SİBER SUÇLAR SÖZLEŞMESİNİN GETİRDİKLERİ
VE
İÇ HUKUK AÇISINDAN KONUYA YAKLAŞIM

INSIGHTS INTO THE CONVENTION ON CYBERCRIME
AND
THE APPROACH IN TERMS OF DOMESTIC LAW

Nusret Onur AKPEK
110692029

Doç. Dr. Leyla KESER BERBER	:	
Dr. Nilgün BAŞALP	:	
Dr. Mehmet Bedii KAYA	:	
Tezin Onaylandığı Tarih	:	
Toplam Sayfa Sayısı	:	132

Anahtar Kelimeler (Türkçe)	Anahtar Kelimeler(İngilizce)
1) Siber	1) Cyber
2) Suç	2) Crime
3) Sözleşme	3) Convention
4) İnternet	4) Internet
5) Türkiye	5) Turkey

ÖZET

Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi küresel düzeyde siber suçlarla mücadelede şimdiye kadar ortaya konmuş en önemli ve kendisine taraf devletler üzerinde bağlayıcılığı bulunan hukuki bir metindir. Sözleşme, sadece Konseye üye olan devletler açısından değil, Konseye üye olmayan devletler açısından da siber suçlar alanında bir model ortaya konulması nedeniyle önemlidir. Sözleşme, dört bölüm ile siber suçlarla ilgili olarak maddi ceza hukukuna, ceza usul hukukuna ve uluslararası adli işbirliğine dair hükümler ihtiva etmektedir.

Türkiye, 2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren Sözleşme'yi 2010 yılında imzalamış ve 2014 yılında "6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" ile kabul etmiştir. Sözleşme'nin, bu şekilde iç hukukumuzun bir parçası haline gelmesine kadar Türkiye, siber suçlar alanında çeşitli yasa çalışmaları yapmış ve bu yasalar onaylanarak yürürlüğe girmiştir. Çalışmanın konusu oluşturan Sözleşme'nin siber suçlarla ilgili yapılan yasalara etkisi ise yok denecek kadar azdır. Ancak bu durum, iç hukukumuzun Sözleşme ile kurulan hukuki çerçeveden uzak olunduğu anlamına gelmemektedir.

ABSTRACT

The Council of Europe's Convention on Cybercrime which has binding effect on state parties is the most comprehensive response to address the most common categories of cybercrimes. The Convention is significant not only for the member states of the Council of Europe but also for the non-members states as a model to be followed. The Convention consists of four chapters, mainly covering issues of substantive and procedural law and international co-operation.

The Convention which was opened for signature in 2001 and came into force in 2004 was signed by Turkey in 2010 and adopted by Turkey with the "Law no. 6533 on the Approval of the Convention on Cybercrime" in 2014. Until the Convention became part of Turkish domestic law, Turkey had introduced and enacted various cybercrime laws. As a focus of this study, the Convention does not have serious impact on those legislative activities. However, it does not necessarily mean that the legal framework regarding Cybercrime in Turkey is in variance with the Convention.

İçindekiler

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
A.g.e.	: Adı Geçen Eser
BM	: Birleşmiş Milletler
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
E.	: Esas
Ed.	: Editör
İHAM	: İnsan Hakları Avrupa Mahkemesi
İHAS	: İnsan Hakları Avrupa Sözleşmesi
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
m.	: Madde
p.	: Paragraf
s.	: Sayfa
SSS	: Siber Suçlar Sözleşmesi
TCK	: 5237 sayılı Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
TİB	: Telekomünikasyon İletişim Başkanlığı
UHDİGM	: Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü
YFCY	: Yeni Fransız Ceza Yasası

KAYNAKÇA

Atar Yavuz, Türk Anayasa Hukuku, Mimoza Yayınları, Konya 2012, 9. Baskı

Bakıcı Sedat – Yalvaç Gürsel, 5237 Sayılı Yasa Kapsamında Ceza Hukuku Özel Hükümleri, Adalet Yayınevi, Ankara 2008, 2. Cilt

Berber Leyla Keser, Adli Bilişim, Yetkin Yayınları, Ankara 2004

Black's Law Dictionary, 2009

Brenner Susan W. , Cybercrime: Criminal Threats from Cyberspace, Praeger, Santa Barbara, 2010

Cezai Konularda Adli İşbirliği Rehberi, Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, Ankara 2014, Şen Matbaa

Clough Jonathan, Principles of Cybercrime, Cambridge University Press, Cambridge 2010

Clough Jonathan, The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World (2012) 23(4) Criminal Law Forum 363

Csonka Peter, The Council of European Convention on Cybercrime: A Response to Challange of the New Age(ed.), Ed. by Roderic Broadhurst and Peter Grabosky, Cyber-crime the Challange in Asia, Hong Kong University Press, 2005

Tutanaklarla Türk Ceza Kanunu, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, Ankara 2005

Doğru Osman - Nalbant Atilla, İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, 2. Cilt, Pozitif Matbaa, Ankara 2013

Döner İsa, "Arama-Elkoyma, Dijital Verilere Elkoyma", AİHM Kararları Işığında Koruma Tedbirleri ve İfade Özgürlüğü Sempozyumu, HSYK Genel Sekreterlik Yayınları, Ankara, 2013

Dönmezer Sulhi, Kişilere ve Mallara Karşı Suçlar, Beta Yayınevi, İstanbul 2001, 16. Bası

Fafinski Stefan, Computer Misuse: Response, Regulation and the Law, Willian Publishing, 2009

Goodman Mark D. - Brenner Susan W., 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 10(2) International Journel of Law and Information Technology 139

Gözübüyük A. Şeref, Anayasa Hukuku, Turhan Kitabevi, Ankara 2004

Helvacıoğlu Aslı Deniz, Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi, İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 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

İnceoğlu Sibel, Adil Yargılanma Hakkı, İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme (Editör, Sibel İnceoğlu), Şen Matbaa, Ankara 2013

Karagülmez Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, Ankara 2011

Kierkegaard Sylvia (konuşmacı), "Çocuk Pornografisi", Ankara Barosu Uluslararası Hukuk Kurultayı, Bilişim ve Hukuk, Ankara Barosu Yayınları, Ankara 2009, Üçüncü gün, İkinci Oturum

Kubilay Taşdemir, Belgelerde Sahtecilik Suçları, Ütopyagrafik, Ankara 2013

Kunter Nurullah - Yenisey Feridun - Nuhoğlu Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Arıkan Basım Yayım, İstanbul 2006, 14. Bası

Marco Gercke, Siber Suç Sözleşme ile 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve Kusurları, İnternet Hukuku ed. Yener Ünver, Seçkin Yayıncılık, Ankara 2013

Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 5. Baskı Ankara 2014

Özbek Veli Özer, Müstehcenlik Suçu, Seçkin Yayınevi, Ankara 2009

Özbudun Ergun, Türk Anayasa Hukuku, Yetkin Yayınları, Anakara 2003, 7. Baskı

Özen Muharrem - Baştürk İhsan, Bilişim- İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara 2011

Özgenç İzzet, Türk Ceza Kanunu Şerhi, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara Açık Cezaevi Matbaası, Ankara 2006, 3. Bası

Parlar Ali, Hatipoğlu Muzaffer, 5237 Sayılı Türk Ceza Kanunu Yorumu, Yayın Matbaacılık ve Tic. İşletmesi, Ankara 2007, 2. Cilt

Ryan M.F. Baron, A Critique of the International Cybercrime Treaty (2011-2002) 10 Commlaw Conceptus 263

Keskin Serap, Avrupa Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İstanbul Üniversitesi Hukuku Fakültesi Mecmuası (İÜHFM) Cilt:LIX, Sayı 1-2, 2001

Smith Russell G., Grabosky Peter, Urbas Gregor, Cyber Criminal on Trial, Cambridge University Press, Cambridge 2004

Tezcan Durmuş – Erdem Mustafa Ruhan - Önok Rifat Murat, Uluslararası Ceza Hukuku, Seçkin Yayıncılık, Ankara 2009

Turrini Elliot – Ghosh Sumit, "A Pragmatic, Experiential Definition of Computer Crimes", Cybercrimes: A Multidisciplinary Analysis, Ed. by Elliot Turrini and Sumit Ghosh(eds), Springer, 2010

Tutanaklarla Ceza Muhakemesi Kanunu, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, Ankara Açık Cezaevi Matbaası, Ankara 2005

Ünver Yener, Hakeri Hakan, Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara 2012

Ünver Yener, Türk Ceza Kanunu ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi, İstanbul Üniversitesi Hukuku Fakültesi Mecmuası (İÜHFM) Cilt:LIX, Sayı 1-2, 2001

Wall S. David, 'Cybercrimes: New Wine, No Bottles', in David S. Wall (ed), Cyberspace Crime, Dartmouth Publishing Company, 2003

Wall, David S., Cybercrime: The Transformation of Crime in the Information Age, Polity Press, Cambridge 2007

Weber Amalie M., The Council of Europe's Convention On Cybercrime (2003) 18 (1) Berkeley Technology Law Journel 425

Yalçın Alemdar, Ceza Hukuku Açısından Bilişim Suçları, Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar(Müslüm Saylı Derin Akdeniz), İçişleri Bakanlığı, 24/03/2001 Bursa

Yaşar Osman – Gökcan Hasan Tahsin -Artuç Mustafa, Yorumlu-Uygulamalı Türk Ceza Kanunu, Adalet Yayınevi, Ankara 2014, 3. Cilt

Yavuz Erdoğan, Türk Ceza Kanunu'nda Bilişim Suçları, Legal Yayıncılık, 1. Baskı, 2012 İstanbul

Yazıcıoğlu ,R. Yılmaz Yazıcıoğlu, Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, Alfa Yayınevi, İstanbul 1997
Yazıcıoğlu Yılmaz, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 2005, Cilt:2 Sayı: 2 Yıl

Yenidünya Ahmet Caner, Gökcen Ahmet, Artuk Mehmet Emin, Türk Ceza Kanunu Şerhi, Adalet Yayınevi, 2. Basım, Ankara 2014

Yenidünya Caner – Değirmenci Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, 2003 İstanbul

ELEKTRONİK KAYNAKLAR

'Charges Dropped in Love Bug Virus Case' (08/01/2015) ABC, (çevrimiçi) http://abcnews.go.com/Technology/story?id=119536, 02.04.2015

'Ratification', Glossary on Treaties, Council of Europe, (çevrimiçi) http://www.conventions.coe.int/?pg=/Treaty/Glossary_en.asp#Ratification , 29.04.2015

"Love Virus Chaos Spread" (4 May 2000) BBC, (çevrimiçi) http://news.bbc.co.uk/2/hi/uk_news/736208.stm, 29.04.2015

23. Dönem 2. Yasama Yılı 47. Birleşim 09/01/2008, (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?P4=20047&P5=B&PAGE1=1&PAGE2=90 , 29.04.2015

5271 Sayılı Yasa Gerekçesi, (çevrimiçi), http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss698m.htm , 29.04.2015

5728 sayılı Temel Ceza Kanunlarına Uyum Amacıyla Çeşitli Kanunlarda ve Diğer Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Genel Gerekçe, (çevrimiçi) http://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss56.pdf, 29.04.2015

A Collective EU Response to Cybercrime, Europol, (çevrimiçi) https://www.europol.europa.eu/ec3 ,29.04.2015

Action Against Cybercrime, Cybercrime Convetion Comittee, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp , 29.05.2015

Activities, Interpol, (çevrimiçi) http://www.interpol.int/Crime-areas/Cybercrime/Activities , 29.04.2015

Adalet Komisyon Raporu, Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 Sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ve İstanbul Milletvekili Gülseren Topuz'un; Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi ile Adalet Komisyonu Raporu (1/1305, 2/958) (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=51984 , 29.04.2015

Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of Racist and Xenophobic Nature Committed Through Computers Systems, Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/en/Reports/Html/189.htm, 29.04.2015

Akdeniz Yaman, An Advocacy Handbook for the Non Governmental Organizations, Cyber-rights.org, (December 2003), (çevrimiçi) http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf , 29.04.2015

Amandine Scherrer, The G8 and Transnational Organized Crime: The Evolution of G8 Expertise on the International Stage (21 January 2008) G8.Utoronto, (çevrimiçi) http://www.g8.utoronto.ca/speakers/scherrer2008.htm , 29.04.2015

Around the Clock Capability Needed Successfully Fight Cybercrime, Workshop Told, BKK/CP/22, 10th mtg, (Bangkok, Thailand, 23 April 2005), (çevrimiçi), http://www.un.org/events/11thcongress/docs/bkkcp22e.pdf , 29.04.2015

Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cybercrime, 5001/01/En/Final, WP 41, (22.03.2001) (çevrimiçi) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp41en.pdf, 29.04.2015

Avrupa Konseyi Çocukların Cinsel Suistimal ve Cinsel İstismara Karşı Korunmasına İlişkin Sözleşme, (çevrimiçi) http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_tur.pdf , 29.04.2015

Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu, Explanatory Report (çevrimiçi) http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 28.04.2015

Avrupa Konseyi, Sözleşme İmza ve onay tablosu, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

Aydın Murat Burak, "Kurgu Eserler, Çocuk Pornografisi ve Cezalandırma", (çevrimiçi) http://www.umut.org.tr/Upload/Document/document_844745e77a5947ecae017baadf884c65.pdf , 29.04.2015

Birleşmiş Milletler, A/RES/63/211, 17/01/2010, (çevrimiçi) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 , 29.04.2015

Brian Harley, A Global Convention on Cybercrime (23 March 2010) Stlr, (çevrimiçi) http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ , 29.04.2015

Chart of Signatures and Ratifications (01.04.2013) Council of Europe (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=4&DF=&CL=ENG , 29.04.2015

Combatting the Criminal Misuse of Information Technologies, A/RES/55/63, UN GAOR, 55th sess, Agenda Item 105, (22 January 2001) (çevrimiçi), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf , 29.04.2015

Consumer Online Shopping Fears,First Data, Market Briefs, (çevrimiçi) http://www.firstdata.com/downloads/thought-leadership/fd_consumeronlineshoppingfears_research.pdf. 29.01.2015

Council Framework Decision of 28 May 2001 Combating Fraud and Counterfeiting of Non-Cash Means of Payment, European Union, 2001/413/JHA, (çevrimiçi) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413 ,29.04.2015

Council of Europe Committee of Ministers, Recommendation No.R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (13 September 1989) 428th mtg (çevrimiçi) https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 , 29.04.2015

Council of Europe Committee of Ministers, Recommendation No.R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with

Infromation Technology (11 September 1995) 543rd mtg (çevrimiçi) http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp , 29.04.2015

Cybercrime Convention Comittee, T-CY Rules of Procedure, Strasbourg, 3.12.2015 (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)25%20rules_v14.pdf , 30.04.2015

Cybercrime Convetion Ratification Leaves Lingering Concerns, 05/03/2013, Pirate Party, (çevrimiçi) http://pirateparty.org.au/2013/03/05/cybercrime-convention-ratification-leaves-lingering-concerns/ , 29.04.2015

Cybercrime Legislation, Country Profile, Turkey, 25.01.2011, (çevrimiçi) http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_Turkey_2011_January.pdf , 29.04.2015

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2013/01 final, (çevrimiçi) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001, 29.04.2015

D'cruz Theodora, Interpol Opens Singapore Center to Fight Cybercrime, 02.10.2014, (çevrimiçi) http://www.reuters.com/article/2014/10/02/us-asia-cybersecurity-idUSKCN0HR0OG20141002 ,29.04.2015

Denver Summit of the Eight: Communiqué, (22 June 1997) G8, (çevrimiçi) http://www.g8.utoronto.ca/summit/1997denver/g8final.htm , 29.04.2015

Directive 2009/136/EC of the European Parliament and of the Council 25 November 2009, European Union, (çevrimiçi) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, 29.04.2015

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093, 29.04.2015

Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, A/RES/45/121, UN GAOR, 68th plen mtg, (14 December 1990) (çevrimiçi) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121 , 29.04.2015

EU Cyber Security Strategy - Open, Safe and Secure, European Union External Action, 07.02.2013, (çevrimiçi) http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm, 29.04.2015

European Committee on Crime Problems, Meeting Reports, CM(97/4) (10 January 1997) Appendix II, 4b (çevrimiçi) https://wcd.coe.int/ViewDoc.jsp?Ref=CM(97)4&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 , 29.04.2015

European Union Agency for Fundamental Rights, Handbook on Data Protection Law, 2014, (çevrimiçi) http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf , 29.04.2015

FATF, 36. Tavsiye, (çevrimiçi) http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf , 29.04.2015

Finklea Kristien M. - Theohary Catherina A., Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement (çevrimiçi) http://www.fas.org/sgp/crs/misc/R42547.pdf , 9 January 2013

Finland's Cyber Security Strategy Government Resolution 24/01/2013, (çevrimiçi) http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy , 30.04.2015

G8 Recommendations on Transnational Crime (01 December 2008) Canada International, pt IV s D (çevrimiçi)
http://www.npa.go.jp/sosikihanzai/kokusaisousa/kokusai1/transg8rece.htm, 29.04.2015

Global Action Against Online Fraud in the Airline Sector Nets 118 Arrests, Interpol, 28.11.2014, (çevrimiçi) http://www.interpol.int/News-and-media/News/2014/N2014-228, 29.04.2015

Global Project on Cybercrime, The cybercrime legistlation of Commonwealth States: Use of Budapest Convention and Commonwealth Law, 27/02/2003, Strazburg, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb%20rev_final_CoE.pdf , 29.04.2015

Home Office, Cyber Crime Strategy (March 2010) Official-documents, (çevrimiçi) http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf, 29.04.2015

Internet Users in the World, Internet World Stats, Usage and Population Stats, (çevrimiçi) http://www.internetworldstats.com/stats.htm ,29.04.2015

Jarrett H. Marshall – Bailie Michael W. , OLE Litigation Series, Prosecuting Computer Crimes, (çevrimiçi) http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf , 29.04.2015

Lack of Applicable Law Allows Alleged Hacker Loose, Amorillo, (çevrimiçi) http://amarillo.com/stories/2000/08/22/usn_hacker.shtml, 01.04.2015

Lev Grossman, 'Attack of the Love Bug' (15 May 2000) Time, (çevrimiçi) http://www.time.com/time/magazine/article/0,9171,996899-1,00.html, 29.04.2015

List of Declarations made with Respect to Treaty No. 185, Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 , 29.04.2015

List of declarations made with respect to treaty no:185, Convetion on Cybercrime, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 , 29.04.2015

Markoff John – Kramer Andrew E., "In Shift, U.S. Talks to Russia on Internet Security", 12.12.2009, New York Times, (çevrimiçi) http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0 ,29.04.2015

Meeting of Justice and Interior Ministers of the Eight (10 Dec 1997) CoE, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Communique_en.pdf , 29.04.2015

Member States of the Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG , 29.04.2015

Member States of the Council of Europe, Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, 29.04.2015

Member States of the United Nations (03 July 2006) UN, (çevrimiçi) http://www.un.org/en/members/index.shtml , 29.04.2015

Michael A. Vatis, The Council of Europe Convention on Cybercrime (2010) National Academics, (çevrimiçi) http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059441.pdf , 29.04.2015

Moor Keith, Police Smash Global Gang Behind 500.000 Aussie Credit Cards Theft (29 November 2012) Herald Sun, [1]-[10] (Çevrimiçi) http://www.heraldsun.com.au/news/law-order/police-smash-global-gang-behind-500000-aussie-credit-card-thefts/story-fnat7jnn-1226526111909, 01.04.2015

Murphy Laura W. - Johnson Marvin J., ACLU Letter to the Senate Foreign Relations Committee on the Council of Europe Convention on Cybercrime (16 June 2004) ACLU, (çevrimiçi) http://www.aclu.org/technology-and-liberty/aclu-letter-senate-foreign-relations-committee-council-europe-convention-cybe , 29.04.2015

Norton Study Calculates Cost of Global Cybercrime: 114 Billion Dolar Annualy, Symantec, Press Release, 07.09.2011, (çevrimiçi) http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 , 29.04.2015

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Society (25 July 2002) OECD, http://www.oecd.org/sti/ieconomy/15582260.pdf, 04.04.2015

Okinawa Charter on the Global Information Society (22 July 2000) G8, (çevrimiçi) http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm , 29.04.2015

Picotti Lorenzo – Salvadori Ivan, National Legislation Implementing the Convention on Cybercrime – Comparative Analysis and Good Practices, 28.08.2008 Strasbourg, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf , 29.04.2015

Project on Cybercrime, The Functioning of 24/7 Points of Contact for Cybercrime, 02/04/2009, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/567_24_7report4public_april09a.pdf , 29.04.2015

Recommendation No. R (85) of the Committee of Ministers to Member States Concerning the Practical Applicaiton of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications, Council of Europe, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1985_10.pdf, 29.04.2015

Recommendation of the Council Concerning Guidelines for the Security of Information Systems (26 November 1992) OECD, (çevrimiçi) http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, 04.04.2015

Reservation, Glossary on Treaties, Council of Europe, (çevrimiçi) http://www.conventions.coe.int/?pg=/Treaty/Glossary_en.asp , 29.04.2015

Review of the 2002 Security Guidelines (2012) OECD, (çevrimiçi) http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf, 01.01.2015

Russell L. Ackoff, From Data to Wisdom Presidential Address to ISGSR, (çevrimiçi) http://fournier.facmed.unam.mx/ib1/2013/students/files/u2/FromDataWisdomAckoff.pdf, 19.03.2015

Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun, TBMM, (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/kanunlar_sd.durumu?kanun_no=6533, 29.04.2015

Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyon Raporu, TBMM, (çevrimiçi) http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, 29.04.2015

Schjolberg Stein - Hubbard Amanda, 'Harmonizing National Legal Approaches on Cybercrime' (10 June 2005) International Telecommunication Union, (çevrimiçi) http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, 20.04.2015

Seger Alexander, The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is web, 16/02/2012, (çevrimiçi) http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf , 29.04.2015

Serkowski Rodney, Submission to the Joint Standing Comittee on Treaties Regarding the Proposed Accession to the Council of Europe Convention on Cybercrime, March 2011, (çevrimiçi) http://pirateparty.org.au/media/submissions/JSCOT%20CoE%20Cybercrime%20Convention.pdf , 29.04.2015

Sieber Ulrich, Legal Aspects of Computer Related Crime in the Information Society (1 January 1998) Europa.Eu, (çevrimiçi) http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html, 20.04.2015

Steinhardt Barry - Calabrese Christopher, ACLU Memo on the Council of Europe Convention on Cybercrime (16 June 2004) ACLU, (çevrimiçi) http://www.aclu.org/technology-and-liberty/aclu-memo-council-europe-convention-cybercrime , 29.04.2015

TBMM Genel Kurul Tutanağı 24. Dönem 4. Yasama Yılı 79. Birleşim 22.04.2014, (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?P4=22125&P5=H&PAGE1=1&PAGE2=73, 29.04.2015

T-CY Guidances Notes, Strasbourg, 08.12.2014 (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY(2013)29rev_GN%20compilation_v3.pdf , 29.04.2015

The Stockholm Programme, Official Journal of the European Union, (çevrimiçi) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504(01)&from=EN , 29.04.2015

Twelfth United Nations Congress on Crime Prevention and Justice, A/Conf.213/9 (22 January 2010), (çevrimiçi) https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf , 29.04.2015

Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, Cezai Konularda Adli İşbirliği Sözleşmeleri, (çevrimiçi) http://www.uhdigm.adalet.gov.tr/sozlesmeler/munhasir_adli_yardimlasma.html , 29.04.2015

United Nations Manual on the Prevention and Control of Computer-Related Crime, 43-44 International Review of Criminal Policy, UN Doc E/94/IV/5 (1994) 117, (çevrimiçi) http://www.uncjin.org/Documents/EighthCongress.html, 01.04.2015

Vogel Joachim, Towards a Global Convention Against Cybercrime, First World Conference of Penal Law In The
XXIst Century, Guadalajara (Mexico), 18-23 November 2007, (çevrimiçi) http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf , 29.04.2015

What is Cybercrime, Symantec Corporation, Norton (çevrimiçi) http://us.norton.com/cybercrime-definition/promo , 29.04.2015

Yeni Fransız Ceza Yasası, (çevrimiçi) http://www.legislationline.org/download/action/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf , 29.05.2015

KARAR DİZİNİ

ELEKTRONİK AĞ ADRESLERİ

http://www.tdk.gov.tr

http://dictionary.cambridge.org

http://www.oxforddictionaries.com

http://www.oxfordreference.com

I. GİRİŞ

Siber Suçlar Sözleşmesi, Avrupa Konseyi tarafından hazırlanmış olup, siber suçlar alanında en kapsamlı ve kapsayıcı uluslararası hukuki bir metindir. Sözleşme 23 Kasım 2011 tarihinde Budapeşte'de imzaya açıldı ve 1 Haziran 2004 tarihinde yürürlüğe girdi. Sözleşme, şu ana kadar 49 devlet tarafından imzalanmasına rağmen 45 devlet tarafından onaylanmıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi, Sözleşme'nin getirdikleri ve Sözleşme'nin iç hukukumuzun ile olan ilişkisi bu çalışmanın kapsamını oluşturmaktadır. Çalışmanın sonunda artık tarafı olduğumuz Sözleşme'nin ortaya çıkış nedeni, amacı, içeriği, olumlu ve olumsuz yanları hakkında bilgi edinilecek, siber suçlarla ilgili olarak Ülkemizin, Sözleşme ile ne kadar uyumlu olduğu görülecektir. Çalışmada, genel olarak Avrupa Konseyi Siber Suçlar Sözleşmesi yerine, sadece Sözleşme veya Budapeşte Sözleşmesi ifadesi kullanılacak, Sözleşme'de yer alan kavramlar üzerinden konular açıklanacak, bazen de ulusal mevzuattaki farklılığa dikkat çekmek için Türk yasalarında kullanılan eş değer kavramlara yer verilecektir.

Çalışma, 7 bölümden oluşmaktadır. İlk bölümde, yani bu bölümde, çalışmamızın genel çerçevesi çizilecektir. İkinci bölümde, siber suç incelenecek, siber suçun tanımı ve özellikleri ele alınacaktır.

Üçüncü bölümde, ulusal ve uluslararası alanda siber suçlarla ilgili olarak yapılan çalışmalara yer verilecek, bu şeklide dördüncü bölümde açıklanacak olan Siber Suçlar Sözleşmesi'ne zemin hazırlanacaktır.

Dördüncü bölümde, Sözleşme, madde madde ayrıntılarına girilmeden genel olarak ele alınacak, ortaya çıkış nedeni ve yapısı ortaya konacak, son olarak Sözleşme'ye getirilen olumlu ve olumsuz eleştirilere yer verilecektir.

Beşinci bölümde, Sözleşme'ye Türkiye'nin taraf olması ve Sözleşme'nin iç hukukumuzun bir parçası haline gelmesi, yapılan yasama faaliyetleri çerçevesinde incelenecektir.

Altıncı bölümde, Sözleşme'nin hükümleri ile iç hukukumuz ayrıntılı ve karşılaştırmalı olarak incelenerek, mevzuatımızın Sözleşme ile ne kadar uyumlu olduğu belirlenmeye çalışılacaktır.

Yedinci ve son bölümde Sözleşme'ye taraf olmanın bir kazanım olduğu, ancak Sözleşme'nin Avrupa hukuku bütününün bir parçası olduğu, tek başına ve bağımsız olarak uygulanmasının sakıncalı olduğu, Sözleşme ve onun bir parçası olduğu hukuk ile uyumlaştırma çalışmalarının yapılması gerektiği belirtilerek çalışmaya son verilecektir.

II. SİBER SUÇ

A. Giriş

Teknoloji, hayatımızda her anlamda yaygın bir hale gelmiş olup, suçlular için daha önceleri hiç mümkün olmayacak ölçüde mümbit bir alan açmıştır. Sanal dünya ya da siber uzay diyebileceğimiz bu yer doğası gereği kimseye ait değildir ve bu âlemin aktörü olan devletler, yine kendileri gibi bu âlemde aktör olan siber suçluları henüz tamamen kontrol altına alabilecek kuralları belirleyememişlerdir. Hatta siber suçluların bu âlemde kuralları kendilerinin koydukları, devletlerin koydukları kuralları daha kolay suç işleyebilmek için manipüle ettikleri ve kendileri için bu âlemde kolluk güçlerinin ulaşamayacağı güven adaları oluşturdukları dahi söylenebilir. Bir başka anlatımla iyi ve kötünün karşılıklı mücadelesinin siber uzay sürümü ile karşı karşıyayız.

Siber suç mağdurları, dijital ortamın kendilerine bahşettiği daha ucuz ve daha hızlı iletişim yolları, bilgi kaynakları, e-ticaret ve eğlence hizmetlerinin tadını çıkarırken farkında olmadan siber suçluların ağına düşebilmektedirler. Siber suçlular, çok kolay bir şekilde bazen mağdurların zaaflarını kullanarak bazen gelişmiş bilgisayar teknolojilerini kötüye kullanarak bilişim sistemlerine girme ve orada kalma, bilişim sistemlerinin işleyişini engelleme veya bozma ve bu yollarla haksız çıkar sağlamak suretiyle fiziki âlemde bulamayacakları imkânlar elde etmektedirler. Yapılan bir çalışmaya göre her gün bir milyondan fazla kişi bilişim suçlarının mağduru olmakta ki, bu her saniyede 14 kişinin siber saldırıya maruz kaldığı anlamına gelmektedir.[1] Bir çalışmaya konu rapora göre, esrar, kokain ve eroin gibi uyuşturucu maddelerin küresel düzeyde ticareti 288 milyar dolar iken, siber suçlar her yıl 338 milyar dolar zarara neden olmaktadır.[2]

Bu yepyeni alem ve beraberinde getirdiği suç ve suçlu tipi, bir fenomen olarak, geleneksel ceza hukukunu sarstığını, bir anlamda zor durumda bıraktığını kabul etmek gerektir. Örneğin, siber suçun şüphelisi mağdur ile aynı yargı

---

[1] Norton Study Calculates Cost of Global Cybercrime: 114 Billion Dolar Annualy, Symantec, Press Release, 07.09.2011, (çevrimiçi) http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 , 29.04.2015

[2] A.g.e.

çevresinde, hatta aynı ülke sınırları içerisinde olmadan mağdura karşı bu suçu işleyebilmektedir. Bu durum farklı ulusal yasalara temas etmekte ve etkin bir soruşturma ve kovuşturma için uluslararası işbirliğini gerektirmektedir.

B. Siber Suçun Tanımı

Siber suç anlamında bu terimin yerine bilgisayar suçu, sanal suç, çevrimiçi suç, dijital suç, ileri teknoloji suçu, bilgisayarla ilgili suç, internetle ilgili suç, telekomünikasyonla ilgili suç, bilgisayar yardımlı suç, elektronik suç ve e-suç gibi birçok terim kullanılmıştır.[3] Ancak literatürde en yaygın kullanılan terim siber suç olmuştur. Bu terim, tezin inceleme alanını oluşturan Avrupa Konseyi Siber Suç Sözleşmesi tarafından da tercih edilmiştir. Bu nedenle çalışmada genel olarak bu terim kullanılacaktır.

Siber suçun, henüz üzerinde görüş birliğine varılmış bir tanımı yoktur. ABD'de en yaygın olarak kullanılan hukuk sözlüğü olan Black's Law sözlüğüne göre, siber suç (bilgisayar suçu), elektronik olarak depolanan verilerin çalınması ve sabote edilmesi gibi bilgisayar kullanımını gerektiren bir suçtur.[4] Avustralya hukuk sözlüğü, siber suçu (internet suçu), "internet, telefon ve kablosuz teknolojileri kapsayan iletişim teknolojileri alanında ortaya çıkan kriminal bir aktivite" olarak tanımlar. [5] Oxford hukuk sözlüğü, "internet üzerinden işlenen suçlar" tanımını getirirken,[6] aynı yayınevinin bilişim sözlüğüne göre ise, siber suç, "bilgisayar ve bilgisayar ağlarına yönelik olarak veya bunları kullanarak işlenen suç" olarak tanımlamaktadır[7].

---

[3]Russell G Smith, Peter Grabosky, Gregor Urbas, Cyber Criminal on Trial, Cambridge University Press, Cambridge 2004, s.5.

[4] Black's Law Dictionary, crime, (9. Baskı, 2009)

[5] Australian Law Dictionary, cybercrime (internet crime), (2010 online versiyon), http://www.oxfordreference.com/view/10.1093/acref/9780195557558.001.0001/acref-9780195557558-e-0921?rskey=eFEDr8&result=4

[6] Oxford Dictionary of Law, cybercrime, http://www.oxfordreference.com/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248-e-1000

[7] A Dictionary of Computing, cybercrime, http://www.oxfordreference.com/view/10.1093/acref/9780199234004.001.0001/acref-9780199234004-e-6333

Wall'a göre, salt davranışın ötesinde, ağ teknolojileri ile kriminal davranışın başkalaşması açısından siber suçun daha geniş bir anlamı vardır ve siber suç, yarar sağlamak için bilginin elde edilmesi veya manipülasyonunu gerektiren kriminal faaliyettir.[8]

Brenner, öncelikle, siber suçu normal suçtan ayırır ve siber uzayda bilgisayar teknolojisi ile işlenen suç olarak tanımlar.[9]

Turrini ve Ghosh ise, daha teknik bir yaklaşımla, siber suçun, siber suçlunun başarılı bir şekilde bilişim süreci üzerinde yetkisiz bir hâkimiyet sağlaması ile işlendiğini düşünür.[10]

Dünyanın en büyük yazılım şirketlerinden bir olan Symantec Corporation, siber suçu, bilgisayar, ağ ya da donanımsal bir aracın kullanılması ile işlenen suç olarak tanımlar.[11]

Çalışmamızın konusunu oluşturan Avrupa Konseyi Siber Suçlar Sözleşmesi'ne göre, siber suç, a) bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve erişilebilirliğine, b) dolandırıcılık ve sahteciliğe, c) çocuk pornografisine, d) telif ve benzeri haklara yönelik bilgisayarla ilgili her türlü kötü niyetli eylemdir. [12]

Bütün bu farklı yaklaşımlardan, çok genel bir yaklaşımla, bilişim sisteminin o suçun bir unsuru olduğu suç, siber suçtur, sonucuna da varılabilir. Görüldüğü alanların çeşitliliği, mümkün olduğu kadar esnek bir tanım ihtiyacı ortaya çıkarmaktadır. Haksız erişim, bir siber suç olduğu gibi, haksız bir şekilde erişilen sistem üzerinden yapılan hakarette siber suç kavramı içine girebilmektedir.

Elbette siber suçlarla ilgili yapılabilecek tanımlar, burada verilen tanımlarla sınırlı değildir. Birçok başka kaynak ve yazar, siber suçun tanımıyla ilgili farklı

---

[8] David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, Polity Press, 2007, s.10.
[9] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, Praeger, 2010, s.9.
[10] Elliot Turrini and Sumit Ghosh, 'A Pragmatic, Experiential Definition of Computer Crimes' in Elliot Turrini and Sumit Ghosh(eds), Cybercrimes: A Multidisciplinary Analysis, Springer,2010, s.9.
[11] What is Cybercrime, Symantec Corporation, Norton (çevrimiçi) http://us.norton.com/cybercrime-definition/promo , 29.04.2015
[12] Avrupa Konseyi Siber Suçlar Sözleşmesi, CETS no. 185, Budapeşte, 23.11.2001

alternatif tanımlar yapmıştır. Siber suçun tanımı, onu diğer suçlardan ayırt etmek, bu suçla özel olarak mücadele etmek ve bu yönde değişik politika ve stratejiler geliştirmek açısından önemli olsa da, bazıları yazarlar, bir suçun soruşturulması ve kovuşturulması itibariyle, bir şemsiye tanım olarak, kimlik bilgilerinin çalınması suçunun gerçek âlemde veya siber âlemde her hâlükârda suç olması örneğinden hareketle, tanımlama konusunda takıntılı bir tavra da gerek olmadığını düşünmüşlerdir.[13]

Ancak, siber suçların neleri kapsadığı konusunda bir uzlaşma olduğu söylenebilir. Bu nedenle, siber suçun tam olarak ne olduğundan ziyade onun neleri kapsadığını belirtmek daha faydalı olacaktır. Genel olarak kabul edilen yaklaşıma göre, siber suç üç ayrı kategoride ele alınır:

- Bilgisayar ve bilgisayar teknolojilerine karşı suçlar,
- Bilgisayar ve bilgisayar teknolojileri aracılığı ile işlenen suçlar,
- Bilgisayar ve bilgisayar teknolojilerinin suçun işlenmesinde önemli rol oynadığı suçlar.[14]

Bu çalışmada siber suç kavramı, yukarıda belirtilen bu üç kategori bağlamında ele alınacaktır.

C. Siber Suçun Özellikleri

Dijital çağ ve teknolojilerinin gelişine kadar hukuk sistemleri, genel anlamda teknolojik gelişmelere uyum sağladı.[15] İnternet ve bilgisayarın aksine, telefon, radyo, televizyon ve otomobillerin icadı yasaların uygulanması açısından herhangi sorun teşkil etmedi. David Wall, hızla gelişen ve yapısı sürekli değişen bu durumu edebi bir şeklide şöyle açıklamıştır: "eski şarap yeni şişede", "yeni şarap yeni şişede" ve "yeni şarap şişe yok".[16] Gerçekten, bir kaba sığmayan ve sınır

---

[13] Finklea Kristien M. - Theohary Catherina A., Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, 9 January 2013 (çevrimiçi) s.16 http://www.fas.org/sgp/crs/misc/R42547.pdf, 29.04.2015

[14] Smith, Grabosky, Urbas, s.7.

[15] Mark D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace', 2002, 10(2) International Journel of Law and Information Technology 139, s. 151.

[16] David Wall, 'Cybercrimes: New Wine, No Bottles', in David S. Wall (ed), Cyberspace Crime, Dartmouth Publishing Company, 2003, s. 5.

tanımayan yeni teknolojiler, diğer ifadeyle şişesiz şaraplar, hukuk sistemlerini ve hukukun uygulanmasını güç durumda bıraktılar. Bu başlık altında siber suçlara özgü, onu diğer geleneksel suçlardan ayıran bu özellikler irdelenecektir. Bu özelliklerin iyi anlaşılması, siber güvenlik açısından da önem arz etmektedir.

1. Siber Suçun Sınırları

Siber suçun en ayırt edici özelliği, onun sınır tanımaz yanıdır. Geleneksel suçların aksine, siber suç ulusal, ekonomik ve sosyal sınırlar ile kısıtlanamaz. Daha açık olmak gerekirse, siber suç, bir suçlu tarafından dünyanın dört bir yanından birçok farklı yargı çevresinde işlenebilmektedir. Bu nedenle, bir ülkenin bilgisayar ve teknolojileri yasaları çıkararak bu suçla mücadele etmesi nerdeyse imkânsızdır. Bu durum o ülkenin, diğer ülke ve uluslararası aktörlerle işbirliği halinde olmasını zorunlu kılmaktadır. Geleneksel olarak, doğası gereği, bir şüphelinin suç işlediği yerde veya bu yere yakın bir konumda olması ve kolluk güçlerinin de sorumluluk alanlarının dışına çıkmaksızın şüpheliyi yargı önüne koyması beklenir. Ancak, bir bilgisayar korsanı (hacker) için suç yeri hiçbir anlam ifade etmez. Örneğin, Romanya ülkesinde bulunan bilgisayar korsanları, benzin istasyonu ve market gibi işletmelerin bilgisayar sistemlerindeki güvenlik açıklarından faydalanarak 500.000 Avustralyalının kredi kartı bilgilerini çalmışlardır.[17] Son olarak, zaman yönüyle de siber suç açısından bir sınır yoktur. Bu suç her an işlenebilir.

2. Siber Suçlarda Soruşturma

Soruşturmanın karmaşıklığı ve delillerin hassasiyeti nedeniyle[18] siber suçlara ilişkin soruşturma teknik bilgi ve donanım gerektir. Siber dünya, merkezi bir yapıya sahip değildir. Parçalı ancak birbiri ile ilişkili ve açık bir alandır. Bu nedenle, internet üzerinde sürekli bir denetim ve gözetim mümkün olmadığı gibi farklı yargı çevrelerinde bulunan siber suçluların takibi çok zordur. Aynı şekilde servis sağlayıcılardan ağ operatörlerinden işlenen suça ilişkin delil elde etmek de

---

[17] Moor Keith, Police Smash Global Gang Behind 500.000 Aussie Credit Cards Theft (29 November 2012) Herald Sun, [1]-[10] (Çevrimiçi) http://www.heraldsun.com.au/news/law-order/police-smash-global-gang-behind-500000-aussie-credit-card-thefts/story-fnat7jnn-1226526111909, 01.04.2015

[18] Leyla Keser Berber, Adli Bilişim, Yetkin Yayınları, Ankara 2004, s 44

bir o kadar sorun teşkil etmektedir. Elektronik halde bulunan delil göz açıp kapayıncaya kadar değiştirilebilir, taşınabilir veya silinebilir. Diğer taraftan, bazen kolluk güçlerinde delil toplarken yapacakları bilinçsiz müdahaleler ile delili bozabilir ya da usuli hatalar ile delili hukuka aykırı hale getirebilir.

3. Araçlar (Zararlı Yazılımlar)

Siber suçlular tarafından suçta kullanılan yazılımlar, bir anda binlerce kişiyi mağdur edebilecek bir zarara yol açabilir. Bir zararlı yazılım olan phishing yöntemiyle, sadece bir kez bilgisayarın klavyesine tıklama, yüzbinlerce kişinin bilgisayarına aynı anda ulaşma anlamına gelebilmektedir.[19] Yarattığı etki alanının dışında, bu suçta kullanılan vekil sunucular (Proxy server), sahte kullanıcılara ait e-posta gönderimi ya da IP adresleri (email spoofing, IP spoofing) gibi araçlar, siber suçlulara anonim kalma imkanı da sunmaktadır.

[19] Home Office, Cyber Crime Strategy (March 2010) Official-documents, (çevrimiçi) s. 10, p 34, http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf, 29.04.2015

III. SİBER SUÇLARDA ULUSAL VE ULUSLARARASI GİRİŞİMLER

A. Giriş

Günümüzde, farklı ırk, yaş, cins, sosyal ve ekonomik sınıftan milyarlarca insan[20], hukuk, sağlık, eğitim, ulaşım, enerji, ekonomi ve eğlence gibi kamu ve özel sektörlerde internet ve bilgisayara dayalı olarak çalışmaktadırlar. İnsanların çevrimdışı bir hayat tarzından çevrimiçi bir hayat tarzına doğru evirildiğini söylemek yanlış olmayacaktır. Bilgisayar ve internet kullanımının artması, elbette suçluların ilgisini de çekmiştir. Öyle ki, siber dünyada işlenen suçlar arttıkça, bu durum insanların çevrimiçi oldukları zamanlarda tercihleri üzerinde belirleyici olmaya başladı. Örneğin, 2008 yılında "müşterilerin çevrimiçi alışveriş korkuları" isimli bir çalışmada[21] "kimlik bilgileri hırsızlığının çevrimiçi alışveriş davranışlarını nasıl etkilediği sorusu altında ayrı ayrı başlıklarda, ankete katılan ve bu suçun mağduru olan kişilerin, %40'ı bilinen alışveriş sitelerinden alışveriş yaptıklarını; %26'sı etkilenmediklerini; %25'i çevrimiçi alışverişi azalttıklarını; %24'ü banka kartını daha az kullandıklarını; %21'i kredi kartını daha az kullandıklarını; %21'i alternatif ödeme yolları kullandıklarını; %19'u daha az para harcadıklarını; %12'si internet üzerinden alışveriş yapmayı terk ettiklerini belirtmişlerdir.

Artık siber uzayda yaşamın kaçınılmaz olduğu gerçeği ile karşı karşıya olduğumuz göz önüne alındığında, bu alanda kullanılan ağların ve verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması için belirli standart ve kuralların konulması gereği açıktır. Yukarıda verilen özelliklerinden de anlaşılacağı üzere yapılacak yasal düzenlemelerin hem ulusal hem de uluslararası düzeyde olması gerekmektedir. Belki de bu durumu en iyi anlatan örnek "Love Bug" virüsüdür ki bu virüs, devletlere siber suç tarihinin en acı dersini vermiştir. "Love

---

[20] Internet Users in the World, Internet World Stats, Usage and Population Stats, (çevrimiçi) http://www.internetworldstats.com/stats.htm ,29.04.2015

[21] Consumer Online Shopping Fears,First Data, Market Briefs, (çevrimiçi) http://www.firstdata.com/downloads/thought-leadership/fd_consumeronlineshoppingfears_research.pdf. 29.01.2015

Bug" virüsü 11 Mayıs 2000 tarihinde ortaya çıkmış ve 10 Milyar Dolar zarara neden olmuştur.[22]Virüs hızlı bir şekilde tüm dünyaya yayılarak Beyaz Saray, FBI ve Pentagon'u dahi etkilemiştir.[23]Ancak, olayın faili de Guzman hakkındaki suçlamalar uygulanabilir bir yasal mevzuat olmadığı için düştüğü gibi olay nedeniyle en çok zarar gören ABD hükümetine de iade edilmemiştir.[24] Her ne kadar Filipinler devleti, olay sonrası e-ticaret ve bilgisayar korsanlığı ile ilgili yasa çıkardıysa da bu durum yasaların geriye yürümezliği ilkesi nedeniyle de Guzman cezalandırılması açısından bir anlam ifade etmemiştir.[25] 10 milyar dolarlık bu acı tecrübe, yasal boşlukların suçlular açısından nasıl güvenli bölgeler oluşturduğunu göstermiştir.

Bu ve bunun gibi olaylar, uluslararası toplumun dikkatine 3 ayrı yargısal soruna çekti: siber suçlara ilişkin ceza yasalarının olmaması, siber suçlara ilişkin ceza usul yasalarının olmaması ve devletler arasında uygulanabilir karşılıklı işbirliğinin olmaması.[26] Bu arada, Siber Suçlar Sözleşmesini bu gereksinimin ortaya çıkardığı söylenebilir.

Sözleşme'ye ve onun hukukumuz açısından incelenmesine geçmeden önce, kısaca ulusal ve uluslararası seviyede siber suçların yarattığı tehdidi ortadan kaldırmak için neler yapıldığı ele alınacaktır. Bu tehdidin boy göstermesi ile bilgisayarın icadı arasında çok zaman yoktur.[27] Bilgisayarların manipülasyonu, sabote edilmesi, casusluk faaliyetlerinde kullanılması gibi suça konu olabilecek eylemler 1960'lardan itibaren gerçekleştirilmeye başlanmıştır.[28]

---

[22] Lev Grossman, 'Attack of the Love Bug' (15 May 2000) Time, p3 - p5 (çevrimiçi) http://www.time.com/time/magazine/article/0,9171,996899-1,00.html, 29.04.2015

[23] "Love Virus Chaos Spread" (4 May 2000) BBC, (çevrimiçi) p. 5. http://news.bbc.co.uk/2/hi/uk_news/736208.stm, 29.04.2015

[24] Lack of Applicable Law Allows Alleged Hacker Loose, Amorillo, (çevrimiçi) http://amarillo.com/stories/2000/08/22/usn_hacker.shtml, 01.04.2015

[25] 'Charges Dropped in Love Bug Virus Case' (08/01/2015) ABC, (çevrimiçi) http://abcnews.go.com/Technology/story?id=119536, 02.04.2015

[26] Amalie M. Weber, The Council of Europe's Convention On Cybercrime, 2003, 18 (1) Berkeley Technology Law Journel, s. 426-428

[27] Jonathan Clough, Principles of Cybercrime, Cambridge University Press, 2010, s 6

[28] Sieber Ulrich, Legal Aspects of Computer Related Crime in the Information Society (1 January 1998) Europa.Eu, (çevrimiçi) s.19 http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html, 20.04.2015.

B. Ulusal Girişimler

Bilgisayar ile ilgili yaşanan sorunlara karşı kabul edilmese bile ilk düzenleme, 1977 yılında ABD'de sunulan, Federal Bilgisayar Sistemlerinin Korunması isimli yasa tasarısıdır.[29]Genel olarak, ulusal anlamda, siber suçlara karşı düzenlemeler, 1970 ve 1980'li yıllarda, verilerin toplanması ve iletilmesi ile sınırlı kalmıştır.[30] İkinci dalga ise, 1980'li yılların başında, daha çok bilgisayar ile bağlantılı ekonomik suçlarla ilgili olmuştur.[31]İkinci dalgayı, 1980'li yıllarda bilgisayar teknolojilerinde ortaya çıkan fikri mülkiyet haklarının korunmasına dair yapılan düzenlemeler takip etmiştir.[32] 1980 ve 1990'lı yılların ortalarına kadar dördüncü dalga, hakaret, pornografi ve nefret suçlarında bulunan yasadışı ve zararlı içeriklerle ilgili yasal düzenlemeler; beşinci dalga ise usul yasasına ilişkin yasal düzenlemeler olurken, son olarak 1990'lı yıllar boyunca ülkeler güvenlik tedbirleri ile ilgilenmişlerdir.[33]Sonrasında ise her devlet kendi ulusal mevzuatları üzerinden siber suçlarla mücadele etmişlerdir.

C. Uluslararası Girişimler

Siber suçların karanlık bir yanı olduğu uluslararası aktörler tarafından kabul edilmiştir. Özellikle, OECD, Avrupa Konseyi, Avrupa Birliği, G8 ve Interpol, siber suçların anlaşılması ve onunla daha etkin mücadele edilmesi için çok değerli katkılar sunmuşlardır. Ancak, Avrupa Konseyi Siber Suçlar Sözleşmesi, siber uzayın kötüye kullanılması karşısında ortaya konun çözümler arasında en etkin ve etkili hukuki bir enstrüman olarak öne çıkmıştır.

1. OECD

Siber suçlarla mücadele tarihinde, OECD (Ekonomik Kalkınma ve İşbirliği Örgütü), 1983 ve 1985 yılları arasında, siber suçlara karşı uluslararası anlamda ulusal ceza yasalarının birbiri ile uyumlu bir şekilde yürütülmesi için çalışma

---

[29] Schjolberg Stein - Hubbard Amanda, 'Harmonizing National Legal Approaches on Cybercrime' (10 June 2005) International Telecommunication Union, (çevrimiçi) s. 5. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, 20.04.2015.
[30] Sieber, s. 25
[31] Sieber, s. 27
[32] Sieber, s 28-31
[33] Sieber, s. 31

başlatan ilk uluslararası bir örgüttür.[34]Daha sonra, 1986 yılında, devletlerin hangi eylemlerin siber anlamda suça konu olduğunu takip edebilecekleri model bir liste hazırlamıştır.[35]6 Kasım 1992 tarihinde ise, örgüt, 24 üye ülkesi ile birlikte "Bilgi Güvenliği Sistemleri için Rehber ile İlgili Kurul Tavsiyesi" kabul etmiştir.[36] Bu tavsiye, kamu ve özel sektörde bilgi sistemleri güvenliği için standart ve prensipleri belirlemeyi ve uluslararası işbirliğini teşvik etmeyi amaçlıyordu.[37] 1997 ve 2002 yıllarında, hazırlanan tavsiye örgüt tarafından tekrar gözden geçirildi.[38] Tavsiyenin 1997 yılı versiyonu, 1992 yılı versiyonunu sorunları çözmede yeterli bulurken, 2002 yılı versiyonu, bilgi sistem ve ağlarını öngörülen risklerden korumak için yeni bir çerçeve sundu ve daha açık bir internet ve ağlar arası artan ilişki karşısında daha etkin olmayı sağladı.[39]2007 yılında, tavsiyenin anılan 2002 versiyonu birinci kez, 2012 yılında ise, ikinci kez gözden geçirilerek güncellendi.[40] Tavsiyenin bağlayıcı bir etkisi olmasa da, genel olarak kabul edilen uluslararası bir ölçüt olarak her zaman devletler üzerinde olumlu bir etkisi olmaktadır. [41]

2. Birleşmiş Milletler

Birleşmiş Milletler, en büyük uluslararası örgütlenmedir. OECD'den farklı olarak, yapılan anlaşmalarla, devletleri bağlayıcı kararlar alabilme gücüne sahiptir. 1990'lar gibi erken bir dönemde 8. Suçların Önlenmesi ve Suçlulara Muamele Kongresi'nde siber tehditler hakkında hazırlanan rapor esas alınarak, Birleşmiş

---

[34] United Nations Manual on the Prevention and Control of Computer-Related Crime, 43-44 International Review of Criminal Policy, UN Doc E/94/IV/5 (1994) p.117, (çevrimiçi) http://www.uncjin.org/Documents/EighthCongress.html, 01.04.2015

[35] A.g.e., p. 118

[36] Recommendation of the Council Concerning Guidelines for the Security of Information Systems (26 November 1992) OECD, (çevrimiçi) http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm, 04.04.2015.

[37] A.g.e.

[38] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Society (25 July 2002) OECD, 16, http://www.oecd.org/sti/ieconomy/15582260.pdf, 04.04.2015.

[39]Review of the 2002 Security Guidelines (2012) OECD, (çevrimiçi) s.33, http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf, 01.01.2015.

[40] A.g.e., s. 45

[41] A.g.e., s. 34

Milletler Genel Kurulu bir karar almıştır.[42] Örgüt, 1994 yılında, maddi ceza ve usul hukuku, bilgisayar bağlantılı suçların önlenmesi ve uluslararası işbirliğine dair hazırlanan BM Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrol Altına Alınması Rehberi yayımlamıştır.[43] 2001 yılında ise, Genel Kurul, uluslararası işbirliği ve koordinasyonu teşvik etmek, suçlular için güvenli bölgeleri yok etmek kolluk güçleri ve savcılara bu alanda eğitim vermek ve devletleri bu sorunları çözmek için gerekli tedbirleri almaya davet etmek için "Bilgi Teknolojilerinin Kötüye Kullanılması ile Mücadele" hakkında ikinci bir karar kabul etmiştir.[44]2005 yılında, ayrı bir siber suçlar sözleşmesi oluşturulması konusu düzenlenen bir kongrede tartışılmış, ancak BM, devletlere teknik destek ve yardım sağlanmasının, sözleşme yapmaktan daha faydalı olacağı sonucuna varmıştır.[45]Daha sonra, örgüt, yasal düzenleme tavsiyeleri yerine, üye devletlere teknik destek vermeye ve teknik yeterlilikleri üye devletler arasında daha uyumlu hale getirmeye öncelik haline getirmiştir.[46]

3. G8

Dünyanın en büyük endüstrileşmiş ülkeleri tarafından oluşturulmuş bir yapılanmadır. Uluslararası bir forum olup, her yıl toplanarak uluslararası politika belirler. 1995 yılında düzenlenen Halifaks zirvesinde, G8 ülkeleri, ülkelerin güvenliğine karşı organize suçların oluşturduğu tehdit nedeniyle Sınıraşan Organize Suçlarla İlgili Uzmanlar Grubu(the Lyon Group) kurmuşlardır.[47] Bu

---

[42] Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, A/RES/45/121, UN GAOR, 68th plen mtg, (14 December 1990) (çevrimiçi) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121 , 29.04.2015

[43] United Nations Manual on the Prevention and Control of Computer-Related Crime, 43-44 International Review of Criminal Policy, UN Doc E/94/IV/5 (1994) 117, (çevrimiçi) http://www.uncjin.org/Documents/EighthCongress.html, 01.04.2015

[44] Combatting the Criminal Misuse of Information Technologies, A/RES/55/63, UN GAOR, 55th sess, Agenda Item 105, (22 January 2001) (çevrimiçi), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf , 29.04.2015

[45] Around the Clock Capability Needed Successfully Fight Cybercrime, Workshop Told, BKK/CP/22, 10th mtg, (Bangkok, Thailand, 23 April 2005), (çevrimiçi), s.2., http://www.un.org/events/11thcongress/docs/bkkcp22e.pdf , 29.04.2015

[46] Stefan Fafinski, Computer Misuse: Response, Regulation and the Law, Willian Publishing, 2009, s. 230.

[47] Amandine Scherrer, The G8 and Transnational Organized Crime: The Evolution of G8 Expertise on the International Stage (21 January 2008) G8.Utoronto, (çevrimiçi) 9 http://www.g8.utoronto.ca/speakers/scherrer2008.htm , 29.04.2015

grup, 1996 yılında, hazırladıkları 40 tavsiye ile İleri Teknoloji Alt Grubu'nun kurulmasını sağlamıştır.[48]1997 yılında düzenlenen Denver zirvesinde, siber suçlarla mücadelede ileri teknoloji suçlarının faillerinin soruşturulması, kovuşturulması ve cezalandırılması için bir bildiri yayımlanmıştır.[49] Aynı yıl G8 üye ülkelerinin Adalet ve İçişleri Bakanları, ileri teknoloji suçları ile ortaya çıkan sorunlara çözüm için 10 prensip ve eylem planı kabul ettiler.[50] 2000 yılında Japonya'da düzenlenen zirvede, OECD Bilgi Güvenliği Rehberi'ne paralel olarak gerekli politika ve tedbirlerin uygulanmasının gerekliliğinin vurgulandığı Okinava Küresel Bilgi Toplumu Bildirisini ortaya konuldu.[51]Bununla birlikte, G8 her vesile ile siber suçlardan arınmış daha güvenli bir siber uzay kararlılığını vurgulamaktadır. Özellikle, bu kapsamda, G8, kendisine üye devletlerin Avrupa Konseyi Siber Suçlar Sözleşmesine taraf olması için çağrıda bulunmakta ve üye devletlerden uluslararası örgütlerin bu yönde vermiş olduğu tavsiyelere uyulmasını istemektedir.[52]

4. Interpol

Bünyesinde 190 üye devleti barındırmakta olup, dünyanın en büyük polis örgütlenmesidir. Interpol, siber suçlarla mücadelesini üç alanda yoğunlaştırmıştır: uyumlaştırma (harmonization), kapasite geliştirme (capacity building) ve operasyonel destek ve adli bilişim.[53] Örgüt,

- uyumlaştırma bağlamında, ulusal mevzuatı takip eder; ulusal polisin altyapı ve teknik kapasitesini gözlemler ve ona tavsiyelerde bulunur; siber

[48] Fafinski, 231.
[49] Denver Summit of the Eight: Communiqué, (22 June 1997) G8, (çevrimiçi) 40 http://www.g8.utoronto.ca/summit/1997denver/g8final.htm , 29.04.2015
[50] Meeting of Justice and Interior Ministers of the Eight (10 Dec 1997) CoE, (çevrimiçi) 3 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/24%208%20Communique_en.pdf , 29.04.2015
[51] Okinawa Charter on the Global Information Society (22 July 2000) G8, (çevrimiçi) 8 http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm , 29.04.2015
[52] G8 Recommendations on Transnational Crime (01 December 2008) Canada International, part IV section D (çevrimiçi) http://www.npa.go.jp/sosikihanzai/kokusaisousa/kokusai1/transg8rece.htm , 29.04.2015
[53] Activities, Interpol, (çevrimiçi) http://www.interpol.int/Crime-areas/Cybercrime/Activities , 29.04.2015

güvenlik stratejilerinin geliştirilmesine yardımcı olur; uluslararası platformlarda yapılan yasa çalışmalarında kolluğu temsil eder; araştırma ve geliştirme çalışmaları yürütür,

- kapasite geliştirme bağlamında, adli bilişim, soruşturma teknikleri ve siber suçlar gibi konularda eğitim kursları düzenler,
- operasyonel destek ve adli bilişim bağlamında, yürütülen soruşturmaların her aşamasında anlık izleme, zararlı internet hareketleri analizi ile istihbari ve uzmanlık paylaşımlarında bulunur. Bu nedenle, Afrika, Amerika, Avrupa ile Asya ve Orta Doğu ile Kuzey Afrika bölgelerinde Interpol çalışma grupları kurmuştur.

Bunların yanı sıra, Interpol, Singapur'da siber suçların belirlenmesi ve önlenmesi amacıyla yaklaşık 200 kişinin çalışacağı ve bir adli dijital laboratuvarından soruşturmaların koordine edileceği "Interpol Global Complex for Innovation (IGCI)" isminde küresel bir koordinasyon merkezi kurmaktadır. [54]

Son olarak, Interpol'ün çalışma sistemi hakkında fikir verebilecek bir operasyona[55] yer vermek faydalı olacaktır. Operasyon, 26 ve 27 Kasım 2014 tarihlerinde 60'dan fazla havayolu şirketi ve 45 ülkeyi kapsayacak şekilde Europol, Interpol IGCI ve AMERIPOL tarafından yönetildi. Şüpheliler, çalıntı ve sahte olarak üretilmiş kredi kartları ile hileli yollarla uçak bileti satın alıyorlardı. Operasyon sırasında, şüpheli görülen bilet satın alma işlemleri hazır bulunan havayolu şirketleri ve American Express, MasterCard, Visa Inc. ve Visa Europe gibi büyük kredi kartı şirketlerinin temsilcileri tarafından tespit edilirken Interpol, aranan şahısların kimliklerinin belirlenmesi ve çalıntı seyahat belgelerinin ortaya çıkarılması işini yürütüyordu. Görüldüğü üzere, İnterpol, uluslararası aktörler ve özel sektör tüzel kişilikleri ile birlikte çalışmaktadır.

---

[54] D'cruz Theodora, Interpol Opens Singapore Center to Fight Cybercrime, 02.10.2014, (çevrimiçi) http://www.reuters.com/article/2014/10/02/us-asia-cybersecurity-idUSKCN0HR0OG20141002 ,29.04.2015

[55]Global Action Against Online Fraud in the Airline Sector Nets 118 Arrests, Interpol, 28.11.2014, (çevrimiçi) http://www.interpol.int/News-and-media/News/2014/N2014-228, 29.04.2015.

5. Avrupa Birliği

28 Avrupa ülkesi arasında ekonomik ve siyasi bir ortaklık olan Avrupa Birliği, siber suçlarla mücadelede 07.02.2013 tarihli AB Siber Güvenlik Stratejisi[56] doğrultusunda uyguladığı bir mevzuata ve desteklediği operasyonel bir işbirliğine sahiptir. Siber Güvenlik Stratejisi, Avrupa Birliği'nin bu alanda ortaya koyduğu en kapsamlı belgedir. Strateji, siber uzayda ortaya çıkabilecek iç pazar, içişleri, dışişleri ve adalet ile ilgili sorunlara çözüm getirmeye çalışmıştır. Strateji, ayrıca sunduğu yasa teklifi (directive) ile özgürlük, açıklık, fiziki dünyada uygulanan AB değerleri ve yasalarının siber dünyada da uygulanması gerekliliği ve siber sorunlarla ilgili karşılıklı işbirliğini öncelemekte ve böylece insanların internet üzerinden ticaret yapacağı ve ekonomik büyümenin gerçekleşeceği beklenmektedir.[57]

Ayrıca, Avrupa Birliği bünyesinde bulunan Avrupa Komisyonu, Europol içerisinde Avrupa Siber Merkezi (European Cybercrime Centre)'ni kurdu ve bu merkez 1 Ocak 2013 tarihinde çalışmalarına başladı.[58] Merkez, siber suçlarla mücadelede Avrupa Birliği içerisinde odak noktası olmayı planlamakta ve şu an Europol'de var olan altyapı ve kolluk gücünü kullanmaktadır.

Avrupa Birliği, yine bu kapsamda, 2001 yılında nakit para dışında yollarla yapılan ödemelerde gerçekleştirilen yasadışı eylemlerin cezalandırılması için "Dolandırıcılık ve Parada Sahtecilik Suçları ile Mücadele için Çerçeve Kararı almıştır. [59]

---

[56] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2013/01 final, (çevrimiçi) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001, 29.04.2015.

[57] EU Cyber Security Strategy - Open, Safe and Secure, European Union External Action, 07.02.2013, (çevrimiçi) http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm, 29.04.2015.

[58] A Collective EU Response to Cybercrime, Europol, (çevrimiçi) https://www.europol.europa.eu/ec3 ,29.04.2015.

[59] Council Framework Decision of 28 May 2001 Combating Fraud and Counterfeiting of Non-Cash Means of Payment, European Union, 2001/413/JHA, (çevrimiçi) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001F0413 ,29.04.2015

2002 yılında ise, elektronik iletişim sağlayan servislerin, verilen servis hizmetinin güvenliğinin sağlanması ve müşterileri ait verilerin korunması için "E-Gizlilik Direktifi(2002/22/EC)" yayımlanmıştır.[60]

AB, "grooming" olarak bilinen internet ortamında yetişkinlerin kendilerini çocuk olarak tanıtıp hileli yollarla çocukların cinsel yönden istismar etmek gibi yeni suçlarla daha iyi mücadele etmek için 2011 yılında 2011/92/EU sayı ile "Çocukların Cinsel İstismarı ve Çocuk Pornografisi ile Mücadele Direktifi"ni[61], 2013 yılında ise Birliğe üye devletlerin siber saldırılara karşı yasalar çıkarması ve bu saldırılara ağır cezalar öngörmesi için 2013/40/EU sayı ile "Veri Sistemlerine Yapılan Saldırılara Dair Direktif"i yayımlamıştır.

Ancak, AB, yukarıda belirtilen strateji belgesinde de belirtildiği üzere, Siber Suçlar Sözleşmesi ya da diğer adıyla Budapeşte Sözleşmesi'ni referans olarak göstermekte ve mevzuat anlamında yeterli bulmaktadır. Hatta bazı hükümetlerin siber güvenliği bahane ederek yeni anlaşma tekliflerinde bulunmasını, bilgiye erişim ve ifade özgürlüğünü sınırlandırma olabileceği ihtimaliyle korkuyla karşılamaktadır.[62]

6. Avrupa Konseyi

Avrupa Konseyi, 47 üye devletten oluşmaktadır. Ayrıca Kanada, ABD, Israil, Japonya, Meksika ve Vatikan gözlemci devlet olarak Konseye katılmışlardır. Uluslar üstü bir yapılanma olarak Konsey, ekonomik, sosyal, kültürel, hukuki ve idari konularla ilgilenir.

---

[60] Directive 2009/136/EC of the European Parliament and of the Council 25 November 2009, European Union, (çevrimiçi) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF, 29.04.2015.

[61] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, European Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093, 29.04.2015.

[62] EU Cyber Security Strategy - Open, Safe and Secure, European Union External Action, 07.02.2013, (çevrimiçi) http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm, 29.04.2015.

13 Eylül 1989 tarihinde, Konsey, 1985 ve 1989 yılları arasında siber suçların ortaya çıkardığı sorunları inceleyen bir komite (Select Committeeof Experts on Computer-Related Crime of hte Council of Europe) tarafından hazırlanan metni bir tavsiye kararı olarak kabul etti.[63] Bu tavsiye kararı, özellikle hukuk ve hukuki uygulamaların uyumlulaştırılması ve uluslararası işbirliği açısından dikkat çekiciydi.[64] Daha sonra, 1995 yılında, Avrupa Konseyi, arama, el koyma, teknik takip, soruşturma birimleri ile işbirliği, e-delil, şifre kullanımı, araştırma, istatistik ve eğitim ve uluslararası işbirliği konularını kapsayan bir başka tavsiye kararı aldı.[65] Ancak, bu tavsiye kararlarının üye ülkeler üzerinde bağlayıcı bir etkisi yoktu. Bilgisayar teknolojilerinin kötüye kullanılmasını önlemek için bağlayıcılığı bulunan uluslararası bir enstrümanın gerekliliğini düşünerek[66], Avrupa Konseyi, 1997 yılında, maddi ve usul hukukunu içeren ve bağlayıcılığı bulunan bir sözleşme hazırlanması için bir komite (the Committee of Experts on Crime in Cyberspace-Committee 'PC-CY') kurdu[67]. Dört yıllık yoğun bir çalışmadan sonra, bu komite, 2001 yılı Haziran ayında hazırladığı taslağı, Suç Sorunları Avrupa Komitesi (CPDC)'nin onayına sundu.[68] CPDC Komitesi'nin onayını, 8 Kasım 2001 tarihinde Bakanlar Komitesi'nin kabulü takip etti.[69] Bakanlar Komitesi, 23 Kasım 2001 tarihinde, siber suçlarla ilgili Budapeşte'de düzenlenen bir konferans vesilesi ile

---

[63] United Nations Manual on the Prevention and Control of Computer-Related Crime, 43-44 International Review of Criminal Policy, UN Doc E/94/IV/5, 1994, 119, (çevrimiçi) http://www.uncjin.org/Documents/EighthCongress.html, 01.04.2015.

[64] Council of Europe Committee of Ministers, Recommendation No.R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (13 September 1989) 428th mtg (çevrimiçi) https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 , 29.04.2015.

[65] Council of Europe Committee of Ministers, Recommendation No.R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Infromation Technology (11 September 1995) 543rd mtg (çevrimiçi) http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp, 29.04.2015

[66]European Committee on Crime Problems, Meeting Reports, CM(97/4) (10 January 1997) Appendix II, 4b (çevrimiçi) https://wcd.coe.int/ViewDoc.jsp?Ref=CM(97)4&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864 , 29.04.2015.

[67] Sieber, s. 180.

[68] Explanatory Report, 15.

[69] Explanatory Report, 1.

Sözleşme'yi imzaya açtı.[70]Budapeşte Sözleşmesi olarak da bilinen sözleşme 1 Haziran 2004 tarihinde yürürlüğe girdi.

Bu Sözleşmeye paralel olarak, Avrupa Konseyi Meclis Kurulu'nun bir tavsiyesi üzerine, Bakanlar Komitesi, CPDC Komitesi ve onun PC-RX olarak bilinen Bilgisayar Sistemleri yolu ile İşlenen Irkçı ve Yabancı Düşmanlığı Suçlarına dair Uzmanlar Komitesi'ne ırkçılık ve yabancı düşmanlığı ile ilgili ek bir protokol hazırlamaları için yetki verdi.[71]Ek Protokol, 28 Ocak 2003 tarihinde imzaya açıldı[72] ve 1 Mart 2006 tarihinde yürürlüğe girdi[73].

[70] Explanatory Report, 1.
[71] Explanatory Report, Additional Protocol to the Convention on Cybercrime, p. 1.
[72] A.g.e., p 6
[73] Chart of Signatures and Ratifications (01.04.2013) Council of Europe (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=4&DF=&CL=ENG , 29.04.2015.

IV. SİBER SUÇLAR SÖZLEŞMESİ

A. Giriş

Çalışmamızın buraya kadar olan kısmına ilişkin çıkarılabilecek en önemli sonuçlardan birisi siber suçların önlenmesi ve ortaya çıkması halinde bastırılması için uluslararası işbirliği hayati önem taşımaktadır. Bu husus ulusal ve uluslararası aktörlerin üzerinde birleştiği bir noktadır. İşbirliği olmaksızın kolluk birimlerinin, özellikle sınır ötesiyle bağlantılı suçlarda etkin bir şekilde soruşturma yürütmesi ve olayın faillerini yakalayarak adalete teslim etmesi çok zor görünmektedir.

Küresel anlamda, belki de, hiçbir suç siber suç kadar zararlı değildir. Bazen polis suça konu olayın aydınlatılması için yeterli hukuki araç ve deneyime sahip olsa da, bu maddi gerçeğin ortaya çıkarılması ve şüphelilerin tespiti açısından yeterli olamayabilmektedir. Bir başka ifadeyle, yerelde polisiye anlamda başarılı bir görüntü vermek, siber suçlular için caydırıcı bir durum yaratmamaktadır. Çünkü siber suçların ucu açık bir suç sahası vardır ve bu saha içerisinde yer alan ögeler aynı anda birbiriyle hem bağlantılı ve bağlantısız olabilmektedir. Böylece işlenen suçun doğasından kaynaklanan bir zeminde suçlular, uzaktan, olay yerine gitmeksizin, insanları mağdur etmektedirler. Buna ilişkin çalışmamızın geride bıraktığımız kısımlarında örnek vermiştik.

Açık bir şekilde görülmektedir ki, küresel bir tehdit küresel bir cevap ve eylem gerektirir. Bu modern bir düzlemde karşılıklı yardımlaşmak suretiyle maddi ceza ve usul yasalarının uyumlulaştırılması anlamına gelmektedir.[74]Fakat henüz küresel bağlamda çok taraflı bir sözleşme kaleme alınmamıştır.[75]Tabi ki, devletlerin kendi siyasi ve sosyal değerlerindeki farklılıklardan kaynaklanan üzerinde uzlaşmaya varılmış bir siber suç tanımının olmaması bu durumu anlaşılabilir kılmaktadır.[76]

---

[74] Peter Csonka, The Council of European Convention on Cybercrime: A Response to Challange of the New Age(ed.), in Roderic Broadhurst and Peter Grabosky, Cyber-crime the Challange in Asia, Hong Kong University Press, 2005, 308-309.

[75]Brian Harley, A Global Convention on Cybercrime (23 March 2010) Stlr, (çevrimiçi) 1, http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ , 29.04.2015.

[76] Goodman - Brenner, s.143.

B. Sözleşme İhtiyacı ve Taraf Devletler

Küresel bir sözleşmenin yokluğu, çözülmesi gereken bir sorun olarak Brezilya'da düzenlenen Birleşmiş Milletler Suçun Önlenmesi ve Adalet 12. Kongresi'nde ele alındı ve burada böyle bir sözleşmesinin geliştirilmesi tavsiye edildi.[77]Bu açıdan, küresel olarak kabul edilmese de, Budapeşte Sözleşmesi, Avrupa Konseyi'ne üye olan ve üye olmayan devletlerin siber suçlarla mücadelede küresel bir adımı olarak kolektif bir çalışma ürünüdür. [78]

Bugün, Budapeşte Sözleşmesi, siber suçlar alanında en kapsamlı ve kapsayıcı uluslararası bir enstrüman durumundadır. Sözleşme, 37. maddesi uyarınca, Avrupa Konseyi'ne üye olup olmadığına bakılmaksızın tüm devletlere açıktır. Ancak, Budapeşte Sözleşmesi, maddi ceza hukuku, usul hukuku ve yargı yetkisini ilgilendiren konularda taraf olmayan devletler tarafından da takip edilmesi gereken bir model ortaya koyduğu için 37. maddede öngörülen prosedür sözleşmeden istifade etmek için tek yol değildir. Örneğin, Arjantin, Botsvana, Mısır, Nijerya, Pakistan ve Filipinler siber suç yasalarını hazırlarken sözleşmeye taraf olmamalarına rağmen ondan ilham almışlardır.[79]

Bu zamana kadar 49 devlet sözleşmeyi imzalarken, 39'u üye, 6'sı üye olmayan devlet (Avustralya, Dominik Cumhuriyeti, Japonya, Mauritis, Panama ve ABD) olmak üzere toplam 45 devlet sözleşmeyi onayladı. Üye ülkelerden Rusya ve San Marino henüz sözleşmeyi imzalamazken, Andora, Yunanistan, İrlanda, Lihtenştayn, Polanya ve İsveç imzaladıkları halde sözleşmeyi onaylamamışlardır.[80]

Sözleşme'nin devamı niteliğinde olan Bilişim Sistemleri Aracılığı ile İşlenen Irkçı ve Yabancı Düşmanı Eylemleri Suç Haline Getirilmesi için Avrupa

---

[77] Twelfth United Nations Congress on Crime Prevention and Justice, A/Conf.213/9 (22 January 2010), (çevrimiçi) p. 46, https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf , 29.04.2015

[78] Csonka, s. 303.

[79] Twelfth United Nations Congress on Crime Prevention and Justice, A/Conf.213/9, p. 33.

[80] Avrupa Konseyi, Sözleşme İmza ve onay tablosu, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, 29.04.2015.

Siber Suç Sözleşmesine Ek Protokol'ü ise 38 devlet imzalarken, sadece 23 devlet ayrıca onaylamıştır.[81]Türkiye, henüz ek protokolü imzalamamıştır.

C. Sözleşmenin Yapısı

Budapeşte Sözleşmesi, dört bölüm ve 48 maddeden oluşmakta olup, maddi ceza hukuku, usul hukuku ve uluslararası işbirliğine ilişkin düzenlemeleri ele alır. Birinci bölüm, Sözleşmede kullanılan temel dört terimin tanımını verir: bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi.

İkinci bölüm, iki kısımdan oluşur. Birinci kısım, tüm devletler için maddi ceza hukuku alanında suç olarak düzenlenmesi gereken eylemlere dair asgari standartların belirlenmesini amaçlar.[82] Bu bağlamda suçlar, bilgisayar veri ve sistemlerinin gizliliği, bütünlüğü ve erişilebilirliğine karşı suçlar; bilgisayar ile bağlantılı sahtecilik ve dolandırıcılık suçları; çocuk pornografisi olarak içerik ile ilgili suçlar; telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar şeklinde dört farklı kategoride düzenlenmiştir. Bu düzenlemelerin devamında, teşebbüs ve suça iştirak nedeniyle sorumluluk ele alınmıştır.

Bu bölümün ikinci kısmında ise, birinci kısımda tanımlanan suçların soruşturması yapılırken takip edilmesi gereken usuli hükümlere yer verilmiştir ve siber tehditlerin hızla değişen yapısına karşı daha canlı bir ceza usul yasası hedeflenmiştir. [83] Ancak, Sözleşmenin 14. maddesine göre, bu usuli hükümler, birinci kısımda belirtilen suçların dışında, bilgisayar ile işlenen diğer suçlarda ve bir suçun delillerinin elektronik ortamda toplanması durumunda da uygulanabilecektir. Bu kısımda öncelikle, uluslararası mevzuata atıf yapılarak insan hak ve özgürlüklerinin korunması ve orantılılık ilkesi şartına dikkat çekilmiş, bu yönde gerekli güvencelerin sağlanması istenmiş ve öngörülen yetki ve usullerin uygulanmasında üçüncü kişilerin hak, sorumluluk ve meşru menfaatlerinin gözetilmesi gerektiği vurgulanmıştır. Öngörülen yetki ve usuller, Sözleşme'nin, 16.

---

[81] Avrupa Konseyi, Sözleşme İmza ve onay tablosu, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, 29.04.2015.
[82] Explanatory Report, 33.
[83] Explanatory Report, 131- 132.

maddesinde, saklı bilgisayar verisinin hızlı korunması; 17. maddesinde, trafik verisinin hızlı korunması ve kısmen açıklanması; 18. maddesinde, şahıslara yönelik veriyi, hizmet sağlayıcılara yönelik abone bilgilerini ilgili makamlara teslim etmelerine yönelik üretim emri; 19. maddesinde, depolanmış bilgisayar verilerinin aranması ve bunlara el konulması, 20. maddesinde, bilgisayar verilerinin gerçek zamanlı toplanması; 21. maddesinde ise, içerik verilerine müdahale başlıkları altında ayrı ayrı düzenlemiştir.

Bu bölümün üçüncü kısmında ise, yargılama yetkisi kapsamında, işlenen suçlar hakkında yer bakımında uygulama ve vatandaş tarafından işlenen suçlara ilişkin düzenlemeler getirilmiştir. Üçüncü bölüm, uluslararası işbirliğine ilişkindir. Özellikle, suçluların iadesi ve karşılıklı yardımlaşmaya ilişkin konularında genel prensipler belirlenmiştir. Dördüncü ve son bölümde ise, son hükümler başlığı altında, Sözleşme'ye taraf olma ve Sözleşme'den ayrılma, çekince ve beyanlar ve uyuşmazlıkların çözümü gibi çeşitli hükümler yer almaktadır.

D. Sözleşme'nin Artıları ve Eksileri

Uluslararası kapsamlı bir Sözleşme olarak, Budapeşte Sözleşmesi şimdiye kadar yaptıkları nedeniyle övgüyü hak etmiştir. Daha önce de bahsedildiği üzere, Sözleşme, Avrupa Konseyi'ne üye olan ve olmayan devletler tarafından model olarak kabul edilmiştir. Anlaşılan o ki, Sözleşme, ileride siber suçlarla ilgili yapılacak yasal düzenlemelerde her zaman kendisine başvurulacak bir referans noktası, yarattığı olumlu ve olumsuz etkiler ve kendisi etrafında dönen tartışmalarla kendisinden istifade edilebilecek bir deneyim kaynağı olmuştur. Sözleşme'nin olumlu ve olumsuz yanları incelenmeksizin, siber suçlar alanında küresel bir hukuk metni ortaya çıkarmak zor olacaktır.

Sözleşme'nin ulusal ve uluslararası seviyede önemine rağmen, çok ciddi bir şekilde eleştirildiği de bir gerçektir. Örneğin, Amerikan Sivil Özgürlükler Birliği (American Civil Liberties Union), Sözleşme'yi, Amerikalıların özgürlüklerine bir tehdit olarak görmüş[84] ve yolsuz devletlerle yapılabilecek muhtemel işbirliği

[84] Laura W. Murphy - Marvin J.Johnson, ACLU Letter to the Senate Foreign Relations Committee on the Council of Europe Convention on Cybercrime (16 June 2004) ACLU, (çevrimiçi) p.9,

nedeniyle Sözleşme'nin onaylanmasının ABD'yi ahlaki açıdan iğrenç bir duruma sokacağını[85] iddia etmiştir.

İç hukukumuz bağlamında, Sözleşme'de yer alan hükümler ileride ayrıntıları ile ele alınacağından, bu bölümde Sözleşme'nin artıları ve eksileri başlıkları altında Sözleşme'nin sunduğu katkılar ve Sözleşme ile ortaya çıkan eksiklikler ele alınacaktır.

1. Sözleşme'nin Artıları

a) Asgari Bir Mutabakat Zemini Sunması

Sözleşme'nin en önemli başarısı, yasa dışı bir zeminde sınır ve kural tanımaksızın işlenmekte olan siber suçlara karşı üzerinde uzlaşılabilecek ortak noktaların tespiti ile ortaya çıkarılan hukuki bir metin üzerinde farklı sosyal, kültürel, ekonomik, hukuki ve siyasal birikim ve deneyimi bulunan devletleri kısmen dahi olsa buluşturabilmesi ve en azından böyle bir imkânı sunabilme kapasitesidir.

Gerçekten, Sözleşme'ye taraf olan devletlerde ve onu model olarak kabul eden diğer devletlerde maddi ceza ve usul hukukuna ilişkin birbirleri ile uyumlu bir mevzuat bulunmakta, bu zemin üzerinde kolluk ve adli işbirliği daha kolay sağlanabilmektedir. Bu özellikleriyle, Sözleşme, uluslararası düzeyde kabul edilmiş ve siber suçlarla mücadele, siber güvenlik ve bilginin korunması anlamında referans bir metin olarak gösterilmiştir.

Birleşmiş Milletler Genel Kurulu tarafından 21 Aralık 2009 tarihinde kabul edilen siber güvenlik küresel kültürünün yaratılması ve önemli bilgi altyapılarını korumak için ulusal çabalar hakkında düşünmeye dair kararda, Budapeşte

---

http://www.aclu.org/technology-and-liberty/aclu-letter-senate-foreign-relations-committee-council-europe-convention-cybe , 29.04.2015.

[85] Barry Steinhardt – Christopher Calabrese, ACLU Memo on the Council of Europe Convention on Cybercrime (16 June 2004) ACLU, (çevrimiçi) p.21 http://www.aclu.org/technology-and-liberty/aclu-memo-council-europe-convention-cybercrime , 29.04.2015.

Sözleşmesi'ne, siber suçların soruşturulması için oluşturulacak yasal çalışmalarda dikkat edilmesi gereken bir hukuki çerçeve olarak işaret edilmiştir.[86]

Avrupa İnsan Hakları Mahkemesi tarafından, K.U./Finlandiya kararında, Sözleşme'nin, bağlayıcılığı bulunan uluslararası bir enstrüman olduğu, bu alanda ilk ve tek uluslararası antlaşma olduğu açıklanarak müracaat edilmesi gereken ilgili bir hukuki materyal olduğu belirtilmiştir.[87]

Avrupa Birliği tarafından, 2010-2014 yılları arasında Birliğin adalet, özgürlük ve güvenlik alanlarında önceliklerinin belirlendiği Stokholm Programında, Sözleşme'nin küresel çapta siber suçlarla mücadelede referans bir yasal çerçeve olarak kabul edilmesi gerektiği belirtilerek, birliğe üye devletlerden en kısa zamanda Sözleşme'nin onaylanması istenmiştir. [88]

OECD'nin bünyesinde karapara aklamanın uluslararası alanda önlenmesi amacıyla kurulan ve Türkiye'nin de üyesi olduğu Mali Eylem Görev Gücü (Financial Action Task Force- FATF) tarafından terörizm ve silahlanmanın finansmanı ve karapara aklamanın önlenmesine dair uluslararası standartlara dair 2012 yılında belirlenen 40 tavsiye içerisinde, Budapeşte Sözleşmesi'ne taraf olunması ve hükümlerinin uygulanmasına da yer verilmiştir.[89]

Gelinen bu noktada artık elde edilen kazanımlardan sonra siber suçların önlenmesi ve bu suçlarla mücadelede başkaca bir sözleşme oluşturulması da bazı sıkıntılar yaratabilecektir. Örneğin, yeniden girişilecek böylesi bir çalışma, Budapeşte Sözleşmesi'nin etkinliği için sarf edilen kaynakların etkisinin azalmasına, Sözleşme ile ulusal düzeyde yapılan mevcut reformların bozulmasına, yılları alabilecek bu çalışma nedeniyle yeniden bir belirsizliğe ve Sözleşme ile

---

[86]Birleşmiş Milletler, A/RES/63/211, 17/01/2010, (çevrimiçi) s.5, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 , 29.04.2015.

[87] Case of K.U. v.Finland, başvuru no. 2872/02, 02/02/2008, (çecvrimiçi) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"]}, 29.04.2015.

[88] The Stockholm Programme, Official Journal of the European Union, (çevrimiçi) s.25 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010XG0504(01)&from=EN , 29.04.2015.

[89] FATF, 36. Tavsiye, (çevrimiçi) http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf , 29.04.2015.

sağlanan teknik desteğin durmasına yol açabilecektir. Sonuç olarak, muhtemelen uluslararası düzeyde daha fazla bölünme ve daha az işbirliği ile belki de Sözleşme ile yükseltilen çıtadan daha düşük bir metin ortaya çıkacaktır.[90]

Sonuç olarak, Budapeşte Sözleşmesi, başlı başına bir kazanımdır.[91]Bu açıdan ona taraf olmakla ve hükümlerini uygulamakla, elde edilecek faydalarda artı bir değer olarak görülmelidir. Devletler için elde edilecek faydalar şöyle özetlenebilir: siber suçlarla ilgili mevzuata tutarlı bir iç yaklaşım sağlanacak, elektronik delilin toplanması kolaylaşacak, siber anlamda karapara aklama, terör ve diğer suçların soruşturmaları kolaylaşacak ve devletlerarası siber suçlarla ilgili mevzuatların birbirleri ile uyum ve uygunluğu sağlanacak.[92]

b) Uygulanabilirlik

Şimdiye kadar 45 devlet Sözleşme'yi imzalamıştır ki bu, 45 devletin iç hukuklarını Sözleşme ile uyumlu hale getirdiği ya da getirmekte oldukları ve bu devletlerin birbirleri ile işbirliğine hazır oldukları anlamına gelmektedir.

Vatis, ABD Adalet Departmanı'nından bir görevli ile yapmış olduğu görüşmede, görevlinin, Sözleşme'nin siber suçlarla ilgili sorunlara çok olumlu etkisi olduğundan, Sözleşme öncesi ve sonrası döneme ait istatistiki verilere sahip olmasa da Sözleşme'nin uluslararası işbirliğini önemli ölçüde arttırdığından bahsettiğini aktarmaktadır.[93]

---

[90] Global Project on Cybercrime, The cybercrime legislation of Commonwealth States: Use of Budapest Convention and Commonwealth Law, 27/02/2003, Strazburg, (çevrimiçi) s. 16, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2571_Commonwealth_cy_leg_v21_27Feb%20rev_final_CoE.pdf , 29.04.2015

[91] Alexander Seger, The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is web, 16/02/2012, (çevrimiçi) s.3, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf , 29.04.2015

[92] Global Project on Cybercrime, The cybercrime legislation of Commonwealth States: Use of Budapest Convention and Commonwealth Law, s. 80.

[93] Michael A. Vatis, The Council of Europe Convention on Cybercrime (2010) National Academics, (çevrimiçi) s. 220, http://sites.nationalacademies.org/xpedio/groups/cstbsite/documents/webpage/cstb_059441.pdf , 29.04.2015.

Sözleşme'nin uygulanabilir olduğuna ve uygulandığına en güzel örneklerden birisi, ilerde açıklanacağı üzere, Sözleşme'nin 35. maddesinde "7/24 Ağ" başlığı ile kurulması öngörülen 7 gün 24 saat çalışma prensibi ile çalışan irtibat noktalarıdır. Anılan maddeye göre, devletler arası işbirliği kapsamında Sözleşme'ye taraf her devlette kurulan irtibat noktası ile bilgisayar sistem ve verileri ile ilgili suçlarla mücadelede ve elektronik delilin toplanmasında araştırma ve soruşturmalar açısından büyük bir kolaylık sağlanacaktır.

24/7 irtibat noktalarının işlevselliğine ilişkin 14 irtibat noktasından alınan cevaplarla ve Ohri Çalıştayındaki değerlendirmelerle 2008 yılında bir çalışma yapılmıştır. Bu çalışmada, genel olarak saklanan bilgisayar ve trafik verilerine ve şüphelilerin kimlik bilgilerine ilişkin olmak üzere, 2007 yılı ve 2008 yılının ilk on ayında, çok acil durumlarda ve istisnaen kullanılmasına rağmen irtibat noktalarından toplam 540 talebin gönderildiği ve 480 talebin alındığı ortaya konulmuştur.[94]

Gercke, uygulanabilirlik durumunu, Sözleşme'nin "işe yarayacağı ispat ispatlandı" diyerek özetlemektedir.[95]

Sözleşme'nin uygulanabilirliği veya Gercke'nin ifadesiyle işe yararlığı, Sözleşme'nin bizzat kendisiyle ilgili olduğu gibi, Sözleşme'nin 46. maddesine istinaden kurulan Siber Suç Sözleşmesi Komitesi (Cybercrime Convention Comittee – T-CY)'nin çalışmaları ile de ilgilidir. Komite tarafından, Sözleşme'nin nasıl uygulanacağına ve nasıl yorumlanacağına dair birçok çalışma bulunmaktadır. Bu çalışmaların Sözleşme'yi daha canlı tuttuğu kuşkusuzdur. Örneğin, hukuki, siyasi ve teknolojik gelişmeler ışığında Sözleşme'nin daha etkin kullanım ve uygulaması için bilgisayar sistemi, botnet, sınıraşırı erişim, kimlik dolandırıcılığı, DDOS saldırıları, önemli altyapı saldırıları, kötücül yazılım ve spam terimleri

---

[94] Project on Cybercrime, The Functioning of 24/7 Points of Contact for Cybercrime, 02/04/2009, (çevrimiçi) s24-25, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/567_24_7report4public_april09a.pdf , 29.04.2015.

[95] Marco Gercke, Siber Suç Sözleşme ile 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve Kusurları, İnternet Hukuku ed. Yener Ünver, Seçkin Yayıncılık, Ankara 2013, s105

tekrar ele alınarak yeniden yorumlanmışlardır.[96] Bugüne kadar 2006 yılından başlamak üzere, Komite, siber suçlarla mücadele ile ilgili toplam 12 önemli toplantı düzenlemiş ve bu toplantıları detayları ile rapor haline getirip resmi sitesinde yayımlamıştır. [97]

Uygulanabilirlik ile ilgili diğer bir önemli husus ise, bilinçli olarak tercih edilen "nötr" bir dil tercihidir. Böylece belirlenen üslup ile, maddi ceza hukuku bölümünde yer alan suçların, şimdiki ve gelecek teknolojilere de uygulanması hedeflenmiştir.[98]

Son olarak, Sözleşme'nin uygulamanın içine kamu kurum ve kuruluşlarının dışında Microsoft, McAfee ve Visa Europe gibi özel sektörden paydaşların da, katılımını sağlayarak siber suçlara karşı çoklu bir işbirliği ile ortak bir payda oluşturması da Sözleşme'nin uygulanabilirliğine katkı sağlamaktadır.[99] Açıklanan nedenlerle, Sözleşme'nin atıl olmadığı, hayatın içinde ve canlı olduğu söylenebilir.

c) İç Hukuku Güçlendirmesi

Sözleşme'ye taraf olan ve iç hukuklarında Sözleşme'nin hükümleri doğrultusunda yasal düzenlemeler yapan ülkelerde siber suçlara karşı alınan önlemlerde artış olduğu gözlemlenmiştir. Örneğin, Almanya'da, Sözleşme'nin 8. maddesine karşılık gelen bilgisayar ile bağlantılı dolandırıcılık suçlarında bulunan yasal boşluk Sözleşme ile birlikte doldurulmuş ve daha sonra polis kayıtlarına göre bu suç nedeniyle çok fazla sayıda suç dosyası oluşturulmuştur.[100] Böylece daha önce işlenen ancak takibi yapılmayan bu suç, yasal değişiklik sonrası birçok soruşturmaya konu olmuştur.

---

[96] T-CY Guidances Notes, Strasbourg, 08.12.2014 (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY(2013)29rev_GN%20compilation_v3.pdf , 29.04.2015.

[97] Action Against Cybercrime, Cybercrime Convetion Comittee, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp , 29.05.2015

[98] Explanatory Note, 36.

[99] Seger, s. 4.

[100] Seger, s. 4.

2. Sözleşme'nin Eksileri

a) Küresel Temsilde Yetersizlik

Küresel olarak, sadece siber suçlarla ilgili değil, herhangi bir suçla mücadelede ortak bir hukuki metin ortaya koymak her zaman için zor olmuştur. Devletlerarasında mutabakat sağlanacak ortak bir zemin bulunsa ve devletler tarafından ilgili sözleşmeye imza atılsa bile, ilgili devlet tarafından atılan bu imzanın ardından sözleşme onaylanmadıkça sözleşmenin herhangi bir bağlayıcılığı bulunmamaktadır.[101]

Uygulamada, devletler tarafından imzalanan, ancak sözleşmeye açık rızanın gösterildiği bir onay olmadığı için hiçbir bağlayıcılığı olmadan bekleyen sözleşmeler sıklıkla görülmektedir. Budapeşte Sözleşmesi bağlamında, Konseye üye devletlerden; Andora, Yunanistan, İrlanda, Lihtenştayn ve Monako, Konseye üye olmayan devletlerden; Kanada ve Güney Afrika açısından bu durum söz konusudur.

Diğer taraftan sözleşmelerin onaylanması da sözleşmeyle tam bir uyum anlamına da gelmemektedir. Yapılan onay işlemi ile birlikte ortaya konulan çekinceler, taraf olunan sözleşmede yer alan hükümlerin etkisini ortadan kaldırmakta ya da değiştirmektedir.[102]Bu anlamda Budapeşte Sözleşmesi'ne de taraf devletler tarafından birçok çekince konulmuştur.[103]

Elbette yukarıda sayılan bu iki sorun Budapeşte Sözleşmesi'ne özgü sorunlar değildir. Uluslararası olma iddiasında olan her sözleşme için geçerli olan bu iki soruna, Budapeşte Sözleşmesi de herhangi bir özel çözüm bulamamıştır.

Bu iki genel sorunun dışında, temsil konusuna da değinmek gerekmektedir. Her ne kadar Sözleşme, uluslararası seviyede, siber suçlarla mücadele alanında,

---

[101] 'Ratification', Glossary on Treaties,
< http://www.conventions.coe.int/?pg=/Treaty/Glossary_en.asp#Ratification >.
[102] Reservation, Glossary on Treaties, Council of Europe
< http://www.conventions.coe.int/?pg=/Treaty/Glossary_en.asp > .
[103] List of Declarations made with Respect to Treaty No. 185, Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 , 29.04.2015

uluslararası tolumun duruşunu sergileme adına haklı bir üne sahip olsa da; bu durum Sözleşmeyi imzalamayan veya Sözleşmeye taraf olmayan devletlerin sayısının, Sözleşmeyi imzalayan veya Sözleşmeye taraf olan devletlerin sayısından çok daha fazla olduğu gerçeğini değiştirmemektedir. Başka bir ifadeyle, Birleşmiş Milletler'e üye olan 193 ülke varken[104], Sözleşmeye sadece 45 devlet taraf olmuştur.[105]Özellikler siber suçluluk açısından, bu suçların yoğun olarak işlendiği Rusya ve Çin'in, Sözleşme'ye taraf olmaması küresellik iddiasında bulunan Sözleşme için ciddi bir handikaptır.[106] Dahası ne Asya kıtasından, ne Afrika kıtasından ne de Güney Amerika'dan henüz Sözleşme'ye taraf olan bir ülke yoktur.[107]Açıkçası Rusya'sız, Çin'siz, Hindistan'sız, Brezilya'sız bir Siber Suçlar Sözleşmesine küresellikten uzak demek çok yanlış olmayacak, küresel bir standart olarak kabulü ise "abartılı"[108]olacaktır.

Sözleşme'nin küreselliğine gölge düşüren bir başka kaygı verici konu ise devletlerin Sözleşme'ye onaylamaları ve taraf olmaları ile ilgili sürecin zaman alması ve yavaş işlemesidir.[109]Taraf devletlerin için bu süre ortalama 8,5 yıldır.[110]Örneğin, Polanya'nın, Sözleşme'yi imzalaması ve onaylaması arasında 13 yılı aşkın bir süre geçmiştir ki bu en uzun süredir. Ülkemiz açısından ise, 2001 yılında imzaya açılan Sözleşme, 2010 yılında imzalanıp 2014 yılında onaylanarak 4 yıl beklenilmiştir. 2001 yılından bu yana ise Sözleşme'yi 15 yıl beklediğimiz görülmektedir. Bu durum siyasilerin siber suçlarla mücadeleyi gündemlerinin son maddelerine bırakması ve devletlerin Sözleşme'ye uygun hukuki altyapı

---

[104] Member States of the United Nations (03 July 2006) UN, (çevrimiçi) http://www.un.org/en/members/index.shtml , 29.04.2015.
[105]Member States of the Council of Europe, Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, 29.04.2015.
[106] Vatis, s.220.
[107] A.g.e., s.220.
[108] Gercke, s.108.
[109] Seger, s. 5.
[110] Gercke, s.109.

hazırlıklarını tamamlamaya çalışması ile açıklansa da[111], yine de gelinen noktanın taraf devlet sayısı ve taraf olma süresi nazara alındığında tatminkâr olmadığı açıktır.

b) Uyumlaştırma Sorunu

Sözleşme, siber suçlarla mücadelede taraf devletler arasında hukuk ve uygulama birliği istemektedir. Sözleşme, bu isteğini bazen asgari standart olarak yapılması gerektiği vurgusu ile ifade ederken bazen de düzenleme yapılabileceği şeklinde daha yumuşak bir vurgu ile ifade etmektedir.[112] Bu nedenle taraf devletlerin en azından yapılması gereken hükümlerle ilgili eksiksiz bir uyumlaştırma sağlaması beklenmektedir.

Ancak Sözleşme'ye taraf devletlerin ilgili mevzuatları ile Sözleşme'nin ilgili hükümleri arasında asgari standartlarda bile bazen birebir uyum bulunmamaktadır. Siber suçların en temel hali olarak tarif edilebilecek haksız erişim ile ilgili Sözleşme'nin hükümleri ile taraf devletlerin haksız erişim suçuna ilişkin düzenlemeleri konuyla ilgili yeterli fikir verecektir.

Sözleşme'nin 2. maddesi yasadışı erişimi düzenlemektedir. Bu düzenlemeye göre, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim suç olarak sayılmıştır. Görüldüğü üzere burada sadece bilgisayar sistemlerine yasadışı bir şekilde erişim sağlandığında suçun işlendiği kabul edilmiştir. Buna rağmen Sözleşme'ye taraf devletlerden İtalya, Fransa ve Belçika sadece sisteme erişimi değil aynı zamanda sistemde yetkisiz bir şekilde kalmayı da suç olarak düzenlemişlerdir.[113]

Kimi devletler ise, Sözleşme'nin "yasadışı erişimin bilgisayar sisteminin bütününe ya da bir kısmına yapılmasını" suçun unsuru olarak düzenlemesine rağmen bilgisayar sisteminin bütününe ya da bir kısmı yerine başka unsurları da

---

[111] Seger, s. 5-6.

[112] Bu durum Sözleşme'nin maddelerinde geçen "shall" ve "may" gibi kiplerden anlaşılmaktadır.

[113] Lorenzo Picotti-Ivan Salvadori, National Legislation Implementing the Convention on Cybercrime – Comparative Analysis and Good Practices, 28.08.2008 Strasbourg, (çevrimiçi) s.14, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf , 29.04.2015

suçun konusu yapmışlardır. Bulgaristan, "kaynaklara erişimi"; Ermenistan, "içerisinde bilgi depolanmış bir bilgisayar sistemine girmeyi"; Hırvatistan, "bilgisayar veri ve programlarına erişimi"; Birleşik Krallık, "bilgisayar materyaline erişimi"; Avustralya, içerisinde bilginin tutulduğu bilgisayara ya da kısıtlı veriye erişimi" suç olarak düzenlemişlerdir.[114]

Görülmektedir ki, Sözleşme standartları ile ulusal mevzuatlar arasında farklılıklar bulunmaktadır ve bu Sözleşme'ye taraf devletlerin esasen Sözleşme'yi eksiksiz bir şekilde uygulama zorunluluğu olmadığını göstermektedir.[115]

c) Güncel Kalma Sorunu ve Kullanılan Dil

Hukukun evrensel ilkeleri hakkında söylenemese de, hemen her yasa eskimeye ve zamanla değiştirilmeye mahkûmdur. Bilgi teknolojilerinin hızla gelişmesi ve bu teknolojilerin kullanımının yaygınlaşması karşısında aynı akıbet ile Sözleşme'nin de karşılaşacağını tahmin etmek güç değildir. Bu nedenle Sözleşme'nin güncelliği ve Sözleşme'de tercih edilen dile eleştirilerin getirilmesi şaşırtıcı bir durum değildir.[116]

Önceden siber suçların, temel kavramlarını bilgisayar ve internet suçu oluştururken, şimdi bu kavramların yerlerini bilişim sistemleri ve verilere terk ettiğini görüyoruz ki [117] Sözleşme hazırlandığı dönem sonrası yaşanan bu değişime ayak uyduramamıştır. Şöyle ki, Sözleşme, sonradan yeni bir olgu olarak ortaya çıkan kritik önemdeki altyapılara saldırılar ve siber terörizm; hizmet aksatma/engelleme (DOS-Denial of Service) saldırıları ve büyük çapta alınan istek dışı e-postalar (spamming); şifrelerin, phishing (yemleme/oltalama) ve pharming

---

[114] A.g.e., s.15.
[115] Gercke, s. 110.
[116] Jonathan Clough, The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World (2012) 23(4) Criminal Law Forum 363, s.374.
[117] Joachim Vogel, Towards a Global Convention Against Cybercrime, First World Conference of Penal Law In The XXIst Century, Guadalajara (Mexico), 18-23 November 2007, (çevrimiçi) s.1, http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf , 29.04.2015.

(site trafiği yönlendirme) yöntemleri ile ele geçirilmesi; kimlik bilgilerine yönelik hırsızlıklar gibi suçlara cevap vermekte zorlanmaktadır.[118]

Bir başka örnek ise, Sözleşme hazırlanırken nadiren kullanılan çevrimiçi çocuk pornosuyla ilgili bir teknolojidir.[119]Bu teknoloji, çocuk pornosu içerikli videonun, web sayfasının video steam sürecinin teknik konfigürasyonu nedeniyle yazılımın bilgiyi ara belleğe almadan izlenmesidir. Sözleşme, bu duruma çözüm sunamazken; 2007 yılında Avrupa Konseyi, bu sorunu, Çocukların Cinsel Suistimal ve Cinsel İstismara Karşı Korunmasına İlişkin Sözleşme'ye "bilgi ve iletişim teknolojileri kullanarak çocuk pornografisine bilerek erişim sağlamak" eylemini bir suç olarak ekleyerek çözmüştür.[120] Yine Sözleşme, pornografik anlamda, ses dosyaları üzerinden çocukların tasvirini suç olarak düzenlememiştir.[121]

Sözleşme'de kullanılan dil ile güncelliğin korunduğu ileri sürülse bile, verilecek örneklerden de anlaşılacağı üzere sorun sadece kullanılan dil ile ilgili değildir. Sorun, bunun ötesinde yapıldığı dönem itibariyle öngörülemeyen ya da öngörülse de yeterli şekilde önem atfedilmeyen konuların çözümsüzlüğü ile ilgilidir.

Kullanılan dil de eleştirilmektedir. Mevcut ve olası suçlara uygulanabilirliğin sağlanması adına tercih edilen bu üslup, içerisinde bir belirsizliği de barındırdığı için özgürlükler açısından sorunlu bulunmuştur.

Sözleşme'nin 6. maddesinde "cihazları kötüye kullanılması" başlığı altında yapılan düzenleme örnek olarak verilebilir. Bu düzenleme, devletlerden, Sözleşme'nin 2. ila 5. maddelerinde tanımlanan suçların işlenmesinde kullanılacak cihazların (bilgisayar programları dahil) üretimi, satışı, kullanım amacıyla tedariki, ithali, dağıtımı veya başka surette elde edilmesini yasaklamalarını istemektedir.

---

[118] A.g.e., s.7.
[119] Gercke, s.116.
[120] Avrupa Konseyi Çocukların Cinsel Suistimal ve Cinsel İstismara Karşı Korunmasına İlişkin Sözleşme, (çevrimiçi) http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_tur.pdf , 29.04.2015.
[121] Gercke, s.117.

Bilgisayar sistemlerinin yetkili kişilerce test edilmesi veya korunması düzenlemenin kapsamı dışında bırakılarak korunmuştur. Düzenlemede sorun, suça konu cihazların yasaklanması ile bu cihazların yasal olarak kullanılması arasında nasıl bir denge kurulacağı noktasında çıkmaktadır.[122]Söz konusu cihazları kullanmak suretiyle bilgisayarını korumak isteyen ortalama bir bilgisayar kullanıcısı, yapılan düzenleme ile bu cihazlara ulaşamama ihtimali ile karşı karşıya kalacaktır.[123]

Belirsiz dil kullanımına bir başka örnek ise, Sözleşme'nin 14. maddesinde yer alan "diğer suçlar" ifadesidir. Bu düzenlemeye göre, taraf devletler bilgisayar vasıtasıyla işlenen diğer suçlara uygulanacak yetki ve usullere ilişkin gerekli yasal ve diğer tedbirleri alacaklardır. Sözleşme'de tanımlanmayan diğer suçlarla ilgili olarak yetki ve usullerin neden genişletilmesi gerektiği ve diğer suçların ne olduğu gerçekten izaha muhtaçtır.[124]

Yine Sözleşme'nin 15. maddesinin 2. fıkrasında yetki ve usullerin tabi olacağı şart ve önlemler üzerinde adli makamların dışında varlığı öngörülen "bağımsız denetim" de sorunlu gözükmektedir. [125]Adli makamların denetiminin neden tek başına yeterli görülemediği anlaşılamamıştır.

Bu yönde kaygılar, kişisel verilerin işlenmesine dair kişilerin korunması hakkında çalışma yürüten Çalışma Grubu (Working Party) tarafından da Sözleşme'nin daha tasarı aşamasındayken dile getirilerek, kullanılan dilin belirsiz ve karışıklığa yol açıcı olması nedeniyle açıklanmaya ihtiyacı olduğu

---

[122] Clough, The Council of Europe Convention on Cybercrime: Defining 'Crime' in a Digital World, s. 378.
[123] Ryan M.F. Baron, A Critique of the International Cybercrime Treaty (2011-2002) 10 Commlaw Conceptus 263, 272.
[124] Yaman Akdeniz, Akdeniz Yaman, An Advocacy Handbook for the Non Governmental Organizations, Cyber-rights.org, (December 2003), (çevrimiçi) s.9, http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf , 29.04.2015
[125] A.g.e., 13-14.

vurgulanmıştır.[126] Gerçekten, insan hak ve özgürlükleri üzerinde etkileri olabilecek Sözleşme hazırlanırken daha dikkatli bir dil kullanılabilirdi.

d) AİHS Açısından Eksiklikler

Sözleşme'nin giriş bölümünde yasanın uygulanması ve temel insan haklarına saygı arasında uygun bir dengenin sağlanması gerekliliği hususunda bir farkındalık ortaya konulmuştur. Yani siber güvenlik ile özgürlükler arasında ortaya çıkabilecek çıkar çatışmasında çıkarların birbirine feda edilmeyeceği ve her iki dengenin de gözetileceği belirtilmiştir.

Yine Sözleşme'nin 15. maddesinde 1950 tarihli Avrupa İnsan Hakları Sözleşmesi ve 1966 tarihli Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'ne özellikle isim zikretmek suretiyle atıfta bulunularak tüm insan hakları belgelerinin bir şart ve tedbir olduğu vurgulanarak yetki ve usulün bu çerçevede uygulanması gerektiği belirtilmiştir.

Sözleşme'de yer alan yukarıdaki iki vurgu, Sözleşme'yi insan hak ve özgürlüklerinin korunmasında yetersiz olduğu eleştirisinden kurtaramamıştır. Sözleşme'den insan hak ve özgürlüklerinin korunması bağlamında daha keskin ve daha açık ifadelerle olası ihlallere karşı daha belirgin bir kararlılığın ortaya konması beklenmiştir.[127]

Sözleşme'nin 18. maddesinin 1. fıkrasının (a) bendine göre, yetkili merciler; sorumluluk alanındaki bir kişiye bilgisayar sisteminde yer alan ya da bilgisayar verilerini saklamakta kullandığı başka bir cihaz içerisindeki bilgisayar verisini teslim etme talimatını verme ile yetkilendirilmişlerdir. Böylece mahkeme, savcılık ya da duruma göre kolluk güçleri, kişilere bilgisayarlarında bulunan verilerin teslimi için talimat verebileceklerdir.

---

[126] Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cybercrime, 5001/01/En/Final, WP 41, (22.03.2001) (çevrimiçi) s.8, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp41en.pdf, 29.04.2015.
[127] Akdeniz, s.11.

Bu şekilde yapılan bir düzenlemeyi şüphelinin susma ve kendini suçlayıcı delil sunmaya zorlamama hakkı ile açıklamanın imkânı yoktur.[128]İHAS'nin 6. maddesinde düzenlenen adil yargılanma hakkı kapsamında değerlendirilen bu haklar, hakkaniyete uygun yargılama hakkının zımni bir parçası olup, kişinin hem aleyhine olan beyanda bulunmama hem de aleyhine olan belgeleri vermeme hakkını kapsar.[129] İHAM'nin Funke kararında bu hususa değinilerek, susma ve kendini suçlamama hakkının geniş bir içeriğe sahip olduğu, belge ve ticari kayıtları vermeyi reddetme hakkını da kapsadığı belirtilmiştir.[130]Böyle haklara sahip şüpheli veya sanıktan kendisini suçlu durumuna düşürecek verileri istemek veya bu verilere ulaştırabilecek şifreleri istemek hak ihlaline neden olacaktır.

Sözleşme'nin, 20. maddesinde düzenlenen trafik bilgilerinin gerçek zamanlı olarak toplanması ve 21. maddesinde düzenlenen içerikle ilgili bilgilere müdahale ile ilgili bazı hükümler de İHAS'ın 8. maddesine temas eden yanları itibariyle eleştirilmiştir.[131]

Sözleşme'nin 20. maddesinin 1. fıkrasının (b) bendinde devletlerin, yetkili mercileri; hizmet sağlayıcıları, mevcut teknik imkânları çerçevesinde, trafik verilerini toplamaya veya kaydetmeye zorlama ya da trafik verilerini toplamak veya kaydetmek için işbirliği yapmaya ve yardım etmeye zorlama ile yetkilendirmesi öngörülmüştür.

Sözleşme'nin 21. maddesinin 1. fıkrasının (b) bendinde devletlerin, yetkili mercileri; hizmet sağlayıcıları, mevcut teknik imkânları çerçevesinde, içerik verilerini toplamaya veya kaydetmeye zorlama ya da içerik verilerini toplamak veya kaydetmek için işbirliği yapmaya ve yardım etmeye zorlama ile yetkilendirilmesi istenmiştir.

---

[128] Akdeniz, s.14.
[129] Sibel İnceoğlu, Adil Yargılanma Hakkı, İnsan Hakları Avrupa Sözleşmesi ve Anayasa, Anayasa Mahkemesine Bireysel Başvuru Kapsamında Bir İnceleme (Editör, Sibel İnceoğlu), Şen Matbaa, Ankara 2013, s.246.
[130] Funke v. France, İHAM, başvuru no. 10828/84, 25.02.2015, p.44.
[131] Akdeniz, s.14-19.

Bu iki maddeden hizmet sağlayıcılardan trafik ve içerik verilerinin toplanması ve kaydedilmesine olanak sağlayacak teknik izleme araçlarının kullanılmasının istendiği anlaşılmaktadır. Hizmet sağlayıcılar, sahip oldukları bu teknik altyapı ile kişilerin bilişim sistemleri üzerinde bıraktıkları izler tespit edecek ve yetkili mercilere yardım edeceklerdir. Siber suçlarla mücadele anlamında öngörülen bu tedbirlerin kapsamına ve nasıl kullanılacağına ilişkin açık bir hüküm bulunmamaktadır.

Sözleşme'de yer alan bu düzenlemeler, yine Sözleşme'nin 20/3 ve 21/3 maddeleri ile birlikte değerlendirildiğinde durum daha da vahim olmaktadır. İlgili düzenlemelere göre, taraf devletler, hizmet sağlayıcıları trafik ve içerik bilgilerinin teminine yönelik kendilerine yetkili merciler tarafından yapılan talepleri gizli tutma sorumluluğundadır. Bu şu demektir: yetkili merciler hizmet sağlayıcılara ait ağlara ulaşma yetkisine sahip olacaklar, gerekirse kitle izleme ve dinlemesi bile yapabilecekler[132] ve bütün bunlar gizlilik içerisinde yürütülecek. Bu gizlilik nedeniyle vatandaş belki de özel hayatına müdahale edildiğini bilemeyecektir.

Halbuki, İHAM; gizlice yapılan teknik izlemenin keyfi kullanılabilme ihtimali nedeniyle riskli olacağını, yetkili merciler tarafından teknik izleme ve müdahalenin hangi şartlarda yapılabileceği konusunda vatandaşlar tarafından anlaşılabilecek bir öngörülebilirliğin olması gerektiğini, sürekli daha da karmaşıklaşan teknoloji karşında bu konuda yapılacak yasal düzenlemelerin daha açık ve ayrıntılı olmasını kabul etmektedir.[133]Aynı husus başka bir yerde, uygulanacak mevzuatta, keyfiliğin önüne geçmek için meşru amaca hizmet bağlamında, yetkili mercilerin takdir hakkının kapsamının ve mevzuatın uygulama yönteminin ortaya konulması gerektiği şeklinde belirtilmiştir.[134] Aksi durumun,

---

[132] Rodney Serkowski, Submission to the Joint Standing Comittee on Treaties Regarding the Proposed Accession to the Council of Europe Convention on Cybercrime, March 2011, (çevrimiçi) s.3, http://pirateparty.org.au/media/submissions/JSCOT%20CoE%20Cybercrime%20Convention.pdf , 29.04.2015.

[133] Valenzuela Contreras v. Spain, İHAM başvuru no. 27671/95, 30.07.1998 p. 46.

[134] Malone v. The United Kingdom, İHAM başvuru no. 8691/79, 02.08.1984, p.68.

yani yeterli ve etkili güvencelerin bulunmamasının, demokrasiyi zayıflatma ve hatta yıkma sonucuna bile götürebileceği düşünülmüştür.[135]

e) Verilerin Korunması Açısından Eksiklikler

Verilerin korunmasına konusunda uluslararası alanda bağlayıcılığı bulunan tek sözleşme, 1981 tarihli Kişisel Verilerin Otomatik İşlenmesine İlişkin Olarak Bireylerin Korunması Sözleşmesi'dir. Bu sözleşme, ister kamu sektörü tarafından olsun ister özel sektör tarafından olsun her türlü verinin işlenmesine uygulanabilecektir. Sözleşme, kişileri toplanan ve işlenen kişisel verilerin kötüye kullanılması karşısında korurken, aynı zamanda sınır aşan veri akışını da düzenlemektedir. Böylece bu sözleşme, kişilere verileri koruma anlamında gerekli yasal garantileri sağlıyor ve hassas bilgi olarak nitelendirilen kişilerin ırkı, sosyal, siyasal ve cinsel durumları ve tercihleri ve sabıka kayıtlarına ilişkin verilerin kullanılmasını yasadışı hale getiriyor. [136]

Her ne kadar Budapeşte Sözleşmesi, yukarıda genel olarak açıklanan 1981 tarihli Sözleşmenin bir alternatifi olmasa da, veriler ile doğrudan bir ilişki halinde olan bir alanda düzenleme getirdiği için verilerin korunması için yeterli tedbirlere yer vermiş olması beklenilmiştir. Bu nedenle Sözleşme'nin, en çok eleştirilen yanlarından birisi de verilerin korunmasına ilişkin güçlü bir vurgu yapmamış olmasıdır.[137] Yalnızca, Sözleşme'nin giriş kısmında 1981 tarihli Sözleşmesi'ne atıfta bulunularak kişisel bilgilerin korunması konusunda bir farkındalığın olduğu belirtilmiştir. Bu atfın dışında herhangi bir şekilde Sözleşme'de atıfta bulunan sözleşmenin ilgili maddelerine ilişkin bir atıf ya da 1981 tarihli Sözleşmesi ile paralel bir düzenlemeye yer verilmemiştir.

Hiç olmazsa Sözleşme'nin 15. maddesinde yer alan şartlar ve tedbir başlığı altında yetki ve usullerin belirlenmesinde, devletlerden, 1981 tarihli sözleşmenin dikkate alınması gerektiği istenebilirdi. Böyle bir husus olmadığı gibi, daha kötüsü

---

[135] Leander v. Sweden, İHAM başvuru no. 9248/81, 26.03.1987, p.60.
[136]European Union Agency for Fundamental Rights, Handbook on Data Protection Law, 2014, (çevrimiçi), s.16, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf , 29.04.2015.
[137] Akdeniz, s.11.

kişisel verilere müdahale niteliği taşıyan ürün talimatı, verilerin aranması ve bunlara elkonulması gibi tedbirlerin uygulanmasında doğrudan bir mahkeme kararının gerekliliği de olmazsa olmaz bir şart olarak getirilmemiştir.

Açıkçası verilerin korunmasına dair sözleşmenin etkisinin, Sözleşme'de güçlü bir şekilde hissedilmemesi kişisel verileri özel ve kamu sektörüne karşı korumasız bırakmıştır.

f) Karşılıklı Yardımlaşma Açısından Eleştiriler

Sözleşme'nin 25. maddesinde karşılıklı yardımlaşmaya ilişkin genel ilkeler düzenlenmiştir. Bu düzenleme ile Sözleşme'ye taraf olan devletlere, bilgisayar sistemleri ve verileri ile ilgili suçların soruşturma veya işlemlerinde ya da herhangi bir suça ilişkin elektronik ortamda yer alan delillerin toplanmasında mümkün olan en geniş ölçüde birbirlerine yardım etmeleri yükümlülüğü getirilmiştir. Bu düzenleme çifte suçluluk açısından, yani kendisinden yardım talep edilen devletin, başka devlet tarafından yapılan talebe konu olayı suç saymasa dahi soruşturma yürütebileceği ihtimali nedeniyle eleştirilmiştir.[138]Bu çevreler tarafından "temel olarak baskıcı ve dengesiz" olarak tanımlanan Sözleşme'nin, zayıf çifte suçluluk hükümleri ile ilgili suça ölüm cezası öngören devletlere, kişilere ait verilerin teslimi riskini taşıdığı belirtilmiştir.[139]

Yardımlaşma ile ilgili diğer bir eleştiri ise, Sözleşme'de yer alan uluslararası yardımlaşmanın ulusal egemenliğe aykırılık taşıyan bir hükmüne getirilmiştir.[140] Sözleşme'nin 32. maddesinin (b) fıkrasına göre, taraf devletler, diğer bir taraf devletin yetkilendirmesi olmaksızın, yani diğer devletin bilgisi ve izni dışında, veriyi açıklamak için yetkisi bulunan kişinin -yasal ve gönüllü rızasıyla- verilerine erişim sağlayabilir veya bu verileri alabilir.

Gerçekten, taraf devletlerden birinin, bir başka taraf devletin sorumluluk sahasında bulunan bir veriye erişim sağlaması ve bir veriyi elde edebilmesi

---

[138] Serkowski, s.3.
[139] Cybercrime Convetion Ratification Leaves Lingering Concerns, 05/03/2013, Pirate Party, (çevrimiçi) http://pirateparty.org.au/2013/03/05/cybercrime-convention-ratification-leaves-lingering-concerns/ , 29.04.2015.
[140] Vatis, s.218.

devletlerin ulusal egemenliği açısından sorunludur.[141]Henüz Sözleşme'yi imzalamayan ve onaylamayan Rusya'nın da en önemli itirazlarından birini de ulusal egemenliğe ilişkin bu düzenleme oluşturmaktadır.[142]

[141] Gercke, s.199.
[142] John Markoff-Andrew E. Kramer, "In Shift, U.S. Talks to Russia on Internet Security", 12.12.2009, New York Times, (çevrimiçi) http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=0 ,29.04.2015.

V. SİBER SUÇLAR SÖZLEŞMESİ VE TÜRKİYE

A. Giriş

Öğretide, sözleşme, milletlerarası hukukun bu alanda yetki verdiği kişiler arasında yapılan ve milletlerarası hukuka uygun bir şekilde hak ve yükümlülükler doğurmak, daha önce kurulmuş bir hukuk ilişkisini değiştirmek ya da ortadan kaldırmak amacına yönelik hukuki işlem olarak tanımlanmaktadır.[143]

Anayasa'nın 90. maddesine göre, genel olarak, yabancı devletlerle ve milletlerarası kuruluşlarla yapılan uluslararası sözleşmeler, Türkiye Büyük Millet Meclisi'nin sözleşmeyi bir kanun ile uygun bularak onaylaması ve Cumhurbaşkanı'nın meclis tarafından yapılan bu kanunu onaylaması ve yayımlaması ile kanun hükmü haline gelir. Bu aşamadan sonra sözleşme, usulüne uygun bir şekilde yürürlüğe girmiştir ve hakkında Anayasaya aykırılık iddiası ile Anayasa mahkemesine başvurulamayacaktır. Ancak, bu düzenlemeye rağmen Yasama organı uluslararası sözleşmelere aykırı düzenleme yapabilecektir. Fakat ilgili ülkenin yükümlülüklerine uymaması demek olan bu durum uluslararası hukuk açısından sorumluluk doğuracaktır.[144]

Diğer taraftan, eğer sözleşmelerle kanunların aynı konuda farklı hükümler içermesi nedeniyle herhangi bir uyuşmazlık çıkarsa, Anayasa'nın 90/5 maddesinin son cümlesi ilgili sözleşmenin, Avrupa İnsan Hakları Sözleşmesi gibi, temel hak ve özgürlüklere ilişkin olması halinde sözleşme hükümlerinin esas alınacağını amirdir. Bunun dışında ortaya çıkan uyuşmazlıkların, sözleşmelerin kanun hükmünde olduğundan hareketle, iç hukukta iki kanun arasındaki çatışmanın çözümünde uygulanacak kuralların, yani önceki düzenleme-sonraki düzenleme veya genel düzenleme-özel düzenleme ölçülerinin uygulanması ile çözülmesi gerekir.[145]Budapeşte Sözleşmesi'nin temel hak ve özgürlüklere ilişkin olmadığı açıktır. Bu nedenle bu sözleşme ile kanunlarımız arasında ortaya çıkabilecek

---

[143] Yavuz Atar, Türk Anayasa Hukuku, Mimoza Yayınları, Konya 2012, s. 357
[144] Ergun Özbudun, Türk Anayasa Hukuku, Yetkin Yayınları, Ankara 2003, s. 212
[145] Atar, s. 358

uyuşmazlıkların çözümünde önceki düzenleme-sonraki düzenleme veya genel düzenleme-özel düzenleme ilkelerine başvurulması gerektiğini düşünmekteyiz.

Son olarak, usulüne uygun olarak yürürlüğe giren bir sözleşmenin, ayrıca bir düzenleme yapılmasına gerek bulunmaksızın, iç hukukun bir parçası haline geldiği, iç hukukta kendiliğinden uygulanabileceği, hakkında anayasa aykırılık iddiasında bulunulamayacağı belirtilmelidir.[146]

B. Siber Suçlar Sözleşmesi'nin Onaylanması

İleride ayrıntıları ile inceleyeceğimiz Sözleşmesi'nin yasalarımız üzerinde etkilerinin daha iyi anlaşılması için TBMM'de bu konuya ilişkin olarak yapılan yasama faaliyetlerini değinilmesi gerekmektedir. Bu nedenle inceleme yapılırken mümkün olduğu kadar komisyon raporları, meclis tutanakları, yasalar ve bu yasalara ait gerekçelere değinilmelidir.

Budapeşte Sözleşmesi, iç hukukumuza 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile girmiştir. Sözleşme, hükümet adına 10.11.2010 tarihinde Strazburg'da imzalandı ve 6533 sayılı Kanun ile 22.04.2014 tarihinde TBMM'de tüm partilerin genel uzlaşı[147] ile kabul edildi. Anılan yasa 02.05.2014 tarihinde Cumhurbaşkanı tarafından onaylandıktan sonra yürürlüğe girdi.[148]

Bu kanun toplam 3 maddeden ibarettir ve Sözleşme'ye konulan 3 ayrı çekince ve 5 ayrı beyan ile birlikte kabul edilmiştir. 6533 sayılı Yasaya ait komisyon raporu[149] Dışişleri Komisyonu tarafından 20.12.2012 tarihinde hazırlandı. Bu raporda, Budapeşte Sözleşmesi'ne, Avrupa Konseyi'ne üye olan ve olmayan devletlerin taraf olduğu belirtilerek, Sözleşme "küresel ölçekte geçerli bir referans belgesi" olarak kabul edilmiştir.

---

[146] A. Şeref Gözübüyük, Anayasa Hukuku, Turhan Kitabevi, Ankara 2004, 13. Bası, s. 307-308
[147] Kullanılan oy sayısı:224, kabul:222, TBMM 24. Dönem, 4. Yasama Yılı, 79. Birleşim, 22.04.2014 tarihli Genel Kurul Tutanağı.
[148] http://www.tbmm.gov.tr/develop/owa/kanunlar_sd.durumu?kanun_no=6533
[149] Sanal Ortamda İşlenen Suçlar Sözleşmesinin Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyon Raporu, TBMM, (çevrimiçi) http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, 29.04.2015

Rapordan, Sözleşme'ye taraf olunmakla Avrupa Konseyi tarafından oluşturulan ortak hukuk sistemine tam anlamıyla uyum sağlama yolunda bir eksikliğin daha giderilmesinin hedeflendiği anlaşılmaktadır. Gerçekten Avrupa Birliği'ne üyelik sürecinde bulunan ülkemiz adına, Avrupa Birliği'ne üye birçok ülkenin Sözleşmeye taraf olduğu göz önüne alındığında, Sözleşme'ye taraf olmak önemli bir adımdır.

Yine rapordan, Sanal Ortamda İşlenen Suçlar Sözleşmesi Komitesi'nde elde edilecek oy hakkının da hedeflendiği görülmektedir. Bu komitenin orijinal ismi "Cybercrime Convention Committee" dir ve kısaca T-CY olarak bilinir. Komite, Budapeşte Sözleşmesi'nin 46. maddesine istinaden kurulmuş olup, siber suçlar alanında Avrupa Konseyi'nin lokomotifi durumundadır. Komite, Sözleşme'nin 46. maddesi ve kendi iç tüzüğünün[150] 1. maddesine göre;

- taraf devletlerin yaptığı uygulamaları değerlendirmek, iyi olan uygulamaları tespit etmek ve paylaşmak;
- Sözleşme'nin uygulama ve yorumlanmasında düşünce ve öneri kabul etmek[151];
- protokol, tavsiye gibi hukuki belgeleri tasarlamak;
- Avrupa Konseyi organları tarafından istenen düşünceleri kabul etmek;
- Sözleşme'nin 35. maddesine göre kurulan 7/24 irtibat noktasını denetlemek;
- Sözleşme'ye taraf olmaya devletleri taraf olmaları için teşvik etmek;
- ilgili uluslararası toplantılarda devletlerin ortak bir duruş sergilemelerini sağlamak;
- Siber suçlara karşı uluslararası işbirliği açısından diyalog yoluyla uluslararası örgütlerle iletişime geçmek;

---

[150] Cybercrime Convention Comittee, T-CY Rules of Procedure, Strasbourg, 3.12.2015 (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2013)25%20rules_v14.pdf , 30.04.2015.

[151] 5.12.2012'de komite tarafından bilgisayar sistemi kavramı ele alınmış ve geleneksel anabilgisayar ve masa üstü bilgisayarın ötesinde, modern cep telefonları, akıllı telefonlar, cep bilgisayarları (PDAs), tablet ve benzeri teknolojiler bilgisayar sistemi olarak kabul edilmiştir. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)21E_guidanceNote1_article1_final.pdf

- siber suçlar ve elektronik delil ile ilgili kapasite geliştirmek;
- özel sorunlara çözüm üretmek için çalıştaylar oluşturmak işlevlerini yerine getirir.

Komite üyelerden, gözlemcilerden ve geçici katılımcılardan oluşmakta, ancak sadece üyelerin oy hakkı bulunmaktadır. Genel kural olarak, kararda oybirliği, oybirliğinin sağlanamaması halinde üçte ikilik çoğunluk aranır. İç tüzüğe ait kurallar oybirliği ile değiştirilir. Komitenin yukarıda sayılan işlevleri ve Sözleşme'nin niteliği nazara alındığında Türkiye'nin siber suçlar alanında oy kullanmak suretiyle belirleyici bir rol oynaması çok önemlidir.

Komisyon raporunda belirlenen Avrupa Konseyi tarafından öngörülen hukuk ile uyumlu görünme ve oy hakkı sahibi olma önemli iki hedef olmasına rağmen çok daha önemli hedefler de belirlenebilirdi. Bunun bu raporda vurgulanması, ileride yargı yerleri tarafından uygulamada Sözleşme'nin özü itibariyle değerlendirilmesinde farklı açılımlar sunabilirdi. Bu iki hedefin zayıf kaldığı kanaatindeyiz.

Bu haliyle Meclis Genel Kurulu'na gelen yasa, hükümet ve çeşitli eleştiriler getirilse de muhalefet partileri tarafından genel olarak desteklenmiştir.[152] CHP Grubu adına konuşan Erdal Aksünger, kişisel veriler kanunun henüz meclise gelmemesi nedeniyle 6533 sayılı Kanunun tek başına yetersiz kalacağını ifade etmiştir. BDP adına konuşan Adi Zozan ise, Sözleşme'nin bugünün ihtiyaçlarına cevap vermediğini, bu nedenle güncel olmadığını ifade etmiştir. MHP adına konuşan Seyfettin Yılmaz ise, destekledikleri Sözleşme'ye göre iç hukukun da uygun hale getirilmesi gerektiğini ifade etmiştir.

Yasa tasarısının tümü üzerinde Hükümet adına Avrupa Birliği Bakanı Mevlüt Çavuşoğlu konuşmuştur. Çavuşoğlu bu konuşmasında öncelikle, Budapeşte Sözleşmesi'nin güncelliğini yitirdiğine dair yöneltilen eleştiriye cevap vermiştir.

---

[152] TBMM Genel Kurul Tutanağı 24. Dönem 4. Yasama Yılı 79. Birleşim 22.04.2014, (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?P4=22125&P5=H&PAGE1=1&PAGE2=73, 29.04.2015

Bu tür sözleşmelerin güncelliğini yitirmediğini, böyle olsaydı, 1950 yılında hazırlanmış Avrupa İnsan Hakları Sözleşmesi'nin güncelliğini yitirmiş olacağını, ek protokollerle güncelliğin korunduğunu belirtmiştir.

Açıkçası bu cevaba katılmak pek mümkün görünmemektedir. Sözleşme'nin güncelliğini yitirdiği eleştirileri, daha önce de açıklandığı üzere sürekli dile getirilmektedir ve hızla gelişen bilgisayar teknolojileri karşısında Sözleşme'nin güncelliğini koruduğunu söylemek güçtür. Çünkü Sözleşme'nin yürürlüğe girmesinden bu yana sadece Bilgisayar Sistemleri yolu ile İşlenen Irkçı ve Yabancı Düşmanlığı Suçlarına dair ek bir protokol hazırlandı. Bu protokol ise, Sözleşme'yi güncel hale getirme amacını taşımaktan ziyade, zaten Sözleşme'nin ilk hazırlandığı dönemde var olan bir konunun ifade özgürlüğüne aykırı olacağı endişesi ile ileri bir tarihe ertelenmesi ile yeniden ele alınmasıydı.[153]Çavuşoğlu'nun yaptığı konuşmada dikkat çeken diğer iki konu ise, Avrupa Konseyi 108 no'lu Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin henüz imzalanmamış olmasının bir eksiklik olarak görülmesi ve Sözleşme'nin onaylanmasından sonra Sözleşme'ye uygun yasaların çıkarılması için isteğin belirtilmesidir. Gerçekten anılan sözleşme onaylanmadığı sürece Siber Suçlar Sözleşmesi; kişisel verilerin korunması bağlamında, şahıslar açısından bir güvenlik unsuru değil, aksine tehdit unsuru bile olabilecektir.

Bir başka eleştiri ise Sözleşme'ye verilen isim üzerinden yapılabilir. Yasama organının Siber Suçlar Sözleşmesi ifadesini yerine 6533 sayılı Kanunda, Sanal Ortamda İşlenen Suçlar Sözleşmesi ifadesini kullanması sanal kelimesine yüklenen anlam nedeniyle isabetli bulunmamıştır.

---

[153] Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of Racist and Xenophobic Nature Committed Through Computers Systems, Council of Europe, Explanatory Report (çevrimiçi) p.4, http://conventions.coe.int/Treaty/en/Reports/Html/189.htm, 29.04.2015

Türk Dil Kurumu'na göre, sanal, "gerçekte yeri olmayıp zihinde tasarlanan, mevhum, farazi, tahminî" anlamlarına gelmektedir.[154]Bu sözcüğün İngilizce'deki karşılığı "virtual"dır.[155]

Virtual sözcüğü ise, bir bilişim terimi olarak, fiziksel olarak var olmayan ancak yazılımlarla varmış gibi görülen anlamına gelir.[156]Bu sözcük, örneğin Virtual Private Network ifadesinde, sanal özel ağ karşılığı kullanılır.

Siber sözcüğü ise, canlılarda ve makinalarda iletişim ve otomasyon kontrol sistemleri bilimi[157] anlamına gelen "cybernetics"[158] sözcüğünün kısaltması olarak, bilgisayar, bilgi teknolojisi ve sanal gerçeklikle ilgili veya bunların bir özelliği[159] ya da özellikle internet olmak üzere bilgisayarı içeren, bilgisayarı kullanan veya bilgisayarla ilgili[160] ya da elektronik veri işleme, elektronik iletişim, bilgi ve bilgisayar sistemleri ile ilgili[161] demektir. Bu haliyle siber tek başına değil de, daha çok başka sözcüklerle birlikte bir önek olarak kullanılır ve o şekilde anlam ifade eder. Siber, esasen, yön vermek, yönetmek, kontrol etmek anlamlarına gelen Antik Yunanca bir kavram olan "kybereo"dan gelir.[162]

Siber önekinin; siber altyapı, siber güvenlik, siber alan, siber çevre, siber tehdit, siber saldırı gibi kullanımları ile altyapı, güvenlik, alan, çevre, tehdit ve saldırı sözcükleri internet ve bilgisayarla ilgili hale gelir.

---

154 http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54dfd22940ee74.92262061

155 http://dictionary.cambridge.org/dictionary/turkish/virtual

156 http://www.oxforddictionaries.com/definition/english/virtual?searchDictCode=all

157 http://www.oxforddictionaries.com/definition/english/cybernetics

158 Cybernetic, otomatik kontrol sistemleri (sinir sistemi gibi) çerçevesinde iletişim ve kontrol teorisinin yer aldığı bilim dalıdır. Aslı Deniz Helvacıoğlu, Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi, İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2004, s.277.

159 http://www.oxforddictionaries.com/definition/english/cyber?searchDictCode=all

160 http://dictionary.cambridge.org/dictionary/british/cyber

161 Finland's Cyber Security Strategy Government Resolution 24/01/2013, (çevrimiçi) http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy , 30.04.2015

162 A.g.e., s.12.

Bu tanımlamalardan hareketle siber sözcüğünün, sanal sözcüğüne tercih edilmesinin daha isabetli olacağı kanaatine varılmıştır. Anlamları itibariyle siber ile ifade edilen olay ya da olgu doğrudan bilgisayar veya internetle ilgili hale gelir. Ancak sanal, diğer bir ifadeyle farazi, tahmini ya da mevhum olan ile bilgisayar ve internet arasında ilk anda doğrudan bir bağlantı kurulamaz. Öte yandan suçların varsayılan bir yerde işlenmediği, var olan elektronik bir ortamda işlendiği düşünüldüğünde[163] "sanal ortamda işlenen" suçlar yerine "siber" ifadesinin kullanılması daha doğru olacaktı.

C. İç Hukukumuzda Siber Suçlar

Mevzuatımızda siber suçlar alanındaki ilk yasal düzenleme, 1991 yılında 3765 sayılı Yasa ile 765 sayılı Türk Ceza Yasası'na 525/a, 525/b, 525/c ve 525/d maddelerinin eklenmesi ile gerçekleştirilmiştir ve bu düzenlemeler "bilişim alanında suçlar" başlığı altında bir bütün olarak ayrıca ele alınmıştır. Bu düzenlemenin,

- 525/a maddesinde; ilk fıkrada, bilgileri otomatik olarak işleme tabi tutmuş sistemden programları, verileri veya diğer herhangi bir unsuru ele geçirme ve ikinci fıkrada, bu programları, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanma, nakletme ve çoğaltma suçları,
- 525/b maddesinde; ilk fıkrada, başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak amacıyla bilgileri otomatik olarak işleme tabi tutmuş sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etme veya değiştirme veya silme veya sistemin işlemesine engel olma veya yanlış biçimde işlemesini sağlama ve ikinci fıkrada bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine yarar sağlama suçları,
- 525/c maddesinde; hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan

[163] Alemdar Yalçın, Ceza Hukuku Açısından Bilişim Suçları, Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar(Müslüm Saylı Derin Akdeniz), İçişleri Bakanlığı, 24/03/2001 Bursa, s.90.

bir sisteme, verileri veya diğer unsurları yerleştirme veya var olan verileri diğer unsurları tahrif etme ve tahrif edilmiş olanları bilerek kullanma suçları,

- 525/d maddesinde 525/a ve 525/b maddeleri hükümlerini ihlal eden kişiler hakkında, ek yaptırımlar yer almaktadır.

Bu düzenlemelerin altyapısını, Adalet Bakanlığı'nın 14/01/1985 tarihli oluru ile kurulan komisyon tarafından hazırlanan Türk Ceza Kanunu Öntasarı metnini ortaya konan olumlu ve olumsuz eleştiriler ışığında tekrar gözden geçirmek için kurulan 2. Komisyon'un 1989 tarihli TCK Öntasarı metni oluşturmaktadır.[164] 2. Komisyon ilgili düzenlemeleri aşağıda Fransa'nın durumunda açıklanacağı üzere Fransa'da yürürlüğe giren ve 1994 tarihli Yeni Fransız Ceza Yasası'nın ilgili bölümüne de model olan 88-19 sayılı Yasa'dan esinlenerek yapmıştır. [165]

Adalet Bakanlığı bünyesinde devam eden yeni yasa çalışmaları ile 1989 TCK Tasarısı'nı, 1997 TCK Tasarısı, bu tasarıyı ise 2001 TCK Tasarısı takip etmiş ve bu son tasarı 14.04.2003 tarihinde Bakanlar Kurulu tarafından kabul edilerek Başbakanlıkça Türkiye Büyük Millet Meclisi'ne gönderilmiştir. Tasarı, Adalet Komisyonu tarafından 28.07.2003 tarihinde geneli üzerinde yapılan görüşmelerden sonra maddeleri üzerinde daha ayrıntılı bir inceleme için alt komisyona gönderilmiştir. Yapılan komisyon çalışmaları neticesinde kabul edilen metin bazı küçük değişikliklerle 26.09.2004 tarih ve 5237 sayı ile meclis genel kurulunda yasalaşmıştır.[166] Bütün bu yasa çalışmaları sonunda, siber suçlar, son halini 5237 sayılı Yasa'da bulmuş ve temelini 1997 TCK Tasarısı'ndan almıştır.[167] Yürürlükte bulunan 5237 sayılı Yasa'ya esas tasarılarda yer alan siber suçlara ilişkin

[164] R. Yılmaz Yazıcıoğlu, s.207.; Yılmaz Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirilmesi, s.394.
[165] R. Yılmaz Yazıcıoğlu, s. 207.
[166] Cemil Çiçek, Önsöz, Tutanaklarla Türk Ceza Kanunu, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, Ankara, Şubat 2005, s.V.
[167] Yılmaz Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirilmesi, s.394.

düzenlemelerde ise 1994 yılında Fransa'da yürürlüğe giren Yeni Fransız Ceza Kanunu'nda yer alan 323-1 ila 323-7 maddelerinin etkisi bulunmaktadır.[168]

Bu aşamada Budapeşte Sözleşmesi'nin iç hukukumuza etkisi olup olmadığını, varsa ne kadar etkisi bulunduğunu belirlemek için Fransa'da siber suçlarla ilgili duruma da göz atmakta fayda bulunmaktadır.

D. Fransa'da Durum

Siber suçlarla mücadelede, en önemli yasal düzenleme 5 Ocak 1988 tarihli 88-19 sayılı *"relative a la fraude informatique"* adlı yasadır. Çünkü bu yasa öncesinde siber suçluluk, mal aleyhinde suçlar kapsamında olan hırsızlık, inancı kötüye kullanma ve dolandırıcılık gibi suçlarla düzenleniyordu.[169] Bu yasa, ayrıca 1 Mart 1994 tarihinde yürürlüğe giren Yeni Fransız Ceza Yasası içerisinde 3. kitap, 2. kısım, 3. bölümde yer alan "verileri otomatik olarak işleme tabi tutan sistemlere yönelik saldırılar" başlığı altında düzenlenen 323-1 ila 323-7 maddelerinde düzenlenen siber suçlara ve ilgili hükümlere de esas teşkil etmektedir.[170]

YFCY'de siber suçlar ve ilgili hükümler aşağıdaki konulara ilişkindir[171]:

- Verileri otomatik olarak işleme tabi tutan sisteme, girme veya bu sistemde kalma (323-1),
- Verileri otomatik olarak işleme tabi tutan sistemin işleyişini bozma ve engelleme (323-2)
- Verileri otomatik olarak işleme tabi tutan sisteme hile ile veri yerleştirme ya da hile ile verinin silinmesi veya değiştirilmesi (323-3)
- 323-1 ila 323-3 arasında sayılan suçlara iştirak (323-4)
- 323-1 ila 323-3 arasında sayılan suçlar için ek yaptırımlar (323-5)
- Tüzel kişilerin bu bölümdeki suçlar nedeniyle sorumluğu (323-6)

---

[168] Sulhi Dönmezer, Kişilere ve Mallara Karşı Suçlar, Beta Yayınevi, İstanbul 2001, s.613.; R. Yılmaz Yazıcıoğlu, s.207.; Yılmaz Yazıcıoğlu, s.394.
[169] R. Yılmaz Yazıcıoğlu, s.197.
[170] A.g.e., s.196.
[171] Yeni Fransız Ceza Yasası, (çevrimiçi) http://www.legislationline.org/download/action/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf , 29.05.2015.

- Bu bölümdeki suçlara teşebbüsün halinde tamamlanmış suça ait cezanın verilmesi (323-7)

Yukarıda sayılan maddelerin dışında, YFCY, siber suçlarla ilgili olarak yasanın; 226-16 ila 226-24 maddelerinde kişilik haklarının bilişim sistemi aracılığı ile ihlalini, 226-8 maddesinde bireylerin resim veya sözlerinin rızasına aykırı bir şekilde montajını, 227-23 maddesinde küçüğün resminin pornografik olarak kullanılmasını, 227-24 maddesinde küçükler tarafından görülmeye elverişli şiddet ve pornografik nitelikli mesaj yayımlanmasını ayrı ayrı birer suç olarak düzenlemiştir.[172]

Fransa, Sözleşme'yi 23 Kasım 2001 tarihinde imzalamasına ve 10 Ocak 2006 tarihinde onaylamasına[173] rağmen siber suçlara ilişkin düzenlemelere yukarıda açıkladığı üzere hemen hemen zaten sahipti. Ancak, Sözleşme'de yer verilen tüm hükümlerin tamamen YCFY ile örtüştüğünü söylemek güçtür. Örneğin, bilgisayar bağlantılı sahtecilik ve bilgisayar bağlantılı dolandırıcılık suçlarına ilişkin özel düzenlemeler yoktur. Bu suçlardan sahtecilik; Fransız Ceza Yasası'nın 313-1 maddesinde, dolandırıcılık suçu ise; aynı yasanın 441-1 maddesinde genel olarak düzenlenmiştir. [174]

Aynı şekilde Sözleşme'nin usuli maddelerinin de Fransız Ceza Usul Yasası ile tamamen örtüştüğü söylenemez. Fakat bu durum uluslararası sözleşmeleri genel olarak esas alan Fransız Ceza Usul Yasası'nın Sözleşme ile uyumlu olmadığı anlamına da gelmemelidir. [175]

[172] Yener Ünver, TCK ve CK Tasarısı'nın İnternet Açısından Değerlendirilmesi, İHFM. Sayı 1-2, 2001, s.71.
[173] Avrupa Konseyi, Sözleşme İmza ve onay tablosu, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG, 29.04.2015.
[174] Picotti - Salvadori, s.6.
[175] A.g.e., s.7.

E. Sözleşme ve İç Hukukumuz

Siber suçlarla ilgili olarak yapılan yasal düzenlemelerde farklı ülkeler tarafından takip edilen üç farklı yol vardır. Bunlar[176]:

- Bu suçları tek başlık altında düzenlemek,
- Bu suçları korudukları hukuki değer esasına göre ilgili yerlerde ayrı ayrı düzenlemek,
- Her iki yöntemi de dikkate alarak karma bir düzenleme yapmak.

Bu kapsamda 765 sayılı Yasa'da düzenlenen siber suçlar, suçla korunan hukuksal yarar gözetilmeksizin yukarıda açıklandığı üzere anılan yasanın 11 no'lu babında dört madde ile düzenlenmiştir.[177]

5237 sayılı TCK ise karma sistemi benimseyerek hem siber suçlar korudukları hukuki yarara göre ilgili oldukları bölümde benzer suç tipleri ile birlikte hem de klasik suçlarla benzer hukuki yararı korumayan ya da korudukları hukuki yararlar karma nitelikte olan siber suçlar "bilişim alanında suçlar" başlığı altında ayrıca düzenlenmiştir.

765 sayılı Yasa'nın ve bu yasada siber suçlarla ilgili düzenlemelerin 2001 yılında imzaya açılan Sözleşme'den önce yapılmış olmaları nedeniyle Sözleşme'den etkilenmiş ya da esinlenmiş olması düşünülemeyeceğinden 765 sayılı Yasa'nın ilgili hükümleri çalışma konumuz dışındadır.

Çalışma konumuzun odak noktasını ise 2001 tarihinden sonra, yani Sözleşme'den sonra yürürlüğe giren yasalarımız oluşturmaktadır.

Siber suçların mevzuatımızda düzenlenişi dağınık bir görünüm arz etmektedir. Siber suçların ağırlıklı kısmı 5237 sayılı TCK'da düzenlenmiştir. Bunun dışında ayrıca konumuzu ilgilendirmesi bakımından 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nda yer alan düzenlemeler oluşturmaktadır.

---

[176] Dülger, s. 226-229.
[177] Age s.229.

5237 sayılı Yasa içerisinde yer alan siber suçlar[178]:

- Bilişim sistemine girme (m. 243)
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme (m.244)
- Bilişim sistemleri aracılığı ile haksız yarar sağlama (m.244/4)
- Banka veya kredi kartlarının kötüye kullanılması (m.245)
- Bilişim sistemlerinin kullanılması suretiyle hırsızlık (m. 142/2-e)
- Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık (m. 158/1-f)
- Haberleşmenin gizliliğini ihlal (m.132)
- Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (m. 133)
- Özel hayatın gizliliğini ihlal (m.134)
- Kişisel verilerin kaydedilmesi (m.135)
- Verileri hukuka aykırı olarak verme veya ele geçirme (136)
- Verileri yok etmeme (m. 138)
- Müstehcenlik (m. 226/3)

5846 sayılı Yasa içerisinde yer alan siber suçlar:

- Manevi, mali ve bağlantılı haklara tecavüz (m. 71)
- Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri (m.72)

Maddi ceza hukukuna ait bu düzenlemelerin dışında ayrıca usul hukukuna ait düzenlemelerin en önemlisi 5271 sayılı CMK'nın 134. maddesinde "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlığı altında yer alan düzenleme ve aynı yasanın 135. maddesinde "iletişimin tespiti, dinlenmesi ve kayda alınması" başlığı altında yer alan düzenlemedir. Yine internet süjelerinin sorumluluğu düzenleyen 5651 sayılı Yasa da önem arz etmektedir.

[178] Sayılan bu suçlar bir sonraki bölümde Sözleşme'de yer alan hükümler ile birlikte karşılaştırmalı olarak ele alınacaktır.

Yukarıda sayılan maddi ceza hukukuna ve usul hukukuna ait bu düzenlemelerde Sözleşme'nin etkisi olduğunu söylemek gerçekten zordur. Fransa Ceza Yasası'nın mevzuatımız üzerinde etkileri olduğunu söylemiştik. Aynı yerde Sözleşme'de yer alan düzenlemeler ile FCY'de yer alan düzenlemeler arasında paralellik olsa da FCY, Sözleşme'nin uygulanması açısından ideal bir örnek değildir. Kaldı ki, FCY, Sözleşme'nin hazırlanmasından önce yürürlüğe girmiştir. FCY ile Sözleşme arasındaki bu durum, aslında mevzuatımız ile Sözleşme arasındaki durumu da ortaya koymaktadır. Yani mevzuatımızın, Sözleşme'den etkilendiğini ya da esinlendiğini söyleyemeyiz.

Bu durum kendisini yasama faaliyetleri sırasında da kendisini zaten göstermiştir. Bu yasama faaliyetleri Sözleşme'nin imzaya açılmasından sonra gerçekleşmiştir ve Sözleşme o dönem itibariyle artık hukuk âleminde bir referans belgesi olarak durmaktadır.

Siber suçların, çoğunluğunun yer aldığı TCK'nın hazırlanması ile ortaya çıkan TBMM Adalet Komisyonu Türk Ceza Kanunu Tasarısı Raporunda, TBMM Adalet Komisyonu Türk Ceza Kanunu Tasarısının tümü üzerindeki görüşmelerde, TBMM Adalet Komisyonu ile Genel Kurulunda Türk Ceza Kanunu Tasarısının maddelerinin görüşmelerinde,[179] madde gerekçelerinde[180] Budapeşte Sözleşmesi'ne herhangi bir atıf bulunmamaktadır.

Aynı şekilde CMK hazırlanırken, TBMM Adalet Komisyonu Ceza Muhakemesi Kanunu Tasarısı Raporunda, Ceza Muhakemesi Kanunu Alt Komisyon Raporunda, TBMM Genel Kurulu Ceza Muhakemesi Kanunu Tasarısının tümü üzerindeki görüşmelerde ve TBMM Adalet Komisyonu ile Genel

[179] Tutanaklarla Türk Ceza Kanunu, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara Açık Cezaevi Matbaası, Ankara 2006

[180] İzzet Özgenç, Türk Ceza Kanunu Şerhi, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara Açık Cezaevi Matbaası, Ankara 2006

Kurulunda Ceza Muhakemesi Kanununun maddeleri görüşmelerde[181] ve madde gerekçelerinde[182] Sözleşme'ye değinilmemiştir.

5846 sayılı Yasa'da yer alan ilgili suçlara ilişkin gerek yasanın ilgili maddelerinin gerekçesinde[183], Adaleti Komisyonu raporunda[184] ve TBMM Genel Kurulu'nda yapılan görüşmelerde[185] yine Sözleşme'ye yer verilmemiştir.

Mevzuatımızda, yasama faaliyetleri kapsamında Sözleşme'ye, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanuna esas olmak üzere hazırlanan 12.04.2007 tarihli Adalet Komisyonu raporunda değinilmiştir. Bu yasa ile siber suçlar düzenlenmediği gibi siber suçlara ilişkin herhangi bir cezai veya idari yaptırım da öngörülmemiştir. Yasa'nın kapsamını, içerik sağlayıcı, yer sağlayıcı ve erişim sağlayıcılar üzerinden başka yasalarda düzenlenen siber suçları önlemek oluşturmaktadır. Adalet Komisyonu, raporunda, içerik sağlayıcının sorumluluğuna ilişkin 4. madde ve yer sağlayıcının yükümlülüklerine ilişkin 5. maddeye ilişkin düzenlemeler yapılırken Avrupa Konseyi Siber Suçlar Sözleşmesi hükümlerinin göz önünde bulundurulduğunu belirtmiştir.[186] Görüldüğü üzere, Sözleşme'nin etkisi sadece iki madde üzerinde kısmen olmuştur.

---

[181] Tutanaklarla Ceza Muhakemesi Kanunu, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, Ankara Açık Cezaevi Matbaası, Ankara 2005

[182] 5271 Sayılı Yasa gerekçesi, http://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss698m.htm

[183] 5728 sayılı Temel Ceza Kanunlarına Uyum Amacıyla Çeşitli Kanunlarda ve Diğer Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, Genel Gerekçe, s. 25-26. (çevrimiçi) http://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss56.pdf, 29.04.2015

[184] A.g.e, s.126-127.

[185] 23. Dönem 2. Yasama Yılı 47. Birleşim 09/01/2008, (çevrimiçi) http://www.tbmm.gov.tr/develop/owa/tutanak_g_sd.birlesim_baslangic?P4=20047&P5=B&PAGE1=1&PAGE2=90 , 29.04.2015.

[186] Adalet Komisyon Raporu, Elektronik Ortamda İşlenen Suçların Önlenmesi ile 2559 ve 2937 Sayılı Kanunlarda Değişiklik Yapılmasına Dair Kanun Tasarısı ve İstanbul Milletvekili Gülseren Topuz'un; Bilişim Sistemi Üzerinden Suç Teşkil Eden Zararlı Yayınlarla Mücadele Hakkında Kanun Teklifi ile Adalet Komisyonu Raporu (1/1305, 2/958) (çevrimiçi), p. 14-16 http://www.tbmm.gov.tr/develop/owa/tasari_teklif_gd.onerge_bilgileri?kanunlar_sira_no=51984 , 29.04.2015.

Sonuç olarak, Sözleşme'nin mevzuatımız üzerinde ciddi bir etkisi olduğunu söylemek yanlış olacaktır. Elbette, bu durum mevzuatımızın Sözleşme ile uyumsuz olduğu anlamına da gelmemektedir. Böyle olsaydı zaten öncelikle iç hukukumuzun Sözleşme'nin hükümleri ile paralel getirilmesinden sonra onaylanması söz konusu olacaktı. Fakat özellikle maddi ceza hukuku ve ceza usul hukuku açısından Sözleşme ile yer yer farklılıkların olduğu da yadsınamaz bir gerçektir. Bu benzerlikler ve farklılıklar çalışmamızın bir sonraki bölümünde ele alınacaktır.

VI. SÖZLEŞME İLE İÇ HUKUKUMUZDA SİBER SUÇLARIN KARŞILAŞTIRILMASI

A. Giriş

Çalışmamızın bu bölümünde Sözleşme'nin tanımlar, maddi ceza hukuku, usul hukuku ve uluslararası işbirliği alanlarında getirmiş olduğu hükümler açıklanacak ve bu hükümlerin iç hukukumuzdaki karşılıkları analiz edilecektir. Böylece iç hukukumuz ile Sözleşme'de yer alan hükümler arasında bir uyum olup olmadığı, böyle bir uyum varsa bu uyumun ne kadar olduğu tespit edilmeye çalışılacaktır.

Sözleşme, devletlerin siber suçlar alanında özel ihtiyaçları doğrultusunda kendilerini ayarlayabilecekleri belli standartlar koyarak devletlerin buna uymasını beklemektedir. Ancak, daha önce de belirtildiği üzere, her devletin Sözleşme ile tam bir uyum içerisinde olduğunu söylemek mümkün değildir.[187] Bu anlamda en iyi örneğin Romanya olduğunu söyleyebilir.[188] Romanya, Sözleşme'de yer alan tüm hükümleri tam bir model olarak kabul etmiş ve kendi iç hukukunun siber suçlara bakan yanını Sözleşme ile paralel şekilde düzenlemiştir.

Sözleşme, bilgi teknolojileri ile telekomünikasyon teknolojilerinin bütünleşmesi ve bu teknolojilerin sağladığı hizmetten kullanıcıların yararlanması ile ortaya çıkan bir alan olan siber uzayın suçlular tarafından kötüye kullanılmasına karşı bir cevaptır.[189] Sözleşme, devletlerin iç hukuklarının maddi ceza hukuku anlamında uyumlaştırılmasını, iç hukuk sistemlerinde siber suçların soruşturulması ve elektronik delilin toplanması için gerekli ceza usul yetkilerinin sağlanmasını ve hızlı ve etkili uluslararası işbirliği rejimini kurmayı hedeflemektedir.[190]

İçel tarafından Sözleşme'ye hâkim olan ilkeler aşağıdaki şekilde sıralanmıştır[191]:

---

[187] Picotti - Salvadori, s.4.
[188] A.g.e., s.8.
[189] Explanatory Report, 8.
[190] Explanatory Report, 16.
[191] Kayıhan İçel, Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İHFM., C.LIX, Sayı:1-2, 2001, s.6-8.

- Temel hak ve özgürlüklerin gereklerine uyulması,
- Bilgisayarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak bir minimum standarda uyulması,
- Suçun işlenebilmesi için eylemin hukuka aykırı olması,
- Suçun işlenebilmesi için eylemin kasten işlenmesi.

Bu ilkeler çerçevesinde hazırlanan Sözleşme'nin sistematiğine uygun olarak öncelikle maddi ceza hukukuna ilişkin olarak öngörülen suçlar, sonrasında usul hukukuna ilişkin tedbirler ve son olarak uluslararası işbirliğine dair hükümler ele alınacaktır. Sözleşmeye ait her hüküm iç hukukumuzda bulunan karşılığı ile ayrıca karşılaştırılacak, iç hukukumuzda karşılığı bulunmayan hükümler ise iç hukukumuz açısından bir eksiklik olarak görülüp bu durum belirtilecektir. Sözleşmeye ait hükümler, temel olarak Sözleşme'nin açıklayıcı raporu (explanatory report) yani gerekçesi dikkate alınarak açıklanmıştır.

B. Getirilen Tanımlar Açısından Karşılaştırmalı Bakış

1. Giriş

İnternet, bilgisayar, cep telefonu ve tablet gibi bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişim kendi terminolojisini de beraberinde getirmiştir. Bu gelişim ve değişime yeni sözcükler üretilerek ya da zaten var olan sözcüklere yan veya terim anlam yüklenerek cevap verildiği gözlemlenmiştir.

Sözleşme'nin 1. maddesinde, Sözleşme hükümlerinin uygulanmasını kolaylaştıracak ve Sözleşme ile belirlenen ilkelerle uyumlu bir çerçevenin çizildiği ve kavramlara yer verilerek gerekli tanımların yapıldığı görülmektedir. Sözleşme, taraf devletleri getirdiği tanımların birebir kopya edilmesi konusunda zorlamamaktadır.[192]

[192] Explanatory Report, 22.

Genel olarak, Sözleşme'de yer alan terimlere yüklenen anlamlar ile iç hukukumuzda aynı terimlere yüklenen anlamlar aynı kavramı ifade etmektedir ve iç hukukumuz ile Sözleşme arasında bu konuda uyum bulunmaktadır.

2. Bilgisayar Sistemi ve Bilişim Sistemi

Sözleşme'nin 1. maddesinin (a) bendinde bilgisayar sistemi kavramının tanımı yapılmıştır. Bu kavramda her ne kadar bilgisayar terimine yer verilmiş olsa getirilen tanım bilgisayardan bağımsızdır. Sözleşmede ayrıca yapılmış bir bilgisayar tanımlaması da yoktur. Aynı durum mevzuatımız açısından da geçerlidir. Zaten, genelde, siber suçlarla ilgili çıkarılan yasalarda gerek yapılacak bir tanımla bağlı kalarak teknolojiye ayak uyduramama ve gerekse de bilgisayar olmayan cihazlarında yasa kapsamı içine girebileceği endişeleri ile bilgisayar tanımı bilinçli olarak yapılmamaktadır.[193]

Ancak, her şeye rağmen, yaygın kullanımı nedeniyle bilgisayarın ne olduğuna değinilmesinde fayda görülmektedir. Bilgisayar, genel amaçlı kullanılabilme yeteneğine sahip, yeterince kavramlaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır.[194] Amerika Birleşik Devletleri'nde uygulanan genel ve sürekliliği bulunan federal yasaların bir araya getirildiği "United States Code", bilgisayara ilişkin 18. başlık 1030 (e) (1) maddesinde genişçe bir tanım ve bir kapsam alanı vermiştir. Bu maddeye göre, bilgisayar; mantıksal ve aritmetik olarak çalışan ya da depolama işlevi gören elektronik, manyetik, optik ya da yüksek hızla veri işleyen bir aygıttır. Bu tanımın ardından madde, tanımlanan aygıta bağlı olarak ya da bu aygıt ile birlikte çalışan veri depolama işlevine ya da iletişim işlevine sahip aygıtları kapsamı içine alırken, otomatik olarak çalışan daktilo, dizgi makinası, taşınabilir hesap makinası ve benzeri cihazları kapsam dışı bırakılmıştır. Yapılan tarif kapsamlı gözükse de, 1030. maddenin 1984 yılında yapıldığı ve sonrasında defalarca değiştirildiği göz

[193] Yılmaz Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 2005, Cilt:2 Sayı: 2 Yıl, s.404.
[194] R. Yılmaz Yazıcıoğlu, Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, İstanbul, Alfa Yayınevi, 1997, s.27

önüne alındığında[195] zamanla gelişen teknoloji karşısında bu tanımın da yetersiz kalacağı açıktır.[196]

Sözleşme, bilgisayarı bir sistem tarifi olarak kullanmıştır. Bilgisayar sisteminin, Sözleşme'de tanımı bir veya birden fazla parçası bir programa göre verileri otomatik olarak işleyerek çalışan bir cihaz veya birbiri ile bağlı veya bağlantılı bir grup cihaz şeklinde yapılmıştır. Açıklayıcı rapora göre, anılan cihaz, bir yazılım ve donanımdan oluşmaktadır ve doğrudan insan müdahalesi olmaksızın önceden belirlenen bir sonuca ulaşmak için bir bilgisayar programı ile verileri yönetmekte ve işlemektedir.[197]Sözleşme Komitesi, bilgisayar sisteminin daha geniş yorumlayarak uygulama alanını genişletmiştir. Komite, internete erişim sağlamak, e-posta göndermek, dosya iletmek, internet üzerinden içerik yüklemek veya içerik indirmek gibi veri üretme, işletme ve iletme işlevlerine sahip çok yönlü modern cep telefonları ve cep bilgisayarlarının başlı başına veri işleme özelliğine sahip olmaları nedeniyle bilgisayar sistemi kapsamında olacaklarına karar vermiştir.

Görülmektedir ki, bilgisayar sistemi ile kast edilen sadece masaüstü veya dizüstü bilgisayarlar değil, veri işleme özelliğine sahip tüm cihazlardır. Böylece, bir bilgi teknolojisi aracı olan bilgisayar, sözcüğünün bilgisayar sistemine kattığı darlık Sözleşme'nin açıklayıcı raporu ve komite kararı ile ortadan kaldırılmaktadır.

Mevzuatımızda, isabetle bilişim sistemi terimi seçimi ile Sözleşme'ye göre daha nötr ve teknolojik gelişmelere daha uyumlu bir dil kullanılmıştır. Bilişim sitemini daha iyi anlamak için bilişim sözcüğüne kısaca göz atmakta fayda bulunmaktadır.

---

[195] H. Marshall Jarrett- Michael W. Bailie, OLE Litigation Series, Prosecuting Computer Crimes, (çevrimiçi) http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf, s. 1-2, 29.04.2015

[196] Ali Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, Ankara 2011, 37

[197] Explanatory Report, p. 23.

Bilişim sözcüğü, Fransızca kökenli enformatik sözcüğü ile aynı anlamdadır ve enformatik sözcüğü ise enformasyon şeklinde Türkçe'de kullanılan Fransızca "informatique" sözcüğüne dayanmaktadır.[198]

Bilişim sözcüğü, Türk Dil Kurumu tarafından, "insanoğlunun, teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir" diye tarif edilmiştir.

Öğretide, bu tanıma paralel şekilde bilişimi bir bilim olarak kabul etmiştir. Örneğin, Yazıcıoğlu, bilgisayarlar aracılığı ile bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesi ile ilgilenen akademik ve mesleki disiplin şeklinde adlandırmıştır.[199] Dülger, daha geniş bir tanımla, bilişimi, "insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir" şeklinde tanımlamıştır.[200]

Kısaca, bilişim, iletişime konu bilginin elektronik yollarla işlenmesi, depolanması veya iletilmesi gibi işlemlere tabi tutulması ile ilgilenen bilimdir. Bilişimin, en önemli inceleme alanlarını, verinin işlenmesi, depolanması ve iletilmesi işlemlerinde en bilinen araç olan bilgisayar ve aynı işlemlere olanak sağlayan benzeri araçlar, daha doğrusu birden fazla bilgisayar ve benzeri aracın oluşturduğu bilgisayar sistemleri oluşturur.

5237 sayılı Yasa'nın 243. maddesinin gerekçesinde, bilişim sistemi, "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" olarak tanımlanmıştır. Ceza Muhakemesinde Ses ve

---

[198] Caner Yenidünya-Olgun Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul, 2003, s.27; Ahmet Caner Yenidünya, Ahmet Gökcen, Mehmet Emin Artuk, Türk Ceza Kanunu Şerhi, Adalet Yayınevi, 2. Basım, Ankara 2014, s. 6902; Karagülmez, s. 38; Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara 2014, s.69.
[199] R. Yılmaz Yazıcıoğlu, s.131.
[200] Dülger, s.71

Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in tanımlar ve kısaltmaların düzenlendiği 3. maddesinin 1. fıkrasının (b) bendinde, "bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sisteme" bilişim sistemi denmiştir. Yargıtay tarafından da bilişim sistemi, TCK'nın 243. maddesi gerekçesinde açıklandığı haliyle kabul edilmiştir.[201]

Görülmektedir ki, Sözleşme, aynı durumu, bilgisayar sistemi ile ifade ederken; mevzuatımız, bilişim sistemi terimi ile ifade etmektedir. Verilerin işleme tabi tutulduğu bu sistem farklı terimlerle ifade edilse bile, gerek bilgisayar sistemi ile gerek bilişim sistemi ile aynı şey ifade edilmektedir: verilerin otomatik olarak işleme tabi tutulmasını sağlayan cihazlar bütünü.

3. Bilgisayar Verisi ve Trafik Verisi

Sözleşme'nin 1. maddesinin (b) ve (d) fıkralarında sırasıyla bilgisayar verisi ve trafik verisi tanımlanmıştır. Bu tanımları incelemeden önce genel olarak veri kavramının ele alınmasında yarar görülmektedir.

Bu kavrama ilişkin en önemli tanımlama, Russell Ackoff tarafından 1988 yılında sistem teori ve bilimleri alanında kurulmuş uluslararası bir organizasyonda (International Society for the Systems Sciences) yapılan konuşmada yapılmıştır. Bu konuşmada veri kavramı başkaca kavramlarla birlikte hiyerarşik bir yaklaşımla açıklanmıştır. Ackoff'a göre, kavram hiyerarşisinde sırasıyla bilgelik (wisdom) başta olmak üzere sırasıyla anlayış (understanding), bilgi (knowledge), enformasyon (information) ve veri (data) yer almaktadır. Ackoff, önce gelenin sonra kalanı kapsadığını düşünmüştür.[202] Çalışmamızı ilgilendirmesi açısından,

- Veri, "gözlem ürünü olan, çevre, olay ve nesnelerin varlığını temsil eden semboller",[203]

---

[201] CGK, 2013/15-239 E – 2013/289 K, 11/06/2013; CGK, 2012/15-1293 E – 2013/111 K, 02/04/2013; CGK, 2009/11-193 E – 2009/268 K, 17/11/2009
[202] Russell L. Ackoff, From Data to Wisdom Presidential Address to ISGSR, http://fournier.facmed.unam.mx/ib1/2013/students/files/u2/FromDataWisdomAckoff.pdf, s3
[203] A.g.e s.3.

- Enformasyon, "veriden gelir; sistem olarak veriyi üretir, depolar, alır ve işler; tanımlama veya betimlemelerin içerisinde yer alır; kim, ne, ne zaman, kaç tane gibi soruların cevaplarıdır",[204]
- Bilgi ise, "öğrenme ile elde edilen, bir sistemin nasıl çalıştığını bilme gibi biliş ki bu enformasyonun, bir şeyin nasıl kullanılacağına dair bir yönergeye dönüşmesini mümkün kılar"[205],

ifadeleri ile açıklanmıştır.

Türk Dil Kurumu, veriyi, bilişim anlamında, olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi olarak[206]tanımlamıştır.

5651 sayılı Yasa'ya dayanılarak hazırlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkındaki Yönetmelik'in 3. maddesinin 1. fıkrasında, tanımlar başlığı altında ise veri, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri; bilgi ise, verilerin anlam kazanmış biçimi olarak tanımlanır.

Görüldüğü üzere, veri, bilgiye göre kapsamı daha dar ve henüz anlam kazanmamış yapıtaşları görünümündedir.

Sözleşme, veri kavramını, bilgisayar verisi olarak ele almayı tercih etmiştir. Bu tercih, bilgisayar verisi dışındaki sistem verilerinin, harici belleklerde yer alan veriler gibi, kapsam dışı kalabileceğini akla getirse de, Sözleşme'nin açıklayıcı raporunda elektronik ya da başkaca doğrudan işlenebilir ortamdaki bir verinin de bilgisayar verisi olduğu ayrıca vurgulanmıştır.[207] Sözleşme'nin 1. maddesinde yer alan veri tanımına göre veri, "bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder".

---

[204] A.g.e s.3.
[205] A.g.e. s.3.
[206] Türk Dil Kurumu, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54e10083b06c16.11562558
[207] Explanatory Report, Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu p 25 (çevrimiçi) http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 28.04.2015

5237 sayılı Yasa'nın Bilişim Sistemine Girme suçunun düzenlendiği 243. maddesinin gerekçesinde, veri kavramının doğrudan bir tanımı verilmeksizin, "sistem içindeki bütün soyut unsurlar" denilerek çerçevesi çizilmiştir. Aynı gerekçede sistem, "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" olarak açıklanmıştır. Bu iki tanım bir arada düşünüldüğünde, veri ile ilgili şu sakıncalı sonuca varılabilecektir: verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler içerisindeki bütün soyut unsurlar veridir. Böyle bir veri tanımı, tüm bilgisayarların manyetik olmak zorunda olmadığı, manyetikliğin bilgisayarın tek özelliği olmadığı dikkate alındığında[208] sadece manyetik özelliği bulunan sistemlerin içinde bulunan verileri koruyacaktır ki, bu dar yaklaşım uygulamada sorunlara neden olabilecektir. Bu nedenle açıklayıcı raporu ile Sözleşme'nin daha geniş bir veri tanımı ortaya koyduğu söylenebilir.

Sözleşme'nin 1. maddesinin (d) bendinde ise trafik verisi tanımlanmıştır. Bu tanıma göre, bir bilgisayar sistemi aracılığı ile gerçekleşen iletişimle ilgili olan, bir iletişim zincirinin bir parçası olan bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, zamanını, tarihini, boyutunu, süresini veya kullanılan hizmetin türünü gösteren herhangi bir bilgisayar verisi trafik verisidir.

Trafik verisi, Telekomünikasyon Kurumu Tarafından Erişim Sağlayıclara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esas Hakkında Yönetmelik'in 3. maddesinde erişim sağlayıcı trafik bilgisi ve yer sağlayıcı trafik bilgisi şeklinde iki ayrı tanımla açıklanmıştır. Buna göre erişim sağlayıcı trafik bilgisi ile internet ortamına erişime ilişkin olarak; abonenin adı, adı ve soyadı, adresi, telefon numarası, abone başlangıç tarihi, abone iptal tarihi, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları gibi bilgiler ifade edilmektedir. Yer sağlayıcı trafik bilgisi ile de, internet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP

[208] Yılmaz Yazıcıoğlu, Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 2005, Cilt:2 Sayı: 2 Yıl, 404

adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri ifade edilmektedir.

Bu tanımlamalardan anlaşılacağı üzere, Sözleşme ve mevzuatımızın trafik verisine yükledikleri anlamlar aynıdır.

4. Hizmet Sağlayıcı

Sözleşme'nin 1. maddesindeki bir başka tanımlama ise hizmet sağlayıcı hakkındadır. Sözleşme, hizmet sağlayıcıyı iki ayrı fıkrada ele almıştır. Bu düzenlemeye göre, ilk olarak, bilgisayar sistemleri aracılığı ile hizmet kullanıcılarına iletişim kurma olanağı sağlayan kamu veya özel tüzel kişiler, hizmet sağlayıcı olarak sayılmıştır. İkinci olarak ise, Sözleşme, kamu veya özel tüzel kişilerinin dışında iletişim hizmeti sunan tüzel kişiler adına veya böyle bir hizmetin kullanıcıları adına bilgisayar verisini işleyen ve depolayan her türlü kişiliği hizmet sağlayıcı olarak saymıştır.

Burada önemli olan, bir iletişim hizmetinin veya bir iletişim hizmeti ile bağlantılı bir veri işleme hizmetinin sunulmasıdır. Aksi halde, bir web sitesinin barındırılması için bir web barındırma şirketi ile anlaşan kişi gibi sadece içerik sağlayıcı hizmeti sunan bir kişinin bu kapsamda kabul edilmesi gerekir ki Sözleşme bunu kabul etmemektedir.[209] Böylece içerik sağlayıcının internet ortamına konulan her türlü içerikten sorumlu tutulmasının önüne geçilmek istenmiştir ki hakkaniyetli olan da budur.

Mevzuatımızda internet öznelerine ilişkin esas ve usuller 5651 sayılı Yasa'da düzenlenmiştir. Yasa'nın 1. maddesinde internet özneleri olarak, içerik sağlayıcılar, yer sağlayıcılar, erişim sağlayıcılar ve toplu kullanım sağlayıcılar sayılmıştır. Yasanın 2. maddesinde ise internet öznelerinin tanımı yapılmıştır.

Bu tanımlara göre, erişim sağlayıcı; kullanıcılarına internet ortamına erişim sağlayan her türlü gerçek ve tüzel kişiyi ifade etmektedir. İçerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren

[209] Explanatory Report, 27.

ve sağlayan gerçek veya tüzel kişilerdir. Yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan ve işleten gerçek ve tüzel kişilerdir. Toplu kullanım sağlayıcı ise, kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan kişilerdir.

5651 sayılı Yasa'da sayılan internet öznelerinin tanımları dikkate alındığında Sözleşme'nin hizmet sağlayıcı tanımı içerisine girdiği söylenebilir. Ancak yasada geçen içerik sağlayıcı tanımından hareketle gelişen yeni web teknolojilerinin sağladığı ortamlarda yorum yapmak, video yüklemek şeklinde içerik üretmek veya bu anlamda bir içeriği değiştirmek hizmet sağlayıcı kapmasına girmemelidir. Çünkü bu durumda iletişim ve veri işleme hizmeti sağlanmadığı açıktır.

5651 sayılı Yasa tarafından internet öznelerine getirilen yükümlülükler de ilgili internet öznelerinin sağladıkları iletişime ilişkin olup, bu husus da onların hizmet sağlayıcı tanımı içerisine girdiğini göstermektedir. Örneğin, 5651 sayılı Yasa'nın 4. maddesi içerik sağlayıcıları bağlantı sağladığı başkasına ait içerik haricinde internet ortamında sunulan her türlü içerikten sorumlu tutmuştur. Yer sağlayıcılar hukuka aykırı içerikleri çıkarmak ve trafik bilgilerini sağlamak ile; erişim sağlayıcılar trafik bilgilerini saklamak, gerektiğinde erişimi engellemek ile yükümlüdür. Toplu kullanım sağlayıcılar ise, konusu suç oluşturan içeriklere erişimi engelleme ve kullanıma ilişkin kayıtları tutmakla yükümlüdür. Bu haliyle anılan internet özneleri hem tanımları hem de yükümlülükleri açısından bilgisayar sistemleri üzerinden iletişim olanağı sağlayarak Sözleşme'de tarifi yapılan hizmet sağlayıcı tanımı içerisine girmektedir.

C. Maddi Ceza Hukuku Açısından Karşılaştırmalı Bakış

1. Giriş

Sözleşme'nin 2 ila 10. maddeleri arasında temel olarak toplam 9 suça yer verilmiştir. Bu suçlar bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine karşı suçlar, bilgisayar bağlantılı suçlar, içerik ile ilgili suçlar ve telif hakları ve benzeri hakların ihlali suçları başlıkları ile dört ayrı bölümde ele alınmıştır. Bu düzenlemeler, ceza özel hukukuna ilişkin olup, Sözleşme'nin 11., 12.

ve 13. maddelerinde ise ceza genel hukukuna ilişkin hükümlere yer verilmiştir. Bu hükümlerde sırasıyla suça teşebbüs ve iştirak, tüzel kişiliğin sorumluluğu ve yaptırımlar ve tedbirler düzenlenmiştir. Sözleşme'nin genel ceza hukukuna ilişkin bu hükümleri ile mevzuatımız açısından genel bir uyum olduğu gözlemlendiğinden, çalışmamızda genel hükümler ayrıca ele alınmamıştır. Zaten Sözleşme'de bu hükümlerle ilgili olarak birebir bir uyum da aramamakta, konuyu büyük oranda taraf devletlerin takdirine bırakmaktadır.[210]

2. Yasadışı Erişim (SSS madde 2)

" Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir kısmına haksız ve kasıtlı olarak erişilmesini suç saymak için gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir. Taraf devlet bu suçun işlenebilmesi için bilgisayar verisini elde etmek niyetiyle veya başkaca kötü niyetle güvenlik önlemlerinin ihlal edilmesini ya da bir bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla güvenlik önlemlerinin ihlal edilmesini gerekli kılabilir."

Sözleşme'de düzenlenen ilk suç tipidir. Bilgisayar sistem ve verilerinin gizlilik, bütünlük ve erişilebilirliğine yönelik işlenen bir suç tipidir. Bu suça ilişkin hareket unsuru, yani erişim, ileride işleyeceğimiz diğer siber suçların da temelini, bir anlamda çıkış noktasını oluşturmaktadır. Siber suçlu öncelikle bilgisayar sistem ve verilerine erişim sağlamalıdır. Sonrasında ise daha nitelikli olan bilgisayar ile ilgili sahtecilik, hırsızlık ve dolandırıcılık suçlarını işleyecektir.[211]

Bu suç ile korunmakta olan hukuksal yarar, kişilerin ve örgütlenmelerin bilgisayar sistemlerini rahatsız edilmeden ve özgürce işletmeleri, yönetmeleri ve kontrol etmeleri, yani bilgisayar sistemlerinin güvenliğidir. [212]

Sözleşme, erişimi, bilgisayar sistemlerinin bütününe veya bilgisayar donanımı, bileşeni, sistem içerisinde saklanmış verileri, dizinleri, trafik ve içerik

[210] Explanatory Report, 118, 122, 126, 130.
[211] Explanatory Report, 44.
[212] Explanatory Report, 44.

verileri gibi sistemin parçalarına girilmesi olarak tanımlamıştır.[213] Sisteme e-posta veya dosya gönderilmesi erişim olarak kabul edilmemiştir. Suçun oluşabilmesi için sisteme girilmesinin herhangi meşru bir hakka dayanmaması gerekmektedir. Diğer bir ifadeyle, Sözleşme yetkisiz erişimi suç olarak düzenlemiştir.[214]

İlgili maddede açıkça belirtildiği üzere bu suçun işlenmesinde kasten hareket edilmesi gerekmektedir. Taksirle eylemin gerçekleştirilmesi suç olarak kabul edilmemiştir.

Sözleşme sadece yetkisiz olarak erişimi suç olarak düzenlediği için bu durum bazı devletler tarafından izlenen suç ve ceza politikaları gereği ağır bir düzenleme olarak görülebilecektir. Bu nedenle ilgili maddenin ikinci fıkrasında yetkisiz erişimin güvenlik önlemlerinin ihlal edilmesi ile birlikte gerçekleşmesi halinde suçun oluşabileceği yönünde suçun daha nitelikli bir hale getirilmesi taraf devletlerin takdirine bırakılmıştır. Böylece taraf devletlere daha dar bir çerçeveden bu suça yaklaşım olanağı sağlanmıştır.[215]

Ülkemiz iç hukuku açısından yukarıda açıklanan suçun karşılığına "bilişim sistemine girme" başlığı altında 5237 sayılı TCK'nın 243. maddesinde yer verilmiştir. Bu maddenin birinci fıkrasına göre, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek ve orada kalmak suç olarak kabul edilmiştir. Sözleşme'den farklı olarak sisteme sadece erişim suç olarak kabul edilmemiş, sisteme girme ile birlikte ayrıca sistemde kalmaya devam etme hali suç olarak düzenlenmiştir. Her ne kadar TCK'nın ilgili maddesinin gerekçesinden sisteme sadece girmenin suç olarak kabul edildiği anlamı çıkarılsa da, öğretide gerekçenin hatalı olduğu ve esas olanın madde metni olduğu gerçeği nazara alındığında böyle bir çıkarım doğru olmayacağı belirtilmiştir. TCK'da düzenlenen bu suçun gerçekleşmesi için sisteme girme ve orada kalma hareketinin gerçekleşmesinin yeterli olması ve bu hareket sonucunda zarar gibi bir neticenin varlığına gerek olmaması nedeniyle bu suç, soyut tehlike suçudur.[216] Suçun varlığı

[213] Explanatory Report, 46.
[214] Explanatory Report, 47.
[215] Explanatory Report, 49-50.
[216] Dülger, s.365; Karagülmez, s.183-184.

için aranan hareketlerden birini de sistemde kalmaya devam etme oluşturduğu için bu suç aynı zamanda mütemadi bir suçtur.[217]

Yargıtay uygulamaları da bu yönde gelişmiştir. Örneğin, Yargıtay tarafından, katılana ait MSN adresine şifresini ele geçirmek suretiyle hukuka aykırı olarak giren ve orada kalmaya devam eden sanığın eyleminin 243/1 maddesi kapsamında kaldığı[218], yine sanığın giriş yaptığı katılana ait adresinden onun arkadaşlarına pek çok sayıda hakaret ve uygunsuz görüntüler içeren mesajlar gönderdiğinden bahisle bilişim suçundan açılan davada, 244/2 de yazılı seçimlik hareketlerin yapıldığına ilişkin bir tespit bulunmaması karşısında, eylemin 243/1 maddesine uygun olduğu[219] değerlendirilmiştir.

TCK, suçun oluşumu için aradığı hareketler itibariyle Sözleşme'ye göre daha dar bir yaklaşım sergileyerek, suçun işlenebilmesi eşiğini sisteme girme ve orada kalma hareketlerini birlikte arayarak yükseltmiştir. Sözleşme'de yer alan güvenlik önlemlerinin ihlal edilmesi unsuruna TCK'da yer verilmemiştir.

TCK, Sözleşmeden farklı olarak 243. maddede iki düzenleme daha yapmıştır. Bunlardan birincisi, maddenin ikinci fıkrasında düzenlenen sisteme girme ve orada kalma eyleminin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesidir. Eylemin bu şekilde gerçekleşmesi halinde daha hafif bir ceza öngörülmüştür. Bir örnekle açıklarsak, bir abonelik bedeliyle internet gazetesi abonesinin, takibini yaptığı gazetenin erişim izninin bulunmadığı abonelerine ait kişisel verilerin yer aldığı alana girmesi ve orada kalması ile bu suçun basit halinin oluştuğu düşünülebilir.

İkinci düzenleme ise, 243. maddenin üçüncü fıkrasıdır. Bu fıkrada, sisteme girme ve orada kalma eylemi neticesinde sistemin içerdiği verilerin yok olması veya değişmesi düzenlenmiştir. Bu suç, maddenin gerekçesinde de belirtildiği üzere suçun neticesi sebebiyle ağırlaştırılmış halidir ve failin kasten girdiği ve orada kaldığı sistem içerisindeki verileri TCK'nın 23. maddesi uyarınca en azından

[217] Dülger, s.365; Karagülmez, s.183-184.
[218] 8 C.D. 2014/5592 E- 2014/14132 K, 09/06/2014
[219] 8 C.D. 2014/607E- 2014/15426 K, 18/06/2014

taksirle yok etmesi veya değiştirmesi söz konusudur. Bu durum Sözleşmesi açısından ilginçtir. Çünkü Sözleşme'de taksirle işlenen suçlara yer verilmediği gibi yer verilen suçların ancak kasten işlenebileceği ayrıca belirtilmiştir.

Sonuç olarak, görüldüğü üzere Sözleşme'nin 2. maddesi ile TCK'nın 243. maddesi gerek suçun basit hâli itibariyle gerekse de nitelikli hâlleri itibariyle birbirleri ile uyum içerisinde değildirler.

3. Yasadışı Müdahale (SSS madde 3)

"Her bir taraf devlet, bir bilgisayar sistemine, bir bilgisayar sisteminden veya bir bilgisayar sistemi içerisinden, bilgisayar verisi taşıyan bilgisayar sisteminden çıkan elektromanyetik dalgalar dâhil olmak üzere bilgisayar verilerinin kamuya açık olmayan bir şekilde iletilmesine teknik araçlarla kasten ve haksız bir şekilde müdahale edilmesini suç saymak için gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir. Taraf devlet bu suçun gerçekleşmesi için kötü niyetle hareket edilmesini ya da bir bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla işlenmesini gerekli kılabilir."

Sözleşme'nin bu maddesi ile bilgisayar verilerinin kamuya açık olmayan bir şekilde iletilmesine teknik araçlarla müdahale edilmesi suç olarak düzenlenmiştir. Burada özel olan bilgisayar verisi olmayıp, iletişimin kendisidir. Yani bu madde ile bilgisayar verisinden ziyade, veri iletişiminin gizliliği korunmaktadır. Burada korunan değer, geleneksel anlamda telefon görüşmelerinin dinlenmesi ve kayda alınması ile ihlal edilen ve İHAS'ın 8. maddesi ile teminat altına alınan[220] haberleşmenin gizliliği hakkı ile aynı haktır.[221]

İşlenen suçun ağırlığı ile daha dengeli bir düzenleme olması ve bu suçun kapsamının daraltılarak gereğinden fazla eylemin yasadışı müdahale suçu haline gelmesini önlemek amacıyla eylemin, iletim hatlarına takılan teknik cihazlar ya da kablosuz iletişimi kaydetmekte kullanılan cihazlar gibi teknik araçlarla iletişim içeriğini dinlemek, izlemek veya gözetlemek suretiyle gerçekleştirilmesi

[220] Osman Doğru-Atilla Nalbant, İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar, Pozitif Matbaa, Ankara 2013, 2. Cilt, s. 53.
[221] Explanatory Report, 51.

gerekmektedir.[222]Teknik araçlar kullanılmaksızın gerçekleştirilecek müdahaleler bu suç kapsamına giremeyecektir. Yine bu suçun kapsamının daraltılması için taraf devletler, bu suçun kötü bir niyetle işlenmesini veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemi ile ilişkili olarak işlenmesini şartını getirebilirler.[223]

Bu suç, kasten işlenebilir ve failin haksız biçimde eylemi gerçekleştirmesi gerekmektedir.[224] Mağdurun rızası, hukuka aykırılık unsurunu ortadan kaldıracaktır. Taraf devletin bir ulusal güvenlik nedeniyle ya da suç ve düzensizliği önleme amacıyla müdahalesi haksız sayılamayacaktır.

Avrupa Konseyi resmi sitesinde siber suçlarla ilgili ülke profillerinin yer aldığı sayfada ülkemiz mevzuatında Sözleşme'nin 3. maddesine karşılık olarak TCK'nın 243. maddesinde düzenlenen "bilişim sistemine girme" suçu gösterilmiş ise de[225], bu yanlıştır. 243. maddede, "yasadışı erişim" konusunda da değinildiği üzere iletişime müdahale düzenlenmemektedir. İletişime müdahale bir noktaya kadar bazen yasadışı erişimi de gerektirmektedir. Ancak eylemler unsurları ile birlikte bir bütün olarak değerlendirildiğinde, "yasadışı müdahale" ile "bilişim sitemine girme" eylemlerinin birbirini karşılamadığı görülecektir.

İç hukukumuz açısından, bilgisayar verilerinin kamuya açık olmayan iletimine teknik araçlarla müdahale edilmesi eylemini suç sayan özel bir düzenleme bulunmamaktadır. Bu eylemi de içine alabilecek daha genel düzenlemeler mevcuttur ve her somut olaya ilişkin olaya uygun suç tipi uygulanmaktadır. Sözleşme'nin 3. maddesine karşılık gelecek düzenlemeleri aşağıda sayılan suçlar üzerinden değerlendirebiliriz.

- TCK'nın 132. maddesinde düzenlenen "haberleşmenin gizliliğini ihlal" suçu: Bu düzenleme ile kişiler arasındaki haberleşmenin ihlali suç sayılmış,

[222] Explanatory Report, 53.
[223] Explanatory Report, 59.
[224] Explanatory Report, 58.
[225] Cybercrime Legislation, Country Profile, Turkey, 25.01.2011, (çevrimiçi) http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/cyber_cp_Turkey_2011_January.pdf , 29.04.2015

haberleşme içeriklerinin kayıt altına alınması suçun nitelikli bir şekli olarak görülmüştür. Araç olmaksızın yapılan iletişim konuşma olacağından, kişiler arasındaki iletişimin haberleşme olması için bir araç gerekmektedir.[226]Madde gerekçesine göre, haberleşmenin hangi araçla yapıldığının önemi yoktur.[227]Yargıtay, eşi tarafından işletilen internet cafede bulunan ana bilgisayardan, görümcesi mağdurenin MSN'de evli bir erkekle cinsel içerikli ikili sohbet görüşmelerine ilişkin elektronik iletileri içeren yazı dökümlerinin alınmasını bu madde kapsamında değerlendirmiştir.[228]

- TCK'nın 133. maddesinde düzenlenen "kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması": Bu düzenleme ile bir alet kullanılmadan, yüz yüze yapılan konuşmaların gizliliği korunmuş ve internet yoluyla veya telefonla yapılan sesli ya da görüntülü iletişim haberleşme sayılarak bu maddenin kapsamı dışında bırakılmıştır.[229]
- TCK'nın 134. maddesinde düzenlenen "özel hayatın gizliliğini ihlal": Madde gerekçesine göre, bu düzenleme ile gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi suç sayılmıştır.[230]Bu düzenleme genel bir düzenleme olup, eylemin başkaca bir suçu oluşturması halinde bu madde uygulanmayacaktır.[231]Örneğin, eylem haberleşmenin gizliliğini ihlal niteliği taşıyorsa TCK'nın 132. maddesi uygulanacaktır.

Bu açıklamalar ışığında, kişiler arasında gerçekleşen konusunu bilgisayar verisi oluşturan ve teknik araçlarla gerçekleştirilen bir iletişim, bir haberleşme niteliğinde ise, bu eylem TCK'nın 132. maddesi kapsamında kalacaktır. Haberleşme niteliği bulunmayan herhangi bir iletişime teknik araçlarla yapılan bir müdahale ise TCK'nın 134. madde çerçevesinde değerlendirilmelidir. TCK'nın

---

[226] Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, Yorumlu-Uygulamalı Türk Ceza Kanunu, Adalet Yayınevi, Ankara 2014, 3. Cilt, s.4307.
[227] Özgenç, s.843.
[228] 12. C.D. 2012/19742 E – 2012/20412 K, 02.10.2012
[229] Yaşar – Gökcan - Artuç, s4345.
[230] Özgenç, s.846.
[231]Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, s4375.

133. maddesinde yüz yüzelik arandığı için bu suçu "yasadışı müdahale" kapsamında değerlendirmek mümkün değildir.

Sonuç olarak, Sözleşme'de yer alan "yasadışı müdahale", özel olarak mevzuatımızda yer almamakla beraber ilgili hüküm ile korunmakta olan bilgisayar verilerinin iletiminin gizliliği hakkı, yukarıda açıklanan daha genel düzenlemeler ile korunmaktadır. Ancak, öğretide Sözleşme'de yer alan "yasadışı müdahale"nin mevzuatımızda karşılığının olmadığı yönünde aksi görüşler de bulunmaktadır.[232]

4. Verilere Müdahale (SSS madde 4)

" 1-Her bir taraf devlet, haksız bir şekilde ve kasten bilgisayar verisine zarar verilmesini, verinin silinmesini, verinin bozulmasını, verinin değiştirilmesin veya engellenmesini kendi ulusal mevzuatı kapsamında suç saymak için gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir.

2 – Taraf devlet 1. paragrafta tanımlanan eylemin ciddi bir zararla sonuçlanması şartına bağlanması hakkını saklı tutabilir."

Bu düzenleme ile bilgisayar verilerine maddede belirtilen seçimlik hareketlerle müdahale edilmesi suç kabul edilmiştir. Suç oluşması için müdahalenin kasten ve haksız bir şekilde gerçekleştirilmesi gerekmektedir.

Verilere müdahale suçu ile geleneksel mala zarar verme suçuna paralel olarak bilgisayar veri ve programlarının da korunması amaçlanmış ve korunan hukuksal yarar olarak bilgisayar veri programlarının bütünlüğü ve düzgün bir şekilde işlemesi olarak görülmüştür.[233]

Maddede seçimlik hareketler, zarar vermek, silmek, bozmak, değiştirmek ve engellemek olarak ayrı ayrı sayılmıştır. Zarar verme ve bozma ile veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz şekilde değiştirilmesi; silme ile fiziki bir varlığı bulunan eşyanın imhası gibi yok edilmesi, tanınmaz hale getirilmesi; engelleme ile verinin erişilmez kılınmasına neden olan herhangi

[232] Karagülmez, s.255; Dülger, s.423.
[233] Explanatory Report, 60.

eylemi; değiştirme ile var olan verinin kötücül yazılımlarla farklı hale getirilmesi dâhil olmak üzere başka biçime sokulması anlaşılmaktadır.[234]

Maddenin ikinci fıkrasına göre, taraf devlet ciddi bir zarar sonucunu doğurmayan veri müdahalesi eylemini suç saymayabilir. Böylece uygulamada hafif nitelikteki basit olayların soruşturulmasına gerek kalmayacaktır.

Mevzuatımız açısından, Sözleşme'nin 4. maddesindeki hükmün karşılığı, TCK'nın "sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlığı altında yer alan 244. maddenin 2. fıkrasındaki düzenlemedir. Bu düzenlemeye göre, bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka yere göndermek suçtur.

TCK'da yer alan bu suç ile Sözleşme'de yer alan veri müdahalesi suçunun tam bir uyum içerisinde olduğu söylenebilir. Her ne kadar TCK düzenlemesinde yer alan seçimlik hareketler ile, Sözleşme'de yer alan seçimlik hareketlerin aynı şekilde ifade edilmediği görülse de, her iki düzenlemenin anlam itibariyle birbirleri ile örtüştükleri açıktır.

Yargıtay kararlarında, sanığın, yetkisi olmadığı halde katılan şirkete ait bilişim sistemine girerek orada bulunan verileri alıp kendi kullandığı bilgisayara ve CD'ye aktarması şeklindeki eylem[235]; sanığın katılana ait elektronik posta adresinin güvenlik şifresini kullanıp şifre değişikliği yaparak katılanın elektronik posta adresine kendi şifresi ile girişini engellemesi şeklindeki eylem[236]; mağdurlara ait e-mail adreslerinin ele geçirilip şifrelerinin değiştirilmesi eylemi[237]; sanığın katılana ait elektronik posta adresi ve facebook sayfasının şifresini değiştirerek katılanın erişimine engel olması şeklindeki eylem[238]; sanığın katılana ait e-posta adresinin ve bu adrese tanımlı facebook hesabının güvenlik şifresini kullanıp şifre değişikliği yaparak katılanın elektronik posta adresine ve bu adrese tanımlı facebook hesabına

[234] Explanatory Report, 61.
[235] 8. C.D. 2013/3173 E – 2014/18506 K,14.07.2014
[236] 8. C.D. 2013/11478 E – 2014/8887 K, 08.04.2014
[237] 8. C.D. 2012/32138 E – 2013/28031 K, 26.11.2013
[238] 8. C.D. 2014/14716 E-2014/20052 K, 17.09.2014

kendi şifresi ile girişini engellemesi şeklindeki eylem[239] 244/2 kapsamında değerlendirilmiştir.

TCK, Sözleşme'den farklı olarak ayrıca veriye müdahalenin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinden gerçekleştirilmesini nitelikli hal olarak görmüştür. Sözleşme'de yer alan bu suç nedeniyle ciddi bir zararın doğması unsuruna TCK'da yer verilmeyerek hareketin gerçekleşmesi ile suçun oluştuğu kabul edilmiştir.

5. Sisteme Müdahale (SSS madde 5)

"Her bir taraf devlet, bilgisayar sistemine veri yükleyerek, verileri aktararak, verilere zarar vererek, verileri silerek, bozarak, değiştirerek veya engelleyerek bilgisayarın sisteminin çalışmasını kasten ve haksız bir şekilde ciddi ağırlıkta aksatma eylemini suç saymak için kendi ulusal mevzuatı kapsamında gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir."

Bilgisayar sabotajı olarak da bilinen sisteme müdahale eylemi ile bilgisayar verilerinin kullanılması veya bu verilere etki edilmesi ile bilgisayar sistemlerinin işleyişinin engellenmesi suç sayılmış olup, bilgisayar ve telekomünikasyon işletmecileri ve kullanıcılarının sistemlerini düzgün bir şekilde çalıştırmaları suçla korunan menfaat olarak kabul edilmiştir.[240] Bu suç için veri yüklemek, verileri aktarmak, verilere zarar vermek, verileri silmek, bozmak, değiştirmek veya engellemek hareketlerinden birinin gerçekleştirilmesi ve bu eylemin ciddi bir sistem aksaması ile sonuçlanması gerekmektedir.

Sisteme müdahale sonucu sistemin işleyişinin ciddi ölçüde aksaması gerekmektedir. Örneğin, hizmet aksatmaya yönelik olarak yapılan DoS saldırıları veya istek dışı sıklıkla ve çok fazla sayıda e-posta gönderilmesi (spam) ile bilgisayar sisteminin çalışmasının tamamen veya kısmen engellenmesi durumunda ciddi ölçüde bir aksama olduğu ve suçun işlendiğinin kabulü gerekmektedir.[241]

---

[239] 8. C.D. 2014/15404 E – 2014/23560 K, 27.10.2014
[240] Explanatory Report, 65.
[241] Explanatory Report, 67.

Sözleşme'de düzenlenen sisteme müdahale suçunun karşılığını, TCK'nın 244. maddesinin 1. fıkrasında yer alan düzenleme oluşturmaktadır. Bu düzenlemeye göre, bilişim sisteminin işleyişini engellemek veya bozmak suç sayılmıştır. Her iki düzenlemede yer alan seçimlik hareketler farklı ifadelere rağmen aynı özü temsil etmektedir. TCK'da yapılan seçimlik hareketlerden sonra bir netice aranmamaktadır. Sistemin ciddi ölçüde aksayıp aksamaması Sözleşme'den farklı olarak TCK'da önem arz etmemektedir.

Yargıtay, sanığın, erişim yetkisini izinsiz kullanarak siteye kendi yazdığı metni koyarak siteye başkalarının olağan erişimini engelleme olayında;[242] sanıkların İl Emniyet Müdürlüğüne ait internet sitesine izinsiz olarak girerek işleyişini engelleyip bozma olayında;[243] sanığın önceden ATM'nin kart yuvasına taktığı aparatla kurduğu düzenek ile bilişim sisteminin bir parçası olan ATM'nin çalışmasını engellediği, mağdur tarafından henüz kart yuvaya yerleştirilmeden emniyet görevlilerinin müdahale ettikleri olayda;[244] 244/1 maddesinde düzenlenen suçun oluştuğunu kabul etmiştir.

Sözleşme'de yer alan sistemde ciddi ölçüde aksama unsuru dışında, sisteme müdahale bağlamında Sözleşme ile TCK'nın birbirleri ile uyumlu oldukları söylenebilir.

6. Cihazların Kötüye Kullanımı (SSS madde 6)

"1- Her bir taraf devlet haksız bir şekilde ve kasten kendi ulusal mevzuatı kapsamında,

a) i. 2 ila 5. maddelerdeki suçları işlemek amacıyla tasarlanmış ya da uyarlanmış bir bilgisayar programı da dahil olmak üzere bir cihazın,
ii. 2 ila 5. maddelerdeki suçları işlemek amacıyla, bir bilgisayar sisteminin tamamına ya da bir kısmına erişimi sağlayan şifre, giriş kodu, ya da benzer verinin,

[242] 8. C.D. 2013/17448 E – 2014/10032 K 21.04.2014
[243] 8. C.D. 2013/4359 E – 2014/12455 K, 15.05.2014
[244] 11. C.D. 2013/20444 E- 2013/18100 K, 02.12.2013

üretimini, satışını, kullanım amaçlı tedarik edilmesini, ithalini, dağıtımını ya da başka şekilde erişilebilir hale getirilmesini,

b) Yukarıda paragrafta i ya da ii ile belirtilen vasıtalara 2 ila 5. maddelerde belirtilen suçların işlenmesi amacıyla sahip olunmasını,

suç saymak için gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir. Bir taraf devlet, cezai sorumluluğun doğması için bu vasıtalara elde bulundurulması için bir sayı sınırlaması öngörebilir.

2- Bu madde, birinci maddenin birinci paragrafında yer alan vasıtaların üretimi, satışı, kullanım amaçlı tedariki, ithali, dağıtımı veya başka şekilde erişilebilir hale getirilmesi veya sahip olunmasının 2 ila 5. maddeler uyarınca suç işlemek amacıyla gerçekleştirilmemesi halinde, örneğin bir bilgisayar sisteminin yetkili olarak test edilmesi veya korunmasında olduğu gibi, cezai sorumluluk doğuracağı şeklinde yorumlanamayacaktır.

3- Her bir Taraf devlet, paragraf 1 (a) (ii) de yer alan vasıtaların satışı, dağıtımı veya başka şekilde erişilebilir hale getirilmesi ile ilgili değilse, bu maddenin birinci paragrafını uygulamama bir hakkını saklı tutabilir."

Bu düzenleme ile cihazlarla ilgili olarak maddede gösterilen seçimlik hareketlerden birinin gerçekleştirilmesi ya da bilgisayar sistemleri ve verilerinin gizliliği, bütünlüğü ve erişilebilirliğine karşı yasadışı erişim, yasadışı müdahale, verilere müdahale veya sisteme müdahale suçlarını işlemek için kötüye kullanılacak verilere erişilmesi ayrı ve bağımsız birer suç sayılmıştır. [245]Böylece bilgisayar korsanlarının suç işlemekte kullandıkları içerisinde kötücül yazılımlar gibi programların olduğu alet çantalarının boşaltılması amaçlanmıştır.

Düzenlemenin birinci fıkrasının (a) bendinin birinci cümlesinde Sözleşme'nin 2 ila 5. maddelerinde tanımlanan suçların işlenmesi için özel olarak tasarlanmış cihazların üretimi, satışı, kullanım amaçlı tedariki, ithali, dağıtımı veya başka şekilde erişilebilir hale getirilmesi yasaklanmıştır. (a) bendinin ikinci

[245] Explanatory Report, 71.

cümlesinde ise aynı eylemlerin bir bilgisayar sisteminin tamamına ya da bir kısmına erişim sağlayan şifre, giriş kodu ya da benzer veriyle ilgili olarak gerçekleştirilmesi yasaklanmıştır. Birinci fıkranın (b) bendi ile de yasaklanan bu cihaz ve verilere sahip olunması suç sayılmıştır.

Burada önemli olan husus, cihaz ve verilerin suçun işlenmesine özgülenmiş olmasıdır. Bu şekilde bilgisayar sistemlerinin yetkilendirilmiş testi ve korunması amacıyla üretilen program, yazılım gibi araçların varlığı korunmuştur.[246]

Bu suç da, açıklanan diğer suçlar gibi kasten ve haksız bir şekilde işlenmelidir.[247]

Bu düzenleme sonucunda bir suçun işlenmesi için özel olarak hazırlanan bir yazılım 6136 sayılı Yasaya göre yasak niteliği haiz silah gibi başlı başına suça konu olacaktır. Böylece henüz suçun işlenmesinde kullanılmayan kötücül bir yazılıma sahip olan biri bu suçun şüphelisi olabilecektir. Tabi ki, bu durumda herhangi bir hak ihlaline neden olmamak için bu suçun soruşturma ve kovuşturmasında daha dikkatli olmak ve şüphelinin kastını iyi araştırmak gerektirmektedir.

Genel olarak, mevzuatımız açısından Sözleşme'de düzenlenen bu suçun karşılığı bulunmamaktadır. Suçta kullanılan cihaz ve veriler müsadereye tabi ise de, ayrıca başlı başına suça konu değildir. Ancak banka ve kredi kartlarını bilişim sisteminin bir parçası olarak değerlendirirsek, TCK'nın 245/2 maddesi ile başkalarına ait banka hesaplarıyla ilişkilendirilen sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etmenin suç olarak kabul edilmesi karşısında, Sözleşme'nin 6. maddesinin kısmen dahi olsa bir karşılığının bulunduğu söylenebilir.

7. Bilgisayarla Bağlantılı Sahtecilik (SSS madde 7)

"Her bir Taraf devlet, sahte verilerin gerçek veriler gibi kabul edilmesi ve işlem görmesi için bilgisayar verilerinin girilmesi, değiştirilmesi, silinmesi veya

[246] Explanatory Report, 77.

[247] Explanatory Report, 76.

engellenmesi eylemlerini, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına bakılmaksızın suç saymak için kendi ulusal mevzuatı kapsamında gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir. Bir Taraf devlet cezai sorumluluğun doğması için aldatma niyeti veya benzeri kötü niyetin varlığını arayabilir."

Bu düzenleme ile fiziki belgede sahtecilik suçlarına paralel bir hüküm getirilerek, hukuki etki ve sonuçları bulunabilecek elektronik verilerin güvenliği ve güvenirliliği korunmuştur.[248]Böylece elektronik belgeler, tıpkı fiziki belgeler gibi korunacak ve elektronik ortamda yapılabilecek müdahale ve saldırılar cezalandırılacaktır. Bu suçta bilgisayar sistem ve verilerinin manipüle edilmesi söz konusudur.[249]

Düzenlemede geçen bilgisayar verilerinin girilmesi ile sahte bir e-belgenin düzenlenmesi ve üretilmesi kast edilirken; verilerin değiştirilmesi (e-belgenin kabul edilebilir şekilde yeniden düzenlenmesi, farklı hale getirilmesi, kısmi değişikliklere tabi tutulması gibi), verilerin silinmesi (verinin saklandığı araçtan çıkarılması) ve verilerin engellenmesi (verinin tutulması, gizlenmesi, saklanması) ile gerçekliği bulunan bir e-belgenin sahte hale getirilmesi amaçlanmıştır.[250]

Sözleşmede yer alan e-belgede veya veride sahtecilik suçunun tam karşılığı mevzuatımızda bulunmamaktadır. Buna rağmen e-belgede sahtecilik suçlarına, 5237 sayılı Yasa'da yer alan sahtecilik suçlarının uygulanmasının önünde bir engel de yoktur.[251]

TCK'da belge tanımı yapılmamıştır. Fakat 6100 sayılı Hukuk Usulü Muhakemeleri Kanunu'nun 199. maddesinde uyuşmazlık konusu vakıaları ispata elverişli elektronik ortamdaki veriler belge olarak; aynı yasanın 205. maddesinin 2. fıkrasında ise usulüne göre güvenli elektronik imza ile oluşturulan veriler senet

[248] Explanatory Report, 81.
[249] Explanatory Report, 80.
[250] Explanatory Report, 83.
[251] Kubilay Taşdemir, Belgelerde Sahtecilik Suçları, Ütopyagrafik, Ankara 2013, s.297.

olarak kabul edilmiştir. Buna göre mevzuatımız açısında e-belgeye genel bir çerçeve verildiği görülmektedir.

Fiziki bir belgede aranan yazılı olmak, yazanı ya da düzenleyeni bilinebilir olmak, içeriğe sahip olmak ve taşınabilir olmak unsurlarının e-belgelerde de bulunduğu açık olduğuna göre, TCK'da yer alan resmi belgede sahtecilik (204. madde), resmi belgeyi bozmak, yok etmek veya gizlemek (205. madde), özel belgede sahtecilik (207. madde) ve özel belgeyi bozmak, yok etmek veya gizlemek (208. madde) suçları e-belgede sahtecilik suçlarına da uygulanabilecektir.[252] Sonuç olarak, bilgisayar bağlantılı sahtecilik suçların karşılığı mevzuatımızda bulunmaktadır.

Bir hususa daha değinmek gerektir ki, TCK'nın 244/2 maddesinde düzenlenen suçun da e- sahtecilik suçlarına uygulanabileceği akla gelmektedir. Ancak TCK'nın 244/2 maddesine konu verilerin, e-belge niteliğini taşımaması nedeniyle bu düzenleme e-sahtecilik suçlarına uygulanamayacaktır.[253] Böyle bir seçenek zaten Sözleşme tarafından da kabul edilmemiştir. Bu seçenek kabul edilseydi, Sözleşme, TCK'nın 244/2 maddesine karşılık gelen "veriye müdahale" suçunu düzenledikten sonra ayrıca bilgisayarla bağlantılı sahtecilik suçuna yer vermezdi. Sözleşme'de yer alan veriye müdahale ve bilgisayar bağlantılı sahtecilik suçları ile korunan hukuksal yarar farklı olduğu gibi TCK'da düzenlenen belgede sahtecilik ile verileri yok etme veya değiştirme suçları ile korunan hukuksal yarar da farklıdır.

8. Bilgisayarla Bağlantılı Dolandırıcılık (SSS madde 8)

" Her bir Taraf devlet, kasten ve haksız bir şekilde, bir başkasının mal kaybına neden olarak, kendisi veya bir başkası için haksız bir menfaat sağlamak niyetiyle,

a) bilgisayar verilerini girme, silme veya engelleme,
b) bilgisayar sistemlerinin işleyişine müdahale etme,

[252] A.g.e., s.296-297.
[253] A.g.e., s.297.

Eylemlerini suç saymak için kendi ulusal mevzuatı kapsamında gerekli yasama tedbirleri ve diğer tedbirleri kabul edecektir."

Bu düzenleme ile dolandırıcılık, kredi ve banka kartlarının kötüye kullanılması gibi ekonomik suçlarla mücadele kapsamında malvarlığının yasadışı transferini sağlamak için verilerin işlenmesi sürecine yönelik manipülasyonların cezalandırılması amaçlanmıştır.[254]Bu suç mal varlığına karşı işlenen suçlar kapsamında değerlendirilmesi gerektiğinden korunmak istenen yarar öncelikle mal varlığıdır.

Bu suç, serbest hareketli bir suç olup, suçun oluşumu için maddede sayılan hareketlerden birinin gerçekleştirilmesi gerekmektedir. Suçun gerçekleşmesi için gerekli bir diğer unsur ise fail ya da 3. bir kişi lehine ekonomik bir değeri bulunan somut veya soyut bir mal varlığı kaybıdır.[255] Bu suçun, diğer suçlarda olduğu gibi kasten ve hakka dayanmaksızın haksız bir şekilde gerçekleştirilmesi gerekmektedir.[256]

Mevzuatımız açısından Sözleşme ile düzenlenen bu suçun farklı görünümleri vardır. Bu suç, TCK'da bilişim sistemlerinin kullanılması suretiyle hırsızlık (madde 142/2-e), bilişim sistemlerinin kullanılması suretiyle dolandırıcılık (madde 158/1-f) veya banka ve kredi kartlarının kullanılması (madde 245) şeklinde işlenebileceği gibi, bu suçların kapsamına girmemekle birlikte bilişim sistem ve verilerine yönelik eylemler sonucunda herhangi bir şekilde menfaat elde edilmesi halinde sistemi engelleme, bozma verileri yok etme veya değiştime suçu (244/4) ile de işlenebilecektir.

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun can alıcı noktasını, verinin hırsızlık suçunun konusu olup olamayacağı hususu oluşturmaktadır. Bu husus uygulamada ve öğretide tartışılmış olup, genel çoğunluğun veriyi bu suçun konusu olarak kabul ettiği söylenebilir. Yargıtay kararları da özellikle Ceza Genel Kurulu'nun 17.11.2009 tarihli kararından sonra

[254] Explanatory Report, 86.
[255] Explanatory Report, 88.
[256] Explanatory Report, 89.

bu yönde gelişmiştir. [257] Hırsızlık suçunun bir konusu olarak veri, temsil ettiği para niteliği ile taşınır bir maldır.[258]Bu kapsamda Yargıtay tarafından, trojan programları vasıtası ile ele geçirilen başkalarına ait hesap numaraları ve şifreler kullanılarak hesaplardaki paraların failin kendisine veya başkasına ait banka hesabına havale edilmesi;[259] sanığın, mağdurun banka hesabına girerek internet bankacılığı yoluyla para transfer etmesi;[260]sanığın katılanın banka hesabına internet bankacılığı yoluyla girip banka hesabındaki 2960 TL parayı onun bilgisi ve onayı dışında kendi hesabına havale ederek haksız menfaat elde etmesi[261] olayları bilişim sistemlerinin kullanılması suretiyle hırsızlık olarak değerlendirilmiştir.

Dolandırıcılık suçu yönünden ise, madde gerekçesine göre, eylemin bilişim sistemlerinin sağladığı kolaylıktan yararlanarak hileli davranışlarla bir kimsenin aldatılması ve onun veya başkasının zararına olarak kişinin kendisine veya başkasına yarar sağlaması ile gerçekleşmesi gerekmektedir.[262]Bu suçun işlenebilmesi için hile, aldatıcı bir nitelik taşımalıdır.[263]Yargıtay Ceza Genel Kurulu'nda bu suçun ancak bilişim sisteminin araç olarak kullanılması ile insanın, bilişim sisteminin değil, aldatılması sonucu gerçekleşeceği, kişilerin aldatılmadan sadece sistemden yararlanılması sonucu çıkar sağlanması durumunda bilişim suçu ya da bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun oluşacağı belirtilmiştir.[264]Bu karara konu somut olayda, bir internet sitesi üzerinden bilgisayar satış ilanı veren sanıklar, şikâyetçinin satın almak istediği bilgisayarların parasını ödemesine rağmen bilgisayarları göndermemişlerdir.

Yine Yargıtay tarafından, sanığın şikâyetçilere ait msn adreslerini kırarak ilgili adreslerdeki kişilerin arkadaşlarından onlarmış gibi yazışarak kendine yarar

---

[257] CGK, 2009/11-193 E – 2009/268 K, 17.11.2009.
[258] Öğretiden bu yönde görüşler, Karagülmez s.243; Dülger, s.580. Aksi görüş, Erdoğan, s.289-290.; Sedat Bakıcı, Gürsel Yalvaç, 6237 Sayılı Yasa Kapsamında Ceza Hukuku Özel Hükümleri, Adalet Yayınevi, Ankara 2008, , 2. Cilt, s.119.
[259] 6. CD. 2011/214 E – 2013/23327 K, 18.11.2013
[260] 8.CD. 2014/30866 E – 2014/32245 K, 23.12.2014
[261] 11. CD. 2012/27951 E – 2014/11829 K, 16.06.2014
[262] Özgenç, s873
[263] Ali Parlar, Muzaffer Hatipoğlu, 5237 Sayılı Türk Ceza Kanunu Yorumu, 2. Cilt, Ankara, 2007, Yayın Matbaacılık ve Tic. İşletmesi, s.1236
[264] CGK. 2012/15-1293 E – 2013/111 K, 02.04.2013

sağlamak amacı ile kontör talep edip şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına kontör yüklemesi,[265] bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık olarak kabul edilmiştir.

Sözleşme'nin 8. maddesine karşılık gelecek diğer bir suç tipi ise TCK'nın 245. maddesinde düzenlenen banka veya kredi kartlarının kullanılması suçudur. Bu maddenin birinci fıkrasında başkasına ait bir banka veya kredi kartı ile yarar sağlama suçu; ikinci fıkrada sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçu; üçüncü fıkrada ise sahte banka veya kredi kartıyla yarar sağlama suçu düzenlenmiştir. Bu suç tipi TCK'nın "bilişim alanında suçlar" bölümünde düzenlenmiştir.

Bu suçların "malvarlığına karşı suçlar" bölümünde değil de, "bilişim alanında suçlar" bölümünde düzenlenmesi suçun konusu olan banka ve kredi kartı veya 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 3/e maddesi uyarınca basılı kart olmaksızın fiziki varlığı bulunmayan kart numarasının bilişim sisteminin birer parçası olması ile açıklanabilir. Yargıtay kararlarına yansıdığı üzere, banka ve kredi kartlarının sıklıkla kullanıldığı ATM'ler bilişim sisteminin bir parçası olarak kabul edilmiştir.[266]

Banka veya kredi kartları fiziki olarak bir ATM üzerinden hukuka aykırı bir şekilde kullanılabileceği gibi, fiziki varlığı bulunmayan hesap numarası ile internet gibi ağlar üzerinden de kullanılmaktadır. Her iki durumda da bilişim sistemleri araç olarak kullanılmakta, eylem suçun konusu olan banka veya kredi kartının varlığı ile özel bir suç tipi haline gelmektedir. Örneğin, Yargıtay, katılanın rızası olmaksızın ele geçirdiği kredi kartı bilgilerini internet üzerinden mail order yöntemiyle kullanan sanığın eyleminin bir bütün olarak TCK.nun 245/1. maddesinde düzenlenen banka veya kredi kartlarının kullanılması suçunu oluşturduğu gözetilmeden, TCK.nun 142/2-e maddesinde düzenlenen ve olayda unsurları

[265] 8. CD. 2013/735 E – 2013/29491 K, 18.12.2013
[266] 11. CD. 2012/1223 E – 2013/8738 K, 28.05.2013

bulunmayan bilişim suretiyle hırsızlık suçundan mahkumiyet verilmesine dair yerel mahkemece verilen kararı bozmuştur. [267]

Sözleşme'nin bilgisayar bağlantılı dolandırıcılık suçuna ilişkin mevzuatımızda yer alan diğer bir önemli düzenleme ise TCK'nın 244. maddesinin 4. fıkrası hükmüdür. Bu hükme göre, aynı maddenin birinci fıkrasında yer alan bilişim sisteminin işleyişine veya maddenin ikinci fıkrasında yer alan bilişim sistemindeki verilere müdahale eylemlerinin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması suç olarak kabul edilmiştir. Ancak bu suçun oluşumu için haksız çıkar elde edilmesi ile sonuçlanan müdahale eyleminin başka bir suç oluşturmaması gerekmektedir. Bu nedenle bu suç tali ve tamamlayıcı niteliktedir. Örneğin, Yargıtay tarafından, Tarım Bakanlığının bilgisayar sistemine girerek gerçeğe aykırı veri yerleştirilmesi ve bunun sonucunda menfaat elde edilmesi şeklindeki eylem bu suç kapsamında değerlendirilmiştir.[268]Görüldüğü gibi faile ait sistemde yer alan verilere müdahale ile haksız çıkar elde etme eylemi bu suç kapsamında görülmekte, ancak bu eylem parayı temsil eden bir veri transferi şeklinde gerçekleşmediği için hırsızlık, kişilere yönelmiş bir hileli hareket olmadığı için dolandırıcılık veya suçun konusunu banka veya kredi kartı oluşturmadığı için banka veya kredi kartlarının kötüye kullanılması bu suç kapsamında kabul edilmemektedir.

Sonuç olarak, bilgisayar bağlantılı dolandırıcılık suçunun veya daha doğru ve anlaşılabilir bir çeviri ile bilgisayar bağlantılı haksız çıkar sağlama suçunun karşılığı mevzuatımızda bulunmakta ve her somut olaya uygun farklı suç tipleri ile karşımıza çıkmaktadır.

[267] 8. CD. 2014/1303 E – 2014/17644 K, 07.07.2014
[268] 8. CD. 2013/1607 E – 2013/14323 K, 03.10.2013

9. Çocuk Pornografisiyle Bağlantılı Suçlar (SSS madde 9)

"1- Her bir taraf devlet, aşağıdaki eylemlerin, kasten ve haksız bir şekilde işlenmesini kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirleri ve diğer tedbirleri kabul edecektir:

a. Bir bilgisayar sistemi aracılığı ile dağıtmak amacıyla çocuk pornografisi üretmek,
b. Bir bilgisayar sistemi aracılığı ile çocuk pornografisi sunmak ya da çocuk pornografisine erişim sağlamak,
c. Bir bilgisayar sistemi aracılığı ile çocuk pornografisi dağıtmak ya da yaymak,
d. Bir bilgisayar sistemi aracılığı ile kendisi ya da bir başkası için çocuk pornografisi temin etmek,
e. Bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak.

2- Yukarıdaki paragraf 1'de geçen "çocuk pornografisi" terimi aşağıdakileri görsel anlamda teşhir eden pornografik malzemeleri içermektedir:

a. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı,
b. Cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı,
c. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren gerçekçi görüntüler.

3- Yukarıdaki paragraf 1'de geçen "reşit olmayan kişi" terimi, 18 yaşından küçük kişileri kapsar. Ancak, bir taraf, 16'dan az olmayacak daha düşük bir yaş sınırı belirleyebilir.

4-Taraflardan her biri, paragraf 1(d) ve 1(e), ayrıca 2(b) ve 2(c)'yi kısmen uygulama ya da hiç uygulamama haklarını saklı tutar."

Bu düzenleme ile çocuklara karşı işlenen cinsel suçlarda bilgisayar sistemlerinin kullanılmasını sınırlandırmak için ceza yasalarını daha modern hale getirerek çocukların korunmasına yönelik koruyucu tedbirlerin güçlendirilmesi amaçlanmıştır.[269]Getirilen bu hükümlerle korunan hukuksal yarar, çocuk ve çocuğun fiziksel, zihinsel, duygusal ve sosyal gelişimidir.

Sözleşme'de, çocuk tanımında 18 yaş sınır olarak kabul edilerek, bu yaşın altındakiler reşit olmayan küçük olarak sayılmışlardır. Öngörülen yaş, çocukların gerçek ya da sanal anlamda cinsel bir nesne olarak kullanılması ile ilgili olup, cinsellik için izin verilen bir dönem başlangıcı değildir.[270]

Çocuk pornosu, madde metninde, gerçekten küçüklerin, küçük görünenlerin ya da küçüğü temsil eden tamamen bilgisayarda üretilmiş resimler gibi gerçekçi görüntülerin cinsel anlamda müstehcenlik içeren bir hal üzere görülebilir olması şeklinde tanımlanmıştır. Çocuk pornosu görselleştirerek izleme imkânı sunan bu malzemelerin elektronik olarak üretilmesi, arz edilmesi, erişilebilir kılınması, dağıtılması, yayılması, temin edilmesi ve bulundurulması suç olarak kabul edilmiştir. Çocuk pornosunun bir bilgisayar sisteminde veya veri depolamaya yarar bir cihazda saklanmasının bir önemi yoktur. Her iki durumda da suç işlenmiş sayılır.

Madde metninde geçen pornografik malzeme terimi ile açık saçık, genel ahlaka aykırı ve ahlak dışı durum;[271] cinsel anlamda müstehcen eylem terimi ile gerçek ya da simülasyon olup olmadığına bakılmaksızın, en az bir tarafı küçük olmak üzere her türlü cinsel ilişki, hayvanlarla cinsel ilişki, mastürbasyon, cinsel anlamda sadistik veya mazoştik kötü muamele, küçüklerin cinsel organ veya bölgelerinin teşhiri[272] kast edilmiştir.

Bu suç serbest hareketli bir suçtur. Madde metninde birinci fıkrada geçen eylemlerden birinin gerçekleşmesi suçun oluşumu için yeterlidir. Suç kasten işlenmelidir ancak cezai sorumluluk için taraf devlet ayrıca içerisinde çocuk

[269] Explanatory Report, 91.
[270] Explanatory Report, 104.
[271] Explanatory Report, 99.
[272] Explanatory Report, 100.

pornosu olan veri üzerinde bilgi ve kontrol gibi daha özel bir ölçü de getirebilir.[273] Diğer suçlarda olduğu gibi bu suç da yine haksız bir şekilde işlenmelidir. Olayın faili eylemini sanatsal, tıbbi, bilimsel bir çalışma kapsamında gerçekleştirdiğini bir savunma olarak ileri sürebileceği gibi düşünce veya ifade özgürlüğü gibi bir hakka dayanarak gerçekleştirdiğini de iddia edebilir.[274] Elbette bu savunmaları geçerliliği somut olaya göre değişecektir.

Mevzuatımızda bilişim sistemleri üzerinden gerçekleştirilen çocuk pornografisi adı altında özel bir düzenleme bulunmamaktadır. Sözleşme'nin 9. maddesi kapsamında çocuklara karşı gerçekleştirilen onların cinsel anlamda sömürülmesine yol açan eylemler "müstehcenlik" başlığı altında TCK'nın 226. maddesinin 3. fıkrasında ele alınmıştır.

Bu fıkrada, müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanmak suçu ile bu ürünleri ülkeye sokmak, çoğaltmak, satışa arz etmek, satmak, nakletmek, depolamak, ihraç etmek, bulundurmak veya başkalarının kullanımına sunmak suçu şeklinde iki ayrı suça yer verilmiştir.

TCK'nın, Sözleşme'ye kıyasla, sadece bilişim sistemleri üzerinden gerçekleştirilen çocuk pornografisi eylemlerini düzenlemediği, daha geniş bir yaklaşım sergilediği görülmektedir. Ancak bu durum Sözleşme'nin daha dar bir düzenleme getirdiği anlamına gelmemektedir. Çünkü Sözleşme, zaten geleneksel olarak var olan çocuk pornografisi kapsamındaki suçlara ek olarak gelişen teknolojilerle ağlar üzerinden işlenen çocuk pornografisi ile mücadele etmek istemektedir. Yani Sözleşme esasen siber dünyada var olan bir boşluğu doldurmaya çalışmaktadır. Bununla beraber Sözleşme'nin görsel içerikli pornografik malzemelere odaklandığı işitsel malzemeleri göz ardı ettiği düşünüldüğünde, TCK'nın çocuk pornografisi ile mücadelede bu açıdan bir adım önde olduğu söylenebilir.

Mevzuatımız açısından ise, sanal çocuk pornografisine açıkça yer verilmemesi ciddi bir eksikliktir. Acaba elektronik ortamda kurgulanmış bir şekilde sanal bir çocuğun sanal bir yetişkin ile cinsel ilişkiye girdiği bir videonun

[273] Explanatory Report, 105.
[274] Explanatory Report, 103.

bilgisayara indirilerek depolanması suç sayılabilecek midir? TCK'nın 226. maddesinin gerekçesine müstehcenlik, toplumda egemen olan değer ölçüleri ve hayâsızca hareketler kavramı dikkate alınarak belirlenecektir. Aynı yasanın 225. maddesinin gerekçesinde hayâsızca hareketler, genel edep ve iffete saldırı niteliği taşıyan davranışlar olarak tanımlanmıştır. Bu durumda verilen örnekte yer alan içerik Türk toplumuna egemen olan değer ölçülerine aykırı ve hayâsız hareketler niteliğindedir. Gerekçeden hareketle failin böyle bir içeriği indirmesi suç olarak kabul edilebilir. Bu şekilde ahlaki bir yaklaşım ile eylem bu madde kapsamına sokulabilecektir.[275] Ancak böylesi bir kabulün de TCK'nın 2. maddesinde düzenlenen "suçta ve cezada kanunilik ve belirlilik ilkesi" açısından da eleştirileceği kesindir. Çünkü sanal çocuk pornografisi eylemi açıkça bir suç olarak gösterilmemiş, suç tanımı açık ve seçik yapılmamıştır.

Henüz sanal çocuk pornografisi hakkında Yargıtay tarafından bir karar verilmemiştir. Öğretide, müstehcenlik suçlarında, gerçek bir durum ile izleyicide böyle bir izlenim yaratılması arasında fark görülmemiştir.[276] Ancak ülkemizde yakında bu konuda tartışmaların başlayacağı beklenilmelidir. İstenilen şekilde görünmeyi sağlayan "Second Life" gibi oyun sitelerinde çocuk gibi giyinmiş avatarlar ile cinsel ilişki teklifinde bulunulabilmekte, hatta Almanya'da böyle bir soruşturma yürütüldüğü bilinmektedir.[277]

TCK'nın müstehcenliğe ilişkin maddesinde küçük görünümlü yetişkinler üzerinden yapılan çocuk pornografisine de sanal çocuk pornografisi gibi açıkça yer verilmemiştir.

Hem Sözleşme hem de ceza mevzuatımızda çocuk pornografisine depolamaksızın sadece erişim gerçekleştirilmesinin suç olarak düzenlenmemesi ise ortak bir eksikliktir.

Sonuç olarak, Sözleşme'de düzenlenen çocuk pornografisine ilişkin suçlar genel olarak mevzuatımız tarafından karşılanmıştır. Sanal çocuk pornografisi ve

---

[275] Aydın Murat Burak, "Kurgu Eserler, Çocuk Pornografisi ve Cezalandırma", (çevrimiçi) s.7 http://www.umut.org.tr/Upload/Document/document_844745e77a5947ecae017baadf884c65.pdf , 29.04.2015.

[276] Veli Özer Özbek, Müstehcenlik Suçu, Seçkin Yayınevi, Ankara, 2009, s.123.

[277] Sylvia Kierkegaard, Ankara Barosu Uluslararası Hukuk Kurultayı, Bilişim ve Hukuk, Ankara Barosu Yayınları, Ankara 2009, s.331.

küçük görünümlü kişinin bu suça konu edilmesi eylemleri ise, suçla korunan hukuksal yarar, maddenin yorumu ve Anayasa'nın 90/son maddesi birlikte değerlendirildiğinde cezasız kalmayacaktır.[278] Artık ülkemizce onaylanmış bulunan ve iç hukukumuzun bir parçası olan Sözleşme'nin 9. maddesi de bunu gerektirmektedir.

10. Telif Hakkı ve Bununla Bağlantılı Hakların İhlaline İlişkin Suçlar (SSS madde 10)

"1-Her bir taraf devlet ulusal mevzuatında tanımlandığı şekliyle Edebi ve Sanatsal Eserlerin Korunmasına ilişkin Bern Anlaşması'nı yeniden ele alan 24 Temmuz 1971 Paris Sözleşmesi, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Telif Hakları Sözleşmesi kapsamında üstlendiği yükümlülüklere bağlı olarak, bu gibi sözleşmelerce tanınan her türlü ahlaki hak hariç olmak üzere, ticari ölçekte ve bilgisayar sistemleri aracılığıyla kasıtlı olarak telif haklarının ihlalinin cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirleri ve diğer tedbirleri kabul edecektir.

2- Her bir taraf devlet ulusal mevzuatında tanımlandığı şekliyle İcracı Sanatçıların, Fonogram Yapımcılarının ve yayım Kuruluşlarının Korunması Hakkında Sözleşme (Roma Sözleşmesi), Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ve WIPO Sanat İcrası ve Fonogramlar Sözleşmesi kapsamında üstlendiği yükümlülüklere bağlı olarak, bu gibi sözleşmelerce tanınan her türlü ahlaki hak hariç olmak üzere, ticari ölçekte ve bilgisayar sistemleri aracılığıyla kasıtlı olarak telif haklarına benzer hakların ihlalinin cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirleri ve diğer tedbirleri kabul edecektir.

3-Taraf devlet, başkaca etkili yasal yolların bulunması ve konulacak çekincenin bu maddenin 1. ve 2. paragrafında geçen uluslararası yükümlülüklerine

[278] Yaşar – Gökcan - Artuç, 5.Cilt, s.6762.

zarar vermemesi şartıyla sınırlı olarak bu maddenin 1. ve 2. paragraflarında belirtilen eylemlere cezai sorumluluk yüklememe hakkını saklı tutabilir."

Dijital teknolojiler ve elektronik ağlar üzerinden eseri kopyalama ve yayma imkânları, telif hakları ihlallerinin çok kolay bir şekilde gerçekleştirilmesine neden olması ve edebi, fotografik, müzikal, işitsel ve görsel eserlerin korumasız kalması ile telif hakları ve benzeri hakların ihlali suç olarak düzenlenmiştir.[279] Korunan hukuksal yarar, kişilerin, daha özelinde hak sahiplerinin mal varlığıdır.

Ulusal mevzuatlarca zaten geleneksel olarak telif hakkı ve benzeri hakların ihlallerinin suç sayılmasına ek olarak, bu düzenlemede farklı bir suç tipi öngörülmüş ve suça konu eylem, bilgisayar sistemleri aracılığı ile ve ticari maksatla gerçekleştirilmesi şartına bağlanmıştır.[280]Madde metninde diğer maddelerden farklı olarak "haksız şekilde" ifadesine yer verilmemiştir. Çünkü metinde geçen "ihlal" ifadesi, "haksız şekilde" ifadesi belirtilen durumu karşılamaktadır.[281]Yine maddede diğer maddelerden farklı olarak kasten anlamında kullanılan "intentionally" yerine "wilfully" ifadesine yer verilerek Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme ile terim birliği sağlanmıştır.[282]

Sözleşme, taraf devletlerce cezai sorumluluk yerine Fikri Mülkiyet Hukuku'na ilişkin olarak madde metninde belirtilen uluslararası sözleşmelere aykırı olmamak şartıyla ve paralel ithalat ve kiralama hakları gibi bazı konularla sınırlı olarak medeni ve idari bazı tedbirlerin uygulanabilmesine olanak sağlamıştır.[283]

Mevzuatımızda telif haklar ve benzeri haklar 5846 sayılı Fikri ve Sanat Eserleri Kanunu ile korunmuştur. Bu yasanın 1. maddesine göre yapılan düzenleme ile "fikir ve sanat eserlerini meydana getiren eser sahipleri ile bu eserleri icra eden veya yorumlayan icracı sanatçıların, seslerin ilk tespitini yapan fonogram yapımcıları ile filmlerin ilk tespitini gerçekleştiren yapımcıların ve radyo-

[279] Explanatory Report, 107.
[280] Explanatory Report, 108.
[281] Explanatory Report, 115.
[282] Explanatory Report, 113.
[283] Explanatory Report, 117.

televizyon kuruluşlarının ürünleri üzerindeki manevi ve mali haklarını belirlemek, korumak, bu ürünlerden yararlanma şartlarını düzenlemek, öngörülen esas ve usullere aykırı yararlanma halinde yaptırımları tespit etmek" amaçlanmıştır.

Sözleşme ile bilgisayar sistemleri aracılığı ile telif hakları ve benzeri haklara yönelik ihlaller suç olarak düzenlenirken 5846 sayılı Yasa'da eylemin bilişim sistemleri ile gerçekleştirilip gerçekleştirilmemesinin suç oluşumuna bir etkisi yoktur. Suçun işlenmesi için 5846 sayılı Yasa'nın "manevi, mali veya bağlantılı haklara tecavüz" suçunu düzenleyen 71. maddesi ve koruyucu programları etkisiz kılmaya yönelik suçu düzenleyen 72. maddesinde yer alan seçimlik hareketlerin gerçekleştirilmesi yeterlidir. Bu nedenle bilişim sistemleri aracılığı ile gerçekleştirilen telif hakları ve benzeri hak ihlalleri de Sözleşme'nin aradığı anlamda mevzuatımız açısından suçtur. Nitekim Yargıtay tarafından bu yönde kararlar verilmiştir.

Sanığın sahibi olduğu … Cafe isimli işyerinde kurulu bulunan 22 adet bilgisayardan birinde Windows XP Professional işletim sistemi ile Microsoft Ofis Professional Editör 2003 programının lisanssız şekilde yüklü olması,[284] müştekiler vekilinin, müvekkillerinin mali hak sahibi olduğu "10 parmak" isimli bilgisayar programının, 29.04.2004 tarihinden itibaren şüphelinin sorumlusu olduğu www. tamindir.com" adlı internet sitesinde bulunduğu ve kullanıcılar tarafından, hak sahibi müşteki şirketlerin izni olmadan 93802 kez indirilmek suretiyle yayılması[285] Yargıtay tarafından telif hakkı ihlali olarak görülmüştür. Yargıtay, bir başka kararında, suça sürüklenen çocuğun kullandığı bilgisayarda müzik eserleri depolamasına ve bu müzik eserlerini rapidshare com isimli internet sitesinde yüklemesine rağmen eylemin kişisel kullanım dışında ticari amaçla depoladığına, bulundurduğuna ve paylaştığına dair delil ortaya konmadığı için yerel mahkeme tarafından verilen mahkûmiyet kararını bozmuştur.[286]

[284] 7. CD. 2013/13518 E – 2014/21259 K, 15.12.2014
[285] 7. CD. 2008/8702 E – 2011/17095 K, 11.10.2011
[286] 7. CD. 2013/2833 E – 2013/22163 K, 12.11.2013

Sonuç olarak, her ne kadar bilgisayar sistemleri aracılığıyla gerçekleştirilen hak ihlalleri için mevzuatımızda özel bir düzenleme bulunmasa da, yukarıda gösterilen mevcut hükümlerin bilgisayar sistemleri aracılığıyla gerçekleştirilen suçları da kapsaması nedeniyle mevzuatımızın Sözleşme'nin 10. maddesi ile uyum içerisinde olduğu düşünülmektedir.

D. Ceza Usul Hukuku Açısından Karşılaştırmalı Bakış

1. Giriş

Siber suçlarla mücadele de bu suçların tanımlamasını yapmak ve bu çerçevede yasal unsurlarını belirlemek kadar maddi gerçeğin ortaya çıkarılması için başvurulacak koruma tedbirlerinin belirlenmesi de önemlidir. Suçluların tespiti, işlenen suçun etki ve sonuçlarının değerlendirilmesi, elde edilen delillerin hassasiyeti ve bütün bunlarla birlikte siber suçlarda zamanla yarış etkin bir soruşturma için çok önemlidir.[287] Özellikle konumuz açısından gelişen teknolojilerin ortaya çıkardığı yeni suç tipleri ve geleneksel suçların bilişim sistemleri aracılığı daha farklı bir şekilde işlenmesi yeni bazı usuli tedbirlerin varlığını zorunlu kılmıştır.

Sözleşme'nin 14 ila 22. maddeleri ceza usul hukukuna ilişkindir. Bu hükümlerde başvurulacak koruma tedbirlerinden önce usul hükümlerinin kapsamına yer verilmiş, daha sonra taraf devletlerce usul hükümlerine dair yapılacak yasama faaliyetlerinde ve çıkarılacak yasaların uygulanmasında uluslararası mevzuatın ve temel hak ve özgürlüklerin referans alınması gerektiği belirtilmiştir.

Sözleşme'nin 14. maddesinde düzenlenecek usuli hükümlerin çerçevesi çizilmiştir. Buna göre, çerçeveyi; Sözleşme'nin 2 ila 11. maddelerinde tanımlanan suçlar (11. maddede düzenlenen teşebbüs ve iştirake ilişkin ceza genel hükümleri dahil), bilgisayar sistemleri aracılığı ile işlenen diğer suçlar ve işlenen herhangi bir suçun elektronik biçimdeki delillerinin toplanması oluşturmaktadır. Görüldüğü üzere, Sözleşme, usule ilişkin konularda sadece Sözleşme'de düzenlenen suçlarla sınırlı kalmamış ve etki alanını bilgisayar sistemleri ile işlenen suçlara ya da

[287] Explanatory Report, 133.

elektronik delilin toplanabileceği herhangi bir suça kadar genişletmiştir. Böylece aynı zamanda, mahkemeler önünde elektronik delilin, geleneksel delilden geçerlilik anlamında farkı olmadığına işaret edilmiştir.[288]Genel çerçeve bu olmasına rağmen Sözleşme'nin 21. maddesinde düzenlenen "içerik verisine müdahale" tedbirinin belli ağırlıkta olan bazı suçlar dışındaki suçlara uygulanması engellenerek istisnai bir durum oluşturulmuştur.[289]Bir diğer istisna ise Sözleşme'nin 20. maddesinde düzenlenen "gerçek zamanlı olarak trafik verisine müdahale" tedbiridir. Taraf devletler, bu tedbirin uygulanabilmesi için "içerik verisine müdahale" tedbirinde olduğu gibi katalog suçlardan birinin varlığı şartını bir çekince olarak ileri sürebilir.[290]Özel hayatın gizliliği ve korunmasına ilişkin bu iki istisnai durum dışında Sözleşme'de yer alan tedbirler 14. maddede sayılan suçlar kapsamına girecektir.

Sözleşme'nin 15. maddesinde ise siber suçlarla mücadele ederken orantılılık ilkesince insan hak ve özgürlüklerinin korunması amaçlanmıştır. Bu düzenlemede güvenlik ile özgürlükler dengesinde herhangi bir tercih yapılmadığı, bu iki değerin birbirine feda edilmediği görülmektedir.

Sözleşme'nin usule ilişkin bu bölümünde altı ayrı tedbire yer verilmiştir. Bu tedbirlerin uygulanması sırasında muhataplarını zorlayıcı bir özelliğe sahip olması, maddi gerçeği bulma yolunda bir araç olması ve geçici nitelikte olması nedeniyle[291] birer koruma tedbiri olduğu anlaşılmaktadır. Keskin tarafından bu koruma tedbirleri, "bilişim koruma tedbirleri" olarak tarif edilmiştir.[292]Bu koruma tedbirleri nitelikleri gereği, Sözleşme'nin 14. maddesi kapsamındaki suçların soruşturulmasına esas olmak üzere verilerin saklanması ve tutulmasını getirmekte, ancak Sözleşme'de böyle bir yükümlülük üzerinde anlaşmaya varılamadığı için bu durumu düzenleyen açık bir emredici bir hüküm bulunmamaktadır.[293] Burada veri

[288] Explanatory Report, 141.
[289] Explanatory Report, 142.
[290] Explanatory Report, 143.
[291] Yener Ünver, Hakan Hakeri, Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara 2012, s.348-349.
[292] Serap Keskin, Avrupa Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İstanbul Üniversitesi Hukuku Fakültesi Mecmuası (İÜHFM) Cilt:LIX, Sayı 1-2, 2001, s.156.
[293] Explanatory Report, 135.

kavramı, özellikle trafik verilerini, içerik verilerini ve abone verilerini kapsamaktadır.[294]Ülkemizde, 5651 sayılı Yasa ile verilerin tutulmasına olanak sağlayan yasal zemin bulunmaktadır.

Bu bölümün son maddesinde ise yargı yetkisine ilişkin bir düzenlemeye yer verilmiştir.

2. Saklı Bilgisayar Verisinin Hızlı Korunması (SSS madde 16)

Sözleşme'nin usul hukukuna ilişkin düzenlediği ilk koruma tedbiri, saklı bilgisayar verilerinin hızlı korunmasıdır.

Bu düzenleme ile taraf devletlerden özellikle kaybolma ve değişme olasılığı bulunan bilgisayar sistemleri içerisinde saklanmış trafik verileri dâhil bilgisayar verilerinin korunmasını sağlaması istenmiştir. Taraf devlet, yetkili makamları aracılığı gerçek veya tüzel kişilere verileri korumaları yönünde talimat vermek suretiyle ya da yetkili makamları tarafından gerçek veya tüzel kişilerden verileri alıp korumak suretiyle bu tedbire başvuracaktır. Eğer taraf devlet birinci yolu seçerse talimata muhatap kalan bilgisayar verisini bulundurma veya üzerinde tasarruf etme yetkisine sahip gerçek veya tüzel kişi 90 günü aşmamak şartıyla gerektiği kadar veriyi koruma ve gerektiğinde veriyi açıklama yükümlülüğü altına girecektir. Veriyi koruma yükümlülüğü altında bulunan gerçek veya tüzel kişiler, yükümlülük süresi içerisinde ayrıca üstlendikleri yükümlülüğün gizliliğine de uyacaklardır.

Verilerin korunmasından maksat, saklanmış şekilde var olan verilerin değişmesini, silinmesini, kalitesini kaybetmesini önlemek için verinin içinde bulunduğu koşulların korunması, sağlam ve güvenlik içinde tutulmasıdır.[295]Tedbir geçmişe dönük olarak servis sağlayıcılar tarafından tutulan veriler üzerinde uygulanmakta olup, şimdi akmakta olan veya gelecekte ortaya çıkacak verileri kapsamamaktadır.[296]

---

[294] Explanatory Report, 136.
[295] Explanatory Report, 159.
[296] Explanatory Report, 149.

Kolaylıkla manipülasyona ve etkiye açık olan verilerin taşıdığı hassasiyet, bu koruma tedbirini çok önemli kılmaktadır. İşlenmiş olan suçların işlendiği sırada failler arasındaki iletişimin tespiti, bu iletişimin kaynağı ve varış noktasının yer aldığı bilgisayar verilerinin bir yerde birileri tarafından korunuyor olması faillerin yakalanmasını ve suçun ortaya çıkarılmasını kolaylaştıracaktır.[297]

Maddede korunması istenen bilgisayar verisi, saklı ya da depolanmış halde bulunan trafik, içerik ve abone verileridir.[298]Bu veriler ticari kayıtları, sağlık kayıtlarını, kişisel kayıtları ve diğer kayıtları kapsamaktadır.[299]

Yetkili makamlar doğrudan bilgisayar verisini koruma yolu yerine güvenilir olduğunu düşündüğü ve veri üzerinde tasarruf hakkı bulunan kişiye saklı bilgisayar verilerinin hızlı korunması talimatını verir. Böylece, örneğin verileri elinde tutan saygın bir şirket, iş yerinin ve bilgisayar sistemlerinin kolluk marifetiyle aranmasından ve elde edilecek suç unsurlarına el konulmasından kurtulur. Rutin faaliyetlerine devam eder. Bu durumda yed-i emin sıfatıyla kişi ya da kurum yürütülmekte olan soruşturmaya zarar vermemek için soruşturmanın gizliliğine uyar ve bilgisayar verilerini en fazla 90 güne kadar korur. Bu koruma, verinin talep edildiğinde açıklanmasını da kapsar.

Mevzuatımız açısından yukarıda açıklanan bu koruma tedbirinin doğrudan bir karşılığı yoktur. Ancak bu anlamda bir boşluğun olduğu da söylenemez. İnternet öznelerinin sorumluluğunun düzenlendiği 5651 sayılı Yasa, içerik sağlayıcılarını, Telekomünikasyon İletişim Başkanlığı'nın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmek ve Başkanlıkça bildirilen tedbirleri almakla; yer sağlayıcıları ve erişim sağlayıcılarını, sağladıkları hizmetlere ilişkin trafik bilgilerini saklamak ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü kılmıştır.

Aynı yasaya göre, içerik sağlayıcı, internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel

[297] Explanatory Report, 155.
[298] Explanatory Report, 136.
[299] Explanatory Report, 161.

kişileri; yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri; erişim sağlayıcı, kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri, trafik bilgisi ise, taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini ifade etmektedir.

Saklı bilgisayar verilerinin hızlı korunması tedbiri bakımından içerik sağlayıcılar, yer sağlayıcılar ve erişim sağlayıcılar, soruşturma kapsamında Anayasa Mahkemesi'nin 02.10.2014 tarihli 2014/149 E. ve 2014/151 K. sayılı kararı ile 5651 sayılı Yasanın 3. maddesinin 4. fıkrasını iptal edene kadar hâkim kararı ile Telekomünikasyon İletişim Başkanlığı aracılığı ile talep edilen bilgileri veriyorlardı. Bu iptal kararı ile Cumhuriyet başsavcılıkları hâkim kararı olmaksızın doğrudan içerik sağlayıcılar, yer sağlayıcılar ve erişim sağlayıcılardan trafik bilgilerini temin etmektedir. Ancak bu uygulamanın hatalı olduğu düşünülmektedir. Çünkü veriler iletişimin bir parçasıdır ve bu verilerin soruşturma makamları tarafından elde edilmesi CMK'nın 135/6 maddesinde telekomünikasyon yoluyla iletişimin tespitine uygulanan usule tabidir.[300] Bu nedenle verilerin sulh ceza hâkimlerince verilen karara istinaden hizmet sağlayıcılardan talep edilmesi gerekmektedir.

Sözleşme'de belirtilen bilgisayar verilerinin gerçek veya tüzel kişiler tarafından korunması için yetkili makamların talimat vermesi hükmünün de doğrudan bir karşılığı yoktur. Buna rağmen 5271 sayılı CMK'nın 132. maddesinin 5. fıkrası bu boşluğu belli bir oranda kapatmak için kullanılabilir. Bu düzenlemeye göre, elkonulan eşya, soruşturma evresinde Cumhuriyet Başsavcılığı, kovuşturma evresinde mahkeme tarafından, bakım ve gözetimiyle ilgili tedbirleri almak ve istendiğinde derhâl iade edilmek koşuluyla, muhafaza edilmek üzere, şüpheliye, sanığa veya diğer bir kişiye teslim edilebilir. Yani usulüne uygun olarak elkonulan bilgisayar verileri, veriyi bulundurma ve üzerinde tasarruf yetkisi bulunan herhangi bir kişi ya da kuruma muhafaza edilmek üzere bırakılabilir. Kendisine bilgisayar verisi korunmak üzere bırakılan kişi ya da kurum, teslim amacı dışında veri

[300] Bu konu ileride Sözleşme'nin 20. maddesi açıklanırken detaylı olarak ele alınacaktır.

üzerinde tasarrufta bulunursa 5237 sayılı TCK'nın "muhafaza görevini kötüye kullanma" suçunun düzenlendiği 289. maddesi uyarınca cezalandırılır.

Burada üzerinde durulması gereken bir diğer nokta ise Sözleşme'nin 16. maddesine konu bilgisayar verilerinin kapsamının genişliğidir. Gerçekten kapsamı bu kadar geniş olan bilgisayar verilerinin hizmet sağlayıcılar tarafından tutulmasını beklemek hizmet sağlayıcı açısından masraflı ve sorumluluk açısından riskli, hizmet kullanıcısı açısından ise özel hayatın gizliliği bağlamında tehlikelidir. Mevzuatımızda erişim sağlayıcılar ve yer sağlayıcılar açısından kapsam trafik bilgileri ile sınırlı olsa da, içerik sağlayıcılar açısından kapsam Sözleşme'nin beklentisi kadar geniştir.

3. Trafik Verilerinin Kısmen Açıklanması ve Hızlı Korunması (SSS madde 17)

Bu düzenlemeyi yukarıda incelediğimiz saklı bilgisayar verilerinin hızlı korunması maddesi ile birlikte değerlendirmek gerekmektedir. Bilgisayar verisinin bir uzantısı olan trafik verilerinin korunması ile birlikte kısmen açıklanması düzenlenmiştir.

Bu madde ile taraf devletlerden trafik verisine konu iletişimin kaç tane hizmet sağlayıcısı üzerinden aktarıldığına bakılmaksızın hızlı bir şeklide trafik verilerinin korunması ve hizmet sağlayıcının ve iletişimin aktarıldığı yolun belirlenmesini sağlayacak yasal düzenlemeler istenmiştir.

Sözleşme'nin 16. maddesine paralel olarak, bu düzenleme de geçmişe dönük olarak işlenmiş bir suçun failini bulmak amacıyla bir iletişimin kaynağı ve varış noktasını gibi bilgileri gösterecek verilerle ilgilidir.[301]Anlık ve geleceğe yönelik veriler bu maddenin kapsamı dışındadır.

Trafik verileri bir veya birden fazla hizmet sağlayıcı tarafından tutulmaktadır. Her bir hizmet sağlayıcı yetkili makamlardan gelecek talimat ile trafik verilerini hızlı bir şekilde koruyacak ve gerektiğinde yetkili makamlara trafik

[301] Explanatory Report, 166.

verilerini açıklayacaklarıdır. Böylece yetkili makamlar, suçun faillerini yakalamak için iletişim zincirinde geriye doğru gitme ve failin çıkış noktasını bulma ya da iletişim zincirinde ileriye doğru gitme ve failin varış noktasını bulma fırsatını elde edeceklerdir.[302]

Sözleşme'nin 17. maddesinin de, mevzuatımızda özel bir karşılığı yoktur. Sözleşme'nin 16. maddesinde yaptığımız açıklamalar bu madde için de geçerlidir. 5651 sayılı Yasa, internet özneleri olan yer sağlayıcıları ve erişim sağlayıcılarını trafik verilerini tutmakla yükümlü kılmıştır. Bir suça ilişkin delil niteliği taşıyan veriler hizmet sağlayıcılardan savcılık ve mahkemeler tarafından doğrudan talep edilmekte, gelen veriler üzerinden suçun faillerine ulaşılmaktadır. CMK'nın 161. maddesi uyarınca adli kolluk görevlileri karşılaştıkları olayı Cumhuriyet savcısına bildirmek ve onun yazılı emirleri, acele hallerde sözlü emirleri doğrultusunda hareket etmek zorunda oldukları için Cumhuriyet savcısının talimatı olmaksızın trafik verilerine ulaşamayacaklardır. Elde edilen veriler, çözümü yapılarak soruşturma dosyası içinde veya adliyelerde harici bellekler içerisinde adli emanette muhafaza edilmektedir.

4. Üretim Emri (SSS madde 18)

Sözleşme, 18. maddesinin (a) bendi ile yetkili makamların ulusal sınırları içerisinde bulunan bir kişiyi sahip olduğu ya da tasarrufu altında bulunan bilgisayar sistemleri içerisinde veya başkaca veri depolama cihazı içerisinde bulunan belli bir bilgisayar verisini teslime zorlamalarına olanak sağlamaktadır. (b) bendi ile de yetkili makamlara ulusal sınırları içerisinde bulunan bir hizmet sağlayıcıyı sahip olduğu ya da tasarrufu altında bulunan sunduğu hizmetle ilgili abonelik bilgilerini teslime zorlama yetkisi vermektedir.

Maddenin 3. fıkrasında da abonelik bilgileri açıklanmıştır. Buna göre, abonelik bilgileri, temel olarak hizmet kullanıcısına ait hizmet sağlayıcı tarafından tutulan her türlü bilgiyi ifade etmektedir. Abonelik bilgileri, bilgisayar verilerinden başka verileri de kapsadığı için diğer verilerin kapsam dışı kalmaması amacıyla

[302] Explanatory Report, 169.

ayrıca düzenlenmiştir.[303]Bu düzenleme ile kullanılan iletişim hizmetinin türü, teknik olanaklar, hizmet süresi, abonenin kimliği, adresi, telefonu numarası veya ulaşılabilecek diğer numaralar, fatura ve ödeme bilgileri, hizmet sözleşmesi ve iletişim donanımlarının kurulduğu yere ait diğer bilgilerin yetkili makamlara talimat üzerine teslimi zorunlu hale getirilmiştir.

Üretim emrine konu veri, Sözleşme'nin 16. ve 17. maddelerinde olduğu gibi saklanmış, depo edilmiş ya da var olan veriler olup, bu düzenleme ile ceza soruşturmaları için arama ve el koyma tedbirine göre daha az müdahaleci bir yöntem geliştirilmiştir. [304]Bu yöntem ile veriyi elinde bulunduran hizmet sağlayıcıları yetkili makamlara yasal bir zeminde veri sağlayarak abonelerine karşı kendilerini zora sokacak sorumluluktan da kurtulmaktadır.[305]Bilgisayar verisi veya abonelik bilgilerine sahip olmayan veya bu veri ve bilgiler üzerinde tasarruf yetkisi bulunmayan gerçek kişi ya da hizmet sağlayıcıları, üretim emrine uyma yükümlülüğünde değillerdir.[306]Diğer bir husus ise, üretim emrinin konusunun sadece suç şüphesi altında bulunan belli bir hizmet kullanıcısı olmasıdır. Veri madenciliğine yol açacak şekilde çoklu abone bilgilerinin teslimi yönünde üretim emri verilemez.[307]

Mevzuatımızda, üretim emrine karşılık gelen özel bir düzenleme yoktur. Hizmet sağlayıcıların, 5651 sayılı Yasa gereğince kendilerinden talep edilen verileri teslim yükümlülüğüne daha önce saklı verilerin hızlı korunması tedbirinde değinilmişti.

Gerçek kişiler açısından ise sorun genel hükümlerle çözülebilmektedir. Bir suç dolayısıyla yapılan bir soruşturmada, ispat aracı olarak görülen eşya, ilgili kişinin rızasının varlığı halinde CMK'nın 123/1 maddesi uyarınca muhafaza altına alınacaktır. Eşyayı yanında bulunduran kişinin rızası yoksa her türlü eşya hakkında aynı maddenin 2. fıkrası uyarınca elkoyma kararı verilecektir. Konumuz açısından bu eşyanın bilgisayar verisi olduğu düşünüldüğünde adli makamlardan gelen

[303] Explanatory Report, 177.
[304] Explanatory Report, 170.
[305] Explanatory Report, 171.
[306] Explanatory Report, 173.
[307] Explanatory Report, 182.

talimat üzerine delil niteliği bulunan bilgisayar verisi ilgilinin rızasıyla alınamazsa, bu veri hakkında CMK'nın 134. maddesine göre elkoyma kararı verilecektir. Usul Yasası, eşyanın bilgisayar verisi olması halinde genel arama ve elkoyma düzenlemesinden ayrılarak özel bir düzenleme yapmıştır. Bu düzenlemeye aykırı olarak elde edilen delil, CMK'nın 206/2(a) maddesi uyarınca reddolunacaktır. Görüldüğü üzere, Sözleşme'de üretim emri ile çözülen sorun mevzuatımızda arama, elkoyma ve muhafaza altına alma tedbirleri ile çözülmektedir.

5. Saklı Bilgisayar Verileri Üzerinde Arama ve Elkoyma (SSS madde 19)

Bu madde ile ceza usul yasalarında yürütülen soruşturma kapsamında delil elde etmek için somut nesneler üzerinde var olan arama ve elkoyma tedbirlerinin, depolanmış bilgisayar verilerini kapsamayacak şekilde genişletilmesi ve ulusal yasaların modernize edilmesi amaçlanmıştır.[308]

Sözleşme'nin 19. maddesinin 1. fıkrasında arama veya benzer şekilde erişme tedbiri düzenlenmiştir. Maddenin 1. fıkrasına göre, yetkili makamlar, bir 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. Maddenin 2. fıkrasına göre ise, 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.

Maddenin 3. fıkrasında el koyma veya benzer şekilde koruma altına alma tedbiri düzenlenmiştir. Bu fıkraya göre, yetkili makamlar, bir bilgisayar sisteminin tamamına veya bir kısmına, bilgisayar verilerini depolama cihazına elkoymaya veya 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 kılınacaklardır.

---

[308] Explanatory Report, 184.

Maddenin 4. fıkrasında arama ve elkoyma işlemleri sırasında alanında uzman bir kişiden yararlanma düzenlenmiştir.

Madde metninde kullanılan arama tabiri ile geleneksel anlamdaki bulmak için bakınma, okuma, araştırma, inceleme ile birlikte verinin aranması ve incelenmesi anlaşılmaktadır. Benzer şekilde erişme kavramı ise aramanın bilgisayar terminolojisindeki karşılığı olup, bu tabir ile geleneksellik ve modernlik aynı anda karşılanmak istenmiştir.[309] Elkoyma ifadesi de koruma altına alma ifadesi ile birlikte kullanılmıştır. Elkoyma tabiri ile veri veya bilgileri kaydedildiği fiziki varlığı bulunan cihazın alınması, veri veya bilgilerin bir kopyasının yapılması ve alınması ifade edilmiştir. Koruma altına almak tabiri ile de fiziki varlığı bulunmayan verilerin çıkarılması, erişilmez kılınması, tasarruf altına alınması, bütünlüğünün korunması, koruyuculuk zincirinin sürdürülmesi ifade edilmiştir.[310] Elkoyma veya koruma altına alma tedbirleri iki işlevin gerçekleşmesi hedeflenmiştir: verileri kopyalama gibi yollarla delil elde etmek ve verileri kopyalamak, verileri erişilmez kılmak veya verileri taşımak gibi yollarla müsadere etmek.

Maddenin 4. fıkrasında bilgisayar verilerine arama ve elkoyma tedbirlerinin uygulanması sırasında kolluk görevlilerinin işini kolaylaştıracak bir tedbir düzenlenmiştir. Buna göre arama ve elkoymaya konu bilgisayar sisteminin işleyişini bilen herhangi bir kimse aramanın nasıl daha iyi gerçekleştirilebileceği gibi konularda gerekli teknik bilgileri paylaşmaya zorlanabilecektir.[311]Sözleşme'nin açıklayıcı raporunda bilgi paylaşımına zorlanacak kişilere örnek olarak sistem yöneticisi verilmiş, bunun daha etkin ve daha az masrafla işlemlerin yürütülmesini sağlayacağı ve yöneticiyi de yükümlülük altına sokabilecek anlaşmalardan koruyacağı belirtilmiştir.[312]Başka bir ifadeyle sistem yöneticisi üzerinde olduğu yasal zemin nedeniyle kendisine karşı açılabilecek cezai ve hukuki davalardan korunmuş olacaktır.

---

[309] Explanatory Report, 191.
[310] Explanatory Report, 197.
[311] Explanatory Report, 200.
[312] Explanatory Report, 201.

İç hukukumuzda açısından Sözleşme'nin 19. maddesine paralel olarak düzenlendiği öne sürülebilecek akla gelen ilk hüküm, CMK'nın 134. maddesinde "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlığı ile yer almaktadır. CMK'nın genel nitelikteki arama ve elkoyma hükümleri ile yetinilmeyerek yasanın 134. maddesinde özel olarak bir düzenleme yapılmıştır.[313]Genel arama yöntemlerinden farklı olarak gecikmesinde sakınca bulunan hallerde dahi 134. maddeye göre arama ve elkoymaya tek yetkili merci hâkimdir.[314]Bu düzenlemeye göre, hâkim, suç dolayısıyla yapılan soruşturmada, somut delillere kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına bu kayıtların çözülerek metin hâline getirilmesine karar verir. Eğer hâkim tarafından verilen bu karar ile şifrenin çözülememesi veya gizlenmiş bilgilere ulaşılamaması durumunda bilgisayar ve bilgisayar programları ile bilgisayar kütükleri üzerinde elkoyma işlemi yapılır.

Görüldüğü üzere mevzuatımızda arama ve elkoyma kararı, Sözleşme'nin getirdiği ölçünün çok üstünde zorlaştırılmıştır. Sözleşme bu işlemler için bir yerde suça delil olabilecek bilgisayar verisinin bulunduğuna ilişkin nedenlerin inandırıcılığını aramaktadır. Ceza usul yasamız açısından bu eşik, genel arama için istenen suç delillerinin elde edilebileceği hususundaki makul şüphe ölçütüne denk gelmektedir. 134. madde somut delillere dayanan kuvvetli şüphe ve başka surette delil etme imkânının bulunmaması koşullarını birlikte arayarak kendi içinde çelişkiye düşmektedir. Kuvvetli şüpheye esas teşkil edecek somut delil varsa, zaten delil elde olduğu için bu tedbire başvurulamayacak ve Cumhuriyet savcısı bu tedbire başvurmadan CMK'nın 170/2 maddesine göre yeterli şüphe ile dava açacaktır. Arama ve elkoymaya karar verebilmek gerekli şüphe eşiği yukarı

---

[313] İsa Döner, Arama-Elkoyma, Dijital Verilere Elkoyma, Aihm Kararları Işığında Koruma Tedbirleri ve İfade Özgürlüğü Sempozyumu, HSYK Genel Sekreterlik Yayınları, Ankara 2013, s.42.

[314] Nurullah Kunter - Feridun Yenisey - Ayşe Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Arıkan Basım Yayım, İstanbul 2006, s.958.

çekildiği gibi bu kararların kimler üzerinde uygulanabileceği konusunda da kapsam daraltılmıştır. CMK, sadece bir soruşturma öznesi olan şüpheliye ait bilgisayar ve bilgisayar programları ile bilgisayar kütükleri üzerinde aramaya izin verirken, Sözleşme böyle bir ayrıma gitmemiştir.

Bir başka sorun ise Sözleşme'nin aksine 134. maddede üzerinde arama yapılabilecek içerisinde verilerin saklandığı bilgisayar dışında başkaca cihazlara yer verilmeyişidir.[315]Bir başka sorun ise, Sözleşme'de geleneksellik ile modernliğin bir araya getirilmeye çalışıldığı arama ile erişimin, elkoyma ile koruma altına alma ifadelerinin kullanılmayarak CMK tarafından Sözleşmeye göre dar bir yaklaşımın benimsenmesidir. Son olarak, bir bilgisayar sistemi üzerinden uzak bilgisayar üzerinde arama olanağının CMK'da sağlanmaması da bir eksikliktir. Her ne kadar buna benzer eksiklikler çıkarılan yönetmeliklerle doldurulmaya çalışılsa da kişilerin temel haklarına temas eden konularda idarenin tasarrufu doğru değildir.[316]

6. Trafik Verilerinin Gerçek Zamanlı Toplanması (SSS madde 20)

Bu düzenlemede, an itibariyle gerçekleşen iletişimin maddi bir varlığı bulunmayan ve delil niteliği bulunan,[317]bir iletişim zincirinin parçası olan ve iletişimin başlangıç noktasına, varış noktasına izlediği yola, saatine, tarihine, süresine ve iletişimin gerçekleştirildiği hizmetin türüne ilişkin trafik verilerinin[318] gerçek zamanlı toplanması[319] söz konusudur.

20. maddesinin 1. fıkrasına (a) bendine göre, yetkili makamlar, bir bilgisayar sistemi aracılığı ile üretilmiş belirli iletişimlerle ilişkili gerçek zamanlı trafik verilerini teknik imkânlarla toplamaya veya kaydetmeye yetkili kılınacaktır. (b) bendine göre ise, yetkili makamlar bir hizmet sağlayıcısı aracılığı ile ve hizmet sağlayıcısının teknik imkânları çerçevesinde belirli iletişimlerle ilişkili gerçek zamanlı trafik verilerini toplamaya veya kaydetmeye ve hizmet sağlayıcılarını bu

[315] Döner, s.85.
[316] A.g.e., s.101.
[317] Explanatory Report, 208.
[318] Explanatory Report, 209.
[319] Explanatory Report, 205.

konuda işbirliğine zorlayabileceklerdir. Maddenin (a) ve (b) bentlerinde belirtilen tedbirler birbirinin alternatifi olmayıp, ikisinin de taraf devlet tarafından sağlanması gerekmektedir.[320]Buna rağmen taraf devlet, ulusal hukuk sistemindeki yerleşik ilkeler nedeniyle paragraf (a)'da yer alan tedbire başvuramıyorsa, maddenin 2. fıkrasına göre, hizmet sağlayıcıları gerekli teknik desteği sağlamaya zorlayabilecektir. Örneğin, taraf devlet, sadece hizmet sağlayıcıların yardımı ile ya da sadece hizmet sağlayıcının bilgisi dâhilinde bu tedbire başvurabiliyorsa;[321] taraf devlet, hizmet sağlayıcıların teknik alt yapısını kullanarak bağımsız bir şekilde bu tedbiri uygulayacaktır. Bu aynı zamanda taraf devletin bu tedbirin uygulanmasında maddenin 3. fıkrasında getirilen soruşturmanın gizliliğini sağlama yükümlülüğüne de hizmet edecektir.

Sözleşme'nin açıklayıcı raporunda trafik verilerinin içinde yer aldığı belirli iletişimler geniş yorumlanmıştır. Bilgisayar sistemlerinin birbirlerine kablolu ya da kablosuz, optik ya da normal, uydu üzerinde ya da uydu olmaksızın gibi farklı yollarla bağlanma şekli, telekomünikasyon bilgi teknolojilerinin birbirine yaklaşması nedeniyle bir önem arz etmemektedir.[322]Bilgisayar sistemleri ile gerçekleştirilen bu iletişime imkân sağlayan kamusal ve özel kuruluşlar ise Sözleşme'de hizmet sağlayıcılar olarak adlandırılmıştır.[323]

Trafik verilerinin eş zamanlı olarak toplanması Sözleşme'de yer alan herhangi bir suç soruşturması kapsamında başvurulabilecek bir tedbirdir. Ancak taraf devlet tarafından bu tedbirin uygulanmasına belirli suçlarla bir sınırlama getirilecekse de belirlenecek katalog suçlar Sözleşme'nin içerik verilerinin gerçek zamanlı toplanması tedbirinin uygulanmasında taraf devlet tarafından belirlenmesi gereken katalog suçların kapsamında daha dar olamayacaktır.[324]Sözleşme, daha etkin ve sağlıklı bir soruşturma için 2 ila 10. maddelerde düzenlenen suçlar bakımından ilgili suçlar taraf devlet tarafından ciddi kabul edilmese bile bu tedbirin uygulanmasını tavsiye etmektedir.[325]Burada, önemli olan husus, özel hayata

[320] Explanatory Report, 223.
[321] Explanatory Report, 224.
[322] Explanatory Report, 206.
[323] Explanatory Report, 207.
[324] Explanatory Report, 213.
[325] Explanatory Report, 214.

müdahale niteliği bulunan bu tedbire başvurulurken Sözleşme'nin 14 ve 15. maddeleri çerçevesinde ve Avrupa İnsan Hakları Mahkemesi'nin içtihatları ışığında gereklilik, ikincil olma ve orantılılık ilkelerini dikkat edilmesidir.[326]

5271 sayılı CMK'nın 135. maddesi, Sözleşme'nin 20. maddesinde düzenlenen ve yukarıda açıklanan tedbirin uygulanmasına hizmet etmektedir. Yasamız, trafik verilerinin gerçek zamanlı toplanması ve gerçek zamanlı olarak içerik verilerine müdahale edilmesi arasında bir ayrım gözetmeyerek iletişim üzerinde uygulanan bu iki tedbiri birlikte 135. maddede düzenlemiştir.

Bu düzenlemeye göre, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebepleri varsa ve başka suretle delil elde etme imkânı bulunmuyorsa, ağır ceza mahkemesi veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir. Maddenin 6. fıkrasında ise şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespitine, soruşturma aşamasında hâkim, kovuşturma aşamasında mahkeme kararı ile olanak sağlanmıştır.

Öğretide, iletişim; haber, yazı, resim, ses veya sinyallerin telefon, telgraf, radyo veya benzeri elektromanyetik dalgalarla gönderilmesi veya alınması olarak tarif edilmiştir.[327]Klasik posta dışındaki her türlü iletişim, elektronik posta, faks gibi araçlarla yapılan iletişimler de dâhil olmak üzere, bu kapsamdadır.[328]

Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş Görev Ve Yetkileri Hakkında Yönetmelik'in 3. maddesinde telekomünikasyon, iletişimin dinlenmesi ve kayda alınması ve iletişimi tespitinin tanımları yapılmıştır.

Buna göre, telekomünikasyon; her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik,

[326] Explanatory Report, 215.
[327] Kunter, Yenisey, Nuhoğlu, s.723.
[328] Ünver, Hakeri, s. 464.

elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması demektir.

İletişimin dinlenmesi ve kayda alınması, telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemler anlamına gelmektedir.

İletişimin tespiti ise, iletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri ifade etmektedir.

Yukarıda yapılan bu açıklamalar doğrultusunda daha önce tanımı yapılan trafik verilerinin, iletişimin tespiti kapsamında değerlendirileceği açıktır. CMK'da iletişimin tespitinin düzenlendiği 135/6 maddesinde iletişimin tespitinde geriye dönük saklanmış veriler ile gerçek zamanlı olarak elde edilebilecek veriler arasında bir ayrım yapmamıştır. Bu nedenle saklı halde bulunan trafik verilerinin ve eş zamanlı olarak elde edilebilecek trafik verilerinin iç hukukumuza göre ağır ceza mahkemesinin heyet halinde vereceği karara ihtiyaç duyulmaksızın tek hâkimin, yani sulh ceza hâkimliklerinin vereceği karar ile elde edilebileceği düşünülmektedir.

Bu tedbirin uygulanması için bir suç sınırlaması getirilmediği için her suçta uygulanabilme imkânı vardır.

CMK'nın 157. maddesi uyarınca yürütülecek soruşturmalarda genel olarak soruşturmanın gizliliği ilkesine dikkat edilmesi gerektiğini amirdir. Ayrıca Sözleşme'nin 20/3 maddesi ile uyumlu olarak bu tedbirin uygulanması sırasında normal olarak uygulanması gereken gizliliğin ötesinde bir gizlilik 135/7 maddesi uyarınca öngörülmüştür.

7. İçerik Verilerine Müdahale (SSS madde 21)

Sözleşme'de öngörülen en ağır koruma tedbiridir. İletişim özgürlüğüne ve özel yaşamın dokunulmazlığına açık ve ağır bir müdahale söz konusudur.[329] Bu nedenle bazı ciddi görülen suçlar üzerinde bu tedbir uygulanabilecektir.

[329] Serap Keskin, s.175-176.

Ancak bilgisayar teknolojileri ile çok miktarda yazılı, görsel ve sesli verileri çok kolay bir şekilde aktarma imkânı göz önüne alındığında, çocuk pornografisi gibi yasadışı içerik barındıran verilerin paylaşılması suçlarının tespiti için ya da bilgisayar sistemine yasadışı erişim veya bilgisayar sistemine kötücül yazılım yerleştirme gibi suçların işlenmesi öncesinde ve sırasında içerik alışverişi ve aktarımının ortaya çıkarılması için bu tedbire başvurmak gerekmektedir. Bilgisayar sistemleri aracılığı ile gerçekleştirilen iletişimlere konu içeriklere gerçek zamanlı olarak müdahale etmek telekomünikasyon aracılığı ile gerçekleştirilen iletişime müdahale etmek kadar önemlidir.[330]

Taraf devletler kendi iç hukuklarına göre belirledikleri ciddi suçlara ilişkin olarak, Sözleşme'nin 21. maddesinin 1. fıkrasının (a) bendine göre, yetkili makamlarını, bir bilgisayar sistemi aracılığı ile üretilmiş belirli iletişimlerle ilişkili gerçek zamanlı içerik verilerini teknik imkânlarla toplamaya veya kaydetmeye yetkili kılacaklardır. (b) bendine göre ise, taraf devletler, yetkili makamlarını bir hizmet sağlayıcısı aracılığı ile ve hizmet sağlayıcısının teknik imkânları çerçevesinde belirli iletişimlerle ilişkili gerçek zamanlı içerik verilerini toplamaya veya kaydetmeye ve hizmet sağlayıcılarını bu konuda işbirliğine zorlayabilmelerine yasal olanak sağlayacaklardır.

Sözleşme, içerik verisini, iletişimin içerisinde yer alıp da trafik verisi olarak değerlendirilmeyen iletişimin anlamı ve amacını ortaya çıkaran içerik ya da iletişim yoluyla aktarılan bilgi veya mesaj olarak tanımlamıştır.

Sözleşme'de düzenlenen bu koruma tedbirinin karşılığı mevzuatımızda CMK'da "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" üst başlığı altında 135. maddede "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" başlığı ile düzenlenmiştir. Trafik verilerinin gerçek zamanlı toplanması konusunu incelerken bu konuya da girildiği için tekrara neden olunmayacaktır. Farklı olarak burada iç hukukumuz açsından ciddi görülen suçlara, yani iletişime konu içerik verilerine hangi suçlarda müdahale edileceğine yer verilecektir. Bu suçlar mevzuatımızda bulunan beş ayrı kanundan alınarak kategorize edilmiştir.

---

[330] Explanatory Report, s.228.

TCK'dan, göçmen kaçakçılığı ve insan ticareti (madde 79, 80), kasten öldürme (madde 81, 82, 83), işkence (madde 94, 95), cinsel saldırı (birinci fıkra hariç, madde 102), çocukların cinsel istismarı (madde 103), nitelikli hırsızlık (madde 142) ve yağma (madde 148, 149), uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188), parada sahtecilik (madde 197), fuhuş (madde 227), ihaleye fesat karıştırma (madde 235), rüşvet (madde 252), suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282), devletin birliğini ve ülke bütünlüğünü bozmak (madde 302) , anayasal düzene ve bu düzenin işleyişine karşı suçlar (madde 309, 311, 312, 313, 314, 315, 316), devlet sırlarına karşı suçlar ve casusluk (madde 328, 329, 330, 331, 333, 334, 335, 336, 337) suçları bu tedbirin kapsamı içerisindedir.

Bunların yanında Ateşli Silahlar ve Bıçaklar ile Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçu, Bankalar Kanununun 22. maddesinin 3 ve 4 numaralı fıkralarında tanımlanan zimmet suçu, Kaçakçılıkla Mücadele Kanununda tanımlanan ve hapis cezasını gerektiren suçlar ve son olarak Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74. maddelerinde tanımlanan suçlar için de bu tedbir uygulanabilecektir.

CMK'nın 135. maddesinde yer alan düzenleme, Sözleşme'nin 21. maddesinde yer alan düzenleme ile uyumludur. Ancak Sözleşme'nin ayrıca bir suç olarak düzenlediği, ayrıntılı bir şekilde ele aldığı çocuk pornografisi suçunun, CMK'da ciddi bir suç olarak görülmeyip bu tedbirin kapsamı dışında bırakılması bir eksikliktir. Bu nedenle müstehcenlik suçunun düzenlendiği 226. maddesinin 3. fıkrasının, CMK'nın 135. maddesine eklenerek bu koruma tedbirinin uygulama alanı içine sokulmalıdır.

8. Yargılama Yetkisi (SSS madde 22)

Bu düzenlemede, Sözleşme'nin 2 ila 11. maddelerinde tanımlanan suçlara ilişkin olarak taraf devletlerin uymakla yükümlü oldukları temel ölçütler belirlenmiştir. [331]

[331] Explanatory report, 232.

Maddenin 1. fıkrasının (a), (b) ve (c) bentleri ile öngörülen ilk ölçüt mülkilik ilkesine[332], (d) bendi ile öngörülen ölçüt ise faile göre şahsilik ilkesine[333] dayanmaktadır.

Mülkilik esasına göre, taraf devletler, Sözleşme'nin 2 ila 11. maddelerinde suç olarak kabul edilen eylemlerin kendi ülkelerinde, kendi bayrağını taşıyan bir gemide ve kendi yasalarına göre kayıtlı bir uçakta gerçekleştirilmesi durumunda yargılama yetkisi için gerekli yasama tedbirlerini alacaklardır.

Faile göre şahsilik ilkesine göre ise, taraf devletler, Sözleşme'nin 2 ila 11. maddelerinde suç olarak kabul edilen eylemlerin vatandaşlarından biri tarafından eylemin cezalandırılabilir olarak kabul edildiği bir yerde veya herhangi bir devletin yargı yetkilerinin bulunduğu sınırlar dışında gerçekleştirilmesi durumunda yargılama yetkisi için gerekli yasama tedbirlerini kabul edeceklerdir.

TCK'nın 8. maddesi, "Türkiye'de işlenen suçlar hakkında Türk Kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç Türkiye'de işlenmiş sayılır" hükmünü amirdir. Yani Türkiye'de işlenen suçların şüphelisinin, mağdurunun, müştekisinin ve sanığının ve katılanın uyrukluğuna bakılmaksızın Türk yasaları uygulanacaktır.[334]Aynı maddede bir suçun; Türk kara ve hava sahaları ile Türk karasularında, açık denizde ve bunun üzerindeki hava sahasında, Türk deniz ve hava araçlarında veya bu araçlarla, Türk deniz ve hava savaş araçlarında veya bu araçlarla, Türkiye'nin kıt'a sahanlığında veya münhasır ekonomik bölgesinde tesis edilmiş sabit platformlarda veya bunlara karşı işlendiği durumlar da ele alınarak o suçun Türkiye'de işlenmiş sayılacağı belirtilmiştir.

Esasen TCK'ya yargılama yetkisi bağlamında hâkim olan ilke mülkilik ilkesi olmasına rağmen bu ilkenin tek başına kabulü devletin kendi sınırları dışında işlenen suçlara müdahale etmesine izin vermemesi ve faillerin cezasız kalmasını neden olması sorunlarına yol açacağı öngörülmüştür. Bu nedenle TCK tarafından

[332] Explanatory report, 233.
[333] Explanatory report, 236.
[334] Özgenç, s.122.

yarı mülkilik sistemi kabul edilerek başkaca ilkeler de kabul edilmiştir.[335]

Sözleşme'nin yukarıda açıklanan maddenin (d) fıkrasına paralel olarak TCK, Türk vatandaşını (yurt dışında memuriyet ve görev üstlenenler hariç) Türkiye dışında işlediği suçlar nedeniyle de iki yolla takip etmektedir. Bunlardan birisi TCK'nın 13. maddesinde düzenlenen (devleti ve vatandaşı) koruma ve evrensellik ilkeleri uyarınca, diğeri ise TCK'nın 11. maddesinde düzenlenen şahsilik ilkesince yapılmaktadır.

TCK'nın 13. maddesi kapsamında kalan suçlar, Sözleşme'nin 2 ila 11. maddelerinde yer alan suçları içermemektedir. Ancak Türk vatandaşları tarafından işlenen Sözleşme'de düzenlenen ve mevzuatımızda karşılık bulan suçlar açısından failler hakkında Türk yasaları uygulanacaktır. TCK'nın 11. maddesine göre, bir Türk vatandaşı, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu işlerse bazı şartlar altında Türk yasalarına göre hakkında soruşturma ve kovuşturma yapılabilir. Bu şartlar şunlardır:

- Eylemin yabancı ülkede işlenmesi,
- Türk vatandaşının Türkiye'de olması,
- Suça konu eylem nedeniyle yabancı ülkede hakkında Türk vatandaşı hakkında hüküm verilmemiş olması
- Suça konu eylemin Türkiye'de kovuşturulabilirliğin bulunması,
- İşlenen suçun 13. maddede yazılı suçlar dışında olması.

Ancak suçun, aşağı sınırı bir yıldan az hapis cezasını gerektiriyorsa ayrıca zarar görenin veya yabancı hükûmetin eylemi gerçekleştiren vatandaşın Türkiye'ye girmesinden itibaren altı ay içinde şikâyette bulunması gerekmektedir.

Sözleşme açısından, Sözleşme'de yer alan ve iç hukukumuzda hapis cezasını gerektiren suçların Türk vatandaşları tarafından işlenmesi durumunda haklarında Anayasa'nın 38/son ve TCK'nın 18/2 maddeleri gereğince iade söz konusu olamasa

[335] Yenidünya – Gökcen -Artuk, s. 1018.

da yargılama yapılabilecektir.

Sonuç olarak, iç hukukumuzun Sözleşme'nin 22. maddesi ile uyum halinde olduğu söylenebilir.

E. Uluslararası İşbirliği Açısından Karşılaştırmalı Bakış

1. Giriş

Siber suçların, sınır aşan özelliği nedeniyle cezai alanda uluslararası işbirliği olmaksızın bu suç ile etkili bir şeklide mücadele etmek mümkün değildir. Devletler arasında karşılıklı yardımlaşma olmaksızın bir ülkeyi içine alan bir siber suç hakkında başlatılacak soruşturma, baştan ölü doğmuş bir soruşturmadır. Bu soruşturma sonunda suçun ortaya çıkarılması ve suçun faillerinin bulunması, yakalanması ve yargılanması beklenmemelidir. Aslında bu durum Sözleşme'nin de varlık nedenidir. Eğer siber suçlar, geleneksel bir suçlar gibi bir doğaya sahip olsa, yani ülke sınırları içerisinde işlenen ve sınır aşma özelliği zayıf bir suç tipi olsaydı, Sözleşme'ye de ihtiyaç duyulmayacak, zaten var olan uluslararası antlaşmalar, teamüller ve mütekabiliyet ilkesine göre hareket edilecekti. Ancak ne siber suçlar geleneksel suçlarla aynı doğaya sahip ve onunla aynı silahlarla mücadele edilebilir ne de mevcut uluslararası antlaşmalar siber suçların getirdiği sorunları çözebilecek esneklik ve güncelliktedir.

Türkiye açısından durum ülke içerisinde sınırlı kalan siber suçlar ve sınır aşan nitelikte işlenmiş olan siber suçlar açısından farklılık göstermektedir. Ülke içerisinde işlenen suçlar ile ilgili genel olarak farklı yasalarla gerekli suç tanımlamaları yapılmış ve ceza usul yasasında uygulanacak usul ve tedbirler gösterilmiştir. Ülke dışı bağlantılı suçlarda, örneğin ilk veya son icra hareketi ya da kesintisiz suçlarda kesinti ya da zincirleme suçlarda son suç Türkiye'de gerçekleşmişse ya da eylem yurt dışında başlamış netice Türkiye'de tamamlanmış ise karşılıklı adli yardımlaşma ile sorun giderilmeye çalışılmaktadır.

Uluslararası adli yardımlaşma, bir devletin yetkili bir adli makamının diğer devleti adli makamı adına yerine getirdiği işlemler olup, istinabe işlemleri, suçluların iadesi, hükümlü nakli muhakemenin ve infazın devri bu kapsamda

değerlendirilmektedir.[336] Ülkemizde, uluslararası adli yardımlaşma, 2992 sayılı Adalet Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin Değiştirilerek Kabulü Hakkında Kanun'un 13/A maddesi gereğince Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü (UHDİGM) üzerinden yürütülmektedir.

Adli yardımlaşma söz konusu olduğunda öncelikle adli yardım talep eden ülke ile Ülkemiz arasında adli yardımlaşmaya ilişkin ikili bir sözleşme olup olmadığına bakılmakta, böyle bir sözleşmenin varlığı halinde o sözleşmeye göre hareket edilmektedir. İkili sözleşmenin bulunmaması ya da böyle bir sözleşme varsa bile içerisinde adli yardımlaşmaya ilişkin bir hüküm yoksa, Ülkemiz ile adli yardım talep eden ülke arasında her iki ülkenin de tarafı olduğu adli yardımlaşmaya dair hükümler barındıran çok taraflı bir sözleşme olup olmadığına bakılmaktadır. Böyle bir ortak sözleşme varsa o sözleşme esas alınarak adli yardımlaşma gerçekleştirilmektedir. Adli yardımlaşmaya ilişkin ikili veya çok taraflı herhangi bir sözleşme bulunmadığı takdirde karşılıklılık ilkesine göre sorun çözülmektedir.[337]Mevzuatımızda, adli yardımlaşmaya ilişkin bağımsız bir kanun bulunmamaktadır.[338]

Ülkemizin taraf olduğu uluslararası adli işbirliğine dayanak teşkil edecek uluslararası sözleşmeler iki grupta ele alınmıştır.[339]Bunlardan ilki, münhasır adli yardımlaşma sözleşmeleridir. Bu anlamda taraf olduğumuz başlıca sözleşmeler şunlardır:

- Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi (ETS:30)
- Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi Ek Birinci Protokol(ETS:99)
- Suçluların İadesine Dair Avrupa Sözleşmesi (ETS:24)

---

[336] Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, Cezai Konularda Adli İşbirliği Rehberi, , Şen Matbaa, Ankara 2014, s.5.
[337] A.g.e., s. 8.
[338] Durmuş Tezcan, Mustafa Ruhan Erdem, Rifat Murat Önok, Uluslararası Ceza Hukuku, Seçkin Yayıncılık, Ankara, 2009, s.181.
[339] Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü, Cezai Konularda Adli İşbirliği Sözleşmeleri, http://www.uhdigm.adalet.gov.tr/sozlesmeler/munhasir_adli_yardimlasma.html

- Suçluların İadesine Dair Avrupa Sözleşmesi Ek İkinci Protokol(ETS:98)
- Hükümlülerin Nakline Dair Avrupa Sözleşmesi(ETS:112)
- Ceza Yargılarının Milletlerarası Değeri Konusunda Avrupa Sözleşmesi(ETS:70)
- Ceza Kovuşturmalarının Aktarılmasına Dair Avrupa Sözleşmesi(ETS:73)

İkinci grupta ise münhasıran olmayıp başka hükümlerle birlikte adli yardımlaşmaya dair hükümlerin de yer aldığı sözleşmeler yer almaktadır. Budapeşte Sözleşmesi de bu gruptadır. Bu grupta yer alan başlıca sözleşmeler ise şunlardır:

- Terörizmin Önlenmesine Dair Avrupa Sözleşmesi(ETS:90)
- Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El konulmasına İlişkin Avrupa Sözleşmesi(ETS:141)
- Birleşmiş Milletler Uyuşturucu Maddeler TEK Sözleşmesi
- Birleşmiş Milletler Uyuşturucu ve Psikotrop Maddelerin Kaçakçılığına Dair Sözleşme
- Birleşmiş Milletler Sınıraşan Örgütlü Suçlara Dair Sözleşme
- Birleşmiş Milletler Terörizm Finansmanının Önlenmesine Dair Uluslar arası Sözleşme
- Birleşmiş Milletler Yolsuzlukla Mücadele Sözleşmesi

Uluslararası adli yardımlaşma, Sözleşme'de "uluslarası işbirliği" başlığı altında 3. bölümde 12 ayrı maddede düzenlenmiştir. Bu bölümde uluslararası işbirliğine ilişkin genel prensipler belirlenmiş, bunların suçluların iadesi ve karşılıklı adli yardımlaşma sırasında uygulamasını göstermiştir. Daha sonra getirilen özel hükümlerle ilgili olarak uygulanacak tedbirler ortaya konulmuştur.

2. Uluslararası Yardımlaşmaya İlişkin Genel İlkeler (SSS madde 23)

Sözleşme'nin 23. maddesinde, taraf devletlerden bilgisayar sistem ve verileri hakkında işlenen suçlarda ve herhangi bir suçun elektronik ortamda bulunan delilinin elde edilmesinde gerek Sözleşme'nin uluslararası işbirliğine ilişkin

bölümünde yer alan hükümlere gerek cezai alanda uluslararası işbirliği ile ilgili tek taraflı veya çoklu antlaşmalara göre mümkün olan en geniş biçimde birbirleri ile işbirliği yapmaları gerektiği hükme bağlanmıştır.

Bu bölümün ilk maddesidir ve burada taraf devletlere herhangi bir özel yükümlülük yüklenmeksizin üç temel ilke belirlenerek genel bir düzenleme yapılmıştır. Bu ilkeler şunlardır:

- Taraf devletler birbirlerine yardım ederken mümkün olan en geniş biçimde yardım edeceklerdir. Bu uluslararası alanda kapsamlı bir işbirliği ve düzgün ve hızlı bilgi ve delil akışı demektir.[340]
- İşbirliğinin kapsamı içerisine bilgisayar sistem ve verileri ile bağlantılı suçlar ve herhangi bir suçun elektronik ortamda bulunan delilinin toplanması girecektir.[341]
- Sözleşme'nin 3. bölümünde yer alan işbirliğine dair hükümler, uluslararası işbirliği ile ilgili tek taraflı veya çoklu antlaşmaların yerine getirilmemiş ve onlardan üstün değildir.[342]

3. Suçluların İadesi (SSS madde 24)

Uluslararası işbirliğinin en önemli kurumlarından biri olan suçluların iadesi Sözleşme tarafından ihdas edilmiş değildir. Ancak Sözleşme'de, iadeye konu edilen suçların çerçevesi Sözleşme'nin 2 ila 11. maddelerinde tanımlanan suçlar üzerinden çizilmiş ve bir alternatif olarak düzenlenmiştir. Böylece Sözleşme, içerisinde adli yardımlaşma hükümlerinin de yer aldığı uluslararası bir sözleşme haline gelmiştir.

Sözleşme'nin 24. maddesinin 1. fıkrasına göre, suçluların iadesi, Sözleşme'nin 2 ila 11. maddesinde düzenlenen suçlara ilişkin olarak suçun failinin en az bir yıl veya daha fazla hapis cezası gerektirecek nitelikte cezalandırılabilmesine olanak sağlayan yasal düzenlemelerin bulunduğu taraf devletlerde uygulanacaktır. Öngörülen bir yıllık süre mahkeme tarafından verilen 1

[340] Explanatory report, s.242.
[341] Explanatory report, s.243.
[342] Explanatory report, s.244.

yıllık mahkûmiyeti değil, kanun metninde geçen ceza miktarıdır.[343]Eğer aralarında iade süreci yürüyen taraf devletler arasında, iade için daha farklı bir süre eşiği öngören bir antlaşma ya da bir düzenleme varsa, bu antlaşma ya da düzenlemede öngörülen süre uygulanacaktır.

Maddenin ikinci fıkrasında ise Sözleşme, taraf devletleri bir taahhüt yükümlülüğü altına sokarak taraf devletlerden mevcut iade antlaşmalarında Sözleşme'nin 2 ila 11. maddelerinde tanımlanan suçları iadeye konu edilebilir saymalarını, ileride akdedilecek iade antlaşmalarının kapsamı içerisine de bu suçları koymalarını istemektedir. Bu husus, ilgili suçların faillerinin doğrudan iadesi anlamına gelmeyip, sadece ilgili suçların faillerinin iadesine olanak veren yasal zeminini oluşturmaktadır.[344]

Taraflar arasında Sözleşme'de düzenlenen suçların faillerinin iadesine yasal zemin teşkil edecek herhangi bir antlaşma yoksa, maddenin 3. fıkrası uyarınca Sözleşme üzerinden suçluların iadesi gerçekleştirilebilecektir. Ancak bunun bir zorunluluk olmadığını da belirtmek gerekir.[345]Diğer taraftan bir taraf devlet, suçluların iadesini bir antlaşmanın varlığına bağlamamış ve sadece kendi ulusal mevzuatı ile yetiniyorsa, taraf devlet maddenin 4. fıkrası gereğince kendi iç hukukunda Sözleşme'de yer alan suçları iadeye konu hale getirmelidir. [346]

Sözleşme'nin suçluların iadesine dair hükümleri, uluslararası mevzuattan bağımsız değildir ve kendisinden iade talep edilen devlet uluslararası mevzuatta yer alan hükümlere göre iade talebini maddenin 5. fıkrası uyarınca reddedebilecektir. Örneğin, iade talep edilen devlet, Suçluların İadesine Dair Avrupa Sözleşmesi'ne göre suçun siyasi olması ya da iade edilecek kişinin ırkı, dini, milliyeti veya siyasi görüşü nedeniyle soruşturma veya kovuşturmaya maruz kalması nedenleriyle iade talebini geri çevirecektir.[347]

---

[343] Explanatory report, s.245.
[344] Explanatory report, s.247.
[345] Explanatory report, s.248.
[346] Explanatory report, s.249.
[347] Explanatory report, s.250.

Maddenin 6. fıkrasında ise, “aut dederu aut judicare” , “ya iade et ya da yargıla” ilkesi düzenlenmiştir. Talep edilen kişinin talebin yapıldığı devletin vatandaşı olması ya da talep yapılan devletin yargı yetkisi iddiası nedenleriyle iade talebi reddedilirse, talebi reddeden devlet talep edilen kişinin yargılanması için davayı adli makamlarına havale edecektir. Suçluyu talep eden ve bu talebi reddedilen devlet, ayrıca suçlunun yargılanmasını ilgili devlet talep etmezse, o devletin iadesi istenen kişiyi yargılama zorunluluğu yoktur.[348]

Maddenin 7. fıkrasında ise, suçluların iadesi sözleşmesinin yokluğunda iade ve tutuklama taleplerinin alınacağı ve gönderileceği merkezi otoritenin taraf devletler tarafından oluşturulması gerektiği belirtilmiştir.

Mevzuatımızda, suçluların iadesine dair hükümler, Anayasa’nın 38/son ve TCK’nın 18. maddelerinde yer almakta ve Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü’nün “Suçluların İadesi ve Hükümlü Nakli Konularında Adli Makamlarımızca Dikkat Edilmesi Gereken Hususlar” konulu 69/4 sayılı Genelge’de uygulama usulü gösterilmiştir. Ayrıca bu konuda yukarıda gösterildiği üzere tarafı olduğumuz uluslararası sözleşmeler vardır. Sözleşme’ye taraf olduğumuz için artık o da artık iç hukukumuzun bir parçası haline gelmiştir ve bağlayıcılığı bulunmaktadır.

Temel olarak suçluların iadesi, TCK’nın 18. maddesinde “geri verme” başlığı altında düzenlenmiştir. Buna göre, bir suç nedeniyle hakkında ceza soruşturması ya da kovuşturması başlatılan veya mahkûmiyet kararı verilmiş olan bir yabancı, talep üzerine, soruşturma ya da kovuşturmanın yapılabilmesi veya hükmedilen cezanın infazı amacıyla geri verilebilir. Ancak bazı durumlarda, yapılan geri verme talebi kabul edilmez. Aşağıdaki durumlar bu kapsamdadır:

- Atılı suçun Türk kanunlarına göre suç olmaması,
- Atılı suçun düşünce suçu veya siyasi ya da askerî suç olması,
- Atılı suç Türkiye Devletinin güvenliğine karşı, Türkiye Devletinin veya bir Türk vatandaşının ya da Türk kanunlarına göre kurulmuş bir tüzel kişinin

[348] Explanatory report, s.251.

zararına işlenmesi,

- Atılı suçun Türkiye'nin yargılama yetkisine giren bir suç olması,
- Atılı suçun zamanaşımına veya affa uğramış olması,
- Atılı suçun failinin vatandaş olması, (Uluslararası Ceza Divanına taraf olmanın gerektirdiği yükümlülükler hariç)
- Atılı suçun failinin talep eden devlete geri verilmesi halinde ırkı, dini, vatandaşlığı, belli bir sosyal gruba mensubiyeti veya siyasi görüşleri nedeniyle soruşturulacağına ya da kovuşturulacağına veya cezalandırılacağına ya da işkence ve kötü muameleye maruz kalacağına dair kuvvetli şüphe bulunması.

Sözleşme'nin dayatmacı bir yaklaşımı yoktur. Amaç, siber suçlunun yargılanmasının sağlanmasıdır. Sözleşme, bir alternatif olarak suçluların iadesi için kendisine taraf olan devletler için beklemektedir. Başkaca uluslararası ikili ya da çoklu sözleşmelerle iadenin gerçekleşmesinin, Sözleşme açısından yeterlidir. Bu anlamda Sözleşme'ye taraf olan Ülkemiz açısından Sözleşme'nin ilgili hükümleri ve mevzuatımız arasında herhangi bir uyumsuzluk bulunmamaktadır.

Sözleşme'nin 7. fıkrasında belirlenmesi istenen merkezi otorite Türkiye için Adalet Bakanlığı'dır.[349]

4. Karşılıklı Yardımlaşmaya İlişkin Genel İlkeler (SSS madde 25)

Sözleşme, taraf devletler arasında işbirliğinin sağlanması ve kolaylaştırılması için bazı temel ilkeler belirlemiştir. Bu ilkeler, karşılıklı yardımlaşmanın sağlanması zorunluluğu çerçevesinde ortaya konmuştur.

Bu ilkeler maddenin ilk fıkrasında ele alınmıştır ve esasen Sözleşme'nin 23. maddesinde belirtilen ilk iki ilkenin tekrarı niteliğindedir. Bu ilkeler, aynı zamanda yardımlaşmanın ne ölçüde ve hangi kapsamda yapılacağı sorularının cevaplarıdır. Birinci fıkrada yer alan ilk ilke, yardımlaşmanın mümkün olan en geniş ölçüde

[349] List of Declarations made with Respect to Treaty No. 185, Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 , 29.04.2015.

yapılacağına dairdir. İkinci ilke ise, yardımlaşmanın, bilgisayar sistem ve verileri ile bağlantılı suçlara ve herhangi bir suçun elektronik ortamda bulunan delilinin toplanmasına ilişkin olacağına dairdir.[350]

Diğer fıkralarda ise belirlenen ilkeler doğrultusunda, taraf devletler çeşitli konularda yükümlülük altına sokulmuşlardır. Bunları maddeler halinde özetleyelim:

- Sözleşme'nin 27 ile 35. maddelerinde yer alan yükümlülükleri yerine getirebilmelerini mümkün kılacak yasal ve diğer tedbirleri almak (25/2),
- Bilgisayar verisinin kaybolma veya silinme riskinden kaynaklanan hassasiyeti nedeniyle onun güvenlinin ve gerçekliğinin korunması dikkate alınarak karşılıklı yardımlaşmayı en hızlı iletişim araçları ile gerçekleştirmek (25/3),
- Temel hakların korunması açısından karşılıklı adli yardımlaşma işlemlerini Sözleşme'de aksi öngörülmedikçe yürürlükteki karşılıklı yardımlaşma sözleşmelerine ve talepte bulunulan taraf devletin ulusal yasalara göre gerçekleştirmek (25/4),
- Taraf devletler tarafından karşılıklı yardımlaşmanın çifte cezalandırılabilirlik şartına bağlandığı durumlarda suçun taraf devletlerde aynı suç kategorisinde olmasına ya da aynı terimlerle tanımlanmasına bakılmaksızın maddi unsurları oluşturan eylemin aynı olması yeterli görmek(25/5).

Ülkemiz açısından ceza alanında uluslararası adli yardımlaşmanın iç hukuktaki dayanağını TCK'nın 8 ila 19. maddeleri, 7201 sayılı Tebligat Kanunu ile 69/2 sayılı "Uluslararası Ceza İstinabe İşlemlerinde Adli Makamlarımızca Dikkat Edilmesi Gereken Hususlar" konulu Genelge ve 69/3 sayılı "Cezai Konularda Uluslararası Tebligat" konulu Genelge oluştururken; uluslararası hukuktaki dayanağını Ülkemizin taraf olduğu uluslararası sözleşmeler, karşılıklılık ilkesi, uluslararası teamüller ve hukukun temel ilkeleri oluşturmaktadır.[351]

69/2 sayılı Genelge'ye göre adli yardımlaşmanın kapsamına,

---

[350] Explanatory report, s.253.

[351] Cezai Konularda Adli İşbirliği Rehberi, s.23.

- Şüpheli veya sanıkların ifadelerinin alınması veya sorgularının yapılması,
- Mağdur, müşteki, katılan, tanık veya bilirkişilerin dinlenilmesi,
- Bilgi ve delil temini, banka kayıtları, muhasebe belgeleri, şirket dosyaları ve ticari belgeler de dâhil olmak üzere, ilgili belge ve kayıtların asıllarının veya tasdikli suretlerinin sağlanması,
- Delil toplamak amacıyla kazançların, malvarlıklarının, araç-gerecin ya da diğer hususların belirlenmesi veya izlenmesi,
- Delil amaçlı arama ve el koyma, eşya ve yer incelemesi,
- El koyma ve müsadereye dair yabancı mahkeme kararlarının infazı girmektedir.

Aynı genelgeye göre, gerek Ülkemizce başka devletlerden istenilen yardımlaşma gerek başka devletlerce Ülkemizden istenilen yardımlaşma düzenlenen bir talepname ile gerçekleştirilmektedir. Her iki durumda da bu işlemlere aracılık eden merkez makam UHDİGM'dir. Hazırlanacak talepnamede, talepte bulunulan adli makamın adı, maddî olguların özeti, uygulanması muhtemel kanun maddeleri, istenilen yardımlaşmanın tanımı, gerekçesi ve talep ediliyorsa herhangi bir özel usûlün ayrıntıları, mümkün olduğu ölçüde, ilgili kişinin kimliği, adresi ve uyruğu ve delil, bilgi veya işlemlerin hangi amaçla talep edildiği hususları yer almaktadır.

Sözleşme, diplomat çantası veya posta gibi geleneksel yöntemlerin ötesinde faks, e-posta gibi daha hızlı ve etkili iletişim araçları ile karşılıklı olarak uluslararası istinabe işlemlerinin gerçekleştirilmesini istemektedir.[352]Siber suçların doğası, elektronik delilin hassasiyeti ve ileride değinilecek olan uluslararası koruma tedbirleri de niteliği gereği bunu gerektirmektedir. İç hukukumuz ile Sözleşme'nin adli yardımlaşmaya ilişkin hızlı ve dinamik hükümler öngören tedbirleri ile uyumlu gözüktüğünü söylemek zordur. Hem mevzuatımızda hem de ilgili genelgelerde

[352] Explanatory report, s.256.

Sözleşme'nin beklentilerini karşılayacak ve uygulamada kolaylık ve açıklık sağlayacak şekilde değişikliklerin yapılması gerekmektedir.

5. Kendiliğinden İletilen Bilgi (SSS madde 26)

Sözleşme'nin bu maddesi ile ETS 141 sayılı Avrupa Konseyi Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve Elkonulmasına İlişkin Sözleşme'nin 10. maddesinde ve ETS 173 sayılı Avrupa Konseyi Yolsuzluğa Karşı Ceza Hukuku Sözleşmesi'nin 28. maddesine paralel bir düzenleme getirilmiştir. Bu düzenlemede taraf devletlere zorunluluğu bulunan bir yükümlülük yüklenmemiştir. Ancak siber suçlarla mücadele kapsamında bir taraf devlet tarafından elde edilen ve başka bir taraf devlet için başlatılacak bir soruşturmaya ya da adli yardımlaşmaya esas olacak nitelikte değerli ve kullanışlı bir bilginin paylaşılabileceği belirtilmiştir.

Bu düzenlemeye göre, bir taraf devlet, herhangi bir soruşturma nedeniyle edindiği bilgileri kendi iç hukukunun sınırları çerçevesinde ve önceden bir talep olmaksızın başka bir taraf devletin Sözleşme'ye göre yürüteceği soruşturma ve kovuşturmasına yardımcı olmak ya da Sözleşme'de öngörülen çerçevede bir işbirliği başlatmasını sağlamak amacıyla o devlete açıklayabilir. Ancak bu bir zorunluluk değildir.

Taraf devlet, bilgiyi ilettiği taraf devletten bilginin gizli tutulmasını isteyebileceği gibi bilginin kullanımını bazı şartlara da bağlayabilir. Çünkü paylaşılan bilginin bilgiyi alan taraf devlet tarafından kamuya açıklanması, bilgiyi aktaran taraf devleti zor durumda bırakabilir.[353]

Ülkemiz tarafından yukarıda belirtilen ETS 141 ve ETS 173 sayılı sözleşmeler sırasıyla 06/10/2004 ve 29/03/2004 tarihlerinde onaylanmıştır. Bu sözleşmelere dayanarak cezai konularda ilgili sözleşmelerin taraf devletlerine onların talebi olmaksızın bilgi paylaşımı yapabilmekteyiz. Sözleşme'nin onaylanması ile de Sözleşme'de düzenlenen suçlar nedeniyle elde edilen bir bilginin taraf devletlere paylaşımı söz konusu olabilecektir.

---

[353] Explanatory report, s.261.

6. Uluslararası Antlaşmaların Yürürlükte Olmadığı Durumlarda Yapılan Karşılıklı Yardımlaşma Taleplerine İlişkin Usuller (SSS madde 27)

Sözleşme'nin 27. maddesinde aralarında uygulanabilir karşılıklı bir adli yardımlaşma sözleşmesi bulunmayan yardım talep eden ve yardım talep edilen devletler arasında alternatif olarak uygulanabilecek usul ve esaslar düzenlenmiştir. Aslında bu husus, Sözleşme'nin 23/3 maddesinin tekrarından ibarettir. Sözleşme, açıkça var olan adli yardımlaşmaya ilişkin uluslararası sözleşmelerin yerine kendisini ikame etmeyi reddetmektedir.[354]Bununla beraber var olan karşılıklı adli yardımlaşma sözleşmeleri, Sözleşme'de yer alan uluslararası koruma tedbirlerini yer vermemeleri halinde, taraf devletlerin bu tedbirlerin uygulanmasını sağlayacak yasal altyapıyı hazırlamaları gerekmektedir.

Sözleşme'de yer alan tedbirler Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi ve ek protokolleri çerçevesinde ve hatta ileride imzalanacak herhangi bir karşılıklı yardımlaşma sözleşmesi çerçevesinde uygulanabilecektir.[355]Bu yönüyle Sözleşme hükümlerini tamamlayıcı ve destekleyici olarak görebiliriz. Buna rağmen taraf devletlerin kendi aralarında anlaşmak suretiyle Sözleşme'nin öngördüğü adli yardımlaşmaya ilişkin usul ve esasları da uygulamalarının önünde herhangi bir engel bulunmamaktadır. Fakat Sözleşme, taleplerin biçimi ve içeriği, tanık beyanlarının alınması, resmi veya ticari belgelerin temini, tanıkların nakli, müsadere gibi konularda düzenleme yapmadığı için Sözleşme'nin 25/4 maddesi uyarınca kendisinden talepte bulunulan tarafın ulusal mevzuatına göre boşluk doldurulacaktır.[356]Uygulanabilir bir adli yardımlaşma sözleşmesinin yokluğunda 25. maddede öngörülen ilkeler şunlardır:

- Her bir taraf devlet, karşılıklı yardımlaşmaya ilişkin talepleri göndermek, cevaplamak ve yerine getirmek ve diğer merkezi otoriteler ile iletişim kurmak ile sorumlu merkezi bir otorite belirleyecektir. (27/2)

[354] Explanatory report, s.262.
[355] Explanatory report, s.263.
[356] Explanatory report, s.264.

- Adli yardımlaşma talepleri, talep edilen taraf devletin ulusal yasalarına aykırı olmadığı sürece, talep eden taraf devletin usulüne göre yerine getirilecektir. (27/3)
- Kendisinden talepte bulunulan taraf devlet, talebin siyasi bir suç veya siyasi bir suçla ilgili bir suç hakkında olması ya da talebin yerine getirilmesinin milli egemenliğine, güvenliğine, kamu düzenine veya diğer temel menfaatlerine zarar vereceğini düşünmesi durumlarında talebi reddedebilir. (27/4)
- Kendisinden talepte bulunulan taraf devlet, talebin yetkili makamlarınca yürütülmekte olan bir soruşturmaya ya da kovuşturmaya zarar vermesi söz konu ise talebin yerine getirilmesini erteleyebilir. (27/5)
- Kendisinden talepte bulunulan taraf devlet, talebi reddetmeden veya ertelemeden önce, uygunsa talep eden taraf devletle görüşmek suretiyle talebi kısmen veya bazı şartlar kabul etmeyi düşünecektir. (27/6)
- Kendisinden talepte bulunulan taraf devlet, yardım talep eden devleti yardım talebinin akıbetine ilişkin durumdan derhal gerekçeleri ile birlikte haberdar edecektir. (27/7)
- Yardım talebinde bulunan taraf devlet, kendisinden talepte bulunulan taraf devletten talebin ve içeriğinin gizli tutulmasını isteyebilir. (27/8)
- Acil durumlarda, karşılıklı yardım talepleri veya bunlara ilişkin iletişimler merkezi otoriteleri aracı kılmaksızın doğrudan adli makamlara iletilebilir.(27/9)

Maddenin 2. fıkrasına göre, Ülkemizde merkezi otorite Adalet Bakanlığı'dır.[357]Daha öncede açıklandığı üzere, Adalet Bakanlığı bünyesinde bulunan UHDİGM aracılığı ile uluslararası adli yardımlaşma gerçekleştirilmektedir.

[357] List of Declarations made with Respect to Treaty No. 185, Council of Europe, (çevrimiçi) http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 29.05.2015

7. Gizlilik ve Kullanımın Sınırlandırılması (SSS madde 28)

Taraf devletler arasında yardım talebine konu bilgi ve materyalin hassas olması durumuna ilişkin bir düzenlemedir. Böyle durumlarda verilerin korunması gibi nedenlerle kendisinden yardım talebinde bulunulan taraf devlet, bilgi ve materyalin kullanımını yardımın sağlanma nedeniyle sınırlı tutulmasını ya da yardım talep eden devletin soruşturma makamlarının dışında kimseye ulaşmamasını şart koşabilir.[358]

Bu düzenlemede yine Sözleşme, bilgi ve materyalin gizliliği ve sınırlı bir şekilde kullanımı çerçevesinde, var olan başkaca tek taraflı veya karşılıklı uluslar arası sözleşmelerle bir çatışma ve çakışmayı önlemek için adli yardımlaşmaya ilişkin yürürlükte olan bir sözleşme veya düzenlemenin olmamasını, başka bir ifadeyle devreye girilmesini gerektirecek bir boşluk olmasını istemektedir.[359] Yardım talep eden ve talep edilen ayrıca aksi bir uygulama istemedikçe, bilgi ve materyalin gizliliği ve sınırlı bir şekilde kullanımı konusunda var olan karşılıklı adli yardımlaşma hükümleri uygulanacaktır.

Bu düzenleme ile her ne kadar gizlilik ve bilgi ve materyalin kullanımının sınırlandırılması istenmiş ise de, esasen bunun mutlak uygulanması[360]ve istisnalarının olmaması[361] mümkün değildir. Örneğin, soruşturma aşamasında sağlanan gizliliğin aleni olarak duruşmaların yapıldığı kovuşturma aşamasındaki yargılama sırasında da sağlanması olanaklı gözükmemektedir.

Sözleşmeye taraf olan Ülkemiz açısından da aynı durum geçerlidir. Bilgi ve materyalin gizliliği ve sınırlı bir şekilde kullanımına ilişkin olarak yürürlükte olan başkaca sözleşme yoksa, Sözleşme'nin ilgili hükümleri uygulanacak ve mümkün olan ölçüde gizlilik ve sınırlı kullanıma talep halinde uyulacak ya da bu yönde talep diğer taraf devlete iletilecektir.

---

[358] Explanatory report, 275.
[359] Explanatory report, 276.
[360] Explanatory report, 277.
[361] Explanatory report, 278.

8. Özel Hükümler (SSS'nin 29 ila 34. maddeleri)

Sözleşme'nin 29 ila 34. maddeleri arasında bilgisayar bağlantılı suçları ve elektronik ortamda bulunan delilleri ilgilendiren olaylara yönelik olarak alınacak etkin ve çok taraflı uluslararası düzeydeki tedbirler düzenlenmiştir.[362]

Bu bölümde yer alan tedbirler esasen Sözleşme tarafından ulusal düzeyde alınması gereken tedbirlerin uluslararası alanda yansımalarıdır. Sözleşme, Dünya'yı bir ülke gibi düşünerek iki ülke arasındaki adli yardımlaşmayı sanki il veya ilçe soruşturma makamları arasındaki yardımlaşmanın basitliğine ve hızına indirgemek istemiştir. Elbette, Sözleşme'nin siber suçlarla mücadele ve elektronik delillerin toplanmasına dair bu isteği siber suçluların isteyeceği en son şeydir. Uluslararası düzeyde soruşturma makamları tarafından alanın daraltılması, suçlular için güvenli bölgeler bırakılmaması uluslararası işbirliği ve bunun somut uygulamaları olan tedbirlerle olur.

Bu tedbirlerden ilki Sözleşme'nin 29. maddesinde düzenlenen saklı bilgisayar verilerinin hızlı korunmasıdır. Bu düzenlemeye göre, taraf devlet, bir başka devletin sorumluluk sınırları içerisinde bulunan bir verinin arama veya benzer şekilde erişme, elkoyma veya benzer şekilde koruma veya açıklama yollarından birisi veya birkaçı ile elde etmeyi amaçlamaktadır. Bu nedenle verinin bulunduğu taraf devletten suça konu bir verinin bilgisayar sistemleri aracılığı ile hızlı bir şekilde korunmasını talep etmektedir. Kendisinden talepte bulunulan taraf devlet ise aldığı bu talep üzerine hizmet sağlayıcılar gibi 3. bir kişiye suça konu verinin hızlı bir şekilde korunması talimatını vermekte ya da veriyi doğrudan korumaktadır. Böylece silinme, taşınma veya değiştirilme tehlikesi altında bulunan veri korunmaktadır. Bu düzenleme, Sözleşme'nin 16. maddesinin uluslararası düzeyde karşılığıdır.[363] Sözleşme, bu tedbirin uygulanması için Sözleşme'de tanımlanan suçlar yönünden çifte cezalandırılabilirlik şartının ileri sürülmesini kabul etmezken[364] Sözleşme'de tanımlanmayan suçlar yönünden ileri

[362] Explanatory report, 281.
[363] Explanatory report, 282.
[364] Explanatory report, 285.

sürülebileceğini kabul etmektedir. Bu çekincenin ileri sürülmesi için verinin açıklandığı zaman çifte cezalandırılabilirlik şartlarının karşılanmadığına dair kendisinden talepte bulunulan taraf devlette yeterli gerekçelerin olması gerekmektedir.[365]

Sözleşme'nin 17. maddesinin uluslararası düzeyde karşılığı olarak, Sözleşme'nin 30. maddesinde "korunan trafik verilerinin hızlı açıklanması" düzenlenmiştir. Bu düzenlemeye göre, kendisinden talepte bulunulan taraf devlet, 29. maddeye trafik verilerinin korunmasını sağlarken başka bir devlette bulunan bir hizmet sağlayıcının iletişimin aktarılmasında katılımının olduğunu tespit ederse; yardım talebinde bulunan devlete katılımı tespit edilen hizmet sağlayıcının ve iletişimin aktarılmasında kullanılan yolun teşhisine imkân verecek miktarda trafik bilgisini açıklayacaktır. Bu açıklama ile 3. bir taraf devlette ya da kendi ülkesinde bulunan bir hizmet sağlayıcının devrede olduğunu fark eden yardım talebinde bulunan taraf devlet, suçun ortaya çıkarılması ve faillerin yakalanması için 3. bir taraf devlet ile adli yardımlaşma yapacak ya da kendi ülkesinde bulunan hizmet sağlayıcıya gerekli talimatları verecektir.[366]

Sözleşme'nin 19. maddesinin uluslararası düzeydeki karşılığı olarak, Sözleşme'nin 31. maddesinde "saklı bilgisayar verilerine erişime dair karşılıklı yardımlaşma" düzenlenmiştir. Bu düzenlemeye göre, bir taraf devlet, başka bir taraf devletin sorumluluk sınırları içerisinde bulunan bilgisayar sistemleri içerisinde saklanmış veriler üzerinde arama veya benzer şekilde erişme, elkoyma veya benzer şekilde koruma veya açıklama talebinde bulunabilir. Bu talebi alan taraf devlet ise bu talebi adli yardımlaşmaya ilişkin ulusal ve uluslararası düzenlemeler çerçevesinde karşılayacak, hatta verinin kaybolma veya değiştirilme tehlikesi altında bulunması ya da tabi olunan bir ulusal ve uluslararası düzenlemede hızlı olunması yönünde bir hükmün bulunması durumunda talep çok daha hızlı

[365] Explanatory report, 286.
[366] Explanatory report, 290.

karşılanacaktır.

Sözleşme'nin 32. maddesinde "saklı bilgisayar verilerine sınır ötesinden erişim" düzenlenmiştir. Bu düzenlemeye göre, bir taraf devlet bir başka devletin sınırları içerisinde bulunan bilgisayar verisine iki istisnai durumda ilgili devletin herhangi bir yetkilendirmesi olmaksızın doğrudan erişebilir. Bunlardan ilki, bilgisayar verisinin kamuya açık kaynaklarda bulunması durumudur. Bu durumda coğrafi sınır gözetilmez. İkincisi ise, başka bir taraf devletin sınırları içerisinde bulunan bilgisayar verisi üzerinde kişisel olarak tasarruf hakkı bulunan kişinin yasal ve gönüllü rızası ile taraf devlet veriye erişme ve veriyi elde etme hakkına sahiptir. Karşılıklı adli yardımlaşma olmaksızın, tek taraflı olarak harekete geçilerek delil toplanması, Sözleşme'nin tasarısı hazırlanırken üzerinde uzun uzadıya tartışılan bir konu olmuş, sadece belirtilen iki durumda anlaşmaya varılmış ve başkaca durumlar zamana, edinilecek deneyimlere ve yapılacak tartışmalara bırakılmıştır.[367]

Sözleşme'nin 20. maddesinin uluslararası düzeydeki karşılığı olarak, Sözleşme'nin 33. maddesinde "gerçek zamanlı şekilde trafik verilerinin toplanmasına dair karşılıklı yardımlaşma" düzenlenmiştir. Bu düzenlemeye göre, iç hukukta yer alan şart ve usul çerçevesinde, taraf devletler bilgisayar sistemi aracılığı ile kendi sınırlarında aktarılan bir iletişim ile ilgili trafik verilerinin gerçek zamanlı olarak toplanması konusunda birbirlerine karşılıklı yardım sağlayacaklardır. Bu yardım en azından taraf devletin kendi iç hukukunda benzer bir olayda uygulanan ölçüde olacaktır. Bu hüküm nedeniyle her bir taraf devlet başka bir taraf devlet için gerçek zamanlı trafik verilerinin toplanması yükümlülüğü altına girmektedir.[368]İç hukukta trafik verilerinin gerçek zamanlı toplanması için öngörülen katalog suçları çerçevesi, uluslararası düzeyde uygulanacak bu koruma tedbirinin alt sınırını oluşturmakta, taraf devlet devletler belirlenen katalog suçların

[367] Explanatory report, 293.

[368]Explanatory report, 295.

ötesinde daha geniş bir çerçevede yardıma teşvik edilmektedirler.[369]

Sözleşme'nin 21. maddesinin uluslararası düzeydeki karşılığı olarak, Sözleşme'nin 34. maddesinde "gerçek zamanlı şekilde içerik verilerine müdahaleye dair karşılıklı yardımlaşma" düzenlenmiştir. Bu düzenlemeye göre, iç hukuk ve uygulanabilir sözleşmeler çerçevesinde, taraf devletler bilgisayar sistemi aracılığı ile kendi sınırlarında aktarılan bir iletişim ile ilgili içerik verilerinin gerçek zamanlı olarak kaydedilmesi konusunda birbirlerine karşılıklı yardım sağlayacaklardır. Özel hayata yönelik en ağır ve en müdahaleci tedbir olduğu için, bu tedbir Sözleşme'nin 14, 15 ve 21. maddeleri ile Telekomünikasyona Müdahale için Talepname Yazılmasına Dair Ceza İşlerinde Karşılıklı Adli Yardımlaşma Avrupa Sözleşmesi'nin Uygulanması Tavsiye Kararı kapsamında ele alınmalıdır.[370] Adı geçen tavsiye kararında telekomünikasyon yoluyla iletişime yapılacak müdahalede uygulanacak usul ve esaslar açıklanmıştır.[371]

Ülkemiz iç hukukunda yukarıda açıklanan uluslararası koruma tedbirlerine ilişkin doğrudan bir düzenleme bulunmamaktadır. Ancak taraf olunan Sözleşme ve diğer uluslararası sözleşmeler, Anayasa'mızın 90/5 maddesi uyarınca bağlayıcı olduğundan uygulamada herhangi bir sorun yaşanmayacağı düşünülmektedir.

9. 24/7 İletişim Ağı (SSS madde 35)

Sözleşme'nin 35. maddesinde, soruşturma ve kovuşturma işlemleri sırasında taraf devletler arasında uluslararası anlık yardımın sağlanacağı, var olan polisiye ve karşılıklı yardımlaşma modellerinin ötesinde yedi gün yirmidört saat çalışan bir irtibat noktasının kurulması öngörülmüştür. Bilgisayar sistem ve verileri ile bağlantılı suçlar soruşturulması ve herhangi bir suça ilişkin elektronik ortamda

---

[369] Explanatory report, 296.

[370] Explanatory report, 297.

[371] Recommendation No. R (85) of the Committee of Ministers to Member States Concerning the Practical Applicaiton of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications, Council of Europe, (çevrimiçi) http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1985_10.pdf, 29.04.2015

bulunan delilin elde edilmesi kapsamında kurulan irtibat noktaları, taraf devletlere teknik destek sağlamak, Sözleşme'nin 29. ve 30. maddeleri doğrultusunda verileri korumak, delil toplamak, yasal bilgilendirme yapmak ve şüphelilerin yerlerini tespit etmekle görevlendirilmiştir.

Türkiye, 24/7 irtibat noktası olarak Kızılırmak Mah. Anadolu Bulvarı 2185.Sk. No: 14 06520 Söğütözü-Çankaya / Ankara adresinde faaliyet gösteren Siber Suçlarla Mücadele Daire Başkanlığı'dır. Ancak irtibat noktasının Adalet Bakanlığı bünyesinde kurulu bulunan UHDİGM olmasının daha doğru olacağı kanaatindeyiz. Taraf devletlerle sürekli adli yardımlaşma çerçevesinde ilişki içerisinde bulunan bu genel müdürlük karşılıklılık ilkesi uyarınca yardım talebine nasıl karşılık verileceği konusunda daha fazla kurumsal tecrübe ve hafızaya sahiptir. Ayrıca UHDİGM, polis teşkilatına göre, adli makamlarla daha kolay iletişime geçecek ve süreci hızlandırabilecektir.

VII. SONUÇ

Budapeşte Sözleşmesi, siber suçlarla mücadelede eksik yanları bulunan bir sözleşmedir. Ondan mükemmeli yakalaması da beklenmez. Hazırlanması aşamasında bir araya gelen taraflar her konuda anlaşmaya varamamışlar ve üzerinde anlaşmaya varılamayan konular zamana bırakılmıştır. Buna rağmen Sözleşme, devletlerce siber suçlarla mücadelede üzerinde en çok mutabakata

varılan ve devletlerin asgari ortak noktalarda bulaşabildiği bir hukuk metni olarak karşımızda durmakta ve bu haliyle alanında yapılanların en iyisi olarak kabul edilmektedir.

Bir adet bilgisayarın bulunduğu yer bile artık siber suçların etki alanındadır. Bilgi topluma olma hedefinde olan ve bilgi teknolojilerinin her çeşidine sahip Ülkemiz de doğal olarak siber saldırılardan muaf değildir ve artan bir oranla siber suçlar her gün işlenmektedir. Bu suçlar tamamen Ülkemizde işlendiği gibi bazen kısmen Ülkemizde işlenmektedir. Yani Ülkemiz bazen işlenen suçlarda tamamen yetkili ve görevli iken bazen de işlenen suçlarda kısmen yetkili ve görevli olmaktadır. Siber suçlar açısından bu şu anlama gelmektedir: siber suçlar devletler gibi sınır tanımaz. Ancak devletler uluslararası kurallar gereği sınır tanımak ve birbirlerinin egemenlik haklarına saygı göstermek zorundadır. Siber suçlular açısından bir avantaj olan bu durum devlet açısından bir dezavantajdır. Bu noktada uluslar üstü akıl, Budapeşte'de siber suçlarla ulusal ve uluslararası düzeyde mücadele etmek için içerisinde maddi ceza hukuku, ceza usul hukuku ve uluslararası işbirliğine dair ilkelerin yer aldığı referans bir sözleşme metni oluşturmuştur. Türkiye ise bu Sözleşme'ye geç olsa da taraf olmuştur. Bu gerçekten de siber suçların etkin bir şekilde soruşturulması, siber suçluluğun ortaya çıkarılması, siber suçluların yakalanması ve yargılanması adına Ülkemiz adına çok önemli bir hamledir. Böylece hem ulusal düzeyde yapılacak mücadelede modern ve kullanışlı suç tanımları ve koruma tedbirleri ile bir yeni bir yaklaşım edinildi hem de uluslararası düzeyde suçun yurt dışı bağlantılarının da ortaya konulması için hukuki bir zemine kavuşuldu.

Sözleşme'ye taraf olmak Ülkemiz adına olumlu bir adımdır. Ancak yukarıdaki bölümlerde görüldüğü üzere, Sözleşme her ne kadar uluslararası metinlere atıflar yapsa da bu onun güvenlik ön planda görüntüsünü değiştirmemektedir. Gerçekten de Sözleşme çok müdahaleci hükümler içermektedir. Bu hükümler kötüye kullanıma açıktır. Bu durum henüz Avrupa müktesebatına uyum sürecini tamamlamamış ve insan hak ve özgürlüklerinin ihlal edilmesi nedeniyle AİHM tarafından aleyhine kararlar verilen Ülkemiz açısından

daha kaygı vericidir. Bu nedenle Avrupa Konseyi tarafından üretilen bu metin Avrupa hukuku içerisinde bir parça olarak görülmeli ve Sözleşme tek başına ele alınmamalıdır. Sözleşme'de yer alan bir hüküm, içerisinde yer aldığı Avrupa hukuku ile birlikte değerlendirilerek uygulanmalıdır. Zaten daha önce de değinildiği üzere Sözleşme'nin bağımsız bir şekilde uygulanma iddiası da yoktur. Somutlaştıracak olursak, Sözleşme, İHAS ve 1981 tarihli Avrupa Konseyi Kişisel Nitelikteki Verilerin Otomatik Olarak İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair Sözleşmesi'den ayrı düşünülemez ve onlardan bağımsız bir şekilde uygulanamaz. Sözleşme, bilgisayar verisi gibi geniş bir ifadeyle doğrudan olmasa da -açıklayıcı rapordan anlaşılacağı üzere- dolaylı olarak hizmet sağlayıcıları kişilere ait verileri toplamaya zorlamaktadır. 1981 tarihli Sözleşme ile kişisel veriler ve İHAS ile temel hak ve özgürlükler korunurken siber suçlarla mücadele edilmelidir. Fakat Ülkemiz İHAS'a taraf iken 1981 tarihli Sözleşmeye taraf değildir.

Tarafı olduğumuz İHAS ve üzerimizde bağlayıcı kararlar veren İHAM ile Anayasa Mahkemesi'nin aşağıda belirtilen kararları bu sorunu çözerken önemli fikirler vermektedir.

Mahkeme, K.U. ve Finlandiya[372] kararında önemli tespitler yapmıştır. Karara konu olayda, 12 yaşındaki bir çocuğun kişisel ve fiziksel verileri kullanılmak suretiyle kendi yaşında ya da daha büyük bir erkekle ilişki yaşamak istediği yönünde mağdurun bilgisi ve rızası dışında internet üzerinden bir reklam yayımlanmış, mağdurun babası reklamı kimin internete koyduğuna dair başvurusu yerel mahkeme tarafından o tarih itibariyle telekomünikasyon yoluyla iletişimin tespitine izin veren yasal bir düzenleme olmadığı için reddedilmiş, daha sonra bu ret kararı temyiz mercii tarafından onanmıştır. Mahkeme, İHAS'ın 8. maddesinde düzenlenen "özel yaşama ve aile yaşamına saygı hakkı" bağlamında konuyu ele alarak, hak ihlali yapıldığına dair karar vermiştir. Mahkeme, vermiş olduğu kararın 49. paragrafında, ifade özgürlüğünün ve iletişimin gizliliğinin önemli ve saygı gösterilmesi gereken haklar olduğunu, ancak bu hakların mutlak olmadığını,

[372] C K.U. v Finland, Başvuru no: 2872/02, 02.03.2009

düzensizlik ve suçun önlenmesi ve başkalarının hak ve özgürlüklerinin korunması gibi meşru gerekçelerle bu haklardan vazgeçilebileceğini, olay tarihi itibariyle Finlandiya'nın bir pozitif yükümlülük olarak böylesi bir yasal çözüm sunamadığı için hak ihlalinde bulunduğunu belirtmiştir. Görüldüğü üzere, devletler üzerine özel yaşamı ihlal eden kişinin yakalanması için bir sorumluluk yüklenmekte ve devletlerin bu sorumluluk nedeniyle hizmet sağlayıcıları şüphelilerin tespiti için gerekli bilgileri teslime zorlayacak yasal düzenlemeleri yapmaları gerekmektedir. Bu husus Sözleşme'de üretim emrine karşılık gelmektedir.

Diğer taraftan Mahkeme, Yıldırım v. Türkiye kararında[373], Türkiye aleyhine İHAS'ın 10. maddesinde düzenlenen "ifade özgürlüğü" hakkının ihlal edildiği kararını vermiştir. Karara konu olayda, Telekomünikasyon İletişim Başkanlığı, Atatürk'ün anısına hakaret edildiği gerekçesi ile bir yerel mahkemenin vermiş olduğu karara istinaden hakaret ile ilgisi olmayan başvurucunun da websitesinin bulunduğu "Google Sites" isimli yer sağlayıcısı sitesine erişimi tamamen engellemiştir. Mahkeme, vermiş olduğu kararın 48 ve 50. paragraflarında, İnternetin erişilebilirliği ve çok miktarda bilgiyi depolama ve iletme özelliği nedeniyle kamunun habere erişmesinde ve bilginin yaygınlaşmasını kolaylaştırmada önemli rol oynadığını hatırlatarak, ifade özgürlüğünün sadece bilginin içeriğini değil aynı zamanda bilginin yaygınlaşmasını sağlayan araçları da koruduğunu belirtmiştir.

Bu karara paralel olarak, Anayasa Mahkemesi, bir kamu idaresi olan TİB tarafından twitter.com isimli siteye erişimin tamamen engellenmesinin hak ihlali olarak görüldüğü 02/04/2014 tarihli kararında,[374] kararın 41. paragrafında ifade özgürlüğüne getirilecek sınırlamaların zorunlu ya da istisnai tedbir niteliğinde, başvurulacak en son çare ya da alınabilecek en son önlem olması gerektiği belirtilmiş, sınırlamalar İHAM tabiriyle "zorlayıcı bir sosyal ihtiyacın" varlığına bağlanmıştır.

[373] Yıldırım v. Türkiye, başvuru no: 3111/10, 18/03/2013
[374] Anayasa Mahkemesi, başvuru no: 2014/3986, 02/04/2014

Trafik bilgilerinin TİB tarafından toplanmasına dair 5651 sayılı Yasa'nın 3. maddesinin 4. fıkrasının ve milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerine bağlı olarak gecikmesinde sakınca bulunan hallerde TİB başkanının talimatı üzerine 4 saat içinde erişimin engellenmesine dair aynı yasanın 8. maddesinin 16. fıkrasının Anayasa Mahkemesi tarafından iptali de konumuz açısından önemlidir.[375] Bu kararda, trafik bilgilerinin kişisel veri kavramı içerisinde yer aldığı, bu verilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olması temel hak ve özgürlüklerin doğrudan ihlaline neden olacağı gerekçesi ile yasanın 3 maddesinin 4. fıkrasını iptal edilmiştir. Yargıya bile sınırları belli ve ölçülülük ilkesi gereğince kademeli olarak kullanılmak üzere verilen erişimin engellenmesi yetkisinin amaç-araç dengesine ve ifade özgürlüğü, haberleşme özgürlüğü ve düşünce ve ifadeyi yayma özgürlüğüne aykırı şekilde TİB'e herhangi bir sınırlama ve kademelendirme yapılmaksızın verilemeyeceği gerekçesi ile de yasanın 8. maddesinin 16. fıkrası iptal edilmiştir.

Görülmektedir ki, siber suçlarla mücadeleye yaklaşım haklar ve özgürlükler temelinde yapılmaktadır. İdarenin keyfiliğine izin vermeden, siber suçlarla yargısal denetim altında kanunilik ve ölçülülük ilkeleri doğrultusunda mücadele sürdürülmelidir. Kamu güvenliği, suçun önlenmesi gibi değerler ile hak ve özgürlüklerin çatışması halinde bu konu tartışılmalı ve denge yakalanmalıdır. Güvenlik ön plana çekilerek hak ve özgürlükler; hak ve özgürlükler ön plana çekilerek güvenlik feda edilmemelidir. Sözleşme'nin gerek başlangıç kısmında gerekse de 14 ve 15. maddelerinde bu durum ortaya konmuştur. Aksi halde, Sözleşme uygulanırken barındırdığı müdahaleci tedbir nedeniyle hak ve özgürlüklerin ihlali ile karşılaşılacaktır. Bu ise Sözleşme'ye taraf devletlerin Ülkemiz ile adli işbirliğine yanaşmamasına neden olacaktır.

Bir diğer husus ise siber suçlara ilişkin olarak mevzuatımızın tekrar gözden geçirilerek Sözleşme ile uyumlu hale getirilmesidir. Her ne kadar yapılan yorum ve elverdiği ölçüde kıyaslarla Sözleşme'de yer alan hükümlerle ilgili başlıklar altında

[375] Anayasa Mahkemesi, 2014/149 E – 2014/151, 02/10/2014

mevzuatımızın benzer olduğu söylense de, bunun yeterli olmadığı açıktır. Bu nedenle acil bir şekilde gerekli yasal düzenlemelerin yapılarak Sözleşme ile ve Sözleşme'nin parçası olduğu hukuk ile paralel bir mevzuat oluşturulmalıdır. Böylece uygulamada yaşanacak sorunların önüne geçilmiş olunacaktır.

Unutulmamalıdır ki, Sözleşme siber suçlara karşı geliştirilmiş sihirli bir sopa değildir. Siber suçların önüne tamamen geçmek mümkün değildir. Trafik kazalarının önüne tüm taşıtları kaldırarak geçebiliriz, siber suçların da tüm bilgi teknolojilerinin ortadan kaldırılması ile. Bunun olası olmadığı ve artık insanlığın geri dönülmez bir yola girdiği açıktır. Bilgi teknolojileri gelişerek var olacak ve aynı zamanda siber suçlularla mücadele edilecektir. Ancak bu mücadele, vatandaşlara bir tehdit olarak dönmemelidir. Siber suçlarla mücadele yapılırken temel hak ve özgürlüklerin korunması ve kollanması gerekmektedir ve Türkiye bu iki değeri aynı anda götürecek yasal kapasite ve potansiyele sahiptir.