendiği 23. maddede belirtilenlerden daha dar bir suç grubuyla sınırlamalarına izin verilmiştir.[131]

f) İçerik Verilerine El Konulmasında Karşılıklı Yardımlaşma (Madde 34)

İçerik verilerine ilişkin Sözleşmenin 21. maddesinin uluslararası iş birliğindeki yansıması bu maddedir. İçerik verilerinin özel hayata müdahale edici niteliği yüzünden, bu hususta yardımlaşma sağlama yükümlülüğü Tarafların geçerli anlaşma ve yasalarının izin verdiği ölçüde sağlanacağı ifadesi ile sınırlandırılmıştır.[132]

[130] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.295.
[131] A.g.e., Art.296.
[132] A.g.e., Art.297.

g) 7/24 İletişim Ağı (Madde 35)

Siber suçların ve elektronik kanıtların kolayca yok olabilen ve değiştirilebilir yapıları gereği etkin ve süratli iş birliği çok önemlidir.[133] Bu doğrultuda Sözleşme ile getirilen en önemli yeniliklerden biri, Taraf ülkelerin haftada 7 gün günde 24 saat erişilebilir irtibat noktaları kurulması ile sürekli ve anlık iletişim ağı kurulmasıdır. Bu 7/24 iletişim ağları ile Sözleşme kapsamındaki iş birliğinin gerçekleştirilmesi mümkün kılınmıştır.

Söz konusu yardım teknik öneri sağlanması, depolanmış bilgisayar verisinin süratli şekilde korunması ile korunan trafik verilerinin süratli şekilde açıklanması uyarınca verilerin korunması ile delil toplanması, yasal bilgi sağlanması, şüphelilerin yerlerinin tespit edilmesi hususlarında kolaylık sağlanmasını, iç hukuk ve uygulamaların izin vermesi halinde doğrudan teminini içerecektir. Taraflar irtibat noktasını bağlı olduğu birimi tayin etme konusunda özgürdür,[134] adalet bakanlığı, içişleri bakanlığı, istihbarat birimleri, savcılık birimleri ya da başka bakanlıklar gibi yapıların bünyesinde konumlandırabilirler.[135] Bütün irtibat noktalarının uygun teçhizata sahip olması ile bilgisayar suçları ve bilgisayarla bağlantılı suçlar ile bunlara nasıl etkin bir biçimde karşılık verileceği konusunda eğitimli ve donanımlı personel varlığı şart koşulmaktadır.

---

[133] Süratli iş birliğinin temini için 2. Ek Protokol ile kullanılacak ortak dil hususunda düzenleme getirilmiştir. Böylelikle tercüme süreci ile hataların en aza indirilmesi ve zaman kaybının ortadan kaldırılması amaçlanmaktadır. Konu ilgili başlıkta detaylı olarak açıklanacaktır.

[134] Sözleşmeye İlişkin Açıklayıcı Rapor, Art.300.

[135] "Türkiye Cumhuriyeti, 7/24 İrtibat Noktası olarak Siber Suçlarla Mücadele Daire Başkanlığını belirlemiştir. Ancak irtibat noktasının Adalet Bakanlığı bünyesinde kurulu bulunan Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü olmasının daha doğru olacağı"(Akpek, s.127) konusunda görüşler vardır.

1.2.6. Sözleşmeye İlişkin Değerlendirmeler

1.2.6.1. Temel Hak ve Özgürlükler ile Veri Paylaşımına İlişkin Değerlendirmeler

Sözleşme, özgürlükçü ve demokratik yaşamın vazgeçilmezi olan internet kullanımına ilişkin ceza hukuku müdahalesi teşkil eden bir düzenlemedir ve böylesi bir düzenleme yapılırken yapısı gereği özgür ve açık olması gereken internet üzerinde temel hak ve özgürlüklerin sınırlandırılmasında ve müdahalesinde oldukça hassas ve titiz olunması gereklidir.[136]

Sözleşme uygulanırken, insan haklarını korumada göz önünde bulundurulacak olan Avrupa İnsan Hakları Sözleşmesi, Birleşmiş Milletler Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi ve diğer uygulanabilir uluslararası insan hakları belgelerine atıf yapılmıştır.[137] Her ne kadar Sözleşme uygulanırken uluslararası insan hakları belgelerine uygun ve orantılı olarak hareket edileceği belirtilmişse de niteliği gereği hassas olan temel hak ve özgürlüklere müdahale konusunda Sözleşmenin eleştirilen ve eksik kalan özellikleri bulunmaktadır. Sözleşmenin internet üzerinde ifade özgürlüğünü engellediği yönünde görüşler bulunmaktadır.[138]

1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi[139] ve bununla ilgili olarak 1999 tarihli Tavsiye

---

[136] Önok, s.1236.
[137] Sanal Ortamda İşlenen Suçlar Sözleşmesi, Giriş kısmı ve 15. madde.
[138] Keyser, s.324.
[139] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108, Strasbourg, 28 January, 1981. https://rm.coe.int/1680078b37#:~:text=The%20purpose%20of%20this%20Convention,(%22data%20protection%22). Türkçe çevirisi için 1981 Tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi. https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf.

R(99)5[140] olmasına rağmen, Sözleşmede internette gizlilikle ilgili olarak veri koruma ilkelerine ciddi bir bağlılık eksikliği görülmektedir.[141] Zira Sözleşmede verilerin korunmasına ilişkin güçlü ve belirgin bir vurgu yapılmamış, yalnızca giriş kısmında ülkelerin 1981 tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne dikkat edileceği ile ilgili atıf yapılarak, kişisel verilerin korunması gerekliliği hususunda bir farkındalıklarını bulunduğu ifade edilmiş, ancak Sözleşmenin veri ihlallerine sebep olacak maddelerinde ayrıca 1981 tarihli sözleşmeye tekrar atıf yapılmamıştır.[142]

Ayrıca, Sözleşmenin aralarında kolluk kuvvetlerinin de yer aldığı yetkili makamlarına soruşturmada olan yetkilerini orantısız bir şekilde genişletmekte olduğu da düşünülmektedir. Sözleşme, kolluk kuvvetlerine yapılan telefon aramaların kaynağı, yönü ve süresi gibi çok geniş çaplı trafik verilerine erişme imkânı vermektedir. Kolluk kuvvetlerince yapılan böylesi bilgi taleplerinde internet hizmet sağlayıcılar, müşterilerinin hangi internet sitesini ne kadar süre ziyaret ettiği, kaç tane resim indirdiği ve hangi hesaplara e-posta gönderdiği gibi bilgileri ifşa etme zorunluluğu altında kalmaktadır. Kolluk kuvvetlerinin de 20. ve 21. maddelerde öngörülen bir mahkeme kararına gerek duyulmaksızın kullanabilecekleri yetkileri dolayısıyla belirtilen bilgilere ulaşabilecek ve gerekirse hizmet sağlayıcıların bu uygulamayı gizli tutmaya zorlanması sonucunda merciiler gizlilik içerisinde teknik izleme yapabilecektir. Bu durum büyük ihlallere sebep olmakta ve dolayısıyla bireylerin mahremiyet ve özel hayatın gizliliği gibi temel haklarını ihlal etmektedir. Ayrıca,

[140] The Council of Europe Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers, Deputies, http://cm.coe.int/ta/rec/1999/99r5.htm.
[141] Akdeniz, Yaman. *An Advocacy Handbook For The Non Governmental Organisations, The Council Of Europe's Cyber-Crime Convention 2001 And The Additional Protocol On The Criminalisation Of Acts Of A Racist Or Xenophobic Nature Committed Through Computer Systems*, 2003, updated and revised in May 2008, s.11, çevrimiçi, https://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf, 10.04.2022.
[142] Akdeniz, s.11.

isteme konu verilerin muhafazası ve Sözleşmeye Taraf bir ülkenin talebi üzerine doğrudan temin edilmesi, özel hayat ve şirketlerin "müşteri gizliliği" politikaları bakımından ihlal teşkil edecektir.[143]

1.2.6.2. Sözleşmenin Usul Hükümlerinin Uygulama Kapsamındaki Değerlendirmeler

Sözleşmenin usul hukuku kısmında yer alan usul hükümlerinin kapsamı başlıklı 14. maddesinin içeriği eleştirilmektedir. Bu maddeye göre, söz geçen yetki ve usuller Sözleşmenin 2 ila 11. maddelerinde tanımlı suçlar, bilgisayar sistemi aracılığıyla işlenene 'diğer' suçlar ile cezai bir suçun delillerinin elektronik ortamda toplanması durumlarında uygulanacaktır. Bu bölümün kapsamı içerik verilerine müdahale etme yetkisinin iç hukukta belirlenecek bir dizi ağır suç ile sınırlandırılacağını öngören 21. madde ile sınırlandırılmış olsa da kapsamının neden bu Sözleşme ile tanımlanmayan cezai suçları da kapsayacak şekilde ve ne anlama geldiğinin hiçbir şekilde açık olmayan şekilde genişletildiği hala belirsizliğini korumaktadır.[144] Sözleşmede yer alan suç tanımları kısıtlıdır, Sözleşmeye ekleme yapmaktaki bürokratik zaman kayıpları nedeniyle ve siber suçların değişen yapısına ayak uydurabilmek adına bu şekilde geniş kapsamlı bir düzenlemenin suç mağdurlarını korumaya hizmet edeceğini düşünmekle birlikte insan haklarına ve veri ihlallerine sebep olma riski dolayısıyla bu düzenlemeyi tartışmaya açık görmekteyiz.

Siber Suç Sözleşmesi'nin uygulama sürecinde usule ilişkin yetkilerin ve hükümler yalnızca Sözleşmede yer alan suçlarla sınırlı olması tavsiye edilmektedir.[145] Hem özel hayatın gizliliği hem de iletişim özgürlüğüne bir müdahale teşkil

[143] Uçkan, Özgür ve Beceni, Yasin. *Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk (derleyen Yeşim M. Atamer),* İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.383-384.
[144] Akdeniz, s.9.
[145] Akdeniz, s.9.

edeceğinden ancak "bir dizi ağır suç" kavramının açık tanımı Sözleşmede yer almaması ve Taraf ülkelerin ulusal hukuk düzenine bırakılması durumunun keyfi uygulamalara ve ciddi veri ihlallerinin yanı sıra temel hak ve özgürlüklerin korunması bakımından da risk doğuracak niteliktedir.[146] Sözleşmenin ulusal düzeyde alınacak tedbirler hükümlerinin yer aldığı ikinci kısmında öngörülen bir takım soruşturma yetkileri; cüz'i nitelikteki ihlaller karşısında dahi özel hayatın gizliliğine ilişkin ağır müdahaleler teşkil etmektedir.[147]

1.2.6.3. Servis Sağlayıcılar Yönünden Oluşacak Olan Yükler Bakımından Değerlendirmeler

Özel sektörde Sözleşmeye farklı bakış açıları vardır; özellikle telif hakkı sahipleri güçlü bir şekilde Sözleşmeyi savunurken, internet hizmet sağlayıcıları ve diğer ağ operatörü kuruluşları, müşterilerinin "kullanıcı verisi" adı altındaki gizli nitelikteki verilerini devlet birimleriyle paylaşmada isteksizdirler ve bunun yanı sıra Sözleşmenin kendilerine oldukça ağır bir yük getireceğinden de endişe duymaktadırlar.[148] Ceza soruşturmaları için bu kurumlardan, telekomünikasyon kanunları hükümlerinin ötesinde bilgi talep edilmektedir. Hizmet sağlayıcıların bu boyutta talepleri karşılayabilmesi için çok büyük hacimde verinin muhafazası gereklidir ve bu durumun kurumlar için büyük masraf oluşturacağından endişe duyulmaktadır. Veri muhafazası ve hizmeti sunabilmek için yapılan bu masraflar da hizmet sağlayıcıların kullanıcıların yüksek bağlantı ve abonelik ücretleri olarak yansıtılacaktır.[149]

---

[146] Keskin Kiziroğlu, Serap. *Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*, 2013, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 59, Sayı 1-2, s.157.
[147] Uçkan ve Beceni, s.383-384.
[148] Vatis, s.218.
[149] Keyser, s.325.

Öte yandan Sözleşmede, servis sağlayıcıların trafik verilerini düzenli toplaması veya belirli süre boyunca saklaması gerekliliği hususuna dair herhangi bir hüküm bulunmamaktadır.[150] Servis sağlayıcıların verileri tutması ve paylaşması husus her ne kadar veri gizliliği ihlâllerine sebebiyet verebilecek ise de bir yandan bu şekilde bir zorunluluklarının bulunmaması da işlenen siber suçların soruşturulması ve kovuşturulması bakımından önemli nitelikteki verilerin yok olması ve suçluların cezalandırılamaması riskini de oluşturmaktadır.

Bir yandan Sözleşmenin uygulanmasında, her bir Taraf ülkenin soruşturmalar için uluslararası iş birliğindeki istekliliği ve bağlılığındaki belirsizlik Sözleşmenin sağlayacağı yararlara gölge düşürmektedir.[151] Zira suçu işleyen failin bulunduğu ülke, suçun meydana geldiği ülke kadar zarar görmemektedir. Bu sebeple, failin bulunduğu ve iş birliği talep edilen ülke zarar görmediği için ekonomik olarak masraf yapmak ve personelini çalıştırmak istemeyebilir, bu durumun yaşanan mağduriyete ve iş birliği taleplerine aynı hassasiyette yaklaşılmaması ihtimalini doğurabileceği düşüncesindeyiz.

1.2.6.4. Siber Suçların Değişen Yapısına Uyum Sağlama Bakımından Değerlendirmeler

Siber suçların sürekli güncellenen yapısı karşısında bu hususu düzenleyen hukuki bir metnin de sürekli güncellenmesi gerekmektedir. Suç yapılarının değişmesi ve çeşitlenmesi aynı çeşitliliği Sözleşme için de gerekli hale getirmekte, yeni suç tiplerinin süratle dahil edilmesi gerekmektedir.

Sözleşme ile ilgili değişikliklerin ne yolla yapılacağı, Sözleşmenin 44. maddesinde düzenlenmektedir. Buna göre; herhangi bir Taraf Sözleşme ile ilgili

[150] Önok, s.1246.
[151] Weber, s.442.

herhangi bir değişiklik yapılması önerisinde bulunulduğunda, öncelikle bu değişiklik talebi Avrupa Konseyi Genel Sekreteri tarafından ülkelere bildirilecektir. Önerilen değişiklik talebi, CDPC'ye bildirilecek, ardından bu Komite görüşlerini Bakanlar Komitesi'ne sunacaktır. Bu görüşler ve değişiklik önerisi Bakanlar Komitesi tarafından incelenerek ardından ülkelerle istişare edilecek ve bunun sonucunda kabul edilebilecektir.

Sözleşmede değişiklik yapılmasına ilişkin getirilen düzenleme; siber suçların çok hızla değişen ve çeşitlilik oluşturan yapısına karşı Sözleşmede eksik kalan kısımların tamamlanmasında veya değiştirilmesinde çok ağır bir bürokratik işleyişe sebep olabilmektedir.[152] Bu durum, Sözleşmenin yeni risklerin gerisinde kalmasına ve etkin mücadelede engellere sebep olacaktır.

Uluslararası sözleşmelerdeki değişiklikler ulusal mevzuattan daha meşakkatlidir. Ancak siber suçlarla etkin şekilde mücadele etmeyi amaçlayan uluslararası nitelikteki bir sözleşmenin, siber suçlardan farklı hususları düzenleyen uluslararası sözleşmelere kıyasla daha hızlı ilerleyecek bir usul benimsemesi beklenmektedir. Zira siber suçlar, ceza kanunlarının bütün sorunlara çözüm sağlayamayacağı türde benzersiz ve önemli sorunlar doğurabilir. Siber suçların hızla değişen ve gelişen teknolojiye dayalı olması, geleneksel hukuk anlayışının ve süreçlerinin yavaş ilerlemesi sebebiyle, çıkarılacak kanunların bu değişikliklerle baş edebilecek yeterlilikte olmasını gerektirmektedir, bunun mevcut olmaması ve uzun müddet sonra gerçekleşen elverişsiz yasa değişiklikleri durumunda da alternatif denetim mekanizmalarına güvenmek durumunda kalınacağı ifade edilmektedir.[153]

[152] Weber, s.442.
[153] Önok, s.1245.

Mevzuatın siber suçlara uyarlanmasında klasik hukuk anlayışı ve ağır işleyen bürokratik yollar terk edilerek, farklı bir yöntem benimsenmelidir. Siber suçlar hususunda hızlı cevap ve en az düzeyde bürokrasiye şiddetle ihtiyaç vardır. Avrupa Komisyonu'nun oluşturacağı bir komitenin süreklilik arz edecek şekilde toplantılar yaparak, güncel suç görünüşleri ve uygulanabilecek yeni hükümler için yasal reformlar yapılması veya alternatif yapılar oluşturması gerektiği, aksi taktirde şekil değiştiren siber suçların faillerin cezasız kalması sonucunun oluşacağı görüşündeyiz.

Rusya'nın daha önce BM toplantılarında sunmuş olduğu öneriler; başka bir ülkenin bilgi kaynakları ve sistemlerini etkileyecek veya zarar verecek nitelikte araçlarının geliştirilmesi, yaratılması ve kullanılması ile casusluk amacıyla daha sonra kullanılmak üzere başka bir ülkenin bilgisayarlarına kötü amaçlı yazılımın gizlice yerleştirilmesi fiillerinin mevzuatta suç tanımı olarak düzenlenmesidir.[154] Buna ek olarak çocuk pornografisi için ses kayıtları ile çocukların tasvir edilmesi de suç olarak düzenlenmemektedir.[155] Sözleşmede yer alan suç tanımları bu şekilde eksik kalan suçlar eklenerek genişletilebilir ve böylesi bir eklemenin Sözleşme için de geliştirici olabileceği görüşündeyiz.

1.2.6.5. Taraf Ülkelerin Sınır Ötesindeki Verilere Tek Taraflı Erişimleri ile Bu Erişimlerin Ulusal Egemenlik İlkesine Etkisi Bakımından Değerlendirmeler

Sözleşmenin, Tarafların yardım talebinde bulunmaksızın ne zaman başka bir Taraf ülkede saklanan bilgisayar verilerine tek taraflı olarak erişebilecekleri hususuna açıklık getirmekte eksiklikleri vardır. Sözleşmenin Açıklayıcı Rapor Taslağı'nda; ülkelerin tek taraflı olarak sınırları ötesinde hareket etmeleri hususunda serbest oldukları ve fakat Komisyon'un yeterli deneyiminin bulunmaması ve genel kurallar formüle etmenin güçlüğü sebepleriyle bu hususu netleştirmeyi reddettikleri açık bir

[154] Vatis, s.222.
[155] Akpek, s.28.

şekilde ifade olunmuştur. 39. maddenin 3. fıkrasında ne izin verildiği ne de engel konulduğu belirtilmemiştir.

Sözleşmeyi kaleme alanlar tarafından etraflıca konunun tartışılmış olmasına karşın Komisyon'un yeterli deneyiminin bulunmaması ve genel kurallar formüle etmenin güçlüğü sebepleriyle bağlayıcı bir kural konulamayacağı kararlaştırılmıştır. Daha fazla deneyim elde edilene kadar, 32. maddede herkesin tek taraflı hareket etmesinin mümkün olduğunda anlaştığı durumların belirtilmesiyle yetinilmesine karar verilmiştir. Sözleşmenin şimdiki halinde ifade olunan, yalnızca söz konusu erişilen verilerin kamuya açık olduğu ve verileri ifşa etme yetkisi bulunan kişinin yasalara uygun ve gönüllü olarak rıza gösterilmesi durumlarında erişme imkânı bulunmaktadır.[156]

Rusya'nın Sözleşmeye karşı çıkmasının en büyük nedenlerinde biri, bu maddenin varlığıdır. Veri sahibinin rızasıyla, ülkelerin kolluk kuvvetleri marifetiyle sınır ötesinde bilgisayarlara ve verilere tek taraflı olarak erişebilme yetkilerini ulusal egemenlik ilkesine bir ihlal olarak görmektedir. Bunu yanı sıra bazı görüşler Rusya'nın Sözleşmeyi imzalamamasının gerçek nedeninin bir kısmı Rus devletinin desteğiyle ya da hoşgörü sağlamasıyla gerçekleştirildiği şüphelenilen ve Rusya'dan kaynaklanan çok sayıda siber saldırının soruşturmasında başka ülkelere yardımcı olma yükümlülüğünü üstlenmek istememesi olduğunu savunmaktadır.[157]

---

[156] Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı ve Açıklayıcı Memorandumu / Haz: Siber Suç Uzmanları Komitesi, Çevirisi: İnternet ve Hukuk Platformu, Ankara Barosu, 2008, 3.Baskı, 293. ve 294. madde. http://www.ankarabarosu.org.tr/siteler/1940-2010/kitaplar/pdf/a/sibersuclar.pdf, çevrimiçi, Erişim Tarihi: 10.03.2022. Orijinali için bkz. https://rm.coe.int/16800cce5b.

[157] Vatis, Michael A. s.218. Ayrıca, bu varsayımı destekleyici nitelikte bir örnek; dünyanın en büyük petrol ve gaz üreticisi olan Suudi Aramco Şirketi'ne 2021 yılının Temmuz ayında düzenlenen siber saldırıdır. Saldırganlar çalmış oldukları veriler karşısında, şirkete 50 Milyon Dolar şantaj yapmıştır. Bazı analistler, raporlarında kötü amaçlı yazılımın Rusya ile İran arasındaki iş birliğinin ürünü olabileceğini ve olası failler olduklarını düşünmektedir. (Ayrıntılı bilgi için bkz. Çevrimiçi, https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/, çevrimiçi, Erişim Tarihi: 10.01.2022.) Rusya ve Çin gibi ülkelerin çevrimiçi muhalefete sansür uygulamak ve engellemek için yetkilerini diledikleri gibi kullanabilmektedir. Hatta Rus istihbaratının fidye çetelerine

1.2.6.6. Sözleşmenin Küresel Temsili Bakımından Değerlendirmeler

Yalnızca siber suçlar değil, herhangi bir suçla mücadele için mutabık kalınan bir hukuki metin ortaya koymak her zaman zor olmuştur.[158] Sözleşmenin Avrupa Konseyi tarafından hazırlanması ve imzaya sunulması da eleştirilere neden olmuştur. Avrupa Konseyi'nin bölgesel bir örgüt olması sebebiyle, evrensellik kazanmasında engeller olabileceği ve Sözleşmenin etkisini artırabilmek ve daha fazla sayıda ülkenin dahil olmasını sağlayabilmek için Sözleşmeyi akdetme görevinin Birleşmiş Milletler'e verilmesi gerektiği de görüşler arasındadır.[159]

Suçla mücadelede ortak bir hukuki metin koymanın zorluğunun bilincinde olarak, 2022 yılı itibariyle Kanada ve Senegal gibi Avrupa Konseyi üyesi olmayan pek çok sayıda ülke tarafından Sözleşmenin kabul edilmiş olması sebebiyle bu görüşe belli ölçüde katılmamaktayız, ancak menfaatlerine hizmet edecek olsa dahi Rusya gibi Avrupa yapılaşması fikrine temelden karşı olan ülkelerin böyle bir anlaşma içinde bulunabilmesi pek mümkün olmayacağından, BM gibi bir yapının bu konuda bir düzenleme yapması gerektiği düşüncesine de belli ölçüde katılmaktayız.

Her ne kadar ülkelerin ortak olarak mutabık kaldıkları bir metin hazırlansa ve ülkeler tarafından imza atılsa dahi metinlerin hukuki bağlayıcılık kazanabilmesi için ülkelerin imza sonrasında metni onaylaması gereklidir. Sözleşme onay ve taraf olma süreci çok zaman almakta ve yavaş işlemektedir. Örneğin, Türkiye Sözleşmeyi 2010 yılında imzalamış, ancak 4 yıl bekledikten sonra 2014 yılında onaylamıştır. Ancak metnin onaylanması tek başına hukuki metnin tam anlamıyla uygulanmasını sağlamamakta, uluslararası sözleşmelere ülkeler tarafından pek çok hükmün etkisini

güvenli bir liman sağladığı, dolaylı olarak istihdam dahi ettiği ile ilgili çalışmalar mevcuttur. (Ayrıntılı bilgi için bkz. Lubin, s.14.)

[158] Akpek, s.29.

[159] Erdem ve Özocak, s.5

ortadan kaldıracak nitelikte çekinceler konulabilme imkânı tanınmaktadır[160] ve Avrupa Konseyi Siber Suç Sözleşmesi'ne de pek çok ülke tarafından[161] çekinceler konulmuştur. Bu husus bir sonraki alt başlıkta detaylandırılmıştır.

1.2.6.7. Sözleşmenin Uygulanması Bakımından Değerlendirmeler

Sözleşmenin hükümlerinin Taraf ülkeler için bir zorunluluk teşkil etmemesi, ülkelere serbesti tanıması ve çok sayıda çekince koyma imkânı tanıması sebepleriyle Sözleşmenin etkililiği bakımından eleştiriler ve öneriler mevcuttur. Sözleşme hazırlanırken, CDPC'nin isteği üzerine hazırlanan Profesör H.W.K. Kaspersen'in "Konvansiyon gibi tavsiyeden daha çok yükümlülük getiren bir hukuki araca başvurulmalıdır." ifadesini içeren raporun da dikkate alınmış olmasına[162] rağmen, Sözleşmede yer alan hükümlerin ülkeler tarafından uygulanma zorunluluğu ve bağlayıcılığı olduğu hakkında bir ifade ve hükümlerin icra edilmemesi durumunda öngörülen bir yaptırım, raporlama ya da denetim mekanizması Sözleşmede bulunmamaktadır ve adli yardımlaşmanın reddedilmesi hususunda Taraf ülkelere çok geniş bir hareket serbestisi tanınmaktadır. Bu durum Sözleşmenin etkililiği açısından bir sorun oluşturmaktadır. Zira yaptırım uygulamadan hukuka aykırı olan davranışları düzenlemek imkansızdır.[163]

Ülkeler, kendi ülkelerinde meydana gelen saldırılardan sorumludurlar. Sözleşmede Taraf ülkelere tanınan iş birliğini reddetme serbestisi daraltılmalıdır. Gelen iş birliği taleplerine cevap vermenin, ülkenin ulusal egemenliğini, güvenliğini,

[160] Akpek, s.29-30.
[161] Bkz. Hangi ülkenin hangi maddelere çekince koyduğu ile ilgili detaylı bilgiye, Avrupa Konseyi Siber Suç Sözleşmesi'nin numarası olan 185 CETS (Council of Europe Treaty Series) ve ülke adı ile sorgulatarak erişilebilir, çevrimiçi, https://www.coe.int/en/web/conventions/concerning-a-given-treaty, Erişim Tarihi: 18.03.2022.
[162] Explanatory Report to the Convention on Cybercrime, II.The preparatory Works, m.10, s.2, çevrimiçi, https://rm.coe.int/16800cce5b, Erişim tarihi: 18.03.2022.
[163] Weber, s.425.

devlet düzenini ve diğer kamu menfaatlerini zarara uğratacağı ile ilgili "önyargıları" gibi net ve inandırıcı olmayan gerekçelerle iş birliği taleplerinin reddedilebilmesi, ülkelere çok fazla esneklik tanımaktadır ve etkin iş birliği için bunun önünde geçilmesi gereklidir. Bu hususta çeşitli çözüm önerileri sunulmaktadır.

Bir Taraf ülkenin yardım talebi reddedildiğinde, geçerli bir sebebe dayanmayarak talebi reddeden ülkeden tazminat isteme hakkı olacağı Sözleşmeye eklenebilir ve bu tazminatın kararını verme yetkisi tarafsız bir hakeme bırakılabilir. Böylesi bir düzenlemenin ülkeler tarafından kabul edilmesi her ne kadar pek olası gözükmese de en azından iş birliğini reddeden ülkenin ret sebebinde meşru olmayan gerekçeler beyan ettiğinin tespiti tarafsız bir hakemce yapılabilmelidir, kuşkusuz böyle bir düzenleme caydırıcı olacaktır. Bunun yanında, Taraf ülkelerin CDPC ya da başka bir kuruluşa belirli aralıklarla iş birliğinin reddetme sebeplerini yazılı olarak raporlaması ve raporların yayınlanması gerektiği ile ilgili bir düzenlemeyi ihtiva edecek şekilde Sözleşmede güncelleme yapılabilir. Önerilen diğer ve en radikal olan çözüm ise meşru ve güvenilir bir ret gerekçesi olmaksızın talebin reddedilmesi ve talep eden ülkenin çok yıkıcı bir siber saldırıya uğraması gibi bir durumda; talepte bulunan ve reddedilen Taraf ülkeye, talepte bulunulan ülkedeki bilgisayarların uzaktan aranması, saldırıda bulunan bilgisayarların uzaktan işlevsiz hale getirilmesi gibi tek taraflı sınır ötesi soruşturma faaliyetlerine girişme yetkisi verecek bir değişikliktir. Böylesi bir düzenlemenin çok dikkatle ve hangi durumlarda uygulanabileceğinin çok açıkça tanımlanarak hazırlanması gereklidir.[164] Her ne kadar çok işlevsel olacağı öngörülse de bu uygulamalardan bir kısmı ülkelerin ulusal egemenlikleri bakımından çok büyük risk oluşturacağı için kabul edilebilmeleri pek olası gözükmemektedir.

Veriye dayalı teknolojilerin büyümesine, siber suçların artması ve evrimine rağmen, Sözleşmede yer alan kavramlar teknolojiden bağımsızdır, böylece maddi ceza

[164] Vatis, s.221.

hukuku hem mevcut hem de gelecekteki teknolojilere uygulanabilir.[165] Sözleşmenin kusurlarına rağmen siber suçlarla ilgili yargısal zorlukları çözmede var olan en iyi çözüm olduğu ifade edilmektedir.[166] Bu çalışmanın ilerleyen bölümlerinde Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin Siber Suç Sözleşmesi'ne İkinci Ek Protokol ile bu eksikliklerin ne ölçüde giderildiği ve giderilme imkanı olabileceği incelenecektir.

[165] Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Explanatory Report, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, çevrimiçi, Erişim Tarihi: 17.04.2022.
[166] Weber, s.425.

İKİNCİ BÖLÜM

2. GELİŞMİŞ İŞ BİRLİĞİ VE ELEKTRONİK KANITLARIN İFŞASINA İLİŞKİN İKİNCİ EK PROTOKOL

2.1. GİRİŞ

Siber suçlar artık insan haklarına, hukukun üstünlüğüne ve ülkelerin demokratik düzenlerine karşı bir risk olarak kabul edilmektedir. Çocukların cinsel istismarı, bireylerin itibarına zarar vermek, verilerin çalınması ile kötü amaçla kullanılması, seçimlere müdahale edilmesi ile demokratik kurumların işleyişine zarar verebilecek eylemler, DDoS ve kötücül yazılımlar aracılığıyla kritik altyapılara karşı saldırılar, teknolojinin terörizm amacı ile kullanılması ve daha pek çok şekilde karşımıza çıkabilmektedir. 2020'den bu yana sürmekte olan Covid-19 pandemisi sürecinde aşı geliştiren sağlık birimleri ve hastanelerin alan adları kötü amaçlı kullanılarak sahte aşı ve tedavi reklamı yapmak gibi çeşitli eylemlerle de karşımıza çıkmıştır.[167]

Sözleşme, hazırlandığı yıllarda, DDos, bilgisayar virüsünün yayılması gibi siber suçlardan etkilenen birden fazla ülkede soruşturulabilmesi ve kovuşturulabilmesi için yasaları uyumlu hale getirmeye ve sınırlar arası iş birliğini artırmaya odaklanmıştır. Sözleşme, bulut bilişimin gelişmesinden ve teknolojinin günümüzdeki önemini kazanmadan çok önce, kanıtların büyük çoğunluğunun ülkelerin kendi

[167] Protokole İlişkin Açıklayıcı Rapor, Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Explanatory Report, Art.5.
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, çevrimiçi, Erişim Tarihi: 17.04.2022.

sınırları içinde tutulduğu zaman yazılmıştı. Bu nedenle Sözleşme, verinin konumu üzerinden yargı yetkisini ön plana çıkarmıştı. Ancak bu durum artık değişmiştir.[168]

Günümüzdeki teknolojik gelişimler ve bulut bilişimin kullanılması durumu, elektronik kanıtları hemen hemen her suç için önemli hale getirmiş ve neredeyse tüm suçları etkili bir şekilde siber suça dönüştürmüştür. Gittikçe artarak, suçun soruşturulması ve kovuşturulmasıyla ilgili, belirli failleri tanımlamak için kullanılan abone bilgileri, e-posta içerikleri gibi, kritik öneme sahip pek çok elektronik kanıt, suçun meydana geldiği veya soruşturulmakta olduğu ülkeden farklı bir ülkede muhafaza edilmektedir.[169] Avrupa Komisyonu'nun 2018 tarihli bir raporunda, tüm soruşturmaların yarısından fazlasının elektronik kanıtlara erişim için sınır ötesi bir talep içerdiğini ifade edilmektedir.[170] Kanıtların küreselleşmesi, devletlerin bölgesel yargı yetkilerinin dışında tutulması ve aktarılması, kolluk kuvvetleri için önemli engeller yaratmaktadır.

Ceza yargılamasında rol alan kişi ve kurumlar da ceza yargılamasında elektronik kanıtlara giderek daha fazla güvenmekte ve ihtiyaç duymaktadır. Bu tür kanıtlar hassas kişisel veriler de dahil olmak üzere, çeşitli türdeki verilerden oluşmaktadır ve çoğunlukla çevrimiçi olarak üretildiğinden, çok kolay şekilde yerleri değiştirilebilir ve yok edilebilir niteliktedirler. Örneğin; bir şüphelinin suç işlendiği andaki yerini tespit etmeye veya şüpheliler arasında yapılan gizli anlaşmaları

---

[168] Daskal, Jennifer ve Kennedy-Mayo, Debrae, *Budapest Convention: What Is It And How Is It Being Updated?*, 02.07.2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/, çevrimiçi, Erişim Tarihi: 11.06.2022.

[169] A.g.e.

[170] Commission Staff Working Document, Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules of the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, European Commission, 6.1.1., s.84, (17.04.2018), çevrimiçi, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN, Erişim Tarihi: 11.06.2022.

kanıtlayan mesajların içeriğine erişmeye olanak tanıyan bilgileri içeren bu tür verilerin elde edilmesi, internet sitelerine veya telekomünikasyon araçlarına erişim imkânı sunan çevrimiçi hizmet sağlayıcılar gibi çeşitli aktörlerle yakın temaslı ve sorunsuz bir iş birliğini gerektirir. Bunun sonucu olarak, çeşitli aktörler, bu tür verilerin korunması ve açıklanması için hizmet sağlayıcılarla doğrudan iş birliği konusunda yeni standartlar geliştirmeye başlamıştır[171] ve Gelişmiş İş Birliği ve Elektronik Kanıtların İfşasına İlişkin İkinci Ek Protokol, bu akademik çalışmanın ilerleyen bölümlerinde kullanılacak adıyla "2. Ek Protokol", bu ihtiyacının küresel olarak çözümlenmesi çabasının bir sonucu olarak kaleme alınmıştır.

Elektronik kanıtların korunması ve ifşa edilme süreci; hizmet sağlayıcıların kamu yetkililerileriyle doğrudan iş birliğine ilişkin ulusal ve bölgesel normlar arasındaki farklılıkların ve uyumsuzlukların azaltılmasını, küresel standartların detaylandırılmasını ve kabulünü gerektirir. Siber suçlarla ilgili güvenli bölgelerin ortadan kaldırılmasını ve etkin iş birliğini kolaylaştırmayı amaçlayan ilk çok taraflı bağlayıcı nitelikteki uluslararası belge, Avrupa Konseyi Siber Suçlar Sözleşmesi'dir. Dijitalleşme ve elektronik kanıtlara duyulan ihtiyaç doğrultusunda, elektronik kanıtlara erişim konusunda uygulanacak olan ve uygulanması gereken usulleri netleştirmeyi ve ortak standartların oluşturulmasını amaçlayarak Sözleşmeye işbu 2. Ek Protokol getirilmiştir.

Protokol, yeni suçları tanımlamakla ilgili değildir. Bunun yerine daha etkili bir şekilde elektronik kanıt elde etmeye odaklanmaktadır.[172] Buna odaklanırken, soruşturma tedbirlerindeki yetkilerin kötüye kullanılmasını önlemek için artan

---

[171] Brière, Chloé. *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*. European Papers 2021 6(1), doi: 10.15166/2499-8249/479, s.493-494.

[172] Seger, Alexander. *A New Protocol To The Convention On Cybercrime: For A More Effective Criminal Justice Response To Crime Online-With Strong Safeguards*, 11.11.2021, çevrimiçi, https://www.linkedin.com/pulse/new-protocol-convention-cybercrime-more-effective-criminal-justice-/?trackingId=CnjE%2BxAERiKTr26OaLL2LA%3D%3D, Erişim Tarihi: 11.06.2022.

güvencelere yer verilmiştir. Etkinliği güvencelerle uzlaştırma ihtiyacı, uzmanların ve Tarafların, metni tamamlamak için çok uzun süre boyunca müzakere etmesine[173] ve Protokolün nihai taslağının hazırlanmasının uzun sürmesine sebep olmuştur.

Protokol, farklı ülkelerde bulunan hizmet sağlayıcılardan ceza yargılaması için gerekli olan elektronik kanıtların talep edilmesi konusunda düzenlenen ilk metin değildir. Büyük hizmet sağlayıcıların genel merkezlerinin bulunduğu ABD, 2018 yılında Cloud Act[174] (Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi Yasası) adı altında özel bir mevzuat çıkartarak, hizmet sağlayıcıların hizmetlerini ABD topraklarında sundukları sürece, verilerin yerelleştirilmesine bakılmaksızın, kamu makamlarının doğrudan doğruya hizmet sağlayıcılardan bu tür kanıtları talep etmelerine izin vermiştir.

Cloud Act, uyuşturucu kaçakçılığı ile ilgili bir davada Microsoft şirketinin şüpheli kişi hakkında, verilerin İrlanda'da saklanıyor olması ve ABD'nin yetki alanı dışında olması dolayısıyla ilgili verileri iletmeyi reddetmesi üzerine, bu ve bunun benzeri uyuşmazlıklara çözüm getirmek amacıyla kabul edilmiştir.[175] Bu mevzuat uyarınca, artık ABD yargı yetkisine tabi hizmet sağlayıcılar, iletişimin nerede gerçekleştiğine bakılmaksızın, kablolu veya elektronik iletişimin içeriğini korumaya ve ifşa etmeye zorlanmaktadır. Ancak örneğin, ABD'nin yargı yetkisine tabi bir hizmet sağlayıcının Cloud Act uyarınca verileri ifşa etmeye mecbur olduğu, ancak aynı zamanda verilerin depolandığı ülkenin ulusal mevzuat ayrıca verilerin ifşasını çifte suçluluğun varlığına bağlı olduğu haller veya verilerin ifşasını yasaklandığı haller olabilmektedir. Dolayısıyla yürürlükteki yasaların farklılık göstermesi, çelişkili

[173] A.g.e.
[174] Ayrıntılı bilgi için bkz. U.S. Congress Clarifying Lawful Overseas Use of Data – CLOUD Act., çevrimiçi, https://www.justice.gov/dag/cloudact, Erişim Tarihi: 08.03.2022.
[175] Kalender, Ata Umur. *Parçalı Bulutlar: Cloud Act ve Etkileri*, 2021, Kişisel Verileri Koruma Dergisi, s.75-76, çevrimiçi, https://dergipark.org.tr/tr/download/article-file/1121221, Erişim Tarihi:10.04.2022.

yükümlülüklere yol açarak verilerin korunmasını ve ifşa edilmesini engelleyebilmekte veya yavaşlatabilmektedir.[176]

Cloud Act yalnızca ABD ile cezai konularda iş birliğini kolaylaştırır, dolayısıyla elektronik veri alışverişi için çok taraflı bir standart oluşturma potansiyeline sahip değildir ve beklentilere tam anlamıyla yanıt verememektedir.[177] 66 üyesi olan[178] Avrupa Konseyi Siber Suçlar Sözleşmesi'ne bu türden bir amaçla getirilen 2. Ek Protokol daha geniş çaplı uluslararası bir metin olması dolayısıyla, küresel nitelikteki kanıtları elde etme amacına daha çok hizmet etmektedir. Uluslararası iş birliği mekanizmaları, adil yargılanma hakkı da dahil olmak üzere, benzer ilkeleri paylaşan demokratik devletler arasında bilgi alışverişini kolaylaştıracağı varsayımı üzerine inşa edilmiştir. [179] Bunun yanında Birleşmiş Milletlerin de siber suçlar ile mücadelede bir metin oluşturmak için görüşmeler içerisinde olduğu da bilinmektedir.[180]

Ülkelerin kanunlarının değişiklik göstermesi ve ortaya çıkan ihtilaflarının bir sonucu olarak hizmet sağlayıcılar, bir başka ülkenin kanunlarına uymak için diğer bir ülkenin kanunlarını ihlâl etme riski ile karşı karşıya kalmaktadır. Hizmet sağlayıcıların ceza yargılamasında rol alan kişi ve kurumlarla iş birliği yapmak zorunda kaldığı durumlarda tabii olacakları yasal kesinlik ve netlik eksikliği vardı, uluslararası iş birliğinin etkin ve hukuka uygun halde işleyebilmesi için önceki bölümlerde de

[176] Brière, s.497.
[177] Rojszczak, Marcin. *E-Evidence Cooperation in Criminal Matters from an EU Perspective*. 2022 The Modern Law Review, DOI: 10.1111/1468-2230.12749, s.1024.
https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12749, çevrimiçi, Erişim Tarihi: 29.09.2022. "Cloud Acct, üçüncü bir ülkenin yasal modelini değerlendirmek için asgari kriterleri ana hatlarıyla belirtse de, bu yönergelerin karşılanıp karşılanmadığını değerlendirmede yürütme organına büyük bir hareket alanı sağlar. ABD kolluk kuvvetlerinin ihtiyaçlarına cevap veren, ancak yabancı ortakların beklentilerini tam olarak dikkate almayan, çok ABD merkezli veri aktarımı görüşü barındırmaktadır." s.1027.
[178] Parties / Observers to the Budapest Convention and Observer Organisations to the T-CY, çevrimiçi, https://www.coe.int/en/web/cybercrime/parties-observers, Erişim Tarihi: 09.04.2022.
[179] Rojszczak, s.1024.
[180] Brière, s.507.

detaylandırıldığı üzere, ulusal mevzuatın ortak hükümleri içermesi, ortak bir mutabakat içinde hareket edilmesi gerekmektedir. Zira internetin çoğulcu, özgür ve kimin önceliğe sahip olduğunu tayininin mümkün olmayan yapısı, internet sağlama hizmetini sunan kurumlar için bireylerin temel hak ve özgürlüklerini doğrudan olumsuz etkileme riski yaratmaktadır.

Toplanan verilerin ifşası, ceza yargılamasında kanıt olarak kullanılarak bir kişinin mahremiyetine ve ifade özgürlüğü ihlallerine önemli bir müdahale teşkil etmesinin ötesinde, mahkemede bir kişiyi mahkûm edecek cezai yaptırımlar şeklinde dahi sonuçlanabilir. Çevrimiçi hizmet kullanıcılarının da bu kullanımları sonucu oluşturdukları verilerinin korunması ve ifşası için hangi yasalara tabii olduklarını bilmeleri, korumalara güvenmeleri ve bunlardan yararlanabilmeleri gerekmektedir.[181]

İlerleyen bölümlerde daha detaylandırılacağı üzere, Protokolde sıklıkla tekrarlanan ifade, Protokolde düzenlenen hususların iç hukuka uygun hale getirilmesi için Taraf ülkelerin gerekli özeni göstererek yasal düzenleme yapması gerektiğidir. Zira kişisel veriler ile ilgili olarak kapsamlı düzenlemeler getirilmiştir.

2.2. PROTOKOLÜN HAZIRLANMA SÜRECİ

2012 yılında Siber Suçlar Sözleşmesi Komitesi (T-CY); Sözleşmenin 46. maddesinin 1. fıkrası kapsamındaki yetkisine uygun şekilde "Sözleşmenin olası ilave veya değişikliklerini" göz önünde bulundurarak", "siber suçlara ilişkin önemli yasal, siyasal veya teknolojik gelişmeler ve elektronik ortamda kanıt toplanması konularında bilgi alışverişinde bulunmak" için Yargı Yetkisi ve Verilere Sınır Ötesi Erişime İlişkin Özel Amaçlı Alt Grubu'nu ("Sınır Ötesi Grup") kurmuştur. 2014 yılının Aralık ayında T-CY, ayrıca Sözleşmenin karşılıklı yardım hükümlerinin bir değerlendirmesini

[181] Brière, s.498.

tamamlayarak, bazıları Sözleşmenin yeni başka bir protokolünde ele alınacak olanlar da dahil olmak üzere, bir dizi tavsiyeyi kabul etti ve bu çabaların sonucu olarak 2015 yılında, Karşılıklı Adli Yardım da dahil olmak üzere Bulutta Depolanan Kanıtlara Ceza Adaleti Erişimi Çalışma Grubu ("Bulut Kanıt Grubu") oluşturulmuştur. [182]

2015 yılında Fransa'da gerçekleşen Bataclan terörist saldırısına ilişkin kapsamlı Fransız soruşturmaları sırasında, elektronik kanıt sisteminin etkin bir reformuna dair yapılan tartışma, Avrupalı yasa koyucuların dikkatini çekmiş, Avrupa kurumlarını karşılıklı adli yardım ve karşılıklı tanıma prosedürlerini basitleştirmenin bir yolunu aramaya yöneltmiştir. [183]

2016 yılında Bulut Kanıt Grubu, siber suç mağdurlarının büyük çoğunluğunun adaletin yerini bulmasını beklemediği ve adaletin temininin mümkün olmadığını düşündükleri bilgisine ulaşmıştır. [184] Bulut Kanıt Grubu tarafından belirlenen ana zorluklar, "bulut bilişim, bölgesellik ve yargı yetkisi" ile ilgili ve dolayısıyla elektronik kanıtlara etkin erişim ve bunların ifşa edilmesindeki zorluklarla ilgiliydi. Ülkeler arası ilişkiler ile bireylerin haklarını koruyabilmek, uluslararası çözümlerin yokluğunda, hükümetler giderek tek taraflı çözümler üretme amacı bulunmaktadır. [185] Bulut Kanıt Grubu, Sözleşmeyi değiştirmeye veya maddi ceza hukuku hükümlerine yeni suç eklemeye gerek olmadığını ifade etmiştir. [186]

---

[182] Protokole İlişkin Açıklayıcı Rapor, Art.9.
[183] Spiezia, Filippo. *International Cooperation And Protection Of Victims In Cyberspace: Welcoming Protocol II To The Budapest Convention On Cybercrime. ERA Forum* (2022) 23:101–108, s.5. 04.04.2022. https://link.springer.com/content/pdf/10.1007/s12027-022-00707-8.pdf, çevrimiçi, Erişim Tarihi: 11.06.2022.
[184] A.g.e., Art.10.
[185] T-CY Cloud Evidence Group, Buluttaki elektronik kanıtlara ceza adaleti erişimi, 17 Şubat 2016. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168053c8, çevrimiçi, Erişim Tarihi: 17.04.2022.
[186] Protokole İlişkin Açıklayıcı Rapor, Art.11.

T-CY'nin 17. Genel Kurulu, Bulut Kanıt Grubu tarafından hazırlanan bir teklife dayalı olarak, 2. Ek Protokolün hazırlanmasına ilişkin görev tanımlarını onaylamış ve Sözleşmenin 46. maddesi uyarınca kendi inisiyatifiyle, bu Protokolün taslağının hazırlanmasına başlamaya karar vermiştir.[187] Görev tanımına göre T-CY, Sözleşme Taraflarının ve T-CY'de gözlemci statüsüne sahip ülkelerin, örgütlerin ve Avrupa Konseyi organlarının gözlemci olarak temsilcilerinden oluşan bir Protokol Hazırlama Genel Kurulu oluşturmuştur. Bu Kurul'a taslak protokolün hazırlanmasında, Sözleşme taraflarının uzmanlarından oluşan bir Protokol Hazırlama Grubu tarafından yardımcı olunmuştur. Bu Grup, belirli hükümler üzerinde çalışmak için birkaç alt grup ve özel çalışma grubu kurmuş ve Taraflardan temsilcilerin ve uzmanların bu Protokolün taslağının hazırlanmasına kapsamlı bir şekilde katkıda bulunmalarına ve yenilikçi çözümler geliştirmelerine olanak sağlamıştır.[188]

T-CY, sivil toplum ve özel sektörden paydaşlarla ve veri koruma uzmanlarıyla Octopus Konferansı ile bağlantılı olarak altı tur istişare gerçekleştirmiştir. Ayrıca, Avrupa Konseyi Kişisel Verilerin Otomatik İşlenmesi Sözleşmesi'ne ilişkin olarak da danışılmıştır.[189] Veri koruma önlemlerinin optimal bir şekilde anlaşılması ve dikkate alınmasını sağlayarak özel hükümlerin hazırlanmasının sağlanması için Avrupa Veri Koruma Kurulu (EPDB) 2. Ek Protokolün oluşturulma sürecini yakından takip etmiş ve danışmanlıkta bulunmuştur. Avrupa Konseyi Siber Suçlar Sözleşmesi ve bu Sözleşmeye getirilen Ek Protokoller bağlayıcı uluslararası belgeler olduğundan Avrupa Birliği Adalet Divanı (CJEU) içtihatları uyarınca; uluslararası bir anlaşmanın getirdiği yükümlülüklerin temel hak ve özgürlükler ile Avrupa Topluluğu'nun anayasal ilkelerine halel getirme etkisine sahip olamayacağını ve bu ilkeler çerçevesinde

[187] 6. Cloud Evidence Group: Terms of Reference for the preparation of a draft Protocol to the Budapest Convention, 17th Plenary Meeting of the Cybercrime Convention Committee (T-CY), Council of Europe (June 2017),
https://rm.coe.int/-draft-terms-of-reference-for-the-preparation-of-a-draft-2nd-additiona/168071b794, çevrimiçi, Erişim Tarihi: 19.04.2022.
[188] Protokole İlişkin Açıklayıcı Rapor, Art.12-15.
[189] Protokole İlişkin Açıklayıcı Rapor, Art.19.

oluşturulması gerektiğini vurgulamaktadır. Bu nedenle 2. Ek Protokolde belirtilen hükümlerin veri koruma alanındaki AB müktesebatına uygun olmasının sağlamasının esas olduğunu ifade etmektedir.[190]

Siber suçlara karşı etkin mücadelede en temel güçlük olan Taraf ülkelerin yetkili makamların birbirleri ve servis sağlayıcılar ile etkili iş birliğinin sağlanmasındaki eksikliğe çözüm getirebilmek ve Taraf ülkelerin yetkili kurumlarının, diğer Taraf ülkedeki servis sağlayıcılar ile doğrudan iş birliğini sağlamak amacıyla Sözleşmeye 2. Ek Protokol getirilmiştir. Sivil toplumun insan hakları ve özgürlükler için endişesinin karşısında, temel haklar ve özgürlükler ile metin arasında makul bir denge olduğu düşünülmektedir ve bu yeni düzenleme ile asıl amacının siber suçların soruşturulması ve kovuşturulmasında daha sert önlemler alınarak asıl olarak mağdurların haklarının korunmasına ve mağdurlara yardım etmek olduğu belirtilmiştir.[191]

2019 yılının Temmuz ayı itibariyle, bu konuyla ilgili hükümler üzerinde geçici bir anlaşma olduğu için müzakereler olumlu bir şekilde ilerlemiştir. Komite, çok sayıda toplantının verilerin korumasına ve hukukun üstünlüğünün gerekliliklerinin sağlanması ve düzenlemelerin Taraf ülkelerin hukuk sistemleriyle uyumlu olması gerektiği konularına ayrıldığını vurgulamıştır.[192]

---

[190] Jelinek, Andrea. *Statement 02/2021 On New Draft Provisions Of The Second Additional Protocol To The Council Of Europe Convention On Cybercrime (Budapest Convention),* https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf, çevrimiçi, Erişim Tarihi: 09.04.2022.

[191] Parliamentary Assembly of the Council of Europe (PACE) tarafından Kamal Jafarov (Azerbaycan) ile yapılan 04.10.2021 tarihli röportaj https://www.youtube.com/watch?v=r9zbJTrH2mc, çevrimiçi, Erişim Tarihi: 08.04.2022.

[192] Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, State of play, 8 July 2019, T-CY (2019)19.

8 Kasım 2019 tarihinde geçici bir protokol metni üzerinde anlaşmaya varılmıştır. Geçici taslak metinde, tarafların yalnızca "savcı veya diğer adli makamlar tarafından veya onların gözetiminde veya bağımsız denetimleri altında verilen" emirleri kabul ederek beyanda bulunmalarına olanak tanınmakta ve ifşanın talepte bulunulan taraftaki cezai soruşturma veya kovuşturmaları tehlikeye düşürmesi halinde, hizmet sağlayıcıya bilgileri ifşa etmeme talimatı vermelerine izin vermekte idi.[193]

Covid-19 pandemisi kısıtlamaları sebebiyle, 2017 yılının Eylül ayı ile 2021 yılının Mayıs ayları arasında 2. Ek Protokolün düzenlenmesi için yapılan altmış beş toplantıdan fazlası sanal ortamda gerçekleştirilmiştir.[194] Protokolün oluşturulma sürecinde Covid-19 pandemisinin yaşanması ve bu sebeple çalışmaların ertelenmiş olması[195] ile insan haklarıyla ilgili endişeler sonucunda uzmanlarla çok sayıda istişarede bulunulması nihai taslağın tamamlanmasını geciktirmiştir. 2017 yılından bu yana, T-CY, 2. Ek Protokolün hazırlanması için müzakereler yürütmektedir. Dört yıl içinde doksandan fazla toplantı sonucunda nihai taslak metin oluşturulmuştur.[196] Nihayet 28 Mayıs 2021 tarihinde T-CY'nin 24. Genel Kurulu, işbu Protokolün taslağını onaylamış ve kabul edilmek üzere Bakanlar Komitesi'ne sunmaya karar vermiştir.[197]

Ortak bir ceza politikası sürdürmek, ceza usul hukuku ile ilgili ortak düzenlemeler getirerek etkin uluslararası iş birliği sağlama amacıyla yürürlükte olan

---

[193] Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, Provisional text of provisions, 8 November 2019, T-CY (2018) 23, 15.
[194] Protokole İlişkin Açıklayıcı Rapor, Art.15.
[195] Daskal, Jennifer ve Kennedy-Mayo, Debrae, *Budapest Convention: What Is It And How Is It Being Updated?*, 02.07.2020, https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/, çevrimiçi, Erişim Tarihi: 11.06.2022.
[196] 5 Conclusion, Summary of Comments on Opinions by Council of Europe Committees and Submissions by Other Stakeholders on the Draft 2nd Additional Protocol to the Convention on Cybercrime, Cybercrime Convention Committee (T-CY), Council of Europe (May 2021), https://rm.coe.int/0900001680a2aa1dVersion, çevrimiçi, Erişim Tarihi: 17.04.2022.
[197] Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Explanatory Report, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, çevrimiçi, Erişim Tarihi: 17.04.2022.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 20. yılını kutlandığı 2021 yılında, Sözleşmeye getirilen 2. Ek Protokolün imzaya açılacak olan metni 17 Kasım 2021 tarihinde onaylanmıştır, metnin 12 Mayıs 2022 tarihinde imzaya açılmıştır.[198] Bu çalışmanın yazıldığı tarih itibariyle 24 ülke Protokolü imzalamıştır.[199]

Protokolü İmzalamış Olan Ülkeler Listesi

Amerika Birleşik Devletleri	İzlanda
Andora	Japonya
Avusturya	Karadağ
Belçika	Kolombiya
Bulgaristan	Kosta Rika
Estonya	Kuzey Makedonya
Fas	Litvanya
Finlandiya	Lüksemburg
Hollanda	Portekiz
İspanya	Romanya
İsveç	Sırbistan
İtalya	Şili

Protokolün yürürlüğe girmesi, Protokolün 16. maddesi uyarınca, Sözleşmenin beş Tarafının, 16. maddenin 1 ve 2. fıkraları hükümleri uyarınca, bu Protokole bağlı kalmaya muvafakatlerini beyan ettikleri tarihten sonraki üç aylık sürenin sona ermesini

[198] Enhanced Cooperation and Disclosure of Electronic Evidence, COE INT., çevrimiçi, https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention#:~:text=Following%20almost%20four%20years%20of,the%20framework%20of%20an%20international, Erişim Tarihi: 25.05.2022.

[199] Chart of signatures and ratifications of Treaty 224, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Status as of 12/06/2022, çevrimiçi, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, Erişim Tarihi: 12.06.2022.

izleyen ayın ilk günü yürürlüğe girecektir. Protokol 24 ülke tarafından imzalanmıştır, ancak henüz onaylama (ratification) işlemini gerçekleştiren bir Taraf bulunmamaktadır.[200]

2.3. PROTOKOLÜN HEDEFLERİ VE İLKELERİ

Elektronik kanıtların elde edilmesi ile ilgili ülkesellik ve yargı yetkisine ilişkin zorluklar; bir ceza soruşturmasında ihtiyaç duyulan belirli verilerin bulutta, yani birden fazla, değişen veya bilinmeyen yargı alanında saklanabilmesinin özellikle endişe verici olması ve belirli cezai soruşturma veya kovuşturmaları için bu tür verilerin etkin ve verimli bir şekilde ifşasını sağlamak için çözümlere ihtiyaç duyulması, bu hususta bir yasal düzenleme yapılmasının motivasyonu olmuştur. Bu zorlukların göz önüne alındığında, 2. Ek Protokolün taslağının hazırlanmasında belirli konulara odaklanılması gerektiği kabul edilmiştir.[201]

Bu Protokolün taslağının hazırlanması sırasında karşılıklı yardım talepleri, Sözleşmenin karşılıklı yardım araçları da dahil olmak üzere, diğer ülkelerden bir suça ilişkin elektronik kanıt elde etmenin başlıca yöntemiydi. Halbuki, kolayca yok olabilen nitelikteki elektronik kanıtların, giderek artan sayıdaki taleplerini işleme koymak için ülkeler arası karşılıklı yardım her zaman etkili bir yol değildir. Bu nedenle, diğer Taraf ülkelerdeki hizmet sağlayıcılara, abone bilgileri ve trafik verileri üretmek için emir vermek veya talepte bulunmak için daha elverişli bir mekanizmanın geliştirilmesi gerekli görülmüştür.

---

[200] A.g.e.

[201] Bu başlık altındaki açıklamaların tamamı Protokolün Açıklayıcı Memorandumu'ndan alıntılanmıştır. Substantive Considerations başlığı, m.22-25, Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Explanatory Report, Art.22-25, çevrimiçi, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, Erişim Tarihi: 17.04.2022.

Belirli bir e-posta veya sosyal medya hesabının veya bir suçun işlenmesinde kullanılan belirli bir İnternet Protokolü (IP) adresinin kullanıcısını belirlemek için kullanılan Abone Bilgileri, siber suçlar ve elektronik kanıt içeren diğer suçlarla ilgili olan ulusal ve uluslararası cezai soruşturmalarda en çok aranan bilgidir. Bu bilgi olmadan, bir soruşturmaya devam etmek çoğu zaman imkânsızdır ve maalesef abone bilgilerinin karşılıklı yardım yoluyla elde edilmesi çoğu durumda etkili değildir ve karşılıklı yardım sistemlerine aşırı yük bindirir. Abone bilgileri normalde servis sağlayıcılar tarafından tutulur. Sözleşmenin 18. maddesinde; diğer Tarafların da hizmet sağlayıcılardan abone bilgilerinin alınmasını bazı yönlerini halihazırda ele alırken, abone bilgilerinin doğrudan başka bir Taraftaki bir hizmet sağlayıcı tarafından açıklanmasını sağlayabilmek için tamamlayıcı araçların gereklidir. Bu araçlar, belli ölçüde sürecin verimliliğini artıracak ve ayrıca karşılıklı yardım sistemi üzerindeki baskıyı da azaltacaktır.

Trafik verileri de cezai soruşturmalarda sıklıkla aranmaktadır ve daha fazla kanıt toplamak veya bir şüpheliyi belirlemek için bir başlangıç noktası olarak bir iletişimin kaynağını izlemek için bunların hızlı bir şekilde ifşa edilmesi gerekli olabilir. Benzer şekilde; çevrimiçi suçların çoğu, suç amaçlı oluşturulan veya istismar edilen alan adları tarafından kolaylaştırıldığından dolayı, bu türden bir alan adını kaydeden kişinin kimliğinin belirlenebilmesi gerekir. Bu tür bilgiler, alan adı kayıt hizmetleri sağlayan kuruluşlar, yani tipik olarak kayıt şirketleri ve kayıt kuruluşları tarafından tutulur. Bu nedenle, diğer Taraflardaki ilgili kuruluşlardan bu bilgileri elde etmek için etkin bir çerçeveye ihtiyaç vardır.

Gerçek bir kişinin hayatı veya güvenliği için önemli ve yakın bir riskin bulunduğu acil bir durumda ya acil karşılıklı yardım sağlayarak ya da Sözleşmenin 35. maddesi kapsamında kurulan 7/24 İletişim Ağı noktalarından yararlanarak hızlı bir şekilde harekete geçilmesi gereklidir. Protokolde acil durum ve bununla ilgili uygulamalar ayrıca tanımlanmıştır.

Ayrıca, kanıtlanmış uluslararası iş birliği araçları tüm Taraflar arasında daha yaygın olarak kullanılmalıdır. Video konferans veya ortak soruşturma ekipleri gibi önemli önlemler, Avrupa Konseyi anlaşmaları (Cezai İşlerde Karşılıklı Yardıma İlişkin Avrupa Sözleşmesinin İkinci Ek Protokolü, ETS No. 182 gibi) veya diğer ikili ve çok taraflı anlaşmalar kapsamında halihazırda mevcuttur. Ancak, bu tür mekanizmalar Sözleşme Tarafları arasında evrensel olarak mevcut değildir ve bu Protokol bu boşluğu doldurmayı amaçlamaktadır.

Sözleşme, belirli ceza soruşturmaları veya kovuşturmaları için bilgi ve kanıtların toplanmasını ile değişimini sağlamaktadır. Taslağı hazırlayanlar, ceza soruşturmaları ve kovuşturmalarıyla ilgili yetki ve prosedürlerin oluşturulması, uyarlanması ve uygulanmasında her zaman insan hakları ve temel özgürlüklerin yeterli şekilde korunmasını sağlayan koşullara ve güvencelere tabi olunması gerektiğini kabul etmişlerdir. Bu nedenle, Sözleşmenin 15. maddesine benzer şartlar ve tedbirler hakkında bir maddenin Protokole eklenmesi gerekliydi. Ayrıca, birçok Tarafın anayasal ve uluslararası yükümlülüklerini yerine getirmek için mahremiyeti ve kişisel verileri koruma gerekliliğini kabul ederek, taslağı hazırlayanlar bu Protokolde belirli veri koruma önlemleri sağlamaya karar vermişlerdir. Bu tür veri koruma önlemleri, aynı zamanda Kişisel Verilerin Otomatik İşlenmesine İlişkin Kişilerin Korunması Sözleşmesi'ne (ETS No.108) de Taraf olan Sözleşme Taraflarının birçoğunun yükümlülüklerini tamamlayacaktır. Ayrıca, bu Protokolün hazırlanma sürecinin, o sırada Avrupa Konseyi'nin veri koruma belgelerine veya Avrupa Birliği veri koruma kurallarına tabi olmayan Tarafları da kapsadığına dikkat edilmelidir. Buna göre, diğer Tarafların anayasalarının ve uluslararası yükümlülüklerinin gerektirdiği şekilde mahremiyetin ve kişisel verilerin korunmasının sağlanmasının önemine saygı duyulurken, bu Protokole Taraf olması muhtemel birçok ülkenin de hukuk sistemini yansıtacak dengeli bir metnin oluşturulması için önemli çabalar sarf edilmiştir.

Taslağı hazırlayanlar, kapsamlı bir tartışmadan sonra bu Protokolde yer almayan diğer önlemleri de değerlendirmiş ve Tarafları yüksek derecede ilgilendiren "bilgisayar sistemi aracılığıyla yürütülen gizli soruşturmalar" ile "aramaların genişletilmesi" konularının da düzenlenmesi gerektiğini ifade etmişlerdir. Ancak bu düzenlemelerin getirilebilmesi için daha çok zaman, ek çalışmalar ve paydaşlarla istişareler gerekmesinden dolayı ve bu Protokolün hazırlanması için belirlenen zaman çerçevesinde düzenlenebilmesi ve uygulanabilmesinin mümkün olmamasından dolayı, Taslağı hazırlayanlar, bu konuların farklı bir formatta ve muhtemelen ayrı bir yasal belgede takip edilmesini önermişler, bu Protokolün hükümlerinin genel olarak hem operasyonel hem de politik açıdan çok değer katacağına inanmışlardır. Bu Protokol, Tarafların kendi aralarında ve Taraflar ile hizmet sağlayıcılar ve diğer kuruluşlar arasındaki iş birliğini geliştirme ve belirli ceza soruşturması veya kovuşturması amacıyla elektronik kanıtların ifşa edilmesini sağlama imkanlarını önemli ölçüde geliştirecektir. Dolayısıyla Sözleşme gibi bu Protokol de insan haklarına ve temel özgürlüklere tam saygı gösterirken, kolluk kuvvetlerinin siber ve diğer suçlara karşı koyma imkânını artırmayı amaçlamakta ve ücretsiz olarak inşa edilen serbest bilgi akışı üzerine kurulan internetin önemini ve değerini vurgulamaktadır.

2.4. PROTOKOLÜN YAPISI VE İÇERİĞİ

Protokol metninin gerekçe kısmında, Sözleşme imzalandıktan bu yana geçen sürede karşılaşılan zorluklarının, duyulan ihtiyaçların ve Sözleşmedeki eksikliklerin neler olduğu ifade edilerek, bunların farkında olunduğu ve bu doğrultuda düzenleme yapıldığı ifade edilmektedir. Protokolün ana ilkeler çerçevesinde düzenlenmesinde göz önünde bulundurulan hususlar genel hatlarıyla; gizliliğin ve kişisel verilerin korunmasının önemi, elektronik kanıtların korunması için önlemler alınması gerektiği, hizmet sağlayıcılar ve diğer kuruluşların veri ifşası hakkında Sözleşmede yer alan düzenlemede eksik olan kısımlar için netleştirmeye ihtiyaç duyulduğu ve insan hakları ve temel özgürlüklerin korunacağının bilincinde olunduğudur.

Bu amaçlar çerçevesinde oluşturulan Protokol, dört bölümden ve 25 maddeden oluşmaktadır, ana hatlarıyla uluslararası iş birliğini geliştirmek için alınacak önlemlere, kişisel verilerin korunmasına ve Protokolün uygulanmasına ilişkin düzenlemelere yer verilmektedir. Protokol dört bölüme ayrılmıştır; I. Ortak Hükümler, II. Gelişmiş İş Birliği İçin Önlemler, III. Şartlar ve Teminatlar ile IV. Son Hükümler.

İlk bölüm, ortak hükümler başlığı altında Protokolün amacı, uygulama kapsamı, tanımlar ve dili düzenlemektedir. Sözleşme ve 1. Ek Protokol ile aynı amacı destekleyen 2. Ek Protokolün uygulama kapsamının, aksi belirtilmedikçe, bilgisayar sistemleri ve verileriyle ilgili ceza soruşturmalarında ve kovuşturmalarında "elektronik olarak kanıtların toplanmasına" ilişkin olarak uygulanacağı belirtilmektedir. Diğer bir ifadeyle; Protokol yalnızca siber suçlarla ilgili süreçlerde değil, aynı zamanda elektronik ya da dijital formdaki kanıtların gerekli olduğu herhangi bir suç tipi için de başvurulabilecek bir metindir.[202] Tanımlar maddesinde, Sözleşmeye atıf yapılarak buradaki tanımların Protokolde de geçerli olduğunu ve ayrıca Protokol metninde kullanılan "merkezi ve yetkili makam, acil durum, kişisel veriler ve aktaran taraf" kavramlarının neleri ifade ettiği açıklanmış ve son olarak Sözleşmenin iş birliğindeki etkisini ve verimliliğini azalttığı şeklide eleştirilen bir unsur olan dil konusunda pragmatik bir düzenleme[203] getirilerek tarafların, hizmet sağlayıcıların ve kuruluşların talep ve bilgilerin sunulmasında kullanılacak olan dil ve dillerin ne olacağı belirtilmektedir.

İkinci bölümde; taraflar için iş birliği yöntemlerini açıklayan bu Protokolün birincil asli maddeleri yer almaktadır. Her iş birliği türü için farklı ilkelerin geçerli olmasından dolayı, gelişmiş iş birliği için alınacak önlemler beş ayrı kısım altında

[202] Plachta, Michael. *Council of Europe Has Adopted the Second Protocol to the Cybercrime ('Budapest') Convention*. 2021, International Enforcement Law Reporter 37 (12): s.494.
[203] Protokole İlişkin Açıklayıcı Rapor, Art.28.

düzenlenmiştir.[204] İlk kısımda bu bölümde uygulanacak olan genel ilkeler, ikinci kısımda alan adı kayıt bilgileri talebi ile abone bilgilerinin ifşasının düzenlendiği diğer Taraf ülkelerdeki sağlayıcılar ve kuruluşlarla doğrudan iş birliğini geliştiren usuller, üçüncü kısımda abone bilgilerinin ve trafik verilerinin hızlandırılmış üretimi için başka bir taraftan gelen emirleri yürürlüğe koymak ve saklanan bilgisayar verilerinin acil bir durumda hızlandırılmış ifşasının detaylandırıldığı depolanan bilgisayar verilerinin ifşası için yetkililer arasında uluslararası iş birliğini artıran usuller, dördüncü kısımda acil karşılıklı yardıma ilişkin usuller ve son olarak beşinci kısımda uygulanabilir uluslararası anlaşmaların yokluğunda uluslararası iş birliğine ilişkin usuller olan video konferans ile müşterek soruşturma ekipleri ve müşterek soruşturmalar düzenlenmiştir.

Üçüncü bölümde uygulamada temel hak ve özgürlüklerinin korunmasının sağlanması için belirtilen şartlar ve teminatlar ile kişisel verilerin korunması için ne şekilde bir yol izlenmesi gerektiği konuları ayrıntılı olarak düzenlenmiştir. Zira, Sözleşmenin en çok eleştiri getirilen özelliklerinden biri temel hak ve özgürlükler ile kişisel verilerin korunmasına ilişkin yeterli özenin gösterilmemiş olduğu idi. Protokol bu hususta ayrıntılı düzenlemeler getirmiştir, hükümlerin içeriği ilerleyen bölümlerde detaylandırılacaktır. Düzenlemeler, tarafların Sözleşmenin 15. maddesine benzer koşulları ve güvenceleri, bu Protokolün yetki ve prosedürlerine de uygulamalarını gerektirmektedir.

Son olarak dördüncü bölümde son hükümler başlığı altında; Protokolün etkileri, imza ve yürürlüğe giriş, federal hüküm, ülkesel uygulama, çekinceler ile bunların durumu ve geri alınması ile beyanlar, değişiklikler, uyuşmazlıkların çözümü, tarafların müzakereleri ve uygulamanın değerlendirilmesi, fesih ve bildirim konuları düzenlenmektedir. "İşbu Protokolün etkileri" ile ilgili 15. madde, "Federal hüküm" ile ilgili 17. madde ve "Tarafların istişareleri ve uygulamanın değerlendirilmesi" ile ilgili

[204] A.g.e.. Art.29.

23. madde, Sözleşmenin benzer hükümlerinden değişen derecelerde farklılık göstermektedir. 23. madde yalnızca Sözleşmenin 46. maddesini uygulanabilir kılmakla kalmaz, aynı zamanda bu Protokol hükümlerinin etkin kullanımı ve uygulanmasının Taraflarca periyodik olarak değerlendirilmesini de sağlar.[205]

2.5. PROTOKOL MADDELERİNİN İNCELEMESİ VE DEĞERLENDİRMELER

Bu başlık altında Protokolün maddeleri incelenecek, tespit olunan olumlu ve olumsuz yönleri değerlendirilecek ve gerektiğinde Sözleşmede yer alan ilgili maddelere atıf yapılarak, konu detaylandırılacaktır.

2.5.1. Ortak Hükümler

Ortak hükümler adlı birinci bölüm; Protokolün amacını, uygulama kapsamını, tanımların neleri ifade ettiğini ve kullanılacak dil ile ilgili başlıkları düzenlemektedir. 2. Ek Protokolün amacının; bu Protokolün Tarafları arasındaki Sözleşme ile yine bu Protokolün ve 1. Ek Protokolün Tarafları arasındaki amacı desteklemek olduğu 1. maddede ifade edilmektedir.

Protokolün uygulama kapsamı Sözleşmenin 14. maddesinin 2. fıkrasında yer alan ifadeler ile aynıdır; "bilgisayar sistemleri ve verileriyle ilgili cezai suçlara ilişkin belirli cezai soruşturma veya kovuşturmalara ve bir cezai suçun elektronik biçimde kanıt toplanmasına ilişkin olarak" uygulanacaktır. Diğer bir ifadeyle, aynı Sözleşmede olduğu gibi bu Protokol de bir suçun bilgisayar sistemi aracılığı ile işlenip işlenmesini şart koşmadan, herhangi nitelikteki bir ceza soruşturmasının veya kovuşturmasının elektronik yollarla kanıt toplanmasını gerektirmesi durumunda da uygulanacaktır.

[205] A.g.e., Art.31.

Ayrıca hem bu Protokole hem de Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesine ilişkin Ek Protokole Taraf olan ülkelerin, bu metinde düzenlenen suçların soruşturma ve kovuşturmalarında da uygulanacaktır.

2. Ek Protokolün 2. maddesinin 2. fıkrası, Tarafların mevzuatında Protokolde belirtilen yükümlülüklerin yerine getirilmesi için henüz gerekli hükümler yer almıyorsa, gerekli olan yasal ve ilgili diğer düzenlemeleri ve uygulamaları yapması gerektiğini ifade etmektedir. Bu düzenleme, uygulanması açık isteğe bağlı olan ve beyan veya çekince konulması mümkün kılan maddeler bakımından bir değişiklik teşkil etmemektedir.[206]

Bu Protokol ile Sözleşmenin 1. ve 18. maddelerinde yer alan; bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı, trafik verisi ve abone bilgisi tanımlamalarına ek olarak, merkezi makam, yetkili makam, acil durum, kişisel veriler ve aktaran Taraf tanımlamalarını getirmiştir. Protokol ile getirilen yeni tanımlamalar, Sözleşme için de aydınlatıcı niteliktedir, zira bu tanımlardan bir kısmı Sözleşmede de yer almaktadır. 3. madde ile getirilen diğer tanımların açıklamaları, işbu akademik çalışmada tanımların yer aldıkları ilgili maddeler incelenirken detaylı olarak ifade olunacaktır.

- Merkezi makam; ilgili Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuata dayalı olarak bir karşılıklı yardım anlaşması veya düzenlemesi kapsamında tayin edilen makam veya makamlar veya bunların yokluğunda, Sözleşmenin 27. maddesi 2. fıkrasının a bendi uyarınca[207] bir Tarafça tayin edilen makam veya makamlar anlamına gelir.

[206] A.g.e. Art.35.
[207] Sözleşmenin 27. maddesi 2. fıkrasının a bendinde yer alan ifade "karşılıklı yardım talebinde bulunmak, bu taleplere cevap vermek, bu taleplerin gereğini yerine getirmek veya bunların gereğini yerine getirecek makamlara bu talepleri iletmekle görevli makam"

- Yetkili makam; belirli cezai soruşturmalara veya kovuşturmalara kanıtların toplanması veya sunulması amacıyla işbu Protokol kapsamındaki tedbirleri emretmek, yetkilendirmek veya üstlenmek için iç hukuk tarafından yetkilendirilmiş bir adli, idari veya diğer kanun uygulayıcı makam anlamına gelir.[208]

- Acil durum; gerçek bir kişinin hayatı ya da güvenliği için önemli ve yakın bir riskin bulunduğu durumdur. Bu tanım Protokolün 9, 10 ve 12. maddelerinde ve Sözleşmenin 25. maddesinin 3. fıkrasında geçmektedir. Düzenlemeye göre, acil durum çok önemi olmayan, uzak gelecekteki ya da geçmişteki bir vaziyetteki durumu değil, gerçek kişinin hayatı veya güvenliği için önemli ve yakında gerçekleşmesi muhtemel bir riskin bulunduğu durumu ifade etmektedir. Örnek olarak; bir kişinin birkaç saat içinde silahla bir okula ya da dini bir birime giderek orada bulunan kişileri öldüreceğine dair bir internet paylaşımı yapması gibi, terör, ölüm, ciddi yaralanma riski, bir çocuğun devam eden cinsel istismarı gibi saldırılar verilebilir.

- Kişisel veri; kimliği belirli veya belirlenebilir gerçek bir kişiye ait bilgiler anlamına gelmektedir. Diğer bir ifade ile, Bu Protokol kapsamındaki "kişisel veri" tanımı, Ek Protokolü ile değiştirilen Kişisel Verilerin Otomatik İşlenmesinde Bireylerin Korunmasına İlişkin Sözleşme, 2013 Tarihli Mahremiyetin Korunmasına ve Kişisel Verilerin Sınır Ötesi Akışlarına Yönelik OECD Yönergeleri, AB Genel Veri Koruma Yönetmeliği ve Veri Koruma Kanun Uygulama Yönergesi ve Siber Güvenlik ve Kişisel Verilerin Korunmasına İlişkin Afrika Birliği Sözleşmesi ("Malabo Sözleşmesi") gibi

[208] 6706 Sayili Cezaî Konularda Uluslararasi Adlî İş Birliği Kanunu'nun 2. maddesi uyarınca Türkiye Cumhuriyeti'nin uluslararası iş birliğini gerektiren hususlarda yetkili makam T.C. Adalet Bakanlığı'dır.

diğer uluslararası belgelerdeki tanımla tutarlılık içerisindedir.[209] Türkiye Cumhuriyeti'nin 6698 Sayılı Kişisel Verilerin Korunması Kanununda da kişisel veriler tanımı bu tanım ile aynıdır.

Madde 4, Taraflara, hizmet sağlayıcılara veya diğer kuruluşlara hitap ederken kullanılabilecek diller için bir çerçeve sağlamaktadır. Böylesi bir düzenleme hizmet sağlayıcılara veya kuruluşlara ek bir yük getirmeden, etkin ve hızlı iş birliğinin sağlanması için önemli ve gerekli idi. Zira, elektronik kanıtlarla ilgili karşılıklı yardım taleplerinde karşılaşılan hatalı ve yüksek maliyete sebep olan tercümeler ceza soruşturması ve kovuşturmasında önemli nitelikte veri hatalarına sebep olarak, kamu güvenliğinin sağlanmasını sekteye uğratacak sonuçlara sebebiyet verebilir. Özellikle daha az yaygın diller ile ilgili yapılan çevirilerde bu sorunla karşılaşılabilir ve süreci geciktirip imkansızlığa dahi sebep olabilir. Maliyet bakımında ise daha az yaygın dillerin konuşulduğu ülkelerden bilgi talebinde bulunan Taraflara orantısız bir yük yükler. Bu orantısız yük nedeniyle, İngilizce konuşmayan bazı Taraflar, İngilizce dilinin büyük hizmet sağlayıcılar tarafından yaygın olarak kullanılan bir dil olduğunu belirterek, bu Protokolde İngilizce dilinin zorunlu kılınmasını istemiştir. Ancak Taslağı hazırlayanlar, yardımı hızlandırmak için, özellikle bu Protokol kapsamındaki acil durum taleplerinin, talepte bulunulan Tarafın resmi diline tercüme edilmesi yerine İngilizce veya ortak bir dilde kabul edilmesi için çaba gösterilmesi gerektiğini ve İngilizce dilinin zorunlu kılınmaması gerektiği özellikle vurgulamışlardır.[210] Nitekim bazı ülkeler İngilizce dışında başka dilleri ortak olarak konuşmaktadır. Örneğin, İspanyolca dilini konuşan İspanya ve Kolombiya'nın iletişimlerini İngilizce dilinde sağlaması işlevsel olmayacaktır. Bu sebeple madde metninde "kabul edilebilir bir dil" ifadesine yer verildiğini düşünmekteyiz. Bu hüküm, veri ifşası için emir veya talep aldıklarında, hizmet sağlayıcılara veya kuruluşlara ek bir yük getirmeden hızlı iş birliğini ve artan kesinliği sağlamak için tasarlanmıştır.

[209] A.g.e., Art.44.
[210] A.g.e. Art.49-52.

2.5.2. Gelişmiş İş Birliği İçin Önlemler

Gelişmiş iş birliği için önlemler başlıklı Protokolün II. Bölümü öncelikle bu bölüme uygulanan genel ilkeleri, ardından iş birliği türlerine göre başlıkları ayırarak; diğer Taraflardaki sağlayıcılar ve kuruluşlarla doğrudan iş birliğini geliştiren usulleri, depolanan bilgisayar verilerinin ifşası için yetkililer arasında uluslararası iş birliğini artıran usulleri, acil karşılıklı yardıma ilişkin usuller ile uygulanabilir uluslararası anlaşmaların yokluğunda uluslararası iş birliğine ilişkin usulleri düzenlemektedir. Bu kısımlar ayrıca, genellikle bir ceza soruşturmasının ilk aşamalarında talep edilecek türdeki yardımlar olan; alan adı kayıt bilgisi ve abone bilgilerinin ifşası talepleri, trafik verileri, içerik verileri talepleri konuları ile genellikle bir soruşturmanın sonraki aşamalarında talep edilecek türdeki bir yardım biçimi olan video konferansı ve ortak soruşturma ekipleri ile müşterek soruşturmalar yürütülmesi hususlarını düzenlemektedir.[211]

2.5.2.1. Gelişmiş İş Birliği İçin Önlemler Bölümüne Uygulanacak Olan Genel İlkeler (Madde 5)

Gelişmiş iş birliği için önlemler bölümüne uygulanacak olan genel ilkeler başlıklı ve aynı ismi taşıyan tek maddelik kısımda, aynı Sözleşmenin 23. ve 25. maddelerinde de vurgulandığı gibi, Tarafların mümkün olan en geniş ölçüde iş birliği yapmaları gerekli olduğu ifade edilmektedir.

Bu maddenin düzenlendiği ikinci bölümde yer alan 6. ve 10 maddelerde öngörülen gelişmiş iş birliği için düzenlenen yöntemlere başvurulurken, ilgili Taraflar

[211] Bu kategorilendirme ile ilgili farklı görüşler de vardır. Bkz. "Protokol, üç ana gruba ayrılmış toplam yedi iş birliği mekanizması sunmaktadır. İlki, yetkili makamların bilgi taleplerini doğrudan başka bir ülkede yerleşik hizmet sağlayıcılara iletebilmesini sağlayacak önlemleri içerir. İkinci grup, Protokole Taraf olan ülkelerin yetkililerine dijital kanıt sağlamak için mekanizmalar içerir. Üçüncü grup, devam eden ceza yargılamaları alanında iş birliğini güçlendirmeyi, ortak soruşturma ekipleri oluşturmayı ve soruşturma çalışmalarında telekonferansı kullanmayı amaçlayan önlemleri kapsar." Rojszczak, s.1015.

arasında tek tip veya karşılıklı mevzuat temelinde bir karşılıklı yardım anlaşması veya düzenlemesinin varlığından etkilenmediğini, her halükârda uygulanacağını açıkça ortaya koymaktadır. 11. ve 12. maddelerin yer aldığı, uygulanabilir uluslararası anlaşmaların yokluğunda uluslararası iş birliğine ilişkin usuller başlıklı kısım, aksi belirtilmedikçe yani 12. maddenin 7. fıkrasının uygulanması dışında, yalnızca böylesi anlaşmalar veya düzenlemelerin olmadığı durumlarda ve ayrıca ilgili Taraflarca yasaklanmadıkça uygulanacaktır.

Bu maddenin 6. fıkrasındaki düzenleme, iş birliği talebinde bulunulan Tarafın iş birliğinde bulunmayı çifte suçluluğun mevcudiyeti koşuluna bağlamasına izin verilmektedir. Ulusal hukuk sistemleri suçları adlandırmada farklılıklar sergileyebilmektedir. İş birliğini talep eden ülkedeki yasalarının talep konusu suçu aynı suç kategorisine yerleştirip yerleştirmediğine veya suçun temelindeki davranış kendi kanunlarına göre ceza gerektiren bir suç ise, iş birliğini talep eden tarafla aynı terminolojiyle adlandırmasına bakılmaksızın, bu koşul yerine getirilmiş sayılacaktır. Bu düzenleme, Sözleşmenin 25. maddesinin 5. fıkrası ile paraleldir ve etkin iş birliğini bu düzenlemeler vasıtasıyla ve teknik aksaklıklara mahal vermeden sağlamak önemlidir.

Maddenin 7. fıkrası, bu bölümdeki hükümlerin uygulanmasının kısıtlanamayacağını, diğer bir ifadeyle iş birliğine ilişkin hükümlerin ortadan kaldırılamayacağı ve kısıtlanamayacağını ifade etmektedir. Son olarak, bu ve Protokolün başka bölümlerinde yer alan bazı hükümler, gizlilik gibi kullanım sınırlamaları veya koşullarının getirilmesine izin vermektedir. Konu ilerleyen başlıklarda detaylandırılacaktır.

2.5.2.2. Diğer Taraflardaki Sağlayıcılar ve Kuruluşlarla Doğrudan İş Birliğini Geliştiren Usuller (Madde 6 ve 7)

Bu başlık altın yer alan Protokolün 6. ve 7. maddeleri; bir Tarafın makamlarının ceza soruşturması veya kovuşturması sürecinde, diğer bir Tarafın topraklarındaki sağlayıcılar ve kuruluşların haiz olduğu alan adı ve abone kayıt verileri hakkında bilgi almak, elektronik kanıtlara sınır ötesi erişim sağlamak için doğrudan doğruya iş birliğini sağlayan prosedür belirlemektedir. Nitekim siber suçların yapısı dolayısıyla, söz konusu suçun işlendiği yer ve suçu işleyen bir fail aynı ülkede olsa dahi elektronik kanıtlar başka bir ülkende bulunan sağlayıcılar ve kuruluşlar bünyesinde olabilir.

Bu kısımdaki hükümler, taraflar arasından yürürlükte olan karşılıklı yardım anlaşması veya düzenlemesi bulunup bulunmadığına bakılmaksızın uygulanır.[212] Madde 6 ve 7'deki düzenlemeler doğrultusunda, talepte bulunan Taraf ülkenin yetkili mercilerinin, diğer Taraf ülkede bulunan servis sağlayıcılardan alan adı kayıt bilgileri ve abone bilgilerini doğrudan talep etme imkânı vardır.[213]

Bu başlık altındaki düzenlemeler doğrultusunda ilgili bilgileri talep etmek ve talep karşılığında bilgilerin ifşa edilmesi için Taraf ülkelerin yetkili makamlarını ulusal mevzuatıyla yetkilendirmelere gerekmektedir. Talep ve ifşa konusu bilgiler kişisel verilerin paylaşılmasını ve işlenmesini gerektirdiği için Protokolde atıf yapılan uluslararası sözleşmeler ve standartları sağlamak adına gerekli önlemleri alınmasını gerektirmektedir.

Ayrıca bu taleplerin, Tarafların topraklarında fiziksel olarak bulunan hizmet sağlayıcılar veya kuruluşlarda bulunması gerekmektedir, diğer bir ifadeyle talepte

[212] Bkz. Protokolün 5.maddesinde yer alan ve bu bölümde yer alan maddelere (m.5-12) uygulanacak olan ilkeler.
[213] Plachta, s.495.

bulunulan Taraf ülkedeki bir şirket ile sözleşmesel bir bağının bulunması ancak bu ülkede fiziksel olarak bulunmuyor oluşu bu maddenin uygulanmasını engeller.[214] Zira, 6. maddenin ve 7. maddenin 1. fıkraları "başka bir Tarafın ülkesindeki" tanımını içermektedir, verilerin hizmet sağlayıcının mülkiyetinde veya kontrolünde olmasını gerektirir. Yükümlünün bulunduğu yerin, verilerin fiziki olarak saklandığı yer olması gerekmediği de unutulmamalıdır. Modern bulut tabanlı hizmetler, aynı bilgileri birden çok veri merkezinde paralel ve eşzamanlı olarak işlemekte, veri depolama konumlarının çoğalmaktadır. Sonuç olarak, Google, Facebook ve Twitter gibi kuruluşlar söz konusu olduğunda, kolluk kuvvetlerinin ilgilendiği, kullanıcıların kimliği veya değiştirilen mesajların içeriği gibi veriler eş zamanlı olarak çeşitli veri merkezlerinde işlenir ve dünya çapında eşit bir şekilde yayılır.[215]

2.5.2.2.1. Alan Adı Kayıt Bilgileri (Madde 6)

Alan adları ile ilgili olarak düzenleme getiren bu maddeyi incelemeden önce alan adının ne ifade ettiğine genel hatlarıyla değinmek gerekmektedir. İnternete bağlanıldığı anda, bağlantı sağladığımız cihaz, internet ağında kendisine özgü günümüzde dört ya da altı haneli (111.22.33.444 gibi) çeşitli rakamlardan oluşan bir numara almaktadır. Bu numaraya Internet Protokol (IP) numarası denilmektedir.

İnternet ağındaki bir web sitesine ulaşmak için bu şekilde uzun numaraları hatırlamak ve kullanmak zor olduğundan, uygulamada bu numaralara tekabül eden ve aynısından bir tane daha olmayan alan adı olarak ifade edilen kelimeler kullanılır. Örneğin Google'ın IP adresi 8.8.8.8'dir, ancak internet arama motorunda Google alan adı yazılarak www.google.com şeklinde kullanılmaktadır.[216] Alan adları ülkeleri de

[214] Protokole İlişkin Açıklayıcı Rapor, Art.99.
[215] Rojszczak, s.1002.
[216] Dal, Seniha. *Türk Hukukunda İnternet Alan Adları (Domain Names) ve Bu Alandaki Son Gelişmeler,* Marmara Üniversitesi İİBF Dergisi, Cilt XXVIII, Sayı I, 2010, s.480, çevrimiçi, https://dergipark.org.tr/tr/download/article-file/3558, Erişim Tarihi: 27.03.2022.

belirtebilmektedir. Ülke kodu birinci derece alan adları, bir ülkeyi veya bir coğrafi bölgeyi iki harflik kısaltmalar ile gösteren ve ISO 3166 Standardında tanımlanan adları ifade etmektedir.[217] Örneğin, Türkiye Cumhuriyeti'nin ülke kodu ".tr", Fas Krallığı'nın ".ma" ve Amerika Birleşik Devletleri'nin ".us"dir. Ülkemizde alan adından sorumlu olan ODTÜ iken, bu yetki 5809 Sayılı Elektronik Haberleşme Kanunu'nu ile önce Ulaştırma Bakanlığı'na ve son olarak 2009 senesinden itibaren bu Bakanlığa bağlı olan BTK'ya geçmiştir.

Protokolün 6. maddesi Taraf ülkelerin alan adı kayıt bilgilerinin talebi ile ilgili koşulları, kuralları ve talebin karşılanmaması durumunda ne şekilde bir yol izlenebileceği ile ilgili bir düzenleme getirmektedir. Bu maddeye göre; alan adı sahibinin kimlik ve iletişim bilgilerini edinme talepleri yalnızca Taraf ülkelerin kendilerinin belirlemiş olduğu yetkili makamları aracılığıyla, belirli koşullar altında ve belirli sınırlar dahilinde, sağlayıcılara ve kuruluşlara yöneltilebilecektir. Diğer bir ifadeyle Taraf ülkelerin, alan adı sahibinin kimlik ve iletişim bilgilerini talep edebilecek olan makamlarını belirlemeleri ve bu taleplerini bu makamları aracılığıyla yöneltmeleri gerekmektedir. Bu bilgi talepleri keyfi ve esnek bir şekilde yapılamayacak, yalnızca belirli ceza soruşturması veya kovuşturma sürecinde ortaya çıkan ihtiyaç sebebiyle yapılabilecek ve işbu talep konusu bilgilerin detayları belirtilerek yalnızca söz konusu soruşturma veya kovuşturma için kullanılacağına dair beyan sunularak, gerektiğinde güvenlik ve kimlik doğrulaması ile bu taleplerini elektronik olarak sunulabilecektir.

Maddenin 2. fıkrası uyarınca; Taraf ülkelerin yetkili makamlarından gelen bilgi talepleri karşısında talepte bulunulan Taraf ülkelerin kurumlarının, alan adı sahibinin kimlik ve iletişim bilgilerini ifşa etme yetkisi olduğu hususu, ulusal mevzuatta makul

[217] Genel Bilgi, Bilgi Teknolojileri ve İletişim Kurumu, çevrimiçi, https://www.btk.gov.tr/internet-alan-adlari-genel, Erişim Tarihi: 26.03.2022.

sınırlar içerisinde düzenlenmelidir. Söz konusu verilerin ifşasının hukuka uygun olarak gerçekleştirilmesi için Taraf ülkelerin bu hususta yasal zemin oluşturması gerektiği ifade edilmektedir. Böylece, bu madde doğrultusunda edinilen kanıtların hukuka uygunluğu sağlanmış olacaktır.

Alan adı kayıt bilgileri pek çok ceza soruşturmasının ilk adımı olarak ve uluslararası iş birliğinde hangi ülkeden talepte bulunulacağını belirleyebilmek bakımından oldukça önemlidir. Nitekim çocuk istismarı gibi pek çok suç, alan adlarının kötü şekilde kullanılması aracılığıyla işlenmektedir. Bu nedenle alan adını ilgili kurumlara kaydettiren kişiye ilişkin olarak, kurumlar nezdinde bulunan bilgilere erişim suça ilişkin soruşturma ve kovuşturmalarda şüphelinin kimliğini belirleyerek, suç isnadının kime yönlendirileceğini tespit bakımından çok önemlidir.[218] Kişinin kimlik ve iletişim bilgilerinin bu madde kapsamında edinilmesiyle birlikte, şüpheli bilgileri ceza dosyasında eksiksiz bir şekilde yer alır ve iletişim bilgileri temini ile kendisiyle iletişime geçerek ilgili tebligatlar ve diğer ilgili işlemler sağlıklı şekilde yürütülebilir. Kamu düzeni adına yürütülen ceza yargılamasının nihayete erebilmesinin ilk aşaması, suç konusu alan adına ve bunu kaydettirene ilişkin bilgilere erişimdir. Alan adı tescil bilgileri, kişilerin özel hayatları ve günlük alışkanlıkları hakkında kesin sonuçlara varılmasına izin vermeyecek türde temel bilgilerdir. Bu nedenle, açıklanması, diğer veri kategorilerinin açıklanmasına kıyasla daha az müdahaleci olabilir.

Her ne kadar bu maddenin 1. fıkrasında her bir Taraf ülkenin, diğer Taraf ülkede bulunan alan adı kayıt bilgisini doğrudan talep edebilmek için ilgili makamlarını yetkilendireceği ve gerekli olabilecek tüm önlemleri alacağı ve talepte bulunulan Tarafın, talep konusu bilgileri ifşa edebilmek için metni yorumlamamız doğrultusunda, veri koruması için makul önlemlerin alınması gerektiği ifade edilse de, bu talep bağlayıcı nitelikte değildir, uluslararası iş birliğinin gönüllü yapısını

[218] Protokole İlişkin Açıklayıcı Rapor, Art.74.

değiştirmemektedir. Ancak maddenin 5., 6. ve 7. fıkraları ile getirilen ve dikkat çeken düzenleme iş birliği taleplerinin reddedilmesi durumunda sunulan alternatiflerdir.

Talepte bulunulan Taraf ülkenin kurumlarının alan adı ile ilgili bilgilerin ifşası için iş birliği yapmaması durumunda, talepte bulunan Taraf iş birliği yapılmamasının nedeninin kendisine sunulmasını ve talepte bulunulan ülke ile bilgileri edinmek için gerekli olan hukuki önlemleri belirlemek amacıyla karşılıklı olarak istişarede bulunmayı talep edebilir. Taraf ülkelerin iş birliğini reddetmesi durumunda istişare edilecek olan kurumlarının Avrupa Konseyi Genel Sekreteri'ne bildirileceği, ayrıntılı olarak güncel ve doğru şekilde kayıtlarının tutulacağı hüküm altına alınmıştır. Sözleşmenin en çok eleştirilen noktalarından biri etkin iş birliğinin sağlanabilmesi için herhangi bir denetim mekanizmasının öngörülmüyor oluşuydu. Her ne kadar bir yaptırım öngörülmüyor olsa dahi, iş birliğinin reddedilmesinin sebeplerinin raporlanması Taraf ülkeler nezdinde bir sorgulama ve izahat gerekliliği teşkil edeceğinden etkili bir uygulama olabilir.

Teknolojinin gelişmesiyle ortaya çıkan ihtiyaçlar doğrultusunda oluşturulan bu metnin amaçlarıyla ve yeni iletişim araçlarıyla tutarlılık içerisindeki 4. fıkra uyarınca, alan adı kayıt bilgileri, bu hizmeti sağlayan kuruluşlarca kabul edilebilir olması durumunda, elektronik biçimde talep edilebilecektir. Bu fıkranın, aynı zamanda ceza hukukunda kanıtlara ulaşmanın ivedi şekilde gerçekleşmesi gerektiğinden ve düşük mahremiyet ihlali riskinden dolayı Protokolün amacına en çok hizmet eden düzenlemelerden biri olduğu düşüncesindeyiz.

2.5.2.2.2. Abone Bilgilerinin İfşası (Madde 7)

Protokol bu maddesi ile önceden bağımsız veya yargısal izin için bir gereklilik oluşturmadan, hizmet sağlayıcılardan abone bilgilerinin ifşa edilmesi için, sınır ötesi doğrudan taleplere izin verir. Abone bilgisi tanımı, Protokolün 3. maddesinin 1. fıkrası

uyarınca, Sözleşmenin 18. maddesinin 3. fıkrasında ayrıntılı olarak açıklanmıştır. Buna göre kısaca; trafik ve içerik verileri hariç olmak üzere, hizmet sağlayıcıların abonelerine ilişkin kullanılan hizmet türü, süresi, abone kimliği, abonenin adresi ve IP adresleri gibi diğer erişim bilgileri ile kişiye ait hizmete erişim aracının bulunduğu yere ilişkin bilgilerdir. Sözleşme, trafik verisi ile abone verisi arasında ayrım yapmıştır.

Madde 7'nin standart prosedürü uyarınca, ifşa emrinde bulunan Taraf ülkenin makamlarının meşru olup olmadığı, emrin yasalara uygun ve orantılı olup olmadığı, ifşa sonucunda veri sahiplerinin haklarını tehlikeye atıp atmayacağı veya ret gerekçesinin geçerli olup olmadığını değerlendirmek hizmet sağlayıcının takdirine bırakılmıştır. Hizmet sağlayıcının böylesi bir muhakeme yapıp yapamayacağı tartışmaya açık bir husustur.

Abone bilgileri, siber suçlarda ve soruşturma sürecinde elektronik kanıtlara ihtiyaç duyulan diğer suç türlerinde en sık aranan bilgidir[219] ve kişiler hakkında çok önemli kanıtlar edinmeyi sağlayabilir. Örneğin, kişinin IP adresi, hangi web sitelerini ziyaret ettiği ve kimlerle iletişim kurduğu gibi bilgilerin edinilmesi, kolluk kuvvetlerince kişinin günlük alışkanlıklarını ayrıntılı bir şekilde analiz edilerek, kişinin profilini oluşturmak ve iletişimlerin içeriğiyle ilgili ipuçları sağlamak için kullanılabilir. Bu durum anonim kimlikleri ifşa ederken zayıf korumaların sonuçları çok zarar verici olabilir.[220] Zira internetin sağladığı imkân ve en önemli özelliklerinden biri, kullanıcılarına belirli ölçüde anonimlik sağlıyor olmasıdır.

Abone bilgileri genellikle diğer soruşturma adımlarının temelini oluşturmakta ve bu nedenle ceza soruşturmalarında en çok talep edilen bilgi türlerinden biri

[219] Protokole İlişkin Açıklayıcı Rapor, Art.92.
[220] Alimonti, Veridiana. *Assesing New Protocol to the Cybercrime Convention in Latin America. Concerns, Human Rights Considerations, and Mitigation Strategies*, Mayıs 2022, s.13-14, çevrimiçi, https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf, Erişim Tarihi: 12.06.2022.

olmaktadır. İletişim içeriğine kıyasla, abone verilerinin ifşası daha az müdahaleci ve daha az gizlilik gerektiren bir veri kategorisi olarak kabul edilmektedir. Abone verilerinin, ilgili kişilerin özel hayatları ve günlük alışkanlıkları hakkında kesin sonuçlara varılmasına izin vermediği, bu özelliğinden dolayı diğer veri kategorilerinin ifşasına kıyasla ifşasının daha düşük derecede müdahaleci olabileceği anlamına geldiği ifade edilmektedir.[221] Ancak, bireylerin faaliyetleriyle bağlantılı kimliklerini açığa çıkarmanın son derece hassas olabileceği göz ardı edildiği, abone bilgilerinin trafik verilerini ortaya çıkarabileceğini ve hatta iletişim içeriği hakkında çıkarımlara izin verebileceği gözden kaçırıldığı ifade edilmektedir.[222]

Yakın tarihli bir örnek olan AİHM'in Benedik-Slovenya davasında[223], Slovenya polisinin dinamik bir IP adresiyle ilişkili abone bilgilerine erişmeden önce mahkeme kararı almaması durumunun, özel hayatın ve aile hayatının gizliliği hakkını ihlal ettiğine karar vermiştir. Mahkemeye göre, Slovenya polisi tarafından öncesinde bir mahkeme emri almadan, IP adresiyle ilişkili abone verilerine erişmek için kullanılan yasal hüküm, Avrupa İnsan Hakları Sözleşmesi'nin "yasaya uygun" olma standardını karşılamamıştır.[224]

Alan adı kayıt bilgilerine kıyasla daha hassas nitelikte olan abone bilgilerinin ifşası için getirilen maddelerden biri de Tarafların kendilerine yöneltilecek emirleri savcı, adli makam ya da gözetim altında verilmiş olmasına bağlı tutabilme imkânı tanımaktadır. Diğer bir ifadeyle, bu hüküm, talepte bulunan bir ülkedeki kolluk kuvvetlerinin, karşılıklı adli yardım sürecinden geçmeden, doğrudan başka bir ülkedeki

[221] Protokole İlişkin Açıklayıcı Rapor, Art.92.
[222] Alimonti, s.16.
[223] Case Of Benedik v. Slovenia (Application No. 62357/14), Judgment Strasbourg 24 April 2018 Final 24/07/2018. (çevrimiçi), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}, Erişim Tarihi: 13.06.2022.
[224] Alimonti, s.14.

bir hizmet sağlayıcıdan doğruda abone bilgilerini alması için bir mekanizma ortaya koymaktadır.[225]

Maddenin 2. fıkrasının b bendi, talepte bulunulan Taraf ülkeye diğer bir ifadeyle hizmet sağlayıcının bulunduğu Taraf ülkeye, "emrin, bir savcı veya başka bir adli makam tarafından veya onun gözetiminde veya başka bir şekilde bağımsız gözetim altında verilmiş olması gerektiği" şeklinde beyanda bulunma imkânı tanımaktadır. İfade etmek gerekir ki, çekince ve beyanların tamamını ve ne zaman başvurulacağını belirten Protokolün 19. maddesi gereği; imza, onay, kabul, uygun bulma sırasında veya katılma belgesini tevdi ederken bu beyanda bulunulabilir. İşbu beyan ile talepte bulunan ve talepte bulunulan Taraflar arasındaki asimetri hafifletilebilir.[226]

Maddenin 4. fıkrasında, abone bilgilerinin ifşası için oluşturulan emirde, soruşturulan veya kovuşturulan suçun düzenlendiği mevzuata atfın yanı sıra, söz konusu suç için uygulanabilecek cezaların da belirtilmesi gerektiği yer almaktadır. Talepte bulunulan ülkelerin kendi hukuklarında kabul edilemeyecek ölçüde bir cezanın öngörüldüğü bir ülkeyle bu suçun soruşturma ve kovuşturmasında iş birliğini reddetmek için bu düzenlemenin bir gerekçe olarak kullanılabileceği düşünülmektedir.

Maddenin 5. fıkrası uyarınca, kendi iç hukuku uyarınca bir Taraf ülke, başka bir Taraf ülkeden emir alan bir hizmet sağlayıcının, belirlenen durumlarda kendisine danışmasını talep edebilir ve c bendinde belirtilen durumlarda danışılan makamlar, abone bilgilerinin açıklanmaması talimatını verebilir. Bu aşama süreçte gecikmeye neden olabilecek niteliktedir. Söz konusu danışma prosedürleri tamamen isteğe bağlıdır. Bir Taraf, herhangi bir prosedür talep etmek zorunda değildir.[227] Ayrıca bu şekilde bir bildirim makamı belirlenmiş ise, bu birim Taraflardan her birinin kendi

[225] Daskal ve Debrae.
[226] Alimonti, s.16.
[227] Protokole İlişkin Açıklayıcı Rapor, Art.108.

takdiri ile belirleneceğinden ve değiştirileceğinden, maddenin 5. fıkrasının f bendi uyarınca, Avrupa Konseyi Genel Sekreteri'ne derhal bildirilmeli ve Genel Sekreter'in kamuya açık güncel bir sicile sahip olabilmesi adına, a ve e bentleri kapsamındaki Tarafların bildirim gerekliliklerinin bir kaydını oluşturması ve güncel tutması gerekmektedir.[228] Aynı 6. maddede de düzenlendiği ve yukarıda ifade olunduğu üzere, abone bilgilerinin ifşasında da bu maddenin 6. fıkrası uyarınca emirler elektronik bir şekilde sunulabilmektedir.

Maddenin 9. fıkrası ile Protokol, Taraflara ulusal yasa çerçevelerinin gerektirdiği güvencelerin uygulanmasını sağlamak için bir dizi çekince imkânı vermektedir. Diğer bir ifadeyle, bir Taraf, kendi iç hukuk sisteminin temel ilkeleriyle tutarsız olması durumunda, abone bilgilerinin bir parçası olarak erişim numaralarını ifşa etmeme hakkını saklı tutabilir. Konu bu çalışmanın çekinceler başlıklı bölümünde detaylandırılacaktır.

Sivil toplum gruplarının konum bilgileri, diğer kişisel ve hassas verilerin gerektiğinden fazla şekilde ifşa edilmesini önlemek için abone bilgilerinin daraltılmış bir tanımı yapılmasını ve ifşa konusu kişiye gerekli bildirimin yapılması ile ilgili endişeleri olduğu ve bu konuda değişiklik yapılması gerektiğini ifade etmişlerdir.[229]

2.5.2.3. Depolanan Bilgisayar Verilerinin İfşası İçin Yetkililer Arasında Uluslararası İş Birliğini Artıran Usuller

Bu kısımda yer alan 8. ve 9. maddeler, yetkili makamlar arasındaki iş birliğini sağlar, ancak geleneksel uluslararası iş birliğinden farklı niteliktedir. Bu kısımdaki

[228] A.g.e., Art.113-115.
[229] Daskal ve Debrae. Ayrıntılı bilgi için bkz., EFF Comments on Additions to Budapest Protocol on Cybercrime, Joint Civil Society Response to the Provisional Draft Text of the Second Additional Protocol to the Budapest Convention on Cybercrime s.1 ve 14., https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime, çevrimiçi, Erişim Tarihi: 11.06.2022.

hükümler, depolanan bilgisayar verilerinin yetkili birimlerin arasında paylaşılması için uluslararası iş birliğini artırıcı nitelikteki, usule ilişkin düzenlemeleri içermekte ve söz konusu verilerin hızlı bir şekilde üretilmesi ve paylaşılması için diğer Taraf ülkelerden gelecek emirlerin uygulanması için bazı hükümler öngörmektedir. Bu kısımda yer alan hükümler, Taraflar arasından yürürlükte olan karşılıklı yardım anlaşması veya düzenlemesi bulunup bulunmadığına bakılmaksızın uygulanır.[230]

Protokolün bu maddesinin kapsamı bir Tarafın, diğer bir Tarafın topraklarındaki hizmet sağlayıcılara belirli emirler vermesine izin vererek, Sözleşmenin 18. maddesinin kapsamını aşmaktadır. Bu uygulama her ne kadar hızlı iş birliği bakımından istenen bir durumu olabilecek ise de pek çok riski de beraberinde getirebilecektir.

2.5.2.3.1. Abone Bilgilerinin ve Trafik Verilerinin Hızlandırılmış Üretimi İçin Başka Bir Taraftan Gelen Emirlerin Yürürlüğe Koyulması (Madde 8)

Bu madde, talepte bulunan Taraf ülkenin, diğer bir Taraf ülkede ve o ülkenin topraklarındaki hizmet sağlayıcının mülkiyetinde veya kontrolünde bulunan abone bilgilerini veya trafik verilerini üretmek için, hizmet sağlayıcıyı zorlayarak bu emri işletebilmek için diğer Taraf ülkeye sunulmak üzere bir emir verme kabiliyetine sahip olmasını sağlamaktır. Geleneksel karşılıklı adli yardımın kullanılmasındaki gecikmeyi kabul ederek, hüküm, abone bilgilerine ve trafik verilerine erişmek için kolaylaştırılmış bir süreç sağlayarak mevcut prosedürleri tamamlamak amaçlanmaktadır.[231] Bilginin elde edilebileceği hızı artırma kararı, abone bilgileri ve trafik verileri için yasal korumaların genellikle iletişim içeriğine göre daha az katı olduğunu yansıtmaktadır.[232]

[230] Bkz. Protokolün 5.maddesinde yer alan ve bu bölümde yer alan maddelere (madde 5-12) uygulanacak olan ilkeler.
[231] Daskal ve Debrae.
[232] A.g.e.

Maddenin 3. fıkrası talepte bulunulan Tarafın emri uygulamayı değerlendirmesi için, talepte bulunan Tarafın hangi temel bilgileri iletmesi gerektiğini belirtmektedir. Fıkranın b bendinde, talepte bulunan Taraf ülkenin, talebini dayandırdığı destekleyici bilgiler, detaylandırılmış talep konusu soruşturma veya kovuşturmaya ilişkin detay, kanun atfı gibi hukuki gerekçeleri, emrin yürürlüğe koyulması için sunması gerekebilecektir. Fıkranın c bendi uyarınca, talepte bulunan Taraf bazı özel talimatların yerine getirmesini talep edebilir. Her ne kadar işleyişte gecikmeye sebep olabilecek ise de böylesi talimatlar kişisel verilerin korunması gibi konularda güçlendirici etkiye sahip olabilir. Bu talimatlara uyulması istenilir ve talepte bulunulan Taraf uymazsa, 7. fıkra uyarınca talepte bulunan Taraf derhal bilgilendirilecek ve yerine getirebilecek koşulları belirleyerek, talebe devam etmek isteyip istemediğini belirleme olanağı tanınacaktır.

Maddenin 4. fıkrası uyarınca, "bir Taraf ülke herhangi bir zamanda, 1. fıkra kapsamındaki emirleri yürürlüğe koymak için ek destekleyici bilgilerin gerekli olduğunu beyan edebilir". Her ülkenin farklı kanunları bulunmakta ve özellikle veri koruması konusunda daha hassas düzenlemeleri mevcut olabilmektedir. Veri korumasını güçlendirmek adına, bu fıkra ile Taraflara emirleri yürürlüğe koymak için ek destekleyici bilgilerin gerekli olduğu şeklinde beyanda bulunma olanağı getirilmekte ve Taraflara bu şekilde beyanda bulunmaları tavsiye edilmektedir.[233]

Protokolün teknolojiye olan uyumluluğunu sağlamak bakımından, elektronik kanıtların yapısına ve iş birliğinin ivedi yapısına uyum içinde bir düzenleme olarak maddenin 5. fıkrasında, bu tür taleplerin elektronik biçimde isteneceğine hükmolunmuştur. Ve yine ceza soruşturması ve kovuşturması dolayısıyla uluslararası iş birliğinin ivedi şekilde yürütülebilmesi için, 6. fıkra ile talepte bulunulan Tarafın, tüm belge ve bilgileri almasından sonraki kırk beş gün içinde talepleri işleme koymak

[233] Alimonti, s.30.

ve hizmet sağlayıcıya hizmet vermek için makul çabayı göstermesi, süratle ilerlemek için makul adımları atması gerektiği, hizmet sağlayıcıya abone bilgilerini yirmi gün içinde ve trafik verilerini kırk beş gün içinde üretmesini emretmesi gerektiği düzenlenmiştir. Bu düzenlemelerin Protokolün amacını ve ceza hukukunun yapısını yansıtması sebebiyle önemli düzenlemeler olduğunu düşünmekteyiz. Zira daha önce Sözleşmede böylesi bir zaman ifadesi bulunmamakta idi.

Talep karşısında, Sözleşmenin 25. ve 27. maddelerinin maddesinin 4. fıkraları uyarınca talepte bulunulan Taraf; talep konusu suçun siyasi suç olması, talebin yerine getirilmesinin kendi egemenliğine veya kamu düzenine zarar verebileceği, karşılıklı yardımlaşma anlaşmalarının varlığı durumlarında, talebi yerine getirmeyi reddedebilir veya özel koşullar talep edebilir. Ayrıca, Sözleşmenin 27. maddesinin 5. fıkrası, kendi makamlarınca sürdürülmekte olan ceza soruşturması veya kovuşturması için bir risk teşkil edeceği düşüncesinde, talepte bulunulan Tarafa bu talebin ertelenmesi için imkân verilmektedir. Sözleşmenin 28. maddesinin 2. fıkrasının b bendindeki şartlarına uygun olarak, kullanım sınırlaması da uygulanabilmektedir. Bu düzenlemeler, Taraflara çok fazla serbesti verildiği şeklinde yorumlanabilecek ise de bu maddenin bulunduğu bölüme uygulanacak ilkelerin düzenlendiği 5. madde uyarınca,[234] ret ve erteleme gerekçeleri dar yorumlanmalı ve uluslararası iş birliğinin etkin ve hızlı şekilde işlemesine halel getirilmemeli, asıl hedefin hukukun temel ilkeleri ve insan haklarının korunması çerçevesinde, adaletin temin edilmesi gerektiği unutulmamalıdır.

Maddenin 10. fıkrası uyarınca, her bir Taraf ülkenin bu hususta emir vermeye ve emir almaya yetkili olan makamları birbirinden farklı olabilecektir. Bununla ilgili olarak, güncel kayıt tutulabilmesi için Avrupa Konseyi Genel Sekreteri'ne bilgi

[234] Ayrıntılı bilgi için bkz. Protokolün 5. Maddesi.

verilmesi gereklidir. İşleyişi aksatmamak adına, Tarafların taleplerin sunulmasında esneklik getirilmelidir.[235]

Maddenin son bendi uyarınca, Taraflar bu maddeyi trafik verilerinin üretimi bakımından uygulamayı saklı tutabileceklerdir. Bu imkân abone bilgileri için değil, yalnızca trafik verileri bakımından Taraflara tanınmıştır.

8. madde prosedürleri, yalnızca abone bilgilerinin doğrudan hizmet sağlayıcının ifşa etmesine yönelik çabalar başarısız olduğunda, talepte bulunan Tarafın bu maddeyi ilk kez kullanmamak için makul bir açıklaması olduğunda veya talepte bulunan Tarafın bu maddeyi uygulamama hakkını saklı tuttuğu durumlarda kullanılacaktır.[236]

Bu madde, talepte bulunulan Tarafın ulusal makamlarının katılımını gerektirir. Bu yollarla, talepte bulunulan Taraftaki yetkililer, abone verilerinin üretimini kendi topraklarında bulunan yerel hizmet sağlayıcılara zorunlu kılarken, kendi ulusal yasalarında yer alan standartları uygulayabilirler. 8. maddenin halihazırda hızlandırılmış bir karşılıklı yardım talebi öngördüğünü, 9. ve 10. maddelerin ise sağlayıcının bulunduğu Taraftaki ulusal makamların rolünü geçersiz kılmadan acil durumlarda uluslararası iş birliğini ele aldığını belirtmekte fayda vardır.[237]

2.5.2.3.2. Saklanan Bilgisayar Verilerinin Acil Durumda Hızlandırılmış İfşası (Madde 9)

Sözleşmenin 35. maddesinin 1. fıkrasının c bendi uyarınca; her bir Taraf bilgisayar sistemleri ve verileriyle ilgili suçların soruşturma veya kovuşturmasında

[235] Protokole İlişkin Açıklayıcı Rapor, Art.145.
[236] A.g.e., Art.121.
[237] Alimonti, s.12.

elektronik ortamda toplanmış kanıtların acil olarak edinilmesi için 7/24 irtibat noktaları belirleyecektir ve kanıt toplanması, yasal bilgi sağlanması ve şüphelilerin yerlerinin tespit edilmesi gerektiği durumlarda her bir Taraf yardımı doğrudan yapacaktır. Protokol taslağını hazırlayanlar, Tarafların çeşitli acil durumlarda, belirli cezai soruşturma veya kovuşturmalarda kullanılmak üzere, başka bir Taraf ülkedeki bir hizmet sağlayıcının mülkiyetinde veya kontrolünde saklanan bilgisayar verilerinin hızlı bir şekilde elde edilmesinin kolaylaştırılması ve bunun pekiştirilmesi gerektiğinin bilincindeydiler, Protokolün 9. madde düzenlemesi, bu ihtiyacın bir yansıması olarak getirilmiştir. Örneklerle somutlaştırmak gerekirse; gerçekleşmiş bir terör saldırısının hemen ardından yakın bir tekrarlama riski olması veya hassas sağlık sistemlerini devre dışı bırakabilecek bir fidye yazılım saldırısı ya da bireyleri kaçırarak alıkoyan kişilerin fidye isterken kullandığı iletişim araçlarının araştırılması gibi hassas durumlar, acil olarak iş birliğini ve hizmet sağlayıcılardan bilgisayar verilerini elde etmeyi gerektirebilir.[238] Zira bu Protokol, hızla gelişen suç yapılarına ve iş birliğinde acil yardımlaşma ve veri paylaşılması ihtiyaçlarının bir sonucu olarak getirilmiştir. Protokolün acil durumlarda özel yollarla en kısa şekilde iş birliğine imkân sağlamak için getirdiği en önemli yeniliklerin başında 9. ve 10. maddelerin olduğunu düşünmekteyiz.

9. maddenin kullanılmasının, 10. maddenin kullanılmasına göre daha avantajlı olduğu ifade edilmektedir.[239] 9. maddeye başvurulması için önceden herhangi bir karşılıklı yardım talebinin hazırlanmasına gerek bulunmamaktadır. Acil bir durumda, iş birliğinde kullanılacak olan en uyumlu kanalın hangisi olduğuna karar vermek Tarafların kendi sorumluluğudur.

[238] Protokole İlişkin Açıklayıcı Rapor, Art.148.
[239] A.g.e. Art.152.

Madde uyarınca, tüm Taraflar belirli bir ceza soruşturması veya kovuşturmasında ihtiyaç duyulan, hizmet sağlayıcıların mülkiyetinde veya kontrolünde olan belirtilmiş, depolanmış bilgisayar verilerinin, karşılıklı bir yardım talebi olmaksızın hızlı şekilde ifşa edilmesini sağlamak ve acil bir yardım talebini almak ve iletmek için Sözleşmede belirtilen 7/24 İletişim Ağı için gerekli olabilecek tüm önlemleri alacaktır. Talepler elektronik veya sözlü bir şekilde iletilebilecek ve kabul edilecektir, böylece acil durumlarda veri alışverişi hızla gerçekleşebilecektir. Burada belirtilen "acil durum" ifadesi Protokolün 3. maddesindeki tanım doğrultusunda tayin edilecek ve gerekçelendirilecektir. Söz konusu talep iletilirken, Protokol uyarınca bu talepte bulunulduğu da belirtilecektir[240], bu suretle bu madde kapsamında yöneltilecek talepler, 7/24 İletişim Ağından gelebilecek taleplerden farklılaşmaktadır.

9. madde lafzında yer alan "belirtilen, depolanmış bilgisayar verilerini elde etmek" ifadesi dolayısıyla, "belirlenmiş depolanmış abone verilerini elde etmek" için düzenlenen 7. madde gibi maddelere kıyasla, 9. madde çok daha geniş kapsamlı bir düzenleme getirmektedir. Bu ifade, belirtilen herhangi nitelikteki bir bilgisayar verisi anlamına gelmekte,[241] abone verisi, trafik ve içerik verilerini de kapsamaktadır. Ancak "depolanmış" ifadesi doğrultusunda mevcut, halihazırda depolanmış olan verileri ifade etmektedir, dolayısıyla ileride var olması muhtemel veriler bu kapsamda değildir.[242] Bu geniş kapsamlı düzenleme, 7/24 İletişim Ağlarına ve hizmet sağlayıcılara oldukça fazla yük getirme eleştirisini de beraberinde getirebilmektedir. Ağır yük karşısında taleplere zamanında cevap verememe riskine karşı, yalnızca abone bilgisi talep eden Tarafların 7. ve 8. madde uyarınca veriye daha hızlı bir şekilde ulaşabilmesi mümkün olabilir.[243] Acil bir durumda, iş birliğinde kullanılacak olan en uyumlu kanalın hangisi olduğuna karar vermek yine Tarafların sorumluluğundadır.

---

[240] Bkz. Protokol m.9/3-b.
[241] Detaylı bilgi için bkz. Sözleşmenin 1.maddesinin 1.fıkrasının b bendi.
[242] Bkz. Sözleşmeye Ilişkin Açıklayıcı Rapor, Art.170.
[243] Protokole İlişkin Açıklayıcı Rapor, Art.157.

Maddenin 6. ve 7. fıkraları uyarınca talepte bulunulan Taraf, taleple ilgili kararını hızlı bir şekilde bildirecek ve şartlar uygunsa alternatif iş birliği ihtimallerini de belirtecektir. Diğer bir ifadeyle, Tarafların talepler karşısında her zaman talepleri kabul etmeleri ve verileri ifşa etmeleri zorunlu değildir. Hatta şartlar uygunsa, talepte bulunulan Taraf, 9. madde uyarınca iş birliğini, veri ifşasını reddedebilir ve alternatif iş birliği kanallarıyla, örneğin bir yetkili makamın acil olmayan bir temelde içerik verilerine ihtiyacı varsa, acil olmayan bir şekilde içerik verilerinin elde edilmesi için, Protokol hükümler içermediğinden, uygun olduğu şekilde ikili bir anlaşma kapsamında veya Sözleşmenin 27. maddesi kapsamında geleneksel bir karşılıklı yardım talebini kullanmayı tercih edecektir. Ancak, abone bilgilerine ihtiyaç duyulursa, Taraf ülke doğrudan bir hizmet sağlayıcıya emir vermek için Protokolün 7. maddesini kullanmayı seçebilir. Bu bildirimin karşısında, talepte bulunan Taraf öneriyi kabul ederek bu kabulle bağlı olacak ya da bu öneriye uymasının mümkün olmadığını bildirerek, talepte bulunulan Tarafın bu başvuruyu tekrar değerlendirmesi sağlanacaktır.

2.5.2.4. Acil Karşılıklı Yardıma İlişkin Usuller (Madde 10)

Acil karşılıklı yardıma ilişkin başlığı düzenleyen bu kısım, yalnızca 10. maddeden oluşmakta ve 3. maddede tanımlanan, acil durumların varlığı ve talep edilen yardımın bu durumla bağlantılı olduğu açıklandıktan sonra, uygulanacak olan hızlandırılmış prosedürü konu almaktadır. Acil karşılıklı yardım, bir karşılıklı yardım hükmü olmasına rağmen, birçok karşılıklı yardım anlaşmasında açıkça öngörülmeyen acil durumlar için önemli bir iş birliği aracıdır. Bu nedenle, ilgili Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuat temelinde geçerli bir karşılıklı yardım anlaşması veya düzenlemesi olup olmadığına bakılmaksızın bu bölümün uygulanacağına karar verildiği düşünülmektedir.

Tüm Tarafların, her an gelebilecek olan acil durumdan kaynaklı yardım taleplerini karşılayabilmeleri için, merkezi makamları veya karşılıklı yardım

taleplerine cevap vermekten sorumlu olan diğer makamlarını haftada yedi gün, günde yirmi dört saat hazır bulunmalarını sağlaması gerekmektedir. Acil durum karşılıklı yardımını yöneten prosedürlerle ilgili olarak, iki olasılık vardır. İlgili Taraflar, tek tip veya karşılıklı mevzuat temelinde geçerli bir karşılıklı yardım anlaşması veya düzenlemesi ile karşılıklı olarak bağlı olduklarında, ilgili Taraflar Sözleşmenin belirli hükümlerini yerine getirmeye karşılıklı olarak karar vermedikçe, 4. bölüm bu anlaşmanın hükümleriyle tamamlanır.[244] İlgili Taraflar bu tür bir anlaşma veya düzenleme ile karşılıklı olarak bağlı olmadıklarında ve bir anlaşmanın olmadığı durumlarda, karşılıklı yardıma ilişkin olarak Sözleşmenin 27 ve 28. maddelerinde belirtilen belirli prosedürleri uygularlar.[245]

9. maddeden farklı olarak, burada taleplerin sözlü olarak da iletilebileceği hususuna yer verilmemiş, yalnızca elektronik yollar ile taleplerin iletilebileceği belirtilmiştir. Bu yönüyle maddeyi eksik buluyoruz. Zira taleplerin iletişimin kaydedildiği bir sesli destek kanalından, sözlü olarak iletildikten sonra örneğin 24 saat içinde yazılı hale getirilmesi gerektiği gibi bir düzenlemenin daha kapsayıcı ve esnek olacağını düşünmekteyiz. Ancak diğer yandan, maddenin 9. fıkrasında INTERPOL gibi teşkilatların, kanal olarak tasvir edilmesi dolayısıyla, 6. fıkrada yer alan düzenleme uyarınca, karşılıklı yardım talebini ileten Taraf ülkenin farklı bir makamına bu yardıma ilişkin cevapların sunulabileceğini düşünüyoruz. Böylece acil durumların hızla çözümlenmesine olanak sağlamak için, talep konusu veriyi suça ilişkin soruşturma veya kovuşturmada kullanacak olan makam ile doğrudan bilgi paylaşımı yapılabilecektir.

Maddenin son fıkrasında, acil karşılıklı yardım taleplerinin emniyet müdürlükleri gibi idari makamlar ya da INTERPOL tarafından doğrudan iletebileceği

[244] Bkz. Protokolün 10. maddesinin 8. fıkrası.
[245] Bkz. Protokolün 10. maddesinin 7. fıkrası.

ifade edilmektedir. Bu düzenleme her ne kadar verilere hızlıca ulaşıp acil durumlara hızla ve etkin müdahale şansını doğuruyor olsa da örneğin Taraf ülkelerin gerçek olmayan ancak sadece siyasi nitelikteki motivasyonları ile kurguladıkları bir senaryo karşısında, olaydaki şüphelinin hassas ve aleyhine olacak nitelikteki kişisel verilerinin istenmeyen makamlarla paylaşılmasına da sebebiyet verebilir. Bu fıkradaki düzenlemeyi eksik ve temel hak ve özgürlükler bakımından tartışmaya açık buluyoruz.

9. ve 10. maddeler hem talepte bulunan hem de talepte bulunulan Taraflara acil durumlar karşısında, büyük ölçüde hızlandırılmış bir şekilde karşılık vermeleri için yoğun emek gerektiren yükümlülükler yüklemektedir. Bu acil durum talepleri sonucunda; daha önceden talep edilmiş yine de önemli nitelikte olan ancak "acil durum" tanımına kıyasla daha az önem teşkil eden vakıaların ikinci planda bırakılarak, acil durum taleplerine daha yüksek bir öncelik verilmesini gerektirir.

2.5.2.5. Uygulanabilir Uluslararası Anlaşmaların Yokluğunda Uluslararası İş Birliğine İlişkin Usuller

Sözleşmenin, uluslararası anlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardımlaşma taleplerine ilişkin usuller başlığını taşıyan 27. maddesinin bir yansıması olarak ve Protokolün 5. maddesinin 5. fıkrasında da belirtildiği üzere, bu Protokolün 11. ve 12. maddelerden oluşan II. Bölümünün 5. Kısmı düzenlenmiştir.

İlgili Tarafların, anlaşma veya düzenleme ile yasaklanmamışsa, hükümlerinin herhangi birini veya tamamını uygulamaya karşılıklı olarak karar vermedikçe, tek tip veya karşılıklı mevzuata dayalı diğer karşılıklı yardım anlaşmaları veya düzenlemelerinin yokluğunda bu kısım hükümleri uygulanır. Diğer bir ifadeyle, Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuat temelinde hiçbir karşılıklı yardım anlaşması veya düzenlemesi bulunmadığında bu kısım hükümleri uygulanacaktır. 12. maddenin 7. fıkrasında belirtilenlerin haricinde, bu tür bir anlaşma

veya düzenlemenin mevcut olduğu durumlarda, 5. kısım hükümleri uygulanmayacaktır. Bununla birlikte herhangi bir anlaşma veya düzenlemenin yasaklamaması halinde, 5. kısım hükümlerinin uygulanmasına karşılıklı olarak karar verilebilir.

Bu kısım hükümlerinin uygulanmasında Taraflara esneklik tanınmaktadır. Örneğin, müşterek soruşturma ekiplerinin çalışmasına ilişkin 12. maddenin 2. fıkrasında, işleyişin Tarafların yetkili makamları arasında kararlaştırılan usulde olacağı, video konferans ile şüpheli ya da sanığın dinlenmesine ilişkin 11. maddenin 8. fıkrasında da özel koşullar belirlenebileceği ve belirlenen şartların karşılanmaması durumunda iş birliğini reddetme esnekliği olduğundan söz edilebilir.

2.5.2.5.1. Video Konferans (Madde 11)

Bu madde, video konferans teknolojisi veya Taraflarca mutabakat sağlandığı durumlarda sesli konferans yoluyla; tanıklık, ifade alınması veya bir uzmandan bilgi alınması ile talepte bulunulan Taraf izin verdiğinde şüpheli veya sanığın ifade veya beyanının alınması hakkında bir düzenlemedir.

5271 Sayılı Türk Ceza Muhakemesi Kanunu'nun 180. maddesinin 5. fıkrası uyarınca, tanık veya bilirkişinin aynı anda görüntülü ve sesli iletişim tekniğinin kullanılması suretiyle dinlenebilmeleri olanağının varlığı hâlinde mahkeme bir naiple veya istinabe yoluyla dinlenmelerine karar verebilir. Buna olanak verecek teknik donanımın kurulmasına ve kullanılmasına ilişkin esas ve usuller yönetmelikte gösterilir. Protokolün 11. maddesi bu düzenleme ile benzerlik göstermekte, yurtdışında bulunan bir tanık ya da uzmanın ifadesini ve tanıklığı ile ilgili bilgilerin alınmasında bu yöntemin kullanılması mümkündür.

Talepte bulunulan Tarafın "buna izin verebileceği" ifadesi dolayısıyla, bu talebi reddetme konusunda talepte bulunulan Tarafa geniş bir takdir yetkisi tanındığı

anlaşılmaktadır. Aynı şekilde 5271 Sayılı Kanun metni de bu usulün uygulanmasında hâkime bir zorunluluk değil geniş bir takdir yetkisi tanımaktadır.

Teknolojik araçların kullanılmasını içeren bu yöntem, oldukça koordinasyonlu bir çalışma gerektirmektedir. Teknik sorunlar sebebiyle iletişimin ve bilgi aktarımının aksaması ya da sorunlu bir şekilde gerçekleşmesi riskini veya aralarında çok saat farkı bulunan ülkeler arasında da gerçekleşmesi mümkün olacağından, belirtilen zamanlarda ilgili kişilerin hazır edilmesi sorununu doğurabilecektir.[246] Ek olarak belirtilen koordinasyonun devamı olarak, Taraflardan hangi ülke mevzuatı uyarınca yeminlerin edileceği ve gerekli uyarıların yapılacağı, çocukların tanıklığında uygulanacak usuller ve alınacak olan önlemler gibi hususların en baştan Taraflarca kararlaştırılması gerekmektedir.

Maddenin 4. fıkrasında, talepte bulunulan Tarafın iç hukukuyla bağdaşmayan, diğer bir ifadeyle, farklı olan kanunlar değil de bu Tarafın kanunlarını ihlal edici nitelikteki haller haricinde, video konferansın yürütülmesine ilişkin usuller talep eden Tarafça belirlenecektir. Talep konusu soruşturma ve kovuşturmayı yürüten, bilgi ihtiyacında olan ve talep konusuna hâkim olan Tarafın, talep eden Taraf olması dolayısıyla, uygulanacak usulün talep eden Tarafça belirlenecek olmasını yerinde bir düzenleme olarak görüyoruz.

Video konferans yönteminin uygulanmasına yönelik bu madde, Tarafların birbirleriyle doğrudan iletişim kurmasını sağlar. Bu madde yalnızca tek tip veya karşılıklı mevzuat temelinde bir karşılıklı yardım anlaşması veya düzenlemesi bulunmadığı durumlarda uygulanmaktadır, dolayısıyla metinde yer alan "merkezi makam" tanımı Protokolün 2. maddesinin 2. fıkrasının a bendi uyarınca, Sözleşmenin

[246] Protokole İlişkin Açıklayıcı Rapor, Art.190 ve 195.

27. maddesinin 2. fıkrasının a bendinde belirtilen anlama gelmektedir. Talepte bulunan Tarafın talebi yerine getirilmez veya yerine getirilmesi geciktirilir ise bu durumun nedenleri talepte bulunan Tarafa bildirilecektir. Ayrıca, talepte bulunulan Tarafça, talep konusu verilerin gizli tutulması ya da yalnızca belirtilen ceza soruşturması veya kovuşturulması için kullanılması şart koşulabilir. Talepte bulunan Tarafın bunu sağlayamayacağı anlaşılırsa ivedilikle haberdar edilecek, şartın kabul edilmesi durumunda bu şartlara uygun olarak hareket edilecektir.[247]

Maddenin 5. fıkrası; görevi kötüye kullanma, yanlış beyan, ifade vermeye mecbur bırakıldığı durumlarda cevap vermeyi reddetme ve diğer suistimal durumlarında bir cezai yaptırım öngörmekte, bu tür durumlarda talepte bulunulan Tarafa, bu fiil kendi işlemlerinde işlenmiş kabul ederek cezai yaptırım uygulama yetkisi vermektedir. Yaptırım uygulanabilmesi riskiyle, yargılama sırasında ifadelerin doğruluğunu temin edebilmek adına bu maddenin önemli olduğunu düşünmekteyiz. Nitekim bu uygulama talepte bulunan Tarafın yargı yetkisini engellemeden uygulanacaktır.

İlgili süreçte masrafların kim tarafından karşılanacağına ilişkin düzenleme maddenin 6. fıkrasında yer almaktadır. Buna göre aksi belirtilmedikçe, bilirkişi, tercüme maliyetleri ile olağanüstü nitelikteki maliyetler talepte bulunan Tarafça, bunlar dışındakiler talepte bulunulan Tarafça karşılanacaktır. "Aksi belirtilmedikçe" ifadesinden dolayı, Taraflar bütün masrafların talep eden Tarafça karşılanmasında da karar kılabilirler. Böylesi esnek bir dil kullanılması ve maliyetin talep eden Tarafa da yüklenebileceği ihtimali, uluslararası iş birliğinde veri paylaşan yani talepte bulunulan Tarafa oldukça fazla mali yük getirebilecek olması dolayısıyla yardımdan kaçınılması

[247] Ayrıntılı bilgi için bkz. Protokol 11. Madde, 2. Fıkra, b bendi. Sözleşmenin 27. Maddesinin 8. Fıkrası ile 28. Maddesinin 2 ila 4. Fıkraları.

noktasındaki eleştiriler bakımından yapıcı bir düzenleme olduğunu, dolayısıyla savunma hakkının temini bakımından önemli bir düzenleme olduğunu düşünmekteyiz.

2.5.2.5.2. Müşterek Soruşturma Ekipleri ve Müşterek Soruşturmalar (Madde 12)

Siber suçların yapısı sınır ötesi niteliği haiz olduğundan dolayı uluslararası düzeyde iş birliğinin ne denli önemli olduğu önceki bölümlerde detaylı olarak ifade olunmuştur. Madde 12, işletilecek olan iş birliğinde farklı ülkelerde bulunan ve Taraflarca belirlenecek olan soruşturma ekiplerinin, gerekli olduğu düşünüldüğü durumlarda, daha etkin bir şekilde elektronik kanıtlara ulaşmasını mümkün kılmak için koordine bir şekilde soruşturma yapılabilmesi için zemin hazırlamaktadır.

Maddenin 4. fıkrası uyarınca, farklı bir uygun iletişim kanalının Taraflarca karşılıklı olarak belirlenmesi durumu haricinde, yetkili ve katılan makamlar, daha fazla merkezi koordinasyon gerektiren istisnai durumlarda doğrudan iletişim kurabilecektir. Burada belirtilen istisnai durumların, Protokolde belirtilen acil durum ifadesine yakın bir anlam taşıdığını düşünmekteyiz.

Bu maddede katılan makam ve yetkili makam ifadeleri kullanıldığı dikkat çekmektedir. “Katılan makam” teriminin Sözleşme ve Protokolde tanımlaması yer almamaktadır. Yetkili makam tanımı, Protokolün 2. maddesinde ifade olunduğu üzere, belirli cezai soruşturma veya kovuşturmalarda kanıtların elde edilmesi ya da sunulmasında bu Protokol kapsamındaki prosedürler için, Tarafların iç hukukunda yetkilendirilen adli, idari ya da diğer kanun uygulayıcı makam anlamına gelmektedir. Madde metninden anlaşılan “katılan makam” tanımının, yetkili makam tanımının dışında kalan, Tarafların ceza soruşturması ya da kovuşturmasında kanıt elde etmesine iç hukukları tarafından imkân tanınan ve süreçte yer alan makamlar anlamına geldiği anlaşılmaktadır.

Protokolün 5. maddesinin 5. fıkrasında belirtildiği üzere; 12. maddenin 7. fıkrasında belirtilenler dışında, talepte bulunan ve talepte bulunulan Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuata dayalı bir iş birliği anlaşması veya düzenlemesi olması halinde 11. ve 12. maddelerin yer aldığı 5. kısım hükümleri uygulanmayacaktır. Ancak, anlaşma veya düzenlemenin yasaklamadığı durumlarda ilgili Taraflar, bunun yerine, 11. ve 12. maddelerin yer aldığı 5. kısım hükümlerinin uygulanmasını karşılıklı olarak belirleyebilirler. Maddenin 7. fıkrası, ilgili Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuat temelinde bir karşılıklı yardım anlaşması veya düzenlemesi olup olmadığına bakılmaksızın geçerlidir. Aşağıda bu husus detaylandırılacaktır.

Madde kapsamındaki müşterek soruşturma işleyişi, usulü ve şartları Taraflarca kararlaştırılan şekilde sürdürülecektir. Taraflar arasındaki kararlaştırmanın yazılı olarak yapılması beklenmektedir.[248] Bu madde; kolluk kuvvetlerine, ülke adına geçici olarak belirli ortak soruşturmaları yönetmek için gayri resmi anlaşmalar yapma yetkisi verdiği gerekçesiyle eleştirilmektedir. Zira, müşterek ekipler ile sınır ötesi soruşturma faaliyetlerinin denetimi, büyük ölçüde yerel polis güçlerine bırakılmıştır.[249]

12. maddenin 5. fıkrası, kolluk kuvvetlerine, belirli soruşturma görevleri için halihazırda yürürlükte olan resmi karşılıklı yardım düzenlemelerini atlama imkânı tanımaktadır. Bu riskin, maddenin 3. fıkrasında olanak tanınan "Tarafların merkezi makamının ekibi kuran anlaşmaya imza atmasını veya başka bir şekilde bu anlaşmaya katılmasını talep edebilir" beyanı ile hafifletilebileceği düşünülmektedir[250] ve riski azaltmak adına Tarafların bu şekilde bir beyanda bulunması önerilmektedir.[251] Ancak ifade etmek gerekir ki, bu beyanda bulunmak imkânı, Protokolün 19. maddesi uyarınca,

[248] Protokole İlişkin Açıklayıcı Rapor, Art. 207.
[249] Alimonti, s.27.
[250] Alimonti, s.29.
[251] Alimonti, s.30.

yalnızca imza anında veya onay, kabul, uygun bulma veya katılma belgesinin tevdii sırasında mümkündür.

Müşterek soruşturma ekiplerinin süreçte kullandığı veya paylaştığı kanıtlar, abone bilgileri, trafik verileri, bilgisayara verileri gibi her türlü bilgi kişisel verileri içerebilir. Bu Protokol kapsamındaki diğer iş birliği yöntemlerinde olduğu gibi, kişisel verilerin aktarımı hususunu düzenleyen Protokolün 14. maddesi, 12. maddedeki iş birliği yöntemi için de geçerlidir.[252]

Maddenin 6. fıkrası, sağlanan bilgi ve kanıtların kullanımının reddi ve kısıtlanması ile ilgili bir düzenleme getirmektedir. Buna göre, maddenin ilk iki fıkrasında belirtilen anlaşmalarda gösterildiği şekilde ret ve kısıtlama hakkı vardır, böyle bir ifade bulunmuyor ise bilgi ve kanıtlar fıkranın a ila c bentlerinde belirtilen şekilde kullanılabilir. Protokolün 14. maddesinde yer alan koruma gerekliliklerine dair hükümler bakidir.[253]

Maddenin 7. fıkrası, ilgili Taraflar arasında yürürlükte olan tek tip veya karşılıklı mevzuata dayalı bir karşılıklı yardım anlaşması ya da düzenlemesi olup olmadığına bakılmaksızın uygulanacaktır hükmünü haizdir. Bu Protokol kapsamındaki tüm iş birliği yöntemlerinde olduğu gibi, bu fıkra kapsamındaki müşterek soruşturmalar da III. Bölümde ifade olunan şartlara ve teminatlara tabidir.

2.5.3. Şartlar ve Teminatlar

III. Bölüm şartlar ve teminatları düzenlemektedir ve bu bölümde yer alan düzenlemeler ile II. Bölümün ikinci kısmında düzenlenen servis sağlayıcılarla doğrudan iş birliği ile ilgili düzenlemeler sivil toplum tarafından getirilen eleştirilere

[252] Protokole İlişkin Açıklayıcı Rapor, Art.208
[253] A.g.e. Art.213

odaklanmaktadır.[254] Pek çok kuruluş, taslak metinde yer alan ve Taraf ülkelere güçlü yetkiler tanıyan düzenlemeler nedeniyle, ülkeler arasındaki gizli nitelikte ikili ya da çoklu anlaşmaların kurulması ihtimalinde, halihazırdaki düzenlemelerden daha az koruma getiren bir duruma yol açılmasından endişe etmekte idi.[255]

2.5.3.1. Şartlar ve Teminatlar (Madde 13)

Protokolün 13. maddesi, insan hakları ve temel özgürlükler için yeterli korumanın sağlanmasına yönelik genel yükümlülükleri düzenlemektedir. Protokolün 13. maddesinde belirtilen ve III. Bölümün başlığını oluşturan şartlar ve teminatlar, Sözleşmenin 15. maddesi uyarınca, her bir Taraf bu Protokolde, diğer bir ifadeyle bilgisayar sistemleri ve verileriyle ilgili cezai suçlara ilişkin belirli ceza soruşturma veya kovuşturmalarında, cezai bir suçun elektronik biçimde kanıt toplanması kapsamında belirtilen yetki ve usullerin oluşturulması, yürütülmesi ve uygulanmasında temel hak ve özgürlüklerin uygun şekilde korunmasını sağlayacak olan kendi iç hukuklarında belirtilen koşullara ve güvencelere tabi olmasını sağlayarak temin edilecektir. 14. madde de bu teminatın sağlanabilmesi için ayrıca detaylı olarak güncel mevzuat doğrultusunda ve bu konuda uzman olan kişi ve kurumların tavsiyesi ile ve danışmanlıklarından yararlanılarak getirilmiş bir maddedir.

Bu madde, birçok Tarafın yasalarıyla ve uluslararası metinlerdeki düzenlemelerle paralel olarak, temel hak ve özgürlüklerini korumaya yönelik bir önlem olarak getirilmiştir, talepte bulunan Tarafa sunulan verilerin zaman zaman sanık için aklayıcı olabileceği ihtimaller de mevcuttur, böylesi durumlarda bu bilgilerin ilgili savunmaya veya bir yargı makamına açıklanması gerekir. Taslağı hazırlayanlar tarafından, bu gibi durumlarda, talebi sonucu veriyi alan Tarafın, ifşa etmeden önce

[254] Plachta, s.495.
[255] A.g.e. Summary of comments, supra note 7.

devreden Tarafı bilgilendireceği ve eğer istenirse, devreden Tarafa danışacağı anlaşılmıştır.

Ceza yargılamaları birer kamu davasıdır, duruşmada kamuya açık hale getirildikten sonra veri de kamu malı haline gelmektedir ve bu durumda talep konusu verinin kullanıldığı soruşturma veya kovuşturmanın gizliliğini sağlamak da mümkün olamaz. Bu istisnalar, Sözleşmeye ilişkin açıklayıcı raporun 278. paragrafında açıklanan Sözleşmenin 28. maddesinin 2. fıkrasının uygulanmasına ilişkin istisnalara benzemektedir. Son olarak, materyal, aktaran Tarafın önceden onayının alındığı durumlarda başka bir amaç için kullanılabilir.[256]

Yetki ve prosedürlerin belirlenmesi ve uygulanmasının devletlerin iç hukukundaki koşullara ve güvencelere tabii olduğunu belirlemek için Protokol, Sözleşmenin genel güvenceleri üzerine inşa edilmiştir. Ancak Taraflar, iç hukukları temelinde hangi korumaların "yeterli" ve "orantılı" olduğuna karar verecekleri hususunda büyük ölçüde yalnız bırakılmışlardır.[257]

2.5.3.2. Kişisel Verilerin Korunması (Madde 14)

Ulusal ve uluslararası metinlerde kişisel veriler kavramı yakın benzerlik göstermektedir. Kişisel veriler kısaca, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Buna göre; belirli veya belirlenebilir bir kişinin kimliğine, etnik kimliği, fiziksel özelliklerine, sağlık bilgileri, genetik verilerine, öğrenim veya meslek durumuna, adresine, banka ve kredi kartı bilgilerine, düşünce ve inanç durumuna, alışveriş ve diğer günlük alışkanlıklarına, telefon rehberine, fotoğrafına, bilgisayarının IP adresine, parmak izine, mesaj ve e-maillerine,

[256] Protokole İlişkin Açıklayıcı Rapor, Art.71
[257] Alimonti, s.23-24.

sosyal paylaşım sitelerindeki aktivitelerine, önceki gün yediği yemeğe kadar varan çeşitli özellikler kişisel veridir.[258]

Kişisel veri kavramını hassas (özel nitelikli) ve hassas olmayan kişisel veri olarak iki gruba ayrılmaktadır. 6698 Sayılı Kişisel Verilerin Korunması Kanunumuz uyarınca hassas veya özel nitelikli kişisel veriler; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. Kişisel verilerin korunması hususu, Avrupa Birliği başta olmak üzere uluslararası toplumun önemli konu başlıklarından birisidir.[259] Kişisel verilerin korunması temel bir insan hakkıdır.

Protokolün gelişmiş iş birliği için önlemler başlıklı II. Bölümünde yer alan önlemler kapsamında yer alan kanıtlar, çoğunlukla kişisel verilerin aktarımını gerektirir. Kişisel verilerin korunması, Tarafların kanuni veya uluslararası yükümlülükleri, kişilerin anayasal haklarının temini gerekliliği dolayısıyla, oldukça önemlidir. Bu sebeple kişisel veriler için özel koruma sağlayan hükümleri içeren bu madde oldukça önemli, Protokolün de en kapsamlı ve en uzun maddesidir. Nitekim Sözleşmeye en çok getirilen olumsuz eleştirilerin başında kişisel verileri koruma hususunda yeterli düzenlemelerin yapılmamış olması ve ihlallere sebep olabilecek olmasıydı.[260]

---

[258] Arınmış Uzun, Sündüs. *Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmes*i, Bilişim Teknolojileri Dergisi, Cilt: 14, Sayı: 3, Temmuz 2021, s.208, çevrimiçi, https://dergipark.org.tr/en/download/article-file/1097727, Erişim Tarihi: 02.11.2022. Ayrıca, 2002/58/EC Elektronik Haberleşme Sektöründe Gizliliğin Korunması ve Kişisel Bilgilerin İşlenmesine İlişkin Avrupa Konseyi Direktifi ise tüzel kişilere ait verilerinde koruma altına alınması amaçlanmıştır.
[259] Erdem, Merve ve Gürkan Özocak. *Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü*. Ankara Üniversitesi Hukuk Fakültesi Dergisi 68, no. 1 (2019): s.190.
[260] Ayrıntılı bilgi için bkz. işbu çalışmanın 2.5. numaralı bölümü.

Kişisel verilerin korunması, her ülkenin gereksinimleri doğrultusunda oldukça farklı çerçevelerle karşılamasını gerektirmektedir. Bu sebeple bu maddenin müzakere edilmesi en zor olan madde olduğu ifade edilmektedir.[261] Protokol bir veri koruma aracı değildir, bir ceza adaleti anlaşmasıdır ve bu nedenle 14. maddenin amacı bu Protokol kapsamında aktarılan kişisel verilerle sınırlıdır.[262]

a) Kapsam

Maddenin 1. fıkrasında izah olunduğu üzere, b ve c bentlerinde aksi belirtilmedikçe söz konusu kişisel veriler, maddenin 2 ila 15. fıkralarına uygun olarak işlenecektir. Diğer bir ifadeyle, b veya c fıkralarında yer alan istisnalar mevcutsa, 2 ila 15. fıkralar uygulanmaz. Buna göre;

- Fıkranın b bendi uyarınca, veri aktaran ve alan Tarafların arasında, veri aktarımlarında veri koruma yönlerinin kapsamlı bir şekilde düzenlendiği bir sözleşme mevcut ise bu fıkralar uygulanmayacaktır. Burada söz edilen kapsamlı düzenlemenin olduğu sözleşmeye örnek olarak ETS 108 numaralı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi benzeri sözleşmelerdir.[263]

- Fıkranın c bendi uyarınca, veri aktaran ve alan Tarafların arasında bir önceki bentte belirtildiği şekilde kapsamlı bir sözleşme mevcut olmadığında, maddenin 2 ila 15. fıkraları yerine, kendi aralarında karşılıklı olarak belirledikleri anlaşma veya düzenlemeler temelinde kurallar uygulayabilirler.

[261] Seger, Alexander. *A New Protocol to the Convention on Cybercrime: For a More Effective Criminal Justice Response to Crime Online-With Strong Safeguards*, 11.11.2021, https://www.linkedin.com/pulse/new-protocol-convention-cybercrime-more-effective-criminal-justice-/?trackingId=CnjE%2BxAERiKTr26OaLL2LA%3D%3D, çevrimiçi, Erişim Tarihi: 11.06.2022. Bu maddenin uygulanması, Protokolün 23. maddesi kapsamındaki değerlendirmelere tabi olacaktır.
[262] A.g.e.
[263] Protokole İlişkin Açıklayıcı Rapor, Art.222.

Böyle bir durum olduğunda, Protokolün II. Bölümünün 2. Kısmı uyarınca, Taraflar aralarındaki böylesi bir anlaşma veya düzenlemenin ve karşılıklı kararlarını açık bir şekilde kamuoyuna iletmeye teşvik edilir.[264] Bu kısmı, otokrasiler bakımından sorunlu olabilir, demokrasiye karşı, siyasi amaçlarla kullanılabilir, bu sebeple kamuoyu baskısı önemlidir ve şeffaflık gereklidir. Böylesi bir anlaşmanın şeffaf bir şekilde paylaşılması gerektiği ile ilgili bir düzenlemenin Protokolde eksik olduğu görüşündeyiz.

Protokol kapsamındaki veri aktarımları için gerekli ve uygun korumalar hususunda, maddenin 1. fıkrasının b ve c bentlerinde belirtilen korumalar ile maddenin 2 ila 15 fıkralarındaki düzenlemelerin eş değerde olduğunu ve veri korumasını yasal düzenlemelerin gerektirdiği ölçüde sağlandığı şeklinde değerlendirilmelidir. Bir veri aktarımı yalnızca, 15. fıkradaki nedenler veya 1. fıkranın b ve c bentlerindeki sebepler ile reddedilebilir.

b) Amaç ve Kullanım

Verileri alan Taraf bu verileri, Protokolün 2. maddesinde belirtilen amaçla, "bilgisayar sistemleri ve verileriyle ilgili cezai suçlara ilişkin belirli cezai soruşturma veya kovuşturmalara ve bir cezai suçun elektronik biçimde kanıt toplanmasına ilişkin olarak ve bu Protokole Taraf olan Birinci Protokolün Tarafları arasında, Birinci Ek Protokol uyarınca oluşturulan cezai suçlara ilişkin belirli cezai soruşturma veya kovuşturmalarda olduğu şekilde" işleyecektir. Alınan veriler, işleme amacını aşan şekilde kullanılmamalı ve bunun için gerekli yasal önlemler alınmalıdır. Aksi bir durum bu maddeye aykırılık teşkil edecektir.

[264] A.g.e,. Art.223

c) Kalite ve Bütünlük

Maddenin 3. fıkrası Tarafların her birinin, kişisel verilerin doğru ve eksiksiz olarak tutulması ve işlenme amaçlarına göre işlenmesi için gerekli ve uygun olduğu kadar güncel olmasını sağlaması gerektiği hükmünü haizdir. Verilerin doğruluğunu, güncelliğini ve bütünlüğünü sağlamak bir ceza soruşturması veya kovuşturmasının aydınlatılması ile adaletin teminini sağlamak için çok önemlidir, sanık ve şüpheliler aleyhine sonuçlar yaratabilecek durumların oluşmasını engeller. Zira, bir ceza soruşturması ya da kovuşturmasında önemli nitelikteki bir verinin Tarafların bu maddedeki yükümlülüğünü yerine getirmemesi sonucu bozulması, o yargılamanın suçsuz kişiler aleyhine sonuçlanması şeklinde dahi sonuçlanabilir

d) Hassas Veriler

Hassas veri, doğrudan veya dolaylı olarak kişilerin ırkı, etnik kökeni, siyasi görüşleri, dini ve felsefi inançlarını, sağlığıyla ilgili bilgileri, cinsel yaşamını ve mahkumiyetleri gibi verileri ortaya çıkaran veriler,[265] diğer bir ifadeyle başkaları tarafından öğrenildiğinde bireyin ayrımcılığa uğramasına veya mağdur olmasına sebebiyet verebilecek veriler olarak tanımlanmaktadır.[266] Hassas nitelikte kişisel veriler çoğunlukla ceza soruşturma ve kovuşturmalarına konu olabilmektedir.

Bu tür verileri işleyen Taraf, verilerin kullanımından kaynaklanacak haksız nitelikte ve önyargıya sebep olabilecek risklere karşı koruma sağlamak için uygun güvenceler sağlamalıdır. Veri talebinde bulunulan Tarafın, talebi detaylı olarak incelemesi, talep konusu soruşturma ve kovuşturmanın aydınlatılması için önemli

[265] Cemil, Kaya. *Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve İşlenmesi*. Journal of Istanbul University Law Faculty 69, no. 1-2 (2011): 318.
[266] Koyuncu, Emel ve Mustafa Coşar. *Hastane Bilgi Sistemlerinin Yetkilendirme Düzeyli Güvenlik Değerlendirmesi,* Hitit Ekonomi ve Politika Dergisi, Mart 2022, Cilt:2, Sayı:1, çevrimiçi: www.cdn.hitit.edu.tr/hepdergi/files/67874_2203291127809.pdf, Erişim Tarihi: 10.05.2022.

olmayacak ve paylaşılması bireylerin ayrımcılığa uğrama riskine sebebiyet vereceği durumlarda bu tür hassas nitelikteki verilerden kaçınılması gerekecektir.

Taraf ülkelerin makamlarının veya o ülkelerde bulunan hizmet sağlayıcıların hassas nitelikteki verilere sahip, iş birliğini sağlayan makamları yoğun iş yükü altında her talep sonucunda ortaya çıkabilecek hassas nitelikteki kişisel verilerin ne şekilde bir sonuca ve mağduriyete sebep olabileceğini öngörmesi ve buna göre hareket edebilmesi ihtimali hayatın olağan akışında zordur. Bunun yanı sıra madde metninde yer alan "ilgili riskler açısından hassas kabul edilen biyometrik veriler" ifadesi tepki toplamıştır.[267]

e) Saklama Süreleri

Kişisel veriler, 14. maddenin 2. fıkrasında belirtilen amaçlar çerçevesinde işlenecektir. Burada belirtilen amaçlar dışında veri işlenmesi mevzuata aykırılık teşkil etmektedir. Bu fıkraya göre işlenmiş olan kişisel veriler yalnızca bu kapsamda gerekli ve uygun olduğu süre boyunca tutulacaktır. Saklama sebebi ve süresi sonlanmışsa veya verileri saklamak artık gerekmiyorsa bu veriler silinmeli veya anonim hale getirilmelidir. Bu yükümlülüğün yerine getirilmesi için Tarafların kendi iç hukukları çerçevesinde belirli saklama süreleri veya periyodik verilerin daha fazla saklanması ihtiyacının gözden geçirmesi gereklidir.

Verilerin silinmesi ve anonim hale getirilmesi ile ilgili ülkemizde 6698 sayılı Kişisel Verilerin Korunması Kanununa (KVKK) dayanılarak Kişisel Verilerin

[267] Israel, Tamir ve Rodriguez, Katitza. *On New Cross-Border Cybercrime Policing Protocol, a Call for Caution, Just Security.* 13.05.2022. https://www.justsecurity.org/81502/on-new-cross-border-cybercrime-policing-protocol-a-call-for-caution/, çevrimiçi, Erişim Tarihi: 11.06.2022. Bu husus 3.7.2. numaralı bölümde detaylandırılacaktır.

Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[268] yürürlüğe girmiştir. Yönetmeliğin 7. maddesinin 3. fıkrası ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi ile ilgili yapılan tüm işlemlerin kayıt altına alınacağı ve bu kayıtların en az üç yıl süreyle saklanacağı ifade edilmektedir. Yönetmeliğin 5. maddesinde kişisel veri saklama ve imha politikalarına ilişkin esaslar düzenlenmiş, veri sorumlularına oluşturdukları kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikası oluşturmak zorunluluğu yüklenmiştir. Verinin yok edilmesi için özel tekniklerin kullanılması gerekir, örneğin "degauss" yöntemi diskin mıknatıs özelliğini yok ederek verilerin uçmasını sağlanmaktadır. Buradaki son aşama ise veriyi barındıran aygıtın fiziksel olarak yok edilmesi amacıyla öğütülmesidir.[269]

f) Otomatikleştirilmiş Kararlar

Maddenin 6. fıkrası, otomatikleşmiş kararlar ile ilgili bir düzenleme getirmektedir ve kişisel verilerin yalnızca otomatik olarak işlenmesine dayanıldığı durumlarda bireylerin korunmasıyla ilgilidir. Makamlar tarafından kanıtların veya bilgilerin belirli bir ceza soruşturması veya kovuşturması amacıyla toplanacağı için, bir Taraf bu Protokol kapsamında başka bir Taraftan kişisel veri aldığında genellikle otomatik karar vermenin mümkün olmayacağı düşünülmektedir. Ancak, kişisel verilerin ilgili olduğu kişinin ilgili menfaatleri üzerinde önemli bir olumsuz etki yaratan otomatik karar verme, verilerin arandığı soruşturmada yer alıyorsa, yetkililerin bu hükme uyması gerektiği hüküm altına alınmıştır.[270] Buradaki önemli derecede olumsuz

[268] Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 30224 sayılı ve 28.10.2017 tarihli Resmi Gazete'de yayınlanmıştır.
[269] Dülger, Murat Volkan. *Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in Getirdikleri Ve Dikkat Edilmesi Gereken Hususlar (The Issues Brought To Be Considered By The Regulation On The Deletion, Destruction Or Anonymization Of Personal Data)*. Available at SSRN 3792237 (2021), s.5, çevrimiçi, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792237, Erişim Tarihi: 10.05.2022
[270] Protokole İlişkin Açıklayıcı Rapor, Art.243.

etki ifadesinin, kişilerin temel hak ve özgürlüklerine müdahale edici veya yarattığı olumsuzluğun geri dönüşünün oldukça zor olduğu durumlar olduğunu düşünmekteyiz.

g) Veri Güvenliği ve Güvenlik Hadiseleri

Maddenin 7. fıkrası uyarınca, kişisel verilerin korunması için her bir Taraf ülkenin gerekli altyapıları temin etmekle yükümlü olduğu ifade olunmaktadır, burada alınacak olan önlemler Taraf ülkelere bırakılmıştır. Bu önlemler; teknolojinin çeşitlenmesi ve bununla paralel olarak suçların da değişkenlik göstermesinden ötürü periyodik bir şekilde güncellenmesi, güvenlik altyapılarının sağlanması, personelin yeterli şekilde eğitilmesi, izinsiz erişimlerin önlenmesi için yeterli güvenlik kontrollerinin olması gibi hem teknolojik hem organizasyon hem de fiziki olarak alınacaktır.[271]

Bir kişi ya da Taraf ülkenin fiziksel olan ya da olmayan önemli bir zarar görme riski olduğu durumda, Taraf ülkelerin buna ilişkin olarak derhal önlem[272] alması gerekmektedir. Bu fıkradaki önemli bir zarar görme riski, maddenin 6. fıkrasında yer alan önemli tanımı ile benzer anlamı taşımaktadır. Kişinin, örneğin adres verisinin paylaşılması sebebiyle ayrımcı bir grup tarafından fiziksel şiddete maruz kalması ya da

[271] A.g.e., Art.246.

[272] "Önlemler özellikle, kayıp ihtimaline karşı (verilerin dosyalanması ve işlenmesi için standart prosedürler), kazara veya yetkisiz erişim (bilgisayara izinsiz girişlere karşı koruma, kağıt veya bilgisayar dosyalarına erişim için yetkilendirme veya kimlik doğrulama gereksinimleri), tesadüfi veya yetkisiz ifşa (tesadüfi veya yetkisiz ifşaları tespit etmek ve önlemek için teknolojik önlemler ve bu ifşaların sonuçlarını özetlemek için kurumsal önlemler) ve verilerin kazara veya başka bir şekilde yetkisiz olarak değiştirilmesi veya imha edilmesi (elektronik verilerin veya kağıt dosyaların yetkili personele girişinin veya değiştirilmesinin kısıtlanması, kayıt sistemlerinin kullanılması, saklama sürelerinin görüntülenmesi, bilgisayar veya kağıt dosya yedekleme sistemlerinin kurulması)" A.g.e., Art.247.,
"Bu gerekliliklerin özel koşullara uygun bir şekilde tam olarak karşılanması ilgili Tarafa bırakılmıştır. Taraflar, örneğin, kişisel verilerin doğası (hassasiyeti dahil), belirlenen riskler ve bir güvenlik olayı durumunda ilgili birey için olası olumsuz sonuçlar gibi faktörleri dikkate alan güvenlik önlemleri tasarlamaya ve uygulamaya teşvik edilir. Aynı zamanda Taraflar, veri güvenliği önlemlerinin tasarlanması ve uygulanmasına dahil olan kaynaklarla ilgili soruları dikkate alabilir. Taraflar, teknolojinin gelişimi ve risklerin değişen doğası göz önüne alındığında, bu tür önlemleri periyodik olarak gözden geçirmeye ve uygun olan durumlarda güncellemeye tabi tutmaya teşvik edilir." A.g.e., Art.248.

bazı bilgilerinin internette paylaşılması sebebiyle hakarete uğrayıp manevi olarak zarar görebilmesi örnek olarak verilebilir. Bu tür bir zarara ilişkin "önemli bir risk" varsa, verileri alan Tarafın zararın "olasılığını ve ölçeğini derhal değerlendirme" ve "bu zararı azaltmak için derhal uygun önlemi alma" yükümlülüğü vardır.[273]

Mevzubahis riskin tespiti ve ilgili güvenliğin temininin sağlanabilmesi için Taraf ülkelerin bunu tespit etmek ve önlemek için gerekli altyapıları ve teknolojileri bünyelerinde bulunduruyor olması gereklidir. Bu konuyla ilgili olayın gerekliliklerine göre makamlara veya bireylere bildirimde bulunmak gerekebilir. Kişisel verilerin yanlış olarak işlenmesi durumunda bireylere yapılacak bildirim ertelenebilir ya da hiç yapılmayabilir.

Fıkranın b bendi, istisnalar ve sınırlamalara tabi olarak, diğer Tarafın ve etkilenen bireylerin olayla ilgili olarak bilgilendirilmesi gereken koşulları da ortaya koymaktadır.[274] Bireylere veya diğer Tarafa ciddi fiziksel veya fiziksel olmayan zarar verme riskinin bulunduğu bir güvenlik olayı olması durumunda, verileri devreden makama veya II. Bölümün 2. Kısmının amaçları doğrultusunda tayin edilen makamlara bildirimde bulunulacaktır. Bununla birlikte, bildirimin daha fazla iletilmesine ilişkin uygun kısıtlamalar getirilebilir. Bildirimin yapılmasının, güvenlik olayından kaynaklanan cezai suçların soruşturulmasını tehlikeye atacağı durumlar dahil olmak üzere, ulusal güvenliği tehlikeye atabileceği durumlarda, bu bildirim yapılmayabilir veya ertelenebilir.[275]

[273] A.g.e., Art.249. Ayrıca diğer Tarafla ilgili olarak, ilgili zarar, özellikle paralel bir soruşturma üzerindeki potansiyel olumsuz etkiyi içerebilir.
[274] A.g.e., Art.251.
[275] A.g.e., Art.252.

h) Kayıtların Tutulması

Her bir Taraf ülke gerektiğinde bir kişisel veriye ne şekilde erişildiğini, bunun nasıl kullanıldığını ve açıklandığını gösterebilecek şekilde kayıtları tutacak veya başka uygun araçlara sahip olacaktır. Taraflar bu kayıtların tutulmasını sağlayacak teknik altyapıya ve teknolojik seviyeye sahip olması gereklidir.

i) Bir Taraf İçerisinde İleriye Dönük Paylaşım

Bu Protokol kapsamında alınan kişisel veriler, daha sonra aynı Tarafın başka bir makamına istisna olmadıkça 14. maddenin 9. fıkrası uyarınca işlenmelidir. Federal yapıda olan bir Taraf ülke, burada belirtilen koşullara uygun olarak, bu Protokolün 17. maddesi kapsamındaki yükümlülüklerine çekince koyması durumunda, 9. fıkranın a bendine bir istisna sağlamaktadır.[276]

Bu istisna "Federal Devletlerin merkezi ve bölgesel otoriteler arasındaki karakteristik yetki dağılımının bir sonucu olarak karşılaşabilecekleri zorlukları" barındırmaktadır. Bu nedenle, 9. fıkranın b bendi, bir Tarafın 17. madde uyarınca çekince koyduğu durumlarda; Tarafın, alıcı makamların verilerin bir düzeyde korunmasını sağlayarak verileri, bu madde ile sağlananla karşılaştırılabilir düzeyde, etkin bir şekilde korumaya devam etmesi için önlemleri almış olması koşuluyla, bu Protokol kapsamında başlangıçta alınan kişisel verilerin aktarımını, kurucu Devletlerine veya diğer benzer bölgesel kuruluşlara yine de sağlayabilir. Bir Tarafın "alıcı makamların bu madde ile sağlananla karşılaştırılabilir bir veri koruma düzeyi sağlayarak verileri etkin bir şekilde korumaya devam etmesi için yürürlükte olan önlemleri" almaması, bu şartın yerine getirilmemesinin ciddiyetine, gerekçesine ve koşullarına bağlı olarak, 14. maddenin 15. fıkrası kapsamında önemli veya sistematik

[276] A.g.e., Art.260.

bir ihlal oluşturabilir.[277] Protokolün 14. maddesi, uluslararası aktarımlar için veri koruma kuralları kapsamında veri aktarımlarını reddetme hakkını sınırlandırmaktadır.[278]

j) Başka Bir Ülkeye veya Uluslararası Kuruluşa İleriye Dönük Aktarım

Maddenin 10. fıkrası uyarınca, verinin aktarıldığı Taraf ülke, kişisel verileri başka bir ülkeye veya uluslararası kuruluşa, yalnızca veriyi aktaran makamın veya diğer Taraflardaki sağlayıcılar ve kuruluşlarla doğrudan iş birliğini geliştiren usullerin düzenlendiği II. Bölümün 2. Kısmının amaçları doğrultusunda, b bendi uyarınca atanan makam veya makamların ön izni ile aktarabilir. Fıkranın b bendi uyarınca, Taraflardan her biri, bu Protokolün imzalanması sırasında veya onay, kabul veya uygun bulma belgesini tevdi ederken, Avrupa Konseyi Genel Sekreterine, II. Bölümün 2. Kısmının amaçları doğrultusunda yetki verecek makam veya makamlarını bildirecektir, verilen bilgiler daha sonra değiştirilebilir.

İleriye dönük bir aktarım için yetki alınması ile ilgili olarak; özel olarak tanımlanmış kişisel verilerin belirli bir üçüncü ülkeye veya uluslararası kuruluşa aktarılmasında yetkilendirme için verinin transfer edildiği Tarafın yetkililerinden, veriyi aktaran Tarafın yetkililerine bireyselleştirilmiş bir talep gönderilmesini gerektirebilir. Ancak, 10. fıkranın a bendi, Tarafların ileriye dönük transferler için, yazılı anlaşma veya diğer düzenlemeler öngörülmesi gibi, önceden kurallar koymasını engellemez. Ayrıca, bir Tarafın verilerin alıcısı tarafından kullanımına ilişkin, veri aktaran Tarafın soruşturmasına halel gelmemesi için alıcı Tarafın kişisel verileri ne ölçüde kullanabileceği veya yayabileceği konusunda sınırlamalar koymak gibi başka koşullar koyma yetkisine engel getirilmemektedir.[279]

[277] A.g.e., Art.260.
[278] 6. maddenin 2. fıkrasındaki talep reddi ile bağlantılı olarak, A.g.e., Art.82.
[279] A.g.e., Art.264.

Bu tür bir koruyucu önlem, ceza kanunlarının uygulanması bağlamında yabancı ortaklara yardımcı olmak için, örneğin, karşılıklı yardım anlaşmaları veya kolluk kuvvetleri arasındaki iş birliği uyarınca, yapılan transferlerin yaygın bir koşuludur. Bu yaklaşım, bu Protokol kapsamında aktarılan kişisel verilerin korunmasının bir aracı olarak da bu bende taşınmıştır.[280] 10. fıkra kapsamında bir aktarıma izin verilip verilmeyeceğini belirlerken, aktaran veya tayin edilen yetkili makamların; cezai suçun ciddiyeti, verilerin orijinal olarak aktarılma amacı, orijinal aktarımla ilgili geçerli tüm koşulları ve üçüncü ülke veya uluslararası kuruluşun kişisel verilerin uygun düzeyde korunmasını sağlayıp sağlamadığı dahil olmak üzere, ilgili tüm faktörleri dikkate alması teşvik edilir.[281]

k) Şeffaflık ve Bildirim

Maddenin 11. fıkrasının a bendiyle, Taraflara şeffaflık ve bildirim gereklilikleri getirilmektedir. Şeffaflık gereği yapılacak bildirimler, kişisel verileri toplanan bireyleri verilerinin nasıl işleneceği; işlemenin yasal dayanağı ve amaçları, saklama süresi, verilerin ifşa edildiği alıcılar ile erişim, düzenleme ve uygun tazmin konularında aydınlatmaktadır. Bu bildirimin ne şekilde yapacağı hususu sınırlandırılmamış, bireylere kişisel bildirim yapılabileceği gibi genel bildirimlerin yayınlanması şeklinde de olabileceği ifade olunmuştur. Protokole ilişkin açıklayıcı raporda belirtildiği üzere, burada amaçlanan husus bildirimin kolaylıkla erişilebilir ve anlaşılabilir olmasıdır ve bu bildirimin örneğin hükümete ait bir internet sitesinde yayınlanması gibi kamuya duyurulması yoluyla dahi yapılabileceği belirtilmiştir.[282] Söz konusu paylaşılan verilerin, hassas nitelikte kişisel veriler olması durumunda böylesi kamuya açık suretle

[280] A.g.e., Art.262.
[281] A.g.e., Art.265.
[282] A.g.e., Art.267.

yapılmış bir bildirimin, kişilerin mahremiyetine karşı bir ihlal teşkil edebileceği riski oluşturduğunu düşünmekteyiz.

Fıkranın b bendi uyarınca bireye kişisel bildirim yapıldığında, bildirim ve şeffaflık şartı verinin hassasiyetine bağlı olarak ve kişilerin meşru menfaatleri göz önünde bulundurularak makul kısıtlamalara tabi olabilir. Fıkranın son bendinde, aktaran Tarafın, maddenin 12. fıkrasının a bendinin i harfli alt bendinde belirtilen kısıtlamanın uygulandığı durumlarda, alıcı Taraf verilerin verilmesinin gizli tutulmasını talep etmişse, kişisel bildirim yapılmayacaktır. Fıkranın b bendinde belirtilen kısıtlamalar karşısında, ceza soruşturma ve kovuşturmalarında adaletinde gizliliğe duyulan ihtiyacı karşılayacak bir dengeleme sağladığı düşünülmektedir.[283]

l) Erişim ve Düzeltme

Taraflardan her biri, Protokol kapsamında kişisel verileri alınan herhangi bir bireyin, kendi iç yasal çerçevesinde oluşturulan süreçlere uygun olarak ve gereksiz gecikme olmaksızın 12. fıkrada yer alan hususları talep ve elde etme hakkına sahip olmasını sağlayacaktır. Burada belirtilen, "yerel yasal çerçevesinde oluşturulan süreçlere uygun olarak" ifadesi, erişim ve düzeltmenin ne şekilde talep ve elde edilebileceğine dair yürürlükteki mevzuat ve yasal uygulamaları dayanak olarak, diğer bir ifadeyle somut bir şekilde atıf yaparak kullanma şartı koştuğunu düşünmekteyiz. Zira, kişisel verinin işlenmesinin yasal dayanağının temin edilmesi, bireylere kişisel verilerin yürürlükte olan yasalara uygun şekilde işlenip işlenmediğini değerlendirmede ışık tutacaktır. Böylece hem şeffaflık temin edilirken, diğer yandan kişilerin bilgiye edinme özgürlüğü ve mahremiyetlerinin temini mümkün olacaktır.

[283] A.g.e., Art.269.

Belirtilen talep ve elde etme hakkı, belirli durumlarda bir Tarafın yerel yasal çerçevesi kapsamında yer alan orantılı kısıtlamalara tabi olabilir. Örneğin; başka bireylerin meşru menfaatleri, hak ve özgürlüklerini, ulusal güvenliği ve genel kamu yararı gibi amaçları korumak gibi. Burada belirtilen "orantılı kısıtlamalar" yerel yasalara göre belirlenmekle birlikte, ETS 5 numaralı İnsan Haklarının ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşmesi ile CETS 223 numaralı Kişisel Verilerin Otomatik İşlenmesine İlişkin Bireylerin Korunmasına İlişkin Sözleşmede Değişiklik Yapan Protokolden kaynaklı orantılılık ilkesi, bu Protokol bakımından da uygulanacak ve bir referans olarak kabul edilebilecektir. Orantılı kısıtlamalar bireylerin hak ve özgürlüklerini, genel kamu yararını ve ulusal güvenliği koruyacak şekilde uygulanmalıdır.[284] Orantılık ilkesi, temel hak ve özgürlüklerin korunmasında çok temel bir öneme sahiptir.

Bireyin kişisel verilerinin yanlış olması veya uygunsuz şekilde işlenmesi durumunda; bireylerin uygun ve makul şekilde düzeltme, ekleme, silme veya anonimleştirme, işlemenin kısıtlanması veya engelleme şeklinde düzeltme hakkını talep ve elde etme imkânına sahip olmasını sağlanacaktır. Burada belirtilen hakkın amacına aykırı ve kötü niyetle kullanılıp kullanılmadığı ile "uygun ve makul" olma değerlendirmesi Taraflara bırakılmıştır. Bu uygulamanın birimlere yük getirme ihtimali mevcuttur. Bu ihtimalin karşısında maddenin b bendi ile erişim ve düzeltme talebinin makul bir masraf ile sınırlı olacağı hükmü getirilmiştir, madde metninden anlaşıldığı üzere Taraflar, erişim ve düzeltme talepleri karşısında makul masrafın aşıldığı noktada ücret talep edebilmelidir.

Fıkranın son bendine göre, a bendi uyarınca erişim veya düzeltme talebi reddedilir veya kısıtlanırsa Taraflar, bireylere gereksiz gecikme olmaksızın, elektronik

[284] A.g.e. Art.272.

ve yazılı biçimde bu uygulama konusunda ve mevcut tazmin imkanları hakkında bilgilendirici bir yanıt sunmalıdır.

m) Gözetim

14. maddenin 14. fıkrası "Taraflardan her biri, bu maddede belirtilen tedbirlerle ilgili olarak tek başına veya toplu olarak, bağımsız ve etkin gözetim işlevleri ve yetkilerini kullanan bir veya daha fazla kamu makamına sahip olacaktır. Tek başına veya toplu olarak hareket eden bu makamların görev ve yetkileri, soruşturma yetkilerini, şikâyetler üzerine harekete geçme yetkisini ve düzeltici önlem alma ehliyetini içerecektir." hükmünü içermektedir.

Bu düzenleme bizlere, Protokole Taraf olan ülkelerin anayasal ve idari alandaki yapılarındaki farklılıklarının bilincinde olunduğunu göstermektedir. Maddede belirtilen makamların sayısında Taraflara esneklik tanındığı ve bu makamların görev ve yetkisinin "soruşturma yetkilerini, şikayetler üzerine harekete geçme yetkisini ve düzeltici önlem almak" olduğu anlaşılmaktadır. Taraf ülkelerin etkin gözetimi sağlayabilmeleri, düzeltici önlemler alabilmeleri için gerekli teknik altyapıların sağlanmış ve görevlilerin eğitimli olması gerekmektedir, diğer bir ifadeyle Taraf ülkelerin uyumluluğunu sağlamış olması gerekmektedir.

n) Müzakere ve Askıya Alma

Maddenin son fıkrası, Protokol kapsamındaki kişisel verilerin başka bir Tarafa aktarımını ne zaman askıya alabileceğini düzenler. Buna göre, bir Taraf, diğer Tarafın 14. maddenin şartlarını sistematik veya esaslı bir şekilde ihlal ettiğine veya önemli bir ihlalin yakın olduğuna dair önemli kanıtlara sahip olduğu durumlarda, kişisel verilerin Taraf ülkeye aktarılmasını askıya alabilme imkânı tanımaktadır.

Bu Protokolün amaçları ışığında, böylesi askıya alma uygulamaları yalnızca katı koşullar altında ve burada açıklanan belirli prosedürlere uygun şekilde gerçekleştirilmelidir. Zira bu maddenin amacı, bir Taraf içinde ileriye dönük veri paylaşımı ve veri aktarımları da dahil olmak üzere, kişisel verilerin korunması amacıyla uygun güvenceler sağlamaktır.[285]

Şartların sistematik veya esaslı bir şekilde ihlal edildiği veya önemli bir ihlalin gerçekleşeceği ile ilgili olarak, veri aktarması istenen Tarafın bu duruma ilişkin önemli kanıtlara sahip olması gereklidir. Ancak bu durumda verinin başka bir Tarafa aktarılması askıya alınabilir. Yakın ihlâl ifadesi dolayısıyla, Tarafların bazı durumlarda somut bir şekilde ihlâli delillendirmesi gerekli olmadığını düşünmekteyiz. Ancak burada yalnızca basit bir şüphe ya da keyfi sebeplerle bu aktarımın askıya alınamayacağı ve son çare olarak başvurulacağı görüşündeyiz, aksi durum Protokolün amaçları ile çelişki gösterecektir. Tarafların makul şekilde, destekleyici nitelikte kanıtlar sunması beklenebilir.

Bunların yanında, veri paylaşımının geçici olarak askıya alınmasıyla ilgili olarak "bir Taraf, gerçek bir kişinin hayatı veya güvenliği için önemli ve yakın bir risk veya önemli bir itibar veya parasal zarar teşkil eden sistematik veya esaslı bir ihlal durumunda, aktarımları geçici olarak askıya alabilir; bu durumda bildirimde bulunacak ve hemen ardından diğer Tarafla istişarelere başlamayacaktır."

Burada belirtilen durumlar Protokolün 3. maddesinde ifade edilen "acil durum" tanımıyla benzerlik göstermektedir. Karşı Tarafa bildirimde bulunulmadan ve makul istişare sürecine girmeden geçici olarak askıya alma işlemi yapılamayacaktır. Tarafların makul sürede istişareye girmesi gerektiği ve sonrasında bu işlemin yapılacağı ile ilgili düzenleme, Tarafların keyfi veya hukuka aykırı şekilde hak kaybına

[285] A.g.e. Art.281.

sebep olabilecek, ceza soruşturması ve kovuşturması sonucunda temin edilebilecek olan adaleti sağlamaya engel olabilecek uygulamaları önleyebilecektir. Taraflar durumu açıklığa kavuşturmak ve söz konusu endişeleri gidermek için imkâna sahip olabilecektir. Müzakerelerin bir çözümle sonuçlanmaması durumunda ise, veri paylaşımını askıya alma işlemi için diğer Tarafın belirtilen koşullara aykırılık olduğuna dair önemli kanıtların bulunması durumunda, Taraflara karşılıklı olarak askıya alma imkânı tanınmaktadır. Askıya alınmadan önce aktarılan herhangi bir kişisel veri, bu Protokol uyarınca muamele görmeye devam edecektir.

Tarafların, bu fıkra kapsamındaki herhangi bir askıya alma uygulaması hakkında, II. Bölümün 2. Kısmı kapsamında talep veya emir yönlendirilebilecek hizmet sağlayıcılar ve kuruluşlar, kamuya açıklama veya resmi olarak bilgilendirme yapmaya teşvik edilir. Böylesi bir uygulama, 14. maddeyi maddi veya sistematik olarak ihlâl eden bir Tarafa kişisel verilerin aktarımını etkin bir şekilde askıya almak için önemli olabilir ve aynı zamanda hizmet sağlayıcıların ve kuruluşların bir Tarafın bu askıya alma hükmüne tabi olduğuna dair yanlış inanca dayanarak bu Protokol kapsamında bilgi veya kanıt transferini kısıtlamalarının önüne geçilebilir.[286]

2.5.4. Son Hükümler

Protokolün dördüncü ve son hükümler başlıklı bölümünde yer alan maddelerden önemli bulduğumuz düzenlemeler çalışmanın bu başlığı altında incelenecektir.

[286] A.g.e. Art.286.

2.5.4.1. İmza ve Yürürlüğe Giriş

Sözleşmenin 36. maddesinin 3. fıkrasında, Sözleşmenin yürürlüğe girmesi için imzacı beş Taraf ülkeden en az üçünün Avrupa Konseyi üyesi olması gerektiğini belirtilmektedir. Buna karşın Protokolün 16. maddesinin 3. fıkrası "İşbu Protokol, Sözleşmeye Taraf olan beş ülkenin, bu Protokol ile bağlı olma rızalarını beyan ettikleri tarihten sonraki üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girecektir." hükmünü amirdir. Katılım için herhangi bir prosedür öngörülmemektedir, yalnızca bu Protokolü imzalamak ve taraf olmak isteyen ülkelerin öncelikle Sözleşmeye Taraf olması gerekmektedir. Bu Protokolün Sözleşmeye bir ek olarak getirildiği ve Sözleşmenin en az beş Tarafının bağlanma rızalarını ifade ettiğinde bu Protokolü uygulama konusunda aynı hakka sahip olmaları gerektiği göz önüne alındığından dolayı, Sözleşmedeki gibi bir gereklilik burada yer almamaktadır.[287]

Sözleşmenin 36. maddesinin 4. fıkrasındaki yaklaşım ile aynı şekilde Protokol de 16. maddenin 1. ve 2. fıkraları hükümleri uyarınca Tarafların bu Protokole bağlı kalmaya muvafakatlerini beyan ettiği tarihten sonraki üç aylık sürenin sona ermesini takip eden ayın ilk günü yürürlüğe girecektir. Protokol, 12 Mayıs 2022 tarihinde imzaya açılmıştır.[288] Halihazırda Protokolü imzalayan 24 ülke bulunmaktadır. Ancak henüz onaylama (ratification) işlemini gerçekleştiren bir ülke bulunmamaktadır.[289]

---

[287] A.g.e., Art.295

[288] Enhanced Cooperation and Disclosure of Electronic Evidence, COE INT., çevrimiçi, https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention#:~:text=Following%20almost%20four%20years%20of,the%20framework%20of%20an%20international, Erişim Tarihi: 05.09.2022.

[289] Chart of signatures and ratifications of Treaty 224, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Status as of 12/06/2022, çevrimiçi, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, Erişim Tarihi: 05.09.2022.

2.5.4.2. Çekince ve Beyanlar

a) Tanım

Bu madde detaylandırılmadan önce, çekince ve beyan imkânının ne şekilde tanımlandığını ifade etmek yerinde olacaktır. Öğretide çeşitli tanımları olsa da bu alanda yol gösterici olarak kabul edilen 1969 tarihli Viyana Sözleşmesi'nde tanımlandığı ve bugüne kadar kabul edildiği üzere çekince; bir devletin bir anlaşmayı imzalarken, onaylarken, kabul ederken, uygun bulurken veya ona katılırken, diğer bir ifadeyle anlaşma ile bağlanma rızası gösterirken, bazı hükümlerin kendisi bakımından herhangi bir hukuki etkisi olmayacağı veya bu hükümleri değiştirerek uygulayacağı yönünde yaptığı tek taraflı bir beyandır.[290] Çekincelerin temel amacı, uluslararası bir anlaşmanın çeşitli hükümlerine çekince ileri süren taraf ülke bakımından o hükümlerle getirilen yükümlülüklerin bir bağlayıcılığı bulunmaması, ilgili hükümlerin hukuki etkilerini bertaraf etmesi veya değiştirmesidir.[291]

Bu noktada açıklayıcı ve yorumlayıcı beyanlara değinmekte de yarar vardır. Açıklayıcı beyan, bir anlaşmaya ya da anlaşma kapsamındaki bir konuya ilişkin olarak bir devletin ya da bir uluslararası örgütün görüşlerinin yer aldığı tek taraflı bildirileri ifade etmektedir. Yorumlayıcı beyanlar, anlaşmanın belirli bir hükmünü veya bir terimini nasıl anladığını açıklayan ve bu devletin anlaşmayı bu anlayış ile akdettiğini belirten bir bildiridir, çekince olarak kabul edilmemektedir ancak uygulamada karıştırıldığı gözlemlenmektedir.[292] Yapılmış olan beyan ile anlaşmayla kurulan

---

[290] Akkutay, Berat Lale. 1*982 Birleşmiş Milletler Deniz Hukuku Sözleşmesi Çerçevesinde Çekinceler ve İhtiyari İstisnalar.* Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni 31 (2012), s.4, (çevrimiçi), https://dergipark.org.tr/tr/download/article-file/410903, Erişim Tarihi: 27.08.2022.
[291] Akkutay, s.7.
[292] Özman, Mehmet Aydoğan. *Milletlerarası Anlaşmalarda Çekinceler: (Ihtirazi Kayıtlar).* Ankara Üniversitesi Hukuk Fakültesi Yayınları, No:259, 1970, Sevinç Matbaası, Ankara, s.18. https://0-search-ebscohost-com.opac.bilgi.edu.tr/login.aspx?direct=true&db=nlebk&AN=703079&site=eds-live, çevrimiçi, Erişim Tarihi: 27.08.2022.

düzenden farklı bir düzen kurulduğu takdirde bunu bir çekince olarak kabul etmek gerekmektedir.[293]

b) Protokolde Tanınan Çekince ve Beyan İmkânları

Protokolün 19. maddesi uyarınca, çekincede veya beyanda bulunma imkânı yalnızca belirli maddelerin belirli fıkraları için Taraf ülkelere tanınmıştır. Sözleşmede olduğu gibi bu Protokoldeki çekinceler, Protokolde belirtilen yükümlülüklerin yasal etkisinin geçerliliğinden, çekince imkanından faydalanan Tarafları muaf tutar veya yükümlülüklerinin yasal etkisinin geçerliliğini değiştir.[294]

Sözleşmenin küresel erişimi ve bu Protokolün de aynı düzeyde üyelik elde etme amacı göz önüne alındığında, bu tür çekinceler Sözleşme Taraflarının bu Protokole kendi iç hukukları, temel yasal ilkeler veya politik duruşları ile uyumlu belirli yaklaşımları ve kavramları sürdürmelerine izin vererek taraf olmalarına imkân sağlamaktadır.[295] Bu Protokolün Taraflarca yeknesak bir şekilde uygulanmasını sağlayabilmek için çekince olanakları sınırlandırılmış ve sayılanlar dışında başka bir çekincede bulunmak imkânı sunulmamıştır.[296]

19. madde ayrıca Taraflara beyanda bulunma imkânı da tanımaktadır. Sözleşmeyle benzer bir şekilde, Protokoldeki beyanlar yoluyla Tarafların hükümlerin kapsamını değiştiren belirli ek usulleri uygulamalarına izin verilmektedir. Bu tür ek usuller, Sözleşmenin küresel erişimi ve bu Protokole eşit erişimi hedefleyen belirli kavramsal, yasal veya pratik farklılıkları barındırmayı amaçlamaktadır.[297] Tarafların her türlü beyan, bildirim, tebligatı ve tayin edilen makamları Avrupa Konseyi Genel

[293] Özman, s.19.
[294] Protokole İlişkin Açıklayıcı Rapor, Art.311.
[295] A.g.e., Art.309.
[296] A.g.e., Art.310.
[297] A.g.e., Art.312.

Sekreteri'ne yazılı olarak bildirmeleri, güncel bilgileri temin etmeleri kayıt için sağladıkları ayrıntıların her zaman doğru olmasını sağlamaları gerekmektedir.

Madde 19 ile getirilen imkanlar iki genel kategoriye ayrılmaktadır. İlk olarak, belirli yetkilerin veya tedbirlerin belirli makamlar aracılığıyla uygulanması ya da belirli kanallardan iletilen iş birliği talepleri doğrultusunda iş birliğinin sağlanması yönündeki beyanlardır.[298] İkinci olarak, Tarafların iç hukuka uyum sağlamak veya birimlerine aşırı iş yükü yüklemekten kaçınmak için belirli iş birliği önlemlerinde ayrı veya ek usul süreçlerini talep etmesine izin veren beyanlardır.[299] Bu kategoriler aşağıda detaylandırılacaktır.

İmza sırasında veya onay, kabul, uygun bulma veya katılma belgesini tevdi ederken öngörülen çekincelerden yararlanıldığı veya beyanda bulunulduğu ifade edilebilir. Bu maddenin 1. ve 2. fıkralarında sıralananlar, bir Tarafın imzası sırasında veya onay, kabul veya tasvip belgesini tevdi ederken yapılmalıdır, buna karşılık, 3. fıkrada listelenenler herhangi bir zamanda yapılabilir.[300]

Sözleşmenin 43. maddesiyle paralel bir şekilde Protokolün 20. maddesinde de herhangi bir süre sınırlaması getirmeksizin koşullar izin verir vermez, Tarafların 19. maddenin 1. fıkrası uyarınca koyduğu çekincelerini geri çekme imkânı bulunmaktadır. Zaman içinde Tarafların Protokolün yeksenak bir şekilde uygulamasını teşvik etmek için mümkün olduğu kadar çok çekincesini kaldırabilecekleri umulmaktadır.[301] Ancak 19. maddenin 2. fıkrasında belirtilen çekinceler ve 3. fıkradaki beyanlar için bu şekilde bir düzenleme Protokolde yer almamaktadır. Bu sebeple 2. ve 3. fıkralarda yer alan bildirimlerin geri çekilemeyeceğini veya düzeltilemeyeceğini anlamaktayız.

[298] A.g.e., Art.313.
[299] A.g.e., Art.314.
[300] A.g.e., Art.315.
[301] A.g.e., Art.288.

b.a. Çekince İmkânları

19. maddenin 1. fıkrasında belirtilen, çekinceden yararlanılması ve çekincelerin geri çekilmesi mümkün olan hükümler aşağıda yer almaktadır:

- Abone bilgilerinin ifşasını düzenleyen 7. maddenin, 9. fıkrasının a ve b bentleri,
- Abone bilgilerinin ve trafik verilerinin hızlandırılmış üretimi için başka bir Taraftan gelen emirleri yürürlüğe koyma hususunu düzenleyen 8. maddenin, 13. fıkrası,
- Federal hükmün düzenlendiği 17. madde.

19. maddenin 2. fıkrasında belirtilen, çekinceden yararlanılması mümkün olan hükümler aşağıda yer almaktadır:

- Abone bilgilerinin ifşasını düzenleyen 7. maddenin 2. fıkrasının b bendi,
- Taraftan gelen emirleri yürürlüğe koyma hususunu düzenleyen 8. maddenin, 11. fıkrası,
- Saklanan bilgisayar verilerinin acil bir durumda hızlandırılmış ifşasının düzenlendiği 9. maddenin 1. fıkrasının b bendi ile 5. fıkrası,
- Acil karşılıklı yardım hakkındaki 10. maddenin 9. fıkrası,
- Müşterek soruşturma ekipleri ve müşterek soruşturmalar hakkındaki 12. maddenin 3. fıkrası,
- Ülkesel uygulama ile ilgili olarak 18. maddenin 2. fıkrası.

b.b. Beyan, Bildirim veya Tebligat İmkânları

19. maddenin son fıkrasında belirtilen beyan, bildirim veya tebligat yapılması mümkün olan hükümler aşağıda yer almaktadır;

- Abone bilgilerinin ifşasını düzenleyen 7. maddenin 5. fıkrasının a ve e bentleri

- Abone bilgilerinin ve trafik verilerinin hızlandırılmış üretimi için başka bir Taraftan gelen emirleri yürürlüğe koyma hususunu düzenleyen 8. maddenin 4. fıkrası ile 10. fıkrasının a ve b bentleri,
- Kişisel verilerin korunması ile ilgili 14. maddenin 7. fıkrasının c bendi ile 10. fıkrasının b bendi,
- Federal hükmün düzenlendiği 17. maddenin 2. fıkrasında öngörülen hususlardır.

c) Çekince ve Beyan İmkânlarının Kategorisi

Yukarıda ifade edilen beyan kategorilerinden birincisi olan, belirli yetkilerin veya tedbirlerin belirli makamlar aracılığıyla uygulanması ya da belirli kanallardan iletilen iş birliği talepleri doğrultusunda iş birliğinin sağlanması yönündeki beyanlar şu şekildedir; 10. maddenin 9. fıkrası için geçerli olan taleplerin merkezi makama ek olarak makamlara da gönderilebileceğine dair bir beyana izin verilmesi, 12. maddenin 3. fıkrasında merkezi makamın, müşterek soruşturma anlaşmasının imzacısı olması veya başka bir şekilde bu anlaşmada aynı fikirde olması gerektiği ile 8. maddenin 11. fıkrasında bir beyanda bulunan Tarafın, diğer Tarafların bu madde kapsamındaki taleplerinin kendi merkezi makamları veya karşılıklı olarak belirlenen diğer makamlar tarafından iletilmesini talep edebilmesidir.[302]

Belirtilen bir diğer beyan kategorisi olan Tarafların iç hukuka uyum sağlamak veya birimlerine aşırı iş yükü yüklemekten kaçınmak için belirli iş birliği önlemlerinde ayrı veya ek usul süreçlerini talep etmesine izin veren beyanlar; 7. maddenin 8. fıkrası ve 9. maddenin 1. fıkrasının b bendi uyarınca, bir Tarafın diğer Taraflardan abone bilgileriyle ilgili olarak belirli usule ilişkin adımlar atmasını talep eden beyanlarda bulunmasına izin vermesidir. Bir diğeri 7. maddenin 2. fıkrasının b bendi ile 5.

[302] A.g.e., Art.313.

fıkrasının a bendi, 8. maddenin 4. fıkrası ve 9. maddenin 5. fıkrasında, ek güvenceler sağlamak veya iç hukuka uymak için ek usule ilişkin adımlar talep etmesine izin verilmesidir.[303]

Beyanların etkilerinin karşılıklı olması amaçlanmamıştır. Örneğin, bir Taraf 10. maddenin 9. fıkrası uyarınca, bu madde kapsamındaki taleplerin merkezi makamına ek olarak başka makamlara gönderilebileceğine dair bir beyanda bulunursa, diğer Taraflar taleplerini, beyan eden Tarafın ek makamlarına iletebilir. Ancak beyanda bulunan Taraf, diğer Tarafların kendileri de böyle bir beyanda bulunmadıkça, talepleri yalnızca diğer Tarafların merkezi makamlarına iletebilir.[304]

2.5.4.2.1. Çekince ve Beyan İmkânı Tanınan Maddelerin Detaylandırılması

Tekrar ifade etmek isteriz ki, Protokolün 20. maddesi uyarınca, yalnızca 19. maddenin 1. fıkrasında yer alan, 7. maddedeki abone bilgilerinin ifşası ile 8. maddedeki abone bilgilerinin ve trafik verilerinin hızlandırılmış üretimi için başka bir Taraftan gelen emirleri yürürlüğe koymak ile 17. maddedeki federal hüküm başlıklı maddelere ilişkin koyulan çekincelerin Taraflarca geri çekilme imkânı bulunmaktadır. 19. maddenin 2. ve 3. fıkralarında belirtilen çekinceler ve beyanlara dair böyle bir düzenleme Protokolde yer almamaktadır. Bu sebeple 19. maddenin 2. ve 3. fıkralarında yer alan bildirimlerin geri çekilemeyeceğini veya düzeltilemeyeceğini anlamaktayız. Maddeler için ayrı ayrı tanınan çekince, beyan, bildirim ve tebligat imkânları aşağıda ilgili başlıklar altında bir arada ve sırasıyla açıklanacaktır.

[303] A.g.e., Art.314.
[304] A.g.e., Art.314.

a) Abone Bilgilerinin İfşası Hakkındaki Çekince ve Beyan İmkânları (Madde 7)

Tekrar ifade etmek isteriz abone bilgileri; bir hizmet sağlayıcı tarafından tutulan, trafik veya içerik verileri dışındaki hizmetlerinin aboneleriyle ilgili olarak bilgisayar verileri veya diğer herhangi bir biçimde yer alan her türlü bilgi ile kullanılan iletişim hizmetinin türü, buna göre alınan teknik hükümler ve hizmet süresi, abonenin kimliği, IP[305], posta veya coğrafi adresi, telefonu ve hizmet sözleşmesi veya düzenlemesi temelinde mevcut olan diğer erişim numaraları, fatura ve ödeme bilgileri ile hizmet sözleşmesi veya düzenlemesi temelinde mevcut olan iletişim ekipmanı kurulumunun sahasındaki diğer bilgileri ifade etmektedir.[306] Protokolün 7. maddesi Taraf ülkelerin belirli, depolanmış söz konusu hizmet sağlayıcının mülkiyetinde veya kontrolünde olan abone bilgilerinin ifşası için başka bir Tarafın ülkesindeki bir hizmet sağlayıcısına doğrudan sunulmak üzere bir emir verme yetkisini düzenlemektedir.

a.a. Protokolün 19. maddesinin 1. fıkrasında belirtilen çekince imkânı

Protokolün 19. maddesinin 1. fıkrası uyarınca Taraflar, 7. maddenin 9. fıkrasının a ve b fıkralarında öngörülen çekincelerden yararlandığını beyan edebilir, başka çekincede bulunulamaz. Burada öngörülen çekinceler; a bendi doğrultusunda Tarafların bu maddeyi uygulamama hakkını saklı tutabilmesi ile b bendi doğrultusunda bu madde kapsamında belirli erişim numaralarının ifşası Tarafların iç hukuk

[305] Kişinin IP adresi, hangi web sitelerini ziyaret ettiği ve kimlerle iletişim kurduğu gibi bilgilerin edinilmesi, kolluk kuvvetlerince kişinin günlük alışkanlıklarını ayrıntılı bir şekilde analiz edilerek, kişinin profilini oluşturmak ve iletişimlerin içeriğiyle ilgili ipuçları sağlamak için kullanılabilir. Bu durum anonim kimlikleri ifşa ederken zayıf korumaların sonuçları çok zarar verici olabilir. İnsanların faaliyetleriyle bağlantılı kimliklerini açığa çıkarmanın son derece hassas olabileceği göz ardı edildiği, abone bilgilerinin trafik verilerini ortaya çıkarabileceğini ve hatta iletişim içeriği hakkında çıkarımlara izin verebileceği gözden kaçırıldığı ifade edilmektedir.

[306] A.g.e., Art.93.

sistemlerinin temel ilkelerine aykırı olacaksa, bu maddeyi bu numaralara uygulamama hakkını saklı tutabilmesidir.

Protokole ilişkin açıklayıcı raporda ifade edildiği üzere, 9. fıkranın a bendi uyarınca bu maddeyi uygulamama hakkını saklı tutan Tarafların, artık bu maddenin 2. fıkrasında belirtilen, abone verilerinin ifşası için gerekli olabilecek yasal ve diğer önlemleri alma zorunluluğu kalmamaktadır. Bunun yanı sıra, eğer bir Taraf ülke 7. maddeyi uygulamama hakkını saklı tutarsa, diğer Taraf ülkedeki bir hizmet sağlayıcıya doğrudan sunulmak üzere abone bilgilerinin ifşasını[307] artık talep edemeyecektir.[308]

Bir hizmetin abonesini tanımlamak amacıyla ihtiyaç duyulan bilgiler, bir hesap oluşturulduğunda kullanılan IP adresi, en son oturum açma IP adresi veya belirli bir zamanda kullanılan oturum açma IP adresleri gibi, belirli IP adresi bilgilerini içerebilir. Bu tür bilgiler bazı Taraflarca, bir iletişimin iletilmesiyle ilgili olduğu düşüncesi de dahil olmak üzere, çeşitli nedenlerle trafik verileri olarak kabul edilmektedir.[309] Buna göre, 7. maddenin 9. fıkrasının b bendi, bazı Taraflar için bir çekince sağlamaktadır. Fıkranın b bendi uyarınca bu maddenin belirli erişim numaralarına uygulama hakkının saklı tutulması durumunda, diğer Taraf ülkedeki hizmet sağlayıcıya doğrudan sunulmak üzere abone bilgilerinin ifşası belirli erişim numaralarına ilişkin olarak artık talep edemeyecektir.[310] Protokolün 19. maddesinin 1. fıkrasında düzenlenmiş olması dolayısıyla geri bu çekince geri çekilebilir.

[307] Protokolün 7. maddesinin 2. fıkrası "Taraflardan her biri, abone bilgilerinin düzenleyen Tarafın özel cezai soruşturmaları veya kovuşturmaları için gerekli olduğu durumlarda, belirli, depolanmış söz konusu hizmet sağlayıcının mülkiyetinde veya kontrolünde olan abone bilgilerinin ifşası için başka bir Tarafın ülkesindeki bir hizmet sağlayıcısına doğrudan sunulmak üzere bir emir verme yetkisini yetkili makamlarına yetkilendirmek için gerekli olabilecek yasal ve diğer önlemleri alacaktır." hükmünü amirdir.
[308] Protokole İlişkin Açıklayıcı Rapor, Art.122.
[309] A.g.e., Art.93.
[310] A.g.e., Art.123.

a.b. Protokolün 19. maddenin 2. fıkrasında belirtilen çekince imkânı

19. maddenin 2. fıkrasına göre Taraflar, Protokolün 7. maddesi 2 fıkrasının b bendinde öngörülen çekinceden yararlandığını beyan edebilir. 7. maddenin 2 fıkrasının b bendinde Tarafların kendi ülkesindeki hizmet sağlayıcılara verilen emirlerle ilgili olarak; 7. maddenin 1. fıkrasındaki emrin "bir savcı veya başka bir adli makam tarafından veya onun gözetiminde veya başka bir şekilde bağımsız gözetim altında" verilmiş olmasının şart koşulabileceği ifade edilmektedir. Unutulmamalıdır ki, isteğe bağlı çekince değiştirilemez. Talepte bulunulan ülke, talep eden ülkeden gerekli bildirimi yapmasını isteyebilir, ancak talebin içeriğini değiştiremez. Diğer bir ifadeyle, kendisine yöneltilen abone verilerine erişim emirlerinin, her ikisinin de emir kabul etme yetkisine sahip olup olmaması nedeniyle savcı değil, hâkim tarafından verilmesini talep edemez, zira her iki Tarafın da bir emri kabul etme veya etmeme yetkisi vardır.[311]

Protokolün tanımlar bölümünde "yetkili makam" terimi, bu Protokol kapsamındaki tedbirlerin uygulanmasını emretmek, yetkilendirmek veya üstlenmek için iç hukuk tarafından yetkilendirilmiş bir adli, idari veya diğer kanun uygulayıcı makamı ifade etmektedir. Tarafların kendi iç hukuk sistemi, hangi makamın emir vermeye yetkili makam olarak kabul edileceğini belirleyecektir. 7. maddenin 5. fıkrası ile Talepte bulunan Taraf, hangi makamlarının emri çıkarabileceğini belirlerken, talepte bulunulan Tarafın, belirlenmiş bir makamın bu madde uyarınca verilen emirleri gözden geçirmesini ve doğrudan iş birliğini durdurma kabiliyetine sahip olmasını talep edebileceği bir güvence sağlanmaktadır.[312]

[311] Rojszczak, s.1016, dipnot 89.
[312] Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence Explanatory Report, Art.98, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, çevrimiçi, Erişim Tarihi: 27.09.2022.

Bir Tarafın iç hukuk sistemi, hangi makamın emir vermeye yetkili makam olarak kabul edileceğini belirleyecektir. Bazı Taraflar, iş birliğinin dolaysız doğası doğrultusunda, emrin yasallığının daha fazla gözden geçirilmesi için ek bir güvenceye sahip olmasının gerekli olduğunu düşünmüştür. Bu sebeple, 19. maddenin 2. fıkrası ile abone bilgilerinin ifşası hakkında Taraflara, 7. maddenin 2. fıkrasının b bendinde belirtilen ek güvence talep etme imkânı tanımıştır.[313] Buna göre; talepte bulunulan Tarafın kendi ülkelerinde bulunan hizmet sağlayıcılara "7. maddenin 1. fıkrası uyarınca verilen emrin, bir savcı veya başka bir adli makam veya başka bir şekilde bağımsız denetim altında verilmiş olması" gerektiği yönünde beyanda bulunulabilecektir. Bu beyanı kullanan Taraflar, aynı şekilde, kendilerinin belirttikleri makamlar tarafından veya bağımsız bir denetim altında verilmiş bir emri kabul etmelidir.[314]

a.c. Protokolün 19. maddesinin 3. fıkrasında belirtilen beyan imkânı

Bu fıkra uyarınca Taraflar, bu Protokolün 7. maddesinin 5. fıkrasının a ve e bentlerinde öngörülen herhangi bir beyanı, bildirimi veya tebligatı yapabilirler. Buna göre, Taraflar, 1. fıkra doğrultusunda kendi ülkesindeki bir hizmet sağlayıcıya emir verildiğinde, tüm emirler için veya belirlenen durumlarda, bu emrin Avrupa Konseyi Genel Sekreterine eşzamanlı bildirim gerektireceğini belirtebilirler.

Bir Taraf, 5. fıkranın a bendi uyarınca bildirim almak için tek bir makam belirleyecek ve bu makamın doğru ve güncel iletişim bilgilerini, a bendi doğrultusunda Avrupa Konseyi Genel Sekreterine ilk bildirimde bulunulduğunda iletecektir. Bildirim prosedürleri tamamen isteğe bağlı olup, Taraflar herhangi bir prosedür talep etmek zorunda değildir.[315] Bildirim gerekliliği beyanında bulunan bir Taraf, hizmet

[313] A.g.e., Art.101.
[314] A.g.e., Art.101.
[315] A.g.e., Art.109.

sağlayıcının emre cevaben abone bilgilerini vermesinden önce, hizmet sağlayıcının beklemesi gereken bir süre zarfı da belirleyebilir.[316]

Fıkranın a bendi uyarınca bilgilendirilen Taraflar, c bendinde belirtilen "ifşanın, o Taraftaki cezai soruşturmalara veya kovuşturmalara zarar verebileceği veya abone bilgilerinin karşılıklı yardım yoluyla istenmesi durumunda, Sözleşmenin 25. maddesinin 4. fıkrası ile 27. maddesinin 4. fıkrası uyarınca[317] ret koşulları veya gerekçeleri geçerli olacağı" gerekçeleriyle bir hizmet sağlayıcıya bilgileri ifşa etmeme talimatı verebilir. Tarafların bilgilendirilme hususu ek bir koruma sağlar. Bunun yansıra, iş birliği prensipte kapsamlı olmalıdır ve ceza soruşturmaları için elektronik kanıtlara sınır ötesi erişime yönelik engelleri ortadan kaldırmak ve daha verimli ve hızlandırılmış prosedürler sağlamak için iş birliğinin önündeki engeller Protokolün 7. maddesinin amaçlarıyla uyumlu olarak sınırlandırılmalıdır.[318]

Beyan imkânı Protokoldeki diğer maddeler için düzenlenen beyan "bu Protokolün imzalanması sırasında veya onay, kabul veya uygun bulma belgesini tevdi ederken ve diğer herhangi bir zaman" için tanınmıştır. Bu doğrultuda Taraflar bildirimi dilediği zaman yapabilir. Aynı şekilde Taraflar, doğrudan iş birliği mekanizması ile edinilen deneyimler sonucunda bir bildirim veya danışma rejimi kurmak istediğine de aynı şekilde karar verebilirler.[319] Fıkranın f bendi uyarınca Avrupa Konseyi Genel

[316] A.g.e., Art.112.
[317] "Örneğin, Sözleşmeye Ilişkin Açıklayıcı Raporun 257. maddesine uygun olarak, bu hüküm, bu hükmün yürürlükteki karşılıklı yardımlaşma anlaşmalarında ve iç hukukta ret gerekçelerine tabi olduğunu ve "talep edilen Tarafta bulunan kişilerin haklarının güvence altına alınmasını" sağlar ve açıklayıcı raporun 268. maddesi uyarınca, "Devletin egemenliğine, güvenliğine, kamu düzenine veya diğer temel çıkarlara önyargı" gerekçesiyle yardım reddedilebilir. Ayrıca, gizlilik gibi talebin yerine getirilmesine izin vermek için gerekli koşulları da getirebilir. Ayrıca, talepte bulunulan Taraf, Sözleşme'nin 27. maddesinin 5. fıkrası uyarınca talebin yerine getirilmesini erteleyebilir. Talepte bulunulan Taraf, talebi reddetme, koşullandırma veya erteleme kararını talep eden Tarafa bildirecektir. Ayrıca, Taraflar, Sözleşme'nin 28. maddesinin 2. fıkrasının b bendi şartlarına uygun olarak kullanım sınırlaması uygulayabilirler." Protokole İlişkin Açıklayıcı Rapor, Art.141.
[318] Protokole İlişkin Açıklayıcı Rapor, Art.110.
[319] A.g.e., Art.114.

Sekreterinin, a ve e bentleri uyarınca bildirilen makamların kaydını oluşturması ve güncel tutması gerekmektedir. Zira, Tarafların herhangi bir zamanda değişebilecek olan bildirim gerekliliklerinden haberdar olmalarını sağlamak kritik öneme sahiptir.[320]

b) Abone Bilgilerinin ve Trafik Verilerinin Hızlandırılmış Üretimi İçin Başka Bir Taraftan Gelen Emirleri Yürürlüğe Koyma Hakkındaki Çekince ve Beyan İmkânları (Madde 8)

Bu madde uyarınca Taraflardan her biri, talepte bulunulan Tarafın ülkesindeki ve o Tarafın belirli cezai soruşturmaları veya kovuşturmaları için gerekli olan hizmet sağlayıcının mülkiyetinde veya kontrolünde olan, abone bilgileri ile trafik verilerine ilişkin belirlenmiş ve depolanmış bilgileri üretmesi için hizmet sağlayıcıyı zorlamak amacıyla diğer Tarafa yapacağı talebin bir parçası olarak sunulacak bir emrin düzenlenmesinde yetkili makamları yetkilendirmek için gereken yasal ve diğer önlemleri alacaktır.

b.a. Protokolün 19. maddesinin 1. fıkrasında belirtilen çekince imkânı

Maddenin 13. fıkrası doğrultusunda Taraflar, bu maddeyi trafik verilerine uygulama hakkını saklı tutabileceklerdir. Bu çekincede bulunan Tarafların, trafik verilerinin hızlandırılmış üretimi için başka bir Taraftan gelen emirleri yürürlüğe koyma zorunluluğu yoktur. Ancak bu maddeyi saklı tutan bir Tarafların, 1. fıkra kapsamında diğer Taraflara trafik verileri için üretim emri vermesine izin verilmemektedir.[321] Protokolün 19. maddesinin 1. fıkrasında düzenlenmiş olması dolayısıyla geri bu çekince geri çekilebilir.

[320] A.g.e., Art.115.
[321] A.g.e., Art.147.

b.b. Protokolün 19. maddesinin 2. fıkrasında belirtilen çekince imkânı

Maddenin 11. fıkrası "bu madde kapsamında Tarafların taleplerinin, talepte bulunan Tarafın merkezi makamı tarafından veya ilgili Taraflar arasında karşılıklı olarak belirlenen başka bir makam tarafından kendisine sunulmasını istediğini beyan edebilir" ifadesiyle Taraflara çekince imkânı vermektedir. Başka çekincede bulunulamaz. Taraflar, taleplerin sunulması için mümkün olduğunca fazla esneklik sağlamaya teşvik edilir.[322]

b.c. Protokolün 19. maddesinin 3. fıkrasında belirtilen beyan imkânı

Protokolün 8. maddesinin 4. fıkrası doğrultusunda bir Taraf, maddenin 1. fıkrası kapsamındaki[323] emirleri yürürlüğe koymak için ek destekleyici bilgilerin gerekli olduğunu beyan edebilir. Örneğin, bazı Tarafların trafik verilerinin üretilmesi ve bu tür verilerin elde edilmesi hususunda, kendi iç hukukları uyarınca kanunlarında ek gereklilikler bulunduğundan daha fazla bilgi gerektirebilir. Ek olarak, talepte bulunulan Taraf, 8. maddenin 3. fıkrasının b bendi uyarınca sağlanan bilgilere ilişkin açıklama isteyebilir. Başka bir örnek olarak, bazı Taraflar emrin bir savcı veya talepte bulunan Tarafın diğer adli veya bağımsız idari makamları tarafından verilmediği veya incelenmediği durumlarda ek bilgi talep edebilirler. Taraflar, böyle bir beyanda bulunurken, gerekli ek bilgi türü konusunda mümkün olduğunca spesifik olmalıdır.[324]

---

[322] A.g.e., Art.145.

[323] Maddenin 1. fıkrasında yer alan emir şu şekilde ifade olunmaktadır; "Taraflardan her biri, talepte bulunulan Tarafın ülkesindeki ve o Tarafın belirli cezai soruşturmaları veya kovuşturmaları için gerekli olan hizmet sağlayıcının mülkiyetinde veya kontrolünde olan, belirlenmiş ve depolanmış olan abone bilgileri ve trafik verileri bilgilerini üretmesi için hizmet sağlayıcıyı zorlamak amacıyla diğer Tarafa yapacağı talebin bir parçası olarak sunulacak bir emrin düzenlenmesinde yetkili makamları yetkilendirmek için gereken yasal ve diğer önlemleri alacaktır."

[324] Protokole İlişkin Açıklayıcı Rapor, Art.137.

Maddenin 10. fıkrasının a ve b bentleri uyarınca Taraflardan her biri, bu madde kapsamında bir emir vermek ve emir almak için tayin edilen makamlarının iletişim bilgilerini Avrupa Konseyi Genel Sekreterine iletecek ve güncel tutacaktır. Maddenin 10. fıkrasının amacı, Tarafların, imza anında veya onay, kabul veya uygun bulma belgelerini tevdii ederken, 8. madde kapsamında emir gönderecek ve emir alacak makamları belirlemelerini sağlamaktır. Tarafların belirli bir kişinin adını ve adresini vermelerine gerek yoktur, ancak bu madde uyarınca emir gönderme ve alma amaçları için yetkili sayılan bir ofis veya birimi belirleyebilirler.[325]

c) Saklanan Bilgisayar Verilerinin Acil Bir Durumda Hızlandırılmış İfşası Hakkındaki Çekince İmkânları (Madde 9)

9. madde uyarınca Taraflardan her biri, acil bir durumda, diğer Taraftaki bir irtibat noktasından, o Tarafın ülkesindeki bir hizmet sağlayıcıdan, o hizmet sağlayıcının mülkiyetinde veya kontrolündeki belirtilen, depolanmış bilgisayar verilerinin, karşılıklı yardım talebi olmaksızın hızlı bir şekilde ifşa edilmesini sağlamak için acil yardım isteyen bir talebi iletmek ve almak için 7/24 İletişim Ağı için gerekli olabilecek yasal ve diğer önlemleri alacaktır.

Yalnızca "belirlenmiş, depolanmış abone bilgilerini" elde etmek için kullanılabilecek 7. madde gibi, bu Protokoldeki diğer maddelerin aksine, bu madde daha geniş "belirtilmiş, depolanmış bilgisayar verileri" terimini kullanmaktadır. Bu terim herhangi bir "belirtilen" bilgisayar verisini kapsar, terimin kapsamı geniştir ve ayrım gözetmemektedir.[326] Acil durumlarda, bir ön koşul olarak karşılıklı yardım talebi sunulmasını gerektirmeden, yalnızca abone bilgilerinin değil, depolanan içerik ve trafik verilerinin elde edilmesinin önemi düşünülerek oldukça geniş terim kullanıldığı ifade

[325] A.g.e., Art.144.
[326] A.g.e., Art.155.

edilmektedir.[327] Daha önceki düzenlemelerde olduğu gibi söz konusu veriler depolanmış veya mevcut verilerdir ve henüz ortaya çıkmamış trafik verileri veya gelecekteki iletişimlerle ilgili içerik verileri gibi verileri içermez.[328]

Protokolün 19. maddesinin yalnızca 2. Fıkrasında yer alan çekince imkânı tanınmıştır. Buna göre Taraflar yalnızca 9. maddenin 1. fıkrasının b bendi ile maddenin 5. fıkrasında öngörülen çekincelerden yararlandığını beyan edebilir. Buna göre, Taraflar yalnızca bu maddeden kaynaklı abone bilgilerinin ifşa edilmesi talepleri yerine getirmeyeceğini beyan edebilirler. Bazı Taraflar için, 9. madde kapsamında yalnızca abone bilgilerine yönelik talepler almak, 7/24 İletişim Ağının kaynaklarını ve zamanını içerik veya trafik verileri taleplerinden uzaklaştırarak bu birimlere aşırı yük bindirme riskini taşımaktadır. Yalnızca abone bilgilerine ihtiyaç duyan Taraflar bu gibi durumlarda, 9. madde doğrultusunda taleplerini iletmek yerine, bu tür bilgilerin hızlı bir şekilde ifşa edilmesini kolaylaştıran 7. veya 8. maddeleri kullanabilirler. Böyle bir beyan sonucunca diğer Taraf ülkelerin, bu madde kapsamında içerik ve/veya trafik verileri için bir talepte bulunurken, diğer maddeler aracılığıyla abone bilgileri için bir talepte bulunmalarını yasaklanmamaktadır.[329]

Maddenin 5. fıkrası uyarınca bir Taraf, talepte bulunan Taraflardan talebin yerine getirilmesini takiben talebi ve bunu desteklemek için iletilen her türlü ek bilgiyi, talepte bulunulan Tarafça belirtildiği şekilde, karşılıklı yardımı da içerebilecek bir formatta ve bu tür bir kanal aracılığıyla sunmasını talep ettiğini beyan edebilir. Örneğin, bir Taraf, özel durumlarda acil durum talebini resmi olarak belgelemek için, talepte bulunan Taraftan daha sonra karşılıklı yardım talebi sunmasını ve böyle bir talebe cevaben veri sağlamaya yönelik önceki kararı talep edeceğini beyan edebilir. Bazı Taraflar için böyle bir prosedür kendi iç hukukları tarafından gerekli kılınırken,

[327] A.g.e., Art.155.
[328] A.g.e., Art.170.
[329] A.g.e., Art.157.

diğer Taraflar böyle bir zorunluluklarının olmadığını ve bir beyan için bu imkândan yararlanmalarına gerek olmadığını belirtmişlerdir.[330]

d) Acil Karşılıklı Yardım Hakkındaki Çekince İmkânı (Madde 10)

Acil bir durumun var olduğunu düşünüldüğü durumlarda, Taraflardan her biri süratle hızlandırılmış bir temelde karşılıklı yardım talep edebilir. Bu madde doğrultusundaki taleplerde, gerekli içeriklere ek olarak, acil bir durum olduğunu gösteren olguların ve talep ile yardımın illiyet bağının bir açıklamasına yer verilmelidir. Protokolün 19. maddesinin yalnızca 2. fıkrası ile çekince imkânı tanınmıştır. Buna göre, Taraflar yalnızca 10. maddenin 9. fıkrasında öngörülen çekincelerden yararlandığını beyan edebilir

Maddenin 9. fıkrası ile bu Protokolün Taraflarının, savcılar veya diğer adli makamlar arasında doğrudan talepte bulunulmasını sağlayabilecekleri bir beyan imkânı sağlanmaktadır.[331] Buna göre Taraflar, taleplerin doğrudan adli makamlarına veya Uluslararası Kriminal Polis Teşkilatı (INTERPOL) kanalları aracılığıyla veya Sözleşmenin 35. maddesi uyarınca kurulan 7/24 İletişim Ağına da gönderilebileceğini beyan edebilir. Bu tür durumlarda, taleplerin bir nüshası da aynı zamanda talepte bulunan Tarafın merkezi makamı aracılığıyla, talepte bulunulan Tarafın merkezi makamına gönderilecektir. Talepte bulunulan Tarafın adli makamına doğrudan bir talep gönderildiğinde ve bu makam ilgili talebi işleme koymaya yetkili değil ise, bu talebi yetkili ulusal makama havale edecek ve bu işlemi gerçekleştirdiğini talepte bulunan Tarafa doğrudan bildirecektir.

[330] A.g.e., Art.168.
[331] A.g.e., Art.181.

Bazı Taraflarda, bu tür doğrudan adli makamlar arası kanallar iyi yapılandırılmıştır, taleplerin iletilmesi ile yerine getirilmesini daha da hızlandırmak için etkili bir araç olabilir. Acil durum taleplerinin 7/24 İletişim Ağı veya INTERPOL aracılığıyla iletilmesi, yalnızca gecikmeyi azaltmak için değil, aynı zamanda güvenlik ve kimlik doğrulama standartlarını artırmak için de faydalıdır. Bununla birlikte, bazı Taraflarda, merkezi makamının katılımı, onayı veya yönlendirmesi olmaksızın, talepte bulunulan Taraftaki bir adli makama doğrudan bir talebin gönderilmesi bu konuda ters etki yapabilir. Talebin iletildiği makam, bağımsız hareket etme yetkisine sahip olmayabilir veya uygulanması gereken usul hakkında bilgili olmayabilir. Bundan dolayı bir Taraf, taleplerinin bu merkezi olmayan otorite kanalları aracılığıyla gönderilebileceğini beyan etmelidir.[332]

e) Müşterek Soruşturma Ekipleri ve Müşterek Soruşturmalar Hakkındaki Çekince İmkânı (Madde 12)

Protokolün 19. maddesinin yalnızca 2. fıkrası ile 12. maddeye ilişkin çekince imkânı tanınmıştır. Buna göre, 12. maddenin 3. fıkrasında öngörülen çekincelerden yararlanıldığını beyan edilebilir. Maddenin 3. fıkrası, bir Tarafın merkezi makamının, ekibi kuran anlaşmaya imza atması veya başka bir şekilde bu anlaşmada mutabık kalması gerektiğini beyan etmesine izin verir. Bu hükmün çeşitli nedenlerle eklendiği ifade edilmektedir. Öncelikle, bazı Taraflar müşterek soruşturma ekiplerini bir tür karşılıklı yardım olarak görmektedir. Diğer bazı Taraflar bakımından ise karşılıklı yardım için merkezi makamların, yetkili makamlar ile bir müşterek soruşturma ekip anlaşması hazırlanması, Tarafların uygulanabilir yerel yasal gereklilikleri yerine getirilmesini sağlamalarında rol oynayabilir.[333]

[332] A.g.e., Art.181.
[333] A.g.e., Art.210.

Son olarak, bu fıkrada belirtilen beyanı yapmış bir Taraf ile müşterek soruşturma ekip anlaşmasına girmek isteyen diğer Tarafların makamları, Protokol kapsamında geçerli olabilmesi için, beyanda bulunan Tarafın merkezi makamının müşterek soruşturma ekip anlaşmasını imzalaması veya başka bir şekilde kabul etmesi gerektiği konusunda uyarılır. Bu, gerekli yetkiye sahip olmayan veya beyanda bulunan Tarafın geçerli yasal gerekliliklerine uymayan bir müşterek soruşturma ekip anlaşmasının akdedilmesine karşı koruma sağlamaktadır.[334]

f) Kişisel Verilerin Korunması Hakkındaki Beyan İmkânları (Madde 14)

Protokolün 19. maddesinin 3. fıkrası doğrultusunda Taraf ülkeler, kişisel verilerin korunması hususunun düzenlendiği 14. maddenin 7. fıkrasının c bendi ve 10. fıkrasının b bendinde öngörülen herhangi bir beyanı, bildirimi veya tebligatı yapabilir. Veri güvenliği ve güvenlik olaylarının düzenlendiği 7. fıkra ve başka bir ülkeye veya uluslararası kuruluşa ileriye dönük aktarımın düzenlendiği 10. fıkrada; Taraflardan her birinin, Avrupa Konseyi Genel Sekreterine, II. Bölümün 2. Kısmının amaçları doğrultusunda yetki verecek makam veya makamlarını bildirecektir, verilen bilgiler daha sonra değiştirilebilir. II. Bölümün 2. Kısmı diğer Taraflardaki sağlayıcılar ve kuruluşlarla doğrudan iş birliğini geliştiren usulleri düzenlemektedir, burada alan adı kayıt bilgileri talebinin düzenlendiği 6. madde ile abone bilgilerinin ifşasının düzenlendiği 7. madde yer almaktadır.

Veri güvenliği ve güvenlik hadiselerinin düzenlendiği 14. maddenin 7. fıkrasının c bendinde şu husus düzenlenmektedir; Taraflardan her biri Avrupa Konseyi Genel Sekreterine, bu fıkranın b bendi uyarınca II. Bölümün 2. Kısmının amaçları doğrultusunda yetki verecek makam veya makamlarını bildirecektir, verilen bilgiler daha sonra değiştirilebilir. Fıkranın b bendine göre, bireylere veya diğer Tarafa fiziksel

[334] A.g.e, Art.210.

olan veya olmayan önemli bir zarar verme riskinin bulunduğu bir güvenlik olayının tespit edilmesi üzerine, verileri alan Taraf bunun olasılığını ve ölçeğini derhal değerlendirecek ve bu tür bir zararı azaltmak için derhal uygun önlemleri alacaktır. Bu tür eylemler, verileri aktaran makama veya II. Bölümün 2. Kısmının amaçları doğrultusunda, c bendi uyarınca tayin edilen makam veya makamlara bildirimi içerecektir.

İleriye dönük bir aktarım için yetki alınması ile ilgili olarak maddenin 10. fıkrası uyarınca; özel olarak tanımlanmış kişisel verilerin belirli bir üçüncü ülkeye veya uluslararası kuruluşa aktarılmasında yetkilendirme için talepte bulunan, verinin transfer edildiği, Tarafın yetkililerinden talepte bulunulan, veriyi aktaran, Tarafın yetkililerine bireyselleştirilmiş bir talep gönderilmesini gerektirebilir. Ancak, 10. fıkranın a bendi, Tarafların ileriye dönük transferler için, yazılı anlaşma veya diğer düzenlemeler öngörülmesi gibi, önceden kurallar koymasını engellemez. Ayrıca, bir Tarafın verilerin alıcısı tarafından kullanımına ilişkin, veri aktaran Tarafın soruşturmasına halel gelmemesi için, alıcı Tarafın kişisel verileri ne ölçüde kullanabileceği veya yayabileceği konusunda sınırlamalar koymak gibi, başka koşullar koyma yetkisine engel getirilmemektedir.[335] Bu yaklaşım, bu Protokol kapsamında aktarılan kişisel verilerin korunmasının bir aracı olarak da bu bende taşınmıştır.[336] 10. fıkra kapsamında bir aktarıma izin verilip verilmeyeceğini belirlerken, aktaran veya tayin edilen yetkili makamların; cezai suçun ciddiyeti, verilerin orijinal olarak aktarılma amacı, orijinal aktarımla ilgili geçerli tüm koşulları ve üçüncü ülke veya uluslararası kuruluşun kişisel verilerin uygun düzeyde korunmasını sağlayıp sağlamadığı dahil olmak üzere, ilgili tüm faktörleri dikkate alması teşvik edilir.[337]

[335] A.g.e., Art.264.
[336] A.g.e., Art.262.
[337] A.g.e., Art.265.

g) Federal Hüküm Hakkındaki Çekince ve Beyan İmkânları (Madde 17)

Protokolün 19. maddesinin 1. ve 3. fıkraları ile federal hükmün düzenlendiği 17. maddeye ilişkin Taraflara çekince ve beyanda bulunma imkânı tanınmıştır.

g.a. Protokolün 19. maddesinin 1. fıkrasında belirtilen çekince imkânları

Protokolün 17. maddesi, federal yapıda bir ülke olan Tarafın "merkezi hükümet ile eyaletler veya diğer benzer bölgesel kuruluşlar arasındaki ilişkiyi düzenleyen temel ilkeleriyle tutarlı olarak bu Protokol kapsamındaki yükümlülükleri üstlenme hakkını belirli şartlarda saklı tutabilir" ifadesiyle çekince koymasına izin vermektedir. Bunun amacı federal ülkelerin, merkezi ve bölgesel otoriteler arasındaki karakteristik güç dağılımının bir sonucu olarak karşılaşabilecekleri güçlükleri karşılamaktır.[338]

Buna göre bir federal ülke, merkezi hükümeti ile bileşen eyaletler veya diğer benzer bölgesel kuruluşlar arasındaki ilişkiyi düzenleyen temel ilkeleriyle tutarlı olarak, bu Protokol kapsamındaki yükümlülükleri üstlenme hakkını 1. fıkradaki şartlarda saklı tutabilir. Maddenin 1. fıkrası öngörülen çekince hakkını şu şekilde sınırlamaktadır; Protokol, federal ülkenin merkezi hükümetine uygulanacaktır. Böyle bir çekince, II. Bölümün hükümleri uyarınca diğer Taraflarca aranan iş birliğini sağlama yükümlülüklerini etkilemeyecektir. Şartlar ve teminatların düzenlendiği 13. madde hükümleri federal ülkenin bileşen eyaletlerine veya diğer benzer bölgesel kuruluşlarına uygulanacaktır.

Federal ülkelerin, yerel cezai suçların ve ulusal usul tedbirlerinin belirlenmesine ilişkin olarak Sözleşmenin II. Bölümündeki yükümlülüklere çekince koymalarına izin verilir. Bununla birlikte, federal ülkelerin Sözleşmenin III. Bölümü

[338] A.g.e., Art.297.

uyarınca diğer Taraflara uluslararası iş birliği sağlayabilmeleri gerekmektedir.[339] Sözleşme, karşılıklı yardım için federal hüküm çekincesi sağlamamış olsa dahi bu Protokolün önlemlerinin çoğu, geleneksel karşılıklı yardım ile aynı şekilde işlememektedir. Bu Protokol, geleneksel karşılıklı yardımdan daha verimli olan ve merkezi hükümetin katılımını gerektirmeyen bir dizi iş birliği önlemi sağlar. Özellikle, bu Protokol, bir Taraftaki yetkili makamların diğer Taraftaki özel şirketlerden doğrudan iş birliği isteyebileceği, madde 6 ve 7 olmak üzere iki önlem getirmektedir. Bu önlemler, bir federal ülkenin, kurucu eyaletlerden veya bölgesel kuruluşlardan yetkili makamların uymasını istemekte güçlük çekebileceği belirli usuli adımları gerektirir. Örneğin; 7. madde, bir Tarafın Genel Sekretere bildirimde bulunarak, yetkililerin diğer Taraflardan, hizmet sağlayıcıya abone bilgilerini talep eden bir emir iletirken aynı anda belirlenmiş bir hükümet yetkilisini bilgilendirmesini gerektirebileceğini öngörmektedir.[340]

Protokol ayrıntılı veri koruma hükümleri içerirken, Sözleşme bunu içermemektedir. Örneğin, ABD anayasası ve federalizmin temel ilkeleri uyarınca, kurucu eyaletleri kendi cezai ve cezai usul yasalarını yürürlüğe koyar, kendi mahkemelerini, savcılarını ve polislerini oluşturur ve cezai suçları soruşturmak ve kovuşturmak için yasa çıkarır. Eyaletin yetkili makamları, federal makamlardan bağımsızdır ve federal makamlara tabi değildir.[341] Eyaletler, merkezi hükümette uygulananlardan farklı usul ve mahremiyet yasaları kapsamında faaliyet gösteriyor olabilirler.

Bu Protokol kapsamında alınan kişisel veriler, daha sonra aynı Tarafın başka bir makamına istisna olmadıkça 14. maddenin 9. fıkrası uyarınca işlenmelidir. Federal yapıda olan bir Taraf ülke, burada belirtilen koşullara uygun olarak, bu Protokolün 17.

[339] A.g.e., Art.298.
[340] A.g.e., Art.299.
[341] A.g.e., Art.299.

maddesi kapsamındaki yükümlülüklerine çekince koyması durumunda, 14. Maddenin 9. fıkrasının a bendine, federal devletlerin merkezi ve bölgesel otoriteler arasındaki karakteristik yetki dağılımının bir sonucu olarak karşılaşabilecekleri zorlukları" barındıran bir istisna sağlamaktadır.[342] Bu nedenle, 14. maddenin 9. fıkrasının b bendi, bir Tarafın 17. madde uyarınca çekince koyduğu durumlarda; Tarafın, verileri alan makamların verilerin bir düzeyde korunmasını sağlayarak verileri, bu madde ile sağlananla karşılaştırılabilir düzeyde, etkin bir şekilde korumaya devam etmesi için önlemleri almış olması koşuluyla, bu Protokol kapsamında başlangıçta alınan kişisel verilerin aktarımını, kurucu Devletlerine veya diğer benzer bölgesel kuruluşlara yine de sağlayabilir.

g.b. Protokolün 19. maddesinin 3. fıkrasında belirtilen beyan imkânı

Bu düzenleme doğrultusunda Taraflar, 17. maddenin 2. fıkrasında öngörülen herhangi bir beyanı, bildirimi veya tebligatı yapabilir. Buna göre; diğer bir Taraf, kendi ülkesindeki makamların, sağlayıcıların veya kuruluşların, doğrudan birleşen ülke veya maddenin 1. fıkrası uyarınca çekince koyan bir federal ülkenin diğer benzer bölgesel kuruluşu tarafından sunulan bir talep veya talimata yanıt olarak iş birliği yapmasını, söz konusu ülke, Avrupa Konseyi Genel Sekreterine, bir birleşen ülkenin veya diğer benzer bir bölgesel kuruluşun bu Protokolün o federal ülke için geçerli olan yükümlülüklerini uyguladığını bildirmezse, engelleyebilir. Avrupa Konseyi Genel Sekreteri, bu tür bildirimlerin bir kaydını oluşturacak ve güncel tutacaktır.

Henüz Protokole Taraf olan ülkelerden Protokole ilişkin çekince veya beyanda bulunan bir ülke bulunmamaktadır.[343]

---

[342] A.g.e., Art.260.

[343] Reservations and Declarations for Treaty No.224 - Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Status as of 11/10/2022, www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=224&codeNature=0, çevrimiçi, Erişim Tarihi: 11.10.2022.

2.5.4.3. Fesih

Protokolün 24. maddesi uyarınca herhangi bir Taraf, herhangi bir zamanda, işbu Protokolü Avrupa Konseyi Genel Sekreterine yapacağı bir bildirim yoluyla feshedebilir. 16. maddede düzenlenen imza ve yürürlüğe giriş hususunda olduğu gibi, fesih bildiriminin Genel Sekreter tarafından alındığı tarihten sonraki üç aylık sürenin sona ermesini izleyen ayın ilk günü fesih yürürlüğe girecektir. Ayrıca, Sözleşmenin feshedilmesi bu Protokolün de feshi anlamına gelmektedir.

Bu Protokolün, kişisel verileri içerebilecek bilgi veya kanıt paylaşımına yaptığı vurgu göz önüne alındığında metni hazırlayanlar, maddenin 4. fıkrası ile feshin yürürlük tarihinden önce aktarılan bilgi veya delillerin, bu Protokol uyarınca muamele görmeye devam edeceği hususunu açıklığa kavuşturmak istemişlerdir.

3. BÖLÜM

3. PROTOKOLÜN GENEL DEĞERLENDİRMESİ

Sözleşmenin ve her iki ek Protokolün amacı, siber suçlarla mücadelede mümkün olduğunca çok ülkenin sürece katılımını, böylelikle sınır tanımayan siber suçların faillerinin cezalandırılması ve mağdurlar için adaletin teminini amaçlamaktadır. Bu doğrultunda 2. Ek Protokolün amacının, internet üzerindeki siber terörizme ve diğer büyük ölçekli saldırılara karşı iş birliğini artırmak ve siber suçlarla mücadelede uluslararası iş birliğini kolaylaştırmak, bunu sağlarken hukukun üstünlüğünü korumak ve suç mağdurlarının temel haklarını korumakla ilgili olduğundan söz edilmektedir.[344]

Bu çalışmanın ikinci bölümünde Protokol maddeleri detaylı olarak incelenirken, maddelere ilişkin olumlu ve olumsuz değerlendirmeler ifade olunmuştur. Bunların yanı sıra daha çok dikkat çeken bazı hususlara ilişkin eklemeler yapılmak istenmektedir. Protokol her ne kadar olumlu ve iş birliğini kolaylaştırıcı pek çok yenilik getiriyor olsa da olumsuz eleştiri topladığı yönleri de mevcuttur.

3.1. ABONE VERİLERİNİN VE DİĞER VERİLERİN İFŞASI İLE İLGİLİ DEĞERLENDİRMELER

İnternet özgürlüğü grupları topluluğu, Protokolün II. Bölümünde yer alan özel kuruluşlarla olacak doğrudan iş birliğine izin verilmesini, üretim emri için zorunlu adli izin olmaksızın alan adı kayıt bilgileri ve abone bilgileri gibi kişisel verilerin gönüllü

[344] Draft Second Additional Protocol to the Convention On Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence, Committee on Legal Affairs and Human Rights, Rapporteur : Mr Kamal JAFAROV, Azerbaijan, EC/DA Origin - Reference to committee: Doc. 15316, Reference 4593 of 21 June 2021. 2021 - Fourth part-session, Report | Doc. 15379 | 28 September 2021, çevrimiçi https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=29475&lang=en, Erişim Tarihi: 22.05.2022.

olarak ifşa edilmesine teşvik ettiği gerekçesiyle hukukun üstünlüğüne yönelik bir tehdit gördükleri yönünde Protokolü sert bir şekilde eleştirmişlerdir.[345]

Protokolün 6. ve 7. maddeleri, alan adı kayıt bilgileri ve abone bilgilerinin belirlenebilmesi amacıyla, bir ülkedeki kolluk kuvvetleri ile diğer ülkeden hizmet sağlayıcılar arasında doğrudan iş birliği için bir çerçeve oluşturmaktadır.[346] Ancak bu durumun, anonim kişilerin istenilen zamanda belirleme yetkisi avukatlar, gazeteciler, siyasi muhalifler, insan hakları savunucuları ve politikacılar için büyük bir tehdit oluşturduğu, bazı grupların temel haklarını baltalayabileceği düşünülmektedir.[347] Avukatlar, doktorlar, gazeteciler, dini görevliler veya parlamenterler gibi belirli meslekleri icra eden kişilerin ayrıcalıklarına, gizliliklerine ve dokunulmazlıklarına saygı gösterilmesi gerektiği ile ilgili bir düzenleme teklif edilmesine karşın, Protokol ve Protokole ilişkin açıklayıcı raporda böylesi bir düzenlemeye rastlanılmamıştır.[348]

Protokolün abone kimlik verilerine sınır ötesi erişim için birincil mekanizması olan 7. maddesi uyarınca; abone bilgilerinin ifşası bir ülkenin makamları tarafından, diğer ülkedeki hizmet sağlayıcıya doğrudan yapılacaktır. Bunun sonucunda ifşa, ülkenin yetkili makamları tarafından değil, veriyi bünyesinde bulunduran hizmet sağlayıcı tarafından yapılacaktır. Bu durumda, verilen emrin hukuka uygun olup olmadığının muhakemesini hizmet sağlayıcı yapmış olacaktır. 7. maddenin 5. fıkrasının b bendi uyarınca ifşadan önce hizmet sağlayıcıların "belirlenen" durumlarda makamlara danışılması gerekebilir, diğer bir ifadeyle, her emir karşısında ifşadan önce

[345] A.g.e. 16. Meclis Başkanı, Rik Daems ve diğer Avrupa Konseyi organlarına gönderilen, 02.05.2021 tarihli ortak mektup.
[346] Israel ve Rodriguez.
[347] A.g.e.
[348] Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Committee on Legal Affairs and Human Rights, Rapporteur : Mr Kamal JAFAROV, Azerbaijan, EC/DA Origin - Reference to committee: Doc. 15316, Reference 4593 of 21 June 2021. 2021 - Fourth part-session, Report | Doc. 15379 | 28 September 2021, 7.5., çevrimiçi https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=29475&lang=en, Erişim Tarihi: 22.05.2022.

makamlara danışılmayacaktır. Kural olarak, merkezi yetkililerin herhangi bir talebi onaylamasına gerek yoktur ve çoğu durumda bir talebin yapıldığının farkında bile olmayacaklardır.[349] Bu yönüyle bu düzenlemeyi kişilerin mahremiyet yönünden endişe verici olduğunu ve bu surette edinilen verilerin hukuka uygunluğu bakımından da sorunlara yol açabileceğini düşünüyoruz.

Protokol, muvafakat istemenin cezai soruşturmalara engel teşkil edebileceğini kabul etmekte ve ülkelere doğrudan hizmet sağlayıcıdan alan adı ve abone bilgilerini talep etme yetkisi vermektedir. Ancak bu madde, trafik verileri gibi veriler için doğrudan talep imkânı sağlamaz, bu da soruşturmaların hızlandırılması konusunda daha fazla fikir birliğine varılamamasına neden olur.[350]

Aşağıda genel değerlendirme ile işbu Protokolün imzası sırasında veya onay, kabul veya uygun bulma belgesini tevdi ederken hangi maddelere çekince konulmasının yararlı olabileceği hususlarıyla ilgili değerlendirmelerimiz yer alacaktır.

3.1.1. Abone Bilgilerinin İfşasını Düzenleyen 7. Madde Hakkında

Bu madde doğrultusunda hizmet sağlayıcılardan abone bilgilerinin ifşa edilmesi için, sınır ötesi doğrudan taleplere izin verilmektedir. Abone bilgileri daha önce de izah olunduğu üzere[351] trafik ve içerik verileri hariç olmak üzere, hizmet sağlayıcıların abonelerine ilişkin kullanılan hizmet türü, süresi, abone kimliği, abonenin adresi ve IP adresleri gibi diğer erişim bilgileri ile kişiye ait hizmete erişim aracının bulunduğu yere ilişkin bilgilerdir.

[349] Israel ve Rodriguez.
[350] A.g.e.
[351] Bkz. Bu çalışmanın 2.5.2.2. bölümü.

Bu maddenin standart prosedürü uyarınca, ifşa emrinde bulunan Taraf ülkenin makamlarının meşru olup olmadığı, emrin yasalara uygun ve orantılı olup olmadığı, ifşa sonucunda veri sahiplerinin haklarını tehlikeye atıp atmayacağı veya ret gerekçesinin geçerli olup olmadığını değerlendirmek hizmet sağlayıcının takdirine bırakılmıştır. Hizmet sağlayıcının böylesi bir muhakeme yapıp yapamayacağı tartışmaya açık bir husustur. Bu sebeple Tarafların, 19. maddede öngörülen çekince imkânlarından faydalanmaları yararlı olabilecektir. 7. maddenin 9. fıkrasında öngörülen çekince imkânları, bu maddenin tamamını uygulamama hakkı ile bu maddeyi yalnızca erişim numaralarına ilişkin olarak uygulamama hakkıdır.

Abone bilgileri arasından IP adresi, trafik verilerini ortaya çıkarabilir ve hatta iletişim içeriği hakkında çıkarımlara izin verebilir. Kişilerin hangi internet sitelerini ziyaret ettiği ve kimlerle iletişim kurduğu gibi bilgilerin edinilmesi, kolluk kuvvetlerince kişinin günlük alışkanlıklarını ayrıntılı bir şekilde analiz edilerek, kişinin profilini oluşturmak ve iletişimlerin içeriğiyle ilgili ipuçları sağlamak için kullanılabilir ve sonuçları zarar verici olabilir. Ancak diğer taraftan abone bilgileri, genellikle diğer soruşturma adımlarının temelini oluşturmakta ve bu nedenle ceza soruşturmalarında en çok ihtiyaç duyulan ve en sık aranan bilgi türlerindendir. Protokole ilişkin açıklayıcı raporda ifade edildiği üzere, 9. fıkranın a bendi uyarınca 7. maddeyi uygulamama hakkını saklı tutarsa, diğer Taraf ülkedeki bir hizmet sağlayıcıya doğrudan sunulmak üzere abone bilgilerinin ifşasını artık talep edemeyecektir. Bu bilgiler soruşturma adımlarının temelini oluşturmaktadır ve bu maddeyi uygulamamak Tarafların soruşturma ve kovuşturma süreçlerini oldukça olumsuz etkileyebilir.

Ancak diğer taraftan, 9. fıkranın b bendi uyarınca Taraflar bu maddenin uygulanmasını belirli erişim numaralarının ifşası bakımından uygulamayabilirler. IP adreslerinin ifşasının riskli olabileceği ve AİHM'in Benedik v. Slovenya davasında polisinin dinamik bir IP adresiyle ilişkili abone bilgilerine erişmeden önce mahkeme kararı almaması durumunun, özel hayatın ve aile hayatının gizliliği hakkını ihlal teşkil

ettiği görüşüne aykırı bir durum teşkil etmemek adına, Tarafların bu çekince imkânından faydalanmasını yararlı görüyoruz. Ancak tekrar belirtmek gerekir ki, bu çekinceden yararlanan Taraflar bu bilgilerin diğer Taraflarca ifşasını talep edemeyecektir. Yararlanılması tarafımızca tavsiye edilen, 7. maddenin 9. fıkrasının b bendi doğrultusunda, bu maddenin uygulanmasının erişim numaraları için saklı tutulması durumu, Protokolün 20. Maddesi uyarınca her zaman Taraflarca geri çekilebilir.

6706 Sayılı Cezaî Konularda Uluslararası Adlî İş Birliği Kanunu'nun 4. maddesi uyarınca; Türkiye'nin egemenlik hakları, millî güvenliği, kamu düzeni veya diğer temel çıkarlarının ihlal edilmesi, Talebe konu fiilin sırf askerî suç, düşünce suçu, siyasî suç veya siyasî suçla bağlantılı bir suç olması**,** Talepte bulunan devlette savunma hakkına ilişkin temel güvencelerin bulunmaması ile talebe konu kişinin ırkı, etnik kökeni, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasî görüşleri nedeniyle bir soruşturma veya kovuşturmaya maruz bırakılacağına veya cezalandırılacağına ya da işkence veya kötü muameleye maruz kalacağına dair inandırıcı nedenlerin bulunması, adlî iş birliği taleplerinin reddi sebebidir.

6706 Sayılı Kanun'a göre Türk adlî mercileri, soruşturma veya kovuşturmanın sonuçlandırılması ya da verilen mahkûmiyet kararlarının yerine getirilmesi için ihtiyaç duyulan konularda adlî yardımlaşma talebinde bulunabilir. Adlî merciler; mahkeme, hâkimlik ve savcılıklar ile kanunla istisnaî olarak ceza soruşturması yapma yetkisi verilen diğer makamları, devletlerin milletlerarası andlaşmalara yaptıkları beyanlarda belirttiği mercileri ifade eder.

5271 Sayılı Ceza Muhakemesi Kanunu'nda düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma ile iletişimin tespiti, dinlenmesi ve kayda alınması koruma tedbirlerine hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet Savcısı tarafından karar verilebilir. Bu sebeple iç

hukukumuzla denk hâle gelebilmesi bakımından; Protokolün 7. maddesinin 2. fıkrasının bendi uyarınca "abone verilerinin ifşasıyla ilgili olarak verilen emrin, bir savcı veya başka bir adli makam tarafından veya onun gözetiminde veya başka bir şekilde bağımsız gözetim altında verilmiş olması gerektiği" ile 8. maddenin 11. fıkrası uyarınca "abone bilgilerinin ve trafik verilerinin hızlandırılmış üretimi için başka bir Taraftan gelen emirleri yürürlüğe koymak ile ilgili olarak diğer Tarafların taleplerinin, talepte bulunan Tarafın merkezi makamı tarafından veya ilgili Taraflar arasında karşılıklı olarak belirlenen başka bir makam tarafından kendisine sunulmasını istediği" şeklindeki çekince imkanlarından faydalanabilir. Bu şekilde belirli konularda adli yardım taleplerinin Talepte bulunan ülkenin adli mercileri veya kararlaştırılmış makam tarafından yapılması ile ilgili çekincede bulunulmasının faydalı olacağı düşüncesindeyiz. İşbu beyan ile talepte bulunan ve talepte bulunulan Taraflar arasındaki asimetri hafifletilebilir. Nitekim birçok yasal modelde elektronik kanıtlar adli izni gerektirmeksizin elde edilebilir, talep edilen bilgilerin niteliğine bağlı olarak, bu tür kararlar bir savcı ve çoğu zaman soruşturma makamları tarafından da alınabilir.[352] Örneğin; Polonya'da, bir hizmet sağlayıcı tarafından tutulan elektronik verilerin sağlanması savcının onayını gerektirirken, elektronik iletişimden elde edilen meta (üst) veriler söz konusu olduğunda polisin kararı yeterlidir.[353]

Veri talebinde bulunulması durumunda ortaya çıkabilecek yüksek suistimal potansiyelini en aza indirmek ve dolandırıcılık ihtimallerini azaltmak adına, ülkelerin, 7. maddenin 2. fıkrasının b bendinde yer alan "emir, bir savcı veya başka bir adli makam tarafından veya onun gözetiminde veya başka bir şekilde bağımsız gözetim altında verilmiş olmalıdır" beyanında bulunması önerilmektedir.[354]

[352] Rojszczak, s.1004
[353] Rojszczak, s.1004 dipnot 27.
[354] Israel ve Rodriguez.

3.1.2. Abone Bilgilerinin ve Trafik Verilerinin Hızlandırılmış Üretimi İçin Başka Bir Taraftan Gelen Emirleri Yürürlüğe Koyma Hususunu Düzenleyen 8. Madde Hakkındaki Görüşler

Bu düzenleme doğrultusunda, talepte bulunan Taraf ülkenin, diğer bir Taraf ülkede ve o ülkenin topraklarındaki hizmet sağlayıcının mülkiyetinde veya kontrolünde bulunan abone bilgilerini veya trafik verilerini üretmek için, hizmet sağlayıcıyı zorlayarak bu emri işletebilmek için diğer Taraf ülkeye sunulmak üzere bir emir verme kabiliyetine sahip olması sağlanmaktır. Protokolün bu maddesinin kapsamı bir Tarafın, diğer bir Tarafın topraklarındaki hizmet sağlayıcılara belirli emirler vermesine izin vererek, Sözleşmenin 18. maddesinin kapsamını aşmaktadır.

Maddenin son bendi uyarınca, yalnızca trafik verilerinin üretimi bakımından bu maddenin uygulamama hakkı saklı tutabileceklerdir. Ancak maddenin uygulamama hakkını saklı tutan bir Taraf, 1. fıkra kapsamında diğer Taraflara trafik verileri için emir vermesine izin verilmemektedir. Bir önceki düzenlemede olduğu gibi, üretim emrinde bulunan Taraf ülkenin makamlarının meşru olup olmadığı, emrin yasalara uygun ve orantılı olup olmadığı, veri sahiplerinin haklarını tehlikeye atıp atmayacağı veya ret gerekçesinin geçerli olup olmadığını değerlendirmek hizmet sağlayıcının takdirine bırakılmıştır. Bu türden hassas bilgiler ile ilgili denetimi sağlayabilmek için maddenin 11. fıkrasında öngörülen çekince imkanından faydalanılmasını yararlı görüyoruz. Buna göre; bu madde kapsamında diğer Tarafların" taleplerinin, talepte bulunan Tarafın merkezi makamı tarafından veya ilgili Taraflar arasında karşılıklı olarak belirlenen başka bir makam tarafından kendisine sunulmasını" istediğini beyan edebilir. Zira denetimin, pratikte yeterli hukuki donanıma sahip olmayan hizmet sağlayıcılar tarafından yapılması yerine, önceden belirlenen usul doğrultusunda sürecin sürdürülmesinin daha az hak ihlaline yol açacağını düşünmekteyiz. Bu çekince imkânı Protokolün 19. maddesinin 2. fıkrası uyarınca Taraflara tanınmıştır.

Bazı Tarafların trafik verilerinin üretilmesi ve bu tür verilerin elde edilmesi hususunda, kendi iç hukukları uyarınca kanunlarında ek gereklilikler bulunduğundan daha fazla bilgi gerektirebilir. 8. maddenin 4. fıkrası uyarınca Taraflar, 1. fıkra kapsamındaki emirleri yürürlüğe koymak için ek destekleyici bilgilerin gerekli olduğunu beyan edebilir, talepte bulunulan Taraf, 8. maddenin 3. fıkrasının b uyarınca sağlanan bilgilere ilişkin açıklama isteyebilir. Başka bir örnek olarak, bazı Taraflar, emrin bir savcı veya talepte bulunan Tarafın diğer adli veya bağımsız idari makamları tarafından verilmediği veya incelenmediği durumlarda ek bilgi talep edebilir. Taraflar, böyle bir beyanda bulunurken, gerekli ek bilgi türü konusunda mümkün olduğunca spesifik olmalıdır.[355] Bu beyan imkânı Protokolün 19. maddesinin 3. fıkrası uyarınca Taraflara tanınmıştır. Tarafların bu beyandan yararlanmasının olumlu etkilerinin olacağı düşüncesindeyiz.

3.1.3. Acil Durumlara İlişkin Düzenlemeler Hakkında

Protokolün 9. maddesi Tarafların çeşitli acil durumlarda, belirli cezai soruşturma veya kovuşturmalarda kullanılmak üzere, başka bir Taraf ülkedeki bir hizmet sağlayıcının mülkiyetinde veya kontrolünde saklanan bilgisayar verilerinin hızlı bir şekilde elde edilmesinin kolaylaştırılması ve bunun pekiştirilmesi ihtiyacının yansımasıdır. Bu madde doğrultusunda hem hizmet sağlayıcıdan hem de irtibat noktasından talepte bulunulabilir. 9. madde doğrultusunda, karşılıklı yardım talebi olmaksızın bilgisayar verilerinin ifşası talep edilebilecektir. Bu maddede düzenlenen "bilgisayar verisi" ifadesi yalnızca abone bilgilerini değil, depolanan içerik ve trafik verilerini de kapsayan, oldukça geniş bir terim kullanılmıştır. Bu geniş kapsamlı düzenleme, 7/24 İletişim Ağlarına ve hizmet sağlayıcılara oldukça fazla yük getirme eleştirisini de beraberinde getirebilmektedir. Taraflar için, 9. madde kapsamında, özellikle abone bilgilerine yönelik talepler almak, 7/24 İletişim Ağının kaynaklarını ve

[355] Protokole İlişkin Açıklayıcı Rapor, Art.137.

zamanını içerik veya trafik verileri taleplerinden uzaklaştırarak bu birimlere aşırı yük bindirme riskini taşımaktadır.

9. maddenin 1. fıkrasının b bendi uyarınca Taraflar, yalnızca abone bilgilerinin ifşa edilmesini amaçlayan 1. fıkranın a bendi kapsamındaki talepleri yerine getirmeyeceğini beyan edebilir. Bu çekinceden yararlanılması birimlerin üzerine düşen yükün hafifletilmesi sonucunu sağlayabilecektir. Bir diğer taraftan, abone bilgilerinin ifşasını düzenleyen 7. maddenin 9. fıkrasının a bendi uyarınca, 7. maddeyi uygulamama hakkını saklı tutan bir Tarafın bu çekinceden yararlanmasının tutarlı olacağı görüşündeyiz. Zira 7. madde ile getirilen çekince abone bilgilerinin 7. madde uyarınca ifşasının önüne geçecektir. Tarafların 7. maddesi için olan çekincesi 9. madde bakımından bir hüküm doğurmayacaktır.

Trafik verileri gibi daha hassas bilgilere ihtiyaç duyulduğu veya doğrudan hizmet sağlayıcıdan abone bilgilerinin alınmasına ilişkin prosedürün izlenmediği durumlarda, diğer ifadeyle acil durumlarda, yetkili kamu otoriteleri arasında kurulmuş iş birliği mekanizmalarından yararlanmak gerekecektir. Bu mekanizmaların amacı, talepte bulunulan ülkenin verilen veri aktarım emrinin yürütülmesini kolaylaştırmaktır. Böyle bir durumda, talep doğrudan hizmet sağlayıcıya değil, Protokole Taraf olan her ülke tarafından atanan belirlenmiş bir irtibat noktasına yönlendirilecektir.[356]

9. maddenin ilk fıkrasında karşılıklı yardım talebi olmaksızın bu ifşa talep edilebileceği ifade olunmaktadır. Bu maddenin 5. fıkrasında Taraflara; Talebin yerine getirilmesini takiben talebi ve bunu desteklemek için iletilen her türlü ek bilgiyi talep edilen Tarafça belirtildiği şekilde, karşılıklı yardımı da içerebilecek bir formatta ve bu tür bir kanal aracılığıyla sunmasını talep ettiğini beyan edebileceği şeklinde çekincede

[356] Rojszczak, s.1017.

bulunma imkânı tanınmıştır. Bu çekinceden yararlanılmasını talepte bulunan birimlerin ve talep usullerinin denetlenebilmesi bakımından yararlı görüyoruz.

Diğer önlemlerden farklı olarak, acil durum mekanizması, veriyi gönderen devletin topraklarında faaliyet gösteren hizmet sağlayıcılar tarafından tutulan her türlü bilgiyi, başka bir deyişle, yalnızca kullanıcı veya trafik verilerini değil aynı zamanda içerik verilerini de iletmek için kullanılabilir. Acil olmayan durumlarda, Protokolde getirilen tedbirler doğrultusunda, yetkililerin bu tür bilgileri elde etmesine izin verilmeyeceğinden, içerik verilerine erişme ihtiyacı duyan talep eden devletin yetkilileri diğer yasal mekanizmaları kullanmak zorunda kalacaklardır. Bu, Protokolde kurulan iş birliği mekanizmalarının bir elektronik iletişimi oluşturan verileri iletmek için kullanılabileceği tek durumdur.[357]

3.2. KİŞİSEL VERİLER İLE İLGILI DEĞERLENDİRMELER

Protokolde kişisel veriler ile ilgili olarak oldukça kapsamlı bir düzenleme getirilmiştir. Bu hususta bazı olumlu ve olumsuz değerlendirmeler mevcuttur. Protokolün uluslararası nitelikteki bir metin olması dolayısıyla, farklı ceza mevzuatı ve veri korumasıyla ilgili çok çeşitlilikte yasal sistemlere sahip pek çok katılımcı ülkenin varlığının gözetilerek asgari koruma standartlarını belirlendiği, ülkelerin belli uygulamalar için daha fazla koruma sağlayan mevzuatı uygulayabileceği esneklikte düzenlemelerin yapıldığını gözlemlemekteyiz. Zira bu çeşitlilik ve önem sebebiyle, Protokolde üzerinde en çok tartışılan madde olmuştur.[358] Her ülke bakımından özel bir düzenleme yapılmasının imkânsız olmasından ötürü, metin esnek bir dile sahiptir. Bu esneklik, veri korumasının yetersiz olduğu şekilde de yorumlanabilir. Bu yönüyle Protokolün, bazı Tarafların gerekli önlemleri aldığı, diğerler Tarafların ise en "verimli

[357] Rojszczak, s.1017.
[358] Bkz. Dipnot 175.

ve hızlandırılmış" prosedürlere ihtiyaç duyduklarına inandıkları için, en müdahaleci yöntemleri tercih ettiği iki aşamalı bir sistem oluşturduğu düşünülmektedir.[359]

Adli gözetimin asgari düzeyde olduğu ülkelerde sınır ötesindeki soruşturmalar insan haklarını tehdit edebilmektedir. Protokolün, yüksek standartlar oluşturmak yerine, neredeyse her fırsatta kolluk kuvvetlerinin erişimine öncelik verdiği ifade edilmektedir. Bu durumun en çok, AİHM ve Avrupa Konseyi'nin kendi veri koruma rejimi olan Kişisel Verilerin Otomatik İşlenmesine İlişkin Kişilerin Korunması Sözleşmesinin Tadil Protokolü olan 108+ Sözleşmesinin gerisinde kalan veri koruma standartlarını benimsemesinde ve gizlilik ile mahremiyet çıkarlarını önemsiz gösteren abone verilerine yaklaşımında açıkça görüldüğü ifade edilmektedir.[360]

EDPB, veri koruma tedbirlerine ilişkin özel hükümlerin temel ilkeleri ve özellikle yasallık, adalet ve şeffaflık, amaç sınırlaması, veri minimizasyonu, doğruluk, depolama sınırlaması, bütünlük ve gizliliği yansıtması gerektiğini düşünmektedir. Aynı şekilde, EDPB, orantılılık ilkesiyle sınırlı herhangi bir kısıtlama ve veri koruma güvencelerinin ihlalleri için veri sahipleri için etkili bir yargısal tazminat ile temel bireysel hakların (erişim, düzeltme, silme) sağlanmasının önemini vurgulamamıştır. Bu hakların kullanılması ayrıca, soruşturmayı riske atmadığından, en azından bir kez veri sahibinin bildirimini gerektirdiği ifade edilmiştir. Burada belirtilenler aynı zamanda, Konseyin Siber Suçlar Sözleşmesinin birçok Tarafının da taraf olduğu 108+ Sözleşmesi ile uyumlu olduğu ve 108+ Sözleşmesine uygun olarak, sürekliliği sağlamak için talepte bulunan Taraftaki verileri işleyen tüm makamlara uygulanması gerektiği ifade edilmektedir.[361]

---

[359] Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime, s.16, çevrimiçi, https://edri.org/files/TCY_Draft_2nd_Additional_Protocol_Civil_Society_Submission_20191107.pdf , Erişim Tarihi: 11.06.2022.
[360] Israel ve Rodriguez.
[361] Jelinek, s.5.

Protokolün kişisel verilerle ilgili 14. maddesinin 4. fıkrasında hassas kişisel veri niteliğindeki biyometrik veriler ile ilgili getirilen düzenleme, bu tür veri paylaşımı sürecinde için aleyhe yorumlanabilecek şekilde düzenlenmiştir. Madde metninde "ilgili riskler açısından hassas kabul edilen biyometrik veriler" ifadesi yer almaktadır. Buna göre, ülkeler riski kanıtlamadıkça, biyometrik verilerin hassas nitelikte kişisel veri olarak ele alınmayacağı ihtimalini de beraberinde getirmektedir.[362] 108+ Sözleşmesine göre yüz tanıma şablonları gibi biyometrik veriler hassas niteliktedir ve işlenirken ek koruma gerektirmektedir.[363] Bu yönüyle Protokol, 108+ Sözleşmesi ile çelişki içerisindedir.

Konseyin kişisel verilerin işlenmesine ilişkin 108+ Sözleşmesi ile olan çelişkili ve endişe verici eksiklikleri olduğu eleştirisi getirilmekte[364], Taraf ülkelerin kişisel verilerin işlenmesiyle ilgili olarak bireylerin korunması için güçlü bir veri koruması öngören 108+ Sözleşmesini öncelikli olarak imzalaması ve onaylaması gerektiği ifade edilmektedir.[365]

Tarafların, insan hakları ve özgürlüklerinin yeterli düzeyde korunmasını sağlamaları ve belirtilen uluslararası insan hakları metinlerinin belirttiği yükümlülüklerini yerine getirmeleri gereklidir. Zira, sınır ötesi kanıt toplama hususu devletlerin neredeyse günlük bir görevi haline geldiğinden, bu soruşturmaların insan haklarını ve mahremiyeti ilk sıraya koyacak şekilde yapılması zorunludur.[366] Baskıcı

[362] Israel ve Rodriguez.
[363] A.g.e
[364] Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime, s.16, çevrimiçi, https://edri.org/files/TCY_Draft_2nd_Additional_Protocol_Civil_Society_Submission_20191107.pdf , Erişim Tarihi: 11.06.2022.
[365] A.g.e. s.2.
[366] Israel ve Rodriguez.

rejimleri olan, güçlü veri koruma düzenlemeleri olmayan ve Konsey üyesi olmayan ülkelere veri aktarımı konusunda endişe vericidir.[367]

3.2.1. Yurtdışına Veri Aktarımı Bakımından Değerlendirme

İç hukukumuzda kişisel verilerin korunması ile ilgili olarak, KVKK ve bu Kanuna dayanan ikincil düzenlemelere tabi bulunulmaktadır. Protokol kapsamında, internet hizmet sağlayıcıların kullanıcıların kişisel verilerinin, bir ceza soruşturması veya kovuşturması kapsamında farklı ülkelerin adli makamları tarafından talep edilmesi ve hizmet sağlayıcıları verileri ilgili adli makama teslim etmesi durumu Kanunun 9. maddesinde düzenlenen kişisel verilerin yurt dışına aktarılması faaliyetini teşkil edecektir. Dolayısıyla, yabancı bir mahkemenin kanıt edinmek adına bir hizmeti sağlayıcısına göndereceği, kişisel verilerin teslimini gerektiren bir karar eğer Türkiye'de depolanan bir veriye ilişkinse KVKK'nın kriterlerini karşılamalıdır.[368]

KVKK'nın 9. maddesi kişisel verilerin yurt dışına aktarılmasını düzenlemektedir. Buna göre kural olarak, kişisel veriler ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. Ancak, kişisel veriler 5. maddenin 2. fıkrası[369] ile 6. maddenin 3. fıkrasında[370] belirtilen şartlardan birinin varlığı ve kişisel verinin

[367] LGBTQ+ bireylerin kullandıkları dating uygulamalarının hizmet sağlayıcı olarak kullanıcı verileriyle ilgili bilgi paylaşımı, bireylerin cinsel yönelimi hakkında bilgi verecek ve hassas nitelikli kişisel verilerin paylaşılması sonucu doğurarak bazı ülkelerde ayrımcılığa maruz kalmaları riski taşıyacaktır.
[368] Kalender, s.96.
[369] KVKK 5. maddenin 2. fıkrası; Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması. c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.
[370] KVKK 6. maddenin 3. fıkrası; Sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler

aktarılacağı yabancı ülkede yeterli korumanın bulunması veya yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. Yeterli korumanın bulunduğu ülkeler henüz ilan edilmemiştir. Protokolün onaylanmasından evvel, bu ülkelerin Kurul tarafından ilan edilmesi gerektiği düşünmekteyiz.

Diğer bir taraftan, Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve veri aktarımına izin verilip verilmeyeceği hususunda; Türkiye'nin taraf olduğu uluslararası sözleşmelerin, karşılıklılık durumunun, kişisel verinin niteliği ile işlenme amaç ve süresinin, aktarılacak ülkenin ilgili mevzuatı ve uygulamasının ile veri sorumlusu tarafından taahhüt edilen önlemlerin değerlendirileceği düzenlenmiştir. Protokolün imzalaması karşılıklılık unsurunu içerecek bir uluslararası sözleşme olarak kabul edilebilecektir. Aksi bir durum, diğer ülkelerin mahkemeleri ya da diğer kurumları tarafından verilmiş bir karar ile verilerin yurt dışına aktarılmasını hukuka aykırı hale getirecektir.

Yabancı ülke mahkemelerinin veya kurumlarının kararları doğrultusunda kişisel verilerin yurtdışına aktarılmasının; kişilerin verileri üzerindeki hâkimiyetlerini azaltacağı, hukuki yükümlülük tanımına ilişkin belirsizlik yaratacağı ve KVKK'nın başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak olarak belirtilen amacına aykırı olacağı ve haberleşme hürriyeti, savunma hakkı ve adil yargılanma hakkı gibi birçok temel hak ve özgürlüğüne zarar verebileceği düşünülmektedir.[371]

ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

[371] Kalender, s.97.

Bununla birlikte, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 4. maddesinin 2. fıkrası, kişisel veriler yurt dışına çıkarılamaz hükmünü amirdir. Dolayısıyla, Protokol kapsamında yurt dışına veri aktarımının hukuka uygun şekilde yapılabilmesi adına, Türk hukukunda yeniden düzenlemelere gidilmesi gerekmektedir.[372]

Türkiye Cumhuriyeti Anayasası, özel hayatın gizliliği ve haberleşme hürriyetinin milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi gibi hâllerde usulüne göre verilmiş hâkim kararı üzerine sınırlanabileceğini düzenlemektedir. Zira, yabancı mahkeme ya da kolluk kuvvetlerince verilecek kararların, usulüne göre verilmiş hâkim kararı niteliğini haiz olmayacaktır, dolayısıyla özel hayatın gizliliği ve haberleşme hürriyetinin sınırlanması için mevzuatın günümüzdeki hali yeterli değildir. KVKK'ya tabi internet hizmeti sağlayıcılarının Protokol doğrultusunda yurt dışına veri aktarımında bulunmalarının hukuka aykırı uygun olması için mevzuatta güncellemeler yapılması gerektiğini düşündüğümüzü önemle vurgulamak isteriz.

3.3. TEMSİL VE DİĞER MADDELER BAKIMINDAN DEĞERLENDİRME

Her ne kadar pek çok Taraf ülke olsa dahi Avrupa Konseyi'nin sürdürdüğü çalışmalar küresel temsilde yetersizdir. Sınır tanımayan nitelikteki siber suçlar ve verilerin doğası gereği BM gibi daha fazla ülkeye hitap edebilecek kuruluşun da bir an önce böylesi bir çalışmayı hayata geçirmesi gerektiği düşüncesindeyiz, mümkün olduğunca çok sayıda ülkenin katılımı gereklidir. Zira, Rusya ve Çin gibi siber suçların en yoğun gözlemlendiği ülkelerin Sözleşmeye ve Protokole taraf olmaması durumu, siber suçluların güvenli limanlardan dünyanın her yerindeki kurbanlarına zarar verebilecek faaliyetlerini sürdürmesine olanak sağlayacaktır.

[372] Kalender, s.99.

Video konferans yönteminin getirilmesi hem savunma hakkına hizmet ederken, diğer taraftan teknolojinin getirdiği yeniliklerden de adalet temininde faydalanılabileceğini bizlere sunmaktadır. Dil ile ilgili olarak getirilen düzenlemenin, sık konuşulmayan dillerle ilgili tercüme hatası ve masraflarıyla ilgili olumsuzlukların önüne geçilebileceğini göstermektedir. İş birliğinin reddedilmesi durumunda bunun sebebinin raporlanacağı ile ilgili olarak getirilen yeniliklerin, uluslararası hesap verilebilirlik bakımından Taraflara sorumluluk yüklediğini ve iş birliğini sağlanmasına hizmet edebileceği düşünülmektedir. Son olarak, Protokolün getirdiği en önemli yeniliğin, verilerin ve elektronik kanıtların çoğunlukla özel sektörün mülkiyetinde olması dolayısıyla, kamu ve özel sektör arasında doğrudan iş birliği için getirmiş olduğu düzenlemelerdir.

SONUÇ

Siber suçların bireylerin mahremiyetini engelleyebileceği gibi, kötücül yazılımlar gibi yollarla kritik altyapılara, terörist saldırılara dahi sebebiyet vereceği yaşanılan vakıalar ile önümüze sunulmuştur. İnternet iletişimi doğrultusunda işlenen veya kanıtları dijital ortamda olan klasik suçlara ilişkin soruşturma ve kovuşturmalar, yapısının hareketliliği, birbirine bağlı olması ve bölünebilirliği sebepleriyle fazlaca teknik ve yasal komplikasyona yol açmaktadır.[373]

Egemen eşitliği ilkesi ve Doktrinin sınırlarında işlenen suçlara yönelik ceza adaletini temin için bazı makul tavizler vermek sadece kaçınılmaz değil, aynı zamanda çok ciddi riskler doğuran siber suçların dünyasında uluslararası düzeni ayakta tutmaya çalışırken de kesinlikle gereklidir.[374] Zira siber dünya ve veri alanı, aynı zamanda egemen güç alanının dışında işleyen bir fikir, etki, ticaret ve yaratıcılık alanıdır, maddi olmayan ve fiziksel kaynağın kendisinden bağımsız, farklı kurumlar ve bölgelerle ilişki oluşturan değerler üretmektedir[375] ve bununla paralel olarak siber güvenlik teminini oldukça zorlaştırmaktadır. Bir egemenin başkalarını dışlama hakkına ilişkin geleneksel anlayışı, uzaktan aramalar ve el koymalar için ortaya çıkan yeni teknolojiler karşısında biraz çağdışı gelmeye başlayabilir.[376] Klasik yargı yetkisi uygulamaları veri temelli yargılamalarda adalete erişmek için oldukça yetersiz kalmaktadır. Ülkeselliği belirsiz olan veri ile ilgili olarak, ülke egemenliği ilkesini körü körüne savunmak, ceza adaletinin tesis edilmemesi, suçluların cezasız kalması riskini doğurur. Burada hassas bir denge vardır, bir ilkenin yok sayılması mümkün değildir. Bu sebeple uluslararası nezaket ve iş birliği yükümlülüklerine özen gösterilmelidir.

---

[373] Daskal, Jennifer. 2015. The Un-Territoriality of Data, 125 Yale Law Journal, s.331.
[374] Lubin, s.3.
[375] Bergé, J-S., Grumbach, S. & Zeno-Zencovich, V., *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, (2018) 5(2) Eur. J. Comp. L. & Gov 5(2), s.144.
[376] Svantesson, Dan. *Preliminary Report: Law Enforcement Cross-border Access to Data*, 2016, çevrimiçi, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238, Erişim Tarihi: 22.05.2022.

Kanıtların çoğunlukla sınırlar ötesinde tutuluyor olması, veri konumu üzerindeki yargı yetkisi anlayışından uzaklaşmayı ve yenilikler getirilmesini gerektirmiştir. Dijitalleşme ve bulut bilişimin yükselişinden dolayı, ceza soruşturmaları Sözleşmenin hazırlandığı tarihteki gibi vuku bulmamaktadır. İşlenen suçlar karşısında kolluk kuvvetleri ve adli makamların, bulundukları ülkeden farklı kurallara bağlı özel taraflardan elektronik kanıt elde etme ihtiyacıyla karşı karşıya kalmaktadırlar. Bu durum, yeni bir yasal çerçevenin merkezine, hizmet sağlayıcılarla doğrudan ilişkiye uzanan adli iş birliği mekanizmalarının güçlendirilmesini yerleştirmektedir.[377] Bir suçun aydınlatılması için gerekli olan verilerin ve bilgilerin, özel yapıları olan internet sağlayıcıların ve kuruluşların ekosisteminde olması yalnızca ülkelerin değil, aynı zamanda kamunun özel sektörle de iş birliğini gerektirmektedir. Bunun sonucu olarak, sınırlar ötesindeki elektronik kanıtların elde edilmesine odaklanan ve kamu otoritelerinin özel şirketler tarafından tutulan verilere erişiminin kolaylaştırılması amaçlayan Protokol metni oluşturulmuştur.

En çarpıcı ve kapsamlı hüküm, bir ülkedeki kolluk kuvvetlerinin resmi kanallardan geçmeden başka bir ülkeden doğrudan abone bilgilerini talep edebileceği bir mekanizma öngörülmesidir. Her ne kadar Protokolde orantılılık ilkesi ve insan haklarını koruyan uluslararası anlaşmalara atıflar yapılmış olsa da kolluk kuvvetlerinin doğrudan hizmet sağlayıcılardan veri elde etmesi, hükümetlerin bu yetkilerini kötüye kullanması ile ilgili endişeleri de beraberinde getirmektedir. Tüm ülkelerin yakın gelecekte fikir birliğine varılmasının muhtemel olmadığını da kabul etmeliyiz.[378] Teknoloji, Cenevre veya New York'ta çok taraflı diplomasiden daha hızlı hareket ediyor.[379] Doktrinin sınırlarında bazı makul tavizler vermek sadece kaçınılmaz değil, aynı zamanda çalkantılı siber dünyada düzeni sağlamak için kesinlikle gereklidir.

---

[377] Spiezia, s.4.
[378] Currie, Robert J. *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*.
[379] Lubin, s.17.

Her sınır ötesi veri aktarımı iki ana aşamadan oluşmaktadır. Birincisi, veri aktarımı talebidir. Bu aşama talep eden devlette ulusal hukuka uygun olarak, ilgili usul makamlarının kontrolü altında gerçekleştirilir. Düzenleyen makamın rolü, kolluk kuvvetleri tarafından talep edilen bilgilerin elde edilmesine ilişkin kriterlerin karşılanmasını sağlamaktır. İsteğin yürütülmesi ile ilgili ikinci aşama, iletim durumunda gerçekleştirilir. Kabul edilen iş birliği modeline bağlı olarak bu aşama ya gönderen devletin kamu makamlarının zorunlu katılımını içerebilir veya hizmet sağlayıcısı gibi yükümlü kuruluşa iletilen talepleri doğrudan yerine getirme yükümlülüğü getirebilir. Ancak ikinci durumda, gönderen devlette yürürlükte olan yasal model dikkate alınarak, talep edilen bilgilerin sağlanmasına yasal olarak izin verilip verilmediğini değerlendirmenin özel kuruluşun görevi olup olmadığı konusunda şüphe ortaya çıkar. Bu konuda uygun bilgi ve yetkinliğe sahip olma gerekliliği göz ardı edilse bile, böyle bir gözetimin uygulanması, fiilen yükümlü varlığı fiilen bir hak koruma makamı haline getirecektir. Böyle bir yaklaşımla, kamu makamlarının usulsüz müdahalesine karşı koruma, özel bir kuruluş tarafından gerçekleştirilecek ve bu da ceza adaleti sisteminin belirli unsurlarının fiili olarak özelleştirilmesine ilişkin haklı suçlamalara yol açacaktır.[380]

Protokolde öngörülen her mekanizmada hem esasa ilişkin hem de usule ilişkin olmak üzere farklı yasal güvenceler getirilmiştir. Buna rağmen, bu güvencelerin yeterli kabul edilip edilemeyeceği konusunda şüpheler mevcuttur. Yetkinin kötüye kullanılması riskine karşı bireylerin haklarını korumaya yeterli, uluslararası elektronik delil alışverişi alanında uygulanabilir ulus ötesi ortak bir yasal güvence standardı geliştirmenin mümkün olup olmadığı temel sorudur. Taraflara çekince ve beyanlarda bulunma imkânı tanınmıştır, verilerin hukuka uygun olarak alışverişinin yapılması, kanıtların hukuka uygunluğunun sağlanması ve hak ihlallerinden kaçınılması için Taraflar bu şekilde de önceden önlem alabilmektedirler.

[380] Rojszczak, s.1002.

Adil yargılanma hakkına saygı, veri taleplerinin sadece talep eden devlette değil, aynı zamanda ileten devlette de incelemeye tabi olmasını gerektirebilir. Unutulmamalıdır ki, birçok yasal modelde elektronik kanıt elde etmek için yargısal yetkiye gerek yoktur. Talep edilen bilgilerin niteliğine bağlı olarak, bu tür kararlar bir savcı ve çoğu zaman soruşturma makamları tarafından da alınabilir. Bu nedenle, veri aktarımı talebine izin verilip verilmeyeceğine ilişkin bir kararın yalnızca talepte bulunan ülkede yürürlükte olan prosedüre dayandırılması veri aktarımının bağımsız bir kuruluş tarafından herhangi bir gözetime tabi olmayacağı bir duruma yol açabilir. Bu konuyla ilgili Protokolün izin verdiği çekince imkânları gözden geçirilmelidir. Öte yandan, gönderen devletteki izinlerin herhangi bir şekilde gözden geçirilmesi, doğrulama prosedürünün önemli ölçüde uzamasına yol açar.[381]

Her ülkenin insan haklarına, kamu düzenine ve adalet sistemine bakış açılarında ideolojik farklılıklar olabilmektedir. Bu çeşitli sebeplerle ortaya çıkan durum karşısında ülkelerin ceza soruşturması ve kovuşturmasındaki tutumlarında birbirlerinden farklılık gösterebilmektedir. Sözleşme ve Protokol tarafı olmaları dolayısıyla birbirleriyle iş birliği içinde olacak olan ülkelerin paylaştığı veya edindiği verilere ilişkin farklı düzeyde koruma sağlayan düzenlemeleri ve uygulamaları bulunabilecektir. Örneğin, bireyi ön plana koyan İskandinav ülkeleri ile üçüncü dünya ülkelerinin uygulamaları arasında pek çok bakımdan fark olacaktır.

Ülkelerin sınırları ötesi uygulama yetkisine ilişkin genel yasağa ilişkin istisnaların getirilmesi pek çok risk de oluşturabilir. Ancak, tek başına bu yasak, ülkeleri ileriye götürmek yerine, otoriter ülkelerin güçlerini artırması işlevi görür.[382]

---

[381] Rojszczak, s.1004. "Örneğin, Polonya'da, Polonya Ceza Muhakemesi Kanununa göre, Madde 218a, hizmet sağlayıcı tarafından tutulan elektronik verilerin sağlanması savcının onayını gerektirirken, Polonya Polis Yasasına göre, Madde 20c(1), elektronik iletişimden elde edilen meta (üst) veriler söz konusu olduğunda soruşturma makamının kararı yeterlidir.

[382] Parrish, Austen L. *The Interplay between extraterritoriality, sovereignty, and the foundations of international law, In The Extraterritoriality Of Law: History, Theory, Politics*, 169, 177-178 (Daniel Margolies, Umut Özsu, Maia Pal, & Ntina Tzouvala eds., 2019)

Bu nedenle, siber suçlarla mücadelede daha fazla iş birliği için çok taraflı çaba, girişim ve iş birliği sağlanmalıdır. Suça ilişkin soruşturma ve kovuşturmalarda ortak kural ve rejimlerin geliştirilmesi teşvik edilmelidir. Ancak bu iş birliğinin suistimal edilmemesi, kişilerin temel hak ve özgürlüklerine karşı hassas bir tutum sergilemek gereklidir.

Protokol aracılığıyla gerçekleşen iş birliği taleplerinin belirli bir ülkeden geldiği için reddedilmesi, en geniş ölçüde iş birliğini hedefleyen bu metinlerin ruhuna aykırı olacaktır. Ancak, belirli durumlarda Sözleşme ve Protokol Taraflara karşılıklı yardımı reddetme imkânı tanımaktadır. Sözleşmenin 25. maddesinin 4. fıkrası uyarınca, karşılıklı yardımda bulunma, kendisinden talepte bulunulan Tarafın yasalarındaki veya uygulanabilir karşılıklı yardımlaşma anlaşmalarındaki şartlara bağlı olacaktır. Özellikle 108+ Sözleşmesine aykırılık teşkil eden taleplerde, bu hükmün ilgili Taraflarca sıklıkla kullanılacağı düşüncesindeyiz. Sözleşmenin 27. maddesinin 4. fıkrası uyarınca yardım talebine konu olan suçun kendisinden talepte bulunulan Taraf ülkece siyasi suç veya siyasi suçla bağlantılı suç olarak değerlendirilmesi veya söz konusu talebin gereğinin yerine getirilmesinin kendisinden talepte bulunulan taraf ülkece kendisinin egemenliğine, emniyetine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğinin düşünülmesi durumunda Taraflara iş birliği talebini reddetme imkânı olarak tanınmaktadır.

Protokol, veri egemenliği yaklaşımı, kanun yaptırımları da dahil olmak üzere veriler üzerinde kontrol sağlamanın bir aracı olarak çerçevelenmiştir. Verilerin sınırlar arasında akmaya devam ettiği bir dönemdeyiz ve önceden belirlenmiş yetki sınırlarını karşılamak için teknoloji üzerinde bu kuralları uygulamaya çalışmak yerine, yargı kurallarını teknolojinin bu yeni kurallarına uyacak şekilde uyarlamaya çalışmak, bir diğer taraftan da kişilerin temel hak ve özgürlüklerini göz önünde tutarak dengeli bir uygulama sürdürmek en yapıcı çözümdür. Bu yönüyle Protokolün ne ölçüde başarılı olduğunu ve amaçlarına hizmet edip etmediğini hep birlikte ilerleyen dönemde gözlemleyeceğiz. Protokolün düzenlediği konular insan haklarının korunması ve

adaletin sağlanması arasında hassas denge oluşturmaktadır. Protokolün yürürlüğe girmesi durumunda iç hukukun uyumlaştırılması, mağdurlar için daha fazla adalet sağlama ve failler için hesap verme sorumluluğu yerine getirilirken insan haklarını gereklilikleri de ihmal edilmemelidir.

KAYNAKÇA

Akdeniz, Yaman. An Advocacy Handbook for the Non Governmental Organisations, The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems, 2003, updated and revised in May 2008. https://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf, çevrimiçi, 10.04.2022.

Akkutay, Berat Lale. 1982 Birleşmiş Milletler Deniz Hukuku Sözleşmesi Çerçevesinde Çekinceler ve İhtiyari İstisnalar. Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni 31 (2012), https://dergipark.org.tr/tr/download/article-file/410903, çevrimiçi, Erişim Tarihi: 27.08.2022.

Akpek, Nusret Onur. Siber Suçlar Sözleşmesinin Getirdikleri ve Iç Hukuk Açısından Konuya Yaklaşım. İstanbul Bilgi Üniversitesi, 2015.

Alimonti, Veridiana. Assesing New Protocol to the Cybercrime Convention in Latin America. Concerns, Human Rights Considerations, and Mitigation Strategies, Mayıs 2022, https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf, çevrimiçi, Erişim Tarihi: 12.06.2022.

Aliusta, Cahit / Benzer, Recep. 2018. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:4, No:2.

Allan, Gregor. "Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative." New Zealand Law Review. 2005(2).

Alvarez - Machain v. US [2003] 9th Cir, 331 F 3d 604 (Lacking Extraterritorial Enforcement Under The Controlled Substances Act To Abduct The Plaintiff From

Mexico), https://casetext.com/pdf-sent?slug=alvarez-machain-v-us-5, çevrimiçi, Erişim Tarihi: 29.05.2022.

Arınmış Uzun, Sündüs. "Türkiye'de Kişisel Verilerin Korunması ve Vatandaş Algısının Ölçülmesi", Bilişim Teknolojileri Dergisi, Cilt: 14, Sayı: 3, Temmuz 2021, https://dergipark.org.tr/en/download/article-file/1097727, çevrimiçi, Erişim Tarihi: 02.11.2022.

Bergé, J-S., Grumbach, S. & Zeno-Zencovich, V., 'The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance' (2018) 5(2) Eur. J. Comp. L. & Gov 5(2).

Bostancı, Ümit / Benzer, Recep. "Türk hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma / Search, Copy And Seizure On The Computers In The Turkish Legal System", International Journal of Human Sciences, sy.12, 2015, https://www.idealonline.com.tr/IdealOnline/pdfViewer/index.xhtml?uId=38281&ioM=Paper&preview=true&isViewer=true#pagemode=bookmarks, çevrimiçi, Erişim Tarihi: 24.09.2022.

Brière, Chloé. EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments." European Papers, 2021 6 (1), doi:10.15166/2499-8249/479.

Cemil, Kaya. Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler Ve Işlenmesi. Journal of Istanbul University Law Faculty 69, No. 1-2 (2011): 318.

Currie, Robert J. Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?.

Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, State of play, 8 July 2019, T-CY (2019)19.

Cybercrime Convention Committee, Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, Provisional text of provisions, 8 November 2019, T-CY (2018)23, 15

Dal, Seniha. Türk Hukukunda İnternet Alan Adları (Domain Names) ve Bu Alandaki Son Gelişmeler, Marmara Üniversitesi İİBF Dergisi, Cilt XXVIII, Sayı I, 2010. https://dergipark.org.tr/tr/download/article-file/3558, çevrimiçi, Erişim Tarihi: 27.03.2022.

Daskal, Jennifer. 2015. The Un-Territoriality of Data, 125 Yale Law Journal.

Delerue, François. 'Covid-19 and the Cyber Pandemic: A Plea for International Law and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace' in T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.). 2021. https://ccdcoe.org/uploads/2021/05/CyCon_2021_Delerue.pdf, çevrimiçi, Erişim Tarihi: 29.05.2022.

Dülger, Murat Volkan. "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in Getirdikleri ve Dikkat Edilmesi Gereken Hususlar (The Issues Brought To Be Considered By The Regulation On The Deletion, Destruction Or Anonymization Of Personal Data)." Available at SSRN 3792237 (2021). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792237, çevrimiçi, Erişim Tarihi: 10.05.2022

Dülger, Volkan Murat. Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi.

Erdem, Merve / Özocak, Gürkan. "Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği, 19. Akademik Bilişim Konferansı, 8-10 Şubat 2017, Aksaray Üniversitesi, Aksaray.

Erdem, Merve / Özocak, Gürkan. "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü." Ankara Üniversitesi Hukuk Fakültesi Dergisi 68, no.1 (2019).

Erdoğan, Yavuz. Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri, Legal Yayıncılık, 2018.

Esposito, Luca G. The Council Of Europe Convention on Cyber-Crime: A Revolutionary Instrument?, in Broadhurst, Roderic. (Ed.), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, Hong Kong, 2004.

İçel, Kayıhan. Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuku Fakültesi Mecmuası (İÜHFM) Cilt: LIX Sayı:1-2, 2001. https://dergipark.org.tr/en/download/article-file/95984, çevrimiçi, Erişim Tarihi: 29.05.2022.

Jelinek, Andrea. Statement 02/2021 On New Draft Provisions Of The Second Additional Protocol To The Council Of Europe Convention On Cybercrime (Budapest Convention).https://edpb.europa.eu/sites/default/files/files/file1/statement022021onbudapestconventionnewprovisions_en.pdf, çevrimiçi, Erişim Tarihi: 09.04.2022

Kalender, Ata Umur. "Parçalı Bulutlar: Cloud Act ve Etkileri" Kişisel Verileri Koruma Dergisi, 2020. https://dergipark.org.tr/tr/download/article-file/1121221, çevrimiçi, Erişim Tarihi:10.04.2022.

Karagülmez, Ali. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 3. Baskı, Ankara, 2011.

Keskin Kiziroğlu, Serap, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1-2. https://0-dergipark-org-tr.opac.bilgi.edu.tr/tr/download/article-file/95999, çevrimiçi, Erişim Tarihi: 13.02.2022.

Keyser, Mike. The Council of Europe Convention on Cybercrime. Journal of Transnational Law & Policy 12 (2), 2003.

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 30224 sayılı ve 28.10.2017 tarihli Resmi Gazete'de yayınlanmıştır.

Koyuncu, Emel / Mustafa Coşar. "Hastane Bilgi Sistemlerinin Yetkilendirme Düzeyli Güvenlik Değerlendirmesi" Hitit Ekonomi ve Politika Dergisi, Mart 2022, Cilt:2, Sayı:1. www.cdn.hitit.edu.tr/hepdergi/files/67874_2203291127809.pdf, çevrimiçi, Erişim Tarihi: 10.05.2022.

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

Lubin, Asaf. The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere (2022). Handbook on Extraterritoriality in International Law (Austen L. Parrish and Cedric Ryngaert eds., forthcoming, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4012007, çevrimiçi, Erişim Tarihi: 16.05.2022.

Gercke, Marco. Understanding Cybercrime: Phenomena, Challenges and Legal Response. (2013). Review of Information & Communications Technology & Development in the Arab Region, 18.

Gulyass, Attila (2021). Dark Web Investigation: edited by Babak Akhgar, Marco Gercke, Stefanos Vrochidis, and Helen Gibson, Switzerland AG, Springer Nature, 2021, ISBN 978-3-030-55342-5, $141.67(hardback), 305 pages. Terrorism & Political Violence, 33(8).

Nacar, Fatma Burcu. Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları. İstanbul Atılım Üniversitesi, 2010. http://cdn.legalbank.net/pdf/e4cce3daacbc42dc8a38f00d22852f94.pdf, çevrimiçi, Erişim Tarihi: 24.09.2022.

Önok, Murat. Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof.Dr. Nur Centel'e Armağan, MÜHFHAD, sy.19/2.

Özbek, Mücahit. Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma, Galatasaray Üniversitesi, 2015.

Özen, Muharrem / Baştürk, İhsan. Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

Özman, Mehmet Aydoğan. Milletlerarası Anlaşmalarda Çekinceler: (Ihtirazi Kayıtlar). Ankara Üniversitesi Hukuk Fakültesi Yayınları, No.259, 1970. https://0-search-ebscohost-com.opac.bilgi.edu.tr/login.aspx?direct=true&db=nlebk&AN=703079&site=eds-live, çevrimiçi, Erişim Tarihi: 27.08.2022.

Parrish, Austen L. 2019. The Interplay between extraterritoriality, sovereignty, and the foundations of international law, in The Extraterritoriality Of Law: History, Theory, Politics, 169, 177-178 (Daniel Margolies, Umut Ozsu, Maia Pal, & Ntina Tzouvala eds., 2019))

Plachta, Michael. Council of Europe Has Adopted the Second Protocol to the Cybercrime ('Budapest') Convention." International Enforcement Law Reporter 37 (12): 494, 2021.

Rojszczak, Marcin. E-Evidence Cooperation in Criminal Matters from an EU Perspective. The Modern Law Review, DOI: 10.1111/1468-2230.12749, 2022. https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12749, çevrimiçi, Erişim Tarihi: 29.09.2022.

Spiezia, Filippo. International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime. ERA Forum (2022) 23:101–108. 04.04.2022. https://link.springer.com/content/pdf/10.1007/s12027-022-00707-8.pdf, çevrimiçi, Erişim Tarihi: 11.06.2022.

Svantesson, Dan. 2016, Preliminary Report: Law Enforcement Cross-border Access to Data, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874238, çevrimiçi, Erişim Tarihi: 22.05.2022.

Uçkan, Özgür / Beceni, Yasin. 2004. Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

Vatis, Michael A. The council of Europe convention on cybercrime." In Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for US policy, 2010.

Weber, Amalie M. The Council of Europe's Convention on Cybercrime. Berkeley Tech-nology Law Journal 18, no.1, 2003.

6. Cloud Evidence Group: Terms of Reference for the preparation of a draft Protocol to the Budapest Convention, 17th Plenary Meeting of the Cybercrime Convention Committee (T-CY), Council of Europe (June 2017)

ELEKTRONİK KAYNAKLAR

1981 Tarihli Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, (çevrimiçi) https://inhak.adalet.gov.tr/Resimler/Dokuman/2712020140848108_tur.pdf, Erişim Tarihi: 10.05.2022.

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), (çevrimiçi) https://rm.coe.int/168008160f, Erişim Tarihi: 10.04.2022.

Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağı ve Açıklayıcı Memorandumu / Hazırlayan: Siber Suç Uzmanları Komitesi, Çevirisi: İnternet ve Hukuk Platformu, Ankara Barosu, 2008, 3.Baskı, sayfa 79, (çevrimiçi) http://www.ankarabarosu.org.tr/siteler/1940-2010/kitaplar/pdf/a/sibersuclar.pdf, Erişim Tarihi: 27.12.2021.

The Budapest Convention and Its Protocols, COE INT., (çevrimiçi) https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[2],%22105166442%22:[2]}, Erişim Tarihi: 04.02.2022.)

Chart of signatures and ratifications of Treaty 224, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Status as of 12/06/2022, (çevrimiçi), https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224, Erişim Tarihi: 12.06.2022.

Check Point, The 5 Most Expensive Phishing Scams of all Time, (çevrimiçi), https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/, Erişim Tarihi: 13.01.2022.

Commission Staff Working Document, Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules of the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, European Commission, (17.04.2018), (çevrimiçi), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN, Erişim Tarihi: 11.06.2022.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No. 108, Strasbourg, 28 January, 1981, (çevrimiçi) https://rm.coe.int/1680078b37#:~:text=The%20purpose%20of%20this%20Convention,(%22data%20protection%22), Erişim Tarihi: 10.05.2022.

Concerning a Given, COE INT., (çevrimiçi) https://www.coe.int/en/web/conventions/concerning-a-given-treaty,
Erişim Tarihi: 18.03.2022.

Cybercrime Convention Committee (T-CY) Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, (18.05.2021), COE INT., (çevrimiçi) https://rm.coe.int/0900001680a2aa1dVersion, Erişim Tarihi: 18.04.2022.

Cybercrime Convention Committee (T-CY) Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic

evidence Explanatory Report, COE INT., (çevrimiçi) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a48e4b, Erişim Tarihi: 17.04.2022.

Cybersecurity in the EU: A strategic priority for 2021-2027, Marie Christine Noujaim, A Grants Office Publication, September 2021, Volume 1, Issue 2, (çevrimiçi) https://www.grantsoffice.com/Portals/0/funded/issues/FUNDEDOct2021.pdf, Erişim Tarihi 26.12.2021.

Daskal, Jennifer ve Kennedy-Mayo, Debrae, Budapest Convention: What Is It And How Is It Being Updated? (02.07.2020), (çevrimiçi), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/, Erişim Tarihi: 11.06.2022.

Details of Treaty No.185, COE INT., (çevrimiçi) https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185, Erişim Tarihi: 23.01.2022.

Draft Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Committee on Legal Affairs and Human Rights, Rapporteur: Mr. Kamal JAFAROV, Azerbaijan, EC/DA Origin - Reference to committee: Doc. 15316, Reference 4593 of 21 June 2021. 2021 - Fourth part-session, Report | Doc. 15379 | 28 September 2021, (çevrimiçi) https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=29475&lang=en, Erişim Tarihi: 22.05.2022.

EFF Comments on Additions to Budapest Protocol on Cybercrime, Joint Civil Society Response to the Provisional Draft Text of the Second Additional Protocol to the

Budapest Convention on Cybercrime (çevrimiçi) https://www.eff.org/document/eff-comments-additions-budapest-protocol-cybercrime, Erişim Tarihi: 11.06.2022.

Enhanced Cooperation and Disclosure of Electronic Evidence, COE INT., (çevrimiçi) https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention#:~:text=Following%20almost%20four%20years%20of,the%20framework%20of%20an%20international, Erişim Tarihi: 25.05.2022.

Explanatory Report to the Convention on Cybercrime, II. The Preparatory Works, COE INT., (çevrimiçi) https://rm.coe.int/16800cce5b, Erişim tarihi: 27.12.2021.

Federal Bureau of Investigation, Internet Crime Report, 2021, (çevrimiçi), www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf, Erişim Tarihi: 30.05.2022.

Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans, (21.07.2021) Gartner, (çevrimiçi) https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we, Erişim Tarihi: 25.11.2021.

Gelişmiş İşbirliği ve Elektronik Kanıtların İfşasına İlişkin Siber Suç Sözleşmesine İkinci Ek Protokol, (çevrimiçi) https://rm.coe.int/turkish-2nd-ap-to-the-bc-nov-2021/1680a55b47, Erişim Tarihi: 13.02.2022.

Groll, Elias. Cyberattack Targets Safety System at Saudi Aramco (21.11.2017) Foreign Policy, (çevrimiçi) https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/, Erişim Tarihi: 28.01.2022.

Growth in United Nations membership, UN, (çevrimiçi) https://www.un.org/en/about-us/growth-in-un-membership, Erişim Tarihi: 07.02.2022.

'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on, (04.05.2020), CNN Business, (çevrimiçi) https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html, Erişim Tarihi: 13.03.2022.

International Idea, Is E-Voting Currently Used In Any Elections With Emb Participation?, (çevrimiçi) https://www.idea.int/data-tools/question-view/742,, Erişim Tarihi: 04.02.2022.

Israel, Tamir ve Rodriguez, Katitza. On New Cross-Border Cybercrime Policing Protocol, a Call for Caution, Just Security. (13.05.2022), (çevrimiçi), https://www.justsecurity.org/81502/on-new-cross-border-cybercrime-policing-protocol-a-call-for-caution/, Erişim Tarihi: 11.06.2022.

İnternet Alan Adları Genel Bilgi, (06.10.2020) BTK, (çevrimiçi). https://www.btk.gov.tr/internet-alan-adlari-genel, Erişim Tarihi: 26.03.2022.

Malaja, Polina. EU Policy Update – October 2021 (10.11.2021), Centr Org, (çevrimiçi) https://www.centr.org/news/eu-updates/october-2021.html, Erişim Tarihi 26.12.2021

Our member States, COE INT., (çevrimiçi) https://www.coe.int/en/web/about-us/our-member-states?desktop=true, Erişim Tarihi: 13.02.2022.

PACE's Kamal Jafarov on the Draft Second Additional Protocol to the Convention on Cybercrime, (04.10.2021) YouTube, (çevrimiçi) https://www.youtube.com/watch?v=r9zbJTrH2mc, Erişim Tarihi: 08.04.2022.

Permanent Court Of International Justice Twelfth (Ordinary) Session The Case Of The S.S. Lotus France V. Turkey Judgment, (S.S. Lotus Davası, Fransa-Türkiye 1927, PCIJ), (07.09.1927), (çevrimiçi) http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm, Erişim Tarihi: 16.05.2022.

Ransomware Exploits and Supply Chain Attacks Lead the Cyber Trends in the First Half of 2021, (çevrimiçi) https://pages.checkpoint.com/cyber-attack-2021-trends.html, Erişim Tarihi: 27.12.2021.

Reservations and Declarations for Treaty No.224 - Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Status as of 11/10/2022, (çevrimiçi), www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=224&codeNature=0, Erişim Tarihi: 11.10.2022.

Sanal Ortamda İşlenen Suçlar Sözleşmesi, (çevrimiçi) https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf, Erişim Tarihi: 31.01.2022

Seger, Alexander. A new Protocol to the Convention on Cybercrime: For a more effective criminal justice response to crime online-with strong safeguards, (11.11.2021), (çevrimiçi), https://www.linkedin.com/pulse/new-protocol-convention-cybercrime-more-effective-criminal-justice-/?trackingId=CnjE%2BxAERiKTr26OaLL2LA%3D%3D, Erişim Tarihi: 11.06.2022.

Shaping Europe’s Digital Future, Cybersecurity Policies, (çevrimiçi) https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies,

Erişim Tarihi:27.12.2021.

The 5 Most Expensive Phishing Scams of all Time, (çevrimiçi) https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/the-top-5-phishing-scams-of-all-times/, Erişim Tarihi: 13.01.2022.

The Council of Europe Guidelines for the protection of individuals with regard to the collection and processing of personal data on information highways adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers, Deputies, (çevrimiçi) http://cm.coe.int/ta/rec/1999/99r5.htm, Erişim Tarihi: 18.04.2022.

Top 20 Countries Found to Have the Most Cybercrime, (çevrimiçi) https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/, Erişim Tarihi: 07.02.2022.

T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group, (17.02.2016), COE INT., (çevrimiçi) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8, Erişim Tarihi: 17.04.2022.

T-YC (Draft) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, (01.07.2017), COE INT., (çevrimiçi) https://rm.coe.int/-draft-terms-of-reference-for-the-preparation-of-a-draft-2nd-additiona/168071b794, Erişim Tarihi: 19.04.2022.

U.S. Congress Clarifying Lawful Overseas Use of Data – CLOUD Act, (26.01.2022), The United States Department of Justice, (çevrimiçi) https://www.justice.gov/dag/cloudact, Erişim Tarihi: 08.03.2022.