KARŞILAŞTIRMALI HUKUK BAĞLAMINDA BİRLEŞİK KRALLIK (İNGİLTERE) HUKUKUNDA BİLİŞİM SUÇLARI MEVZUATI VE UYGULAMASI

The Cybercrime Law and Its Practice in United Kingdom Within the Context of Comperative Law

Doç. Dr. Murat Volkan DÜLGER[1]

Geliş Tarihi: 02.02.2017 Kabul Tarihi: 24.05.2017

ÖZET

Bu makalenin konusunu karşılaştırmalı hukuk bağlamında Birleşik Krallık (İngiltere) hukukunda bilişim suçlarına ilişkin mevzuat ve bunun uygulanması oluşturmaktadır. Bu amaçla Birleşik Krallık'ta bu alanı düzenleyen temel yasalar ve bu yasalarda yer alan suç tipleri incelenmiştir. Bunun yanı sıra uygulamayı göstermek için belli bazı davalardaki savcılığın suçlaması, savunma avukatlarının savunmaları ve yargı makamlarının verdiği kararlar incelenmiştir. Bu alanda Birleşik Krallık hukukunun seçilmesinin öne çıkan nedenleri bu ülkede bilişim suçlarının sıklıkla işlenmesi ve uluslararası boyutunun olması, günlük yaşamın ve iş yaşamının büyük ölçüde bilişim sistemlerine bağlı olması ve devlet olarak bu suçlarla mücadelenin bir politika olarak seçilmesidir. Mevzuat ve uygulamadan örnekler verilirken, Anglo Amerikan hukuk sisteminin önemli bir üyesi olan Birleşik Devletler'in mevzuatı ve mahkeme kararlarına da yer verilmiştir. Sonuç olarak hem Anglo Amerikan sisteminin hem de Avrupa Konseyi'nin bir üyesi olarak bu sisteme dahil olan Birleşik Krallık'ın bilişim suçlarına ilişkin rejimi incelenerek, bu açıdan ülkemizle arada bir köprü kurulmaya çalışılmıştır.

Anahtar Kelimeler: Anglo Amerikan hukuk sistemi, Birleşik Krallık (İngiltere) hukuku, bilişim suçları, bilgisayarların kötüye kullanılması, yetkisiz erişim.

ABSTRACT

The subject of this article is the computer crime legislations and practice in United Kingdom in respect of comperative law. In this respect, the essential statuaries United Kingdom and the related offences are examined. Also the accusative arguments of prosecutors, the defence arguments of defendand's attorneys and the court decisions for certain cases are also cited in order to explain the practice in field. The reasons of choosing the United Kingdom law are, the frequency and international nature of this kind of offences in UK, the dependecy of the daily and business life on ICT systems, and existence of a Govermental policy to tackle this kind of offences in UK. When examining computer crimes legislations and practice, also legislations and court decisions of the U.S which is an important member of common law system are discussed. Consequently, the regime against the computer crimes in UK, which is both a member of the common law system and a member of Council of Europe, is examined, an in this way it is aimed to establish a law bridge (liason) beetwen UK's and Turkey's computer crimes and practices.

Keywords: Anglo American law system, common law system, the law of United Kingdom (English), cybercrimes, computer misuse, unauthorized access.

[1] İstanbul Medipol Üniversitesi Hukuk Fakültesi Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku Öğretim Üyesi, mvdulger@medipol.edu.tr

GİRİŞ

I. NEDEN BİRLEŞİK KRALLIK HUKUKU?

Aslında bu sorunun yanıtı oldukça basit: Bilgisayarın ve bilişim sistemlerinin ilk çıktığı yer Amerika Birleşik Devletleri (ABD) ve Birleşik Krallık (United Kingdom /UK); dolayısıyla bilişim hukukuna ilişkin ilk sorunların çıktığı, ilk hukuki düzenlemelerin yapıldığı, ilk soruşturmaların yapıldığı ve ilk mahkeme kararlarının verildiği ülkeler de bunlar. Benim de makalenin yazarı olarak hâkim olduğum yabancı dil İngilizce olduğu için öncelikle bu iki ülkenin hukuklarını incelemeyi tercih ettim. Özellikle Birleşik Krallık'ı seçmemin nedeni ise bir yandan bizim yabancısı olduğumuz Anglo Amerikan hukuk sistemine ait ve hatta onun kaynağı olmasına rağmen, öte yandan Avrupa Konseyi'ne ve çıkmak üzere olsa da Avrupa Birliği'ne üye olması, bunun sonucunda da bu örgütlerin yarattığı hukuk düzenlerini iç hukukunun bir parçası haline getirmiş olmasıdır. Türkiye ise bunlardan sırasıyla birine taraf diğerine aday ülke olmakla, bu anlamda bir şekilde Birleşik Krallık ile paydaştır. Dolayısıyla Türk hukuku ile farklılıklarının yanı sıra elverişli bir karşılaştırma yapabilmek amacıyla Birleşik Krallık sistemini incelemeyi tercih ettim.

Benzer çalışmalarda sıklıkla İngiltere ifadesinin anılmasına rağmen bu çalışmada Birleşik Krallık ifadesini seçmemin de bir nedeni var. Aslında İngilizce yazılmış yayınlar, bu ülkedeki mahkeme kararları veya Avrupa İnsan Hakları Mahkemesi kararları okunduğunda İngiltere için *"United Kingdom"* yani *"Birleşik Krallık"* ve bunun kısaltması olarak da *"UK"*nin kullanıldığı görülür. Bu ise devletler hukukundan kaynaklanan, yargı ve egemenlik yetkisi ile ilgili olduğu için konumuzu da ilgilendiren bir husustur.

İngiltere (England), Britanya Adası'nda bulunan ve adanın ortasında ve güneyinde yer alan bir ülkedir. Ancak aynı adanın kuzeyinde kısmen bağımsız olan İskoçya (Scotland), adanın orta batısında Galler (Walles) ve İrlanda adasının kuzeyinde bulunan Kuzey İrlanda (North Ireland) yer alır. Ülkeden ülkeye değişmekle beraber bunların içinde bulundukları statüye göre kendi parlamentosu, bakanlar kurulu ve başbakanları bulunur. Ancak bunlar Kral ya da Kraliçenin yönetiminde (hali hazırda Kraliçe II. Elizabeth) Birleşik Krallık'ı oluştururlar. Bunun üstünde ise eski Birleşik Krallık sömürgeleri olan Avustralya, Yeni Zelanda, Kanada gibi ülkelerin oluşturduğu İngiliz Milletler Topluluğu (Commonwealth) bulunmaktadır. Ancak bunlar artık bağımsız devletlerin oluşturduğu bir topluluktur.

Birleşik Krallık üç farklı yargı çevresini içerir. İngiltere ve Galler, İskoçya ve Kuzey İrlanda. Bunların üçünü birlikte ifade etmek için Birleşik Krallık (UK) kısaltması kullanılır. Bazı yasalar, örneğin 1990 tarihli Bilgisayarların Kötüye Kullanılması Yasası (Computer Misuse Act, 1990) tüm Birleşik

Krallık'ta uygulanmaktadır. Yargı çevresinden kaynaklanan farklılıklar söz konusu olduğunda ise çalışmanın odağında İngiltere ve Galler olacaktır. Aslında İngiltere/Galler, İskoçya ve Kuzey İrlanda ülkelerinin farklı yasaları, mahkemeleri ve hukuk düzenleri olması rağmen özellikle İskoçya dışındakiler birbirlerine çok benzerler. Bunun yanı sıra özellikle İngiltere hukuk sistemi son derece gelişmiştir. Bu ülkelerden herhangi birinde bir hukuk eseri yayınlandığında genellikle bu ülkelerdeki tüm yasalar ve mahkeme kararları dikkate alınır ve bunlara atıf yapılır. Hatta aralarındaki benzerlikler ve ortak geçmişleri nedeniyle ABD, Kanada, Avustralya ve Yeni Zelanda yasalarına ve mahkeme kararlarına da atıf yapılır. Ortak hukuk mirasına sahip olmanın yanı sıra, gelişmiş ekonomilere sahip olan bu ülkeler, bilişim suçlarıyla ilgili olarak kendi yasalarında önemli değişiklikler gerçekleştirmişlerdir. Hukukun gelişen bu alanında, bilişim suçlarının ortaya çıkardığı zorluklarla mücadele edebilmek için bu ülkelerin birbirlerinin deneyimlerinden öğrenecekleri çok şey bulunur[2]. İngiltere'den farklı olarak Avustralya, Kanada ve ABD'de federasyon sistemi geçerli olduğundan, çalışmamızda bu federal yasalar (federe devletlerin üzerinde tüm ülke çapında geçerli olan yasalar) dikkate alınmıştır.

Bu bağlamda Birleşik Krallık hukuk sistemi dikkate alınarak bir karşılaştırmalı hukuk çalışması yapıldığında, bir anlamda söz konusu diğer ülkeler hakkında da örnekler verilmiş ve benzeşimler kurulmuş olmaktadır[3]. Bu ülkeyi seçmemin bir diğer önemli nedeni de budur.

Makalede diğer kaynaklar, mahkeme kararları ve diğer uluslararası mevzuat ve içtihat ile uyumu sağlamak adına özgün dildeki United Kingdom'ın karşılığı olan Birleşik Krallık ifadesini; Birleşik Krallık hukukunda yer alan yasa isimlerinin ya da çeşitli kurum ve kuruluşların adlarının kısaltılmasında ya da mahkeme kararlarında ise United Kingdom'ın İngilizce kısaltması olan "UK"yi kullanacağım.

Birleşik Krallık Hukukunun bilişim suçlarına ilişkin düzenlemeleri ve uygulamalarını aktarmaya ve açıklamaya geçmeden önce, konunun daha iyi anlaşılması için öne çıkan kavramları ve suç politikasının belirlenmesinde etkili olan süreç ve düşünceleri de aktarmaya çalışacağım. Bu nedenle ilk sayfalar adeta bir giriş niteliğinde olacak.

---

[2] Jonathan Clough, Principles of Cybercrime, Second Edition, Cambridge, Cambridge University Press, 2015, s. 27.

[3] Birleşik Krallık hukuk sisteminin bütünü hakkında bilgi için bkz: Alisdair A. Gillespie, The English Legal System, 5th Edition, Oxford, Oxford University Press, 2015, s. 1 vd.; Catherine Elliott, English Legal System Essential Cases and Materials, Second Edition, Harlow, Pearson Longman, 2009, s. 3 vd.; Stefan Fafinski/Emily Finch, English Legal System, 3rd Edition, Harlow, Pearson Longman, 2010, s. 1 vd.; Catherine Elliott/Frances Quinn, English Legal System, Eleventh Edition, Harlow, Pearson Longman, 2010, s. 11 vd.; Jacqueline Martin, English Legal System: Key Facts Key Cases, London and New York, Routledge, 2014, s. 1 vd.

Son olarak bu çalışmanın tüketici bir çalışma olmadığını (Birleşik Krallık hukukçularının kendileri dahi herhangi belli bir konuyu tam olarak tüketmekte zorlanmaktadırlar) belirterek okuyucuların makalemi yalnızca örnek çalışma; ufkumuzu açmak, olumlu ve olumsuz yanlarımızı görerek ders çıkarmak için bir basamak olarak görmelerini dilerim.

II. TEKNOLOJİNİN KONUSU VE TERMİNOLOJİ

A. Sanal Ağların Önemi

Sanal ağlar (internet, intranet, LAN vb.) günümüzde bilişim suçları ile ilgili bir düzenlemenin veya çalışmanın temel konularından birini oluşturur. Bu temel, yalnızca bilgisayarlar için sanal ağların alt yapıyı oluşturmasından değil; bilgisayarlara güç vermek için elektriğin gerekli olduğu gibi, sanal ağların bilgisayarlar için bir teknolojik fenomen olmasından da kaynaklanır[4]. Dolayısıyla UK hukukunda yer alan bilişim suçlarına ve bunların soruşturma ve kovuşturmasına ilişkin düzenlemelerin tamamında sanal ağlar dikkate alınmıştır.

B. Kişisel Verilerin Önemli Bir Bileşen Olması

Birleşik Krallık açısından kişisel veriler, bunların korunması ve bunlara karşı işlenen suçlar bilişim hukukunun önemli bileşenlerinden birini oluşturur. Bu nedenle bu konu hakkında da bazı açıklamalar yapmak gerekir. Avrupa veri koruma hukukunun "kişisel bilgi" (personal information) yerine "kişisel veri" (personel data) terimini kullanmasının tek bir nedeni vardır: Mahremiyete yönelik tehditler; işlenmemiş, yığın halindeki verilerin bireylerle bağlantılı hale getirilmeden (kişiselleştirilmeden) kullanılmasıyla birlikte başlar, dolayısıyla hukuk da daha bu ilk aşamada konuyla ilgilenmeye başlamalıdır. Bu nedenle henüz belirli bir bilgi olmadan, bireyi tanımlayabilecek bir bilgi kırıntısı düzeyindeki verinin varlığı halinde dahi bu veri koruma hukukunun kapsamında olmalıdır. Bu nedenle kişisel veri kavramı tercih edilmiştir[5].

Bundan hareketle Birleşik Krallık hukukunda da bu alanda kullanılan terminoloji hem bu gerekçeyle hem de bu alandaki uluslararası mevzuatla uyumlu olabilmek adına "kişisel veri" olarak belirlenmiştir.

C. Yasa ile Yapılan Tanımların Potansiyel Bir Dezavantaj Oluşturması

Teknolojik gelişmeler için yasa ile yapılan tanımların potansiyel bir dezavantajı görülür: Tarihin belli bir anında kabul edilmiş ve politik uzlaşmayla yasalaşmış tanımlar kullanışlı değildir. Buna karşın, herhangi bir tanımın yokluğu halinde, bir "bilgisayar" ile karşılaşıldığında bunun

[4] Ian Walden, Computer Crimes and Digital Investigations, Second Edition, Oxford, Oxford University Press, 2016, pn. 1.05.

[5] Walden, pn. 2.12.

mahkemeler tarafından tanımlanması gerekir. Kablosuz taşınabilir cihazların gelişmesi (örneğin, akıllı cep telefonları), birçok bireyin bilgisayar hakkındaki tanımlamasıyla uyuşmaz. Televizyonlardan çamaşır makinelerine kadar genel olarak "Nesnelerin İnterneti" (Internet of Things / IoT) olarak adlandırılan nesnelerin içine yarı iletken ciplerin entegre edilmesi süreci, bunların birer bilgisayar olarak kabul edilmesi ve bu nesnelerin yetkisiz kullanılması halinde cezalandırmanın sınırlarının genişletilmesine yol açmıştır. Geleceğin taşınabilir cihazlarına internet iletişimi sağlayacak sistemlerin gömülmesi, bir yandan uzaktan kontrol edilebilir nesnelerin işlevselliğinin artırılması olasılığının habercisi olurken, diğer yandan yeni tür suç aktivitelerinin de ortaya çıkmasına yol açacaktır[6]. Dolayısıyla bilgisayar, veri ya da ağ gibi terimler arasında kesin ve net bir çizgi çizmek, bunları açık ve çerçevesi belirli bir biçimde tanımlamak mümkün değildir[7]. Yapılacak her tanım içerisinde eksikler barındıracağı gibi, bugün için geçerli olan tanım, bu makaleyi altı ay sonra okuyacaklar için ya yetersiz olacak ya da geçerli olmayacaktır[8].

Örneğin, bilişim hukuku hakkındaki eserlerde yer alan tartışmaların çoğunu, geleneksel hukuki metinlerde yer alan terimlerin bilişim hukuku alanına uygulanmaya çalışılması oluşturur. Örneğin, ABD'de yürürlükte bulunan Çocukların Online Yayınlardan Korunması Yasası'nda (The Child Online Protection Act – COPA) ağların ağı olan internet yalnızca "World Wide Web" olarak tanımlanmıştır. Bu tanımlama günümüz teknolojisi karşısında çok dar ve bir alana özgülenmiş olması nedeniyle eleştirilmektedir· Dolayısıyla teknoloji alanındaki gelişmelerin çok hızlı olması nedeniyle belli bir teknolojik ortama yönelik yasa ile yapılan tanımlama girişimleri birkaç yıl içinde eskir ve işlevsiz kalır[9]. Bu nedenle Birleşik Krallık hukukunda bu tür aygıtların ya da bileşenlerin kesin bir biçimde tanımlanmasından kaçınılmıştır. Benim de katıldığım ve doğru bulduğum bu bakış açısı ülkemiz mevzuatı açısından da geçerlidir. Hatta ülkemiz bir adım daha öne geçerek "bilişim sistemleri" kavramını kullanarak her yeni gelişmeyi ve aygıtı kapsayabilecek bir düzenleme yapmıştır.

D. Adlandırma Sorunu: Bilgisayar, Bilişim ya da Siber Suçlar mı?

"Teknolojinin olanaklı kıldığı suçların kapsamı daima gelişmektedir, bu gelişim hem teknolojik değişimin fonksiyonları hem de yeni teknolojilerle sosyal etkileşim açısından olmaktadır"[10].

---

6 Walden, pn. 2.17.

7 Walden, pn. 2.19.

8 Bilgisayarın ve bilişim sistemlerinin tanımı hakkında ayrıntılı bilgi için bkz: Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 6. Bası, Ankara, Seçkin Yayıncılık, 2015, s. 63 vd.

9 Walden, pn. 2.23.

10 Lawrence Lessig, Code and other Laws of Cyberspace, New York, Basic Books, 1999, s. 85-99.

Çalışma konumuzun tanımlanması yalnızca klasik hukuk tekniği ile sınırlı değildir, bunun yanı sıra söz konusu tanımlama kritik hukuki analizlerin yapılmasında bize "temel bir düşünsel araç"[11] olarak adlandırma ve plan oluşturmada yardımcı olacaktır[12].

Bilişim suçlarının işlenme biçimlerinin sayısı kadar bu suçları tanımlayan terimler de bulunur[13]: "Bilgisayar suçları / computer crime", "bilgisayar ile ilgili suçlar / computer-related crime" ya da "bilgisayarlar tarafından işlenen suçlar / crime by computer" gibi terimler erken dönemde kullanılmıştır[14]. Dijital teknolojilerin daha yaygın hale gelmesiyle birlikte, sözlüğe "ileri teknoloji / high technology" suçları gibi terimler de eklenmiştir[15]. İnternetin ilerleyişi bizlere "siber suçlar / cybercrime" ve "internet" veya kısaca "net" suçları terimlerini de getirmiştir[16]. Bunlardan başka "dijital", "elektronik" (ya da kısaca e-), "virtüel", "IT", "ileri tek / high-tech" ve "teknoloji sayesinde / technology enabled" suçlar gibi terimleri de kullanılmıştır[17].

Bu sözcükler tam manasıyla (sözlük anlamıyla) alınırsa, her terim içerisinde bir veya birden fazla eksikliği barındırır. Bilgisayara odaklanan terimler "ağları" içermezler. Siber suçlar veya sanal suçlar gibi diğerleri ise yalnızca internete odaklanmış olarak görülürler. Dijital, elektronik veya ileri teknoloji suçları gibi terimler ise anlamını yitirecek kadar geniş görünürler. Örneğin, ileri teknoloji suçu, nanoteknoloji ya da biyomühendislik gibi diğer ileri teknoloji gelişmelerini içerecek kadar ağa dayalı bilgi teknolojilerin ötesine gidebilirler[18].

Bu nedenle bu terimlere sözlük anlamıyla yaklaşılmamalıdır; zira bunlar sözlük anlamından ziyade suçun işlenmesinde teknolojinin rolünü vurgulayan geniş anlamda betimleyici terimlerdir. Bununla birlikte henüz hiçbir terim

---

11 "Basic intellectual tool" kavramı için bkz: Jeremy Horder, "The Classification of Crimes and the Special Part of the Criminal Law", Defining Crimes: Essays on The Special Part of the Criminal Law, Ed: R. A. Duff/Stuart P. Green, Oxford, Oxford University Press, 2005, s. 21.

12 Walden, pn. 2.26.

13 Alisdair A. Gillespie, Cybercrime: Key Issues and Debates, London and New York, Routledge, 2016, s. 1.

14 House of Commons Standing Committee on Justice and Legal Affairs, Computer Crime, Final Report, 1983, s. 12; Donn B. Parker, Crime by Computer, New York, Scribner, 1976, s. 1 vd; Ulrich Sieber, Legal Aspects of Computer – Related Crime in the Information Society - COMCRIME Study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf; 25.11.2016, s. 1 vd.

15 Susan W. Brenner, "Cybercrime Metrics: Old Wine, New Bottles?", Virginia Journal of Law and Technology, Vol. 9, No. 13, Fall 2004, s. 4.

16 Sheridan Morris, The Future of Netcrime Now: Part 1 – Threats and Challenges, Home Office Online Report 62/04, 2014, s. vi.

17 Clough, s. 9,10; Gillespie, Cybercrime, s. 1.

18 Morris, The Future of Netcrime, s. vi; Clough, s. 10. Ayrıca bkz: Susan W. Brenner, "Nanocrime?", University of Illinois Journal of Law, Technology and Policy, No. 1, 2011, s. 39-105.

gerçek anlamda bu alanın tamamını kapsayan ve tam anlamıyla açıklayıcı bir terim haline gelmemiştir. Bu nedenle terimlerin çoğu birbirlerinin alternatifi olarak kullanılırlar.

Bu bağlamda, örneğin bilişim hukuku alanında önemli bir isim olan Avustralyalı hukukçu Prof. Dr. Brian Clough kitabında şu nedenlere dayanarak "siber suç" terimini kullanmıştır: İlk olarak bu terim öğretide ve edebiyatta yaygın olarak kullanılmaktadır[19]. İkinci olarak bu, yaygın olarak kullanılan bir terim haline gelmiştir[20]. Üçüncü olarak, bu terim ağa bağlı bilgisayarların önemini vurgulamaktadır. Dördüncü olarak, bu terim uluslararası alanda tanınmakta ve kullanılmaktadır; Birleşmiş Milletler tarafından[21] ve Avrupa Konseyi Siber Suçlar Sözleşmesi tarafından kullanılan bir terimdir[22].

Bilişim hukuku alanında bir başka önemli isim olan İngiliz hukukçu Prof. Dr. Ian Walden, "siber suçlar" kavramının, "bilgisayar suçlarının" alt kümesini oluşturduğunu, bu alandaki dikkatin ise daha geniş bir alana yöneltilmesi gerektiğini ifade eder. Ancak yine de bilgisayar suçları (computer crimes) ile siber suçları (cyber crimes) eş anlamlı olarak kullanır[23]. Oysa ben tam tersine "bilgisayar suçları" kavramının "siber suçlar" kavramının alt kümesini oluşturduğunu düşünmekteyim. Ancak Walden ve Walden'ın görüşünü haklı bularak buna atıf yapan İngiliz hukukçu Prof. Dr. Alisdair A. Gillespie, bunun bilinçli ve doğru bir tercih olduğunu şu şekilde ifade etmektedirler: *"Herhangi bir bilgisayar siber alana bağlı olmak ihtiyacında değildir (bizim konumuz açısından internete), dolayısıyla bir internet suçuyla ilgileniyorsak, bazı bilgisayar suçları bununla ilgili olmakla birlikte, aslında buna bağlı olarak bilgisayar suçundan daha dar bir alanla ilgileniyoruz demektir. Benzer biçimde "dijital" ve "ileri teknoloji" suçlarının, "e-suçlar" ya da "siber suçlar" da olduğu gibi mutlaka internete bağlı olmayı gerektirmeyen daha geniş kapsamlı suçlar olduğu söylenebilir"*[24]. Gillespie bu tanımlamayı şu örnekle daha iyi açıklamaktadır: *"A gizlice bir ofise girer ve B'nin bilgisayarından gizli bilgileri bir USB hafıza kartına aktarır. Sonrasında bu bilgileri B'nin rakibi olan C'ye satar. Bunun bir siber suç olması mümkündür –A'nın B'nin ofisine gizlice girmek yerine B'nin bilgisayarının bilişim güvenliğini kırması ve verileri aktarması halinde–*

---

19 Ayrıca terim, (seyrek de olsa) mevzuatta da görülmektedir, bkz: the Cybercrime Act 2001.

20 Oxford İngilizce Sözlüğü "siber suçu", "bilgisayar ya da internet kullanılarak işlenen suç ya da suçlar" olarak tanımlamaktadır, Oxford English Dictionary Online, Oxford University Press, December 2014.

21 United Nations Office on Drugs and Crime, Comprehensive study on cybercrime, 2013.

22 Clough, s. 10.

23 Walden, pn. 2.26.

24 Gillespie, Cybercrime, s. 1; Paul Hunton, "The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model", Computer Law and Security Report, Vol. 25, 2009, s. 529.

buna rağmen A internete bağlanmamıştır. Bütün işlemleri ağa bağlanmadan (offline) gerçekleştirmiştir". Dolayısıyla soruşturmacılar da olayı aynı şekilde incelemek durumundadırlar (polislerin kendi çalıştıkları birimin adını "siber suçlardan" ziyade "ileri teknoloji suçları" olarak kullanmamalarının nedeni de budur). Böyle bir olaya ilişkin soruşturma sonucunda yapılacak iddia faaliyeti de aynı şekilde yapılacaktır. Dolayısıyla bu tür olaylar için tam olarak siber suç denmesi olanaklı değildir[25].

Terminolojideki tüm bu farklılıklar, bunların neleri kapsadığı konusunda artık bir uzlaşmaya varılmıştır. Siber (bilişim) suçların iki ilke kategorisi, *"sibere bağlı/cyber-dependent"* ve *"siber sayesinde/cyber-enabled"* işlenen suçlardır[26]. Sibere bağlı suçlar, *"yalnızca bir bilgisayar, bilgisayar ağı ya da bir başka tür ICT kullanılarak işlenebilen"* suçlardır[27]. Bunlar sıklıkla bilişim yazılımları, kötücül yazılımlar veya DoS atakları gibi, teknolojinin suç aktivitelerinin hedefinde olduğu suçlarla ilgilidir[28].

Siber sayesinde suçlar ise, *"bilgisayarlar, bilgisayar ağları ya da bir başka tür ICT kullanılarak işlenen ya da* işlenme oranı artan geleneksel *suçlardır"*[29]. Örneğin, çocuk pornografisi, takipçi tacizci (stalker), fikri mülkiyet hırsızlığı ya da dolandırıcılık gibi. Bu suçların failleri de yaygın bir biçimde teknolojiyle ilgilenmekle birlikte, sibere bağlı suçlardan farklı olarak bu suçların bilişim teknolojileri olmadan da işlenmeleri mümkündür[30].

Üçüncü bir kategori ise *"bilgisayar destekli suçlardır / computer suported"*[31]. Bu suçların işlenmesinde bilgisayarın kullanılması rastlantısaldır, ancak bunlar suça ilişkin önemli deliller sağlayabilirler. Örneğin, bir cinayetin şüphelisinin adresi bilgisayarda bulunabilir ya da cinayet öncesinde failin ve mağdurun birbirlerine gönderdikleri mesajların kayıtlarının bilgisayarda bulunması mümkündür. Bu tür davalarda teknoloji suçun işlenmesi için önemli bir etken değildir, ancak delillerin bulunması için önemli bir etken ve zengin bir kaynaktır[32].

---

25 Gillespie, Cybercrime, s. 3.

26 Mike McGuire/Samantha Dowling, Cyber Crime: A Review of the Evidence, Research Report 75, Summary of Key Findings and Implications, Home Office, October 2013, s. 5.

27 McGuire/Dowling, s. 5.

28 Clough, s. 10, 11.

29 McGuire/Dowling, s. 5.

30 Clough, s. 11.

31 Melaine Kowalski, Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics, Cat. No. 85-558-XIE, Canadian Centre for Justice Statistics, 2002, s. 6.

32 Computer Crime and Intellectual Property Section, The National Information Infrastructure Protection Act of 1996, Legislative Analysis, US Department of Justice, 1998; Clough, s. 11.

Bu sınıflandırma ya da bunun varyasyonları[33]; Avustralya[34], Kanada[35], Birleşik Krallık[36] ve ABD[37]'de benimsenmiştir. Bu sınıflandırma ayrıca bir soruya da işaret etmektedir: Bilişim suçları tamamıyla yeni tür suçlar mıdır yoksa basitçe eski suçların yeni işleniş biçimleri midir?[38] Aslında cevap her ikisidir. Çalışmamızda tartışma konusu yaptığımız bilişim suçlarının büyük bir çoğunluğu yeni biçimlerde işlenen eski (klasik) suçlardır. Gerçek bilişim suçları, bilgisayarlara ve bilgisayar ağlarının kendisine karşı gerçekleştirilen ve bilgi işlem olmaksızın var olması olanaklı olmayan suçlardır[39].

Görüldüğü üzere Anglo Amerikan hukuk sistemlerinde ve hatta Kıta Avrupası hukuk sistemine ait bazı ülkelerde[40], "cybercrime" yani "siber suçlar" terimi yerleşmiş durumdadır. Ancak ben bunun yerine Türkçe bir kavram olan ve ülkemizde hem öğretide hem de mevzuatta yaygın bir biçimde kullanılan "bilişim suçları" kavramının kullanılmasının ülkemiz öğretisi ve uygulaması açısından daha uygun olduğunu düşünmekteyim. Buna karşın Anglo Amerikan kaynakları incelenirken, hala pek çok kaynakta "computer crimes / bilgisayar suçları" kavramının da kullanılmasının nedeni, bunun eski kullanımlara bağlılığın yanında, bazı yazarlar tarafından bunun daha kapsayıcı bir kavram olduğunun düşünülmesinden kaynaklandığını da belirtmeliyim[41].

Yukarıda yapılan açıklamalardan görüldüğü üzere, bilişim suçlarının sınırlarının açıkça belirlenmesi, diğer benzer konulardan ayrımının açıkça ortaya konulması mümkün değildir. Buna ek olarak, suç oluşturan bir hareket genellikle aynı anda birkaç farklı türdeki suç tipiyle uyuşmakta ya da aynı anda başka suçlarla birlikte bir suç serisinin parçası olarak işlenebilmektedir. Bu alandaki bir isimlendirme ya da sınıflandırma çalışmasının amacı, bu alanın olduğu gibi tanımlanmaya kalkışılmasından ziyade, siber uzayda hali hazırda gerçekleşen farklı türdeki suç aktivitelerinin etkin bir biçimde incelebilmesi için bir çerçeve sağlanmasıdır[42].

---

33 Söz konusu sınıflandırmalar hakkında ayrıntılı bilgi için bkz: Gillespie, Cybercrime, s. 3-8.

34 Attorney General's Department (Australia), National plan to combat cybercrime, 2013, s. 4, 5.

35 Kowalski, s. 6.

36 McGuire/Dowling, s. 5.

37 Computer Crime and Intellectual Property Section, The National Information Infrastructure Protection Act of 1996.

38 Brenner, Cybercrime Metrics, s. 15

39 Clough, s. 11.

40 Örneğin bkz: Eddy Willems, Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können, Wiesbaden, Springer Vieweg, 2015, s. 1 vd.

41 Dülger, s. 77-80.

42 Walden, pn. 2.46.

III. TARİHÇE

Aslında insanların teknolojik gelişmeleri suç işlemede araç olarak kullanmalarının tarihi oldukça eskilere dayanır. Basit bir tarih okuması bizlere teknoloji ile suç arasındaki ilişkinin yeni olmadığını ve teknolojik gelişmelerin getirdiği faydalı kullanımların yanı sıra bunlar kullanılarak zarar verme potansiyelinin, getirmiş olduğu faydalara çok da uzak olmadığını gösterir. Bununla birlikte, her ne kadar teknolojik fikirler ve donanımlar zamanla değişikliğe uğrasalar da birçok temel suç işleme düşüncesi aynı kalmıştır. Özellikle teknolojinin yarattığı güvenin kullanılarak suç işlenmesi düşüncesi hala geçerlidir. 19. yüzyılda ilk telgraf sistemleri kullanılarak işlenen bazı dolandırıcılık suçları ile günümüzün modern bilişim –korsanlık– suçları arasında esrarengiz bir benzerliğin bulunduğu görülür. Suç ve teknoloji arasındaki bu uzun süreli ilişki, her ne kadar kolay olmasa da, aynı zamanda suçtan korunma ve güvenlik kavramları için de söylenebilir. Örneğin; Mısır piramitlerinin mimarisi, mezar soyguncularının önlenmesi için yüksek düzeyli güvenlik teknolojilerinin kullanılmasını gerektirmiştir. Birkaç küçük yanlış adımın atılması ya da hareketin yapılması mezarın kapısının sonsuza kadar kapanmasına yol açmaktaydı. Bu sistem, günümüzün havaalanlarında normal dışı hareketliliğin takip edilerek potansiyel terörist aktivitelerin tespit edilmesinde kullanılan yöntemlerin benzeridir. Yine telgrafla ilgili olarak, icadından kısa bir süre sonra suçluların yakalanmasında kullanıldığı bilinmektedir. Bir katil olan John Tawell, 1845'teki infazından dakikalar önce bu durumu ifade etmiştir; zira kendisi metresini öldürdükten sonra trenle Londra'ya gitmek üzere yol çıktığında, Tawell hakkındaki bilgi telgrafla polis merkezlerine bildirilmiş ve kendisi Londra'ya vardığında polis tarafından yakalanarak gözaltına alınmıştır[43].

Bugün de suçlular ile soruşturma makamları arasındaki "kedi – fare oyunu" geçmişte olduğu gibi devam etmektedir. Suçlular yeni teknolojiler üretir ve kullanırlarken, soruşturma makamları da onların seviyesini yakalamaya ve suçların soruşturulması, tespiti ve önlenmesi için aynı teknolojileri kullanmaya çalışmaktadırlar. Günümüzün modern zamanlarında değişen asıl husus, küresel bir iletişim sistemiyle birbirine bağlı olarak kişisel bilişim sistemlerinin (bilgisayarların) kullanımının ortaya çıkması ve artmasıdır. Zararlı hareketlerin oluşumu ve esastan değişimine ilişkin zaman aralığı, söz konusu ağın oluşumu ile son derece kısalmıştır. Özellikle dikkate alınması gereken husus ise, bir bilişim suçunun işlenmesi için gereken zaman, bilişim suçu dalgası için gereken zamana dönüşmüş ve yıllar ve aylardansa, saatler ve dakikalar konuşulmaya başlanmıştır. Sonuç olarak, bugün bilişim sistemleri ve ağ teknolojileri basitçe "çarpan etkisi yaratan bir güç" olmanın ötesine geçmiştir. Suçun işlenmesinin,

[43] David S. Wall, Cybercrime: The Transformation of Crime in the Information Age, Cambridge, Polity Press, 2014, s. 2.

soruşturulmasının ve önlenmesinin küresel çapta paylaşılması artık yalnızca bir düşünce değildir; ancak bunun gerçekleşmesi yüksek düzeyde bilgisayar gücü gerektirmektedir. İşte bunların gelişmesi son derece hızlı bir şekilde olmakta, bilişimdeki hız bu alanın en önemli belirleyici özelliklerinden birini oluşturmaktadır. Nitekim Moore'un hesaplamasına[44] göre bir internet yılı yaklaşık olarak normal bir takvim yılına göre üç ay ya da daha az bir süreye denk gelmektedir[45]. İşte aşağıda yer alan kronolojik sıralama bu bilgiler ışığında değerlendirilmelidir.

Birleşik Krallık'ta ve Anglo Amerikan hukuk sisteminde yer alan ülkelerde bilişim suçları ve bilgisayarlar hakkında ciltler dolusu kitap ve makale bulunur. Bu yayınların tarihi 1970'lerden itibaren başlar. Bu alanda İngiltere'de yayınlanan ilk kitap *"Gerald McKnight, Computer Crime, Walker and Co., 1973"* tarihli eserdir[46].

İngiliz bilim insanı Hollinger, 1997 tarihine gelinceye dek, bu alanda yapılan araştırmaları ve yazılanları dört periyoda ayırır[47]. Yazara göre 1946'dan 1976'ya dek süren "keşfetme" periyodunda, bilgisayarların ve iletişim araçlarının kötüye kullanılması, ilk olarak "telefon hatlarının kötüye kullanılması" (phone phreaking) olarak ortaya çıkmış ve bu şekilde kayıtlara ve yazına geçmiştir. 1977'den 1988'e dek süren "suça dönüşme" (criminalization) periyodunda ise, ceza hukukunun müdahalesini gerektirecek şekilde ortaya çıkan sorunlar, buna bir tepki olarak çeşitli hukuk düzenlerinde bu alana özgü yasama çalışmalarının yapılmasını sonuçlamıştır. Bu alanda "tek başına ilk düzenlemeyi yapma ödülünü" ise bir Amerika Birleşik Devletleri (ABD) eyaleti olan Florida kazanmıştır[48]. Üçüncü periyod ise 1989'den 1993'e kadar süren, "bilişim korsanlarının (hackers) şeytanlaşması" dönemidir. Bu dönemde kolluk güçleri, bilgi ve iletişim teknolojilerindeki (Information and Communications Technologies / ICT) devrimin getirdiği ve başını bilişim korsanlarının çektiği tehditlere karşı yoğun bir mücadele vermişler, çok uğraşmışlar, ancak sıklıkla başarısızlığa uğramışlardır. Son olarak Hollinger, kitabını yazdığı dönemi "denetim" periyodu olarak açıklar. Bu dönemde bilişim sistemlerinin iletişim bütünlüğüne yönelik suçlardan çocuk pornografisine ilişkin materyallerde olduğu gibi hukuka aykırı içeriklerin internetten erişilebilirliğine kadar çok sayıda suç söz konusudur[49].

---

44 G. E. Moore, "Cramming More Components onto Integrated Circuits", Electronics, Vol.38, No. 8, 1965, s. 114–117.

45 Wall, Cybercrime, s. 2, 3.

46 Walden, pn. 2.49.

47 Richard C. Hollinger, Crime, Deviance and the Computer, Aldershot, Dartmouth Publishing, 1997, s. xviii.

48 Florida Computer Crimes Act (Florida Bilişim Suçları Yasası), Fla. Stat. Ch. 815, yürürlüğe giriş tarihi 1 Ağustos 1979.

49 Walden, pn. 2.50.

Hollinger'in tarihsel sınıflandırmasını kabul etmemek için hiçbir neden bulunmamaktadır. Ancak bir noktaya işaret etmek gerekir, günümüzde bilgisayarlar ve bilişim suçları iki önemli tehdit tarafından yönlendirilmekte: Terörizm ve organize suçlar. Ayrıca hukuka aykırı içerikler de hala suç politikasının gündeminde önemli bir yer işgal etmekte. Dolayısıyla, bu dönem "kritik altyapılar" dönemi olarak adlandırılabilir; zira bu dönemde bireyselden ziyade toplumsal seviyedeki konular ceza hukuku ve ceza muhakemesi hukukundaki reformlara yönelik politikaların oluşturulmasında daha önemli hale gelmiştir[50].

Bilişim suçlarının tarihçesinin oluşturulmasında alternatif seçenekler de mevcuttur. Örneğin, ünlü Alman ceza ve bilişim hukukçusu Prof. Dr. Ulrich Sieber, bilişim suçlarının ortaya çıkardığı tehlikelere karşı ulusal hukukların yasama alanında gösterdiği tepkilere göre bunu "altı ana dalgaya" ayırır[51]. 1970'ler ve 1980'ler boyunca görülen ilk dalgada yasalar, bilgisayarların bireyler hakkındaki verileri işleme kapasitelerindeki artışa bir yanıt olarak, verilerin korunması ve mahremiyet konularıyla ilgilidir. 1980'lerin başlarında, bilgisayarların kullanıldığı ekonomik çıkar amacıyla işlenen suçlarla ilgili olarak, mevcut ceza yasaları güncellenmiş ve bunlara ekler yapılmış, ancak bunlar da yetersiz kalmıştır. 1980'ler boyunca ve 1990'ların başında ise bilgisayar yazılımları ve geleneksel olarak korunan eserlerin yeni formları gibi internet ve bilişim teknolojileri sayesinde ortaya çıkan yeni tür mülkiyet haklarının korunması amacıyla ulusal fikri mülkiyet rejimlerinde gelişmeler yaşanmıştır. 1990'ların ortalarında internetin yaygınlaşmasıyla birlikte dikkatler hukuka aykırı ve zararlı içeriklere karşı korunmak için yasaların güncellenmesi ihtiyacına odaklanmıştır. Ceza muhakemesi hukukundaki reform ise, internet ve bilişim teknolojilerindeki gelişmelerin geleneksel uygulama ve yöntemlere meydan okumasıyla 1980'lerde başlamıştır. Son dalga ise, Sieber tarafından, 1990'ların ikinci yarısı boyunca devam eden, kriptoloji ve elektronik imza gibi güvenlik gerekçeleriyle yapılan düzenlemeler olarak tanımlanır[52].

Buna paralel bir tarih, örneğin bilişim korsanları ve virüs yazılımcılarında olduğu gibi, suç aktiviteleriyle değişken motivasyonlarla ilgilenen kişilerin etrafında yapılandırılabilir. Erken dönem bilişim korsanları, Holliger'in "keşfetme" dönemi olarak adlandırdığı periyotta, öncelikle hukuka aykırı yarar elde etme amacından çok merak ve yeni deneyimler yaşama güdüsüyle hareket etmekteydiler. Teknolojilerin yayılmasıyla birlikte ekonomik çıkar amaçlı, endüstri kaynaklı bilişim suçlarının varlığı kural haline gelmiştir. New York'ta 2001 yılında gerçekleştirilen terör saldırılarından sonra ise ilgi, öncelikli olarak terörizme kaymıştır; çünkü internet ve bilişim teknolojilerinin siber

50 Walden, pn. 2.51.
51 Sieber, COMCRIME Study.
52 Walden, pn. 2.52.

teröristler için hem bir araç hem de silah olduğu açıkça görülmüştür[53].

Sonuç olarak kabul etmek gerekir ki, bilişim suçlarının tarihi açısından temel ve belirgin bir ayrım bulunmaz; eğer mutlaka bir ayrım yapılması gerekiyorsa bu ayrım internet öncesi gerçekleştirilen eylemler ve internet sonrası siber uzayda gerçekleştirilen eylemler olarak yapılabilir. Her ikisi ile de ilgilendiğinizde, Hollinger'in de vurguladığı gibi, bu alandaki ilk yasama çalışmaları, teknolojiyi hedef alan eylemler olup, internet öncesi dönemde, bilişim çağının ilk zamanlarında gerçekleşmiştir ve o tarihlerde çok farklı bir bilişim çevresi söz konusudur. Şimdiki ve bundan sonraki çalışmalarımız ise internetin bilişim alanında meydana getirdiği deprem nedeniyle, sanal ağları içerecek biçimde olmak zorundadır[54].

Nitekim Birleşik Krallık bu zorunluluğu dikkate alarak, başlangıçta da ifade ettiğim üzere, bilişim alanına ve özellikle ceza hukuku ceza muhakemesi hukukuna ilişkin düzenlemeleri ve uygulamalarını sürekli olarak sanal ağları dikkate alarak yapmış ve bunu bir devlet politikası haline getirmiştir. Ülkemizde ise buna karşıt olarak özellikle ceza muhakemesi hukuku açısından önemli politika ve mevzuat eksiklikleri bulunmaktadır.

IV. BİLİŞİM SUÇLARI ALANINDAKİ KAMU POLİTİKALARI, KRİTİK ALTYAPILAR, SUÇLARIN İŞLENİŞ SIKLIĞI, SUÇLARIN RAPORLANMASI VE AYIRT EDİCİ ÖZELLİKLER

A. Kamu Politikaları

Hukuk ve yasalar, belirli tipteki insan davranışlarını kolaylaştırmak ve bazılarını da sınırlandırmak için bulunurlar. Bir hareket ile ilgili suç ve cezai yaptırım koymak, özellikle yaptırımın özgürlüğü bağlayıcı hapis cezası olması halinde, açıkça bireyi kamu hukukunun uygulaması açısından bu alandaki spektrumun en ucuna koymaktır. Dolayısıyla cezai yaptırımlar, devletin üst düzey yöneticileri ve yasa yapıcıları tarafından hatta bazı durumlarda hukukçular tarafından açıkça onay verilmeden, buna yönelik açık suç politikası amaçları tanımlanmadan ve dile getirilmeden yürürlüğe konulmamalıdır[55].

İngiltere'de yasaların hazırlık sürecinde önemli yetkilere sahip Hukuk Komisyonu'nun (Law Comission)[56] belirttiği üzere, zarar ya da olası zarardan duyulan korku, internet ve bilişim teknolojilerinin gelişmesini ve kullanılmasını durduran bir fren işlevi görür ki bu da ekonomik gelişim üzerinde olumsuz

[53] Walden, pn. 2.53.
[54] Walden, pn. 2.54.
[55] Walden, pn. 2.55.
[56] Hukuk Komisyonlarının işlevi, yetkileri ve etkileri hakkında ayrıntılı bilgi için bkz: Matthew Dyson/James Lee/Shona Wilson Stark (Ed), Fifty Years of the Law Commissions: The Dynamics of Law Reform, Oxford and Oregon, Hurt Publishing, 2016, s. 1 vd.

bir etki doğurur. Eğer insanlar sanal alanda kendilerini güvende hissetmezler ve bu alana güvenmezler ise, bu konuda ileri sürülen öngörülerde belirtildiği üzere, bu alanı kullanmaktan kaçınabilirler ya da bu alanda gerçekleştirecekleri aktivitelerin kapsamında son derece ihtiyatlı ve seçici olurlar. Bu suskunluk eğer çok geniş bir alana yayılırsa, internetin ve internet üzerinden erişilebilir hizmetlerin büyümesini ve gelişmesini engelleyebilir[57].

İşte bu son paragraf yalnızca bilişim hukuku ya da ceza hukuku değil, hukukun her disiplini açısından bizlere önemli dersler veren bir karşılaştırmalı hukuk çıktısıdır. Zira bu anlayış bizlere, yasaların günlük bir sorunu gidermek ya da belli bazı olaylara tepki vermek için değil, bu alanda düşünülüp taşınıldıktan sonra; sosyal, ekonomik, kültürel ve yönetimsel duyarlılıklar ve politikalar göz önünde bulundurularak yasa yapılması ya da yasada değişiklik yapılması gerekliliğini ve zorunluluğunu gösterir. Kısacası suç normları ve karşılığında yaptırımlar konulurken suç politikası ve bunun olumlu ve/veya olumsuz etkileri mutlaka dikkate alınmalıdır. Ülkemiz açısından durumun böyle olduğunu söylemek ise son derece güçtür. En temel yasalar dahi bir sorun ortaya çıktığında (amiyane tabiriyle yumurta kapıya dayandığında) bu soruna bir tepki olarak çıkmaktadır. Dolayısıyla birçok temel yasamız dahi tepki yasası niteliğindedir. Dileğim bu durumun bir an önce değişmesidir.

Ancak şunu belirtmeden geçmemek gerekir: Önlem almak tedavi olmaktan iyidir (prevation being better than cure)[58]. Buna karşın tahmin edilebilir ve öngörülebilir gelecekte yasal yükümlülükler ve güdüleyici faktörler; teknolojinin kendisinin sunduğu, bilişim mühendisliğinin kriptoloji, elektronik imza, anti-virüs yazılımları ve casus yazılımlara karşı uygulama tekniklerinin yanı sıra suç için ortaya çıkardığı yeni fırsatlar karşısında, veri güvenliği konusundaki politikaların üretilmesinde düşük düzeyde bir bileşen olarak kalacaktır[59]. Dolayısıyla bu konuda yalnızca yasa yapma ve hukuk uygulama ajanslarının (Law Enforcement Agencies / LEA)[60] çalışmalarıyla bir sonuca varmak tek başına yeterli değildir. Bu konuda toplumun eğitilmesi ve herkesin üzerine düşeni yapması gerekir. Aksi halde bir bilişim dünyası kaosu kaçınılmazdır.

---

57 Walden, pn. 2.61.

58 Walden, pn. 2.62.

59 Walden, pn. 2.69.

60 Hukuk öğreti ve uygulamamızda kısaca "kolluk" ya da "kolluk güçleri" dediğimiz, suç ve suçlularının soruşturulması ve önce savcılık sonra da mahkeme önüne çıkarılması için yetkilendirilmiş ve görevlendirilmiş kuruluşlara (Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı vb.), Birleşik Krallık'ta kısaca hukuk uygulama ajansları (law enforcement agencies) kısaca LEA denilir. Bu ifadede geçen "uygulama (enforcement)" sözcüğü içerisinde bir miktar zorlayıcılığı ve görevin yerine getirilmesi anlamlarını da içerir. Bu ifadenin kullanılmasının nedeni ise polisin ulusal ve yerel düzeyde, farklı ya da benzer yetkilere sahip hatta bazı olaylarda yan yana çalışan çeşitli birimlerden oluşması nedeniyle bunları tek bir başlık altında toplanmaya çalışılmasıdır.

B. Kritik Altyapılar

Modern toplumlar artan bir biçimde internet üzerinden işleyen yaşamsal önemdeki sistemleri çalıştıran bilgisayarlara, bilgisayar sistemlerine ve bilişim ağlarına bağlıdırlar. Bu dijital devrim, sivil alt yapılar olduğu kadar, devletin alt yapılarına ve hatta silahlı güçlerin alt yapılarına kadar uzanmaktadır. *The Economist* dergisi ünlü bir makalesinde bunu şu şekilde ifade etmektedir: *"Bombalar GPS uyduları tarafından yönlendirilmekte, dronlar dünyanın herhangi bir yerinden uzaktan kumanda ile yönetilmekte, savaş uçakları ve savaş gemileri birer büyük veri işleme merkezi olarak çalışmakta ve hatta sıradan bir piyade eri bile bilişim ağına bağlı hareket etmektedir"*[61]. Ancak dijitalleşme iki tarafı keskin bir bıçaktır: 21. yüzyılda bitler ve baytlar, mermilerin ve bombaların yerin almıştır. Aslında dijital sistemlere daha fazla bağlı olan devletler siber ataklara karşı daha kırılgandırlar: Eğer bilişim sistemleri toplumun sinir sistemini oluşturuyorsa, bunların etkisizleştirilmesi ülkenin paralize hale getirilmesi anlamına gelecektir[62].

Bilişim suçlarının, siber terörle birlikte anılmasının artmasıyla birlikte devletler, sanal ağlar tarafından oluşturulan ve "kritik altyapılar" olarak tanımlanan yapıların hassaslığına dikkati çektiler. Bu yerleşkelerin, ağların, servislerin veya yapıların yok edilmesi ya da işleyişlerinin aksatılmasının sağlık, kamu düzeni, güvenlik veya bireylerin ekonomik iyiliği ya da devletin fonksiyonlarının etkinliği üzerinde ciddi etkileri olabilecektir[63]. Kritik altyapıların neler olduğu buna ilişkin öznel ilgiye göre ülkeden ülkeye değişiklik gösterirken, bilgisayar ve iletişim ağları interneti de kapsayacak şekilde genellikle açıkça tanımlanmıştır[64].

Örneğin, ABD hükümeti, daha kapsamlı olan anavatanın güvenliği için ulusal strateji çalışmasının bir parçası olan "Güvenli Siber Alan İçin Ulusal Strateji" isimli bir çalışmayı yayınlamıştır. Bu dokümanda sanal alanının "ülkenin kontrol sistemi" ve "siber alanının sağlıklı işleyişi ulusal güvenlik ve

---

61 "War in the fifth domain", The Economist, 1 Temmuz 2010, http://www.economist.com/node/16478792; 1.2.2017.

62 Marco Rosci, Cyber Operations and the Use of Force in International Law, Oxford, Oxford University Press, 2014, s. 1.

63 Bu konuda ayrıntılı bilgi için bkz: Murat Volkan Dülger, "Teknolojideki ve Kitle İletişim Araçlarındaki Gelişmelerin Uluslararası Terörizme Etkileri", Hukuk ve Adalet Eleştirel Hukuk Dergisi, İstanbul, Y. 4 S. 8, Nisan 2007, s. 55–76; Philip W. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet", A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, Ed: Marianne Wade/Almir Maljević, Heilderberg, Springer, 2010, s. 51-80; Ulrich Sieber, "Instruments of International Law: Against Terrorist Use of the Internet, A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, Ed: Marianne Wade/Almir Maljević, Heilderberg, Springer, 2010, s. 171-220.

64 Walden, pn. 2.72.

ulusal ekonomi için esastır" şeklinde kullanılan dil, potansiyel ya da algılanan kırılganlık ölçüsünü son derece açık hale getirmiştir[65]. İnternetin stratejik öneminin kabul edilmesi, Birleşmiş Milletler Bilgi Toplumu Dünya Zirvesi'ne (WSIS) konu yapılan, ABD hükümetinin kritik bir internet kaynağı olan internet alan adları üzerindeki kontrolünü uluslararası bir yönetici yapıya devretmesi yönündeki görüşü reddetmesinin nedenlerinden birini oluşturur[66].

Artık şunu açıkça görmekteyiz: Siber alanın oluşturduğu kırılganlığın doğası nedeniyle bir ikilem ile karşı karşıyayız: Bir kırılganlık kaynağı olarak limanlar ya da güç istasyonları gibi kritik altyapılara karşı yapılacak saldırılarda sanal ağların bir kanal oluşturma özelliği ve siber alanın bizatihi kendisinin önemli bir alt yapı olması dolayısıyla kırılgan bir varlık olması.

Önemli bir bilgi alt yapısı olarak internetin kaybedilmesine bağlı olarak bizim karşı karşıya olduğumuz kırılganlığımız bir parça ironiktir, zira internetin çıkış kaynağı ABD Savunma Bakanlığı'nın iletişim ağlarına yapılması olası bir saldırıya karşı güçlü bir şekilde dizayn edilmiş bir girişim olması gerekir[67]; ancak söz konusu saldırılardan internetin yaratıcısı olan bu kuruluş da fazlasıyla nasibini almaktadır.

C. Suçların İşleniş Sıklığı

Bilişim suçları ile ilgili ampirik verilerin görece yetersizliği çok sayıda nedene bağlıdır. İlk olarak ifade edilmelidir ki kolluk güçlerinin ve soruşturma makamlarının bu konudaki deneyimleri eksiktir ve veri kaynakları yetersizdir: Örneğin, kolluk güçleri ve soruşturma makamları öncelikli olarak bu alanla ilgilenmemektedirler, zira şiddet suçları gibi diğer geleneksel ve önemli alanlar bu kişilerin ilgileri için bilişim suçları gibi diğer alanlar ile rekabet halindedirler[68]. Bu durum sıklıkla personelin yetersiz eğitimi ile daha da üst seviyelere çıkmaktadır; öyle ki bazen şüpheliler soruşturmacıları işledikleri iddia edilen suçun yapısı hakkında eğitmek zorunda kalmaktadırlar.

Elektronik Sınırlar Vakfı'nın eş kurucusu John Perry Barlow, bir bilişim korsanlığı soruşturması sırasında ilgili FBI ajanıyla yaptığı görüşmeyi şöyle aktarmıştır:

---

65 US Government, The Natonal Strategy to Secure Cyberspace, February 2003, bkz: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, 11.7.2016.

66 Walden, pn. 2.75. Buna karşın, ABD Mart 2014'de, anahtar internet alan adı fonksiyonlarının küresel paydaşlar topluluğuna geçişine niyetli olduğunu duyurmuştur, bkz: Ulusal Telekomünükasyon ve Bilgi İdaresi (National Telecommunications and Information Adminastiration – NTIA), "NTIA anahtar internet alan adı fonksiyonlarının geçişine yönelik niyetini duyurdu", Basın Açıklaması, 14 Mart 2014, https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions, 11.7.2016.

67 Walden, pn. 2.77.

68 Marc D. Goodman, "Why the Police Don't Care about Computer Crime", Harvard Journal of Law and Technology, Vol. 10, Number 3, Summer 1997, s. 465 vd.

"Bildiğiniz üzere işlerin yoluna girmesi için genellikle potansiyel şüpheliler soruşturma güçlerine işledikleri iddia edilen suçların yapısını anlatmak zorundadırlar!"[69].

Söz konusu ikinci faktör açıkça bilişim suçlarının eksik rapor edildiği görüşüne katkı sağlamaktadır, zira mağdurlar soruşturma makamlarından zayıf bir karşılık alacaklarını algıladıklarında, mağduru oldukları suçu rapor etmek için çaba göstermek konusunda daha isteksiz olmaktadırlar[70].

D. Suçların Bildirimi (Raporlanması)

Bildirilmeyen suçların bildiriminin yapılmasına yönelik bir yaklaşım, bir güvenlik ihlali olduğunda bunun bildirilmesi için kurumlara hukuki yükümlülük getirilmesidir. Örneğin, 2003'den beri, Kaliforniya Eyaleti Medeni Kanunu[71], özel girişimlere ve kamu idarelerine kişisel verilerin söz konusu olduğu (finansal verileri de içerek şekilde) bir güvenlik ihlaline uğramaları[72] halinde bildirimde bulunma yükümlülüğü getirmiştir. Bu düzenlemenin belirgin amacı büyüyen bir sorun olan kimlik hırsızlığı ile mücadele etmektir. Bu girişim aynı zamanda bir kuruluş tarafından işlenen verilerin, verilerin konusu bireylere ait olduğunda, genellikle bireylerin çıkarlarıyla ve kamu yararıyla çatıştığını da göstermektedir. Ancak bu ihlal, hakları ihlal edilen kuruluşların özel çıkarlarını ihlal etmemektedir. Avrupa Birliği (AB) de 2009 senesinde kamuya açık telekomünikasyon servis sağlayıcılar için benzer şekilde ihlal bildiriminde bulunma yükümlülüğü getirmiştir[73]. Şimdi ise bu tür ihbar yükümlülüklerini kişisel veri işleyen tüm veri denetçilerine (kamu yöneticileri ve pazarlama uzmanları gibi) genişletmek için iki teklif bulunmaktadır. Bu tür yasalar hukuk sistemlerine, kimin bildirimde bulunacağına (örneğin; düzenleyiciler, veri özneleri, genel kamu gibi), ihlalin alt eşiğinin ölçüsüne (örneğin; ihlalin ne kadar ciddi olduğuna göre) veya ihlalin konusuna göre (örneğin; finansal veri ya da sağlık verisi olmasına göre) oldukça değişkenlik gösterebilirler. Ayrıca konulan yükümlülükler ile yasa yolları da değişkenlik gösterirler[74].

---

69 John Perry Barlow, "Crime and Puzzlement: in advance of the law on e electronic frontier", Whole Earth Review, No. 68, Fall 1990, s. 44-57. Bu durumun yirmi yıl önce gerçekleşmesine rağmen yazar, 2005 yılında Birleşik Krallık'ta yapılan bir soruşturmada benzer bir durumun halen geçerli olduğunu bildirmektedir.

70 Walden, pn. 2.82.

71 California Civil Code, m. 1789.29 ve 1798.80 et seq. Hâlihazırda ABD eyaletlerinin ekseriyetinde bu tür düzenlemeler yer almaktadır; bkz: National Congerence of State Legislatures (NCSL), "Güvenlik İhlali Bildirim Yasaları", http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, 13.7.2016.

72 California Civil Code, m. 1789.82(d): "Kişisel bilgilerin güvenliğini veya gizliliğini tehlikeye atan dijitalleştirilmiş verinin yetkisiz olarak elde edilmesi anlamına gelir".

73 2009/136/EC nolu direktif, OJ L 337/11, 18 Aralık 2009; 02/58/EC nolu Direktifin 4. maddesine eklenmiştir.

74 Walden, pn. 2.96.

Mağdurlara getirilen bu bildirim yükümlülüklerinin yanı sıra, bu konuya bir diğer yaklaşım, suç aktivitesinde rol alabilen belli bazı aracı konumundaki kişilere bildirim yükümlülüğü getirilmesidir. Arada yer alan kişiler hukuka aykırılığın varlığı konusunda bilgi sahibi olduklarında ya da bu konuda bilgilendirildiklerinde, bunların bildirim zorunluluğu önceden etkili izleme ya da tepki gösterme şeklinde bazı kurallara bölünmek suretiyle oluşturulabilir. Söz konusu yükümlülük ister önceden önlem alma ister sonradan tepki gösterme şeklinde olsun, bunun algılanması genellikle arada yer alan kişilerin suç oluşturan hareketlerin ne kadarıyla ilgili olduklarına bağlıdır. Ekonomik çıkar amacıyla işlenen suçlarla mücadele için, örneğin birçok devlet suç gelirlerinin aklanmasıyla mücadele yasaları çıkarmakta ve finans kurumları ile profesyonel danışmanlara, ceza hukukunun desteğiyle, şüpheli transferlerin yetkili otoritelere bildirilmesi konusunda zorunluluklar getirmektedir[75]. Hukuka aykırı içerik suçları alanında, bazı devletler internet servis sağlayıcılara çocuklara ilişkin görüntülerin kötüye kullanılması hakkında bilgi edinmeleri[76] ya da bu konuda haberdar olmaları[77] halinde vakit kaybetmeksizin bildirimde bulunmaları konusunda yükümlülük getirmekte, bunun ihmal edilmesi halinde ise yine ceza hukukunun yaptırımları devreye girmektedir.

Birleşik Krallık'ta ise, 2000 tarihli Terörizm Yasası kişilere, *"terörizmle ilgili bir kişinin yakalanması, soruşturulması ya da cezalandırılmasına yol açabilecek bir terör hareketini önlemek için bir bilgiye sahip olması halinde"* bu bilgiyi *"olabilecek akla uygun ve en pratik biçimde"* ilgili makamlara bildirmeleri hususunda bir yükümlülük getirmektedir[78].

E. Yönelim ve Ayırt Edici Özellikler

Bilişim suçları gelişmekte olan ülkelerin sürdürülebilir kalkınmaları için önemli bir tehdit olma özelliğini de gösterirler; zira kısa dönemde çeşitli yardım fonlarının kötü amaçlara yönlendirilmesine yol açarlarken, uzun dönemde ülke ekonomisinde yer alan yatırımcıların güvenini olumsuz yönde etkilerler[79].

Birleşik Krallık uluslararası toplumda politika oluşturan ve bunları uygulatmaya çalışan ülkelerden biridir. Bunu sağlamanın yollarından biri de, hem doğrudan hem de Brexit öncesi AB üzerinden gelişmekte olan ya da

[75] Bu konuda ayrıntılı bilgi için bkz: Murat Volkan Dülger, Suç Gelirlerinin Aklanmasına İlişkin Suçlar ve Yaptırımlar, Ankara, Seçkin Yayıncılık, 2011, s. 240-278.

[76] Bkz: US federal law (Birleşik Devletler Federal Yasası at 42 USC m. 13032 (Reporting of child pornography by electronic communications service providers / çocuk pornografisinin elektronik iletişim sağlama servisleri tarafından raporlanması).

[77] Australian Criminal Code Act (Avustralya Ceza Kanunu) 1995, m. 474.25 (Obligations of Internet Service Providers and Internet Contens Hosts / İnternet Sağlayıcıları ve İnternet İçeriği Barındıranlara İlişkin Yükümlülükler).

[78] Walden, pn. 2.97.

[79] Walden, pn. 2.103.

AB'ye üyelik sürecinde olan ülkelere çeşitli alanlarda fonlama yapılması, bir başka deyişle kaynak aktarılmasıdır. İşte Birleşik Krallık kendi ulusal çıkarları açısından bu durumu bir tehdit olarak gördüğü için bilişim suçları ile ciddi bir biçimde ilgilenmekte ve bu konuda politikalar oluşturmaktadır.

V. BİLİŞİM CEZA HUKUKUNA İLİŞKİN POLİTİKALAR VE YÖNELİMLER

A. Ceza ve Muhakemesi Hukukuna İlişkin Yaklaşım

Birleşik Krallık'taki hukuk kuramcıları ve uygulayıcılarına göre, bilişim suçları hakkındaki bir rejim, yalnızca maddi ceza hukukunun bir sorunu olarak farklı suç tiplerinin uygun bir şekilde tanımlanması değil, bunun yanı sıra ceza muhakemesi hukukunun bir sorunu olarak soruşturma ve kovuşturma işlemlerinin kolaylıkla yapılmasıyla tanımlanabilir. Bunlardan ikincisinde söz konusu olan bir başarısızlık ilkinin de altını oyar. Uygulanamaz ceza hukuku kuralları, herhangi bir hukuk sisteminin bir anlamda lekesidir; ancak bu muhakeme hukukunun yetersizliğinden kaynaklanmak zorunda da değildir[80]. Bu yetersizlikler suç normlarının iyi tanımlanmaması ve işlevsizliğinden de kaynaklanabilir. Ancak her durumda bu çok önemli bir olumsuzluktur.

B. Bilişim Suçları Açısından Yaptırım

Uluslararası ve tarihsel bir perspektiften bakıldığında yaptırım teorisinde en ağır ceza ölüm cezasıdır. Ancak; Birleşik Krallık, Avrupa Konseyi'nin bir üyesi ve Avrupa İnsan Hakları Sözleşmesi (AİHS) ve ek protokollerinin tarafı olarak ölüm cezasını ilga etmiştir.

Ayrıca bilişim suçları için genellikle böyle bir ceza öngörülmemektedir. Ancak, Çin Halk Cumhuriyeti'nde bilişim korsanlarına bu ceza verilmektedir. Örneğin, 1998 yılında, bir bankanın bilişim güvenliği sistemini kırmak suretiyle kendi hesaplarına para aktaran müşterek faillerden Hao Jing-long ömür boyu hapis cezasına, Hao Jing-wen ise ölüm cezasına mahkûm edilmişlerdir[81].

Ülkemizde de hem uluslararası sözleşmeler hem de iç hukukun gereği hiçbir suç için ölüm cezası öngörülmemiştir. Ayrıca, bilişim suçları açısından suçun haksızlık içeriği dikkate alınarak, ölüm cezasına benzer müebbet hapis cezası gibi cezalar da öngörülmemiştir. Bu düzenlemeleri olumlu bulduğumu belirtmeliyim.

---

80 Walden, pn. 2.108.

81 Cong Lixian, "Chinese E-Commerce (2) and Legal Environment", Chinese Intellectual Property and Technology Laws, Ed: Rohan Kariyawasam, Edward Elgar Publishing, 2011, s. 279. Walden, pn. 2.142.

C. Güvenlik Tedbirleri (Yasaklamalar ve Haktan Vazgeçme)

Birleşik Krallık'ta işlenen suçların yargılanması sonucunda sanığın suçlu bulunması halinde faile ceza yanında bizdeki güvenlik tedbirine benzer tedbirler de uygulanabilmektedir. Bu durum suçta kullanılan araçların müsaderesi veya söz konusu araçların gönüllü olarak teslim edilmesi şeklinde olabilir. Ayrıca, gelecekte işlenmesi olası suçların engellenmesi için önemli bilişim araçlarının kullanılmasının yasaklanması da söz konusu olabilir[82]. Bunlardan ilki ülkemizde olmakla beraber, ikincisi ve özellikle üçüncüsü bulunmamaktadır. Üçüncü tedbir benzeri bir normun yaptırım sistemimizde uygulanmasının suçun önlenmesi açısından yararlı olacağını düşünüyorum.

Ünlü Amerikalı bilişim korsanı Kevin Mitnick yargılanırken, savcılık makamı, kendisinin herhangi bir bilgisayar, yazılım ya da iletişim ağı aracını bulundurmasının ve kullanmasının yasaklanmasını talep etmiştir. Ancak, bu talebe itiraz edilmiştir. Sonuç olarak mahkeme, ancak gözetim memurunun oluruyla bilgisayara erişebilmesine ve kullanmasına izin vermiştir[83]. Gerçekten yargılama boyunca, Mitnick'in arayabileceği telefon numaraları bile sınırlanmıştır[84]. Benzer biçimde, bilişim korsanı Kevin Poulsen de denetimli serbestlik süreci içinde özel koşullara tabi tutulmuştur[85]:

"…denetim memurunuzun izni ve onayı olmadan herhangi bir bilgisayarı ya da bilgisayarla ilgili bir aracı ya da yazılımı edinemez ya da zilyetliğinizde bulunduramazsınız; ayrıca denetim memurunuzdan önceden onay almaksızın bilgisayar ekipmanlarına erişiminizi sağlayacak bir işi alamazsınız ya da sürdüremezsiniz"[86]*.*

İngiltere'de *Collard* davasında[87] sanık, çocuklara ilişkin müstehcen resimler oluşturmak ve bulundurmaktan suçlu bulunmuştur. Mahkeme, sanığa vermiş olduğu hapis cezasının yanı sıra 1997 tarihli Cinsel Suçlular Yasası'nın (Sex Offenders Act 1997) 5A maddesi[88] gereğince şu yasaklama emrini vermiştir:

---

82 Walden, pn. 2.150.

83 Arthur L. Bowker/Gregory B. Thompson, "Computer Crime in the 21st Century and Its Effect on the Probation Officer", Federal Probation: A Journal of Correctional Philosophy and Practice, Vol. 65, No. 2, September 2001, s. 18-24.

84 Katie Hafner/John Markoff, Cyberpunk: Outlaws and Hackers on the Computer Frontier, New York, Simon and Schuster, 1991, s. 342.

85 Walden, pn. 2.151.

86 Marc J. Stein'den Birleşik Devletler Denetim Memuru Kevin Poulsen'e gönderilen 22 Mayıs 1996 tarihli mektup, akt: Douglas Thomas, "Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker", Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed: Douglas Thomas/Brian D. Loader, London & New York, Routledge, 2000, s. 30.

87 [2004] EWCA Crim 1664.

88 Bu düzenleme hâlihazırda yürürlükten kaldırılmış ve yerine 2003 tarihli Cinsel Suçlar Yasası

*"… Herhangi bir kişisel bilgisayara, dizüstü bilgisayara ya da internete herhangi bir biçimde erişim sağlayarak materyal indirilmesini sağlayacak araçlara sahip olmanız, kullanmanız, zilyetliğinizde bulundurmanız ya da bunlara herhangi bir şekilde erişim sağlamanız yasaklanmıştır. Bu yasaklama, hukuka uygun bir işte söz konusu araçların bulundurulması ve kullanılması halinde, yalnızca bu hukuka uygun ama*çla sınırlı olmak üzere *uygulanmayacaktır"*[89].

Bu yasaklamaya karşı temyiz mahkemesine başvuru yapılmıştır. Mahkeme temyiz başvurusunu kabul etmiş, böyle bir yasaklamanın kişinin eşini ve çocuklarını etkili bir şekilde internete erişimden mahrum edeceğini ve yan zararlara neden olacağını belirterek, kararı kaldırmayıp yasaklama emrine aşağıdaki ibareyi eklemiştir:

"…internetten herhangi bir materyal indirmeniz yasaklanmıştır. Ancak bu yasaklama hukuka uygun bir iş için ya da hukuka uygun bir öğrenim/araştırma için yapılacak internetten indirmelere uygulanmayacaktır".

Bu yaptırımın belirsiz bir zamanı kapsıyor olması her nasılsa "aşırı" olarak değerlendirilmemiştir. *Halloren* davasında[90] ise, benzer olarak aynı zamansal belirsizlikle verilen bir karar, hükmü veren hakimin yasanın ölçütlerini yeterince dikkate almadığı ve söz konusu yasaklama emrinin arzu edilenden ziyade gerekli olup olmadığı gerekçelerine dayanılarak bozulmuştur[91].

D. Suç Gelirlerinin Geri Alımı

Birleşik Krallık'ta, 2002 tarihli Suçtan Elde Edilen Gelirler Yasası (Proceeds of Crime Act 2002) ile Kazançların Geri İadesi Ajansı (Asstes Recovery Agency) suçlular tarafından gerçekleştirilen hukuka aykırı eylemlerden elde edilen gelirlerin geri alınması amacıyla kurulmuştur[92]. Bu ajans, şimdiki ismi Ulusal Suç Ajansı olan, ancak kurulduğu tarihteki adı Ciddi ve Organize Suç Ajansı olan yapının da bir alt kuruluşudur. Suç gelirlerinin geri alımı, ya müsadere emrinde olduğu gibi ceza muhakemesi işlemleriyle birlikte yürümekte ya da özel hukuk yargılamasında "geri alım emri" olarak işlemektedir[93].

(Sexual Offences Act 2003) getirilmiş, anılan madde de "cinsel suçları önleme emri" olarak düzenlenmiştir.

89 Walden, pn. 2.152.

90 [2004] EWCA Crim 233; [2004] 2 Cr App R (S) 57.

91 Ayrıntılı bilgi için bkz: Ian Walden/Martin Wasik, "The Internet: Access Denied Controlled!", Criminal Law Review, Issue 5, 2011, s. 377-387; Alisdair A. Gillespie, "Restricting Access to the Internet by Sex Offenders", International Journal of Law and Information Technology, Vol. 19, No. 3, 2011, s. 165-186; Walden, pn. 2.152.

92 POCA, m. 241.

93 Walden, pn. 2.158.

Örneğin, *McKinnon* davasında[94], ABD'de bulunan ve müstehcen yayınlar içeren web sitesinden sanığın elde ettiği gelirlerin alınması için bir müsadere emri verilmiştir. Ancak, söz konusu resimler Birleşik Krallık'ta çekildikten sonra ABD'ye gönderilmiştir. Temyiz yargılaması esnasında sanık, web sitesi sayesinde elde edilen söz konusu gelirlerin yalnızca suçtan elde edilen gelirler olmadığını, dava konusu resimlerin yayınlanmasının suç oluşturmadığı ülkelerden elde edilen gelirlerin de bunların arasında olduğunu iddia etmiştir. Bu iddia mahkeme tarafından reddedilmiştir; zira elde edilen gelirlerin bu mantıkla parçalara ayrılması mümkün değildir, özgün suç (müstehcen yayınların üretilmesi) Birleşik Krallık'ta işlenmiştir ve müsadereye tabi olması mümkündür.

E. Hukuk Reformu: Sorunlar ve İlkeler

Bilişim suçlarının konusunun genellikle bilişim sistemleri yani makineler hakkında olması bazı sorunları beraberinde getirir. Dolandırıcılık suçunda olduğu gibi suçların büyük bir çoğunluğunda eylem, bir kişiye yönelik gerçekleştirilir. Siber alanda ise, eylemler genellikle bir insan ara yüzüne ihtiyaç duymamakta, tamamen dijital olarak gerçekleşmektedir. Dolayısıyla ceza kanunlarında, insandan makineye ve makineden makineye yönelik eylemler hukukun konusu olarak düzenlenmelidir[95]. Ancak, Roma hukukundan kalan "kişi – eşya" ayrımına dayalı hukuk algımız ve sistemimiz henüz buna hazır değildir. Önce bu alana ilişkin algımız sonrasında ise düzenlemelerimiz değişmelidir.

Avrupa İnsan Hakları Hukuku'na göre şeffaflık, bir bireyin haklarının hukuka uygun bir biçimde kısıtlanabilmesi için gerekli olan bir bileşendir. Hukuki belirginlik ilkesi, bir kişinin hangi hareketinin hukuka uygun hangisinin hukuka aykırı olduğunu yeteri kadar açık bir biçimde bilecek durumda olmasını gerektirir. Hukuki belirginlik ilkesinin, örneğin bireyleri elektronik ticaret yapmaya cesaretlendirmek gibi, bireylerin olumlu davranışlarda bulunmayı sağlayacak ölçüde ekonomik getirileri vardır[96].

Belirginlik ilkesine son derece yakın olan bir diğer ilke ise, hukuk kurallarının devamlılığına olan ihtiyaç, yani hukuki istikrardır. Devamlılık ya da sürdürülebilirlik, anahtar niteliğinde iki görünüme sahiptir. Bunlardan ilki, bir dizi hukuk kuralının, bunların getiriliş amacı doğrultusunda uzunca bir süre getirildiği alanda uygulanabilmesidir. İkinci olarak, söz konusu kurallar yasaklanan davranışlara uygulanabilmelidir. Ancak, hukukun herhangi bir alanında, kuralların yüzde yüz uygulanabilmesine ulaşılabilmiş değildir;

94 [2004] 2 Cr App R (S) 46.
95 Walden, pn. 2.166.
96 Walden, pn. 2.173.

özellikle siber alandaki çok sayıdaki ve birbiriyle çatışma halinde olan hukuki egemenlik alanlarının varlığı dolayısıyla geniş bir aralıkta kuralların uygulanabilirlik yoksunluğu hukuk kurallarının değerinin altını oymaktadır[97].

Görüldüğü üzere, özellikle ülkemizde son yıllarda karşılaşılan ceza mevzuatının sıklıkla değiştirilmesi, yalnızca bizde değil, gelişmiş bir ekonomik, sosyo-kültürel ve hukuki alt yapıya ve sisteme sahip olan Birleşik Krallık'ta da önemli bir sorun olarak görülmektedir. Doğrusu, çok düşünüp uzun süreler sonunda iyi mevzuat üretmek ve üretilen mevzuatı mümkün olduğunca uzun bir süre layıkıyla uygulayabilmektir.

F. Kriminolojik Açıdan Fail

Bilişim suçlularını motive eden, suç işlemeye iten nedenler nelerdir? Grabosky ve arkadaşlarının belirttiğine göre, bilişim suçlularının geleneksel suç işleme nedenleri bulunur; bunlardan en çok görünenleri açgözlülük, ihtiras, güç, intikam, macera ve yasak ağacın meyvesini elde etme isteğidir[98]. Bundan farklı olarak Kilger ve arkadaşları ise söz konusu motivasyonu "MEECES"[99] olarak kısaltarak tanımlar; buna göre para, eğlence, ego, yapabilmek, sosyal bir gruba dahil olmak ve statü sahibi olmak suça iten nedenlerdir[100]. Bütün bu motivasyon etkenleri hakkında verilen örnekler ve halihazırda bu alandaki dikkate değer kaynaklarda yapılan çeşitli açıklamalar, zaten faillerin kendileri tarafından da dile getirilmektedir[101]. Bu motivasyonları, suçtan elde edilen gelirler bağlamında matematiksel formüllerle ifade etmeye çalışan girişimler de bulunmaktadır[102].

Bilişim hukuku alanında dünya çapında tanınan ünlü İngiliz hukukçu Prof. Dr. David S. Wall'un belirttiği üzere, *"suç* fırsat*ları takip etmeye meyilli olduğundan ve internet de çok sayıda yeni fırsat ürettiğinden, gerçekten çok sayıda yeni suç tipi ortaya çıkmıştır"*[103].

---

97 Walden, pn. 2.174.

98 Peter Grabosky/Russell G. Smith/Gillian Dempsey, Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge, Cambridge University Press, 2001, s. 2.

99 İngilizce, "money", "entertainment", "ego", "cause", "entrance to socail groups" ve "status" sözcüklerinin baş harflerinden oluşmaktadır.

100 Max Kilger/Ofir Arkin/Jeff Stutzman, "Profiling", in Honeynet Project, Know Your Enemy, Learning about Security Threats, 2nd edn, Addison-Wesley Professional, 2004, Bölüm 16.

101 Kevin D. Mitnick/William L. Simon, Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing, 2005, s. 1 vd.; Ayrıca bkz: Zhengchuan Xu/Qing Hua/ Chenghong Zhang, "Why Computer Talents Become Computer Hackers", Communications of the ACM, Vol. 56, No. 4, 2013, s. 64-74.

102 Bkz: Nir Kshetri, "The Simple Economics of Cybercrimes", IEEE Security and Privacy, Vol. 4, No. 1, January/February 2006, s. 8-13, (available at SSRN: http://ssrn.com/abstract=881421); Walden, pn. 2.185.

103 David S. Wall, Cyberspace Crime, London, Dartmouth, 2003, s. xv.

İnternet, yeni suç tiplerinin ortaya çıkmasının yanında klasik suçların işlenmesi için de yeni olanaklar sağlamıştır. Bu durum Levi tarafından *"suç olanaklarının demokratikleşmesi"* olarak bir başka şekilde de ifade edilmiştir[104]. Özellikle içerik suçlarının işlenmesinin, bilginin dijitalleşmesi ve bunların kopyalanmasının, bunlara erişimin ve iletişim olanaklarının artmasıyla birlikte kolaylaştığı görülür. Telif hakları açısından, hak ihlallerinin ticarete etkisinin olup olmadığı konusundaki tartışmalar devam ederken, hak ihlallerinin yaygınlaştığı gerçeği ise tartışmasızdır. Teknoloji günlük yaşamlarımıza iyiden iyiye girerken, bilgisayarlar ve bilişim teknolojileri ile gerçekleştirilen dolandırıcılık ve sahtecilik suçları genel kural haline gelmekte; öte yandan pornografi siber alandaki anahtar endüstrilerden biri haline gelirken, dolayısıyla hukuka aykırı ve aşırı istekleri bulunan tüketicilerde çoğalma görülmekte, özellikle çocuk pornografisi bakımından bu husus ciddi boyutlara ulaşmaktadır[105].

Dolayısıyla ticaretin zarar görmesinin engellenmesi, bireylerin temel hak ve özgürlüklerinin korunması ve genel anlamda suçun engellenebilmesi için, hem mevzuat hem de soruşturma/kovuşturma açısından bu makalede görüldüğü üzere çeşitli önlemler alınmakta ve düzenlemeler yapılmaktadır.

G. Suç Örgütleri

Suç örgütü kavramı İngiliz hukukunda açık bir şekilde tanımlanmaz. Bu sürecin bir ucunda tamamen hukuka aykırı oluşumlar olan çıkar amaçlı suç örgütleri ve suç çeteleri varken, diğer ucunda da hukuk tarafından tanınan, şirket ya da ticari girişimlerin bir formu olan tüzel kişiler bulunur. Türkiye'den farklı olarak İngiliz hukukunda, bunların kendi başlarına gerçekleştirmiş oldukları işlemlerden dolayı ceza sorumluluğu bulunur. Bu bağlamda, örneğin AB hukukuna göre, maddi hukuka ilişkin temel uyumlaştırma düzenlemeleri tüzel kişilerin ceza sorumluluğuna atıf yapmakta ve bunu şu şekilde tanımlamaktadır[106]:

"… uygulanan hukuka göre tüzel kişi statüsünde olan oluşumlar anlamına gelmektedir; ancak bunlara devletler ya da devlet otoritesi altında hareket eden kamusal yapılar ya da uluslararası kamusal organizasyonlar dahil değildir"[107]

Ceza hukuku alanında, tarihsel olarak tüzel kişilerin ceza sorumluluğunu belirleme konusunda bir mücadele söz konusudur. Bu mücadele suçun

[104] Michael Levi, "Between the Risk and the Reality Falls the Shadow", Crime and the Internet: Cybercrimes and Cyberfears, Ed: David S. Wall, London & New York, Routledge, 2001, s. 44-58.

[105] Walden, pn. 2.188.

[106] Walden, pn. 2.196.

[107] Directive 2013/40/EU, m. 2(c).

maddi unsurunun ve manevi unsurunun tüzel kişiler tarafından değil ancak gerçek kişiler tarafından gerçekleştirilebilmesine rağmen, modern ceza hukuku sistemlerinin tüzel kişilerin ceza sorumluluğunu kabul etmeye ve bu konudaki yeni düzenlemelerin sisteme uydurulmaya doğru evrilmelerinden beri devam etmektedir[108]. Bu iki aşırı ucun arasında, birbirinden oldukça farklı derecede formaliteler, eş güdümler ve süreklilikler görülür. İngiliz hukuku açısından, organizasyonların basit bir biçimde kişilere komplo kurmak veya dolandırıcılık suçunu işlemek için anlaşmış olmaları ceza hukukunun konusunu oluşturmaktadır[109].

Sonuç olarak, diğer suçlarda olduğu gibi, bilişim suçları açısından da Birleşik Krallık'ta ve diğer Anglo Amerikan sistemine dahil olan ülkelerin ceza hukuku sistemlerinde tüzel kişilerin ceza sorumluluğu (corporate criminal liability) kabul edilmektedir[110]. Uygulanan cezalar ise TCK m. 60'ta yer alanların daha geniş varyasyonları olan güvenlik tedbirleridir.

H. Suç İşlemeye Tahrik

Bizim hukuk sistemimizden farklı olarak, Anglo Amerikan hukuk sisteminde suça tahrik ya da şeriklik türleri iç içe geçmiş bir biçimde bizim verdiğimizden faklı anlamlar verilerek incelenirler[111]. Özellikle Anglo Amerikan hukuk sistemiyle yapılan karşılaştırmalı hukuk çalışmalarının zorluğu, bu sistemlerin doğalarından kaynaklanan bu farklılıktan ortaya çıkmaktadır[112].

Birleşik Krallık hukuk sisteminde bilişim suçları açısından suç işlemeye tahrik ve suça yardım etme konularında ilgi alanımıza giren önemli bir husus, başkalarının bilişim korsanlığı gibi suçları işleyebilmesini sağlamak için, bunlara gerekli araç ve olanakların sağlanmasıdır. Ashworth'ün belirttiği üzere, zilyetliğe ilişkin suçların zilyedin eşya ya da ekonomik değer ile ne yapacağı

---

108 Bu konuda bkz: David Ormerod/David Perry, Blackstone's Criminal Practice 2017, Oxford, Oxford University Press, 2016, Bölüm 10; Amanda Pinto/Martin Evans, Corporate Criminal Liability, Second Edition, Sweet & Maxwell, 2008, s. 1 vd.

109 Walden, pn. 2.197.

110 Konu hakkında ayrıntılı bilgi ve karşılaştırmalı hukuk örnekleri için bkz: Mark Pieth/Radha Ivory, Corporate Criminal Liability: Emergence Convergence and Risk, Ius Gentium: Comparative Perspectives on Law and Justice 9, Heidelberg, Springer, 2011, s. 3 vd.

111 Anglo Amerikan hukuk sistemi ceza hukuku ile Alman ceza hukukunun karşılaştırılması için bkz: Markus D. Dubber/Tatjana Hörnle, Criminal Law: A Comparative Approach, Oxford, Oxford University Press, 2014, s. 1 vd.

112 Bu zorluklar hakkında bkz: Murat Volkan Dülger, ""Hukuka Uygunluk Nedenleri ile Mazeret Nedenleri Arasındaki Ayrımın Tarihçesi, Niteliği ve Gerekliliği Üzerine Karşılaştırmalı Bir Deneme", Ceza Hukuku Dergisi, Y. 9, S. 24, Nisan 2014, s. 124, 125. Özellikle hukuki konularda İngilizce'den ya da İngilizce'ye yapılan çevirilerin zorluğu başlı başına bir çalışmanın konusu olmuştur, bkz: Rosanna Masiola/Renato Tomei, Law, Language and Translation From Concepts to Conflicts, Heidelberg, Springer, 2015, s. 5 vd.

temel alınmak suretiyle, suç olarak tanımlanmasından bu yana bunlar doğal anlamda "teşebbüs aşamasında kalmış suçlar" olarak kabul edilebilirler[113]. Böyle bir sonuç, duruma göre başkalarını suç işlemeye teşvik / yardım etme anlamına gelir. Siber alanda bu biçimdeki suça teşvike / yardıma yönelik zilyetlik, suçta kullanılacak araçlar bakımından şüphesiz bunun ayrı bir suç olarak tanımlanmasını gerektirir. Bu tür araçlar, bir suça teşebbüs halinde ya da suç anlaşmasında açıkça suça teşvik / yardım eden kişi tarafından sağlanmalıdır. Bununla birlikte, bu tür bilişim suçlarının işlenmesinde kullanılan araçlara ilişkin piyasanın doğası, en uygun biçimde cesaretlendirme ve yardım etme hareketleri olarak tanımlanabilecek şekilde görünürler[114].

Bu açıklamanın, ülkemizde 6698 sayılı Yasanın 30. maddesi ile TCK'ya eklenen 245/A maddesinde yer alan "yasak cihaz veya programlar" başlıklı suç açısından değerlendirilmesi gerekir. Aynı durum ülkemiz açısından da geçerli olduğu için bu suç tipi getirilmiştir. Bazı bilişim suçlarının bunlara ilişkin özel yazılım ve donanımlar olmaksızın işlenmesi mümkün değildir. Ancak kolluk güçlerinin yaptığı bir operasyon sırasında bu aygıtlar ile o anda bir işlem yapılmıyorsa, bunların sadece bulundurulması, cezalandırılmayan önceki hareket olan hazırlık hareketi kapsamındadır. İşte İngiliz hukukundakine benzer bu düzenleme ile hazırlık hareketi konumundaki bu davranışlar tek başına cezalandırılabilir suç olarak düzenlenmiştir.

İ. Aradaki Süjeler: Sorumluluk Kuralları ve Sorumluluktan Kurtuluş

Herhangi bir aktivite için sorumluluktan kurtulma, bilgi ya da kontrol yoksunluğunu gösterecek şekilde dizayn edilen, sıkı şartların varlığına bağlıdır[115]. İngiliz hukukunda geçerli olan *"yalnızca mecra olma / mere conduit"* ilkesine dayanılarak sorumluluktan kurtulabilmek için içerik açısından üç kuralın gerçekleşmesi gerekir: İlk olarak, internet servis sağlayıcı (ISS) iletimi başlatmamış olmalı; örneğin, içeriğin iletimi ya da içeriğe erişim kararı ISS tarafından verilmemiş ve başlatılmamış olmalı ve hatta bu durum verilen hizmete ilişkin operasyonel verilerden (göstergelerden) belirlenebilmelidir[116]. Yani; örneğin, bir kullanıcı bir e-mail mesajı gönderdiğinde, bu doğrudan doğruya ISS'nin mesajın alıcıya iletimi zamanına denk gelmemelidir. İkinci

---

[113] Andrew Ashworth/Jeremy Horder, Principles of Criminal Law, 7. Bası, Oxford, Oxford University Press, 2009, s. 487.

[114] Walden, pn. 2.222.

[115] 2000/31/EC sayılı AB direktifi, iç pazardaki, özellikle elektronik ticaretteki, bilgi toplumu servislerinin belli hukuki yönlerine ilişkindir; OJ L 178/1, 17 Temmuz 2000 (eCommerce Directive). Bu direktif Birleşik Krallık iç hukukuna 2002 tarihli Elektronik Ticaret Düzenlemesi ile aktarılmıştır (Electronic Commerce [EC Directive] Regulations 2002 [SI No 2013] 2002 Regulations). İşte bu şartlar söz konusu düzenlemede yer almaktadır: eCommerce Directive, Beyanat 42.

[116] eCommerce Directive, m. 42; 2002 Regulations reg 17.

olarak, ISS iletimin alıcısını seçmemelidir[117]. Üçünü olarak, ISS iletinin içindeki bilgiyi seçmemeli ya da dönüştürmemelidir[118]. İletide yer alan bilgi üzerinde bu şekildeki bir editöryal kontrol çalışması, "içerik hizmeti" olarak yorumlanabilir[119]. Bununla birlikte bu husus, verinin iletimi ya da erişimi esnasındaki, veri içeriğinin bütünlüğünü bozmayan teknik manipülasyonları kapsamaz[120].

Ayrıntıları aşağıda dipnotta verilen AB Direktifi ve Birleşik Krallık düzenlemesinde yer alan "önbellek düzenlemesinden" yararlanabilmek için, ISS'lerin, herhangi bir suçlamayı boşa çıkartmak amacıyla etkin bir ispatı sağlamaya yönelik şu yedi şartı yerine getirmeleri gerekir[121]: İlk olarak, herhangi bir depolama kendiliğinden (otomatik), aracı sıfatıyla ve geçici olmalıdır. Önbellek hizmetinin gerekli ayarlarının yapılabilmesi için insan müdahalesi büyük ihtimalle başlangıçta gerekir, fakat her olay için ve devam eden bir şekilde müdahale olmamalıdır. Yedekleme amacıyla depolama yapılması gündeme gelebilir, bu önbellek hizmetinin gerektirdiğinden daha fazla kalıcı depolamanın yapılması gerektiği anlamına gelmektedir. İkinci olarak, amaca yönelik bir zorunluluk bulunmalıdır; örneğin, kopyalamanın yegâne amacı hizmet alıcısının iletisinin sağlanması olmak zorundadır. Üçüncü şart ISS'nin veri üzerinde değişiklik yapmamasıdır[122]. Dördüncü şart, veriye erişmeye yönelik ISS üzerinde bulunan şartların, telif hakkı lisansı gibi haklarla tamamlanması gerekliliğidir[123]. Beşinci şart, bilgiyi güncellemeye yönelik herhangi bir kuralın, örneğin verilerin periyodik olarak güncellenmesi gerekliliği, mevzuata uyumlu olmasıdır[124]. Altıncı olarak, "kurabiyelerden / cookies" dijital hak yönetimi sistemlerine (DRM) kadar veri kullanımını gözlemek amacıyla veri sağlayıcı tarafından yararlanılan sistemler zararlı olmamalıdır[125]. Son olarak ISS'ler; özgün kaynağın çıkarıldığı, erişiminin engellendiği veya bir mahkeme kararıyla bunlara erişimin engellendiği ya da içeriğin çıkarıldığı hususunda güncel bilgiye sahip olmaları halinde; bilgiye erişimi engellemeli ya da içeriği çıkarmalıdırlar[126]. Bu koşullara uyulmaması halinde ISS'lerin sorumluluğu söz konusu olacaktır[127].

---

117 eCommerce Directive, m. 12(1)(b).
118 eCommerce Directive, m. 12(1)(c).
119 Framework Directive, m. 2(c). Bu tür "görsel-işitsel medya servisleri" (Direktif 2010/13/EU, OJ L 95/1, 15 Nisan 2010) ya da bir gazetenin web sitesi. Bu konu hakkında bkz: Papasavvas v. O Fileleftheros Dimosia Etairia Ltd and others [2015] 1 CMLR 24.
120 eCommerce Directive, m. 13(1)(a); Walden, pn. 2.233.
121 eCommerce Directive, m. 13; 2002 Regulations reg 18.
122 eCommerce Directive, m. 13(1)(a).
123 eCommerce Directive, m. 13(1)(b).
124 eCommerce Directive, m. 13(1)(c).
125 eCommerce Directive, m. 13(1)(d).
126 eCommerce Directive, m. 13(1)(e).
127 Walden, pn. 2.234, 2.235.

Yukarıda yasaya dayanan sorumluluktan kurtulmaya ilişkin yapmış olduğumuz açıklamalarda görüleceği üzere, internetin bir ortam olarak gelişmesine yönelik hukuk politikası kendine özgüdür (sui generis). Bu politikanın özünde geleneksel İngiliz ceza hukukunun ilkelerinden radikal bir kopuş görülmez. Yasal düzenlemelerin uygun gördüğü istisnai durumlar haricinde, kusursuz sorumluluk çok nadir uygulanır; belli bir düzeyde olan ihlallerden sorumluluk için "bilme", yani kast standart manevi unsurdur. Ancak bu alandaki düzenlemeler "ihmali sorumluluğun" bir türünü de içerir, buna göre bulut bilişim hizmetini verenler güncel bilginin görülebildiği hallerde harekete geçmek durumundadırlar; bunların "adil uyarma" ilkesi[128] gereğince hareket etmeleri gerekir ve herhangi bir yasa uygulayıcı idareye haber vermeksizin, süratle suç oluşturan içerikleri çıkarmalılar ya da bunlara erişimin engellenmesini sağlamalıdırlar[129].

J. Özel Mahkemeler

Hindistan ve Bangladeş gibi ülkelerde bilişim suçlarına bakmakla görevli özel mahkemeler kurulmuştur. Böylelikle yargı sisteminin deneyim ve bilgi eksikliklerinin önüne geçilmek istenmekte ve bu mahkemeler söz konusu ülkelerin yargı sistemlerinde çok önemli bir yer işgal etmektedir[130]. Ancak, ne İngiltere'de ne de diğer Anglo Amerikan hukuk sistemine dahil bir diğer ülkede bilişim suçlarına bakmakla görevlendirilmiş özel mahkemeler bulunmamaktadır.

K. Özel Hukuk Uygulamaları

İnternetin doğası ve kaynağı, kendi kendine düzenlemenin (self regulation)[131] ve özel hukuk uygulama mekanizmalarının, bilişim alanında işlenen suçlara verilecek yanıtların merkezinde yer alan bir bileşen olduğunu bizlere gösterir. Bu tür düzenlemeler, geniş bir zamana yayılarak işlerler; esasen bu uygulamalar bir yandan kamu hukuku uygulamaları ile de örtüşmektedir. Bu uygulamalar yalnızca kullanıcıları ve ilgili grupları kapsamayıp, ayrıca ve çok önemli olarak, internet iletişim sağlayıcıları gibi kullanıcıların internete erişimini sağlayan altyapı hizmetlerini sunan aracı kurumları da kapsarlar[132]. Dolayısıyla Birleşik Krallık'ta, bir bilişim suçuna ilişkin mahkûmiyet söz konusu olduğunda, bünyesine uygun olduğu hallerde özel hukuk yaptırımları da bunu izlemektedir.

---

128 Ashworth/Horder, s. 55.
129 Walden, pn. 2.246.
130 Walden, pn. 2.275.
131 Konu hakkında ayrıntılı bilgi için bkz: Jeanne Pia Mifsud Bonnici, Self-Regulation in Cyberspace, The Hague, TMC Asser Press, 2008, s. 9 vd.
132 Walden, pn. 2.276.

Ülkemizde müsadere, suç gelirlerine el koyma ve tüzel kişilere özgü yaptırımlar bunları kısmen karşılasa da, anılanlar bu alana özgü özel hukuk yaptırımı niteliğinde değildir. Ülkemiz hukuk sisteminde özel hukuka ilişkin bu alana özgü yolların oluşturulması ve ceza hukuku tedbir ve yaptırımlarından ayrı olarak işletilmesi gerekli ve zorunludur. Bu da iki hukuk sistemi arasındaki yapısal farklılıktan kaynaklanmaktadır.

L. Soruşturmada Özel Kişilerin Rolü ve Özel Kişiler Tarafından Uygulanabilecek Yaptırımlar

Bilişim suçlarının, özellikle de çocuk pornografisinin izlenmesi ve yetkili makamlara ihbar edilmesi konusunda ABD ve batılı ülkelerde özel kişi/kuruluşların ve sivil toplum kuruluşlarının çeşitli girişimleri bulunmaktadır. Bu sivil girişimlerin eylemlerine ek olarak, bilişim suçları çevrimiçi (online) ya da dijital hareket eden kendiliğinden hukuk uygulayıcıları (vigilantes) olan bireyler ya da gruplar tarafından da polise bildirilmektedir. Örneğin *US v. Jarrett* davasında[133] bir Türk bilişim korsanı tarafından iki ABD vatandaşının bilgisayarlarının "hack"lenmesi sonucu bu kişilerin bilgisayarlarında bulunan çocuk pornografisi içerikleri Alabama Polis Departmanına verilmiş ve bu içerikler söz konusu kişilerin suçlanmasında delil olarak kullanılmıştır[134].

Hepsi kendi açısından haklı olan farklı politik temellere dayalı olan ve göreceli olarak onarıcı adalet ve suçun önlenmesi bakış açısıyla, her bir olayda özel sektörün ve kamu sektörünün gerçekleşen bilişim suçları hakkında birbirlerine bilgi vermelerinin en etkili sonucu, verilecek cezanın yerine geçecek ya da onu tamamlayacak bir yaptırımın, tazminat talepleriyle birlikte uygulanmasıdır[135]. Ancak bu tür bir yaklaşım, uygunluğunun sınırlarına ilişkin politik sorunlar da ortaya çıkarmaktadır. Daha önce belirtildiği üzere bu tür bir yaptırım, suçlunun bilgisayar kullanmasının ya da internete erişiminin engellenmesidir. Buna alternatif bir yaklaşım, polisin suçluya hizmet veren ISS'ye bir rapor göndermesidir. Böylelikle bazı ISS'ler bu kişinin hesabını kapatmayı tercih edebilecek ve bu sektörde yer alan diğer oyuncular da kendilerine bilgi verildiğinde, suçluları müşteri olarak kabul etmeyecektir. Bu yaptırım *"e-ölüm cezası"* olarak anılmaktadır[136].

---

133 338 F 3d 339 (Va, 2003).

134 Walden, pn. 2.280.

135 Bu konuda ayrıntılı bilgi için bkz: Christopher T. Marsden, Internet Co-Regulation: European Law Regulatory Governance and Legitimacy in Cyberspace, Cambridge, Cambridge University Press, 2011, s. 43 vd.

136 EURIM, Policing the Internet, Submission to the Internet Governance Forum, July 2006, http://www.eurim.org.uk/activities/ecrime/eurim_IGF06paper.pdf, s. 3.

Bununla birlikte bu tür sınırlayıcı düzenlemeler hukuki gözetimin ve insan hakları hukukunun ilgisini çekmekte ve konusunu oluşturmaktadır. Bu tür bilgileri paylaşma mekanizması "olmaması gerektiği halde" kötüye kullanımlara açık olabilir[137]. Bu tür kaygılar nedeniyle AB kuralları, özellikle özel kişiler arasında gerçekleşen veri transferlerine ilişkin olarak AB üyesi devletlerin kolluk güçleri arasında işbirliğinin sağlanması amacıyla kişisel verilerin işlenmesinin korunmasını düzenler[138].

VI. BİRLEŞİK KRALLIK CEZA HUKUKUNDA BİLİŞİM SUÇU TÜRLERİ

Bilişim teknolojilerinin toplum üzerindeki etkisi son derece derin ve şiddetlidir[139]. Bu etki, bir sanayi toplumu olan Birleşik Krallık için de geçerlidir. İngiltere'de toplum, 1990 tarihli Bilgisayarların Kötüye Kullanılması Yasası (Computer Misuse Act 1990) öncesinde de bilişim teknolojileri kullanılarak gerçekleştirilen eylemlerle karşı karşıya kalmış ve bunlarla mücadele etmeye çalışmıştır. Bu hukuka aykırı eylemlere genellikle dolandırıcılık, hırsızlık ya da kişilere karşı suçlara ilişkin normlar uygulanmıştır. Buna rağmen ceza hukukunun sunduğu korumada çeşitli boşluklar söz konusu olmuştur. Bu hususa, özellikle Hukuk Komisyonu 1988 tarihinde yayınlamış olduğu Çalışma Raporunda işaret etmiştir[140]. Komisyon, yapmış olduğu çalışmalarda, özellikle yetkisiz erişim eylemlerine yoğunlaşmış ve bunları dikkate alarak bir hazırlık yapmıştır. Ancak final raporunu hazırlamadan önce finans ve bilişim sektöründen temsilcilerle yapılan görüşmeler neticesinde, yalnızca yetkisiz erişime ilişkin düzenleme yapılmasının yetersiz olduğu görülmüş ve bu grupların teklifiyle yetkisiz erişimin daha ağır başka suçların işlenmesinde araç (basamak) olarak kullanılması ve bilgisayarda yer alan verilerin yetkisiz olarak değiştirilmesinin de düzenlenmesi gerektiğine karar verilmiştir. Sonuçta, söz konusu yasa 1990'da yürürlüğe girmiş ve birçok sorunun da kaynağını oluşturmuştur[141].

Yasanın yürürlüğe girmesinden hemen sonraki on yıl içinde ve devamında eleştirmenler; yasanın eskidiğini, yasanın taslağının oluşturulduğu tarihlerde bilgisayarların bu kadar sofistike olmadığını, internetin ise henüz emekleme

---

137 Ben Wagner, Global Free Expression – Governing the Boundaries of Internet Content, Law Governance and Technology Series, Vol. 28, Switzerland, Springer, 2016, s. 11 vd.

138 Walden, pn. 2.283.

139 David Ormerod, Smith & Hogan's Criminal Law, 13th Edition, Oxford, Oxford University Press, 2011, s. 1045.

140 The Law Commission, Working Paper No 110, Computer Misuse. Ayrıca bkz: Martin Wasik, "Law Reform Proposals on Computer Misuse", Criminal Law Review, 1989, s. 257-270.

141 Neil MacEwan, "The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future" Criminal Law Review, Vol. 12, 2008, s. 955-967; Ormerod, Smith & Hogan's Criminal Law, s. 1045, 1046.

döneminde olduğunu belirtmişlerdir[142]. Buna bağlı olarak yasanın kapsamının genişletilmesine yönelik baskılar artmıştır[143]. Parlamento Tüm Partiler İnternet Grubu, yasayı gözden geçirmiş ve yasada yapılması gereken reforma ilişkin tavsiyelerde bulunan bir rapor hazırlamıştır[144]. Söz konusu grup, yasa hakkında dile getirilen sorunların "yürürlükteki yasada mevcut olan geniş boşluklardan" kaynakladığı sonucuna varmıştır. Buradaki özellikli bir husus, yasanın DoS saldırılarına uygulanabilirliği konusundadır, zira bu saldırılar yüzünden hukuka uygun olarak hareket eden kullanıcıların ticari web sitelerine erişimi engellenmektedir. Mahkemeler, 1990 tarihli Yasada yer alan suçların DoS saldırılarına uygulanabileceği şeklinde yorumda bulunmuştur[145]. Ancak bu tür hukuka aykırılıklarla mücadele edebilmek için bu konuya özgü suçların bulunmasının gerekli olduğu herkes tarafından bilinen bir gerçektir. Bu alandaki daha ileri baskılar, uluslararası sözleşmelerden kaynaklanmıştır[146]. 2006 yılında, Polis ve Adalet Yasası (Police and Justice Act 2006) ile CMA'da yer alan suçlara eklemeler yapılmış ve bilgisayarların kötüye kullanıma ilişkin yeni suç tipleri düzenlenmiştir. Bunlara daha sonra 2007 tarihli Ağır Suçlar Yasası (Serious Crime Act 2007) ile yeni eklemeler de yapılmıştır[147].

Son yıllarda, organize suçlarla mücadelede, hükümetlerin ve kolluk güçlerinin dikkatlerini, suç gelirlerinin aklanmasından elde edilen gelirleri hedef alacak şekilde değiştirdikleri görülmektedir. Bu yöndeki yasalar, diğer suçlara nazaran bu tür suçları biraz daha geniş kapsamlı ele almaktadır; bu bağlamda, örneğin yetkisiz değişiklikler yapılması gibi bir seri kişisel eylemden ziyade, haksız kazanç elde etmek için gerçekleştirilen eylemin arkasında yatan asıl amaca odaklanmaktadır. Sonuçta bilişim suçları da organize suçların bir parçasıdır ve bu tür yasalar bu suçlarla mücadele için de artarak kullanılmalıdır[148].

Bilgisayarların ve özellikle internetin sağladığı fırsatlardan ve kolaylıklardan yararlanmak suretiyle bunları istismar etmeyi seçerek geniş çapta zararların oluşmasına neden olan ve hukuka aykırı eylemler olan dolandırıcılık, pedofili, casusluk, korsan yayıncılık, suç gelirlerinin aklanması ya da haksız rekabette

---

142 Stephan Fafinski, "Access Denied: Computer Misuse on an Era of Technological Change" Journal of Criminal Law, Vol. 70, Issue 5, 2006, s. 424-442.

143 Buna karşın bunların tamamının bir reform isteği olduğu söylenemez, bkz: C. Holder, "Staying One Step Ahead of the Criminals", IT Law, Vol. 10, Issue 3, 2002, s. 17 vd.

144 Bu konudaki tartışmalar için bkz: G. Fearon, "All Party Internet (APIG) Report on the Computer Misuse Act", Comps. & Law, Vol. 15, 2004, s. 36 vd.

145 DPP v. Lennon [2006] EWHC 1201.

146 Bkz: Ian Walden, "Harmonising Computer Crime Laws in Europe", European Journal of Crime, Criminal Law and Criminal Justice, Vol. 12, Issue 4, 2004, s. 321-336.

147 Ormerod, Smith & Hogan's Criminal Law, s. 1046.

148 Walden, pn. 3.04.

bulunma vb. gibi yolları seçmiş olanlarla ceza hukukunun mücadelede çeşitli zorluklarla karşı karşıya kalmaya devam edeceğini öngörmek bir kehanet değil, gerçeğin tespitidir[149].

Bu alanda işlenen suçların sayısını hesaplamak son derece güçtür. İş dünyası kendisine karşı işlenen suçları raporlamakta isteksizdir; zira bildirimde bulunmaları güvenliklerindeki zafiyetlerinin ortaya çıkmasına ve müşterilerin iş yapmaktan caymasına yol açabilir. Öte yandan bu alandaki mevzuatın oldukça karmaşık olması nedeniyle yapılacak suçlamaların sayısında bir azalmanın gerçekleşebileceği de düşünülebilir[150]. Nitekim bu konuya yaklaşıma daha önce değinmiştim.

Birleşik Krallık'ta, yukarıda bahsetmiş olduğum, bu ve buna benzer çeşitli yasalarda bilişim suçlarına ilişkin düzenlemeler yapılmıştır. Bu alana ilişkin çalışmaların çoğunluğunda görüldüğü gibi, söz konusu yasaları ve bunların birkaç maddesini alt alta sıralamak yerine, bu suçlardan önemli gördüğüm bazılarını, bunların unsurlarını ve hangi mahkeme kararlarına konu olduklarını aktarmanın bir karşılaştırmalı hukuk çalışması açısından daha uygun olacağını düşünüyorum.

A. Bilgisayarla İlgili Suçlar

1. Bilişim Casusluğu

Casusluk faaliyetleri, uluslararası ilişkiler dünyasında daima rol almıştır. Hükümetler, teröristler ve diğerleri, yabancı hükümetlerin ve diğer kuruluşların, özellikle savunma ve ulusal güvenlik konularıyla ilgili olarak, neler yaptığını öğrenebilmek için casuslar kullanmışlardır. Siber alan, bu tür gizli bilgilere erişim için alternatif bir yol sunar. Siber casusluk hakkındaki klasik bir örneklerden biri, Markus Hess'in faaliyetleridir. Bu kişi, 1980'ler boyunca, internetin öncüsü olan ARPANET'i kullanarak, Hannover Almanya'daki üssünden 400'den fazla ABD askeri bilgisayarına erişim sağlayarak Sovyetler Birliği'ne bilgi sağlamıştır[151]. Devlet tarafından yapılan yabancı istihbarat faaliyetleri bakımından, Edward Snowden'in yapmış olduğu ifşaatlar[152], ABD'nin sinyal casusluğu aktivitelerinin (SIGINT), düşmanlarına olduğu kadar aralarında Birleşik Krallık'ın da olduğu müttefiklerine de uzandığını ortaya koymuştur[153].

---

149 Morris, The Future of Netcrime, s. 13-19; Ormerod, Smith & Hogan's Criminal Law, s. 1047.
150 Ormerod, Smith & Hogan's Criminal Law, s. 1047.
151 Detaylı bilgi için bkz: Cliff Stoll, Cuckoo's Egg, New York, Pocket Books, 1998.
152 Bkz: Snowden Surveillance Archive, https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library. cgi, 12.8.2016.
153 Walden, pn. 3.15.

Belli bazı devlet sırrı niteliğindeki bilgilerin elde edilmesi ve açıklanması uzun zamandan beri suç olarak düzenlenmektedir. Aynı ölçüde, açık ve şeffaf bir devlet, öncelikle liberal ve demokratik bir toplumun varlığını gerektirir. Bunun için uygun bir dengenin sağlanmasının ve yürütülebilir kuralların oluşturulmasının başarılması, açıkça görülen bir gerilimin ortaya çıkmasına neden olur. İngiliz hukukuna göre; 1911, 1920 ve 1989 tarihli Devlet Sırrı Yasaları (Official Secrets Acts), belli bazı devlet sırrı niteliğindeki bilgilerin elde edilmesini ve açıklanmasını suç olarak düzenlemektedir. Bu bilgilerin niteliğine bağlı olarak kişilerin suç işlemesi mümkün olabilmektedir[154].

Bu yasalarda devlet sırrının ne olduğu açıkça tanımlanmamıştır. Bu bilgilerin, düşmanlar tarafından kullanılabilecek bilgiler olması yeterlidir. Konumuzla doğrudan ilgili olan husus ise bu bilgilerin nerede bulunduğuna ilişkindir. 1911 tarihli Devlet Sırları Yasası'na göre "yasaklanmış alanlara" girilerek gizli bilgilerin elde edilmesi suçtur; bu yasada yer alan "yasaklanmış alanlar" kavramı oldukça geniş anlaşılmıştır. Ancak yasada düzenlendiğinde bu kavram "fiziksel alanlar" olarak tanımlanmıştır; tarihsel ve mantıksal olarak bu kavramın "sanal" dünyada yasaklanmış alanlarda bulunan bilgisayarlara ve bilişim sistemlerine girilerek bilişim sisteminin güvenliğinin kırılması ve hukuka aykırı olarak sisteme girilmesini içerecek şekilde düzenlenmiş olması mümkün değildir[155].

Bir bilişim sisteminde yer alan devlet sırlarının hedef alınarak suçun işlenmesi halinde, kıyas yapmak suretiyle, yetkisiz erişim suretiyle sistem bütünlüğüne karşı işlenen suçlarla dolaylı bir koruma sağlanabilir (zira Anglo Amerikan ceza hukuku sisteminde kıyas ve genişletici yorum mümkündür). Gerçekten de, ABD'de bilgisayarın bütünlüğüne yönelik suçları düzenleyen temel yasa olan Bilgisayar Dolandırıcılığı ve Kötüye Kullanılması Yasası'nda (the Computer Fraud and Abuse Act), öncelikle "Birleşik Devletler Hükümeti tarafından kullanılan", sınıflandırılmış ya da sınıflandırılmamış bilgiler korunur[156]. Bu yasa, çok gok geniş bir kapsamda özel ve kamusal bilişim sistemlerini korumak[157] için getirilmiştir[158].

Bu tür bilgi açıklamalarında internetin potansiyel rolüne ilişkin bir örnek, Richard Tomlinson olayıdır. Tomlinson, İngiliz istihbarat servisi olan MI6'te çalıştığı yıllarını anlatan bir kitabı yayınlatmak isterken[159], 1997 yılında 1989

---

154 Walden, pn. 3.16.

155 Walden, pn. 3.17-3.20.

156 Computer Fraud and Abuse Act, Pub L No 98-473, Title II, Chapter XXI, s 2101(a), 98 Stat 1837, at 2190 (1984).

157 "Korunan biligisayarlar" 18 USC s 1030(e)(2)'de tanımlanmaktadır.

158 Walden, pn. 3.21.

159 Tomlinson sonrasında bu kitabı Moskova'da yayınlatmayı başarmıştır bkz: Richard

tarihli Devlet Sırları Yasası'nı ihlal etmekten suçlu bulunmuş ve hapis cezasına çarptırılmıştır[160]. Sonrasında bu kişi MI6 ajanlarının listesini web sitesinde yayınlamaktan suçlanmıştır. Bu liste, listenin internet üzerinden yayınlanması devletin avukatları tarafından önleninceye kadar çok, geniş bir çevrede defalarca yeniden yayınlanmıştır; ayrıca Tomlinson'ın bu konuyla ilgisi hiçbir zaman ispatlanamamıştır[161].

Devlet sırlarını korumaya yönelik işleyişin rejimi 2000 tarihli Bilginin Özgürlüğü Yasası (the Freedom of Information Act 2000) ile yürürlüğe girmiştir. Bu yasa ile ileriyi etkileyen (proaktif) yayınların gerekli olması veya bireysel bilgi edinme taleplerine yanıt verme yükümlülüğünün olması halinde, devlet tarafından nasıl bilgilendirme yapılacağına ilişkin bir açıklama rejimi oluşturulmuştur[162].

Geçmişte, devlet sırlarının korunmasına ilişkin rejim çok geniş düzenlendiği için eleştirilmiştir; çünkü devlet güvenliğiyle uzaktan ilgili olan bilgiler dahi ceza sorumluluğunun doğmasına yol açabiliyordu[163]. Ancak bu rejimde yapılan reform, idare hukuku düzenlemelerini ve uygulamasını değiştirmiştir; en dikkat çekici husus ise Bilginin Özgürlüğü Yasası'nın, devlet sırlarının ceza hukuku tarafından aşırı derecede korunduğuna yönelik pekçok kişinin algısını değiştirmiş olmasıdır. İleride internetin, bu kuralların etkinliğinin altını oyduğu görülebilir; çünkü internette, üzerindeki bilgilere küresel düzeyde ulaşılabildiği için, bu bilgiler bir kere yayınlandıktan sonra bunlar üzerindeki ulusal hukuki kontrol en iyi şartlarda geçici olabilmektedir. Wikileaks bu konudaki en iyi ve bilinen örneği oluşturur. Bu, Birleşik Krallık'ta, 1980'lerin ortalarında Peter Wright'ın "Casus Avcısı / Spycatcher" isimli kitabının yayınlanması ile Thatcher Hükümetinin yüzleştiği bir durumdur. Hükümet, öncelikle kitabın yayınlanmasının önlenmesine ilişkin mahkemeden bir tedbir kararı alabilirken, diğer yargı çevrelerinde söz konusu kitap bir kere internet üzerinden yayınlandığı için, kalıcı tedbir talebi mahkeme tarafından reddedilmiştir[164].

Tomlinson, The Big Breach: From Top Secret to Maximum Security, Narodny Variant Publishers, Moskova, 2001.

160 A. S. Reid/N. Ryder, "The Case of Richard Tomlinson: The Spy Who Emailed Me", Information and Communications Technology Law, Vol. 9, Issue 1, 2000, s. 61 vd.

161 Walden, pn. 3.23.

162 Bu rejimin tarihçesi, teorik alt yapısı, uygulaması ve ilgili düzenlemeleri için bkz: Philip Coppel, Informations Rights: Law and Practice, 4th Edition, Oxford & Portland, Hart Publishing, 2014, s. 1 vd.; Walden, pn. 3.24.

163 Bkz: D. Williams, Not in the Public Interest; the Problem of Security in Democracy, London, Hutchison, 1965.

164 Attorney-General v. Guardian Newspapaers [1987] 1 WLR 1286, Walden, pn. 3.26.

2. Ticari Sırlar ve Gizli Bilgilere İlişkin Suçlar

Endüstriyel casusluk, modern iş yaşamında sıklıkla görülen bir husustur, zira bir iş yapış modeli ya da "know-how" artan bir şekilde değerli bir araç haline gelebilir. Bugün bu tür aktiviteler; bilgiye ulaşmanın bir yolu olarak bilişim sistemlerinin güvenliğinin kırılması (hacking), casus yazılımlar (spyware)[165], elektronik gizli dinleme, USB hafıza kartının bir araç olarak yararlı bilgilerin yerinin değiştirilmesi için kullanılması gibi biçimlerde, ICT'lerin kullanılması suretiyle gerçekleştirilir. Bu tür casusluk, rakip şirket ve bireyler arasında söz konusu olduğu gibi, devletler düzeyinde de olabilir[166]. Bu tür eylemler, bilgiye erişim hakkı olan mağdur kuruluşun içinden birilerinin suç ortaklığı ile başarılabildiği gibi, dışarıdan kişilerin hukuka aykırı eylemleri kendilerinin yapması ya da bunun için üçüncü kişileri kullanması (ticari bir hizmet olarak bunlardan hizmet alınması) yoluyla da gerçekleştirilebilir. Ticari sırların değerinin paraya çevrilmesi ise karmaşık bir yöntemdir; bu, genellikle bu tür bilgilerin spekülatif bir temelden ziyade, mevcut düzeni korumak için (rekabetin önlenmesi) elde edildiği anlamına gelir[167].

Siber endüstriyel casusluk alanında en öne çıkan örnek İngiltere'nin dışında çalışan, hem İsrail hem de Alman vatandaşı olan Bay ve Bayan Haephrati olayıdır. Bu ikili ve çok sayıdaki önemli iş adamı, İsrail iş yaşamına karşı endüstriyel casusluk yapmaktan gözaltına alınmışlardır. Bu çift, geliştirdikleri ve yaydıkları bir Truva atı yazılımıyla, rakip şirketlerin bilişim sistemlerine gizlice girerek erişim için rıza alınması ve bu yolla rakip şirketler tarafından işe alınan özel soruşturmacılar tarafından rakip şirketlerin ticari sırlarının öğrenilmesini sağlamakla suçlanmıştır. Söz konusu kötücül yazılım, mağdura gönderilen bir elektronik postanın açılması ya da bir ticari iş teklifinde bulunan bir diskin mağdura gönderilmesi ve mağdurun bilgisayarında çalıştırılması suretiyle çalışmaya başlamaktadır. Söz konusu kötücül yazılım ABD'de ve İsrail'de bulunan FTP sunucularında yer almaktadır. Haephrati'ler, sonrasında İsrail'e iade edilmişlerdir. Duruşma öncesi yetkili makamlarla yapılan pazarlıklar neticesinde, özel soruşturmacılara karşı sağladıkları deliller sayesinde hapis cezasının indirilmesini sağlamışlardır[168].

---

165 Bkz: Ashton Investmets Ltd and another v. OSJC Russian Aluminium and others [2006] All ER (D) 209 (Oct), bu davada bir Rus şirketi, tarafları ilgilendiren devam eden bir davada önemli bilgileri elde etmek için karşı taraf olan İngiliz şirketinin bilişim sistemlerine uzaktan erişmek iddiasıyla suçlanmıştır.

166 Örneğin bkz: US Department of Justice (DoJ), "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Press Release, 19 Mayıs 2014, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage, 1.1.2017.

167 Walden, pn. 3.39.

168 Walden, pn. 3.40.

Esas olarak pekçok hukuk sisteminde ticari sırların hukuka aykırı olarak elde edilmesi, diğer fikri mülkiyet haklarının korunmasına benzer şekilde, öncelikle özel hukuk uyuşmazlıklarının konusu olarak görülmüştür[169]. Ancak ticari bilgilerin artmasının bir sonucu olarak, pek çok gelişmiş ülke söz konusu bilgilerin korunması amacıyla mevcut özel hukuk kurallarının yanına ek olarak ceza hukuku normlarını da eklemişlerdir.

Birleşik Devletler'de ticari sırlar, federal düzeydeki ceza hukuku kurallarıyla korunurlar[170]. Söz konusu yasa uyarınca görülen örnek bir olay *US v. Lange* davasıdır[171]. Sanığın mutsuz bir eski işçi olduğu bu davada sanık, eski işvereninden elde ettiği elektronik ticarete ilişkin sırları satmaya teşebbüs etmekten suçlu bulunmuştur[172].

Ticari bilgilerin ceza hukuku tarafından koruma altına alınması hususu İngiltere'de, Hukuk Komisyonunun bir tavsiye kararının konusunu oluşturmuştur. Buna göre, ticari sırların açıklanması veya yetkisiz kullanılmasının suç haline getirilmesi önerilmiştir[173]. Bu tür bir suç "ticari sırrın" açık bir biçimde tanımlanmasını ve bu tanımlamanın bir takım kriterlerinin bulunmasını gerektirmelidir. İlk olarak, bilgi sahibi açıkça ya da zımnen bu bilgilerin gizli kalması yönündeki isteğini göstermelidir. Bilişim sistemlerinin bütünlüğüne ilişkin suçlardaki yetkilendirmeye benzer şekilde bilginin sahibi üzerinde, bundan dolayı bir davranışta bulunma yükümlülüğü bulunmalıdır. İkinci olarak, gizli bilginin yeterli gizlilik niteliğinin olmasına benzer şekilde, söz konusu bilgi kamuoyu tarafından bilinmemelidir[174]. Üçüncü olarak, söz konusu bilginin gizli tutulmasının ekonomik bir değeri olmalıdır, böylelikle bu bilginin ceza hukuku tarafından korunmasının akılcı bir yönü olmalıdır[175].

Suçun işlenmesi için, kişi gizli ticari sırrın hem başkasına ait olduğunu hem de bu bilgiyi açıklamak ya da kullanmak için bilgi sahibinin rızasının olmadığını bilerek, söz konusu gizli ticari sırrı kullanmalı ya da açıklamalıdır. Hukuk Komisyonuna göre bu tür bir suç, diğer pek çok ülke hukukunda olduğu gibi İngiliz hukuk sisteminde de yer almalıdır[176].

---

169 Bkz: C. D. Freedman, "Criminal Misappropriation of Confidential Commercial Information and Cyberspace: Comments on the Issues", International Review of Law, Computers and Technology, Vol.13, 1999, s. 147 vd.

170 The Economic Espionage Act of 1996, Pub L No 104-294, 110 Stat 3488 (1996), codified at 18 USC s 1832. En ağır ceza on beş yıl hapis cezasıdır.

171 312 F 3d 263 (7th Cir 2002).

172 Walden, pn. 3.43.

173 Law Commission, Legislating the Criminal Code: Misuse of Trade Secrets, Consultation Paper No 150, 1997.

174 Coco v. AN Clark (Engineers) Ltd [1969] RPC 41.

175 Walden, pn. 3.49.

176 Law Commision, pn. 5.3 ve 5.8; Walden, pn. 3.50.

Bugüne kadar Hukuk Komisyonunun girişimleri bir ilerleme gösterememiştir. Ancak bazı durumlarda 2006 tarihli Dolandırıcılık Yasası'nın 4. maddesinde (Fraud Act 2006) yer alan şeklinin uygulanması mümkündür: *"Durumunun kötüye kullanılması suretiyle dolandırıcılık"*. Bunun için en iyi ve sık karşılaşılan örnek, işten ayrılan ancak işvereninin bilişim sistemlerine erişim hakkı olan bir çalışanın, bu hakkı kullanarak eski işverenine ait değerli bilgileri, (örneğin, müşteri listesi gibi) bu hareketinin şirket kurallarına aykırı olduğunu bilmesine rağmen, gelecekteki işverenine vermek amacıyla kopyalamasıdır. Bu tür bir senaryo, iş hukuku açısından da sadakat ve gizlilik yükümlülüğünün ihlali nedeniyle çeşitli taleplere yol açabilir[177].

İngiltere'de böyle bir hükmün eksikliğinin çekilmesine ve bunun düzenlenmesinin teklif edilmesine karşın, ülkemizde 2005 yılından beri böyle bir düzenleme TCK'da yer almaktadır. TCK'nın *"Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması"* başlıklı 239. maddesinde açıkça dijital ortamda bulunan verilerden bahsedilmeksizin, ticari sır niteliğindeki bilgilerin yetkisiz kişilere verilmesi veya ifşa edilmesi suç olarak düzenlenmiştir. Suçun konusunu oluşturan ticari sırların içine dijital ortamda veri olarak tutulan sırların da girdiğine şüphe yoktur. Ancak, ülkemiz uygulamasında buna ilişkin bir mahkeme kararına rastlamadığımı belirtmeliyim. Zira, özellikle uygulamada, bu tür bilgilerin gizli ticari sır olduğunun soruşturma ve kovuşturma makamlarına anlatılmasında, bu yapılsa bile gerçekleştirilen eylemin ispatında (Zira soruşturma makamları bu tür olayları ticari bir uyuşmazlık görüp yeterli ve gerekli ekip, ekipman ve zamanı ayır(a)mamaktadırlar.) zorluklar çekilmekte, bu da uyuşmazlığın mahkeme önüne taşınması, karar oluşturulması ve bu kararın üst dereceli mahkemelerin denetiminden geçmesine olanak tanınmamaktadır.

3. Dolandıcılık Suçu

Birleşik Krallık'ta, bilgisayarlar ile ilgili davaların büyük çoğunluğunda, "Hırsızlık Yasası" (Theft Act) suçlamada bulunmak için yeterliydi. Örneğin *Thompson* davasında[178], Kuveyt'te bulunan bir bankanın çalışanı bankanın bilgisayarlarında başkalaştırma yaparak (manipülasyon) kendi idaresindeki bazı müşterilerinin hesaplarından ve kredi hesaplarından zimmetine para geçirmiştir. Daha sonra bu kişi Birleşik Krallık'ta bulunuyorken, paraların burada bulunan hesaplarına transferi için bir transfer emri göndermiştir; işte bu noktada gerçekleştirdiği dolandırıcılık işlemleri keşfedilmiştir. Bununla birlikte, ceza hukukunun diğer alanlarında da olduğu gibi, geleneksel

[177] Örneğin bkz: Shepherds Investments Ltd v. Walters [2006] EWHC 836; Corporate Express Ltd v. Day [2004] EWHC 2943; Gabem Group Ltd v. Mahatma [2002] EWHC 2221; Intelsec Systems Ltd v. Grech Cini [2000] 1 WLR 1190; Walden, pn. 3.51.

[178] [1984] 3 All Er.

hukuki düzenlemelerin tanımlamaları, bilgisayarın ortaya çıkışından önce öngörülmeyen bazı uygulama sorunlarının ortaya çıkmasına neden olmuştur. Birleşik Krallık Hırsızlık Yasası'nda da olduğu gibi bazı ülkelerin düzenlemelerinde, dolandırıcılık suçunun oluşması için gerçek bir kişinin aldatılması gerekir[179]. Bu durum ülkemiz hukuku açısından geçerli olup, bilişim sistemleri kullanılmak suretiyle nitelikli dolandırıcılığın düzenlendiği TCK m. 158/1-f'ye göre de dolandırıcılık suçunun oluşabilmesi için gerçek bir kişiye karşı aldatıcı nitelikte hareketlerin bilişim sistemleri kullanılmak suretiyle yapılması gerekir.

İngiliz mahkeme kararları aldatma eylemini ve dolayısıyla dolandırıcılık suçunu daha geniş bir çerçevede tanımlarlar. Ancak, hem yukarıda anılan düzenlemelerin hem de mahkeme kararlarının yeterli olmaması ve bu alanda bir boşluk oluşması nedeniyle, İngiltere'de yasa yapmanın ön aşamasında oluşturulan Hukuk Komisyonu, 2002 yılında yayınladığı Dolandırıcılık Raporunda, özellikle dürüst olmayan bir şekilde internet üzerinden alınan servislerin suç olarak tanımlanması gerekliliği üzerinde durmuştur. Mayıs 2004'te İçişleri Bakanlığı, Hukuk Komisyonunun hazırladığı rapora yanıt olarak bir sonuç belgesi yayınlamıştır. Bunu ise Hukuk Komisyonunun hazırladığı "servis hırsızlığı" önerisini de içeren dolandırıcılık suçunda reform için tavsiyeler izlemiştir. Sonuçta 2006 tarihli Dolandırıcılık Yasası (The Fraud Act 2006) ile internet servislerinden sahtecilikle ve aldatmayla hizmet alınması suç haline getirilmiştir[180].

Bu yasadaki suç tanımıyla birlikte, suçun oluşması için yasada yazılı olmayan diğer üç unsurun da bulunması gerekir. Bunlardan ilki verilen hizmetin şartlarına odaklanmıştır; buna göre hizmet ücret karşılığı verilmiş ya da verilecek olmalıdır. İkinci unsur, fail bu ücreti ödemeksizin hizmeti almış olmalıdır. Üçüncü unsur ve suçun ikinci manevi unsuru ise, fail bu hizmetin elde edilebilir ya da elde edilebilecek olduğunu bilmeli ancak ödeme yapma niyetinde olmamalıdır[181].

4. Sahtecilik Suçu

Günlük yaşamlarımızda, yirmi liralık banknottan, sürücü ehliyetine ya da sigorta poliçesine kadar geniş bir alanda belge kullanmaktayız. Bu belgelerin birçoğu belli bir konuda ya kimliğimizi tanımlamak ya da konunun doğruluğunu tevsik etmek için kullanılır. Bu fiziksel belgelerin sahtelerinin üretilmesi, bilişim teknolojilerindeki gelişmelerin bir faydası olarak suç dünyasının önemli

[179] Örneğin Alman Ceza Kanunu (Strafgesetzbuch - StGB) m. 263; ayrıca bilgisayar dolandırıcılığı için ayrı bir suç tipi eklenmiştir (m. 262a). Walden, pn. 3.54.

[180] Walden, pn. 3.55-59.

[181] Walden, pn. 3.60.

konularından birini oluşturur. Günümüzde en orijinal belgelerin dahi sahteleri bilgisayarlar aracılığıyla yapılabilmektedir; buna bağlı olarak bilgisayarlar, bunların sıklıkla tespit edilemeyeceği yöntemlere olanak sağlar. Günümüzdeki yazılım temelli dijital manipülasyon uygulamaları, en amatör sahtekârlara dahi en güçlü araçları sağlamaktadırlar[182].

Siber alanda failler, geniş kaynaklardan elde ettikleri bilgileri kullanarak, yeni haklar oluşturabilecekleri gibi sahte belgeleri kullanarak mevcut hakları da istismar edebilirler. Bu bilgiler, sosyal mühendislik teknikleri kullanılmak suretiyle mağdurların kendilerinden elde edilmektedir; zira insanların bilgilerini açıklamaları için yine insanlar tarafından gerçekleştirilen hileli hareketler, veri güvenliği için getirilen mekanizmaların ve prosedürlerin üstesinden gelinmesinde yardımcı olmaktadır. Bu tekniklerin başarısı kısmen insanların internet üzerinden mahrem bilgilerini açıklamaya hazır olmalarından (örneğin, sosyal arkadaşlık sitelerinde olduğu gibi) dolayı kolay olmaktadır. Bu alandaki bir başka seçenek ise failin, bir elektronik ticaret sitesinin müşteri veri tabanının güvenliğini kırarak kredi kartı bilgilerini ve müşterilere ait diğer belgeleri ele geçirmesidir. Bu her iki hareket de İngiliz hukukunda 1981 tarihli Sahtecilik ve Kalpazanlık Yasası (Forgery and Counterfeiting Act 1981) gereğince suç oluşturmaktadır[183].

B. İçerikle İlgili Suçlar

1. Fikri Mülkiyet Suçları

Londra Şehir Polisi tarafından, Eylül 2013 tarihinde, "Polis Fikri Mülkiyet Suçları Bölümü" (Police Intellectual Property Crime Unit – PIPCU) isimli bir bölüm kurulmuştur. Bu bölüm, birçok etkinliğinin yanında Haziran 2014 tarihinde, "Yaratıcı Operasyon" isimli reklam değiştirme girişimini başlatmıştır. Buna göre, içeriğinde fikri mülkiyet haklarını ihlal eden ürünlere yer veren internet sitelerin bilişim sistemi güvenliği bizzat polis tarafından kırılarak (hacking), bu siteleri ziyaret edenlere yönelik olarak sitenin reklam alanları değiştirilmek suretiyle bu alanlara "söz konusu sitenin cezai soruşturma geçirdiği" duyurusu konulacaktır. Bu proje, Birleşik Krallık reklam endüstrisi ile birlikte yürütülmekte ve yalnızca Birleşik Krallık çıkışlı IP adreslerine erişim sağlayan ziyaretçilere uygulanabilmektedir; ancak bu tür sitelerin gelir akışını bozacak şekilde dizayn edilmiş bir projedir[184].

Bu yaklaşım Birleşik Krallık'ta fikri mülkiyetin ne kadar çok önemsendiği ve bu hakların ne kadar sıkı bir biçimde korunduğuna ilişkin son derece önemli bir örnektir.

---

182 Örneğin Adobe Photoshop CC gibi yazılımlar. Walden, pn. 3.88.
183 Walden, pn. 3.89.
184 Walden, pn. 3.120.

2. Pornografi

Hukuki bir yaklaşım olması açısından genel pornografik görüntüler ile çocuk pornografisi gibi özel alt bölümlere ayrılmış pornografik görüntüler arasında ayrım yapılması gerekir; zira hukuk uygulayıcı güçlerin işlemleri özellikle bu alt bölümlere odaklanmıştır. Çocuk pornografisine karşı olan yasalar öncelikle bu görüntülerin oluşturulması sırasında gerçekleşen çocuk istismarı ile ilgilenmektedir; ikincil olarak ise bu ürünlerin tüketilmesinin sonuçlarına eğilmektedir. Bu bağlamda çocuk pornografisi suçları, diğer pornografik ve müstehcen görüntülerden esaslı bir biçimde farklıdır; bu suçlarda söz konusu materyallerin tüketicileri üzerindeki, işlenecek potansiyel suçlardan cinsel işlev bozukluklarına, şiddetten uyuşturucu kullanımına kadar etkilerine odaklanılmaktadır[185].

Geleneksel müstehcenlik alanında, çocukların müstehcen materyallere erişimi, söz konusu ürünün fiziksel çıkışının sağlandığı mecranın yöneticisi tarafından erişimin kontrol altına alındığı bir yerde (örneğin, dergi ya da kitap satışı gibi) önemli bir sorun değildir; ancak internet alanında yaşın doğrulanması gibi uygulamalar yeterli olmamakta, bu da çeşitli suçların ortaya çıkmasına neden olmaktadır. Dolayısıyla şu hususların önceden öngörülmesi gerekir: İnternet kullanıcılarına, arama motorları ve "meta-tags" gibi tamamlayıcı teknikler yoluyla materyale erişim için yerleştirme kontrolü yapmaksızın, pornografik materyallere erişimi agresif bir biçimde teşvik eden bir sitenin, çocukların bu sitelere ilgileri çekilebilecek ziyaretçiler olması temeline dayanılarak sorumlu tutulmaları mümkündür. Bu görüş, potansiyel olarak müstehcen içerik barındıran ve alıcının istemi olmayan bir elektronik postanın gönderilmesi halinde çok daha kuvvetli hale gelmektedir[186].

Bu konuya ilişkin bir yargılama esnasında jürinin konu hakkında karar verirken güttüğü amaç, sayısal çokluk (nicelik) değildir; soruşturmanın gerçekte kaç adet kişinin ve hangi tipteki insanların bu tür bir siteyi ziyaret ettiğini göstermesi gerekli değildir; esas güdülen amaç çocuklar gibi kırılgan varlıkların potansiyel olarak söz konusu siteleri ziyaret edip edemeyeceklerinin ortaya konulmasıdır. Buna bağlı olarak jürinin, çocukların içerikleri görebilme olasılıkları hakkında karar verirken bu konudaki eşik sayısal değerin ne olduğu hususunda hala sorular bulunmaktadır. *Calder ve Boyars Ltd* davasında Yargıç Salmon *"kayda değer orantının"* gerektiğini belirtmiştir[187]. Buna karşın bu yaklaşım *DPP v. Whyte*[188] davasında Lord Pearson tarafından reddedilmiştir,

[185] Walden, pn. 3.129.
[186] Walden, pn. 3.132.
[187] [1969] 1 QB 151, at 168.
[188] [1972] AC 849, at 866F.

Lord Pearson'a göre *"de minimis"*[189] ilkesi gereğince bazı insanların etkilenmesi yeterlidir.

Koprofili[190] görüntülerini tasvir eden sayfalara internet üzerinden herkesin erişebileceği şekilde bir çeşit ön izleme sağlayan ABD kaynaklı "sewersex.com" sitesi hakkındaki *Perrin* davasında[191], mahkeme *"ihmal edilebilir sayıdan fazlası"* argümanına karşı *"kayda değer orantı"* görüşüne dayanan iddiayı (savunmaya yönelik iddiadır) reddetmiştir. *Perrin* davasının devamı sürecinde hükümet, çocukların ulaşabileceği olası materyallere ilişkin müstehcenliğin eşiği ile ilgilendiklerini, örneğin *"ruhsatlı erotik mağazalarda 18 yaş ve üstündekilerin erişebildiklerine karşılık gelen cinsel açıklığın derecesinin"* ne olması gerektiğini tartıştıklarını belirtmiştir. Bu tür bir erişim, materyal *"uygun bir ödeme bariyerinin ya da diğer genel kabul edilen yaş tanımlama sisteminin arkasında"* değilse, örneğin materyal pornografi sitesinin açılış sayfasında ise ve ticari olmayan kullanıcı tarafından sağlanan materyal ise, *"olası"* sayılmaktadır[192].

Siber alanda yayınlama hareketini oluşturan nedir? Yayınlamak ne anlama gelmektedir? Müstehcen bir içeriğin web sitesinden indirilebilir hale getirilmesi ya da P2P bağlantısıyla transfer edilmesi yayınlamayı oluşturur mu? İletim, gönderici tarafından alıcıya bilgi gönderilmesinin diğer anlamıdır, bir diğer anlatımla göndericinin gönderdiği bilginin alıcı tarafından alınmasıdır. Benzer bir anlamsal sorun, telif hakkı alanında da ortaya çıkmıştır. Bu alandaki yasal reform daha açık hale getirmektedir ki, topluma telif hakkına tabi bir ürünün nakledilebilmesi için buna ilişkin münhasır bir yetki gerekir; bu yetki, hak sahiplerinin bireysel olarak seçtiği yer ve zamanda söz konusu ürüne toplumu oluşturan bireylerin erişebilmesi anlamına gelir. Mahkemeler bu noktayı yorumlamakta güçlü bir yaklaşım sergilemektedirler, *Fellows ve Arnold*[193] davasında mahkeme; yayınlamanın, bilginin erişime hazır halde tutulması şeklindeki pasif bir işlemden ziyade bir şekilde aktif bir işlem gerektirdiği yönündeki görüşü reddetmiştir[194]. Dolayasıyla bir içeriğin pasif bir biçimde erişime açık tutulması da aktif bir eylem gerektirmeksizin "iletim" olarak kabul edilmektedir. Kısacası iletim eylemi, ihmali bir hareket ile de gerçekleşebilir.

---

189 Bu ilke şu iki önermenin birleşmesinden oluşmaktadır: Kayda değer bir oranın yozlaştırılması ve ayartılması ve ihmal edilebilir sayıdaki olası kişilerden fazla olması.

190 Dışkı görüntüsü ve dışkı yemekten zevk alınan cinsel yönelim.

191 [2002] EWCA Crim 747.

192 Gillespie, Cybercrime, s. 209; Walden, pn. 3.133.

193 [1997] 2 All ER 548.

194 Walden, pn. 3.135.

Waddon[195] davasında sanık *"ekstrem sapıklık"* başlıklı bir web sitesini yönetmekteydi. Bu siteye bir polis memuru tarafından erişim sağlanarak müstehcen görüntülerin indirilebilmesi için üye olundu. Davanın temyiz aşamasında savunma makamının sanığın web sitesine söz konusu içeriklerin iletimi sağlamasından ve aynı şekilde bu içeriklerin polis memuruna da iletilmesinden dolayı sorumlu olduğu kabul edildi. Ancak yine de mahkeme, bireyin sonraki iletimini kast etmeden siteye içerik yüklemesi halinde durumunun ne olacağına ilişkin kuralı sorguladı. Mahkeme bu konudaki kurala karşı çıktı ve yayınlamanın yalnızca tek ve basit bir eylemden oluşmadığına, bunun çoklu hareketlerden oluştuğuna, içerik her indirildiğinde devam eden yayınlama hareketinin gerçekleştiğine ilişkin görüşünü açıkladı. Bu bağlamda ilk olarak, içeriğin internete yüklenmesiyle fail tarafından suçun maddi unsuru gerçekleştirilmektedir, ancak devamında içeriğin indirilmesiyle mağdur tek başına ya da fail ile birlikte harekete devam etmektedir. Buna ek olarak eylemin kapsamlı bir biçimde ele alınması, sonuçta *Waddon* davasındaki tali gerekçenin yayınlamanın birden çok yerde gerçekleşmesi ve buna bağlı olarak suçun birden fazla yargı yetkisinin kapsamına girmesi ihtimalini artırmaktadır[196]. Bu duruma daha sonra *Perrin*[197] davasında yalnızca değilnilmiştir[198]. Ancak her iki davada da derinlemesine bir inceleme yapılmamıştır[199].

Smith (Gavin)[200] davasında, sanık canlı internet sohbetinde çocuklara karşı sadistçe cinsel davranışları da içeren çeşitli cinsel fanteziler hakkında açık seçik konuşmalar yapmak suçlamasıyla yargılanmıştır. Yargılama esnasında sanık, görüşmenin diğer tarafınca ilerleyen zamanda konuşmanın yayınlamasının beklenilmediği hallerde, yalnızca bir kişiyle iletişim halinde olmanın yayınlama sayılamayacağı görüşünü başarıyla savunmuştur. Bu yorum, temyiz mahkemesi tarafından geri çevrilmiştir. Mahkemeye göre yalnızca bir alıcı olduğunda bunun yayınlama olarak kabulü mümkündür; zira bu bir kişinin, söz konusu içerik tarafından kötüye yöneltilmiş ve ahlakı bozulmuş tek kişi olması olanak dahilindedir[201].

Dijital bilgi söz konusu olduğunda, özellikle bir kişinin müstehcen içerikleri dosya paylaşım programları aracılığıyla dağıtmayı kast etmesi halinde, söz konusu içeriklerin yayılmasının daha ileri etkisinin, fiziksel basılı bir içeriğinin yayılmasından daha farklı olarak bir üst derecede olması "makul bir beklenebilirlik" gösterir[202].

---

195 [2000] All ER (D) 502.
196 Gillespie, Cybercrime, s. 211.
197 [2000] All ER (D) 359.
198 Walden, pn. 3.136.
199 Gillespie, Cybercrime, s. 212.
200 [2012] EWCA Crim 398.
201 Walden, pn. 3.137.
202 Walden, pn. 3.138.

3. Uç Noktadaki (Ekstrem) Pornografi

Uç noktadaki (ekstrem) pornografik materyalleri bulundurma suçu İngiliz hukukuna göreceli olarak yeni girmiştir. Öğretinin büyük bir çoğunluğunda müstehcenlik ile ekstrem pornografi arasında ayrım yapılır; zira müstehcenlik suçunun düzenlendiği 1959 tarihli Müstehcen Yayınlar Yasası'nda (Obscene Publications Act 1959 / POA) bu tür içerikleri konu edinen bir suç bulunmaz. Ancak belirtilmelidir ki; ekstrem pornografi ile ilgili yapılan düzenleme, POA'yı yürürlükten kaldırmamıştır. Görüleceği üzere, ekstrem pornografi bir bulundurma (zilyetlik) suçudur, POA'daki suçlar ise bulundurma ile ilgili değildir (bu yasa yayınlama üzerine odaklanmıştır). Dolayısıyla ekstrem pornografik içeriklerin yayınlanması halinde "teknik olarak" POA uygulanmalıdır; ancak uygulamada da görülmüştür ki, bu durumda dahi ekstrem pornografi bulundurma suçunun uygulanması tercih edilmektedir, zira bu suçun uygulanması daha kolaydır[203].

Ağustos 2005 tarihinde İngiltere İçişleri Bakanlığı *"ekstrem pornografik materyallerin zilyetliği"* hakkında bir danışma raporu yayınlamıştır. Bu girişim, kısmen *Coutts*[204] davasında sunulan bazı rahatsız edici deliller tarafından tahrik edilmiştir. Graham Courts'un Jane Longhurts'ü öldürdüğü iddiasıyla yapılan yargılamada, sanığa karşı ileri sürülen bir delile göre, suçun işlendiği ilgili zaman diliminin öncesinde, sanık nitelikli cinsel saldırıyı da içeren cinsel şiddet, cinayet ve ölü sevicilik içerikleri barındıran çok sayıda web sitesini ziyaret etmiştir[205].

Danışma Raporunda, 1959 tarihli Müstehcen Yayınlar Yasası'nın (Obscene Publications Act 1959) bu tür eylemlere uygulanabildiği süreçte, yayıncıların genellikle yurtdışında yerleşik olduğu bu tür materyallerin internet aracılığıyla sağlanmasının problem oluşturması üzerine odaklanılmıştır. Dolayısıyla bu rapor, söz konusu materyallerin bulundurulmasını dahi suç haline getirilmesi suretiyle, talepte bulunan kişiyi adres göstererek, çocuk pornografisi için yapılan düzenlemelerin bu alana da aktarılması için bir teklifte bulunmaktadır[206].

Bu teklif, 1984 tarihli Video Kayıt Yasası'na (Video Recording Act 1984) benzer şekilde belirli bazı içerikleri suç haline getirmek suretiyle, bu tür materyallerin izleyiciler üzerindeki olası etkilerine yönelik bir yaklaşım gösteren Müstehcen Yayınlar Yasası'ndan farklıdır. Kötüye yöneltme ve ahlakını bozma kavramlarının belirsiz doğası nedeniyle, 1959 tarihli Yasaya bu şekilde bir bulundurma suçunun eklenmesi, belirlilik ve açıklık ilkelerini

[203] Gillespie, Cybercrime, s. 213.
[204] [2005] EWCA Crim 52.
[205] Gillespie, Cybercrime, s. 213; Walden, pn. 3.149.
[206] Walden, pn. 3.150.

zedeleyebilecektir[207]. Dolayısıyla ayrı bir suç tipi olarak şu materyallerinin gerçekte bulundurulması ya da gerçeğe uygun tasvirlerinin bulundurulmasının suç oluşturması önerilmiştir: a) Bir hayvanla oral, anal ya da vajinal yoldan ilişkiye girilmesi, b) Bir insan cesedine cinsel hareketlerde bulunulması c) Cinsellik bağlamında ciddi oranda şiddette bulunulması, d) Ciddi cinsel şiddette bulunulması[208], [209].

Buna karşın bu odaktaki değişim, yasa yapıcılar açısından hâlihazırda hukuka uygun olarak gerçekleştirilen bazı sado-mazoşist uygulamalar ve film endüstrisi gibi aktivitelere zarar vermeksizin uygun bir tanım yapılması konusunda sorun çıkarmaktadır. Söz konusu teklif, son iki tür içerik açısından da farklı görüşler ortaya çıkarmıştır[210]. Söz konusu materyallerin bulundurulmasının cezası üç yıl hapis cezasıdır. Müstehcen Yayınlar Yasası'ndaki beş yıla kadar hapis cezası nedeniyle her iki yasanın kapsamına giren yayınlar arasında ayrım yapılması gerekir[211].

Söz konusu teklif konusunda keskin bir biçimde birbirinden ayrılmış görüşler olmasına rağmen, Hükümet öneri sürecini devam ettirmiş ve 2008 tarihli Ceza Adalet ve Göçmenlik Yasası'nda (Criminal Justice and Immigration Act 2008)[212] düzenlediği yeni suç tipini uygulamaya koymuştur. Yeni yasa, ekstrem pornografik görüntülerin bulundurulmasını suç haline getirmektedir[213]. Bir görüntünün cinsel uyarılmayı sağlama amacıyla üretildiği *"makul bir şekilde varsayılıyor"* ise o görüntü pornografik olarak kabul edilir[214]. Bunun yanı sıra içeriğin uç noktada yani ekstrem olması gerekir. Bu ise, yasanın 63(7) maddesine uyması ve ağır biçimde saldırgan, iğrenç veya müstehcen karakterden farklı olması anlamına gelir[215].

Söz konusu suç, esas olarak dört tür içeriği düzenlemektedir[216]: Bir kişinin hayatını tehdit eden eylemler; bir kişinin anüsüne, göğüslerine ya da genital

---

[207] Jacop Rowbottom, "Obscenity Laws and the Internet: Targeting the Supply and Demand", Criminal Law Review, February 2006, s. 102.

[208] Bu tür bir saldırıda bulunulması, İngiltere ve Galler'de ağır bedeni zarar soruşturmasına konu olmaktadır.

[209] Walden, pn. 3.151.

[210] Bu görüşler için bkz: Gillespie, Cybercrime, s. 214, 215.

[211] Walden, pn. 3.152.

[212] CJIA 2008, m 63-8.

[213] Bu bağlamda Oliver (Philip) [2011] EWCA crim 3114 davasında mahkemenin belirttiği üzere, sanığın diğer kişilerin de bu tür görüntülere erişebilmesini sağlamak için bilgisayarına "TeamViewer" yazılımı indirmiş olması, bulundurma suçunun daha ağır nitelikli halini oluşturmaktadır.

[214] CJIA 2008, m. 63(3).

[215] Gillespie, Cybercrime, s. 216.

[216] Gillespie, Cybercrime, s. 217.

organlarına zarar veren ya da zarar verme olasılığı olan ciddi yaralamalar[217]; hayvanlarla ya da insan cesediyle gerçekleştirilen cinsel aktiviteler[218]. Bu liste, 2015 yılında nitelikli cinsel saldırı görüntülerini kapsayacak şekilde genişletilmiştir[219]. Zira maddenin ilk olarak düzenlenme amacını tam olarak karşılamadığı ifade edilmektedir; Prof. Dr. Gillespie "Cybercrime" adlı eserinde şu örneği vermektedir:

"X isimli kişi, Y isimli 19 yaşındaki bir kıza zorla Z isimli bir kişinin önünde striptiz yaptırılan ve bu esnada Z'nin elindeki palayla Y'nin elini bileğinden kesip attığı ve sonrasında da Z'nin Y ile cinsel ilişkiye girdiği bir filmi bilgisayarına indirmiştir"[220].

Bu yasa maddesine göre söz konusu filmin bulundurulması tamamen hukuka uygundur. Kişinin zarar verilen bölümünün anüs, göğüs ya da genital organlar olmadığı son derece açıktır, dolayısıyla kişiye karşı gerçekleştirilen böylesine ağır bir yaralamanın gösterilmesi m. 63(7) uyarınca suç oluşturmaz. Buna verilecek yanıt "peki ama bu yaşama karşı bir tehdit oluşturmaz mı?" olacaktır; ancak filmde Y'nin bu zaman zarfında tıbbi yardım aldığı da gösterilirse ne olacaktır? Bu uç bir örnektir; ancak yasanın, altı özellikle çizilen amacına ulaşamadığını göstermektedir[221]. İşte bu nedenle, söz konusu satırların yazılışından kısa bir süre sonra, söz konusu maddede değişiklik yapılmıştır.

Müstehcenlikte ve ahlaksızlıkta olduğu gibi, mahkeme öncelikle materyalin pornografik olduğunu tespit etmeli ve bununla birlikte gerçek bir hareket mi yoksa gerçek hareketmiş gibi gösterilen canlandırma (animasyon) mı olduğunu ortaya koymalıdır. Bu yasa, 1988 tarihli Ceza Adalet Yasası'nda (Criminal Justice Act 1988) çocukların kötüye kullanıldığı imajlara ilişkin düzenlemelerin aktarılmasını düzenlenmektedir[222]. Buna ek olarak yasa, diğer hareketlerden farklı olarak hayvanlar açısından, eylemin doğada normal olduğunun kanıtlanmasını bir savunma (hukuka uygunluk nedeni) olarak kabul etmektedir[223]. Diğer bir türdeki suçların azami hadlerinden daha az olarak, ciddi şiddet içeren materyallerin tasvir edilmesi halinde azami olarak üç yıl

---

217 Pornografik materyallerin ceza hukuku açısından ayrıntılı olarak incelendiği çalışmalar için bkz: Carmen C. Cusack, Pornography and yhe Criminal Justice System, Boca Raton, CRC Press, 2015, s. 79 vd. Pornografide kadınların gördüğü şiddet açısından bkz: Walter S. DeKeseredy/Marilyn Corsianos, Violance Against Women in Pornography, New York, Routledge, 2016, s. 57 vd.

218 CJIA 2008, m. 63(7).

219 2015 tarihli Ceza Adaleti ve Mahkemeler Yasası (Criminal Justice and Courts Act 2015) ile CJIA 2008, m. 63(7A) ve (7B) maddelerinde yapılan değişiklik.

220 Gillespie, Cybercrime, s. 217.

221 Gillespie, Cybercrime, s. 217, 218.

222 CJIA 2008, m. 65.

223 CJIA 2008, m. 66.

hapis cezası öngörülmektedir. Diğer ifade ile ilgili suçlarda olduğu gibi, bu suçun da soruşturması yalnızca Kamu Savcılığı İdaresi tarafından yapılabilir[224], [225].

4. Çocuk İstismarı ve Pornografi

Politikacıların, medyanın ve kamuoyunun, internetin karanlık yüzü hakkında tartışmasız bir biçimde birleştikleri bir konu var ise o da çocuk pornografisidir[226]. Belki de internetin ve dijital teknolojinin yaygınlaşmasının en trajik yönünü, bunların çocuk pornografisinin ve çocuk istismarının diğer formlarının görüntülerinin üretimini ve dağıtımını kolaylaştırması oluşturur[227]. Çocuk istismarı ve pornografisi, son dönemde bilişim hukuku alanında gündemi en çok işgal eden konudur[228].

Bazı görüntüler çocukla doğrudan bir etkileşime girilmeden gizlice oluşturulmaktadır, buna karşın çok büyük miktardaki çoğunluk "açık saçık" (hard-core) görüntüler, doğrudan çocukların istismar edilmesiyle oluşturulmaktadır. Aslında belirtilmelidir ki "pornografi" terimi çocuklar konusunda uygun değildir, zira bu terim yarı yasal bir endüstriyi tanımladığı için toplumun kafasında karışıklığa yol açmaktadır, özellikle de ergen çocukların görüntüleri söz konusu olduğunda bu kafa karışıklığı daha da artmaktadır[229]. Bu nedenle bu konudaki daha uygun olan terim basitçe "çocuk istismarıdır"[230].

Atkins & Goodland v. Director of Public Prosecutor[231] davasında mahkeme, suçlamanın temelini oluşturan, sanığın makinesinin ön belliğinde bulunan ve suçun konusunu oluşturan görüntülerin durumunu irdeleme gereği hissetmiştir[232]. Bu tür kopyalar daha etkin işlem yapabilmek adına genellikle internet tarayıcısı yazılım tarafından kendiliğinden oluşturulmakta ve depolanmaktadır. Davaya sunulan bilirkişi raporu göstermektedir ki, bilgisayar

---

224 CJIA 2008, m. 63(10).

225 Gillespie, Cybercrime, s. 215; Walden, pn. 3.153.

226 Walden, pn. 3.154. Bu alana özgü monografi için bkz: Alisdair A. Gillespie, Child Pornography: Law and Policy, London & New York, Routledge-Cavendish, 2012, s. 1 vd.

227 Clough, s. 289.

228 Çocuk pornografisi sorununu tüm yönleriyle tartışan kapsamlı ve güncel bir çalışma için bkz: Carissa Byrne Hessick (Ed), Refining Child Pornography Law: Crime, Language and Social Consequances, Michigan, University of Michigan Press, 2016, s. 19 vd.

229 Bu husus İngiltere Ulusal Suç Departmanı'nın Genel Müdür Yardımcısı olan Jim Gamble tarafından Londra'da 19 Ekim 2005'de gerçekleştirilen "İnternette Çocuk Pornografisi: Araştırma ve Soruşturma" başlıklı bir konferansta dile getirilmiştir.

230 Walden, pn. 3.155. Clough da bunu kabul etmekle beraber yine de bu alanda en yaygın olan terimin "çocuk pornografisi" olduğunu belirterek bu terimi kullanmıştır; bkz: Clough, s. 298.

231 [2000] 2 All ER 245.

232 Görüntüler aynı zamanda bir başka dizinde de bulunmuştur; ancak suçlamanın konusunu oluşturan görüntüler zamanaşımı nedeniyle görünmez hale gelmişlerdir.

kullanıcılarının büyük bir çoğunluğu önbellek hafızasının makinelerinde gerçekleştirdiği işlemlerden haberdar değildirler[233].

Bu bağlamda mahkemenin önünde iki sorun bulunmaktadır: Önbellek kopyaları 1978 tarihli POCA'nın 1(1)(a) maddesi gereğince "üretme" olarak mı, yoksa 1988 tarihli CJA'nın 160(1) maddesi gereğince "bulundurma" olarak mı kabul edilecektir? Bu davadan önceki tarihli *Bowden*[234] davasında mahkeme, internetten görüntü indirilmesinin ve yazdırılmasının *"üretme"* anlamına geldiğini, bu terimin *"yalnızca orijinal fotoğraflara uygulanmakla kalmayıp bunun yanı sıra negatiflere, fotoğrafların kopyalarına ve bilgisayar diskinde depolanan verilere de"* uygulanacağını belirtmiştir. Buna karşın *Atkins* davasında iddia makamı sanığın önbellek kopyalarından haberi olduğunu ispat edememiş ve buna bağlı olarak sanığın *"üretmekten"* veya *"bulundurmaktan"* dolayı sorumluluğunun yalnızca sırasıyla m. 1(1) ya da m. 160(1)'den dolayı olabileceği belirtilerek, bunların bilme unsurunun gerekliliğinden ziyade, kusursuz sorumluluk ilkesinin geçerli olduğu suçlar olduğunu belirtmiştir. Mahkemelerin bir ceza yasasını yorumlarkenki genel varsayımları, Parlamentonun masum bir bireyin cezalandırılması niyetinde olmadığı ve dolayısıyla suçun manevi unsurunun yasanın anlamından çıkartılması gerektiği yönündedir[235]. Buna bağlı olarak mahkeme, bilmenin gerekli olduğuna karar vermiş ve temyiz başvurusu bu noktada başarılı olmuştur. Eğer iddia makamı, bellek fonksiyonlarının varsayılan hallerinde değişiklik yapıldığını göstererek sanığın önbellek işlemlerinden haberdar olduğunu ispat edebilseydi, sanık suçlu bulunabilirdi[236].

Atkins davasında mahkeme, "bulundurma" suçunun gerçekleşmesi için öznel bilmenin gerekli olduğunu kabul etti; bir başka yargılama olan *Warwick*[237] davasında ise mahkeme, konuya daha fazla ilgi göstererek, bilişim sistemleri açısından "bulundurmanın" ne anlama geldiğinin belirlenmesi gerektiğini ifade etti. Bu davada sanık yaklaşık 3000 hareketsiz görüntü ve 40 adet film dosyası bulundurmaktan ayrı ayrı suçlanıyordu. Bu arada, suçun işlendiği iddia edilen esnada görüntülerin ve dosyaların işletim sisteminin çöp kutusuna atıldığı ve çöp kutusunun da boş olduğu, söz konusu dosyaların ya yalnızca küçük boyutlarının (thumbnail)[238] görüntülenebildiği ya da yalnızca önbellekte bulundukları konusunda tartışma bulunmamaktadır. Bunun gibi, önbelleğe alınmış dosyaların haricinde, silinmiş diğer dosyalar ancak buna özgü yazılımların kullanılması ile geri dönüştürülebilmektedirler; ki bu davada

---

233 Walden, pn. 3.171.

234 [2000] 1 Cr App R 438.

235 Sweet v. Parsley [1970] AC 132, at 148 H.

236 Walden, pn. 3.172.

237 [2006] EWCA Crim 560.

238 Görüntünün kendi tam boyutlarını değil yalnızca alt kümesini içeren halidir. Bu durumda silinmiş bir dosya bilgisayarın bir başka yerinde ayrı bir dosyada tutulmaktadır.

sanığın böyle bir yazılıma sahip olmadığı kabul edilmektedir[239]. Yargılama esnasında yargıç, gerçekte uygunsuz görüntülerin bulundurulması ile silinmesi arasında yargılamanın konusu etkileyen bir ilişkinin bulunmadığı yönünde jüriyi yönlendirmiştir; sonuçta sanık suçlu bulunmuştur[240].

Temyiz aşamasında savunma makamı, bir materyalin daha fazla "okunabilir durumda erişilebilir" olmaması halinde, özellikle kişinin söz konusu materyallerin silinmesi ve erişilmez hale getirilmesi için makul tüm aşamaları gerçekleştirmesi halinde, bulundurma suçunun oluşmayacağı görüşünü ileri sürmüştür. Bu konu hakkında karar verirken mahkeme, m. 160'ın sağladığı bir savunmaya atıfta bulunmuştur; buna göre *"uygunsuz bir fotoğraf, kişi tarafından ön istek yapılmadan ya da onun adına böyle bir istek yapılmadan alındığında ve makul bir süre için tutulmadığında"* kişi sorumlu tutulmaz[241]. Mahkemenin vurguladığı bu savunmaya göre, eğer "bulundurma" bir kişinin bulundurduğu görüntüleri basitçe silinmiş dosyaların bulunduğu bilgisayar üzerindeki kontrol ya da gözetim temeli üzerinden yorumlanırsa, bilgisayar konusunun altı oyulur. Mahkeme, *"eğer kişi bir görüntüye yeniden erişemezse ya da onu elde edemezse, kişi söz konusu görüntüyü daha fazla kontrol edemiyor ya da gözetim altında tutamıyor demektir"*; dolayısıyla m. 160'ta yer alan suçun amacının "bulundurma" olduğu söylenemez şeklinde karar vermiştir. Mevcut koşulların bazıları sanığın silinmiş dosyalar üzerindeki kontrolünün devam ettiğini gösterse de göstermese de, sanığın teknik yetenek ve kabiliyetlerine bağlı olarak bu, her dava açısından jürinin karar vermesi gereken bir konu olacaktır. Mahkeme, bunu bilme unsuru ile birlikte suçun ikinci öznel unsuru olarak sunulduğunu kabul etmiştir[242].

Bir diğer teknik savunma ise *"Truva atlarının"* görüldüğü çocuk pornografisi davalarında geliştirilmiştir. Bunlar kendilerini yararlı gibi gösteren yazılımlar olup, kullanıcının bilgisi olmadan bilgisayarın bazı işlevlerini kullanmaktadırlar. *Schofield*[243] davasında, sanık kendi bilgisi dışında bilgisayarına pornografik görüntüler indiren bir Truva atının bilgisayarında bulunduğunu iddia etmiştir. Bu senaryonun olabilirliği bilirkişi raporuyla kanıtlanmıştır, iddia makamı ise buna karşı bir delil ileri sürememiştir[244].

---

239 Küçük boyutlu resimler ancak Birleşik Devletler Federal Hükümeti'nin yetkilendirmesiyle tedarik edilebilen tamamıyla bu konuya özgülenmiş son derece özel yazılımlar ile geri dönüştürülebilmektedir.

240 Walden, pn. 3.173.

241 CJA 1988, s. 160 (2)(c).

242 Walden, pn. 3.174.

243 Schofield, The Times, 18 Nisan 2003.

244 Walden, pn. 3.175.

Westgarth Smith ve Jayson[245] davasında da *Atkins* davasındakine benzer bir şekilde, pornografik bir görüntüyü ek olarak içeren bir elektronik posta alımına ilişkin bir görüş geliştirilmiştir. Bu davada Smith'in müdafii, "üretmenin" Atkins davasındaki önbellek kopyasına benzer bir biçimde istenmeyen bir elektronik postanın alınmasıyla ilgili olduğu görüşünü ileri sürmüştür. Genel olarak mahkeme bu görüşü kabul etmiştir, ancak bunun mahkeme önündeki durumla ilgili olmadığına karar vermiştir. Jayson açısından ise iddia makamı, sanığın kullandığı tarayıcı yazılımının önbellek işlevinden haberdar olduğunu ispat edebilmiştir. Buna karşın mahkeme, sadece *"uygunsuz bir görüntünün bir bilgisayar ekranında görünmesi için gönüllü olarak internetten indirilmesinin dahi üretme eylemi"* olduğuna karar vermiştir; bu eylemin devamında görüntünün saklanmasına ilişkin bir kastın bulunup bulunmamasının ise bir önemi yoktur[246].

Jayson davasında, *Atkins* davasının bir parçası olan teknik cahilliğe güven sorununa bir savunma olarak dayanılması, bir bilginin indirilmesi biçimindeki siber alandaki en temel elektronik işlemin, "üretmenin" bir çeşidi olarak kabul edilmesine mal olmuştur. Çocuk Koruma Yasası'nda yer alan suçlar çocuk pornografisinin tedarik edilmesini adreslemektedir, bunların alınmasını, üretilmesini, dağıtılmasını, gösterilmesini veya reklamının yapılmasını suç haline getirmektedir. Buna karşın, Ceza Adaleti Yasası bu tür materyallere olan taleple ilgilenmekte ve sadece bulundurmayı suç haline getirmektedir. Bunların ikisi açıkça birbirleriyle ilişkilidir, bu ilişkinin doğası gereği talep tedariki doğurmaktadır; özellikle bu görüntüleri bulunduran bazı kişilerin kapsamı, çocukları istismar eden kişilere kadar uzanmakla birlikte bunlar tam olarak bilinmemektedir. Buna rağmen Parlamento "bulundurmayı" daha az ciddi bir sorun olarak algılamakta ve daha az ceza verilmesini uygun görmektedir. Ancak yine de *Jayson* davasında bulundurma sürecinin kendisi, bir tedarik etme hareketi olarak görülmektedir. İddia makamı bu tür materyallerin satın alınmasını dahi tedarik etmenin kışkırtılması olarak kabul etmekte ve suçlamada bulunmaktadır, böylelikle yine tedarik etme ile bulundurma arasında çizgi bulanıklaşmaktadır[247].

Tedarik etme ile bulundurma arasındaki çizginin bulanıklaştığı bir diğer örnek, dağıtma ya da gösterme amacıyla bulundurma suçu açısından ortaya çıkmaktadır[248]. *Dooley*[249] davasında, sanık bir P2P yazılımı olan "KaZaA" ile uygunsuz görüntüler elde etmiştir. Bu tür görüntüler, sanığın "Paylaşılan

[245] [2002] EWCA Crim 683.
[246] Walden, pn. 3.176.
[247] Walden, pn. 3.177.
[248] POCA 1978, m. 1(1)(c).
[249] [2005] EWCA Crim 3093.

Dosyalarım" klasörüne indirildikten sonra sanığın kullandığı bilgisayarın, aynı yazılımı kullanan diğer kişiler tarafından erişilemeyen bir başka bölümüne aktarılmaktadır. Sanık, bilgisayarındaki "Paylaşılan Dosyalarım" klasöründe altı adet uygunsuz görüntü bulunması nedeniyle POCA 1(1)(c) maddesini ihlal etmekten suçlanmıştır. Savunmanın görüşleri şu yöndedir: Sanığın söz konusu görüntüleri dağıtmak ya da başkalarına göstermek gibi bir kastı bulunmamaktadır, bunun tam tersine, aslında sanığın kastının söz konusu görüntüleri bilgisayarının başka kişilerin erişimine açık olmayan bir bölümüne taşımak olduğudur. Bununla birlikte bu taşıma işlemi tamamlanana kadar söz konusu görüntüler üçüncü kişilerin erişimine açık kalmaya devam etmektedir. İlk aşamada, Kraliyet Mahkemesi (Crown Court)[250] "amacıyla" ifadesinin sanığın kastıyla aynı anlama gelmediğini ve dolayısıyla görüntülere erişilebilirlik hakkındaki salt bilginin yeterli olduğuna karar vermiştir. Temyiz aşamasında ise mahkeme, jürinin ayırt etmesi gereken doğru sorunun, sanığın "Paylaşılan Dosyalarım" klasöründe bazı görüntüleri bırakmasının nedenlerinden birinin daha sonra bunların paylaşılmasını sağlamak olup olmadığının belirlenmesi olduğuna karar vermiştir. İddia makamı tarafından böyle bir kast ileri sürülmemiştir, dolayısıyla mahkeme de mahkûmiyet kararını bozma ihtiyacı hissetmiştir[251].

Genellikle davalar, çok sayıdaki görüntünün tedarik edilmesi ve/veya bulundurulması hakkındadır; sıklıkla bu sayılar binlerle ifade edilmektedir. Gerçekten de suçluların bu tür gruba katılmak ve içeriklere erişimi kontrol altında tutabilmek için geliştirilen mekanizmalardan birisi, istekli kişinin bunun karşılığı olarak belli bir sayının üstünde görüntü sağlamasıdır. Söz konusu görüntülerin hacmi bu konuda bir iddianame hazırlanırken zorluk oluşturmaktadır, zira her görüntü hakkında detaylı bilgi verilmesi uygun bir yöntem değildir. Sonuçta, mahkemeler bu konuda bir yeknesak uygulama kılavuzu belirlemişlerdir[252]. Buna göre:

— İddianame hem örnek oluşturacak sayıda hem de kapsamlı bir sayıda görüntü içermelidir;

— Örnekler, görüntüleri geniş bir kapsamda temsil edecek sayıda olmalıdır;

---

[250] İngiltere ve Galler Kraliyet Mahkemesi (The Crown Court of England and Wales) Yüksek Adalet Mahkemesi (the High Court of Justice) ve Temyiz Mahkemesi (the Court of Appeal) ile birlikte İngiltere ve Galler'deki üst düzey mahkemelerin kurucu unsurlarından biridir. Bu mahkeme ilk derece ceza mahkemelerinin yüksek mahkemesidir, buna karşın bazı nedenlerden dolayı Kraliyet Mahkemesi, hiyerarşik olarak Yüksek Mahkemenin ve ona bağlı olan Bölgesel Mahkemelerin altında yer almaktadır.

[251] Walden, pn. 3.178.

[252] Thompson (Richard) [2004] EWCA Crim 927.

— Bu şekilde yapılacak örnekleme elverişli değilse, görüntüler farklı uygunsuzluk ölçütlerine göre sınıflandırılmalı ve savunmanın da inceleyebileceği hale getirilmelidir;

— Örnekler, gerçek görüntüler ve gerçek benzeri görüntüler olarak ayrılmalıdır;

— Her görüntünün bizatihi kendisi dosya ile ilişkilendirilmelidir;

— Her örnekleme için çocukların yaklaşık yaş aralığı belirtilmelidir[253].

Görüldüğü üzere yukarıda belirtilenlere bağlı olarak Mahkeme, davaların ciddiyetini belirlerken görüntülerin sayısı, çocukların yaşı, görüntülerin konusu ve görüntülerin gerçek mi gerçek benzeri mi (animasyon görüntü / virtual child pornography)[254] olduğu gibi anahtar faktörleri dikkate almaktadır[255].

5. Grooming

İnternet, göreceli olarak kısa olan yaşamında, bizlere çok sayıda yeni kavramlar ve olaylar tanıtmıştır. Bunlardan önemle dikkat edilmesi gereken hususlardan biri, çocukların çevrimiçi seksüel konuşma ya da eylemlere davet edilmesi ya da kısaca "grooming"dir[256].

Grooming sözcüğü *"hazırlama, tımarlama"* anlamına gelmektedir. Tarihsel olarak, çocuk istismarı olaylarının büyük bir çoğunluğu, çocuğu tanıyan aile üyelerinden ya da yakınlardan biri tarafından gerçekleştirilmektedir. Ancak internet, pedofillerin çocuk istismarı amacıyla çocuklarla iletişime geçebilmeleri için yeni olanaklar sağlamıştır; işte buna "internet grooming" adı verilmektedir. Bu tür aktivitelerde internet, çocuklar ile iletişim kurmak ve onların güzellikle ikna edilebilmeleri için bir aracı olarak kullanılmaktadır. Örneğin[257], sohbet odaları vasıtasıyla çocuklarla fiziksel buluşma ayarlanmaya çalışılmakta, çocuklara pornografik içerikler gösterilmek suretiyle bu tür görüntüler normalleştirilmeye çalışılmakta ve çocuklar cinsel aktivitelerde bulunmak için cesaretlendirilmektedir[258].

Geniş bir biçimde kullanılan "grooming" terimi, ne tam olarak açıklanabilen ne de tanımlanabilen karmaşık bir olguyu belirtir. Grooming'in aşamaları şunlardır: a) Çeşitli manipülatif ya da kontrol edici tekniklerin kullanılması, b) Kırılgan bir mağdurun bulunması, c) Kişiler arası ve sosyal kurguların olması

253 Walden, pn. 3.186.
254 Bu konuda ayrıntılı bilgi için bkz: Clough, s. 313-325; Gillespie, Cybercrime, s. 245-253.
255 Walden, pn. 3.187.
256 Clough, s. 377.
257 Örnek için bkz: Mansfield [2005] EWCA Crim 927.
258 Walden, pn. 3.188.

(belli bir kapsamda) d) Zarar verici seksüel davranışların normal gösterilmesi için güven ortamının oluşturulması, e) İstismarı kolaylaştırmak için ve/veya ortaya çıkmasını engellemek için tüm bu sayıların gerçekleştirilmesi[259]. Söz konusu tanım şu şekilde de özetlenebilir: "Olası bir tacizci tarafından, çocukları taciz oluşturan aktivitelere razı etmek amacıyla, çocukların güvenini ve sırdaşlığını kazanmaya yönelik (teşebbüs eden) işlemler bütünü"[260].

Grooming'in kendisi yeni olmasa da, internet ve diğer elektronik iletişim kanalları suçluların çocuklarla irtibat kurmaları için çok daha fazla olanak sunmaya başlamıştır[261]. Geçmişte yalnızca aile üyeleri veya yakın arkadaşlar veya rahip ya da öğretmenler çocuklara özel anlamda yaklaşma şansına sahipti. Şimdi ise tamamen yabancı kimseler için bile çocuklarla özel olarak irtibat kurmak mümkün hale gelmiştir. Çocuklarının gerçek hayatta kimlerle ilişki içinde olduğu konusunda sürekli tetikte olan ebeveynler, çelişkili bir biçimde çocuklarının çevrimiçi hayatı üzerinde çok az kontrol sahibidirler ya da hiç kontrol sahibi değildirler[262]. Avusturalya'da yapılmış yakın tarihli bir araştırmaya göre sekiz ila on bir yaş arası çocukların %95'i, on altı ila on yedi yaş arası çocukların ise %100'ü bir önceki ay internete bağlanmıştır[263]. Gençlerin mobil telefon kullanımı yaşla birlikte artmaktadır; araştırmaya göre sekiz ile on bir yaş arası çocukların % 11'i mobil telefon kullanırken, on altı ile on yedi yaş arası çocuklarda ise bu oran %94'tür[264].

Bu tür aktivitelerle mücadele etmek için, 2003 tarihli Cinsel Suçlar Yasası (Sexual Offences Act 2003) ile *"cinsel 'grooming'e yönelik çocukla tanışma"* suçu düzenlenmiştir. Söz konusu suç şu hareketleri düzenlemektedir:

"Bir kişi (A) bir başka kişi (B) ile bir ya da daha fazla ortamda iletişime geçer ya da görüşürse ve devamında –

(i) A kasten B ile görüşürse,

---

259 Anne-Marie McAlinden, 'Grooming' and the Sexsual Abuse of Children; Instituonal, Internet and Familial Dimensions, Oxford, Oxford University Press, 2012, s.11.

260 Alasdair A. Gillespie, "Child Protection on the Internet – challenges for Criminal Law", Child adn Family Law Quarterly, Vol. 14, No. 4, 2002, s. 411, 412; Clough, s. 377, 378.

261 Grooming hakkında detaylı tartışma için bkz: Stephen Webster/Julia Davidson/Antonia Bifulco/Petter Gottschalk/Vincenzo Caretti/Thierry Pham/Julie Grove-Hills,/Caroline Turley/Charlotte Tompkins/Stefano Ciulla/Vanessa Milazzo/Adriano Schimmenti/Giuseppe Craparo, European Online Grooming Project, Final Report, European Commision Sefer Internet Plus Programme, Mart 2012, Bölüm 3, s. 37-60.

262 Helen Whittle/Catherine Hamilton-Giachritsis/Anthony Beech/Guy Collings, "A Review of Online Grooming: Characteristics and Concerns" Aggression and Violence Behaviour, Vol. 18, Issue 1, 2013, s. 65.

263 Australian Communications and Media Authority, "Like, post, share: Young Australians' experience of social media", Quantitative Research Report, 2013, s. 6.

264 Australian Communications and Media Authority, s. 7; Clough, s. 378.

(ii) A, B ile görüşmek kastıyla dünyanın herhangi bir yerine seyahat ederse ya da dünyanın herhangi bir yerinde B ile görüşmek için ayarlama yaparsa veya,

(iii) B, A ile görüşmek için dünyanın herhangi bir yerine seyahat ederse[265]..."

Bu suç için öngörülen ceza, azami on yıl hapis cezasıdır; buna rağmen söz konusu ceza toplumun korunması temeline dayanılarak belirsiz cezalı bir suç olarak düzenlenmiş, yalnızca azami haddi belirtilmiştir. Bu suç, taciz konusunda kullanılan yönteme benzer şekilde düzenlenmiştir, suçun hedefinde potansiyel fail tarafından suça hazırlık amacıyla gerçekleştirilen aşamalar bulunmaktadır. Bu aşamalar teşebbüsün dışında kalan hareketlerdir (hazırlık hareketi). Suç, geniş kapsamlı, tüm iletişim şekillerini kapsayacak şekilde düzenlenmekle birlikte, hükümetin belirtmiş olduğu üzere amacı, internet temelli aktiviteleri suç haline getirmektir. Suça teşebbüsün kabul edilebileceği aşamaya gelmeyen bir eylemin varlığı halinde, cinsel saldırıyı önleme emri için başvuruda bulunulabilir, böylelikle şüphelinin sohbet odaları ya da benzer olanakları kullanarak kişilerle iletişime devam etmesi önlenebilir[266].

Dünyada ve tabii ki Birleşik Krallık'ta büyük sorun olan ve suç haline getirilen bu tür aktivitelerin, her gün giderek daha fazla farkına vardığımız çocuk istismarı olayları dikkate alındığında ülkemiz hukuk düzeninde de bir an önce suç haline getirilmesi gerektiğini düşünüyorum.

6. Cinsellik Konulu İletişim

Grooming, failin hedeflediği çocukla fiziksel olarak görüşmesine, hazırlık hareketlerine odaklanmaktadır. Ancak bazı vakalarda kasıt, çocukla fiziksel bir görüşme niyetinde olmaksızın, yalnızca kurulan iletişimin kendisinden cinsel tatmin sağlanması olabilmektedir.

2015 yılında, 2003 tarihli Cinsel Suçlar Yasası'na *"çocukla cinsel konulu iletişim kurulması suçu"* eklenmiştir[267]. İletişimin içeriği, mantıklı bir insanın kabul edebileceği bir şekilde "cinsel aktivite" ile ilgili olmak zorundadır. İletişim, yetişkin bir kişi ile on altı yaşından küçük bir çocuk arasında gerçekleşmelidir. Bu suçun cezası azami iki yıl hapis cezasıdır, ayrıca not edilmesi gereken ilginç bir husus da, düşünce açıklama ile ilgili diğer suçlardan farklı olarak, bu suçun soruşturulması için başsavcılığın (Director of Public Prosecutions)[268] iznini

[265] SOA 2003, m. 15.

[266] Walden, pn. 3.189.

[267] 2015 tarihli Ciddi Suçlar Yasası'nın 15. maddeyle, SOA 2003'ün 15A maddesine eklenmiştir.

[268] İngiltere ve Galler'de başsavcılık ilk olarak 1880 yılında İçişleri Bakanlığı'nın bir parçası olarak kurulmuş ve 1908 yılında kendi başına bir kurum haline gelmiştir. Kısaca "DDP" olarak bilinen bu kurum, 1986 yılında soruşturma yükümlülüğü kendisinin de başı olduğu yeni kurulan Kraliyet Soruşturma Servisine devredilene kadar yalnızca çok az sayıdaki önemli davaların soruşturulmasından sorumluydu. Bu kurumun idarecisi olan başsavcı İngiltere ve

gerektirmemesidir[269].

Yukarıda belirttiğim üzere, benzer bir suçun yukarıdaki suç tipiyle birlikte aynı maddede, ancak farklı fıkralarda ve suçun yaptırımları arasında da derecelendirme yapılarak düzenlenmesinin son derece yararlı olacağını düşünüyorum.

7. Kötücül ve Uygunsuz İletişim

İletişim araçları kullanılarak işlenen içeriğe ilişkin bilişim suçlarının bir başka türü de *"intikam pornosu"*dur. Bunlar genellikle eski partnerler tarafından gönderilmekte ve açık cinsel görüntüler içermektedir. Bu tür eylemler suç olarak tanımlanmadan önce, bu tür zararlı hareketlerin her zaman gerekli olan eşiğe ulaşmadığına ilişkin sorunlar baş göstermiştir.

2015 yılında, yeni bir suç olarak *"mahrem cinsel fotoğrafların ve filmlerin sıkıntı vermek amacıyla ifşa edilmesi"* kabul edilmiştir[270]. "Cinsel" terimi, hem bedenin belirli bir bölümü (örneğin, genital organlar ya da pubik bölgesi) hem de makul bir insan tarafından cinsel olarak kabul edilen davranış ya da görüntü anlamına gelmektedir. Bu ifşaat, resimde ya da filmde görülen kişinin rızası dışında gerçekleşmeli ve karşıdaki kişiye sıkıntı vermek kastıyla gerçekleştirilmelidir. Bu suçun cezası olarak azami iki yıl hapis cezası öngörülmüştür[271].

Zararlı iletişimi düzenleyen mevcut hukuk düzeni, *"bireyden bireye"* iletişim teknikleri ve özellikle sözlü telefon görüşmesi üzerine temellendirilmiştir; hala da bu temel üzerinde devam etmektedir. Ancak, siber alandaki kişisel web siteleri gibi, *"bireyden çoğula"* iletişim tekniği seçenekleri, söz konusu mevcut kuralların duruma uygunluğuna karşı meydan okumaktadır. Kötücül, uygunsuz veya zararlı iletişimin hedefleyerek neden olduğu sıkıntı ve anksiyete, iletişimin bireyselden ziyade toplumsal doğası dikkate alındığında, muhtemelen dikkate değer bir büyüklüktedir[272].

C. Bilgisayarın Bütünlüğüne İlişkin Suçlar

1. Suçun Konusu

Doğrudan bilgisayarları hedefleyen ve bilişim sistemlerinin bütünlüğüne karşı işlenen suçlar en sık görülen bilişim suçlarındandır. Bu tür suçlar

Galler Genel Savcısı tarafından atanmaktadır.

269 Walden, pn. 3.192.

270 2015 tarihli Ceza Adaleti ve Mahkemeler Yasası m. 33 (Criminal Justice and Courts Act 2015).

271 Gillespie, Cybercrime, s. 219-223; Walden, pn. 3.214.

272 Walden, pn. 3.219.

genellikle "bilişim sisteminin güvenliğinin kırılması / hacking"[273] üst başlığıyla adlandırılır. Bu üst başlık, geniş bir kapsamdaki amaçlarla hareket eden kişilerin aynı geniş kapsamda gerçekleştirdikleri hareketleri içerir. Bilişim sistemlerinin modern yaşamın her yerinde birden görünmesiyle ve modern ticari ilişkilerin bilişim ağlarına bağlı hale gelmesiyle bu tür suçların ciddi sonuçları görülmeye başlanmıştır[274]. Bilgisayarın ya da bilişim sistemlerinin ne olduğu sorusu açısından; sorun, tümleşik bir donanımı, aygıt yazılımı, işletim ve diğer yazılımları ve verileri olan bir aygıttan ziyade, işleme tabi tuttuğu verilerden ayrı kendi başına fiziksel, tekil objeler olarak algılanmasından kaynaklanır. Oysa bilgisayar, kendisini oluşturan donanımsal ve yazılımsal parçalarından ayrılmaz bir bütün olarak sanal bir makinedir (burada teknik anlamda sanal makineler kastedilmemektedir / virtual machine ware). Ceza hukuku ise söz konusu sanal makinelerin gizliliğini, bütünlüğünü ve işlerliğini, bunu bileşenlerine ayırma ihtiyacı duymaksızın korumalıdır. Bu makinelerin bir parçasına ya da bütününe yetkisiz erişilmesi veya araya girilmesi gibi eylemler haksızlık olarak görülür. Farklı uygulamalar, gerçekleştirilen eylemin, verilen zararın ve/veya failin kusurunun doğasından kaynaklanır. Dolayısıyla söz konusu farklılık bazı belirsiz ve uygunsuz teknik farklılıklardan kaynaklanmamaktadır[275].

2. Yetkisizlik ve Hukuka Uygunluk Nedeni

Bazı yargı çevrelerinde sistem yöneticilerine, ceza sorumluluğu sınırlandırmak amacıyla, iyi güvenlik uygulamalarını cesaretlendirici biçimde, sistemleri üzerinde işlemlerini gerçekleştirirken uymaları gereken bazı özel yükümlülükler getirilmiştir. Örneğin, Almanya'da veriler yetkisiz erişimlere karşı *"özellikle korunmalıdır"*[276]. Benzer bir hüküm Norveç hukukunda da yer almaktadır, buna göre sorumluluk *"korunmakta olan bir aygıta ya da benzer bir tarzdaki araca"* karşı, birey tarafından erişim sağlandığında söz konusu olmaktadır[277]. Aslında birer sonuç olan bu hükümler Yüksek Mahkeme

[273] Kullanım kolaylığı olması için, "hack" (kıymak, kesmek, darbe) sözcüğü ve bunun varyasyonları, bilgisayarlara ve bilgisayar sistemlerine yapılan yetkisiz erişim hareketlerini tanımlamak için kullanılmaktadır. Bazen, aslında her ikisi de yetkisiz erişim olan ve iyi amaçlı bir girişim olarak görülen "hacking" ile bunun tam karşısında yer alan ve kötü amaçlı bir girişim olarak kabul edilen "cracking" arasında bir ayrım olduğu kabul edilir. Bunların cezalandırılmasına etkili olan motivasyon unsuruna ilişkin hukuki ilişki dışında, popüler kullanımda bunlar arasında çok az ayrım yapıldığı görülmektedir.

[274] Clough, s. 31.

[275] Walden, pn. 3.234.

[276] StGB m. 202a. Ayrıca bkz: Brezilya Ceza Kanunu m. 154-A (güvenlik mekanizmasının hukuk aykırı şekilde ihlal edilmesi), Japonya Bilgisayara Yetkisiz Erişim Yasası m. 3(2)(1) (erişim kontrol fonksiyonu ile sınırlandırılmıştır).

[277] Norveç Genel Bireysel Ceza Yasası, m. 145. Bu hüküm 1987 yılında yürürlüğe girmiştir, ancak 2005 yılında yeniden düzenlenmiştir, şimdiki hali şöyledir: "Bir kişi hukuka aykırı olarak

tarafından basitçe şu şekilde ortaya çıkarılmıştır: *"Güvenliğin kırıldığının gösterilmesi amacıyla internete sondaj bilgisayarlarının bağlanması hukuka aykırıdır"*[278]. Sistem yöneticisinin bu tür önlemleri uygulamakta ihmalde bulunması, savcılığın yetkisiz bir erişimi suç olarak nitelendirebilme olanağının altını oymaktadır. Avrupa Siber Suçlar Sözleşmesi, suçun gerçekleşmesi için sözleşmeci taraflara *"suçun güvenlik önlemlerinin ihlal edilmesi halinde gerçekleşmesi gerekebilir"*[279] şeklinde bir seçimlik sınırlayıcı unsur sağlamaktadır. Bu tür bir sınırlama Avrupa Birliği'nde AB Çerçeve Kararı'na[280] göre de seçimliktir, ancak Direktif tarafından zorunlu hale getirilmiştir[281]. Avrupa Komisyonunun orijinal önerisi, bir güvenlik önleminin ihlal edilmesi ve özellikle *"ek olarak alınan yapısal unsurların"*[282] özel bir şekilde uyarılması gerekliliğini içermemekteydi. Ancak Avrupa Parlamentosu, Yeşiller / Avrupa Özgür Birliği'nin temsilcisi milletvekili Jan Albrecht'in girişimiyle, bu öneriye katılmadığını belirterek bir sınırlama getirilmesi gerektiğine karar verdi[283]. Ancak yine de; özellikle, işçilerin kendilerinin iş bilgisayarlarını yetkisiz olarak kendi özel işlerinde kullanmalarının cezai sorumluluğu gerektireceği konusunda endişeler[284] bulunmaktadır[285].

İngiltere'de Bilgisayarın Kötüye Kullanılması Yasası'nın (Computer Misuse Bill) şu maddenin[286] yürürlükte olması nedeniyle, eğer bir bilgisayar kullanıcısı güvenlik önlemlerini uygulamamışsa, bilişim korsanlarının bunu bir savunma olarak sunmaları yönünde bir hüküm eklenmesi için girişimde bulunulmuştur:

---

bir başka kişinin mektubuna ya da diğer bir kapalı dokümanına veya benzer bir şekilde içeriklerine erişim sağlarsa ya da bir başka kişinin kilitli bir muhafazasının içindekilere zorla kırarak erişirse…". Ayrıca bkz: Finlandiya Ceza Kanunu m. 8(1) (korumanın kırılması).

278 Dosya No 83 B, RT-1998-1971, 15 Aralık 1998.

279 Avrupa Siber Suçlar Sözleşmesi, m. 2.

280 Bilişim sistemlerine karşı gerçekleştirilen saldırılar hakkında Konsey Çerçeve Kararı, OJ L 69/67, 16 Mart 2005, m. 2(2) (Çerçeve Kararı).

281 Bilişim sistemlerine karşı gerçekleştirilen saldırılar hakkında Direktif 13/440/EU, OJ L 218/8, 14 Ağustos 2013, m. 9(5).

282 Avrupa Komisyonu, "Bilişim sistemlerine karşı gerçekleştirilen saldırılar hakkında direktif önerisi ve 2005/222/JHA', COM (2010) 517 final sayılı ve 30 Eylül 2010 tarihli Konsey Çerçeve Kararı değişikliği hakkında rapor, s. 7.

283 Bkz: Sivil Özgürlükler, Adalet ve İçişleri Komitesi (Raportör M. Hohlmeier), bilişim sistemlerine karşı gerçekleştirilen saldırılar hakkında Avrupa Parlamentosu ve Konseyi direktif önerisi ve 2005/222/JHA', A7-0224/2013 sayılı ve 19 Haziran 2013 tarihli Konsey Çerçeve Kararı değişikliği hakkında rapor.

284 Bkz: Direktif 13/40/EU, m.17; ayrıca Kıdemli Politika Danışmanı Ralf Bendarth'tan Jan Albrecht'e gönderilen 7 Temmuz 2015 tarihli elektronik posta.

285 Walden, pn. 3.242.

286 İngiliz hukukunda yer alan mevzuatın çoğunluğunda, Türk hukukunda "madde" karşılığı olarak "section" sözcüğü kullanılır. Bunun tam çevirisi ise "bölüm"dür. Ben kullandığımız ve alışkın olduğumuz dille uyumlu olması için "section/bölüm" karşılığı "madde" sözcüğünü kullanmaya devam edeceğim.

"Bu maddenin amaçları doğrultusunda, erişimin ya da erişime kalkışmanın engellenmesinin önlenmesi için, özenli bir şekilde, şartların makul bir şekilde gerektirdiği önlemlerin alınmadığının kanıtlanması bir savunma olabilir".

"Güvenlik önlemlerinin" konulmasındaki eşiğin daha fazla hukuki belirsizlik üretmesi olasıdır, bu bağlamda bir mahkemenin güvenlik önlemlerinin uygunluğu ve yerindeliğine ilişkin bir yorum yapması gerektiğinde ve bununla birlikte savunma makamının da savcılığa meydan okuyarak iddialara yoğun bir inceleme yöneltmesi sonucunda jürinin kafasında şüpheler oluşacaktır. Güvenlik önlemlerinin bulunması konusu bir erişimin "yetkisiz" olarak gerçekleşip gerçekleşmediği konusuyla dolaylı olarak ilgili olmasına rağmen söz konusu teklif reddedilmiştir. Öğretide bazı yazarlar ise yetkisiz erişimler için ceza sorumluluğunun yalnızca *"kod temelli önleme"* söz konusu olduğunda tetiklenebileceğini iddia etmeye devam etmişlerdir[287]. AB'nin 13/14/EU nolu Direktifinde ise konu şu şekilde açıklanmaktadır: *"Kullanıcı politikaları veya hizmet şartları yoluyla bilişim sistemlerine erişimi kısıtlayan sözleşmesel yükümlülükler ya da anlaşmalar"* yetkisiz erişimlere ilişkin ceza hukuku uygulamalarının tek başına temelini oluşturmamalıdır[288].

İnternet öncesi devirde 1980'li yıllarda, bilgisayarların kötüye kullanılmasına ilişkin düzenleme ilk olarak teklif edildiğinde, karşılaştırma geleneksel ceza yasasından gelen görünürde paralel konularla gerçekleşti: Yetkisiz erişimle sisteme izinsiz girme eylemleri ve yetkisiz müdahale ile hukuken cezai yaptırım gerektiren eylemler. Bu karşılaştırma, yetkilendirmeye ilişkin sorular hakkında devam eden, özellikle de izinsiz giriş hakkındaki tartışmanın etkisi altında kalmıştır. Gerçekten izinsiz girme, "siber izinsiz giriş" (cybertrespass)[289] gibi, öğretide yetkisiz erişim için kullanılan açıklayıcı bir terimdir. Bu terim hukuki düzenlemelerde kullanılmakta[290] ve ABD'deki bilişim suçları davalarında hukuki girişimlerin temeli olarak ileri sürülmektedir[291]. Açık bir eve girilmesi hukuka aykırı olabilir, ancak girecek kişi uygun bir şekilde uyarılmadığı takdirde suç oluşturmaz, dolayısıyla bu görüşün devamında güvenliksiz bir bilgisayarın da açık bir eve yakın olduğu söylenebilir. Benzetmenin çekiciliğine karşın, izinsiz girişlerde olduğu gibi bilişim sistemlerine karşı gerçekleştirilen kötüye kullanım tiplerinin belirtilmesi için, bilişim suçlarına ilişkin yasal düzenlemelerin

[287] Orin S. Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", New York University Law Review, Vol. 78, 2003, s. 1600.

[288] Walden, pn. 3.243.

[289] David S. Wall, "Policing the Internet: Maintaining Order and Law on the Cyber-beat", The Internet, Law and Society, Ed: Yaman Akdeniz/Clive Walker/David Wall, Longman, 2000, Section 7, s. 157.

[290] Örneğin, Brezilya Ceza Kanunu m.154-A "Bilgisayarla ilgili bir aygıta izinsiz girilmesi".

[291] Intel Corp v. Hamidi, 71 P 3d 296 (Cal 2003), istenmeyen elektronik postalar açısından taşınır bir mala karşı izinsiz girişe ilişkin bir haksız fiil iddiasının sürdürüldüğü yerde iddia başarısızlığa uğramıştır.

mülkiyet temelli çözümlerin başarısızlığına bir yanıt olarak benimsenmesi fikri de ayrıca akıllara gelmiştir[292].

Dinlemeye ilişkin hukuki düzenlemelerde yetkilendirmeye ilişkin sorunlar, erişim ve araya girmeden çok daha karmaşıktır ve üç farklı boyutu ilgilendirmektedir. İlk olarak, kişilerin iletişim ağını denetleyen bir otorite bulunur. Bu boyut, doğası gereği diğer sistem bütünlüğüne karşı işlenen suçlara son derece benzemektedir. İkinci olarak, söz konusu ağdan yararlanabilmek için ya bir otorite ya da iletişimde olan tarafların rızası bulunmalıdır. Dinleme yasalarının ilk amacı, kullanıcıların mahremiyetlerinin korunmasıdır. Son olarak, bir soruşturma aracı olarak ve gücün kullanılması açısından, soruşturma makamları bir dinleme işlemiyle görevlendirildiklerinde, bu işlemi hukuka uygun hale getirebilmek için gerekli bir yetkilendirmeye sahip olmalıdırlar[293].

Yetkili olma ve yetkisizlik üzerine kurulması zorunlu olan, sınırları aşan ve sınırlarla kesişen konu ise kamusal ve özel alan arasındaki ayrımdır. Gerçekten de, siber alanda yetkilendirme konusunda çok sayıda sorun ortaya çıkmıştır; bunların bir kısmı internetin geleneksel "kamusal ve özel alan" ayrımını rahatsız eden ve ona meydan okuyan tarzı nedeniyledir. Zımni yetkilendirme ile yönetilmekte olan internetin popüler kavramı "World Wide Web", büyük bir bölümü kamusal alanda işleyen, "ağların ağı" olarak kullanılabilen özel bir hizmet olup, bilginin değişimine ve ulaşılmasına zemin oluşturmaktadır[294]. Aynı zamanda, internetin kamusal bilinci genellikle anonimlik, mahrem ilişkilerin ve alanların çevresi olma, devletin gözetimi tarafından engellenmeme ve izlenmeme algısı ile ilişkilidir. Bunlar birlikte ele alındığında bu eğilimler, sistem bütünlüğüne ilişkin suçlardaki yetkilendirmeye olan güvene itiraz edebilirler[295].

Bilgisayarların Kötüye Kullanılması Yasası'na göre bir erişim şu hallerde yetkisiz bir erişim olarak kabul edilir: Eğer;

a) Bir kişinin kendisi, söz konusu olan yazılım ya da verinin erişimini kontrol etmek için yetkilendirilmemişse veya

b) Bu kişi, söz konusu olan yazılım veya veriye erişmek için yetkilendirilmiş olan bir kişiden rıza almamışsa,

bunlar alt bölüm madde 10'da düzenlenen suçların konusunu oluştururlar[296].

---

[292] Kerr, s. 1602; Walden, pn. 3.244.
[293] Walden, pn. 3.245.
[294] Chris Reed, Internet Law: Text and Materials, 2nd Edition, Cambridge, Cambridge University Press, 2004, s. 66.
[295] Walden, pn. 3.246.
[296] CMA, m. 17(5).

Failin, mağdurun organizasyonunun dışından birisi olması hali, bir yetkilendirmenin var olmadığını göstermekte ya da rıza konusu genellikle bir sorun oluşturmayıp yukarıda tartıştığımız senaryoların konusunu oluşturmaktadır. Ancak failin, organizasyonun (şirketin, hastanenin, üniversitenin vs.) bir çalışanı olması halinde, savcılığın sırtına, açık ya da örtülü bir erişim hakkının kötüye kullanıldığını göstermektense, "böyle bir erişimin" yetkisiz olarak yapıldığını sanığının bildiğini gösterme yükümlülüğü binmektedir; örneğin, hesap memurunun hatalı harcama kalemleri girmesi gibi[297]. Hukuk Komisyonu bu konuda şu hususu belirtmiştir:

"Bir çalışan bir suçtan dolayı ancak şu halde suçlu bulunabilir: Eğer işvereni çalışanın yazılıma ya da veriye erişimine ilişkin yetkisini açıkça tanımlamışsa"[298].

Birleşik Devletler federal yasaları, madde 1'deki suça benzer biçimde, salt yetkisiz erişimi suç olarak düzenlememektedir. Bu tür bir erişimin suç olabilmesi için, ulusal güvenlik bilgilerinin ya da finansal kayıtların elde edilmesi gibi başkaca amaçlarla bağlantısının bulunması gerekir[299]. Bunun yanı sıra Birleşik Krallık'tan farklı olarak, Birleşik Devletler federal yasası yetkilendirme açısından iki farklı senaryo arasında açıkça ayrım yapmaktadır: "Bir bilgisayara yetki olmaksızın erişilmesi ve yetki aşımıyla erişilmesi"[300]. İkinci terim, işçiler gibi "içeriden olanları"[301] kapsamak amacındadır ve aşağıdaki şekilde tanımlanmaktadır[302]:

"Bir bilgisayara yetkili olarak erişmek ve bu erişimi bilgisayarda bulunan bilgileri almak ya da değiştirmek için yetkilendirilmediği halde, bu bilgileri almak ve değiştirmek üzere kullanmak anlamına gelmektedir"[303].

Buna karşın, işten ayrılan işçilerin davalarında yetkilendirme eşiğinin ne zaman gerçekleştiğine ilişkin çelişkili kararlar bulunur. *International Arort Centers LLC v. Citrin* davasında[304], işten ayrılan bir işçi mülkiyeti işverene ait olan dizüstü bilgisayara bir yazılım indirmiştir ve işveren şirketin mülkiyetinde olan tüm verileri güvenli (geri döndürülemeyecek biçimde) bir biçimde silmiştir. Mahkeme, Citrin'in şirketin bir çalışanı olarak yetkilendirilmesini *"bir işçi*

297 Walden, pn. 3.247.

298 Hukuk Komisyonu, Bilgisayarların Kötüye Kullanılması, Rapor No 186, Cm 819, Londra, HMSO, 1989, pn. 3.37.

299 18 USC m. 1030 "Bilgisayarla bağlantılı olarak gerçekleştirilen dolandırıcılık ve bağlantılı hareketler".

300 18 USC m. 1030(a)(1). Benzer şekilde, Belçika hukukunda da "bir kişinin yetkisini aşarak bir bilişim sistemine erişmesi" ayrı bir suç olarak düzenlenmiştir.

301 Örneğin, EF Culturak Travel BV v. Explorica, Inc, 274 F 3d 577 (1st Cir 2001), s. 583, 584.

302 Walden, pn. 3.248.

303 18 USC m. 1030(e)(6).

304 440 F3d 418 (7th Cir 2006). Daha önceki tarihli bir karar olan Shurgard Storage Centes, Inc v. Sefaguard Self Storage, Inc, 119 F Supp 2d 1121 kararını izlemiştir.

olarak sadakat yükümlülüğünü ihlal ettiği anda" kaybettiğine karar vermiştir. Bu karar çok düşük bir eşik belirlemektedir, böylelikle işçinin izin verilen ve verilemeyen davranışlarını açıkça belirlemektense, işçinin yapması gereken uygun davranışlarına yönelik yükümlülüğünü birinci sıraya koymaktadır. *Lockheed Martin Corporation v. Speed* davasında[305], bu tür bir geniş yaklaşım mahkeme tarafından açıkça reddedilmiştir. Bu dava işten ayrılan üç işçinin rakip bir şirkete geçmeden önce mülkiyeti Lockheed'e ait olan bilgileri içeren çeşitli medya verilerini kopyalamaları hakkındadır. Mahkeme, "sadakatin ihlal edilmesi" testinin, bu tür bir yetkilendirmenin sınırlarının aşılmasına nazaran, bir işçiyi etkin bir biçimde "yetkisiz" olarak konumlandırdığını dikkate almıştır. Bu ikinci yorum daha mantıklı ve "olmaksızın" ile "aşma" arasındaki anlamlı farkı ortaya çıkarma açısından daha ilkeli görülmektedir. Ancak bu kararın ceza hukuku açısından tam olarak örnek olabilmesi yüksek bir mahkemenin onayını almayı ve bir özel hukuk davasından ziyade ceza davasının konusunu oluşturmayı gerektirir[306].

Bilgisayarların Kötüye Kullanılması Yasası'na göre "yetkilendirmenin" işçi bağlamındaki yorumuyla ilk kez detaylı olarak *DPP v. Bignell* davasında[307] ilgilenilmiştir. Bu dava kişisel amaçlarla bir operatör vasıtasıyla görevdeki iki polis memurunun Ulusal Polis Bilgisayarı'na (Police National Computer – PNC) erişim sağlaması hakkındadır. Bu kişiler CMA madde 1'deki suçla itham edilmişler ve Sulh Ceza Mahkemesi (Magistrates' Court) tarafından suçlu bulunmuşlardır. Haklarındaki mahkûmiyete ilişkin yaptıkları temyiz başvurusu neticesinde Kraliyet Mahkemesi'nde (Crown Court) başarılı olmuşlar ve bu karar Bölge Mahkemesindeki bir sonraki temyiz başvurusunun konusunu oluşturmuş ve bu başvuru reddedilmiştir[308].

Mahkeme tarafından belirtilen merkezi konu, bir kişinin belirli ve sınırlı bir amaç için (örneğin, polis faaliyetleri) bir bilişim sistemine erişmeye yetkilendirilmesi halinde, bu tür bir yetkilendirmenin, yetki kapsamında olmayan bir amaç için (örneğin, kişisel amaç) kullanılmasının madde 1'de tanımlanan suçu oluşturup oluşturmayacağıdır. Kraliyet Mahkemesi, CMA'nın öncelikli ilgi alanının *"bilgisayarda bulunan bilgilerin bütünlüğünden ziyade bilgisayar sisteminin kendisinin bütünlüğünün korunması"* olduğunu açıklamıştır; dolayısıyla bu tür yetkisiz kullanımlar Yasanın kapsamında değildir. Bu görüş, Bölge Mahkemesi tarafından da onaylanmıştır. Yargıç Astill,

---

305 2006 US Dist LEXIS 53108, 1 Ağustos 2006.

306 Walden, pn. 3.249.

307 [1994] 1 Cr App R. Dana önceki tarihli bir dava olan Bernett davasında (Bow Street Magistrates' Court, 10 Ekim 1991), bir polis amiri, bir kişinin halihazırda görünen kişinin karısından önceki karısının kim olduğunu öğrenebilmek için PNC'yi kullanması nedeniyle madde 1'de yer alan suçtan mahkûm olmuştur.

308 Walden, pn. 3.250; Clough, s. 97.

öncelikle madde 17(5)(a)'da şu hususun yer aldığını belirtmiştir: *"Bu şekilde bir erişim" madde 17(2)'de detaylandırılan erişim tiplerine atıf yapmaktadır; değiştirme, silme, kopyalama, taşıma, kullanma ve çıktılar elde etme. İkinci olarak, "erişimi kontrol etme" ifadesi polis memurlarının PNC'ye erişim yetkisi verilmesine atıfta bulunmaktadır"*. Yargıç Astill, bunun Yasada bir boşluk yaratmadığı, bu eylemin gerçekleştirildiği zamanda 1984 tarihli Veri Koruma Yasası'nın (Data Protection Act 1984) kişisel verilerin yetki dışı amaçlar için kullanılmasıyla ilgili uygun suçları içerdiği sonucuna varmıştır[309]. Sonuçta fail CMA madde 1'den değil, 1984 tarihli Verilerin Korunması Yasasını (Data Protection Act 1984) ihlal etmekten suçlu bulunmuştur[310].

Bignell davasına benzer bir durum Birleşik Devletler'de de bir mahkemenin önünde görülmüş ve benzer şekilde sonuçlanmıştır. *State v. Olson* davasında[311], polis memuru yerel bir kolejdeki kız öğrencinin arabasının plakasının ayrıntılarını bulmak için polis veri tabanına izinsiz girmekten suçlu bulunmuştur. Polis memurunun hakkındaki ilk mahkûmiyet kararı temyiz mahkemesi tarafından bozulduktan sonra mahkeme *"bölüm politikalarına rağmen alınan verilerin bu tür kullanımlarının, verilerin kullanımının şarta bağlandığı bilgisayarlara erişime izin verildiğini göstermediğine"* karar vermiştir. İşte böylelikle bir kere erişim sağlandığında ne olabileceği ile erişim kavramı kesin olarak ayırt edilmiştir; ayrıca bu davada mahkeme görüşünü herhangi bir yasal tanımlamayla desteklememiştir. Yeni Zelanda'da, ilgili hüküm, *"bir kişinin bilişim sistemine erişime yetkisi olduğunda, bu kişiye verilen yetkinin dışında bir başka amaçla sisteme erişim sağlaması halinde"* yetkisiz erişim suçunun gerçekleşmediğini açıkça belirtmektedir[312]. Bu durumda diğer hükümlerin[313] ihlal edilmesi söz konusu olabilecektir[314].

Bignell kararının, *Sean Cropp* kararında olduğu gibi, önemli eleştirileri üzerine çektiği ve Yasanın kapsamını önemli derecede sınırlandırdığı görülmektedir[315]. Buna karşın kararın kilit noktaları *Allison* kararında[316]

---

309 Veri Koruma Yasası m. 5(6). Bu hüküm DPA 1998 m. 55'te yer alan hukuka aykırı veri elde etme suçu ile değiştirilmiştir. Ayrıca bkz: Rooney (2006) EWCA Crim 1841, bir Straffordshire Polisi çalışanının kişisel amaçlar için PNC'ye erişim sağlaması hakkında dava. Walden, pn. 3.251.

310 Ormerod, Smith & Hogan's Criminal Law, s. 1050; Clough, s. 97, 98.

311 735 P 2d 1362 (Wash Ct App 1987).

312 Crimes Act 1961, m. 252(2).

313 Örneğin maddi yararlar elde etmek için bir bilgisayara dürüst olmayan yollarla erişilmesi: Crimes Act 1961, m. 249.

314 Walden, pn. 3.252.

315 Örneğin bkz: David Bainbridge, "Cannot Employees also be a Hackers?", Computer Law and Security Report, Vol. 13, No. 5, 1997, s. 352-354; Paul Spink, "Misuse of Police Computers", Juridical Review, Vol. 42, 1997, s. 219-231.

316 Bow Street Magistrate and Allison (AP), tek taraflı olarak (hasımsız) US Government (HL))

Lordlar Kamarası tarafından yeniden değerlendirilmiştir. Bu dava, sahte kredi kartlarının üretilmesinde kullanılmak üzere kişisel tanımlama numaralarını elde etmek için bilişim sistemlerine erişim yetkisini kullanan ve bu nedenle dolandırıcılıkla suçlanan American Express çalışanı bir kişinin Birleşik Devletler Hükümeti tarafından suçluların iadesi çerçevesinde yapılan iadesi istemine ilişkindir. *Bignell* davasında olduğu gibi, savunma makamı, işçinin söz konusu bilişim sistemlerine erişim yetkisi olduğu gerekçesiyle madde 1'de tanımlanan suçun oluşmadığı görüşünü ileri sürmüştür. Bignell kararıyla aynı görüşte olan Lordlar Kamarası, bu kararın devamında Yargıç Astill tarafından yapılan madde 17(5) hakkındaki açıklamayı[317] ise reddetmiştir[318].

Lord Hobhouse tarafından ilk olarak, "bu tür bir erişim" ifadesinin basitçe madde 17(5)'e göre verilen yetkinin bazı tür yazılımlar ve veriler için sınırlanmış olduğu ve 17(2)'de detaylandırılan türdeki erişimlere atıf yapmadığı anlamına geldiği belirtilmiştir. Deliller göstermektedir ki American Express çalışanı yetkilendirilmediği verilere erişim sağlamıştır, dolayısıyla sağlamış olduğu erişim yetkisiz bir erişimdir. İkinci olarak, "erişim kontrolü" sisteme kişisel erişim yetkilendirmesi anlamına gelmemektedir, aksine organizasyonel yetki, bireylere yetki vermektedir. Bignell davasında, bu tür bir kontrolü yapan, bizzat polis müdürünün kendisiydi ve çalışma kuralları gereğince erişim yalnızca polisiye amaçlara özgülenmişti. Allison kararının bir sonucu olarak, PNC'nin polis tarafından kötüye kullanılmasına ilişkin sonraki bir davada[319] sanığın yetkisiz erişimden dolayı suçlu bulunması sağlanmıştır[320].

Allison kararı madde 17(5)'e göre "kontrolün" anlamını açıklığa kavuşturmuştur, mahkemenin *Bignell* kararını kabul etmesi ise CMA'dan kaynaklanan mahkeme kararının belirsizliğini devam ettirmiştir. İlk olarak Lord Hobhouse, *Bignell* davasındaki bilgisayar operatörünün yetkisini aşmadığı ve dolayısıyla bir suç işlemediği noktasına vurgu yapmıştır. Operatör yalnızca masum bir çalışan olduğuna göre[321], bu vurgu *Bignell*'in madde 1'de tanımlanan suçu işleyip işlemediği sorusu ile ilgili görünmemektedir; ayrıca *Bignell*'in talebiyle yetkisiz erişim arasında nedensellik bağını da kırmamaktadır. İkinci

[1999] 4 ALL ER 1.

317 Bu açıklama karar temyiz edildiğinde Bölge Mahkemesi tarafından takip edilmiştir. Bkz: R v. Bow Street Magistrates' Court, tek taraflı olarak (hasımsız) Allison [1999] QB 847.

318 Walden, pn. 3.253.

319 Begley, Coventry Magistrates' Court, akt: Michael J. L. Turner, "Computer Misuse Act 1990 Cases" http://www.computerevidence.co.uk/Cases/CMA.htm, 30.8.2016. Ayrıca bu kişinin suiistimal dolayısıyla işten çıkarılmasına ilişkin dava üzerine yapılan temyiz başvurusunda hukuki bir inceleme için bkz: R (Begley'in başvurusu üzerine) v. Chief Constable of the West Midlands [2001] EWCA Civ 1571.

320 Walden, pn. 3.254.

321 Örneğin R v. Manley (1844) 1 Cox 104.

olarak Lord Hobhouse, yetkilendirmenin kapsamının bu tür güvenli erişimlere yetkilendirme açısından saflaştırılmaya (düzeltilmeye) ihtiyacı olduğunu ve verilerin görülebilmesi için verilen erişim yetkisinin bunların kopyalanması veya değiştirilmesini kapsamadığı örneğini kabul etmiştir. Bu gerekçelerle mahkeme dolaylı olarak, verileri görmek için verilen yetkinin özel durumlar tarafından sınırlandırılmamasına karar vermelidir ki bu durum bağdaşmaz görünmektedir. *Bignell* davasındaki sanıklar yalnızca polisiye amaçlarla PNC'ye erişim sağlamaya yetkilerinin olduğunu biliyorlardı ve kendi ihtiyaçları doğrultusundaki amaçlarını bilerek ortaya koymuşlardı[322].

Siber Suçlar Sözleşmesi'nde ve AB Direktifinde kullanılan "hakkı olmaksızın" kavramı "teamül hukuku" (common law) yaklaşımına karşı temel bir farklılık olarak ortaya çıkmaktadır. Anglo Amerikan ceza hukukunda bir husus aksi belirtilmedikçe hukuka uygundur; oysa Kıta Avrupası ceza hukuku sisteminde bir husus ancak açıkça belirtilmişse hukuka uygundur (Kıta Avrupası ceza hukuku sisteminde ceza yasalarındaki suç tiplerinde eylemin açıkça hukuka aykırı olduğunun belirtilmesi gerekmez, zira tipiklik hukuka aykırılığın karinesidir). Sözleşmenin Açıklayıcı Raporu "hakkı olmaksızın" ifadesinin, "yetki olmaksızın gerçekleştirilen" davranışa -ki bu yetki hukuki düzenlemeler ve rıza gibi çok sayıda kaynaktan elde edilmektedir- veya iç hukukun tanıdığı "meşru savunma, mazeret nedeni, hukuka uygunluk nedeni veya benzer diğer ilkeleri" kapsamayan davranışların her ikisine de işaret ettiğini belirtmektedir[323]. Birleşik Krallık hukuku açısından, ilk ifade "pozitif" bir yetkiye ikincisi ise "negatif" bir yetkiye işaret etmektedir. Açıklayıcı raporu hazırlayanlar, özellikle kolluk güçlerinin bir bilişim suçu soruşturmasındaki davranışlarının söz konusu yeni suç tiplerinden etkilenmeyeceği hususunda emin olmaya heveslidirler[324].

Kolluk kuvvetleri, dinleme gibi bazı soruşturma işlemlerini gerçekleştirebilmek için "pozitif" yetkiye ihtiyaç duyarlar; ancak aynı zamanda sistem bütünlüğüne karşı bir suçun işlenmesi durumuna ilişkin bir savunma nedeni olması için "negatif" hukuka uygunluk yetkisi de gerekir. CMA uyarınca gerçekleştirilen kolluk güçlerinin davranışlarının belirtilen ikinci görünüşü bunun karmaşıklığını kanıtlamakta ve zamanla değişiklik göstermektedir. Yasanın özgün halinde, kolluk güçleri dinleme, arama ve el koyma yetkilerini kullandıklarında, araya bunu uygulanamaz hale getiren, yetkisiz erişim suçları hakkında korumacı bir hüküm eklenmiştir[325]. Ancak bir kolluk görevlisi bu tür bir yetkiyi kullanmadığında, böyle bir sorumluluğa maruz kalma potansiyeli

322 Walden, pn. 3.255.
323 Avrupa Siber Suçlar Sözleşmenin Açıklayıcı Raporu pn. 38.
324 Avrupa Siber Suçlar Sözleşmenin Açıklayıcı Raporu pn. 38; Walden, pn. 3.256.
325 CMA, m. 10 (1990 tarihli özgün hali).

devam etmektedir. Gerçekten de, bazı web siteleri bu boşluktan yararlanarak, kolluk güçlerinin web sitelerine erişim yetkilerinin olmadığını özellikle belirtmeye başlamıştır. Bu hususa değinmek için koruyucu hüküm 1994 yılında şu şekilde değiştirilmiştir[326]:

"…kolluk güçleri gibi kişilerin herhangi bir yazılıma ya da veriye erişim izinlerinin kısıtlanmasına yönelik bir düzenleme söz konusu değildir, kolluk güçleri madde 1(1)'de belirtilen amaçları gerçekleştirmek için yetkisiz erişimde bulunabilirler".

Çok yakında, koruyucu hüküm hakkında başkaca düzenlemeler yapılmıştır[327], bu hükmün her iki odağı CMA'da düzenlenen sistem bütünlüğüne ilişkin tüm suçları kapsayacak şekilde genişletilmiştir; bu bağlamda söz konusu düzenleme daha etkili polisiye davranışlar için bir savunma sağladığı gibi aynı zamanda söz konusu güç bu tür davranışlara da yetki vermektedir[328].

Ayrıca AB Direktifinde belirtilen "hakkı olmaksızın" kavramına özgü bir sorun olduğu da görülmektedir. Sözleşmede, kontrole ilişkin yetkilendirme, tümüyle sisteme atıf yapmanın yanı sıra, bu tür bir erişime de izin verilmektedir. Ancak Direktifte, yetkilendirme sistemin sahibinin ötesinde bir diğer hak sahibi üçüncü kişiye ya da bunun bir parçasına dek genişlemektedir[329]. Bunun kapsamı yukarıda tartışıldığı üzere kısmen, sistem ile veri arasındaki ayrım üzerine dayanmaktadır. Hangi genişlikteki veri, sistemin bir parçasıdır? Eğer veri, sistemin bir parçası ise, o halde ürün fikri mülkiyet hukuku tarafından korunmalıdır (örneğin; telif hakkı, dizayn hakkı ya da çip koruması gibi). Bu durumda hak sahibinin izni olmaksızın ürünün kullanımı, potansiyel olarak bir suçun gerçekleşmesine neden olmaktadır. Bilgisayarın bütünlüğüne karşı suçların arka kapısı vasıtasıyla bu tür bir fikri mülkiyet hakkı ihlalinin suç haline getirilmesi, kesinlikle bu direktifi hazırlayanların amacını oluşturmamaktadır[330].

İngiltere Uluslar Topluluğu Model Yasası'nda kullanılan "hukuka uygun bir mazeret nedeni veya hukuka uygunluk nedeni olmaksızın" ifadesi de problemli bir formülasyon olarak görünmektedir. Bu ifade, Model Yasada ayrıntılı bir biçimde tanımlanmamaktadır. Ancak "hukuk uygun bir mazeret nedeni olmaksızın" ifadesi İngiliz hukukunda suçtan kaynaklanan bir zararının meydana gelmesi halinde söz konusu olmaktadır; bu mazeret iki şekilde açıklanabilir: Rızanın varlığına ilişkin bir kanaatin olması ya da olacağı veya malvarlığının korunması için gerekli olması[331]. "Kanaat" ifadesi özneldir, haklı

[326] Walden, pn. 3.257.
[327] CMA, m. 10. Söz konusu düzenleme 2015 tarihli Ciddi Suçlar Yasası m. 44(2) ile yapılmıştır.
[328] Walden, pn. 3.257.
[329] Direktif 13/40/EU m. 1/d.
[330] Walden, pn. 3.258.
[331] 1971 tarihli Suçtan Kaynaklanan Zararlar Yasası (Criminal Damage Act 1971) m. 5(2).

olmak veya makul olmak ile bir ilgisi yoktur. Savunma makamının, örneğin failin eyleminin hukuka uygunluğunun güvenlik alanında alınan önlemlerin kırılganlığını gösterdiğini ileri sürmesi beklenebilir. Bu husus *Grey* davasında[332] ileri sürülmüştür: *"Sizin iddia edilen güdünüz gerçekte elektronik ticaret perakendecilerinin güvenlik bilinçlerinin olmadığını göstermekte ve ilan etmektedir…"*.

Herhangi bir kişi, bu tür bir hukuka uygunluk nedeninin, jüriye karşı güçlü bir Robin Hood başvurusu olduğunu hayal edebilir. Bu arada "rıza", "yetkilendirme" yaklaşımıyla ortak noktaları paylaşır; bu anlatım, yetkilendirme açısından "bilmenin" gösterilmesinin gerekli olmasından ziyade bir tür savunma tarzı olarak ifade edilir. Bu ikinci gereklilik, sistemin bütünlüğüne ilişkin suçlar açısından ceza hukukunun kapsamını indirgeme olasılığı olduğundan, pozitif bir özellik olarak görülür[333].

3. Yetkisiz Erişim

a. CMA madde 1'de Düzenlenen Yetkisiz Erişim Suçu

CMA madde 1, yetkisiz erişimi temel bir suç olarak düzenlenmiştir[334]. Suçun oluşması için "bilgisayarın herhangi bir işlevinin yürütülmesine neden olma" maddi unsurunun gerçekleşmesi gerekir. Dolayısıyla bilgisayarla bir şekilde etkileşimde bulunulması gerekir, ancak bunun gerçekleşmesi için fiili bir erişimin bulunması gerekmez. Bu genişlikte bir tanımlama, bilgisayarın basitçe başlatma düğmesine basılmasının yeterli olduğu ve tek başına bu hareketin maddi unsuru oluşturduğu anlamına gelir[335]. Buna rağmen bilgisayarın yalnızca sonradan satılması amacıyla çalınmasının CMA madde 1'de düzenlenen suçu gerçekleştirmesi olanaklı değildir[336].

Bu suçun oluşturulmasının arkasındaki düşünce, aslında bilişim korsanlarının yüzüne tüm kapıların kapanmasıdır. Bilişim korsanının kötü bir amacı olmasa ya da eylemini merak dürtüsünün ötesinde bir amaçla yapmıyor olsa da suç oluşur. CMA madde 1'de düzenlenen suçun esasını, yetkisiz bir erişimi güvenceye almak adına kasten bir bilgisayarın işlem yapmasını sağlamaktır. Fail tarafından belli bir bilgisayarın hedef alınması gerekmez,

---

332 [2001] Swansea Kraliyet Mahkemesi, 6 Temmuz 2001, pn. 4C.

333 Walden, pn. 3.259.

334 Ancak bu suçtan dolayı cezalandırmanın son derece az olduğu belirtilmektedir. Yasanın yürürlüğe girdiği 1990 ile 2006 yılları arasında 161 olayda bu suçtan dolayı ceza verilmiştir. Organizasyonların, güvenlik açıklarının ortaya çıkmasını engellemek adına kendilerine karşı işlenen suçları rapor etmedikleri belirtilmektedir. Ormerod, Smith & Hogan's Criminal Law, s. 1048. Ayrıca bkz: MacEwan, s. 962.

335 Clough, s. 72.

336 Walden, pn. 3.261.

yetkisiz olarak erişim sağlanmaya çalışılması yeterlidir. Aslında, yetkisiz olarak erişim sağlanmasına yönelik bir düzenek oluşturulması, bu suçun oluşması için yeterlidir[337].

Bu suçun kapsamı, *"neden bir ofis bilgisayarındaki dosyalara erişmek suç olarak düzenleniyorken, dosya dolabında bulunan bir kâğıda erişmenin suç olarak düzenlenmediği"* sorusunu akla getirir[338]. Hukuk Komisyonu, dolandırıcılık yapmaya niyetlenen ya da bunun daha ileri aşamalarında suçlar işlemek isteyen veya yetenekleri yüzünden başkaları tarafından kötücül amaçlarla suç işlenmesine yardım ettirilmek istenenlerin hepsinin caydırılması amacıyla bilişim korsanlarına tüm kapıların kapanmasının en iyi yol olduğunu düşünmüştür. Bu açıdan; bu soru, cezalandırmama yönünde ikna edici bir gerekçe değildir; cezalandırmamanın seçilmesi halinde failin hareketi uygun bir şekilde cezalandırılmayacaktır, çünkü bu hareketler bir suçun işlenmesine öncülük yapabilecektir. Bu tür hareketleri suç haline getirmedeki gerekçelerden biri, sistemin malikinin, yetkisiz erişim sağlayan kişi yüzünden sistemini korumak için dikkate değer bir harcama yapmak zorunda kalmasıdır[339]. Elbette kâğıt dosyaların maliki de eğer bir kişi ofisteki dosyalara bakmak için ofisin güvenliğini kırarak zorla içeri girerse bunu tamir etmek için bir harcama yapmak zorunda kalacaktır. Ancak basılı belgeler ile bilişim sistemleri arasında önemli farklar bulunur: Basılı belgeler açısından mütecavizin ofisin güvenliğini kırıp içeri girmeden basılı belgelere ulaşması mümkün değildir; öte yandan bilişim sistemleri söz konusu olduğunda, failin ülkenin bir başka yerinden hatta birçok olayda görüldüğü üzere dünyanın bir başka yerinden sisteme girmesi ve belgelere (verilere) ulaşması mümkündür[340]. Bilişim sistemleri, azimli bilişim korsanları için her zaman kırılgandırlar. Gittikçe artan bir biçimde bilgisayarlara ve bu bilgisayarların sağlamlığına (veri bütünlüğüne) bağımlı hale gelen bir dünyada, ceza hukukunun, bilişim korsanlarının cesaretini kırmak için kullanılması tamamıyla doğru bir seçim olarak görülmelidir[341].

---

337 Ormerod, Smith & Hogan's Criminal Law, s. 1048.

338 Yasa hakkında ileri sürülen bazı görüşlerde bunun aşırı bir düzenleme olduğunu, 1. maddedeki suçun "güvenlik önlemlerinin" ihlal edilmesine ilişkin hareketler olarak sınırlandırılması gerektiği ileri sürülmektedir. Bkz: S. Room, "Criminalising Cybercrime" (2004), 154 NLJ 950; akt: Ormerod, Smith & Hogan's Criminal Law, s. 1048.

339 Hukuk Komisyonu vermiş olduğu bir örnekte, yetkisiz erişime takiben sistemi yeniden yapılandırabilmek için bu konudaki uzman çalışanlar tarafından 10.000 saatlik bir çalışma yapılması gerektiğini ve bunun maliyetinin 300.000 Sterlin olduğunu belirtmiştir. Bkz: Baker [2011] EWCA Crim 928.

340 Yargı yetkisi konusuyla ilgili olarak bkz: Uta Kohl, Jurisdiction and Internet: Regulatory Competence over Online Activity, Cambridge, Cambridge University Press, 2007, s. 1 vd.; Michael Hirst, Jurisdiction and the Ambit of the Criminal Law, Oxford, Oxford University Press, 2003, s. 193 – 196.

341 Ormerod, Smith & Hogan's Criminal Law, s. 1048.

Sırf yetkisiz erişim ilk olarak suç haline getirildiğinde, bu tür durumlara ceza hukuku normlarının uygulanmasının uygunluğu, tartışmaların odağını oluşturmuştur. Gerçekten yukarıda belirtildiği üzere, uluslararası mevzuat açısından söz konusu tartışma halen devam etmektedir. Ancak, Birleşik Krallık'ta, bunu suç haline getirmeye karşı çıkan görüşlerin azaldığı, bunun yerine suç oluşturmaya ilişkin girişimlerin büyük bir ciddiyetle ele alındığı görülür[342].

Yetkisiz bir erişim dolayısıyla bir sistem sahibine zarar verilmesi, failin kast ettiklerinden farklı olarak, üç geniş tipe bölünür. Bunlardan ilki, sistemin gizliliğinin ihlalinin ve veri gizliliğinin, bütünlüğünün ve erişilebilirliğinin üzerinde herhangi bir etkisinin olup olmadığının kontrol edilmesi için yapılması gerekli olan soruşturmanın maliyetidir. İkincisi, sistemin gelecekteki bu tür hukuka aykırı erişimlerden korumak için gerekli olan iyileştirici önlemlerin maliyetidir. Üçüncüsü ise, failin hareketleri neticesinde istemi olmaksızın sisteme ya da verilere verdiği zararların ya da meydana getirdiği değişimlerin onarılması için gerekli olan maliyettir. Ancak tüm örnekler, istem olmaksızın verilen zarar ya da değişiklik gibi, üç tipe bölünmüş olan yetkisiz erişimlere daha ciddi yaptırımların uygulanmasının gerekçesi olarak kullanılmaktadır. Yetkisiz erişim suçu neticesinde beliren bu gibi kayıpların, erişim (access) konusu ile müdahale (interference) konusu arasında karışıklığa yol açtığı görülür; bunlardan ikinci suç daha ağırdır ve yetkisiz bir erişimin bulunmasını gerektirmez[343].

CMA madde 1/1'de düzenlenen suçun maddi unsurunu, yukarıda da belirtildiği üzere, bir bilgisayarın işlevde bulunmasına neden olmak oluşturur[344]. Yukarıda da belirttiğimiz üzere, suçun tanımına göre failin yalnızca bilgisayarı başlatma düğmesine basması suçun oluşumu için yeterli görünür, ancak failin tüm yaptığının bu hareket olması halinde suçun manevi unsurunun (mens rea) ispatı son derece güç olur. Öte yandan ispat yükünün sıkı şartlara bağlı olmasının CMA'ya göre yapılan suçlamalarda zorluklara neden olduğuna ilişkin olaylar bildirilmektedir. Bu suçun oluşması için, verilerin yalnızca bilgisayar ekranında görülmesi yeterli değildir; ancak örneğin, failin geri alma ya da dönüş tuşunu kullanarak, son kullanıcının sisteme bağlıyken bırakıp gittiği bilgisayarı kullanmak suretiyle üniversitenin bilişim ağına bağlanması halinde bu suç oluşur[345]. Bu suça ilişkin davalarda bilgisayarın bir işlev yaptığını ortaya koymak için her zaman bilirkişi raporu (expert evidence) gerekmez[346].

---

342 Örneğin PJA ve 2015 tarihli Ciddi Suçlar Yasası ile yapılan değişiklikler.

343 Walden, pn. 3.272.

344 Ormerod, Smith & Hogan's Criminal Law, s. 1048.

345 Bkz: Ellis v. DPP [2001] EWHC 362. Bu davada failin, gerçekleştirdiği eylemin çöpe atılmış bir gazete ile aynı olduğu yönündeki savunması başarılı olmamıştır.

346 Ormerod, Smith & Hogan's Criminal Law, s.1049. Önceki dipnotta verilen dava bunun

Fail, bir bilgisayarın işlem yapmaya neden olma hareketini (i) herhangi bir bilgisayarda bulunan bir yazılım ya da veriye güvenli bir erişim sağlama kastıyla ve (ii) güvenli bir şekilde gerçekleştirmeye çalıştığı erişimin yetkisiz olduğunu bilerek gerçekleştirmelidir. Bu eylemin taksirle işlenmesi suç değildir[347]. Erişimin hangi hallerde yetkisiz olacağı CMA'nın 17(5) maddesinde tanımlanmıştır. Buna göre *"(i) Failin söz konusu yazılım ya da veriye erişim için bir şekilde yetkilendirilmemiş olması, (ii) Faile, söz konusu yazılım ya da veriye erişim için yetkilendirilmiş bir kişi tarafından bir şekilde rıza gösterilmemiş olması"* hallerinde veriye erişmesi durumunda yetkisiz erişim vardır[348].

Fail, anlamsız olsa da, erişim sağlamak için yetkili olduğuna ya da yetkili bir kişi tarafından kendisine bu konuda yetki verildiğine inanıyorsa, erişiminin yetkisiz olduğunu bilemez. Bu konuda denetlenmesi gereken, büyük bir olasılıkla şu husustur: Failin yetkilendirme ya da yasaklama için yetkisi var mıdır? Daha zor olan konu ise failin yetkili olup olmadığı, hatta daha sıklıkla görülen biçimde yetkisinin sınırının ne olduğu hususunda emin olmadığı halde buna rağmen yetkisinin var olup olmadığı veya var olan yetkisinin sınırını kontrol etmeden hareket etmeye karar vermesi halinde ne olacağıdır. Eğer, davalarda sıklıkla görülüğü üzere, fail yetkisinin olup olmadığını veya yetkisinin sınırının ne olduğunu kolaylıkla öğrenebilecekken bunu öğrenmeyi seçmemiş ve erişime yetkili olduğuna karar vererek risk üstlenmişse, bu gerçekten erişiminin yetkisiz olduğunu gösterir. Bu durumda failin erişiminin yetkisiz olduğunu bilmediği söylenebilecekse de, bu bilgisizlik yalnızca failin bunu öğrenmek istememesinden kaynaklanır. Bu tür kasıtlı körlük, bilmenin oluşması için yeterli sayılır. Bir diğer uçta ise, failin yetkisinin sınırının aşmış olabileceğini aklından geçmekte oluşu yer almaktadır ki bu durum bilme için yeterli değildir[349].

Failin bilgisayarı kullanmak için yetkili olduğu, ancak belli bir yazılımı kullanmak için yetkisinin olmadığı durumlarda da suç oluşabilir[350]. Failin belli bir bilgisayara erişmek için (örneğin, X bilgisayarı) yetkisinin olması, ancak failin erişim yetkisinin olmadığı bir başka bilgisayara (örneğin Y bilgisayarı) erişmesi de söz konusu olabilir. İşte bu durumda failin Y bilgisayarına erişebilmek için önce X bilgisayarına erişmesi, ancak henüz Y bilgisayarına erişmemesi halinde dahi suç oluşur[351]. Buna benzer bir biçimde, failin sınırlı bir erişim izninin olması, ancak bu iznin sınırını aşarak hareket etmesi halinde de suç oluşmaktadır. Örneğin, bir American Express çalışanı, yalnızca belli bazı

örneğini oluşturur.

347 Ormerod, Smith & Hogan's Criminal Law, s. 1050.

348 CMA m. 17(10)'a göre yazılım, yazılımın bir parçasını oluşturan verileri de içerir.

349 Ormerod, Smith & Hogan's Criminal Law, s. 1050, 1051.

350 Bkz: Ellis v. DPP [2001] EWHC 362.

351 Ormerod, Smith & Hogan's Criminal Law, s. 1051.

hesaplara erişim yetkisine sahipken, diğer hesaplara da erişmek suretiyle bu suçu işlemiştir[352].

Görüldüğü üzere İngiliz hukukunda ülkemizden farklı olarak henüz teşebbüs ve hatta kimi zaman hazırlık hareketi sayılabilecek hareketler dahi suçun içinde kabul edilmekte ve tamamlanmış suç gibi cezalandırılmaktadır. Bu anlamda bizdeki teşebbüs kavramıyla Anglo Amerikan hukuk sistemindeki teşebbüs kavramı ciddi farklılıklar gösterir.

Avrupa boyunca, AB üyesi devletler, benzer yetkisiz erişim suçlarını iç hukuklarına uyarlamıştır[353]. Bundan farklı olarak Birleşik Devletler ise CMA madde 1'de düzenlenen suça benzer bir düzenlemeye federal yasalarında yer vermemektedir. Yetkisiz erişim yalnızca belli düzeyde bir eşik aşıldığında suç olarak kabul edilir; örneğin, bir bilgisayara yetkisiz erişim on iki aylık bir zaman diliminde beş bin dolardan fazla bir zarara ulaştığında suç oluşur[354].

Bu suç için öngörülen ceza en fazla iki yıla kadar hapis cezasıdır.

b) CMA madde 2'de Düzenlenen Başka Suçların İşlenmesini Kolaylaştırmak İçin Yetkisiz Erişim Suçu

CMA madde 2'ye göre, m. 1'de düzenlenen suçun, başka (daha ileri / ağır) suçların işlenmesini sağlamak ya da kolaylaştırılmak için işlenmesi ayrı bir suçtur. Bu suçların ve yalnızca erişim sağlamanın arasındaki ayrım, amaçlardaki farklılıkların, Hukuk Komisyonunun deyişiyle "gizli amacın" bulunması nedeniyledir[355]. Yetkisiz erişim hareketiyle diğer eklenen amaçlar arasında bağlantı kurulması, diğer ülke hukuklarında da sıklıkla görülen bir durumdur. Gerçekten Siber Suçlar Sözleşmesi, sözleşmeci taraflara "bilgisayar verisi elde etme kastı ya da diğer dürüst olmayan kast" şeklinde suçta ek kast aranması düzenlemesi yapma yönünde seçenek tanımıştır[356]. CMA madde 2'de belirtilen başka suçların cezaları yasa tarafından belirtilmiştir; örneğin, cinayet için müebbet hapis cezası, bilişim sistemleri suretiyle gerçekleştirilen dolandırıcılık için beş yıl veya daha fazla hapis cezası gibi. Erişimin ve başka suçun aynı anda işlenmesine kast edilmesi gerekli değildir, ayrıca başka suçun işlenmesinin mümkün olmaması ya da sonrasında işlenecek suçun bilişim

---

352 Bow Street Magistrate, ex p Government of USA [2000] 2 AC 216, [2000] 1 Cr App R 61, HL. Bu karar Bignell kararını doğru bulmamaktadır.

353 Örneğin Fransız Ceza Kanunu m. 323-1: "Hileyle bir bilgi sistemine erişim sağlayan ve bunu devam ettiren".

354 18 USC m. 1030(a)(4). Walden, pn. 3.273.

355 Law Commission, Computer Misuse, Report No 186, Cm 819, London, HMSO, 1989, pn. 3.49

356 Siber Suç Sözleşmesi m. 2. Yalnızca Birleşik Devletler bu ek seçeneği kullandığını beyan etmiştir.

sistemleriyle işlenebilecek bir suç olması önemli ve gerekli değildir[357] (CMA madde 2(2), (3), (4)). Mahkûmiyetin gerekçesine bağlı olarak failin yirmi bir yaşın üstünde olması ve daha önceden mahkûmiyeti olmaması halinde bu suçtan beş yıla kadar hapis cezasına çarptırılması mümkündür[358]; jürisiz yapılan yargılama sonucunda ise bu suça altı aydan on iki aya kadar hapis cezası verilebilir (CMA madde 2(5))[359].

Uygulamada bu suçlar, büyük olasılıkla fail tarafından malvarlığına karşı işlenecek suçları işlemek kastıyla veya bunları kolaylaştırmak amacıyla işlenmektedir; ancak madde 2'de yer alan suçun yalnızca malvarlığına karşı suçlarla sınırlanmadığı belirtilmelidir[360]. Muhtemelen, CMA yürürlüğe girdiği zaman, Hırsızlık Yasası (the Theft Act) (makinelerin aldatılmasına ilişkin ek bir suçla birlikte[361]) bu tür malvarlığına karşı suçlara uygulanması açısından da uygundu. Bu, CMA taslağı hazırlandığı zaman Hukuk Komisyonunun soruna ilk aşamadaki bakış açısını göstermektedir. Ancak buna ilişkin ikinci bir görüş ve varılan sonuç ise, bilişim korsanları henüz esas suçu işlemeden ya da esas suçu işlemeye teşebbüs etmeden, bunların hareketlerine ceza hukukunun normlarının uygulanma alanının genişletilmesi tercih edilebilir bir yaklaşımdır. CMA madde 1'de olduğu gibi, madde 2'de de hazırlık hareketlerini hedeflemektedir. Bu bağlamda konuya ilişkin Hukuk Komisyonu tarafından verilen örnek şöyledir: Hırsızlık yapmak amacıyla bir hesaba giriş için şifre arayışında olan bir bilişim korsanı hırsızlığa teşebbüsten suçlu bulunamaz, benzer biçimde tehdit mesajı göndermek için mahrem bilgi arayan bir bilişim korsanı da tehdit mesajı göndermeye teşebbüsten suçlu bulunamaz[362]. Ancak her ikisi de CMA madde 2'ye göre suç işlemiş olurlar. Bu suçun faili alışılageldiği üzere yalnızca bilişim korsanları değildir; banka verilerine erişim sağlayan bir banka çalışanının, suç ortaklarının dolandırıcılık eylemlerini gerçekleştirebilmeleri için bu verileri onlara açıklaması halinde de[363] bu suç oluşur[364].

Hukuk Komisyonu, CMA madde 2'deki suçun "bir nevi teşebbüse ilişkin bağlantılara" kapı açacağını, böylelikle sonraki suçun işlenmesinin gerekmeyip yalnızca bu suça kast edilmesinin yeterli olacağını ve madde 2(4) uyarınca

---

357 Ormerod, Smith & Hogan's Criminal Law, s. 1052.
358 Ormerod, Smith & Hogan's Criminal Law, s. 1051.
359 Walden, pn. 3.274.
360 Yaralama ve hatta öldürme amacıyla bir kara trafik ya da hava trafik sistemine girilmesi mümkündür. Ancak vatana ihanet amacıyla bilişim korsanlığı suçunun işlenmesi pek de mümkün görülmemektedir (casusluk bunun dışındadır).
361 Bu suç şu anda 2006 tarihli Dolandırıcılık Yasasında (Fraud Act 2006) bulunmaktadır.
362 Örneğin bkz: Zezev [2002] Crim LR 648.
363 Delamare [2003] All ER (D) 127 (Feb).
364 Ormerod, Smith & Hogan's Criminal Law, s. 1052.

sonraki suçun işlenmesi mümkün olmaması halinde dahi madde 2'deki suçun gerçekleşeceğini düşünmüştür. Bu hükmün gerekli olmadığı, ancak bunun koruma (yardımcı) norm olduğu görüşü ileri sürülmüştür. Örneğin, failin mağdurun banka hesabına ilişkin bilgileri elde etmek için mağdurun bilgisayarına girmesi, ancak halihazırda mağdurun banka hesabını kapatmış olması durumunda bu suç uygulanır[365].

CMA madde 2'de düzenlenen suç, bir temel suç oluşturduğunda ise bir komplo suçu söz konusu olabilir, zira suçun işlenmesine teşebbüs oluşturmakta veya suçun işlenmesine yardım etmekte ve işlenilmesini cesaretlendirmektedir. Bu, karşımıza oldukça geniş düzenlenmiş bir suçu çıkarır. Fail A, fail B ile mağdur C'nin bilgisayarına gelecekte erişmek ve elde edebildikleri bilgileri alarak bir başka suçun hazırlanmasında kullanmak üzere anlaşmış olabilir. Bu suçun hazırlık hareketi niteliğindeki yapısı nedeniyle suça teşebbüs için çok az bir aralık kalmaktadır[366].

Aşağıdaki olaylar CMA madde 2 uyarınca gerçekleşebilecek suçlara örnek oluştururlar[367]:

— *Pearlstone*[368] davasında, şirketin eski bir çalışanı şirketin telefonunu ve bir başka abonenin hesabını kullanarak bilgisayar ile yönetilen telefon sistemini aldatmış ve Birleşik Devletler'deki kişilerle ücretsiz telefon görüşmeleri yapmıştır.

— *Borgy*[369] davasında, bir yatırım şirketi analisti "canlı" fon yönetim sistemi adıyla sahte hesaplar oluşturmaktan suçlanmıştır. Suçlamaya konu olan "başka suçlar" hileli işlemlerden elde edilen gelirlerin sahte hesaplara aktarılması beklentisidir.

— *Grey*[370] davasında sanık, Microsoft İnternet Bilgi Sunucusu uygulamasını kullanan bir elektronik ticaret sitesindeki zayıflığı kullanarak, sitenin müşteri veri tabanına ulaşarak en azından 5.400 müşteriye ait kredi kartı bilgileri ile kişisel verileri elde etmiştir. Daha sonra bu bilgiler, internette yayınlamış ve bununla birlikte bu bilgileri kullanarak çeşitli mal ve servisleri satın almıştır.

---

365 Ormerod, Smith & Hogan's Criminal Law, s. 1052.

366 Ormerod, Smith & Hogan's Criminal Law, s. 1052.

367 Walden, pn. 3.275.

368 Bow Street Magistrates' Court, Nisan 1991; bkz: Rupert Battcock, "Prosecutions under the Computer Misuse Act 1990", Computers and Law, Vol. 6, No. 6, 1996, s. 22-26.

369 Battcock, s. 22-26.

370 [2001] Swansea Crown Court, 6 Temmuz 2001.

— *Brown*[371] davasında sanık, çalıntı banka ve kredi kartı bilgilerini elde etmiş, bu bilgileri çevrimiçi olarak hesap bilgilerini değiştirmek için kullanmış ve hesap sahibinin yerine geçerek yeni kartlar ve PIN numaraları oluşturmuş sonrasında da hesapların içini boşaltmıştır.

CMA madde 2 gereğince yapılan suçlamaların göreceli olarak sık görülmemesi ya da diğer suçlarla içtima sorunları ortaya çıkması ihtimal dahilindedir. Zira savcılar yetkisiz erişimdense, bu hareketten geçilerek işlenen başka (ileri / ağır) suçlardan suçlamada bulunmayı tercih etmektedirler. Buna rağmen bazı münferit olaylarda, öncelikle madde 2'den suçlamada bulunulduğu görülür. Buna ek olarak, failin yetkisiz erişim hareketi, daha ağır suça teşebbüsten suçlamada bulunmak için yeterli olabilir[372], hatta bunların "hazırlık hareketi" olarak atılan adımlar olarak kullanılması daha olasıdır[373].

Etkin bir ceza kanunu, hangi eylemlerin suç işlemeyi "kolaylaştırıcı" suçlar olarak kabul edileceğinin belirlenmesini gerektirir. Bunlar, bir suçlunun soruşturulmasını ve failin daha ağır suçlardan suçlanmasını sağlayan suçlardır; ancak bunlar, genellikle temel ya da öne çıkan suçlar olarak kullanılmazlar. CMA'nın hem 1. hem de 2. maddesinde bulunan suçlar bir çeşit "kolaylaştırıcı suç" olarak tanımlanabilirler. Buna rağmen, gerçek şu ki diğer teşebbüs ya da hazırlık hareketi suçlarında olduğu gibi, bunlar sınırlı uygulanmalı ve bunların güncel kullanımlarının suçla mücadelede kendiliğinden değerli olmayan araçlar olarak görülmesine yol açmamalıdır[374].

4. Yetkisiz Müdahale

a) Sistem Bütünlüğünü ve Verileri Bozma

Bir bilişim sistemine yetkisiz erişim sağlanması, o sistemde yer alan bilgilerin gizliliğine yönelik açık bir tehdit oluşturur. Bununla birlikte, bir bilişim sistemine erişim sağlanmasından daha önemli olan husus, failin sistemde bulunan veri ya da donanıma müdahale etmek suretiyle işlem gören bilgilerin bütünlüğüne ve erişilebilirliğine etkide bulunabilmesidir. Bu tür müdahaleler, bir çeşit elektronik vandalizm ya da bilişim korsanlarının sistem içinde hareketlerini gerçekleştirirlerken ortaya çıkan yan ürün olarak, kasıtlı bir hareketin sonucu olabilir. Gerçekten, bir sisteme sırf yetkisiz erişimin suç olarak tanımlanmasının lehinde ileri sürülen görüş, bu tür bir erişimin kasıtlı

---

371 [2014] EWCA Crim 695.

372 Bkz: 1981 tarihli Suça Teşebbüs Yasası (Criminal Attempts Act 1981) m. 1: "Eğer, bu maddenin uygulandığı suçun işlenmesine kastedilmişse, kişi suçun gerçekleşmesi için yalnızca hazırlık hareketinden daha fazlasının yapılması halinde suça teşebbüsten suçlu bulunur".

373 Martin Wasik, Crime and the Computer, Oxford, Clarendon Press, 1991, s. 84; Walden, pn. 3.276.

374 Walden, pn. 3.277.

olmayan bir zarara da yol açabileceğidir. Yetkisiz erişim sonucu ortaya çıkan değişiklikler, basit zorluklardan insan yaşamına kasteden olaylara kadar değişiklik gösterir; örneğin *Rymer* davasında[375], hastanede çalışan bir hemşire hastanenin bilişim sistemini kırarak sisteme erişim sağlamış ve bir hastanın ilaç reçetesini değiştirmiştir[376]. Bu dava, ağa bağlı bilgisayarların bir cinayette nasıl kullanılabileceğini gösteren iyi bir örnektir[377].

Bu konudaki ikinci önemli endişe, uygulamada olayların mevcut yasalardaki suçtan kaynaklanan zararla nasıl örtüştüğünün yargıçlara ve jürilere açıklanması hususunda polisin ve savcılığın karşılaştığı zorluklardır[378].

Whitaker davasında[379], mahkeme bir fikri mülkiyet hakkı sahibine karşı gerçekleştirilen yetkisiz değiştirme suçunun kapsamının ne olduğunun belirlenmesini gerekli bulmuştur. Dava, bir yazılım geliştiricisi ve onun müşterisi hakkında olup, geliştiricinin, ödeme konusunda bir uyuşmazlık olması halini takiben yazılımın kullanılmasını engellemek amacıyla geliştirdiği bir mantık bombasını çalıştırmasından kaynaklanır. Sanık yazılımcı, sözleşme gereğince yazılıma ilişkin her türlü fikri mülkiyet hakkının kendisine ait olduğunu (mülkiyetin ödeme yapılması halinde devredilmiş olacağını); kendisinin yazılımı değiştirmeye hakkı olduğunu ileri sürer. Mahkeme, yazılımın telif hakkının var olmasına rağmen, yazılımı geliştirmeye ilişkin sözleşmenin yapısının, geliştiricinin hakları üzerinde bir sınırlandırma oluşturduğuna karar verir. Buna karşın mahkeme, örneğin lisans sahibi ödemede temerrüde düşmesinin sonuçlarından haberdar ise, böyle bir hareketin sözleşme tarafından açıkça belirtilmesi halinde bunun gerçekleştirilmesini haklı bulur. Sonuç olarak sanık, CMA madde 3 gereğince suçlu bulunur. Bu karar, yazılım endüstrisi hizmetlerinin karşılığı olan alacaklarını garanti altına almak için bu tür yöntemlere başvurduğu için çok önemlidir[380].

---

375 Aktaran: Turner, "Computer Misuse Act 1990 Cases". Ayrıca bkz: "Nurse Alters Hospital Prescriptions", Computer Fraud & Security Bulletin, Issue 2, 1994, s. 4-5.

376 Walden, pn. 3.278.

377 Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, Santa Barbara, Praeger, 2010, s. 101; Susan W. Brenner, Cybercrime and the Law: Challanges Issues and Outcomes, Boston, Northwestern University, 2012, s. 116.

378 Walden, pn. 3.281.

379 Scunthorpe Magisrates Court (Sulh Ceza Mahkemesi), 1993, bkz: Battcock, s. 22-26.

380 Benzer şartlarda görülen bir özel hukuk davası için bkz: Rubicon Computer Systems Ltd. v. United Paints Ltd. (2000) 2 TCLR 453. Birleşik Devletler'de, 1999 tarihli Yeknesak Bilgisayar Bilgi Aktarımları Yasası (Uniform Computer Information Transactions Act 1999) m. 816 ile bu tür bir "elektronik kendi kendine yardım etme" mekanizmasını açıkça sağlamaktadır, buna karşın 2000 tarihli değişiklik ile kitlesel pazar ürünleri bu düzenlemenin dışında bırakılmıştır. Walden, pn. 3.292.

Mayıs 1993'te, ilk klasik "bilişim korsanına" CMA'nın 1. ve 3. maddelerinde tanımlanan suçları işlemeye yönelik anlaşma yaptığı için altı ay hapis cezası verilmiştir[381]. Sanık, "Sekiz Ayaklı Çentik Makinesi" (Eight Legged Groove Machine – 8LGM) olarak bilinen, güvenliğini kırdığı bilişim sistemleri arasında Londra Merkez Politeknik Enstitüsü'nden NASA'ya kadar çeşitli kuruluşlar bulunan ve neden olduğu zararın miktarı 123.000 Sterlin olan bir kişidir. Yargıcın kararında yer alan ve bilişim korsanlığına bakış açısını gösteren paragraf şöyledir:

"Oralarda bir yerlerde bilişim korsanlığını zarar vermeksizin gerçekleştiren birileri olabilir; ancak bilişim korsanlığı zararsız bir eylem değildir. Artık bilgisayarlar hayatımızda merkezi bir rol almakta ve kişisel ayrıntılarımızı içermektedirler… Bu sistemlerin bütünlüğünün korunması temel bir konudur ve güvenlik ihlalleri bilgisayarların bütünlüğüne *zarar vermektedirler"*[382]*.*

Eğer yasanın önemli bir caydırıcı etkiye sahip olması isteniyorsa bu tür yargısal duyarlılıklar kritik öneme sahiptir. Ancak jüri, aynı davada yargılanan Bedworth isimli sanığın beraatine karar vermiştir, çünkü savunma makamı bir tıp uzmanın tanıklığıyla (tıbbi bilirkişi raporu ile) sanığın "obsesif" bir bilişim korsanı olduğu iddiasını başarıyla ileri sürmüştür[383]. Bu davanın geniş bir biçimde reklamı yapılmış ve birçokları tarafından potansiyel *"bilişim korsanlığı beratı"* olarak görülmüştür. Ancak karar, iddia makamının CMA'ya göre bir suçlamada bulunmak yerine, suç işlemek için komplo kurmak suçlamasını tercih etmesi nedeniyle kısmen hatalı olarak verilmiştir[384].

b) Sistem Bütünlüğüne Yönelik Önemli Bir Saldırı Örneği: Suç İşleme Modeli, İddia, Savunma ve Karar

aa. Denial-of-Service Attacks / DoS Saldırıları

Özellikle eBay ve Amazon gibi ticari web siteleri ve diğer çevrimiçi kaynaklara karşı yapılan DoS saldırıları hakkında CMA madde 3'ün ilk halinde yer alan *"yetkisiz değişiklikte bulunma suçunun"* uygulanabilirliği, üzerinde durulması gereken bir konudur. Bu tür saldırılar, bir sitenin işleyişinin aksatılması / bozulması için, içeriğin barındırıldığı sunucuya kasten *"adeta bir sel şeklinde"* çoklu bilgi isteminde bulunulması şeklinde dizayn edilmişlerdir[385].

---

381 R. v. Strickland, R. v. Woods, Southwark Kraliyet Mahkemesi, 21 Mayıs 1993.

382 Walden, pn. 3.293.

383 Southwark Kraliyet Mahkemesi, 17 Mart 1993.

384 Walden, pn. 3.293.

385 Bu tür hareketler güya meşru amaçlarla gönderilen çoklu istemlerle karşılaştırılmalıdırlar, örneğin bir rakibin halihazırda geçerli olan fiyatları kontrol etmesi gibi. Bkz örneğin: eBay v. Bidders Edge, 100 F Supp 2d 1058 (ND Cal 2000), bu davada eBay, taşınır mallarının kötüye kullanılması iddiasına dayanarak başarılı bir biçimde uygulamayı durdurma (ihtiyati tedbir)

DoS saldırıları, bazen hedefteki makineden ziyade, iletişim hatlarında yoğunluğa neden olurlar. Nitekim böyle bir olay, Ekim 2002 tarihinde on üç alan adı sistemine ait (domain name system / DNS) kök ad sistemlerine yapılan saldırı ile gerçekleşmiştir[386]. Saldırı ister bağlantı kapasitesi ister bant genişliği üzerinde etkili olsun, birincil hedefi sistemin bütünlüğü ya da gizliliği olmayıp, çevrimiçi kaynaklara erişilebilirliğin tehlikeye atılmasıdır. Bu tür saldırıların amacı kumar sitelerine karşı yapılan şantajdan[387], küreselleşme karşıtı aktivistlerin Dünya Ticaret Örgütü'ne[388] ya da çok uluslu şirketlere[389] karşı gerçekleştirdikleri politik protestolara kadar uzanır[390].

Gerekli yoğunluğu elde etmek ve saldırganların bulunduğu yeri gizlemek için yapılan "dağıtık hizmeti engelleme saldırısı" (Distributed Denial of Service Attack / DDoS) bu alanda standart saldırı biçimini oluşturur. Çoklu bilgisayar istemini hareketli hale getirmek için saldırganlar genellikle gizlice "zombi" ya da "botnet" olarak bilinen ve sahiplerinin bilgisi dışında saldırganların kontrolü altına giren bilgisayarları ele geçirirler. Gerçekten de "botnetler" için, bilgisayarların yüzlük, binlik, hatta yüz binlik setler halinde suç aktiviteleri için kiralandığı bir karaborsa bulunur[391]. Bir güvenlik uzmanının belirttiği üzere; *"bilişim korsanları artık bilgisayarlara zarar vermek istememekte, bilgisayarlara sahip olmak istemektedirler"*[392].

Suç oluşturan davranış açısından, genellikle hukuka aykırı erişimi de içeren ve "botneti" de kapsayan tekil sistemlerin kontrolünün elde edilmesiyle (DoS), genellikle erişilebilirliği etkilemek üzere dizayn edilen hedefteki sisteme DDoS

---

kararı almıştır.

386 Paul Vixie/Gerry Sneeringer/Mark Schleifer, "Events of 21 Oct 2002", 24 Kasım 2002, http://c.root-servers.org/october21.txt, 23.9.2016.

387 Örneğin bkz: Mark Ward, "Bookies suffer Online Onslaught", BBC News, 19 Mart 2004, http://news.bbc.co.uk/2/hi/technology/3549883.stm, 23.9.2016.

388 Örneğin bkz. DJNZ and The Action Tool Development Group of the Electrohippies Collective, "Client-side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?", The Electrohippies Collective, Occasional Paper No.1, Şubat 2000.

389 22 Mayıs 2006 tarihinde Frankfurt Bölge Yüksek Mahkemesi, 13.000 gösterici tarafından Lufthansa'nın şirket web sitesine karşı yapılan, iki saat süren DDoS saldırısı şeklindeki çevrimiçi gösterinin hukuka aykırı bir zorlama ya da veri başkalaştırma olmadığına karar vermiştir. Andreas Thomas Vogel'e karşı açılan dava, Dava No 1 Ss 319/05 991 Ds 6100 Js 226314/01-1009, daha detaylı bilgi için bkz: http://post.thing.net/node/1370, 23.9.2016.

390 Walden, pn. 3.294.

391 Bkz: Depertmant of Justice, "Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers", Press Release, 3 Kasım 2005, https://www.justice.gov/ archive/criminal/cybercrime/press-releases/2005/anchetaArrest.htm, 23.9.2016; Drew Cullen, "Dutch Smash 100.000-Strong Zombie Army, DDoS Attacks and Paypal Fraud", The Register, 7 Ekim 2005, http://www.theregister.co.uk/2005/10/07/dutch_police_smash_zombie_network/, 23.9.2016.

392 Walden, pn. 3.295.

saldırısı yapılması arasında ayrım yapılması gerekir. CMA madde 3'te yer alan suçun değiştirilmeden önceki halinde, DDoS saldırısını gerçekleştirenlerin sorumluluğuna gitmek için açılan davalar iki nedenden kaynaklanan sorunla karşılaşmaktaydı; bunlar hareket ve kusurdur. İlk olarak suçu oluşturan hareket açısından, saldırının başlatıldığı bilgisayarın sahibi siz dahi olsanız, saldırının başlatıldığı kaynak makineye ilişkin sorumluluğun bulunmadığının ortaya konulması savunma için geçerli bir yoldur. Zombi makinelerin hüküm sürmekte olduğu bir çevrede, makine ile onun sahibinin hareketi arasındaki delile dayalı bağlantıyı ispatlamak oldukça güçtür[393].

bb. Caffrey Davası ve Truva Atı Savunması

Örneğin *Caffrey* davasında[394] sanık, Birleşik Devletler'de bulunan Houston Limanı'nın işleyişini sekteye uğratan DDoS saldırısının kendi bilgisi dışında bilgisayarında işleyen bir Truva atı virüsü tarafından başlatıldığı savunmasını başarıyla ileri sürmüştür. Bu husus, böyle bir kötücül yazılımın varlığını ortaya koyan bir delilin bulunmamasına rağmen yapılmıştır. Görüldüğü üzere sanık, suçun maddi unsurunun gerçekleştirilmesinden sorumlu tutulmamıştır; dolayısıyla sorumluluğunun da yönetilmesine gerek bulunmamaktadır[395]. Benzerleri ülkemizde de olan bilişim suçları alanındaki ispat zorluğunu ve yargılamayı yapan / karar veren makamın bu alanda bilgili olması gerektiğini ortaya koyan bu örnek davanın ayrıntılı incelenmesi gerektiğini düşünüyorum.

20 Eylül 2001 tarihinde Houston Limanı'nda bulunan bilişim sistemi bir DDoS atağı sonucunda çöker[396]. Saldırı, bilişim sistemini çökertir ve limana yanaşma, demirleme ve destek hizmeti veren şirketlerin ve römorkör pilotlarının gemilerin navigasyonuna yardım etmek için kullandıkları veri tabanının bulunduğu sisteme erişim isteklerini reddederek, dünyanın sekizinci en yoğun limanını devre dışı bırakır. Bir gözlemcinin belirttiği üzere, saldırı "yaşam ve uzuvlar üzerinde felaket düzeyinde yansımalara" neden olabilecek niteliktedir[397]; ancak neyse ki buna neden olmamıştır. Bu esnada ABD henüz 9/11 saldırısının sinir bozucu yılgınlığı içerisindedir[398].

Birleşik Devletler yetkilileri "elektronik izi takip ederek", Birleşik Krallık'ta yaşayan 18 yaşındaki Aaron Caffrey'in yaşadığı eve ulaşmışlardır. Daha açık bir ifadeyle, dijital soruşturmacılar Houston Limanı'na ait sistem kayıt dosyalarını

393 Walden, pn. 3.296.
394 Southwark Kraliyet Mahkemesi, 17 Ekim 2003.
395 Walden, pn. 3.296.
396 Steve Bird, "Lovelorn Hacker Sabotaged Network of U.S. Port", Times (UK), 7 Ekim 2003, s. 9.
397 Bird, s. 9.
398 Brenner, Cybercrime: Criminal, s. 104.

incelemişler ve saldırıyı başlatan bilgisayarın IP adresini ve saldırının hedefinde olan IP adresini tespit etmişlerdir. IP adresi numerik bir formül olup bilişim ağına bağlanan bir bilgisayarın ya da diğer bir bilişim aygıtının tanımlayıcısıdır ve her bir IP adresi benzersizdir. Her bir IP adresi bilgisayarın bağlı olduğu ağa ve bilgisayarın kendisine ait tanımlayıcı bilgileri içerir. Houston'lı soruşturmacılar, saldırının başlatıldığı ve saldırının gerçek hedefinin IP adresini bulduklarında, bu saldırıdan sorumlu olan kişinin de izini takip edebilmişlerdir[399].

Soruşturma, saldırganın hedefinin Houston Limanı olmayıp başka bir ülke olduğunu göstermiştir. Saldırgan gerçek hedefine saldırıda bulunmak için bir araç olarak Houston Limanı'ndaki ve diğer sistemleri ele geçirdiğinde limanın bilişim sistemi kapanmıştır. Soruşturmacılar, saldırıda kullanılan yazılımın sistem sunucusunda kullanılan yazılımın bir zayıflığından yararlanan ve bizzat kişinin kendisi tarafından özel olarak hazırlanan (coded by Aaron) bir yazılım olduğunu ortaya çıkarmışlardır[400]. Bunun üzerine soruşturmacılar, Aaron Caffrey'in ailesiyle birlikte yaşadığı Fairland Shaftesbury Dorset'teki evine kadar saldırının izini takip etmişlerdir[401].

İngiliz polisi Caffrey'in bilişim sistemine el koymuş ve kendisini Birleşik Krallık yasalarına göre suç oluşturan "bilgisayar materyallerinde yetkisiz değişiklikte bulunmak" suçlamasıyla yakalamış ve gözaltına almıştır[402]. Bilgisayar Suçları Bölümünden polisler Caffrey'in bilgisayarında adli bilişim incelemesi yaptıktan sonra Caffrey, Houston Limanı'nın bilişim sisteminin güvenliğini kırmak nedeniyle suçlanmıştır. *McKinnon* davasından farklı olarak bu davada ABD'li yetkililer, davayı İngiliz yetkililere bırakmak konusunda tartışma çıkarmışlardır[403].

Davanın yargılamasına Ekim 2003 tarihinde başlanmıştır. Suçlama, Caffrey'in Houston Limanının bilişim sistemlerini kapatmak kastıyla hareket etmesi nedeniyle yapılmamıştır.

Savcılığın teorisi, Houston saldırısının kasıtsız, ancak sonuçları önceden öngörülebilir bir "intikam" saldırısı olduğudur (TCK'nın 243/3 maddesinde düzenlenen neticesi sebebiyle ağırlaşan bilişim sistemine hukuka aykırı erişim sağlama suçu benzeri). Bir kişi, Caffrey'in Amerikalı kız arkadaşına hakaret etmiş, Caffrey de bu kişiden intikam almak için bu eylemi gerçekleştirmiştir.

---

399 Brenner, Cybercrime: Criminal, s. 104.

400 Andy McCue, "'Revenge' Hack Downed US Port Systems", ZDNet UK, 7 Ekim 2003, http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/; 25.12.2016.

401 Brenner, Cybercrime: Criminal, s. 104.

402 Alison Purdy, "Hacker Cleared of Causing Biggest US Systems Crash", Birmingham Post, 18 Ekim 2003, s. 5, https://www.thefreelibrary.com/Hacker+cleared+of+causing+biggest+US+systems+crash.-a0109001502; 25.12.2016.

403 Brenner, Cybercrime: Criminal, s. 104.

Savcılık, Caffrey'in çevrimiçi ilişki kurduğu Jessica'ya "deliler gibi aşık olduğunu"[404] ve "Bookie" isimli bir Güney Afrika İnternet Aktarımlı Söyleşi (IRC) yazılımı kullanıcısının IRC sohbet odasında anti-Amerikancı yorumlarda bulunmasından sonra saldırının gerçekleştirildiğini ifade etmiştir. Kraliyet soruşturmacıları yalnızca Bokkie'nin yorumlarını takip etmemişler, bunun yanı sıra "Aaron'dan" gelen ve "Bokkie'nin molaya çıkması gerektiğini, çünkü bu kişi Amerika'dan nefret ediyorsa, bunun Jessica'dan da nefret ettiği anlamına geldiğini" belirten yorumlarını da bulmuşlardır[405].

Deliller yalnızca Caffrey'in bilgisayarı ile Houston Limanı'nın bilgisayar sistemi arasındaki bağlantıyı göstermekle kalmayıp, aynı zamanda Bokkie anti-Amerikancı yorumlar yaptıktan sonra Caffrey'in Bokkie'nin IP adresini bulmak için araştırma yaptığını da göstermektedir[406]. Bokkie'nin IP adresini bulduğunda ise, hazırlamış olduğu DDoS saldırısı yazılımını çalıştırarak saldırısını gerçekleştirmiştir, bu sırada kazara Houston Limanı'nın bilgisayar sistemini de kapatmıştır[407].

Bu, Kraliyet soruşturmacılarının teorisiydi ve adli bilişim uzmanlarının bulduğu ve analiz ettiği dijital delillerle iyi şekilde de desteklenmişti. Caffrey'e karşı ileri sürülen deliller son derece kuvvetliydi ve avukatı, savcılığın ileri sürdüğü pek çok vakaya karşı çıkamamıştı. Bu nedenle savunma Caffrey'in bilgisayarından Houston Limanı'nın bilişim sistemlerine bir DDoS atağı gerçekleştirildiğini kabul etmişti. Ancak savunma, Caffrey'in bu eylemden sorumlu tutulamayacağını, zira kendisinin (en azından suçlamaya göre) asıl amacının Bokkie'ye karşı bir saldırıda bulunmak olduğunu belirtmiş ve bunun yerine farklı bir yaklaşım göstermiştir[408].

Savunmanın teorisi ise Caffrey'in bir saldırıda bulunmadığı, O'nun bilgisayarının bir saldırıya uğradığıdır. Caffrey'in avukatına göre, "birisi" Caffrey'in bilgisayarına bilgisi dışında bir Truva atı yazılımı yüklemiş ve Houston Limanı'nın sistemini kapatan saldırıyı gerçekleştirmek için bilgisayarını kullanmıştır[409]. Truva atı kötücül bir yazılım olup, kendini gizleyerek bir bilgisayara yüklenebilmekte ve Truva atını yükleyenin, yazılımın yüklendiği bilgisayarın kontrolünü ele geçirmesini sağlamaktadır[410].

---

404 John Chapman, "The Nerdy Brit Who Paralysed a U.S. City", Express (UK), 7 Ekim 2003, s. 24.

405 Brenner, Cybercrime: Criminal, s. 104, 105.

406 McCue, ZDNet UK.

407 Brenner, Cybercrime: Criminal, s. 105.

408 Brenner, Cybercrime: Criminal, s. 105.

409 Örneğin bkz: John Leyden, "Caffrey Acquittal a Setback for Cybercrime Prosecutions", Register, 17 Ekim 2003, http://www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback/, 15.12.2016.

410 Brenner, Cybercrime: Criminal, s. 105.

Caffrey, Türk bilişim korsanlarını kendisine komplo kurmakla ve düzenli olarak sohbet odalarını ve internet sitelerini ele geçirmekle suçlamıştır[411]. Bilgisayarının işletim sisteminin uzaktan erişime ve kontrole izin verdiğini, bu nedenle Truva atı yazılımlarına açık hale geldiğini belirtmiştir. Caffrey, soruşturmacıların kendisini saldırıdan sorumlu tutmak için dayandıkları kayıt dosyalarının, kendisine karşı kurulan komploda değiştirildiğini iddia etmiştir[412]. Caffrey'e göre, "birisi kayıt dosyalarını düzenlemiştir. Bunun böyle söyleniyor olması, bu kayıtların gerçekte böyle olduğu anlamına gelmez"[413]. Sonunda, soruşturmacılar tarafından Caffrey'in bilgisayarında bulunan ve "coded by Aaron" isimli DDoS yazılımı kendisine sorulduğunda Caffrey "Aaron'ın çok, çok yaygın bir isim" olduğunu söylemiştir[414].

Caffrey'in, Houston Limanı'nın sistemini kapatmak için birisi tarafından bir Truva atının manipüle edildiğine ilişkin savunmalarının aksini ispat etmek, Kraliyet soruşturmacılarına kalmıştır. Savcılık, yalnızca bir tek argümanla karşılık vermiştir: Adli bilişim uzmanları, Caffrey'in bilgisayarı üzerinde çok dikkatli inceleme yaptıkları ve bir Truva atı yazılımına ilişkin herhangi bir iz bulamadıkları yönünde tanıklık yapmışlardır[415]. Caffrey, uzman tanıklığına karşı yapmış olduğu savunmada, jüriye söz konusu uzmanların bilgisayarında bulunan her bir dosyayı incelemelerinin mümkün olmadığını söylemiştir. Ayrıca Truva atı yazılımının kendi kendini silebilen bir yazılım olabileceğini, dolayısıyla saldırıdan sonra bilgisayarından kendini silmiş olabileceğini ifade etmiştir[416].

Savcılık, Caffrey'in kendi kendini silen Truva atı yazılımı savunmasını, adli bilişim uzmanları kendisinin bilgisayarını incelediğinde yalnızca buna ilişkin hiçbir belirti bulamadıkları gerekçesiyle değil, bunun yanı sıra kayıt dosyalarının değiştirildiğini gösteren veya Truva atını silmek için herhangi bir "silme aracına" ilişkin bir delil bulamadıkları gerekçeleriyle çürütmeye çalışmışlardır[417]. Soruşturma uzmanları, Caffrey'in saldırının sorumlusu gösterdiği Truva atı yazılımı kendi kendini silmiş olsa bile, silme işleminin Caffrey'in bilgisayarında izler bırakmış olması gerektiğini, oysa kendilerinin böyle bir ize rastlamadıklarını ileri sürmüşlerdir[418].

411 McCue, ZDNet UK.
412 Munir Kotadia, "Accused Port Hacker Says Log Files Were 'Edited'", ZDNet.co.uk, 8 Ekim 2003, http://www.zone-h.org/news/id/3300?zh=1, 25.12.2016.
413 Walden, pn. 3.300.
414 McCue, ZDNet UK; Brenner, Cybercrime: Criminal, s. 105.
415 Purdy, s. 5.
416 Purdy, s. 5; Brenner, Cybercrime: Criminal, s. 106.
417 Neil Barrett, "Scary Whodunit Will Have Sequels" IT Week, 27 Ekim 2003.
418 Barrett, IT Week; Brenner, Cybercrime: Criminal, s. 106.

Dava, iki haftalık yargılamanın ardından jürinin kararına bırakılmıştır. Beş erkek ve altı kadından oluşan jüri Caffrey'in tüm suçlamalardan beraatine karar verene kadar aralarında üç saat boyunca tartışmışlardır[419]. Karar savcılığa iletildiğinde, polisler verilen karardan dolayı buz kesmişlerdir. Suçlama için tanıklık yapan bir uzman şunları ifade etmiştir: "Bir kişi bunu yaptı ve sonra da kaçtı gitti argümanına karşı çıkmak son derece güçtür. Biz eğer birileri bunu yaptıysa parmak izi bırakmış olmaları gerektiğini … ancak parmak izi olmadığını göstermek istedik"[420].

Caffery davası, savcılığın bilişim suçlarına ilişkin soruşturmalarda ve iddia faaliyetlerinde çeşitli delillendirme zorluklarıyla karşı karşıya olduğunu göstermiştir. Bu zorluklardan birisi sanığın suçlu olduğunun, makul şüphenin ötesinde kanıtlanmasıdır[421]. Diğer zorluklar ise kabul edilebilecek türde delilleri elde edebilme becerisiyle ilgilidir[422].

Caffery'in başarıyla kullandığı Truva atı savunması, eski bir savunma yöntemi olan SODDI'nin (Bir Başka Dost Yaptı / Some Other Dude Did It) güncellenmiş versiyonudur[423]. Bir hukuki makalede açıklandığı üzere bir savunma avukatı, müvekkilinin kendisine yüklenen suçun hareketini gerçekleştirmediği (hareket masumiyeti) ya da savcılığın müvekkilin suçluluğunu makul şüphenin ötesinde kanıtlayamadığı (ispatın başarısızlığı) gerekçeleriyle müvekkilin suçsuz olduğuna jüriyi ikna etmeye çalıştığında, jüriye alternatif bir teori vermek zorunda kalacaktır, bu diğer teori "diğer bir şüphelidir"[424]. Zira bir jüri kurulu tarafından sanığın beraatine karar vermek için savcılığın delillerin değerini ve eksikliğini ölçmektense, bir başka kişinin suçu işlendiğine ilişkin bir neden bulmanın daha kolay olduğu varsayılır[425].

SODDI savunması uzun süreden beri savunma avukatları tarafından jürinin daha kolay beraat kararı vermesi için kullanılan bir araçtır. Ancak bu, fiziki dünyadaki suçlar için genellikle başarılı olmasa da; istisnaları bulunmaktadır (örneğin, O. J. Simpson'ın yargılandığı cinayet davası gibi)[426].

---

419 Leyden, Caffrey Acquittal.

420 Leyden, Caffrey Acquittal; Brenner, Cybercrime: Criminal, s. 106.

421 Hem Birleşik Krallık hem de Birleşik Devletler sanığın cezalandırılmasını istemişlerdir, jüri ise savcılığın makul şüphenin ötesinde suçun tüm unsurlarını masının gerektiğini aramıştır. Örneğin bkz: Mark Murdo Urquhart v. Her Majesty's Advocate, [2009], HJJAC 18 (Birleşik Krallık hukuku), Harris v. United States, 536 U.S. 545 (2002) (Birleşik Devletler hukuku).

422 Brenner, Cybercrime: Criminal, s. 106.

423 Susan W. Brenner/Brian Carrier/Jef Henninger, "The Trojan Horse Defense in Cybercrime Cases", Santa Clara Computer & High Technology Law Journal, Volume 21, Issue 1, 2004, s. 9.

424 W. William Hodes, "Seeking the Truth versus Telling the Truth at the Boundaries of the Law: Misdirection, Lying, and 'Lying with an Explanation'", South Texas Law Review, Vol. 44, Winter 2002, s. 59, dn.18.

425 Brenner, Cybercrime: Criminal, s. 106.

426 Brenner, Cybercrime: Criminal, s. 107.

SODDI savunmasını fiziki dünyadaki bir suçlamada başarıyla sunmanın önündeki en önemli engel güvenilirliktir. Varsayalım ki Caffrey, Houston Limanı'nın ofis binasına zorla içeri girmekten suçlanmış olsun. Soruşturma görevlilerinin, bir ofise doğru yönelmiş Caffrey'in çamurlu ayak izlerini bulduklarını ve bunu takip ederek girdikleri ofiste bir mobilyanın üzerinde parmak izini de bulup Caffrey'i bina içinde hırsızlık yapmaktan suçladıklarını düşünelim. Yargılama esnasında soruşturma görevlileri buldukları deliller konusunda tanıklık yaparlar ve parmak izi uzmanları ofiste bulunan parmak izlerinin neden Caffrey'e ait olduğunu ayrıntılı bir şekilde açıklarlar. Caffrey'e karşı yöneltilecek davayı daha da kuvvetlendirmek için soruşturmacıların ofiste Caffrey'in DNA'sını da bulduklarını düşünelim[427].

Bu varsayımsal durumda Caffrey, avukatına suçu işlemediğini, ancak bir "alibi" (ben orada değildim) durumu olmadığını da söyler; bu nedenle savunma için tek seçenek SODDI savunması yapmaktır. Caffrey'in avukatları gerçek davada olduğu gibi jüriye bazı argümanları ifade ederler: Caffrey'in parmak izleri, kendisine komplo kurmak isteyen bazı kişiler tarafından bırakılmıştır. Ofiste bulunan DNA için de aynı şeyler söz konusudur; hem parmak izleri hem de DNA kendisine karşı komplo kurmak için değiştirilmiştir. Savcı, Caffrey'inkinden ayırt edilemeyecek şekilde parmak izi bırakmanın çok zor olduğunu belirtir ve jüriye ne parmak izlerinin ne de DNA delilinin değiştirilebileceğini hatırlatır. Herhangi bir delilin değiştirilmesi son derece güçtür, çünkü bunlar somut, fiziksel delillerdir. Caffrey davasının bu versiyonunda, jüri şüphesiz SODDI savunmasını reddedecek ve kendisinin suçlu olduğuna karar verecektir. Bu savunma, basitçe sağduyulu bir bakış açısıyla güvenilir değildir. Jüri ayak izlerini, parmak izlerini, DNA'yı ve bunların nasıl Caffrey'i işaret ettiğini açıklayan uzmanları güvenilir bulacak ve durumu anlayacaktır[428].

Ancak, gerçek Caffrey davası sabit disklerin, yazılımların ve siber uzayın sanal dünyasında gerçekleşmiştir. Bilgisayar kullanan herhangi bir kişi, Caffrey'in bina içinde hırsızlıktan suçlu bulunduğu farazi davasındaki fiziksel delillerde olduğu gibi dijital verilerin (dolayısıyla delillerin) somut olmadığını, değişmez olmadığını anlamalıdır. Haberleri takip eden herhangi bir kişi bilişim korsanlarının bulunduğunu ve bu korsanların bilişim sistemleriyle etkileşimde bulunabileceklerini bilirler. Sonuç olarak Caffery'in savunmasının bu parçası güvenilirdir; çünkü bu, jüriye farazi soygun davasında olanın aksine, belirli bir "diğer dost" argümanı verir[429].

[427] Brenner, Cybercrime: Criminal, s. 107.
[428] Brenner, Cybercrime: Criminal, s. 107.
[429] Brenner, Cybercrime: Criminal, s. 107.

Bu davada "diğer dost", belirli bir kişi değildir. Bunun yerine bir grup insan söz konusudur: Web sitelerine ve bilgisayarlara karşı korsanlık yapan Türk bilişim korsanları. Bu, jüriye Caffrey'in SODDI savunması için belirlenebilir bir kişiye olayı dayandırma olanağı vermiştir. Jürinin tümden ya da göreceli olarak dijital delilleri yok sayması ve adli bilişimin karışıklığının eklediği kayıp element, Caffrey'in savunmasına inanmalarını ve uzmanların tanıklığını yok saymalarını olanaklı hale getirmiştir. Farazi soygun davasında, jürinin ayak izlerini anlamaya ilişkin sağduyusu ve DNA ile parmak izlerinin değerine güvenleri vardı; bu ise SODDI savunmasını reddetmelerini onlar için kolaylaştırmıştır. Şimdi ise jürinin sağduyusu onlara dijital verilerin her yöne çekilebilir ve yetersiz olduğunu söylemektedir. Jürinin deneyimine göre, veriler herhangi bir iz bırakmaksızın değiştirilebilir veya silinebilir; dolayısıyla Caffery'in SODDI savunması onlara "makul bir alternatif teori" olarak görünmüştür. Sonuçta davayı Caffrey kazanmıştır[430]. Diğer bilişim suçluları da bu savunma yolunu takip etmişledir[431].

Sonuçta şu hususu not etmeliyiz: Truva atı savunması mükemmel bir biçimde geçerli olabilmektedir. Truva atını ya da benzer bir yazılımı kullanarak bir kişinin bilgisayarına çocuk pornosu materyalleri ya da bir başka suçun delillerinin yerleştirilmesi ve komplo kurulması mümkündür[432]. Aynı şekilde kişinin hiç dikkat etmeyeceği şekilde ana belleğin herhangi bir yerine materyal indirilmesi mümkündür. Düşünün: Bilgisayarınızda yer alan her dosyayı biliyor musunuz? Emekli bir federal savcının belirttiği üzere, Truva atı savunması hakkında "ürkütücü olan şey" bunun "gerçek olabileceğidir"[433].

c) CMA madde 3'te Düzenlenen Kasten veya Olası Kastla / Bilinçli Taksirle (Recklessness) Zarar Verici Yetkisiz Hareketlerde Bulunmak

İngiliz Hükümeti Temmuz 2003'te, 1990 tarihli Yasayı kısmen, bazı DoS saldırılarıyla mücadele ortaya çıkan boşluğu doldurmak ve konuyla ilgili uluslararası düzenlemelerle uyum sağlamak amacıyla gözden geçirmek niyetinde olduğunu duyurmuştur[434]. CMA'da değişiklikler yapan hükümler, 2006 tarihli Polis ve Adalet Yasası ile getirilmiştir[435]. Var olan hükümlere

---

430 Brenner, Cybercrime: Criminal, s. 107, 108.

431 Brenner/Carrier/Henniger, s. 7-9.

432 Bkz: United States v. Miller, 527 F.3d 54 (U.S. Court of Appeals for the Third Circuit 2008) (iddia ve savunma uzmanları bir Truva atı yazılımıyla çocuk pornografisi ya da diğer materyallerin gizlice bir bilgisayara indirilebileceği konusunda hemfikirdirler).

433 John Schwartz, "Acquitted Man Says Virus Put Pornography on Computer", New York Times, 11 Ağustos 2003 (Adalet Bakanlığı Bilgisayar Suçları Bölümünün başkanına atıf yapmaktadır); Brenner, Cybercrime: Criminal, s. 108.

434 İçişleri Bakanı Parlemanto Müsteşarı ve milletvekili olan Caroline Flint'in 14 Temmuz 2003 tarihinde EURIM toplantısında yapmış olduğu konuşma.

435 Police and Justice Act, 2006 m. 36.

tamamlayıcı bir suç getirmektense, CMA madde 3'te yer alan suç tamamen değiştirilmiştir.

aa. CMA madde 3'te Yer Alan Suçun Geçmişi[436]

1971 tarihli Cezai Zarar Yasası'nda (Criminal Damage Act 1971) bilgisayara ya da bilgisayar yazılımına zarar verme veya yok etme suç olarak düzenlenmiştir; örneğin, bir çekiç alarak bilgisayarı kırmak suretiyle zarar verme bir suçtur. Somut bir malvarlığına fiziksel olarak zarar verildiğinde, 1971 Yasasının uygulanmasında bir sorun yoktur. Söz konusu zarar somut bir malvarlığına verilmiş olsa bile, bu zararın duyuların algılayamayacağı şekilde verilmesi mümkün olamaz mı? Fail, bilgisayar yazılımlarının yapması için dizayn edildiğinin dışında işlevler yapması için bilgisayarı işlevsiz hale getirdiğinde ya da bir takım işlevlerini sınırlamak için yazılımlara müdahale ettiğinde bu soruya "mümkün olabilir" yanıtı verilebilir. İşte bu durumda duyular tarafından algılanabilen fiziksel bir zarar olmaksızın zarara neden olunabilir[437].

Cox v. Riley davasında[438], failin programlanan tasarıma göre tahtaları kesen bir testerenin plastik devre kartını silerek zarar vermekten suçlu olduğuna karar verilmiştir. Failin müdafii, Cezai Zarar Yasası gereğince söz konusu programın "fiziksel yapıya sahip olan bir malvarlığı" olmadığını ileri sürmüştür. Bu açıdan müdafiin haklı olduğu hususunda şüphe yoktur; ancak mahkemenin bakış açısına göre müdafi, failin programa zarar vermekten değil plastik devre kartına zarar vermekten suçlandığı olgusunu dikkate almakta hataya düşmüştür. *Whitely* davasında[439] ise fail, olması gerektiği biçimde bilgisayar diskine zarar vermekten mahkûm edilmiştir, zira fail bir akademik bilgisayar sistemine yetkisiz erişim sağlamayı başarmış ve manyetik parçalarını değiştirmek suretiyle dosyaların silinmesine ve yeni dosyalar eklenmesine yol açmıştır. Bu kişinin müdafiinin "yalnızca diskte yer alan fiziksel olmayan bilgilerin zarar gördüğüne" ilişkin savunması reddedilmiştir; çünkü diskin kullanışlılığının zarar görmesi nedeniyle disk de zarar görmüştür[440].

Bu kararlar, bilgisayarın kötüye kullanılmasını belirtiyorlarmış gibi görünebilirler; çünkü bunların zarar verme açısından görünen potansiyelleri ve Cezai Zarar Yasasının zorlayıcı anlamından[441] da bu anlaşılabilir; dolayısıyla

---

436 Genel olarak konuyla ilgili eski suçlarla ilgili olarak bkz: Yaman Akdeniz, "Section 3 of the Computer Misuse Act 1990 – An Antidote for Computer Viruses", Web Journal of Current Legal Issues, 1996.

437 Ormerod, Smith & Hogan's Criminal Law, s. 1053.

438 (1986) 83 Cr App R 54, DC.

439 [1991] Crim LR 436, CA.

440 Ormerod, Smith & Hogan's Criminal Law, s. 1053, 1054.

441 Wasik, Crime and the Computer, s. 137 – 145.

her iki karar da bu yasa açısından savunulabilir. *Cox v. Riley* davasındaki plastik devre kartının her ne kadar kullanışsız hale getirildiği ve kendine özgü işlevini yerine getirmek için yeniden programlanabileceği kabul edilmese de, aslında disk fiziksel olarak zarar görmemiştir. Disk yalnızca programlandığı işlerden birini yapamaz hale gelmiştir ve bu dava *Fisher* davasından[442] farklı görülmemelidir. *Whitely* davasına benzer olarak bilgisayarın kendisi zarar görmemiştir, ancak kontrol mekanizması kurcalandığı için işlev göremez olarak kabul edilmiştir, yani programlar diskin üzerindedir. Ancak diskin tamir edilebilir olması, geçici bozulmadan kaynaklanan yetersizlikle ilgili değildir[443].

Hukuk Komisyonu, bir şekilde, bilgisayarların kötüye kullanılmasıyla daha doğrudan mücadele edilmesinin gerektiği görüşüne sahip olmuştur. Cezai Zarar Yasası'na verilere ve yazılımlara müdahale etmeye ilişkin bir suç eklenmesi, sorunun çözümüne ilişkin bir olasılık olarak görülmüştür; ancak Komisyon, iki nedenle yeni bir suç oluşturulması gerektiğine karar vermiştir. Bunlardan ilki, "zarar konusunu yazılımı ya da veriyi fiziki olmayan malvarlığına uygulamanın ortaya çıkardığı teorik zorlukların" ortaya çıkardığı belirsizliğin hukuk açısından kabul edilmesindeki güçlüktür. Diğeri ise, ceza hukuku açısından önemli olan zarara, olası kast/bilinçli taksir (recklesness)[444] ile yol açılabilir; Hukuk Komisyonu, yeni oluşturulacak suçun olası kast/bilinçli taksirle bilgisayardaki materyalleri başkalaştıranların eylemlerini kapsamasını düşünememiştir[445]. Buna ek olarak, görüldüğü üzere, Komisyon 1990 tarihli CMA'da yer alan başkalaştırma suçu ile Cezai Zarar Yasası'nda yer alan zarar verme suçu arasındaki ilişkiyi de netleştirmeye çalışmıştır[446].

---

442 (1865) LR 1CCR 7, bu dava için bkz: Ormerod, Smith & Hogan's Criminal Law, s. 1014, dn. 17.

443 Ormerod, Smith & Hogan's Criminal Law, s. 1054.

444 Anglo Amerikan hukuk sisteminde suç temel olarak iki unsurdan oluşur "maddi unsur / actus reus" ve "manevi unsur / mens rea". Bunlardan manevi unsur ise "kast / intention", "taksir / negligence", "olası kast – bilinçli taksir / recklessness" ayrımından oluşur. Bunlardan sonuncusu olan "recklessness" kavramında esas olan failin yapacağı hareketin olası neticeleri öngörmesi ancak buna rağmen riskin gerçekleşmeyeceğine güvenip ya da bu riski üstlenip hareketini gerçekleştirmesidir. İşte bu öngörme ve neticenin gerçekleşmeyeceğine güvenme ya da üstlenme, bizim ülkemizde yürürlükte olan TCK'nın 21 ve 22. maddeleri ile öğretideki baskın görüşte "olası kast ve bilinçli taksir" olarak kabul edilir. Bu nedenle ben de kelimenin kavramsal karşılığını yazmayı tercih ettim.
Bu kavram hakkında kısa ancak yeterli açıklama için bkz: Joshua Dressler, Understanding Criminal Law, Sixth Edition, San Francisco, LexisNexis, 2012, s. 135**;** Wayne R. LaFave, Criminal Law, Fourth Edition, St. Paul, Thomson & West, 2003, 269, 270. Konu hakkında daha ayrıntılı açıklama için bkz: Andrew Simester/G. Robert Sullivan, Criminal Law: Theory and Doctrine, Second Edition, Portland, Hart Publishing, 2004, s.139-147.

445 Yeni yürürlüğe giren ve hazırda yürürlükte olan 3. madde ise olası kast/bilinçli taksirle işlenen eylemleri de suç olarak tanımlamaktadır.

446 Ormerod, Smith & Hogan's Criminal Law, s. 1054.

CMA madde 3'te yer alan suç, yasada sonradan yapılan değişiklikten önceki halinde dar şekilde düzenlenmiş ve bilgisayarların içinde yer alan verilerin başkalaştırılmasıyla sınırlandırılmıştı. Buna rağmen suçun bu hali mahkemeler tarafından oldukça geniş yorumlanmıştır. Örneğin, *Zevez* davasında[447]; bir kişiden gelen (aslında herhangi bir kişiden gelen) bir bilgi (bir e-mail) eğer bir bilgisayarın bir bilgiyi (bir e-maili) kaydetmesine neden olmuşsa; bu, söz konusu bilginin güvenirliğini açıkça etkiler. Bu, söz konusu suç tipinin önemli ölçüde genişletildiğini göstermektedir. E-mail, kendisi hakkında yalan söylemektedir, ancak bilgisayardaki diğer verilerin güvenilirliğini etkilememektedir. Daha sonrasında mahkemeler, DoS saldırıları olduğunda, söz konusu suçun kapsamını daha da genişletmiştir. *DDP v. Lennon* davasında[448], fail bir "mail (posta) bombardımanı" yazılımı kullanmak suretiyle eski işverenine beş milyon adet elektronik posta göndermiştir. Bölge Mahkemesi, bölge yargıcı ile aynı görüşü paylaşmamış ve failin veri eklemek suretiyle "yetkisiz bir başkalaştırmaya" neden olduğuna karar vermiştir. E-mail alabilen bir bilgisayarın sahibinin kendisine gönderilen elektronik postaları almaya normalde rıza gösterdiği varsayılır. Ancak bu zımni rıza sınırsız değildir, bu rıza kişiyle iletişim kurmak amacıyla olmayıp kişinin bilgisayar sistemini sekteye uğratmak amacıyla gönderilen elektronik postaları kapsamaz. Mahkeme, "eğer fail eski işverenine başvursaydı, eski işverenin kendisine beş milyon elektronik posta gönderilmesine rızasının olup olmadığının" test edilmesi gerektiği görüşünü ileri sürmüştür. Aşağıda incelediğimiz CMA'nın yeni 3. maddesi, bu tür DoS ya da DDoS saldırılarına uygulanabilecek şekilde oluşturulmuş[449] ve *Lennon* davasında baş gösteren bazı şüphelerin ortadan kalkmasını sağlamıştır[450].

bb. CMA madde 3'te Düzenlenen Suçun Değişiklik Sonrası (Hâlihazırdaki) Hali

Bu suçun oluşması için bir bilgisayarla ilgili yetkisiz bir hareket olmalıdır. Yetkisizliğin genişletilmiş anlamı, yasanın 17(8) maddesinde tanımlanır. Bilgisayara, programa, veriye ya da benzerlerine zarar verilmesi gerçekte gerekmez. Söz konusu zararının gerçekleşmesine kast edilerek ya da olası kast/bilinçli taksirle yetkisiz hareketin gerçekleştirilmesiyle suç oluşur[451].

---

447 [2002] Crim LR 648.

448 [2006] EWHC 1201 (Admin). Bu dava hakkındaki yorumlar için bkz: Stefan Fafinski, "Divisional Court: Computer Misuse: Denial-of-Service Attacks" Journal of Criminal Law, Vol. 70, Issue 6, 2006, s. 474-478.

449 Yasaya yapılan bu ek, AB'nin Bilgi Sistemlerine Karşı Yapılan Saldırılara İlişkin Çerçeve Kararının 3. maddesiyle İngiliz hukukunu uyumlu hale getirmiştir.

450 Ormerod, Smith & Hogan's Criminal Law, s. 1054, 1055.

451 Ormerod, Smith & Hogan's Criminal Law, s. 1055.

Esasen madde 3'te, madde 3(2)'de tanımlanan herhangi bir hareket ya da hareket serileri gerçekleştirilmek suretiyle bilgisayar sistemine sabotaj düzenlemek ya da zarar vermek düzenlenir. Bu hususta en açık örnekleri, bilişim sistemlerine virüs[452], Truva atı ya da kurtçukların gönderilmesi veya web sitelerinin çökertilmesi oluşturur[453]. Hareketin diğer kişilerin sisteme erişimi engellemesi ya da aksatması, suçun oluşumu için yeterlidir; örneğin, DoS ya da posta (mail) bombardımanı saldırısı ile sunucunun kapasitesinin aşılması halinde suç gerçekleşmiş olur. Bunun dışında verinin silinmesi ya da herhangi bir şeyin değiştirilmesi gerekmez, dolayısıyla bu açıdan suç tipinin özgün haline göre kapsamı oldukça genişlemiştir. Bozma / zarar verme kavramının bazı olaylarda ispat edilmesi oldukça güçtür, örneğin programın bozulduğunun kabul edilmesi için failin programın bozulmadan önceki haline göre ne kadar yavaşlatmayı kast etmesi gerekir? Bu açıdan yetkisiz kullanım yeterli olabilir; örneğin fail kasten ya da olası kast / bilinçli taksirle (recklessness) verinin güvenilirliğine zarar vermesi halinde bu durum söz konusudur. Bir bilgisayarın, mağdurun banka hesabını borçlandırarak failin hesabına para yatırmasına neden olunması halinde suç oluşur, çünkü artık mağdurun banka hesabıyla ilgili veriler güvenilir değildir[454]. Ayrıca kasten ya da olası kast / bilinçli taksirle gerçekleştirilen bozmanın geçici olması, suçun oluşması için yeterlidir. Tekrar edelim ki bu değişiklik suçun kapsamını genişletmiştir[455].

Suçun gerçekleşmesi şunların varlığına bağlıdır:

a) Fail, kasten madde 3(2)'de belirtilen neticelerden birinin (bozulma vb.) gerçekleşmesine yetkisiz hareketle neden olmalıdır.

b) Fail, bozulmaya neden olan kasten ya da olası kast /bilinçli taksirle gerçekleştirdiği hareketinin yetkisiz olduğunu bilmelidir. Bilme unsuru, bozma kastıyla gerçekleştirdiği hareketinin yetkisizliğine ilişkin olmalıdır. Bozulmanın yetkisiz gerçekleştirildiğinin fail tarafından bilindiğinin ispat edilmesi gerekmez (3. maddenin eski halinde ise, başkalaştırmanın yetkisiz olduğunun bilinmesi gerekmekteydi).

Kasıt, olağan anlamında kullanılmıştır. Olası kast / bilinçli taksir (recklessness) ise *G* davasında[456] belirtildiği üzere "öznel" anlamında anlaşılmalıdır[457]. Suçun

---

[452] Örneğin bkz: Vallor [2004] 1 Cr App R (S) 54, olayın gerçekleştiği tarihte dünyadaki üçüncü en ölümcül virüsü dağıtmakla ilgili bir davadır.

[453] Örneğin bkz: Lindesay [2002] 1 Cr App R (S) 370, işten atıldığı için üzgün olan çalışanın eski çalıştığı şirketin web sitesini çökertmesiyle ilgili bir davadır.

[454] Thompson [1984] 3 All ER 56, [1984] 1 WLR 962, CA.

[455] Bkz: MacEwan, s. 955-967; Stephan Fafinski, "Computer Misuse: The Implications of the Police and Justice Act 2006", Journal of Criminal Law, Vol. 72, Issue 1, 2006, s. 53-66.

[456] [2004] AC 1034.

[457] Olası kast / bilinçli taksirin karşılığı olan "recklessness" kavramının "öznel" (sübjektif) yorumunun irdelendiği ve kabul edildiği R v. G davası ve buna ilişkin açıklamalar için bkz:

olası kast / bilinçli taksirle (recklessness) işlenebilmesi, suçun kapsamını önemli ölçüde genişleten 2006 tarihli değişikliğin öne çıkan yanlarından biridir. Suçun ilk halinde, olası kast / bilinçli taksirin varlığı suçun oluşması için yeterli değildi, çünkü Hukuk Komisyonu kişilerin yanlışlıkla bir bilgisayarın içeriğini başkalaştırabileceği kaygısıyla sınırlı bir manevi unsur düzenlemesinin gerekli olduğunu açıklamıştı[458].

Failin kastının ya da olası kast / bilinçli taksirinin, belli bir bilgisayarın ya da yazılımın doğrudan yasa tarafından yasaklanmış bozma neticesine yönelik olması gerekmez. Sorun şudur ki, IT güvenliği danışmanlarının hukuka uygun aktiviteleri de bu düzenleme ile suç haline getirilmiştir[459].

Bugüne kadar, DoS saldırıları öncelikle ve sıklıkla içeriden olanlar tarafından gerçekleştirilen yetkisiz erişim eylemlerine karşıt olarak dışarıdan olanların saldırıları açısından tartışılmıştır. Ancak farklı biçimde ve elverişli saldırıların gerçekleşmesi de mümkündür. Örneğin, 2006 yılında İkinci Yaşam (Second Life) adlı çevrimiçi oyun çevresinde yer alan bir grup kullanıcının "sanal dünyanın" kırılmasına neden olan, tekrar eden şekilde DoS saldırıları gerçekleştirdiklerine ilişkin bilgilerin FBI'ın eline geçtiği rapor edilmiştir[460].

cc. CMA madde 3A'da Düzenlenen, Madde 1 ve Madde 3'te Yer Alan Suçların İşlenmesinde Kullanılan Araçların Sağlanması veya Elde Edilmesi Suçu

2006 tarihli Polis ve Adalet Yasası'nın (The Police and Justice Act 2006) 37. maddesi ile üç yeni suç tipi CMA'ya eklenmiştir. Bu suçlar için öngörülen ceza; azami iki yıl hapis cezası ya da para cezasıdır, bazı durumlarda ise her iki ceza birlikte uygulanabilir.

Madde 3(A)1'e göre, eğer bir kişi "CMA madde 1 veya 3'te tanımlanan bir suçu işlemek ya da işlenmesine yardımcı olmak kastıyla herhangi bir aracı yapar, uyarlar, sağlar ya da sağlamayı teklif ederse" bu hüküm uyarınca suç işlemiş olur. Bu suç tipi, 2006 tarihli Dolandırıcılık Yasası'nın (Fraud Act 2006) bilişim suçlarına son derece benzer bir yansımasını oluşturur. Normal şartlarda suçun oluşması için gerekli olan manevi unsur kasttır[461].

Ormerod, Smith & Hogan's Criminal Law, s. 123-125.

458 Ormerod, Smith & Hogan's Criminal Law, s. 1055.

459 Ormerod, Smith & Hogan's Criminal Law, s. 1056.

460 Aleks Krotoski, "Population Explosion Puts Our Virtual Worlds at Risk", Guardian, 12 Ocak 2006, https://www.theguardian.com/technology/2006/jan/12/games. guardianweeklytechnology section, 23.9.2016.

461 Ormerod, Smith & Hogan's Criminal Law, s. 1056.

Madde 3(A)2'ye göre, CMA madde 1 veya 3'te tanımlanan bir suçu işlemek ya da işlenmesine yardımcı olmak olasılığına inanılarak herhangi bir aracın sağlanması ya da sağlanmasının teklif edilmesi suç olarak düzenlenmiştir. "İnanmak" kavramı, ceza hukukunda olduğu anlamıyla anlaşılmalıdır, bu bağlamda yalnızca şüphe etmekten daha fazlasıdır. Ancak bilmek kadar kesin değildir. Aracın CMA madde 1 veya 3'te tanımlanan bir suçu işlemek "olasılığıyla" kullanılıp kullanılmadığı sorusu, uygulamada çeşitli zorlukların çıkmasına yol açmaktadır. İçişleri Bakanlığı'nın Açıklayıcı Notuna göre, eğer fail araçların sayısının çokluğuna bağlı olarak suçlanırsa, savcılık davasını "söz konusu araçların belli bir tanesi veya birkaçını dikkate alarak" ispatlamalıdır. Buna göre "failin, araçların belli bir kısmının CMA madde 1 veya 3'te tanımlanan bir suçu işlemek olasılığıyla kullanacağına inanmasını ispatlamak yeterli değildir"[462]. Yani savcılık hangi araç ya da araçların kullanılacağının olasılık dahilinde görüldüğünü tespit etmeli ve bunu ispat etmelidir.

Madde 3(A)3 ise, bir kişinin CMA madde 1 veya 3'te tanımlanan bir suçun işlenmesinde kullanılması ya da suçun işlenmesine yardımda bulunmayı sağlamak amacıyla bir aracı bulundurmasını suç olarak düzenler. Bu suçun manevi unsurunun, Temyiz Mahkemesinin bir başka konu bağlamında belirttiği üzere[463], sınırlayıcı bir biçimde kastın yanında "amacı" da gerektirdiği ileri sürülebilir. Göreceli olarak bu, suçun alışılmamış bir biçimidir, zira "aradaki kişinin" (tedarikçinin) hareketlerini başlı başına suç haline getirir. Failin yalnızca aracı elde etmesi ya da bulundurması suçun oluşumu için yeterli değildir. Suçun gerçekleşmesi, sonraki bir amacın varlığını da gerektirir. Bu suç tipi, madde 3(A)1'de yer alan suçu, failin aracı sağlaması ya da sağlamayı teklif etmesinden önceki aşamaya taşıdığı için, daha ileri bir aşamaya taşır[464]. Aslında bu, hukuk sistemimizin bakış açısıyla hazırlık hareketlerinin cezalandırılması anlamına gelip, 6698 sayılı Yasa ile TCK'ya eklenen 245/A maddesine büyük bir benzerlik gösterir. Nitekim nasıl ki İngiliz hukukunda tüm bilişim suçları açısından söz konusu hazırlık hareketleri cezalandırılabilir hale getirilmişse, ülkemiz açısından da durum aynı şekildedir.

Madde 3(A)4 gereğince her üç suç tipi açısından da, "araç", herhangi bir yazılımı ya da elektronik formda bulunan veriyi ifade eder. Bu suçlardan her biri için manevi unsurun varlığı son derece önemli ve zorunludur. Zira bilişim suçlarının işlenmesinde araçların kullanımı, bir tornavidadan karmaşık bir yazılıma ya da bir bilgisayar şifresine kadar inanılmaz geniş bir kapsamdadır[465]. Dolayısıyla kullanılan aracın ne olduğunun belirlenmesi failin bunu kullanmaktaki kastıyla belirlenebilir.

---

462 Ormerod, Smith & Hogan's Criminal Law, s. 1056.
463 Bkz: Dooley [2005] EWCA Crim 3093.
464 Ormerod, Smith & Hogan's Criminal Law, s. 1056.
465 Ormerod, Smith & Hogan's Criminal Law, s. 1056.

Bu yeni suçların düzenlenmesinin amacı, Hükümet tarafından, bilişim sistemlerinin güvenliğinin kırılmasına yönelik yapılan saldırılar (hacking) ve bu saldırılarda kullanılan araçların (hacking tools) pazarlandığı yerlerle mücadele etmek için gerekli olduğu şeklinde açıklanmıştır. Ancak, bilgisayar güvenlik sistemleriyle ilgili hukuka uygun araştırmaların da suç oluşturma ihtimali, çeşitli sorunların ortaya çıkmasına yol açmıştır[466]. Bu hükümler de Avrupa Konseyine ve Siber Suçlar Sözleşmesi uyarınca yerine getirilmesi gereken yükümlülükleri[467] karşılamaktadır[468].

dd. CMA madde 3ZA'da Düzenlenen Ciddi Tehlike Yaratan ya da Buna Neden Olan Yetkisiz Hareketler Suçu

Daha önce belirtildiği üzere, Nisan 2015'te, CMA'da yeni bir suç düzenlenmiştir: *Ciddi tehlike riski yaratan ya da buna neden olan yetkisiz hareketler*[469]. Bu suç maddi zararlara yol açabilecek[470], ulaşım ya da finans sistemleri gibi kritik ulusal altyapıları hedef alan en ciddi siber ataklar[471] için düzenlenmiştir. Saldırganlar, davranışlarının yetkisiz olduğunu bilmeli ve ayrıca saldırganların böyle bir zararı vermek konusunda kastı ya da böyle bir zararın meydana gelmesinde taksiri olmalıdır[472]. İnsanların refahına ya da ulusal güvenliğe ciddi zarar verilmesi halinde, cezanın azami haddi müebbet hapis cezası, zararın ekonomiye ya da çevreye verilmesi halinde ise on dört yıla kadar hapis cezasıdır[473]. Bu durum, Birleşik Krallık'ta bilişim sistemlerinin bütünlüğüne karşı işlenen bir suç için verilebilecek hapis cezasının miktarının oldukça anlamlı bir şekilde artırıldığını ve başarılı bir şekilde hedefteki sisteme zarar verilmesi halinde ortaya çıkan zararın hükümetin de dikkatini çektiğini göstermektedir[474].

---

466 Bkz: House of Lords Science and Technology Report, Personal Internet Security, 2007. Ancak Hükümetin bu konuya ilişkin yanıtları ağır bir biçimde eleştirilmiştir, bkz: Tim Wright/ Dominic Hodgkinson, "Government Response to House of Lords Science and Technology Committee Report on Personal Internet Security", Computer and Telecommunications Law Review, Vol. 14, 2008, s. 65.

467 Avrupa Siber Suçlar Sözleşmesi'nin 6(1)(a) maddesi.

468 Ormerod, Smith & Hogan's Criminal Law, s. 1056.

469 CMA m. 3ZA

470 CMA m. 3ZA(2).

471 İçişleri Bakanlığı, 2015 tarihli Ağır Suçlar Yasası (Serious Crime Act 2015), Sirküler 008/2015, 25 Mart 2015, pn. 8, bkz: http://www.legislation.gov.uk/ukpga/2015/9/contents/enacted, 24.9.2016.

472 Duruma göre CMA m. 3ZA(1)(b) ve (d).

473 Duruma göre CMA m. 3ZA(7) ve (6).

474 Walden, pn. 3.304.

5. Yetkisiz Araya Girme

a) Genel Çerçeve

Bilişim sisteminin bütünlüğe ilişkin suçlar, bir saldırgan tarafından erişilen veya değiştirilen sistemde bulunan "durağan" verilere yöneliktir. Buna karşın ceza hukuku, ağlar arasında aktarım halinde bulunan ve üçüncü kişiler tarafından araya girilerek etkide bulunulan verileri de korumalıdır. Aktarım halindeki verilere karşı yapılan saldırılarla, sistem içinde bulunan verilere karşı yapılan saldırılarda güdülen amaç aynı olabilir; bunlar, örneğin gizliliğe ve bütünlüğe zarar verilmesi veya verilere erişimin engellenmesi olabilir; ancak birincil zarar geleneksel olarak doğasında bulunan gizliliğin ve mahremiyetin ihlal edilmesidir. Bu eğilim, ilgili yasal düzenlerde de yansımasını göstermektedir[475], örneğin:

"Bu hüküm veri iletişiminin mahremiyetini korumayı amaçlamaktadır"[476].

"İletişime yetkisiz erişimi engellemek için alınması gereken önlemler iletişimin mahremiyetinin korunması amacıyladır…"[477]

Mahremiyet konusuna odaklanılması; hukuka aykırı araya girmenin bilişim sisteminin bütünlüğüne karşı bir suç olarak kabul edilmesindense, genellikle öncelikli olarak devlet tarafından yapılacak araya girmelerden korunması gereken bireyin, özel yaşamın bir parçası olarak görüldüğü anlamına gelir[478]. Buna rağmen araya girme suçları bir kişinin iletişiminin içeriğine erişim sağlanmasına ilişkindir, bunlar içerikle ilgili bir suç olarak sınıflandırılmaz; çünkü hukuk düzeni, konuşmanın gizliliğine yönelik hakkı, bunların özel ya da kamusal, hukuka uygun ya da hukuka aykırı olup olmadığına bakmaksızın korumaktadır[479].

Diğer bilişim sisteminin bütünlüğüne yönelik suçlarda, örneğin bilişim korsanlığında olduğu gibi; araya girme, suçu oluşturan hareketin gerçekleştirilmesini sağlamakta ya da suç soruşturmasını yapan kolluk güçlerinin soruşturmaları esnasında kullandıkları bir araç olabilmektedir. Bununla birlikte günümüz hukuk politikası yapıcıları bunlardan ikincisi ile daha çok ilgilenmektedirler[480].

---

475 Walden, pn. 3.309.

476 Avrupa Siber Suçlar Sözleşmesi'nin Açıklayıcı Raporu, pn. 51.

477 Avrupa Parlamentosu'nun 02/58/EC nolu Direktifi ve Avrupa Konseyi kişisel verilerin işlenmesi ve elektronik iletişim sektöründe mahremiyetin korunması ile ilgilenmektedir. OJ L 201/37, 31 Temmuz 2002, 21 nolu beyanat.

478 Örneğin AİHS m.8/1 ve Avrupa Birliği Temel Haklar Şartı m. 7.

479 Walden, pn. 3.309.

480 Walden, pn. 3.310.

b) 2000 tarihli Soruşturmacıların Yetkileri Yasası[481]

Birleşik Krallık'ta Soruşturmacıların Yetkileri Yasası'nın (Regulation of Investigatory Powers Act 2000 / RIPA) I. Bölümünün I. Kısmı, bu alandaki temel düzenleyici hukuki metindir. I. Bölüm, sırasıyla iletişim içeriğinin arasına girilmesi ile iletişim verilerinin elde edilmesi ve açıklanması olmak üzere iki alt kısma ayrılmaktadır. Yasa birincil olarak halkı oluşturan bireylerden ziyade, soruşturma makamlarının işlemlerine yönelmiştir; soruşturma yetkilerinin kullanılmasını insan haklarına uyumlu bir şekilde düzenlemektedir[482]. Buna rağmen RIPA uyarınca yapılan ilk suçlama, Eylül 2005 tarihinde, bir özel kişiye karşı yapılmıştır[483]. Özel bir dedektiflik şirketinde çalışan bu kişi, telefon konuşmasının arasına girmek gerekçesiyle Ocak 2006 tarihinde cezalandırılmıştır[484]. Bu nedenle bu tür eylemlerin bilişim sistemlerinin bütünlüğe karşı bir suç olarak değerlendirilmesi talep edilmiştir[485].

RIPA'da iki suç düzenlenmektedir. Bunlardan bir tanesi kişinin *"kasten ve hukuka uygun bir yetkisi olmaksızın kamusal bir iletişim sistemi aracılığıyla bir iletişimin aktarımı esnasında araya girmesidir"*. Aynı eylemin *"özel bir iletişim sistemi"* kullanılarak gerçekleştirilmesi de suç olarak düzenlenmektedir[486]. Bu suçun cezasının azami sınırı iki yıl hapis cezasıdır[487]. Ayrıca kast olmaksızın gerçekleştirilen araya girme eylemlerine uygulanmak üzere "para cezası bildirimi" olarak bilinen bir idari ceza da 2011 yılında eklenmiştir[488].

Her iki suçta da kullanılan terminolojinin daha fazla değerlendirilmeye ve açıklığa kavuşturulmaya ihtiyacı vardır. İlk olarak, bilgisayarların kötüye kullanılmasına benzer biçimde, yetkili makamlar konusuyla ilgilenilmesi gerekir. RIPA, kapsamlı ve ayrıntılı bir biçimde bu tür yetkili makamların bulunduğu durumları açıklamaktadır[489]. Bunlar özellikle Kısım III, IV ve V'te ayrıntılı bir şekilde yer almakta ve genellikle soruşturma makamları tarafından

---

481 Regulation of Investigatory Powers Act 2000 (RIPA).

482 2000 tarihli Soruşturma Yetkilerinin Düzenlenmesi Yasası, Açıklayıcı Not pn. 3.

483 "Elektronik posta korsanları NHTCU'nun soruşturması neticesinde cezalandırıldılar". Police Oracle, 19 Eylül 2005, http://www.policeoracle.com/news/Email-Hackers-Sentenced-Following-NHTCU-Investigation_8343.html, 25.9.2016.

484 "On sekiz dedektif gizli soruşturma yapmakla suçlandı", BBC News, 28 Ocak 2006, http://news.bbc.co.uk/2/hi/uk_news/4656780.stm, 25.9.2016.

485 Walden, pn. 3.311.

486 Duruma göre RIPA m. 1(1) ve (2).

487 RIPA m. 1(7): Olası cezalar, iddianameye göre, azami iki yıl hapis cezası ya da para cezası, ya da jürisiz yargılama sonucunda verilen mahkûmiyet kararı (summary conviction) ile 5000 Sterlini geçmemek üzere verilecek para cezası (1980 tarihli Sulh Ceza Mahkemeleri Yasası [Magistrates' Courts Act 1980] m. 32).

488 RIPA m. 1(1A) ve Sch A1. Bu tür notlar İletişim Araya Girme Komisyonunu tarafından empoze edilmiş olabilir. **Walden**, pn. 3.312.

489 RIPA m. 1(5)

kullanılan yetkiler ile ilgilenmektedir. Özel bir kişinin[490] "hukuka uygun bir yetki" ile araya girme eyleminde bulunduğu sınırlı iki durum, araya girenin, her iki tarafın[491] bu konuda rızasını almış olması ya da devlet bakanı tarafından bu konuda çıkarılan bir düzenleme ile yetkilendirilmiş olmasına bağlıdır[492].

Araya girme aşağıdaki şekilde tanımlanır:

"…bir kişi telekomünikasyon sistemi aracılığıyla bir iletişimin aktarımı esnasında araya girerse, bu kişi ancak ve ancak,

(a) sistemi ya da onun işleyişini değiştirir ya da engeller/müdahale ederse,

(b) sistem aracılığıyla gerçekleştirilen iletişimi izlerse veya,

(c) kablosuz telgraf sistemi veya sistem kapsamında yer alan bir araç ile iletimi izlerse,

iletişimin bazı ya da tüm içerikleri, iletim esnasında, gönderici ya da gönderilmek istenen kişi dışında bir kişi için erişilebilir hale gelirse…"[493]

Sistemin verileri, sesli mesaj kutularında olduğu gibi, sonraki erişimler için depolaması ya da kastedilen alıcılar tarafından toplanması halinde, bunlar hala "iletimine devam edilen veriler" olarak kabul edilir[494]. Bu hükmün anlamı, Dünyadan Haberler (News of the World) gazetesinden bir gazetecinin gerçekleştirdiği telefon korsanlığı hakkındaki *Edmondson* davasında[495] kapsamlı bir şekilde inceleme konusu yapılmıştır. Sanıklar, sesli bir mesajın, servis sağlayıcının sisteminde alıcının alması için hazır bulunduğu sürece bunun halen iletimde olduğunun kabul edilemeyeceğini ileri sürmüşlerdir. Mahkeme bu görüşü reddetmiş, hükmün doğal anlamının "İletişimin ilk alıcısı, iletimi sonlandıran kişi olarak görülmelidir". önermesini desteklemediğine karar vermiştir. Mahkeme, sesli mesajın kastedilen alıcısının söz konusu mesaja erişebilmek için hizmet sağlayıcıya "tamamen bağlı olduğunun" önemli olduğunu düşünmektedir. Dolayısıyla, erişilebilen sesli mesaj ile kastedilen alıcının mesajlarını bir bilgisayar ya da akıllı telefon gibi kendi araçları üzerinden

---

490 Telekomünikasyon hizmeti verenlerden farklı bir kişidir, soruşturmada üstlenmiş olduğu role bağlıdır. 2003 tarihli İletişim Yasası'ndan önce, iletişim hizmeti verenler tarafından açıklanması ayrı bir suç olarak düzenlenmekteydi. (1985 tarihli Telekomünikasyon Yasası m. 45, öncesinde 1981 tarihli Britanya Telekomünikasyon Yasası).

491 RIPA m. 3(1). Hükmün özgün halinde araya girenin yalnızca böyle bir "rızanın varlığına ilişkin makul bir temele dayanmasının" gerekli olduğu düzenlenmekteydi. Bkz: Chand v. Police of the Metropolis [2006] Po LR 301 (IPT). Bu davada olası gözlemenin farkında olunması ve sistemin kullanılmaya devem edilmesi rızanın varlığı için yeterli kabul edilmiştir.

492 RIPA m. 4(2). Walden, pn. 3.313.

493 Walden, pn. 3.314.

494 RIPA m. 2(7). Buna karşın Birleşik Devletler hukukunda, bir iletişim bellek tarafından alınmışsa araya girme söz konusu olmaz, bkz: United States v. Steiger, 318 F 3d 1039 (11th Cir), cert denied (temyiz başvurusu reddedilmiştir) 538 US 1051 (2003).

495 Edmondson and other v. R [2013] EWCA Crim 1026.

elde edebildiği elektronik posta sistemleri arasında bir ayrım yapılabileceğinin ileri sürülebilir olduğu görülmektedir[496].

Neyin kamusal neyin özel olduğunu ayırt etmek konusundaki zorluk yalnızca siber suçlara özgü bir tartışma değildir. Bu tartışma bütünleşik ve ağ tabanlı toplumumuzda daha da karmaşık bir hal almıştır. Bu görüş, telekomünikasyon sektöründeki genel taşıyıcıların koruma yükümlülüğüne ilişkin tarihi tartışmayı da desteklemektedir[497]. 2003 tarihli Telekomünikasyon Yasası, kamusal bir servisin *"toplumun bir üyesi tarafından kullanılabilir olması"* açısından tanımlanması ayrımıyla mücadele etmektedir[498]. Bunun üzerine bu husus sektör düzenleyicileri tarafından iyice detaylandırılmıştır; Oftel bunun *"ödeme yapacak ve uygulanacak kurallara ve şartlara uyacak herkes"* anlamına geldiğini belirtmektedir[499]. İnternet dünyasında sorun, bir iletişimin aktarımında kullanılan bileşenleri olan çeşitli ağların nasıl nitelendirileceğidir. Örneğin, BT FON, BT müşterilerinin kendilerine ait WiFi bant genişliğinin bir parçasını evlerindeki yönlendiricide (home router) bulunan ayrı bir kanalla, sinyallerinin menzili içindeki diğer üyelerle güvenli bir biçimde paylaşmasını mümkün hale getiren bir girişimdir. Normalde "yönlendirici" kişisel/özel olarak nitelendirilen bir telekomünikasyon sistemidir, ancak kapasitesini paylaştığı zaman kamusal telekomünikasyon sisteminin görünüşte bir parçası haline gelmektedir[500].

Bu tanımlamalarda gereken açıklığın bulunmaması, kamusal tarafın doğal sonucunda olduğu gibi, Ashwort'un *"azami açıklık"* ilkesinin ihlali ve Avrupa İnsan Hakları Mahkemesi'nin hukuk kurallarının vatandaşların davranışlarını düzenleyebilecekleri yeterlilikte açık bir biçimde düzenlenmesi gerektiğine ilişkin içtihatlarıyla[501] çelişkili olduğu şeklinde yorumlanabilir[502].

Bu tür bir dar teknik açıklama, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde yer alan mahremiyet hakkı ve buna ilişkin Mahkeme içtihatları açısından gerekli olan mahremiyete koruma sağlanmasının başarısızlığa uğradığı izlenimini vermektedir[503]. Bunun yerine, araya girmenin belirleyici

---

496 Walden, pn. 3.316.

497 Genel olarak bkz: Eli M. Noam, "Beyond Liberalization II: The Impending Doom of Common Carriage", Telecommunications Policy, Vol. 18, No. 6, 1994, s. 435-452.

498 2003 tarihli Telekomünikasyon Yasası m. 151. Bu yasa "sistem" terimine nazaran "ağ" terimini kullanmaktadır, "ağ" terimi AB hukuku ile uyumlu olup, "sistem" terimi ise 1984 tarihli BTA'da kullanılmaktadır.

499 Office of Telecommunications (Oftel) Guidelines for the Interconnection of Public Electronic Communication Networks, 23 Mayıs 2003, m. 6.1.

500 Walden, pn. 3.321.

501 Sunday Times v. UK (1979) 2 EHRR 245, pn. 49.

502 Walden, pn. 3.322.

503 David Ormerod/Simon McKay, "Telephone Intercepts and their Admissibility", Criminal Law Review, January 2004, s. 15-38.

etkeni bunun gerçekleştirilmesinin amacı olmalıdır. Örneğin, iletişimin doğasında yer alan gizliliğin ihlal edilmemesi hakkı, böyle bir yasal düzenlemenin koruma amacıdır. Bu yaklaşımın desteği RIPA'nın kendisinde bulunabilir, kullanışlı bir yaklaşımın benimsendiği yerde araya girme, hukuka uygun ticari uygulamalar için gerçekleştirilmektedir[504]. 2002 tarihinde çıkarılan İçişleri Bakanlığı Gizli Gözetim Uygulamaları Yönetmeliği'nde şu hüküm yer almaktadır:

"Bir gözetim aracının kullanılması basit bir biçimde düzenlenmemelidir çünkü rastlantısal olarak bir ya da her iki telefon görüşmesini de elde edebilir… Ancak, aktarım bir telekomünikasyon sistemi aracılığıyla yapıldığında, salt amacın gizli dinleme olması ve aynı zamanda gözetim yapılması halinde bu yöntemin kullanılması uygun değildir. Bu gibi durumlarda iletişimin arasına girilmesi için *gerekli olan emrin alınması için gerekli olan başvuru 2000 tarihli Yasanın 5. maddesi uyarınca yapılmalıdır"*[505]*.*

Bu, açıkça "araya girme" kavramının tekil bir anlamdan ziyade amaç üzerinde temellendiğini teyit etmektedir. Ancak, bu yaklaşım Yönetmeliğin yeniden gözden geçirilen 2010 ve 2014 tarihli versiyonlarında terk edilmiştir. Halihazırdaki tavsiye şu şekildedir:

"Bir ya da her iki telefon görüşmesinin bir dinleme aracı tarafından dinlenilmesi ya da kaydedilmesi … söz konusu işlem ile elde edilen ürün telekomünikasyon sistemine ya da onun yürütülmesine müdahalede bulunma ya da değiştirme içermiyorsa … araya girme oluşturmaz"[506]*.*

Siber Suçlar Sözleşmesi'nin "araya girmenin" geniş biçimdeki yorumunu desteklediği görülebilir; bundan dolayı Sözleşme "bir bilişim sisteminden kaynaklanan elektromanyetik yayımları" da araya girmenin bir türü olarak içermektedir[507]. Hatta bu tür teknikler, casus dinleme cihazlarına (böceklere) benzer şekilde, gizli dinlemenin sofistike bir yöntemi biçiminde kolaylıkla kullanılabilir[508].

c) Kontrol Hakkı

Denetim sorunu, madde 1 uyarınca yapılan ilk suçlamanın merkezinde yer almıştır. Redbus Interhouse Plc şirketinde daha önce çalışmış olan Stanford, şirketin başkanı da dahil olmak üzere üç şirket çalışanının elektronik

---

504 RIPA m. 4(2).

505 Home Office, Covert Surveillance: Code of Practice, The Stationery Office, 2002, pn. 4.32.

506 Home Office, Covert Surveillance and Property Interference: Revised Code of Practice, The Stationery Office, 2014, pn. 2.10.

507 Siber Suçlar Sözleşmesi m. 3.

508 Walden, pn. 3.325.

postalarının arasına girebilmiştir. Stanford, şirketin kıdemli bir çalışanı tarafından sağlanan kullanıcı adı ve parolayı kullanmak suretiyle şirketin elektronik posta sistemine erişim sağlamak için şirketin söz konusu çalışanını ikna etmiştir. Bunu takiben sisteme indirilen bir yazılım sayesinde elektronik postaların bir kopyasının özel bir soruşturmacı olan George Liddell tarafından yönetilen bir Hotmail hesabına gönderilmesi sağlanmıştır[509]. Stanford, erişim sağlayan çalışanın madde 1(6)(a) uyarınca kontrol hakkı olduğunu iddia etmiştir. Demon & Redbus'un kurucusu olan Cliff Stanford ve George Liddell, yargıcın *"kendilerinin ne kontrol etme hakkına ne de buna ilişkin açık ya da zımni bir rızaya sahip olduklarına"* karar vermesinden sonra suçu kabul etmişlerdir[510].

Temyiz aşamasında mahkeme, yargıcın kararını onamıştır. Mahkeme, *Alison* davasında Lord Hobhouse tarafından CMA'ya göre kabul edilen "kontrol" ifadesinin anlamını ele almıştır; örneğin, "kontrol" bir bilgisayarın kullanılması için "yetkilendirmeye ya da yasaklamaya" hakkı olmak anlamında olup, yalnızca onu kullanabilme kabiliyeti anlamında değildir[511]. Buna ek olarak Temyiz Mahkemesi, altı ay süreli gözetim altına alma cezası ve eylemin asıl amacı olarak ticari açıdan bir avantaj sağlanması olması nedeniyle para cezası verilmesi hususunda alt derece mahkemesiyle aynı görüştedir[512]. Görülmektedir ki, yetkisiz erişim ve değiştirmede olduğu gibi, yetkilendirme konusunun özellikle kuruluş içerisinden birinin eylemde bulunması halinde birçok problemi çıkarması olasıdır[513].

6. Hukuka Aykırı Araçlar

Bilişim sisteminin bütünlüğü ile bilişim sistemi ve içerik ile ilgili suçlar arasındaki yapılan öncelikli ayrım, bunlardan ikincisinde suç oluşturan bir hareketin gerçekleştirilmesinde bilgisayarın ve iletişim sistemlerinin, adeta suçun bir ön unsuru gibi[514], bir araç olarak kullanılmasıdır. Suçun işlenmesinde teknoloji, suçun öznesini (konusunu) oluşturmaktansa, salt bir araç konumundadır. Ancak, bir suçun işlenmesine yardım etmek için özel

---

509 Bkz: Claire Walker, "Email Interception and RIPA: the Court of Appeal Rules on the 'Right to Control' Defence", Communications Law: Journal of Computer, Media & Telecommunication, Vol. 11, Issue 1, 2006, s. 22 vd.

510 Walden, pn. 3.329.

511 Stanford, Times Law Reports, 7 Şubat 2006.

512 Walker, s. 22 vd.

513 Walden, pn. 3.330.

514 Ülkemizde geçerli olan ceza hukuku sistemi ve benimsediğim suç teorisi açısından suçun ön unsurları kavramını kabul etmediğimi ifade etmeliyim. Suçla ilgili bir husus suçun ya unsurudur ya da değildir. Ancak Anglo Amerikan hukuk sistemi ceza hukukunun bakış açısı farklıdır. Bu nedenle söz konusu kavram kullanılmaktadır.

olarak dizayn edilen araçların tedarik edilmesinin veya bulundurulmasının suç haline getirilmesi genel başlığı, esas olarak üç kategoriye ayrılmaktadır. Bu aletler genellikle şifre kırmak, kriptoloji ve tuş kaydı tutma (keylogging) için geliştirilmiş yazımları içermektedirler[515].

Dolandırıcılık suçu açısından, dolandırıcılık eyleminde kullanılmak üzere bir aracın taşınması ya da tedarik edilmesi[516] veya hileli bir biçimde elektronik iletişim hizmetlerinden yararlanmayı sağlayan araçların bulundurulması veya tedarik edilmesi suçtur[517]. Sahtekârlık suçunda, belirli bir aracın yapılması için özellikle dizayn edilen ya da uyarlanan bir *"makine, alet, belge ya da herhangi bir materyalin"* yapılması, bulundurulması ya da kontrol altında bulundurulması bir suçtur[518]. Fikri mülkiyet hukukunda, teknolojik koruma önlemlerinden kurtulmak için dizayn edilmiş araçların tedarik edilmesi suçtur[519]. Benzer şekilde, bilişim hukukunda da bilişim sistemlerinin bütünlüğü açısından suç işlemek için dizayn edilen araçların bulundurulması ve tedarik edilmesi suç haline getirilmiştir[520].

Tüm bu suçlar, tamamlanmış asli bir suçun işlenmesini sağlayan nedensel bileşenler olarak belirtilen "öncül" suçlar olarak nitelendirilebilir. Ayrıca bunlar, bilgisayarın bir suçun öznesi ile nesnesi olması ayrımının sınırında bir yerlerde bulunmaktadır. Suçun maddi unsurunu oluşturan bulundurma, bir makinenin çalınmasına benzemektedir; suçun manevi unsuru ise bir başka yere yönelmiştir, örneğin sistemin ya da verinin sahip olduğu bütünlüğe ya da gizliliğe yönelmiştir[521].

Siber Suçlar Sözleşmesinin 6. maddesi uyarınca, sözleşmeye taraf devletler; araçların, bilgisayar şifrelerinin, giriş kodlarının veya benzer verilerin bulundurulmasını ve tedarik edilmesini suç haline getirmek yükümlülüğü altındadırlar. Bu yükümlülük, örneğin Windows işletim sisteminde genellikle "sömürü" (expolits) olarak adlandırılan ve bir başka kişinin sistemine kötücül yazılımları tanıtmak için kullanılan yazılım gibi bir uygulama yazılımının bilinen bir zayıflığı ya da kırılganlığı hakkında bilgiler gibi araçları suç olarak tanımlamayı içermektedir. Söz konusu madde, bilişim suçlarının kaçınılmaz bir özelliği haline gelen ve "kötücül pazar yeri"[522] olarak tanımlanan "bilişim

---

515 Walden, pn. 3.336.

516 Duruma göre Fraud Act m. 6 ve m. 7. Bkz: Charles Brown [2014] EWCA Crim 695, bu davada sanığın bilgisayarında çalınti banka ve kredi kartı bilgileri bulunmuştur.

517 CA, m. 126.

518 FCA, m. 5(3) (4).

519 CDPA 1988, m. 296ZB.

520 Walden, pn. 3.337.

521 Walden, pn. 3.338.

522 Yorumlar için bkz: Roger Cummings, Director of the UK National Infrastructure Security Coordination Centre (NISCC) in Tom Espiner, "Foreign Powers are Main Cyberthreat, UK

korsanları için araç" pazarlanmasını suç haline getirmek için tasarlanmıştır[523].

"Araç" terimi Sözleşmede ayrıntılı olarak tanımlanmamaktadır, bununla birlikte "araç" terimi "bilgisayar yazılımını" içermekte ve "bilgisayar sisteminin" tanımlanmasında kullanılmaktadır[524]. Sözleşmeye İlişkin Açıklayıcı Rapor bir aracın "dijital verilerin kendiliğinden işletilebilmesi için geliştirilen donanım ya da yazılımdan" oluştuğunu not etmektedir[525]. Buna bağlı olarak Sözleşmenin, araç ile veri arasında bir ayrım yaptığı görülmektedir; buna karşın bir bilgisayar yazılımı açıkça verinin özel bir görünümüdür ve bu durum potansiyel bir karışıklık yaratmaktadır. Buna ek olarak, "bilgisayar şifresi, erişim kodu veya benzeri veriler" gibi veri bileşenlerine ait liste, sistemdeki belirli bir istismarı, sızma faaliyeti hakkında veri içeriyor şeklinde yorumlanmayabilir. Zira bu tür verilerin istismarı, sızma faaliyetinin niteliğine göre değişmekle birlikte, şifre erişim kodu ya da değişiklikle aynı mahiyette değildir. Bir aracın veri formunda olması halinde bu tür bilgilerin taşınmasının veya tedarik edilmesinin suç haline getirilmesi, içerikle ilgili suçlarla benzer niteliktedir[526].

Tedarik etmek, geniş anlamda "yapım, satım veya kullanmak üzere satın alma, ithal etme, dağıtma veya bir şekilde elde edilebilir hale getirme" olarak anlaşılır[527]. Bir şekilde elde edilebilir hale getirme kavramı, böyle bir materyali indirilmek üzere bir web sitesinde bulundurmayı, P2P ağ sistemi ya da hyperlink (köprü) aracılığıyla erişim sağlamayı kapsar[528]. Sorumluluğu yüklemek için tedarik etmeye yönelik bir genel kast ve söz konusu aracın kullanılması suretiyle sistem bütünlüğüne ilişkin suçlardan birisini işlemeye yönelik bir özel kastın bulunması gerekir. İngiliz ceza hukuku açısından, içinde bulunduğu şartlara göre, tedarik sağlayan bir kişi suç ortağı (accessory), komplucu/azmettiren (conspirator) ya da maddi (assisting) veya manevi (encouraging) yardım eden olarak nitelendirilebilir[529].

Daha fazla belirliliğin sağlanması için, *"bir bilişim sisteminin yetkilendirilmiş olarak test edilmesi veya korunması amacıyla suç oluşturan bir eylemin gerçekleştirilmesi halinde, tedarik etme ceza sorumluluğunu gerektirir*

Says", CNET News.com, 23 Kasım 2005, http://www.cnet.com/au/news/foreign-powers-are-main-cyberthreat-u-k-says/, 27.9.2016.

523 Walden, pn. 3.339.

524 Siber Suçlar Sözleşmesi m. 1(a).

525 Siber Suçlar Sözleşmesine İlişkin Açıklayıcı Rapor, pn. 23.

526 Walden, pn. 3.340.

527 Siber Suçlar Sözleşmesi m. 6(1)(a).

528 Siber Suçlar Sözleşmesine İlişkin Açıklayıcı Rapor, pn. 72. Örneğin bkz: Universal City Studios, Inc and others v. Corley and others, SD Cal, 17 Ağustos 2000, DVD'lerin bölgesel korunmasını sağlayan mekanizmanın şifresini çözen "DeCCS" yazılımına yapılan bağlantı hakkında görülen bir davadır.

529 Walden, pn. 3.341.

biçimde yorumlanmamalıdır" ifadesini içeren bir hükümle suç tipinin daha açık olması için eksiklikler giderilmiştir[530]. Bu madde kasıt sorunuyla ilgili görünmektedir. Her ne kadar Açıklayıcı Rapor bunu yalnızca "hukuka aykırılık" konusu ile ilişkilendirse de, madde kasıtlı kullanım üzerine odaklanmaktadır[531]. Söz konusu hükmü değiştiren ifade, ister akademik isterse de ticari açıdan olsun, hukuka uygun işlemleri için bu tür araçlardan yararlanan veri güvenliği alanında çalışan kişileri korumak için zorunludur[532].

Bu madde ayrıca aracın öncelikli olarak sistem bütünlüğüne ilişkin suçlardan birisini işlemek için dizayn edilmesini veya değiştirilmesini gerektirir ki bu husus iddia faaliyeti açısından önemli bir ispat yükümlülüğüdür ve mahkeme tarafından nesnel bir biçimde ayrıştırılması gereken çok önemli bir sorundur. Buna karşın genellikle, tedarik işiyle uğraşan kişiler tarafından yapılan hareketler ve açıklamalar göz önünde bulundurulmalıdır. Örneğin; *Invicta Plastics Ltd v. Clare* davasında, sanıkların yaptıkları işin 1949 tarihli Kablosuz Telgraf Yasası'nı ihlal ettiğine ilişkin uyarı olmasına rağmen, polisin radar tuzaklarını belirlemek için kullanılan araçların satışında kullanılan reklamda dolaylı olarak belirtilen bir kışkırtma vardır[533]. Birleşik Devletler ve Avustralya'dakine benzer biçimde mahkeme, şirketlerin bu tür hukuka aykırılıkları kasten desteklediklerini gösteren delillere dayalı olarak P2P yazılımları dağıtmak suretiyle fikri mülkiyet ihlalinde bulunduklarına karar vermiştir. Bizim de burada ilgilendiğimiz sistem bütünlüğüne ilişkin suçlarda kullanılan araçlar, fikri mülkiyet ihlallerinde kullanılan araçlara benzerlik gösterir. Önceden de belirtildiği üzere, fikri mülkiyet ihlalini sağlayan tarzdaki bilgisayarlar ve ağlar, kopyalama önlemlerinin aşılmasını sağlayan araçlara[534] ve şartlı erişim sağlayan araçlara[535] karşı işlenen yeni suçlar için uyarlanmıştır[536].

Bulundurma açısından yine iki ayrı kastın varlığı gerekir. Bunlardan ilkine göre, kişinin söz konusu aracı tesadüfen bulundurmuyor olmasını, kişinin aracı bulundurma kastının olmasını ve suçlardan birini işlemek üzere hakkı olmaksızın aracı kullanmaya yönelik kastının bulunmasını gerektirir. Siber Suçlar Sözleşmesi, taraf devletlere kişilere ceza sorumluluğunun yüklenebilmesi için belirli sayıda aracın bulundurulmasının gerekli olması yönünde düzenleme yapmaları hususunda izin vermektedir[537]. Bunun kasıt

[530] Siber Suçlar Sözleşmesi m. 6(2).
[531] Siber Suçlar Sözleşmesine İlişkin Açıklayıcı Rapor, pn. 77.
[532] Walden, pn. 3.342.
[533] [1976] TRT 251.
[534] 1988 tarihli Telif Hakkı, Dizayn ve Patent Yasası, m. 296ZB.
[535] 1988 tarihli Telif Hakkı, Dizayn ve Patent Yasası, m. 297A.
[536] Walden, pn. 3.343.
[537] Siber Suçlar Sözleşmesi m. 6(1)(b). Ayrıca bkz: Milletler Topluluğu Model Yasası m. 9(3). ABD hukukuna göre, 18 USC m. 1029(a)(3) uyarınca bulundurma yalnızca on beş ya da daha fazla

konusuna yöneldiği görülür, en az sayıda araç bulundurma hukuka aykırı işlemlerde kullanma kastının belirlenmesi açısından bir temel sağlar. Hatta bu tür bir kasıt, büyük olasılıkla, kişisel kullanımdan ziyade, başkalarına bu ürünlerin tedarik edilmesine yönelik olduğunun göstergesidir. Ayrıca taraf devletler, bulundurmayı suç olarak düzenlememekte özgürdür[538].

"Hakkı olmama" zorunluluğunun suça dahil olmasına, bir otorite tarafından sağlanan pozitif bir algıdan ziyade, hukuka aykırılık ve mazeret nedenleri açısından bakılması gerekir. Bir kişiye karşı, araç tedarik etmesinden dolayı soruşturma/kovuşturma başlatıldığında, suçlama yalnızca ikili kastı ispatlamak zorunda değildir, genel kast duruma göre yeterlidir. Fakat söz konusu ikili kastın varlığı, suçun oluşmasından başka, tedarik edilen bir aracın "hukuka uygun" mu yoksa "hukuka aykırı" mı olduğunun belirlenmesinde de kullanılır. Bu durum, özellikle araçların ikili kullanımı açısından, gereksiz düzeyde fazla suç haline getirmenin önlenmesi içindir[539].

Bunun yanı sıra AB Direktifi, 2005 tarihli Çerçeve Çalışmasından ayrı olarak, "suç işlemek amacıyla kullanılan araçlar"[540] hakkında bir madde içerir. Bu madde, iki tip araca yönelik tedarik sağlamayla sınırlıdır: Bilgi sistemine erişimi sağlayan Siber Suçlar Sözleşmesi'ndekine benzer biçimde "öncelikli olarak bunun için dizayn edilmiş ve tasarlanmış bir bilgisayar yazılımı" veya "bilgisayar şifresi, erişim kodu ya da benzer veri". Bu suç, hakkı olmaksızın davranışta bulunmayı ve bilişim sisteminin bütünlüğüne karşı bir suç işlemeye yönelik kastın varlığını gerektirir[541].

CMA'nın ilk halinde "araçlara" ilişkin bir düzenleme bulunmamakla birlikte, bu tür araçları tedarik eden kişinin, suç ortağı veya suça yardım eden olarak suçlanması mümkün olmaktaydı[542]. Sonuç olarak Siber Suçlar Sözleşmesi'nin getirdiği yükümlülük gereğince Hükümet önce 2006 tarihli yasaya bu yönde bir hüküm koymuş, Nisan 2015'te de söz konusu hükmü şu şekilde değiştirmiştir:

"3A. madde 1, 3 veya 3ZA'da tanımlanan suçları işlemek için yapılan, tedarik edilen veya bulundurulan araçlar.

(1) Kişi eğer madde 1, 3 veya 3ZA'da tanımlanan suçların işlenmesinde ya da bu suçlara yardım edilmesinde kullanılmak kastıyla bir aracı yaparsa, uyarlarsa, tedarik ederse ve aracın tedarik edilmesini teklif ederse suçlu bulunur.

---

sayıda sahte ya da yetkisiz erişim aracının söz konusu olması halinde suç oluşturmaktadır.

538 Siber Suçlar Sözleşmesi m. 6(3). Azerbaycan, Almanya, Japonya, Norveç, İsviçre, Ukrayna ve Birleşik Devletler bu madde ile ilgili bildirimde bulunmuşlardır. Walden, pn. 3.344.

539 Walden, pn. 3.345.

540 Direktif 13/40/EU m. 7.

541 Walden, pn. 3.346.

542 PJA m. 42 ile CMA'ya m. 3A eklenmiştir.

(2) Kişi eğer madde 1, 3 veya 3ZA'da tanımlanan suçların işlenmesinde ya da bu suçlara yardım edilmesinde kullanılma olasılığını bilerek bir aracı tedarik ederse ve aracın tedarik edilmesini teklif ederse suçlu bulunur.

(3) Kişi şu araçlardan birini bulundurursa suçlu bulunur:

(a) Bölüm 1, 3 veya 3ZA'da tanımlanan suçları işlemek ya da bu suçlara yardım etmek için aracı kullanma kastı varsa,

(b) Madde 1, 3 veya 3ZA'da tanımlanan suçları işlemek ya da bu suçlara yardım etmek amacıyla söz konusu araçlar tedarik edilmişse."

Bu madde söz konusu "araçların" tedarik edilmesini adreslemektedir. Bu araçlar büyük olasılıkla hem somut hem de soyut niteliktedir. Ancak yalnızca soyut olanlar maddede açıkça bir biçimde ifade edilmişlerdir: *"Elektronik formda bulunan herhangi bir yazılım ya da veri"*[543]. Bir aracın yapılması, uyarlanması ya da tedarik edilmesi, ancak kişi yetkisiz bir erişime ya da yetkisiz erişimle işlenen bir suça kastederse bir suçtur. Bu ise, bir suçlama yapıldığında karşılaşılacak oldukça yüksek bir eşiktir[544]. Bununla birlikte ikinci suçun farklı bir manevi unsuru vardır; buna göre, aracın bilişim korsanlığında ya da yetkisiz erişimde kullanılma olasılığının bulunduğuna inanılmalıdır. Bu tür aracın bulundurulmasına ilişkin üçüncü suç, söz konusu aracı kullanma ya da tedarik etme amacıyla bulunduran, bu tür araçların dağıtımını sağlamakta yer alacak müstakbel aracıyı hedefine almaktadır. Bu üçüncü suç 2006 tarihinde Yasaya alındığında, yalnızca üçüncü bir kişiye araç tedarik edilmesine ilişkindi. Bu durum çok dar olarak değerlendirilmekteydi; bu nedenle madde, söz konusu araçların sistem bütünlüğüne karşı suçların işlenmesinde "kişisel kullanımı"[545] içerecek şekilde genişletildi. Her üç suçun da azami cezası iki yıl hapis cezasıdır. Sırasıyla cezaları on ve beş yıl olan, dolandırıcılıkta kullanılmak üzere araç tedarik edilmesi ve bulundurulması suçlarının cezası ile karşılaştırıldığında, bu suçların cezasının oldukça yetersiz oldukları görülür[546].

Bu suçlar duyuru panoları gibi kimin, nasıl, nerede ve ne zaman kullanacakları hususunda belli bir niyeti olmaksızın bireylerin diğer bireylere suçta kullanılacak araçları satma olanağı bulduğu "kötücül marketlerin" büyümesi hedeflenerek düzenlenmiştir[547]. Buna karşın, tedarik edilen aracın

[543] CMA, m. 3A(4).

[544] Bkz: Lewys Stephen Martin [2013] EWCA Crim 1420.

[545] Home Office, Serious Crime Act 2015, Circular 008/2015, 25 Mart 2015, pn. 13. https://www.gov.uk/government/publications/circular-0082015-serious-crime-act-2015, 1.10.2016.

[546] Walden, pn. 3.347.

[547] Örneğin bkz: Europol, "Cybercriminal Darkode forum taken down through global action", Press Release, 15 Temmuz 2015, https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action, 1.10.2016.

suçta kullanılacağına inanmaya ilişkin ikinci suç, potansiyeli suç haline getirdiği gerekçesiyle eleştirilmekte ve bu nedenle bilimsel çalışmaların da ya da işlerinde kullanmak üzere bu tür araçları geliştiren ve bulunduran bilgi güvenliği alanındaki araştırmacılar, penetrasyon testi yapanlar ve bu alandaki diğer çalışanlar için de hukuki açıdan belirsizlik oluşturmaktadır. "İnanmanın" gerekli olduğu durumlardaki hatanın niteliği halihazırda İngiliz hukukunda belirgin bir biçimde açıklanmamıştır. Buna rağmen, indirilen nesnelerin bazı bölümlerinin kötü amaçlar için kullanılmak üzere yanlış ellere düşmesine ilişkin salt şüphe hatta muhtemel bilgidense, bu tür bir kötü kullanım lehine olarak "olası" ifadesi bir olasılık önermektedir[548].

Araçların "ikili kullanımı" olarak da adlandırılan konu hakkında Hükümet, Başsavcılıktan bu bölüme ilişkin yürüteceği soruşturma ve suçlamalar hakkında bir rehber yayınlanmasını istemiştir. Söz konusu rehber "olası" ifadesinin ne anlama geldiği hususunda, savcıların "nesnenin işlevselliğini ve eğer varsa şüphelinin nesneyi hangi kişiye vereceğini" dikkate alması gerektiğini belirtmektedir[549]. Diğer ilgili etkenler ise nesnenin meşru kanallar vasıtasıyla ticari bir ortamdan elde edilebilir olup olmadığı ve önemli bir montaj tabanının olup olmadığıdır[550].

ABD federal hukukuna göre, söz konusu madde, tüm kategorilerdeki bilgisayar ve siber suçları kapsayacak şekilde, "erişim araçlarının" dolandırıcılıkta kullanılması için oluşturulmuştur ve geniş bir biçimde şu şekilde tanımlanmıştır[551]:

"para, mal, hizmet veya değeri olan herhangi bir şeyi sağlamak için veya para fonlarının aktarımında kullanmak için (yalnızca kâğıt belge ile yapılan aktarımlardan farklı olarak); birlikte ya da tek başına erişim sağlayan; herhangi bir kart, plaka, kod, hesap numarası, elektronik seri numarası, mobil araç tanımlama numarası veya diğer telekomünikasyon hizmeti, donanımı veya tanımlayıcı aleti veya hesaba erişimde kullanılabilecek diğer araçlar[552]*."*

"Sahtecilik erişim araçları" ile "yetkisiz erişim araçları" kavramları arasında ayrım yapılmalıdır; bunlardan ilki yanlış bir kavramdır, ikincisi ise doğrudur ve hak sahibi kullanıcının zilyetliğinde olmadığı (örneğin, kaybedilmiş ya da çalınmış) veya daha fazla geçerli olmadığı (örneğin, son kullanım tarihi geçmiş ya da geçersiz hale getirilmiş) anlamına gelir. Bu tür bir aracın üretilmesi,

548 Walden, pn. 3.348. Ayrıca bkz: Ormerod, Smith & Hogan's Criminal Law, s. 855, 856.

549 CPS, Legal Guidance to Computer Misuse Act 1990, at "Section 3A CMA – Making, supplying or obtaining articles" http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/index. html, 2.10.2016.

550 Walden, pn. 3.349.

551 Walden, pn. 3.350.

552 18 USC m. 1029(e)(1).

ticaretinin yapılması, kullanılması ve bulundurulması, yirmi yıla kadar hapis cezasını gerektiren bir suçtur[553].

7. İstenmeyen İletişim

İstenmeyen elektronik posta ya da daha çok bilinen diğer adıyla "spam", tüm internet kullanıcılarının oldukça aşina oldukları bir aktivitedir. Bize, çeşitli kötücül uygulamalar aracılığıyla, bir şeyleri satmaya, göstermeye ve benimsetmeye çalışan mesajların durmaksızın gelmesi hem çok iyi bilinen hem de üzerinde çok şey yazılan bir konudur. Tüm elektronik posta trafiğinin önemli bir kısmını kapsadığına inanılan bu sorunun geçtiğimiz yıllardaki ölçeği, bu tür aktivitelerin siber alanın geleceği hakkında oluşturduğu tehdit algısı ile birleştirildiğinde, bu problemle mücadele için hem hükümetlerin hem de bilişim endüstrisinin buna ilişkin çok sayıda girişimde bulunmasını sonuçlamaktadır. Buna benzer teknikler, "spimming" [554] olarak bilinen blog (weblogs) ve anlık mesajlaşma gibi diğer mesajlaşma servislerine de dağılmıştır[555].

Hükümetler yalnız istem dışı alınan elektronik posta ile ilgilenmemektedir, bunun yanı sıra diğer iletişim araçlarıyla, özellikle de sesli aramalar ve fakslar ile de ilgilenmektedir. Tarihsel olarak bu tür iletişimlerin gönderilmesi, eğer gönderilen mesajın içeriğinin kendisi (örneğin, çocuk pornografisi) ya da tarzı (örneğin, düşmanlık) hukuka aykırı değilse, suç olarak nitelendirilmez. Buna karşın, bu mesajların artan tekrarlanma sıklığı ve kötüye kullanımlarının yoğun bir iletişimi başlatma kabiliyetinin olmasından dolayı, endüstriyel ölçüde etkili olacak biçimde, çeşitli yargı çevrelerinde, bu tür aktiviteleri suç haline getirmek açısından girişimler bulunmaktadır. İzinsiz girmenin ayrı formlarının ve buna bağlı olarak meydana gelen zararının yansımasına göre hukuksal yanıt, sıklıkla iletişimin farklı araçları arasında değişiklik göstermektedir. Sesli aramalar, doğrudan iletişimde bulunan kişileri gerektirmektedir; istenmeyen elektronik postalar, alıcının posta kutusunun gereksiz yere dolmasına neden olurken istenmeyen fakslar da alıcının makinesini ve kağıtlarını kullanmak suretiyle maliyete neden olmaktadır[556].

Bunun yanı sıra istenmeyen iletişim, içerikle ilgili suç olarak sınıflandırılabilir. Bazen içeriğin yalnızca kendisi suç oluşturmaktadır.

---

553 Walden, pn. 3.351.

554 ABD'de Mart 2005'te Anthony Greco, şantaj kastıyla MySpace.com'un bilişim sistemlerine zarar verme tehdidinde bulunmaktan suçlu bulunmuştur; bkz: https://www.justice.gov/archive/criminal/ cybercrime/press-releases/2005/grecoPlea.htm, 2.10.2016.

555 Walden, pn. 3.352.

556 Bkz: Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?", Ed: Bert-Jaap Koops/Miriam Lips/Corien Prins/Maurice Schellekers, Starting points for ICT Regulation: Deconstructing Prevalent Policy One-liners, IT & Law Series Vol. 9, The Hague, TMC Asser Press, 2006, s. 77-108; Walden, pn. 3.353.

Spamhaus Projesinde belirtildiği üzere *"spam içerikle değil, rıza ile ilgili bir konudur"*[557]; rıza ise yetkilendirme ile yakın bir ilişki içinde olup; ICT'lerin gizliliğini, sistem bütünlüğünü ve erişilebilirliğini tehdit eden hareketlerin suç haline getirilmesinde merkezi bir öneme sahiptir. Bu tür kanunlaştırma hareketleri için ifade edilen kamusal politikaların amaçları, aynı zamanda mesajın kaynağı gibi bu tür mesajlarda yer alan bilgilerin dokunulmazlığında olduğu üzere, bu tür trafiğin internetin ve elektronik posta hizmetlerinin kullanılabilirliği ve bütünlüğü üzerindeki etkilerini yansıtmaktadır. Bu bölümde tartışılan, istenmeyen iletişimler ile diğer sistem bütünlüğüne karşı suçlar arasında yapılan ayrım, genellikle mağdurun ICT kaynakları ile çakışmasının derecesine bağlıdır. Kaynakların gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı gerçekleşen doğrudan ve önemli tehditlerin suç haline getirilmesi daha ihtimal olasıdır[558].

Birleşik Krallık hukukuna göre, istenmeyen iletişim sorunu doğrudan iki hukuki aracı işaret etmektedir. Bunların her ikisi de AB ölçütlerini aktarmakta ve ceza hukukuna değil, özel hukuka başvuru yolunu sağlamaktadır. 2002 tarihli Elektronik Ticaret Regülasyonu (ET Direktifi 2002) servis sağlayıcılara istenmeyen elektronik postaların "temiz ve açık bir şekilde tanımlanabilir" olması gibi hususlarda emin olmalarına ilişkin bir yasal yükümlülük getirmektedir[559]. Bu yükümlülüğünün yapısı oldukça hafif olmasına rağmen, Direktifin üzerine kurulduğu temel, bu tür iletişimlerin "etkileşimli ağ sistemlerinin aksamadan çalışmasını" etkileyebileceğini kaydederek, ağ sistemlerinin bütünlüğüne ve kullanılabilirliğine tehdit oluşturduğunu teyit etmektir[560]. İkinci tedbir, modern iletişim teknolojilerinin ortaya çıkardığı mahremiyete yönelik tehditlere ilişkindir: 2003 tarihli Mahremiyet ve Elektronik İletişim Regülasyonu (ET Direktifi 2003)[561]. Buradaki hükümler, otomatik arama sistemleri, fakslar, sesli telefon aramaları ve elektronik postalar tarafından yapılan istenmeyen iletişimi düzenlemekte ve belli şartlar altında yapılan bu tür aktiviteleri yasaklamaktadır. Elektronik postalar açısından, göndericinin daha fazla koruma için sözleşme yapması halinde göndericinin kimliğinin ya da adresinin saklanması, siber alandaki anonimlik sorununu belirtmek için bir girişimdir. Direktif, diğer bir önlem olarak, yasaklamayı meşrulaştırmak için, yüksek miktarda istenmeyen mesajların elektronik iletişim ağlarında ve terminal ekipmanlarında zorluklara

[557] Bkz: https://www.spamhaus.org/consumer/definition/, 4.10.2016.
[558] Walden, pn. 3.354.
[559] SI No 2013, reg 8.
[560] Özellikle elektronik ticaretteki "iç pazarlara" ilişkin bilgi toplumu hizmetlerinin belli bazı hukuku yönleri hakkında 2000/31/EC sayılı Direktif. OJ L 178/1, 17 Temmuz 2000, 30 nolu beyanat.
[561] Electronic Communications (EC Directive) Regulations 2003, SI No 2426.

neden olabileceğine atıfta bulunmaktadır[562]. Bu yükümlülüklerin ihlali, yine yalnızca özel hukuk yaptırımlarını gerektirmektedir; nitekim Bilgi Komiserinin bu tür ihlallere ilişkin olarak 500.000 Sterline kadar para cezası verme yetkisi[563] bulunmaktadır[564].

Birleşik Devletler'de gerçekleşen istenmeyen iletişimin gönderilmesi işlemlerinin suç haline getirilmesinin görünümü, hem eyalet hem de federal düzeydeki mevzuat açısından, Birleşik Krallık'taki görünümün tersinedir. Federal düzeydeki ilk önlem, 2003 tarihli İstenmeyen Pornografi ve Pazarlama Saldırılarının Kontrol Altına Alınması Yasası'dır (Controlling the Assault of Nonsolicited Pornography and Marketing Act of 2003 / CAN-SPAM Act)[565]. AB Direktifinde olduğu gibi, kongrenin bulguları istenmeyen elektronik postaların, iletişim alt yapılarının ve hizmetlerinin aşırı kullanımının bu sistemlerin bütünlüğü ve kullanılabilirliği üzerindeki etkisine atıfta bulunmaktadır[566].

Başlığında, bir çeşit "saldırı" eylemine yer vermekle, geleneksel ceza hukuku terminolojisini kullanılmasının yanı sıra, CAN-SPAM Yasası özellikle aşağıda yer alan aktiviteleri suç olarak düzenlenmektedir:

— İstenemeyen elektronik postaların gönderilmesi amacıyla bir bilgisayara yetkisiz erişim sağlamak; bu "zombi" bilgisayarlar oluşturmayı da içerir.

— "Açık röle" ve "açık vekil sunucu" tekniklerini kullanmak suretiyle aldatmak veya yanıltmak amacıyla oluşturulmuş orijinaline ilişkin mesajlar göndermek[567]. Bu hüküm Birleşik Krallık'ın 2003 tarihli mahremiyet düzenlemesine benzerlik gösterir.

— "Üst başlık"[568] bilgisinin ve gönderilen mesajların çarpıtılması, bu yukarıda anılan aldatma suçundan farklıdır.

---

[562] Avrupa Parlamentosunun ve Konseyinin, elektronik iletişim sektöründe kişisel verilerin işlenmesine ve mahremiyetin korunmasına ilişkin 02/58/EC nolu Direktifi. OJ L 201/37, 31 Temmuz 2002, 40 nolu beyanat.

[563] SI No 2426, reg 31 ve DPA 1998, m. 55A. Bu yetki SI 2015/355 tarafından değiştirilmiş olup, istenmeyen iletişim hükümleri açısından "ciddi bir ihlalin" varlığını tespit etmek için gerekli olan eşiği düşürmüştür.

[564] Walden, pn. 3.355.

[565] Public Law 108-87, 108th Congress, 15 USC m. 7701.

[566] 15 USC m. 7701(a)3; Walden, pn. 3.356.

[567] Bir "açık röle", elektronik postaları yetkisiz olarak kullanan kişileri aklamayı sağlayan posta sunucusudur. "Açık vekil sunucu" ise yetkisiz kullanıcıların diğer yer sağlayıcılara yetkisiz olarak bağlanmasını sağlayan bir ağ sunucusudur.

[568] Üst başlık (header) şu şekilde tanımlanır: Bir elektronik posta mesajına iliştirilen; bir kişi tarafından başlatılan mesaja ait alan adı ve elektronik posta adresi kaynaklı ve hat tanımlayıcı veya kimlik belirten diğer bilgileri de içeren; kaynak, varış yeri ve güzergâh bilgisidir. Bkz: 15 USC m. 7702(8).

— Elektronik posta, kullanıcı hesabı veya alan adı ve kasten gönderilen mesajlar için aldatıcı tanımlama bilgilerinin kaydedilmesi. Sahte sertifikalar kullanmak suretiyle sayısız hesabın kaydedilmesi biçimindeki bu yöntem zombi bilgisayarların kullanılmasına bir seçenektir.

— Kendini sahte olarak kaydettiren, varis ya da IP adresi olarak tanıttıran kasten mesajlar göndermek. Buradaki amaç "kara listede" yer almayan blok halindeki IP adreslerinin ele geçirilmesidir.

Söz konusu temsil edici aktiviteler, spam göndericiler (spammer) tarafından, iletişim hizmeti sağlayanlar tarafından uygulanmakta olan filtrelerden ve sakınma tespiti yapan soruşturma makamlarından kaçınmak amacıyla gerçekleştirilir. Bu hükümler, Birleşik Devletler Ceza Kanunu'nda diğer bilişim suçlarının yer aldığı yere konulmuşlardır[569]. Bu suçların soruşturması, "Adalet Bakanlığı Ceza Hukuku Bölümü Bilişim ve Fikri Mülkiyet Suçları Kısmı" (Computer Crime and Intellectual Property Section in the Criminal Division of the Department of Justice) tarafından yapılır[570].

Bu Yasaya göre birkaç suçlama yapılmıştır. Bu suçlamaların önemli bölümünde suçluluğun kabul edildiği not edilmektedir[571]. Cezalar, ağır suçun bir parçası olarak suçu oluşturan hareketlerinin gerçekleştirilmesi veya failin daha önce aynı ya da benzer bir suçtan mahkûm olması halinde azami beş yıl hapis cezası olarak düzenlenmiştir[572]. Cezalar, gönderilen mesajın hacmi ya da kayıt edilen sahte hesapların sayısı gibi diğer etkenlere bağlı olarak değişkenlik göstermektedir. Birleşik Devletler Ceza Komisyonu'nun rehberi, elektronik posta adreslerinin toplanması gibi belli durumlarda cezanın artırılmasını içerir[573]. Sonuç olarak bu durumda, hem suçtan elde edilen gelirleri hem de suçun işlenmesinde kullanılan ICT aygıtları hakkında el koyma ve müsadere kararları verilebilir[574].

---

569 18 USC, Bölüm I "Suçlar", Kısım 47 "Dolandırıcılık ve Sahtecilik", m. 1037 "elektronik postalarla bağlantılı dolandırıcılık ve ilgili işlemler".

570 Bu Yasa Federal Ticaret Komisyonu (Federal Trade Comission / FTC) tarafından yürürlüğe konulmuştur. Daha fazla bilgi için bkz: www.ftc.gov; Walden, pn. 3.357.

571 Örneğin; "AOL spammeri" Jason Smathers, "wi-fi spammeri" Nicholas Tombros, "zamanpaylaşımı spammeri" Peter Moshou gibi. Genel olarak DoJ tarafından yayınlanan basın bülteni için bkz: www.usdoj.gov.

572 18 USC m. 1037(b). Nisan 2005'te Jeremy Jaynes Virjinya Eyaleti anti-spam yasasını (Başlık 18.2 – 152.3:1) ihlal ettiği için dokuz yıla mahkum edilmiştir. Bkz: David Hancock, "Spammer gets 9 years", CBS News, 8 Nisan 2005, http://www.cbsnews.com/news/spammer-gets-9-years/, 6.10.2016.

573 US Sentencing Commission, Guidelines Manual (yürürlüğe giriş 1 Kasım 2015), m. 2B1.1; bkz: http://www.ussc.gov/guidelines/2015-guidelines-manual/archive, 6.10.2016.

574 18 USC m. 1037(c). Walden, pn. 3.358.

İstenmeyen iletişimin ceza hukukuna ilişkin yapısının görünümüne Birleşik Devletler'in bakış açısı Birleşik Krallık'takinden tamamen farklıdır. Ayrıca diğer Avrupa ülkelerinin büyük bir bölümü ve Avustralya gibi ülkelerdeki farklılıklar ilk anılanlardan daha az önemlidirler. Birleşik Krallık hukukuna göre, istenmeyen postaların gönderilebilmesi için bir makinenin güvenlik sisteminin kırılması ve içine "zombi" yazılımının yerleştirilmesi, CMA'nın 1. ve 2. maddelerinde göre değerlendirilmektedir. Dolandırıcılık ve sahtecilik suçları, özellikle de 2006 tarihli Dolandırıcılık Yasası'nda yer alan yeni dolandırıcılık suçu (sahte tanıtımla dolandırıcılık ve üstü kapalı bilgilendirme ile dolandırıcılık), spammerların aldatma ve sahtesini yapma işlemlerine uygulanabilirler. Üstü kapalı bilgilendirme ile dolandırıcılık suçu, bir kişinin gerçeğe uygun açıklamada bulunmak hususunda yasal yükümlülüğü bulunmasına rağmen bir kişiye dürüst olmayan bir şekilde açıklamada bulunması halinde gerçekleşir. Bu tür bir yükümlülük 2003 tarihli Mahremiyet Düzenlemesi'nde bulunabilir[575]. Buna karşın Birleşik Devletler yaklaşımının avantajı, bu tür önemlerin –hem genel toplum hem de potansiyel spammerlar açısından– söz konusu işlemlerin suç olarak kabul edildiğini göstermesidir. Bununla birlikte politik kararlar ve hukuk uygulayıcılarının bilgi kaynaklarından çıkan sonuçlar bu tür aktivitelerle mücadele etmek için söz verimde bulunmaktadırlar[576].

SONUÇ

Bilişim suçları, hali hazırda mevcut olan ceza hukuku sistemine meydan okumaktadır. Hem suç tiplerinin tanımlandığı maddi ceza hukuku açısından hem de suçluların soruşturulması ve kovuşturulmasıyla ilgili usul kuralları açısından bu meydan okuma geçerlidir. Bu meydan okuma, kolluk güçlerinin ihtiyaçlarına layıkıyla yanıt verilebilmesi, suça maruz kalan mağdurların haklarının daha iyi korunabilmesi ve tüm toplumun suçtan korunabilmesi için, ceza hukuku sisteminin yeniden gözden geçirilmesini ve eklemeler yapılmasını gerektirir. İngiliz hukuku açısından bu konuda getirilen en önemli eleştiri bu alanda kuralların yeknesaklığını ve topluca bir arada bulunmasını sağlamak amacıyla uygun bir ceza kanunu yapılması gerekliliğidir[577].

Birleşik Krallık, bu eleştiriyi karşılamak için yukarıda incelemiş olduğumuz 1990 tarihli Bilgisayarların Kötüye Kullanılması Yasası'nı (Computer Misuse Act) yürülüğe koymuş, sonrasında değişen ve artan ihtiyaçlara göre bu yasada çeşitli değişiklikler yapmıştır. Bunun yanı sıra bilişim sistemleri suretiyle işlenen dolandırıcılık, sahtecilik, müstehcenlik, ekstrem pornografi, grooming

[575] 2003 tarihli Mahremiyet ve Elektronik İletişim Düzenlemesi (Privacy and Electronic Communications [EC Directive] Regulations 2003) (SI No 2426).
[576] Walden, pn. 3.359.
[577] Walden, pn. 2.289.

gibi suçlar için de bu suçların fiziksel alandaki karşılıklarının düzenlendiği yasalarda gerekli değişiklikleri yapmıştır. Ayrıca kişisel verilerin korunmasına ilişkin eylemleri de suç haline getirerek bununla ilgili yasada bu eylemleri ayrıca suç olarak düzenlemiştir. Bunların dışında Birleşik Krallık, Avrupa Siber Suçlar Sözleşmesi'nin de tarafı olarak, sözleşmenin yükümlülüklerini yerine getirmek amacıyla da yasalarında bilişim suçlarına ilişkin çeşitli değişiklikler yapmıştır.

Ancak görüldüğü üzere bilişim suçlarının tek bir yasada bütün halinde toplanması mümkün olmamıştır. Bunun önemli bir nedeni de Anglo Amerikan hukuk kültüründe bizde olduğu gibi yeknesak bir ceza kanununun bulunmayışıdır. Bizde yeknesak bir ceza kanunu olmasına rağmen yine de diğer kanunlarda ceza normları düzenleniyorken, Birleşik Krallık'ta bunun olmaması son derece olağandır. Birleşik Krallık'ta yeknesak bir model ceza kanunu tasarısı oluşturulmasına rağmen bu da başarılı olamamıştır. Dolayısıyla yakın gelecekte bilişim suçlarının tek bir çatı yasa altında düzenlenmesi beklenmemektedir.

İngiltere'de, yukarıda belirtmiş olduğum bilişim suçları hakkında, özellikle 90'lı yılların başından itibaren çok sayıda dava açılmış ve örnek kararlar verilmiştir. Anglo Amerikan ceza hukuku sisteminde kıyas ve genişletici yoruma izin verilmesi nedeniyle, mahkemelerin bu tür aktivitelere reaksiyonu ve yasaların (ve önceki mahkeme kararlarının) bu tür eylemlere uygulanarak faillerin cezalandırılması hızlı olmuştur. Ancak ülkemizde yaşanan bir sorun, aynen Birleşik Krallık için de geçerlidir: İspat. Yukarıda vermiş olduğum örnek kararlarda da görüldüğü üzere (özellikle *Caffrey* davası) deliller ne kadar güçlü olursa olsun, bunların yargılamayı yapan makam / karar veren organ tarafından anlaşılamaması halinde suçluların beraati ya da tam tersinine masumların mahkûmiyeti söz konusu olabilmektedir. Bunun önüne ancak uzmanlaşma ile geçilebileceği düşüncesindeyim.

İngiltere'de yasaların hazırlık ve yapım sürecinde Hukuk Komisyonu (Law Comission) önemli yetkilere ve etkiye sahiptir. Bu kurum, İngiltere'nin gerçek anlamda hukuk politikalarını oluşturmakta ve yasaların sosyal, kültürel, ekonomik, kriminolojik vb. gibi pek çok tarafını düşünerek raporlarını hazırlamaktadır. Parlemanto'nun her iki kanadı da (Avam ve Lordlar Kamarası) bu raporları dikkate ve ciddiye almaktadırlar.

İşte bu yalnızca bilişim hukuku ya da ceza hukuku değil, hukukun her disiplini açısından bizlere önemli dersler veren bir karşılaştırmalı hukuk çıktısıdır. Zira bu anlayış bizlere, yasaların günlük bir sorunu gidermek ya da belli bazı olaylara tepki vermek için değil, bu alanda düşünülüp taşınıldıktan sonra; sosyal, ekonomik, kültürel ve yönetimsel duyarlılıklar ve politikalar göz önünde bulundurularak yasa yapılması ya da yasada değişiklik yapılması gerekliliğini ve zorunluluğunu göstermektedir. Kısacası suç normları ve

karşılığında yaptırımlar konulurken, suç politikası ve bunun olumlu ve/veya olumsuz etkileri mutlaka dikkate alınmalıdır.

Ülkemiz açısından durumun böyle olduğunu söylemek ise son derece güçtür. En temel yasalar dahi bir sorun ortaya çıktığında (amiyane tabiriyle yumurta kapıya dayandığında) bu soruna bir tepki olarak çıkmaktadır. Dolayısıyla birçok temel yasamız dahi tepki yasası niteliğindedir. Dileğim bu durumun bir an önce değişmesidir.

KAYNAKÇA

Kitap ve Makaleler

Akdeniz, **Yaman,** "Section 3 of the Computer Misuse Act 1990 – An Antidote for Computer Viruses", Web Journal of Current Legal Issues, 1996.

Ashworth, **Andrew/Jeremy Horder,** Principles of Criminal Law, 7. Bası, Oxford, Oxford University Press, 2009.

Bainbridge, **David,** "Cannot Employees also be a Hackers?", Computer Law and Security Report, Vol. 13, No. 5, 1997, s. 352-354.

Barlow, **John Perry,** "Crime and Puzzlement: in Advance of the Law on the Electronic Frontier", Whole Earth Review, No. 68, Fall 1990, s. 44-57.

Battcock, **Rupert,** "Prosecutions under the Computer Misuse Act 1990", Computers and Law, Vol. 6, No. 6, 1996, s. 22-26.

Bonnici, **Jeanne Pia Mifsud,** Self-Regulation in Cyberspace, The Hague, TMC Asser Press, 2008.

Bowker, **Arthur L./Gregory B. Thompson,** "Computer Crime in the 21st Century and Its Effect on the Probation Officer", Federal Probation: A Journal of Correctional Philosophy and Practice, Vol. 65, No. 2, September 2001, s. 18-24.

Brenner, **Susan W.,** Cybercrime and the Law: Challanges Issues and Outcomes, Boston, Northwestern University, 2012.

Brenner, **Susan W.,** "Nanocrime?", University of Illinois Journal of Law, Technology and Policy, No. 1, 2011, s. 39-105.

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

Brenner, **Susan W.,** "Cybercrime Metrics: Old Wine, New Bottles?", Virginia Journal of Law and Technology, Vol. 9, No. 13, Fall 2004, s. 1-54.

Brenner, **Susan W. /Brian Carrier/Jef Henninger,** "The Trojan Horse Defense in Cybercrime Cases", Santa Clara Computer & High Technology Law Journal, Volume 21, Issue 1, 2004, s. 3-53.

Brunst, **Philip W.,** "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet", A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, Ed: Marianne Wade/Almir Maljević, Heilderberg, Springer, 2010, s. 51-80.

Clough, Jonathan, Principles of Cybercrime, Second Edition, Cambridge, Cambridge University Press, 2015.

Coppel, Philip, Informations Rights: Law and Practice, 4th Edition, Oxford & Portland, Hart Publishing, 2014.

Cusack, Carmen C., Pornography and yhe Criminal Justice System, Boca Raton, CRC Press, 2015.

DeKeseredy, **Walter S./Marilyn Corsianos,** Violance Against Women in Pornography, New York, Routledge, 2016.

Dressler, **Joshua,** Understanding Criminal Law, Sixth Edition, San Francisco, LexisNexis, 2012.

Dubber, **Markus D./Tatjana Hörnle,** Criminal Law: A Comparative Approach, Oxford, Oxford University Press, 2014.

Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, 6. Bası, Ankara, Seçkin Yayıncılık, 2015.

Dülger, **Murat Volkan,** "Hukuka Uygunluk Nedenleri ile Mazeret Nedenleri Arasındaki Ayrımın Tarihçesi, Niteliği ve Gerekliliği Üzerine Karşılaştırmalı Bir Deneme", Ceza Hukuku Dergisi, Y. 9, S. 24, Nisan 2014, s. 121-180.

Dülger, **Murat Volkan,** Suç Gelirlerinin Aklanmasına İlişkin Suçlar ve Yaptırımlar, Ankara, Seçkin Yayıncılık, 2011.

Dülger, **Murat Volkan,** "Teknolojideki ve Kitle İletişim Araçlarındaki Gelişmelerin Uluslararası Terörizme Etkileri", Hukuk ve Adalet Eleştirel Hukuk Dergisi, İstanbul, Y. 4 S. 8, Nisan 2007, s. 55–76.

Dyson, **Matthew/James Lee/Shona Wilson Stark (Ed),** Fifty Years of the Law Commissions: The Dynamics of Law Reform, Oxford and Oregon, Hurt Publishing, 2016.

Elliott, **Catherine/Frances Quinn,** English Legal System, Eleventh Edition, Harlow, Pearson Longman, 2010.

Elliott, **Catherine,** English Legal System Essential Cases and Materials, Second Edition, Harlow, Pearson Longman, 2009.

Fafinski, **Stefan/Emily Finch,** English Legal System, 3rd Edition, Harlow, Pearson Longman, 2010.

Fafinski, **Stephan,** "Computer Misuse: The Implications of the Police and Justice Act 2006", Journal of Criminal Law, Vol. 72, Issue 1, 2006, s. 53-66.

Fafinski, **Stephan,** "Access Denied: Computer Misuse on an Era of Technological Change" Journal of Criminal Law, Vol. 70, Issue 5, 2006, s. 424-442.

Fafinski, **Stefan,** "Divisional Court: Computer Misuse: Denial-of-Service Attacks" Journal of Criminal Law, Vol. 70, Issue 6, 2006, s. 474-478.

Fearon, **G.,** "All Party Internet (APIG) Report on the Computer Misuse Act", Comps. & Law, Vol. 15, 2004.

Freedman, C. D., "Criminal Misappropriation of Confidential Commercial Information and Cyberspace: Comments on the Issues", International Review of Law, Computers and Technology, Vol. 13, 1999.

Gillespie, **Alisdair A.,** Cybercrime: Key Issues and Debates, London and New York, Routledge, 2016.

Gillespie, **Alisdair A.,** The English Legal System, 5th Edition, Oxford, Oxford University Press, 2015.

Gillespie, **Alisdair A.,** Child Pornography: Law and Policy, London & New York, Routledge-Cavendish, 2012.

Gillespie, **Alisdair A.,** "Restricting Access to the Internet by Sex Offenders", International Journal of Law and Information Technology, Vol. 19, No. 3, 2011, s. 165-186.

Gillespie, **Alasdair A.,** "Child Protection on the Internet – challenges for Criminal Law", Child adn Family Law Quarterly, Vol. 14, No. 4, 2002, s. 411-425.

Goodman, **Marc D.,** "Why the Police Don't Care about Computer Crime", Harvard Journal of Law and Technology, Vol. 10, Number 3, Summer 1997, s. 465-494.

Grabosky, **Peter/Russell G. Smith/Gillian Dempsey,** Electronic Theft: Unlawful Acquisition in Cyberspace, Cambridge, Cambridge University Press, 2001.

Hafner, **Katie/John Markoff,** Cyberpunk: Outlaws and Hackers on the Computer Frontier, New York, Simon and Schuster, 1991.

Hessick, **Carissa Byrne (Ed),** Refining Child Pornography Law: Crime, Language and Social Consequances, Michigan, University of Michigan Press, 2016.

Hirst, **Michael,** Jurisdiction and the Ambit of the Criminal Law, Oxford, Oxford University Press, 2003.

Hodes, **W. William,** "Seeking the Truth versus Telling the Truth at the Boundaries of the Law: Misdirection, Lying, and 'Lying with an Explanation'", South Texas Law Review, Vol. 44, Winter 2002, s. 53-79.

Holder, **C.,** "Staying One Step Ahead of the Criminals", IT Law, Vol. 10, Issue 3, 2002, s. 17 vd.

Hollinger, **Richard C.,** Crime, Deviance and the Computer, Aldershot, Dartmouth Publishing, 1997.

Horder, **Jeremy,** "The Classification of Crimes and the Special Part of the Criminal Law", Defining Crimes Essays on The Special Part of the Criminal Law, Ed: R. A. Duff/Stuart P. Green, Oxford, Oxford University Press, 2005.

Hunton, **Paul,** "The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model", Computer Law and Security Report, Vol. 25, 2009, s. 528-535.

Kilger, **Max/Ofir Arkin/Jeff Stutzman,** "Profiling", in Honeynet Project, Know Your Enemy, Learning about Security Threats, 2nd edn, Addison-Wesley Professional, 2004.

Kerr, **Orin S.,** "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes", New York University Law Review, Vol. 78, 2003, s. 1596-1668.

Kohl, **Uta,** Jurisdiction and Internet: Regulatory Competence over Online Activity, Cambridge, Cambridge University Press, 2007.

Koops, **Bert-Jaap,** "Should ICT Regulation Be Technology-Neutral?", Ed: Bert-Jaap Koops/Miriam Lips/Corien Prins/Maurice Schellekers, Starting points for ICT Regulation: Deconstructing Prevalent Policy One-liners, IT & Law Series Vol. 9, The Hague, TMC Asser Press, 2006, s. 77-108.

Kowalski, **Melaine,** Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics, Cat. No. 85-558-XIE, Canadian Centre for Justice Statistics, 2002.

Kshetri, **Nir,** "The Simple Economics of Cybercrimes", IEEE Security and Privacy, Vol. 4, No. 1, January/February 2006, s. 8-13, (available at SSRN: http://ssrn.com/abstract=881421).

LaFave, **Wayne R.,** Criminal Law, Fourth Edition, St. Paul, Thomson & West, 2003.

Lessig, **Lawrence,** Code and other Laws of Cyberspace, New York, Basic Books, 1999.

Levi, **Michael,** "Between the Risk and the Reality Falls the Shadow", Crime and the Internet: Cybercrimes and Cyberfears, Ed: David S. Wall, London & New York, Routledge, 2001, s. 44-58.

Lixian, **Cong,** "Chinese E-Commerce (2) and Legal Environment", Chinese Intellectual Property and Technology Laws, Ed: Rohan Kariyawasam, Edward Elgar Publishing, 2011.

MacEwan, **Neil,** "The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future" Criminal Law Review, Vol. 12, 2008, s. 955-967.

Marsden, **Christopher T.,** Internet Co-Regulation: European Law Regulatory Governance and Legitimacy in Cyberspace, Cambridge, Cambridge University Press, 2011.

Martin, **Jacqueline,** English Legal System: Key Facts Key Cases, London and New York, Routledge, 2014.

Masiola, **Rosanna/Renato Tomei,** Law, Language and Translation From Concepts to Conflicts, Heidelberg, Springer, 2015.

McAlinden, **Anne-Marie,** 'Grooming' and the Sexsual Abuse of Children; Instituonal, Internet and Familial Dimensions, Oxford, Oxford University Press, 2012.

McKnight, **Gerald,** Computer Crime, Walker and Co., 1973.

Mitnick, Kevin D./William L. Simon, Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing, 2005.

Moore, **G. E.,** "Cramming More Components onto Integrated Circuits", Electronics, Vol. 38, No. 8, 1965, s. 114–117.

Morris, **Sheridan,** The Future of Netcrime Now: Part 1 – Threats and Challenges, Home Office Online Report 62/04, 2014.

Noam, **Eli M.,** "Beyond Liberalization II: The Impending Doom of Common Carriage", Telecommunications Policy, Vol. 18, No. 6, 1994, s. 435-452.

Ormerod, **David /David Perry,** Blackstone's Criminal Practice 2017, Oxford, Oxford University Press, 2016.

Ormerod, **David,** Smith & Hogan's Criminal Law, 13th Edition, Oxford, Oxford University Press, 2011.

Ormerod, **David /Simon McKay,** "Telephone Intercepts and their Admissibility", Criminal Law Review, January 2004, s. 15-38.

Parker, **Donn B.,** Crime by Computer, New York, Scribner, 1976.

Pieth, **Mark/Radha Ivory,** Corporate Criminal Liability: Emergence Convergence and Risk, Ius Gentium: Comparative Perspectives on Law and Justice 9, Heidelberg, Springer, 2011.

Pinto, **Amanda/Martin Evans,** Corporate Criminal Liability, Second Edition, Sweet & Maxwell, 2008.

Reed, **Chris,** Internet Law: Text and Materials, 2nd Edition, Cambridge, Cambridge University Press, 2004.

Reid, **A. S. /N. Ryder,** "The Case of Richard Tomlinson: The Spy Who E-mailed Me", Information and Communications Technology Law, Vol. 9, Issue 1, 2000, s. 61 vd.

Rosci, **Marco,** Cyber Operations and the Use of Force in International Law, Oxford, Oxford University Press, 2014.

Rowbottom, **Jacop,** "Obscenity Laws and the Internet: Targeting the Supply and Demand", Criminal Law Review, February 2006, s. 97-109.

Sieber, **Ulrich,** Legal Aspects of Computer – Related Crime in the Information Society - COMCRIME Study, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf; 25.11.2016.

Sieber, **Ulrich,** "Instruments of International Law: Against Terrorist Use of the Internet, A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications, Ed: Marianne Wade/Almir Maljević, Heilderberg, Springer, 2010, s. 171-220.

Simester, **Andrew /G. Robert Sullivan,** Criminal Law: Theory and Doctrine, Second Edition, Portland, Hart Publishing, 2004.

Spink, **Paul,** "Misuse of Police Computers", Juridical Review, Vol. 42, 1997, s. 219-231.

Stoll, **Cliff,** Cuckoo's Egg, New York, Pocket Books, 1998.

Thomas, **Douglas,** "Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker", Cybercrime: Law Enforcement, Security and Surveillance in the Information Age, Ed: Douglas Thomas/Brian D. Loader, London & New York, Routledge, 2000, s. 17-35.

Tomlinson, **Richard,** The Big Breach: From Top Secret to Maximum Security, Narodny Variant Publishers, Moskova, 2001.

Xu, **Zhengchuan /Qing Hua/ Chenghong Zhang,** "Why Computer Talents Become Computer Hackers", Communications of the ACM, Vol. 56, No. 4, 2013, s. 64-74.

Wagner, **Ben,** Global Free Expression – Governing the Boundaries of Internet Content, Law Governance and Technology Series, Vol. 28, Switzerland, Springer, 2016.

Walden, **Ian,** Computer Crimes and Digital Investigations, Second Edition, Oxford, Oxford University Press, 2016.

Walden, **Ian /Martin Wasik,** "The Internet: Access Denied Controlled!", Criminal Law Review, Issue 5, 2011, s. 377-387.

Walden, **Ian,** "Harmonising Computer Crime Laws in Europe", European Journal of Crime, Criminal Law and Criminal Justice, Vol. 12, Issue 4, 2004, s. 321-336.

Walker, **Claire,** "Email Interception and RIPA: the Court of Appeal Rules on the 'Right to Control' fence", Communications Law: Journal of Computer, Media & Telecommunication, Vol. 11, Issue 1, 2006.

Wall, **David S.,** Cybercrime: The Transformation of Crime in the Information Age, Cambridge, Polity Press, 2014.

Wall, **David S.,** Cyberspace Crime, London, Dartmouth, 2003.

Wall, **David S.,** "Policing the Internet: Maintaining Order and Law on the Cyber-beat", The Internet, Law and Society, Ed: Yaman Akdeniz/Clive Walker/ David Wall, Longman, 2000.

Wasik, **Martin,** Crime and the Computer, Oxford, Clarendon Press, 1991.

Wasik, Martin, "Law Reform Proposals on Computer Misuse", Criminal Law Review, 1989, s. 257-270.

Whittle, **Helen /Catherine Hamilton-Giachritsis/Anthony Beech/Guy Collings,** "A Review of Online Grooming: Characteristics and Concerns" Aggression and Violence Behaviour, Vol. 18, Issue 1, 2013, s. 62-70.

Willems, **Eddy,** Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können, Wiesbaden, Springer Vieweg, 2015.

Williams, D., Not in the Public Interest; the Problem of Security in Democracy, London, Hutchison, 1965.

Wright, **Tim /Dominic Hodgkinson,** "Government Response to House of Lords Science and Technology Committee Report on Personal Internet Security", Computer and Telecommunications Law Review, Vol. 14, 2008, s. 65 vd.

Rapor ve Haberler

Australian Communications and Media Authority, "Like, post, share: Young Australians' experience of social media", Quantitative Research Report, 2013.

Attorney General's Department (Australia), National plan to combat cybercrime, 2013.

Barrett, **Neil,** "Scary Whodunit Will Have Sequels" IT Week, 27 Ekim 2003.

Bird, **Steve,** "Lovelorn Hacker Sabotaged Network of U.S. Port", Times (UK), 7 Ekim 2003, s. 9.

Chapman, John, "The Nerdy Brit Who Paralysed a U.S. City", Express (UK), 7 Ekim 2003, s. 24.

Computer Crime and Intellectual Property Section, The National Information Infrastructure Protection Act of 1996, Legislative Analysis, US Depertmant of Justice, 1998.

CPS, Legal Guidance to Computer Misuse Act 1990, at "Section 3A CMA – Making, supplying or obtaining articles" http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/index. html, 2.10.2016.

Cullen, Drew, "Dutch Smash 100.000-Strong Zombie Army, DDoS Attacks and Paypal Fraud", The Register, 7 Ekim 2005, http://www.theregister.co.uk/2005/10/07/dutch_police_smash _zombie_network/, 23.9.2016.

Cummings, Roger, Director of the UK National Infrastructure Security Coordination Centre (NISCC) in Tom Espiner, "Foreign Powers are Main Cyberthreat, UK Says", CNET News.com, 23 Kasım 2005, http://www.cnet.com/au/news/foreign-powers-are-main-cyberthreat-u-k-says/, 27.9.2016.

DJNZ and The Action Tool Development Group of the Electrohippies Collective, "Client-side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?", The Electrohippies Collective, Occasional Paper No. 1, Şubat 2000.

Depertmant of Justice, "Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers", Press Release, 3 Kasım 2005, https://www.justice.gov/ archive/criminal/cybercrime/press-releases/2005/anchetaArrest.htm, 23.9.2016.

Europol, "Cybercriminal Darkode forum taken down through global action", Press Release, 15 Temmuz 2015, https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action, 1.10.2016.

Hancock, **David,** "Spammer gets 9 years", CBS News, 8 Nisan 2005, http://www.cbsnews.com/news/spammer-gets-9-years/, 6.10.2016.

House of Lords Science and Technology Report, Personal Internet Security, 2007.

Kotadia, **Munir,** "Accused Port Hacker Says Log Files Were 'Edited'", ZDNet.co.uk, 8 Ekim 2003, http://www.zone-h.org/news/id/3300?zh=1, 25.12.2016.

Krotoski, **Aleks,** "Population Explosion Puts Our Virtual Worlds at Risk", Guardian, 12 Ocak 2006, https://www.theguardian.com/technology/2006/jan/12/games.guardianweekly technologysection, 23.9.2016.

Law Commission, Legislating the Criminal Code: Misuse of Trade Secrets, Consultation Paper No 150, 1997.

Leyden, **John,** "Caffrey Acquittal a Setback for Cybercrime Prosecutions", Register, 17 Ekim 2003, http://www.theregister.co.uk/2003/10/17/caffrey_acquittal_a_setback/, 15.12.2016.

McCue, **Andy,** "'Revenge' Hack Downed US Port Systems", ZDNet UK, 7 Ekim 2003, http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/; 25.12.2016.

McGuire, **Mike/Samantha Dowling,** Cyber Crime: A Review of the Evidence, Research Report 75, Summary of Key Findings and Implications, Home Office, October 2013.

"Nurse Alters Hospital Prescriptions", Computer Fraud & Security Bulletin, Issue 2, 1994, s. 4-5.

Office of Telecommunications (Oftel), Guidelines for the Interconnection of Public Electronic Communication Networks, 23 Mayıs 2003.

Oxford English Dictionary Online, Oxford University Press, December 2014.

Purdy, **Alison,** "Hacker Cleared of Causing Biggest US Systems Crash", Birmingham Post, 18 Ekim 2003, s. 5, https://www.thefreelibrary.com/Hacker+cleared+of+causing+biggest+US +systems+crash.-a0109001502; 25.12.2016.

Schwartz, John, "Acquitted Man Says Virus Put Pornography on Computer", New York Times, 11 Ağustos 2003.

Turner, **Michael J. L.,** "Computer Misuse Act 1990 Cases" http://www.computerevidence.co.uk/ Cases/CMA.htm, 30.8.2016.

United Nations Office on Drugs and Crime, Comprehensive study on cybercrime, 2013.

US Department of Justice (DoJ), "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Press Release, 19 Mayıs 2014, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage, 1.1.2017.

US Sentencing Commission, Guidelines Manual (yürürlüğe giriş 1 Kasım 2015), s 2B1.1, bkz: http://www.ussc.gov/guidelines/2015-guidelines-manual/archive, 6.10.2016.

Vixie, **Paul/Gerry Sneeringer/Mark Schleifer,** "Events of 21 Oct 2002", 24 Kasım 2002, http://c.root-servers.org/october21.txt, 23.9.2016.

Ward, **Mark,** "Bookies suffer Online Onslaught", BBC News, 19 Mart 2004, http://news.bbc. co.uk/2/hi/technology/3549883.stm, 23.9.2016.

Webster, **Stephen/Julia Davidson/Antonia Bifulco/Petter Gottschalk/Vincenzo Caretti/Thierry Pham/Julie Grove-Hills,/Caroline Turley/Charlotte Tompkins/Stefano Ciulla/Vanessa Milazzo/Adriano Schimmenti/Giuseppe Craparo,** European Online Grooming Project, Final Report, European Commision Sefer Internet Plus Programme, Mart 2012.