

Ömer MENEKŞE (*)

“SİBER HIRSIZLIK” ÖRNEKLEMİNDE İSLAM HUKUKUNDA SİBER SUÇLAR VE CEZASI

Öz

Günümüzde internetin ve bilişim teknolojilerinin hızlı bir şekilde gelişip yaygınlaşması, bilişim sistemlerine yönelik işlenen suçların da artmasını ve suç işlenmenin kolaylaşmasını sağlamıştır.

Teknolojideki bu hızlı gelişim ve değişimlerden ceza hukuku da nasibini almış ve siber suç gibi internet ortamında işlenen suçların hükmü İslâm hukukçuları tarafından tartışılmaya başlanmıştır.

Bu makalede, her ne kadar klasik İslâm hukuku doktrininde bugünkü tabirle doğrudan “siber suç” veya bunu dolaylı olarak ifade eden bir başka kavram bulunmasa da, günümüzde ilmî, teknik ve teknolojik gelişmelerle ortaya çıkan bu problemi, modern hukukçuların yaklaşımlarını da değerlendirerek dinin temel ilke ve amaçları doğrultusunda çözümlenmeye çalışacağız.

Çalışmada öncelikle siber suçun tanımı, tarihsel gelişimi ele alınmış, siber suç türleri ve özellikleri incelenmiş, bilahare de “siber hırsızlık” örneğinde siber suçlara yönelik verilen cezalandırma sistemi irdelenmiş, İslam hukuku açısından günümüz mevzuatıyla bir karşılaştırma yapılmıştır.

anahtar kelimeler

İslâm Ceza Hukuku, İnternet, Siber Suçlar, Bilişim Suçları, Siber Hırsızlık, Bilgisayar

abstract

The Cyber Crimes and its Punishment in Islamic Law- in the “Cyber Theft” Sample-

The rapidly developing and spreading information technologies and the Internet today have led to an increase in crimes committed against information systems and made it easier to commit such crimes.

Criminal law has had its share of the rapid improvement and changes in technology and rulings on crimes committed on the Internet such as cybercrime have been debated by Islamic jurists.

Although there is no concept in classical Islamic law doctrine which directly or indirectly refers to “cybercrime” in modern terms, this paper will attempt to analyze this problem, which has emerged following scientific, technical, and technological developments, in line with the fundamental principles and purposes of religion by also evaluating approaches from modern scholars of law.

The paper initially covers the definition and historical development of cybercrimes; it analyzes types and characteristics of cybercrime. Subsequently, in the “cyber theft” sample, it examines the system of penalties imposed for cybercrimes and draws a comparison with modern regulation in terms of Islamic law.

keywords

Islamic Criminal Law, Internet, Cyber Crimes, IT Crimes, Cyber Theft, Computer

Giriş

İletişim ve teknolojinin insana tanıdığı imkânlarla modern dünyanın küresel boyutta büyük bir dönüşüm yaşadığı günümüzde, bilgisayar teknolojisinde yaşanan gelişmeler ve internet kullanımının hızla yaygınlaşması ile birlikte hem yeni suç tipleri hem de geleneksel suçların farklı işleniş biçimleri ortaya çıkmış, elektronik ortam birçok suç türünün işlendiği bir alan haline gelmiştir. (Bir iletişim vasıtası olarak interneti kullanmanın dinî/fıkhî hükmü ile ilgili bkz. Abdurrahman b. Abdullah es-Sened, 2004:98-104; Muhd Rosydi-Marjan, 2003: 634) Böylelikle birçok internet kullanıcısı da mağduriyet yaşayarak bilmeden adli bir konunun tarafı olmuş, suçtan zarar gören bir mağdur iken kendi kimlik/ kullanıcı bilgileri ile adeta suç işleyen veya suça aracılık eden konumuna düşmüştür. (Murat Önok, 2013: 1230; Berrin Akbulut, 2000: 547-548; Musa Sürer, 2014: 1; Abdi O. Shuriye-Masud T. Ajala, 2014: 517)

İnterneti iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanan kullanıcıların varlığına karşılık; intikam alma duygusu, güce sahip olma, aç gözlülük, şehvet, macera gibi bireyleri suç işlemeye götüren nedenlerle hareket eden, sabotaj veya kargaşa yaratmak amacıyla çeşitli sistemlerin açıklarını bularak bu sistemlere atak yapan ve sisteme izinsiz girerek çeşitli hasarlar yaratan “hackerların” (işletim sistemlerinde mevcut olan güvenlik açıklarını tespit edip bu açıkları kullanarak sisteme yetkisiz giriş yapan kişi, bilişim korsanı. Bkz. Murat Volkan Dülger, 2004: 72; Oğuz Turhan, 2006: 62) ortaya çıkması, bilişim teknolojilerinden faydalanarak internetteki yerini almak isteyen “terör örgütleri”nin faaliyetlerini bu ortama taşınması, “hırsızlık” ve “dolandırıcılık” gibi suçların bu ortamda işlenmeye başlanması, internette izinsiz yayınlanan film, müzik ve oyunların oluşturduğu “lisans hakları ihlalleri” şeklindeki suçların genişlemesi, hakaret amaçlı sitelerin kurulması, pornografik yayınların giderek artması, internetin kötü amaçla kullanılabilceğini açıkça gözler önüne sermiştir. (Turhan, 2006: 1; Sezen Yeşil-Mustafa Alkan, 2007: 132.)

İşte bu çalışmada da, gelişen teknolojinin doğurduğu hukuki sorunlardan biri olan internet ortamında işlenen siber suçlar üzerinde durulacak; bu kapsamda dinî perspektiften incelenmesini zaruri gördüğümüz siber suç olgusunun “siber hırsızlık” örneğinde fikhî açıdan bir değerlendirmesi yapılacaktır.

Şüphesiz İslam hukuku alanında bilişim hukuku ve siber suç konusunu ele alan çalışmaların literatürde yeni yeni zuhur etmeye başladığı söylenebilir. Öyle ki Bahreyn Üniversitesi Bilişim Uzmanı Dr. Mansur el-Âlî, bir makalesinde literatürde e-ticaret suçları ve İslam temalı iki makalenin (Norazlina , Fauziah , & Siti Hartini , 2004; Mancuso, 2007) dışında İslam hukuku ve bilişim teknolojileri alanında yapılmış çalışmalara pek rastlanmadığını belirtmektedir. (Al-A'ali , 2007) Ancak son yıllarda hızla gelişen bilim ve teknoloji alanındaki gelişmelere de bağlı olarak İslam hukuku bağlamında siber suçlara yönelik kaleme alınan tez, kitap, makale vb. türdeki eserlerin sayısında bir artış görülmektedir. Nitekim üretilen bu çalışmalar, bilişim suçlarının fikhî boyutunu irdelemekte, buna yönelik çağdaş yaklaşımları, bilgi görüş ve fetvaları serdetmektedir. (Örnek olarak bkz. Sagir, 2013; Suveyr, 2011; el-Halife, 2004; Maghaireh, 2008; Illar, 2010)

Bu itibarla önemli, gittikçe de önemi artan bu konu ülkemizde de henüz yeterli ilgiyi görmüş değildir. Bilebildiğimiz kadarıyla müstakil bir çalışmaya da konu edilmemiştir. İşte bu bağlamda biz, bilişim sistemlerinin bilfiil içinde olan biri de olarak, siber suçlar meselesini hem teknik düzeyde tanımaya çalışacak hem de fikhî bir tahlile tabi tutmaya gayret edeceğiz.

I. SİBER SUÇLAR

A. Terminoloji, Terim ve Tanım Sorunu

Ceza hukuku açısından, -suçun unsurları itibarı ile açık ve seçik olması, tipiklik unsurunun gereğince tebarüz ettirilmesi ve kanunilik ilkesinin belirsiz ve muğlak ifadelerle geniş bir kısıtlamaya tabi tutulmaması amaçları doğrultusunda iyi ifade edilmiş, sınırları belirlenmiş bir tanım yapılması önemlidir.

Siber suçlar gibi hukukun alanına yeni dâhil olmuş, henüz yeterince işlenmemiş, tam anlamıyla henüz sınırları belirlenememiş teknik bir olgunun da tanımlanıp kurumsallaşabilmesi için multi-disipliner bir yaklaşım içerisinde ilgili alanların uzmanlarınca ortak bir çalışma yapılması, olgunun aydınlatılması, sınırlarının net bir şekilde anlaşılması ve her şeyden önce tanımlama kriterlerinin ortaya konulması gerekmektedir. (Eker, 2006:102-103)

Nitekim bilişim sistemlerinin yaygınlaşması ile birlikte ceza hukuku alanında, bu sistemlerin kötüye kullanımına ilişkin fiillerin cezalandırılabilirliği konusu gündeme gelmiş, son dönem ceza kanunlarının hene hemen hepsinde bilişim suçları dolayısıyla siber suçlarla ilgili birçok tanım yapılmış ve bu tanımları ifade etmek üzere de birçok kıstas ortaya konmuştur. (Ketizmen, 2008; Söz konusu kıstaslarla ilgili geniş bilgi için de bkz. Dülger, 2004: 66-67; Berrin Akbulut, 1999: 36-42; (Değirmenci, 2002: 56-58) Ancak ne var ki üzerinde uzlaşma sağlanmış genel bir tanım henüz ortaya çıkmış değildir.

Tanımlama sorunu aynı zamanda bu olgunun yeniliğinin yanı sıra bilişim teknolojilerinin sürekli bir değişim, dönüşüm ve gelişme içerisinde bulunması ve dolayısıyla her geçen gün bir yeniliğin ve var olan teknolojilerin farklı, değiştirilmiş/dönüştürülmüş biçimlerinin gündeme gelmesi gibi sebeplerden kaynaklanmaktadır. Böylece kanun koyucular siber suçları kesin sınırlar çerçevesinde tanımlamaktan çekinmişlerdir. Yapılan tanımlar ise sıklıkla genellemeler, tasvirler düzeyinde bırakılarak bilişim teknolojilerinde yakın gelecekte gerçekleştirilecek yeniliklere açık hâle getirilmeye çalışılmıştır. (Eker, 2006:102-103)

Tanımlama hususundaki bir başka sorun da söz konusu olgunun adı açısından çıkmaktadır. Nitekim olguyu adlandırma çabalarında farklı isimlerin gündeme geldiği görülmektedir. Öyle ki bu kapsamda bilişim ortamında işlenen suçları belirtmek için "*bilgisayar suçları*" (computer crimes), (Tiedemann, 1975:319; Erem, 1991) "*bilgisayarla ilgili suç*" (computer-related crime), (Dursun, 1998; Yazıcıoğlu, 1997: 126) "*bilgisayar ihlalleri*" (computer abuse), (Yazıcıoğlu, 1997: 126-128.) "*yüksek teknoloji suçları*" (high-tech crimes), (Turhan, 2006: 28) "*internet suçları*" (internet crimes) (Örnek olarak bkz. Özbek, 2002: 106-107, — yazar "internet suçları" ifadesini tercih etmektedir; Yenisey, 2002: 447; Sinar, 2001: 129; Tanılır, 2002: 1) "*bilişim suçları*" (computer crimes) (Ör-

nek olarak bkz. Dülger, 2004; Karagülmez, 2011; Yenidünya & Olgun, 2003; Akbulut B. , 1999; Ketizmen, 2008) gibi kavramlar kullanılmaktadır. (Karagülmez, 2011:44; Pocar, 2004)

Arapça yazılan çağdaş İslam hukuku eserlerinde de söz konusu suçlar; “*Cerâimü’l-Kemputer ve’l-İnternet*”, “*el-Cerîmetü’l-Elektroniyye*”, “*el-Cerâimü’l-Ma’lûmatiyye*”, “*Cerâimü’l-hâsibi’l-âli*”, “*el-Cerîmetü’s-Saybiriyye*”, “*Cerâimü’t-Takniyyeti’l-âliye*” vb. adlarla anılmaktadır. (Sagir, 2013: 7; https://ar.wikipedia.org/wiki/جريمة_الالكترونية; <http://www.startimes.com/?t=33677893>; Minşavi, 1423)

Kavramlardaki bu çeşitlilik ve kavramların çoğunda geçen bilgisayar terimi, internetin günümüzdeki gibi etkin olarak kullanılmadığı dönemlerde suçluluğun bilgisayar ve ona bağlı sistemler yolu ile ortaya çıkmasından kaynaklanmaktadır. İnternet kullanımının yaygınlaşmasıyla birlikte, bilgisayar aracılığıyla işlenen suçlar yeni gelişmelere ayak uydurmuş ve gelişen teknoloji ve sağladığı imkanlar sayesinde oluşan yeni yarar sahalarına eş olarak, yeni ihlal tipleri ortaya çıkmıştır. Bu da beraberinde bütün ihlalleri tek bir kavram altında toplama ihtiyacını doğurmuştur. (Turhan, 2006:29) Nitekim bu ihtiyaca binaen uluslararası hukukta “siber uzay ortamında işlenen suç” anlamında “cybercrime” denilen, ülkemizde ilk olarak “sanal suç” olarak isimlendirilen “siber suç” terimi, daha sonra uluslararası kullanıma paralel olarak bilişim teknolojileri ile işlenen suçlar için kullanılmaya başlanmıştır. (Turhan, 2006:181; Yetim, 2014:183; Ergün, 2008: 14; Zakir & Gürsel, 2010: 47)

Dünyadaki pek çok devlet tarafından temel kabul edilen düzenlemelerden biri olarak Avrupa Konseyi Siber Suç Sözleşmesi’nin adına uygun olması ve uluslararası hukukta ve literatürde yaygın olarak kullanılması nedeniyle “siber suç” ifadesi bu çalışmada da kavramsal olarak tercih edilmiştir.

Siber suçların niteliği ve tanımı konusunda farklı tarifler yapılmakta ve ortaya birbirinden farklı tanımlar çıkmaktadır. Özellikle bir taraftan gelişen teknoloji karşısında bilgisayar suçlarındaki teknik ve yöntemlerin sürekli nitelik ve şekil değiştirmesi, diğer taraftan konunun hem hukuki hem de cezai yanının bulunması herkesin üzerinde birleşeceği bir tanım yapılmasını zorlaştırmaktadır. Ancak konuya ilişkin yapılan tanımlar ne kadar çeşitli olursa olsun temelde dar alandan geniş alana uzanan iki farklı yaklaşım bulunmaktadır:

Buna göre dar anlamda siber suçlar, bilgisayar sisteminin güvenliğini veya veri işlemini hedef alan, bilgisayar teknolojisini bilen ve bunu uygulayan kişilerin gerçekleştirdikleri istismar eylemleri olarak tanımlanırken; (Brenner, 2001:3; Turhan, 2006:33; Yücel, 1992: 506; (Tulum, 2006: 21. Ayrıca bkz. Sagir, 2013: 12; Suveyr, 2011:13; el-Beâdî, 2012: 5) geniş anlamda ise bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış olarak ta-

nımlanmaktadır. (Yücel, 1992: 505; Dülger, 2004: 38; Kurt, 2005:50; el-Beâdî, 2012: 5; Sagir, 2013:13)

Siber suçların, sadece bilgisayar ve veriye yönelik fiilleri esas almadığı, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşması ile birlikte çeşitlilik arz ettiği görülmektedir. Veri hırsızlığı ve tahribinden elektronik sabotaja; bilişim sistem ağları vasıtasıyla dolandırıcılıktan emniyeti suiistimale; hakaret ve tehditten kalpazanlığa; telif hakları, para, mal ve hizmet hırsızlığından bilgisayar sahteciliğine kadar varabilen çeşitli suçlar işlenebilmektedir. (Dursun, 1998:336; Ketizmen, 2008: 61; Brenner, 2001:9-26; Yıldız, 2007: 617)

Görüldüğü üzere siber suçların işlenmesinde suç aleti olarak ya doğrudan bilgisayar ve network sistemleri kullanılmakta ya da bizzat bilgisayara yönelik bir saldırı olmaktadır.

Ancak şunu da belirtmek gerekir ki, bilgisayarın kullanıldığı her suç siber suç olmayabilir. Zira bilgisayar siber faaliyetlerin gerçekleştirilmesinde kullanılan bir araçtır. Nitekim hırsızlık, banka soygunu veya başka herhangi bir suç işlenirken, faillerin aralarındaki iletişimi bilgisayar yoluyla sağlaması, bilgisayarın CPU veya herhangi bir bileşenini maddi zarar kastıyla tahrip ederek bilgisayar ve bilgisayar sistemine saldırı yapılması vb. durumlarda bir siber suçtan söz etmek mümkün değildir.

Yukarıda belirtilen hususlar doğrultusunda, siber suçun tanımı konusunda hukuki doktrinde ortaya çıkan farklılıkların, aslında temel alınan kıstas ve bu tür suçlara yönelik genel bakış açısından kaynaklandığını ifade etmek mümkündür.

Nihayetinde ana-hatlarıyla, kapsayıcı ve karma bir tanım yapılmaya çalışılırsa, siber suç; bilgisayar teknolojilerinin kötüye kullanıldığı, ulusal ve kamu güvenliğinin tehlikeye düşürüldüğü, bireyin esenlik ve ahlaki değerlerinin tehdit edildiği bir suç türüdür. (Yetim, 2014:183)

Bu suçun işlenme yeri; bilgisayar ve yan teknolojilerinin birbirleri ile bağlantıları ve haberleşmeleri sırasında oluşturdukları sanal alandır.

B. Siber Suçların Özellikleri

Suçta elverişli bir ortam olarak internetin gelişmesiyle siber suçların işlenmesi hem kolaylaşmış hem de işleniş biçimleri çeşitlenmiştir. (Akbulut B. B., 2000: 551; Eker, 2006: 106; el-Halife, 2004:43)

Nitekim siber suçları geleneksel suç tiplerinden ayıran ve kendine özgü suçlar olmasını sağlayan en önemli özellik; klasik suç tiplerinde suçun maddi unsurlarını oluşturan eylemler, faillerin fiziki hareketleriyle meydana gelmekte iken siber suçlarda genellikle failin bir bilgisayar klavyesine dokunması veya

fareyi tıklaması dışında başkaca bir fiziki hareket olmamakta, suçun neticesinde ise fiziki hareketlerle meydana getirilebilecek zararlardan çok daha fazlası oluşabilmektedir. (Dülger, 2004:69; Ergün, 2008:16)

Siber suçlar; cinayet, uyuşturucu, silahlı soygun ve gasp suçlarında olduğu gibi suç aleti ve şiddet kullanımı gerektirmez. Örneğin, verilerin illegal yollarla bir bilgisayardan bir diğerine aktarılması veya banka hesaplarının elektronik ortamda soyulması gibi suçlar herhangi bir şiddet kullanımı veya güvenlik güçleriyle silahlı çatışmaya girilmesini gerektirmemektedir. (en-Neccar, 2009: 19)

Siber suçlar, bilinen usullerin dışında çok daha hızlı ve kolay işlenebilmekte, fail ile mağdur arasında mekânsal bir mesafe, sınır aşan bir boyut bulunması sebebiyle (Önok, 2013: 1234; Ergün, 2008:44; Karagülmez, 2011:380; Brenner, 2001:23; Gercke, 2011:134.) çoğu zaman mağdurun fark edemeyeceği ve varlığını bilemeyeceği çok çeşitli ve gizli biçimlerde görülmekte, (en-Neccar, 2009:18-19; el-Halife, 2004:43; el-Beâdî, 2012:43; Yazıcıoğlu, 1997:150) hem de parmak izi ve fiziksel etkiler gibi klasik suç izleri taşımaması, arkalarında bulunması çok zor, silik ipuçları bırakması sebebiyle de suçlunun kimliğinin ve suç alanının tespit edilmesi, fail belirlense bile yakalanması, fail yakalansa bile kişinin uğradığı zararın veya suça konu zararlı içeriğin web ortamından tamamen kaldırılması, alınan veya yayılmış üçüncü dördüncü taraflardaki kopyaların silinmesi, yok edilmesi daha zor olmaktadır. (Akbulut B. , 1999:551; Değirmenci, 2002:75; Özcan, 2004: 326-327; Turhan, 2006: 47; Ergün, 2008:43; Suveyr, 2011: 12; el-Beâdî, 2012: 17; Sagir, 2013: 9; Sürer, 2014: 9)

Siber suçta ortaya çıkarmaya yarayacak delillerin türü ve formatı (Grabosky, 2007: 213), bir de bunları elde etme yöntemleri geleneksel suçlara nazaran farklıdır. (Özen & Baştürk, 2011:91)

Siber suçları diğer suçlardan ayıran temel özelliklerden birisi, toplanan delillerin klasik delil yerine daha çok dijital delil olmasıdır. Her ne kadar siber suçlarda da parmak izi tespiti, DNA testi yapma, olay yeri inceleme gibi eskiden beri var olan klasik deliller ve delil toplama yöntemleri kullanılsa da siber suçlar açısından bu deliller yan deliller olarak değerlendirilmekte, esaslı ve önemli deliller her zaman için dijital deliller olmaktadır. (Yetim, 2014:184; Al-A'ali , 2007)

Siber suç delillerinin “adli bilişim” adı verilen “potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan” uygulamalarla ortaya konması, dijital delillerin derlenip adli makamlara sunulması, korunması; bu suçları soruşturacak personelin çok ciddi bir uzmanlığa sahip olmasını gerektirmektedir. (Uçkan & Beceni, 2004: 423; Önok, 2013:1235; Tulum, 2006:95-97)

Siber suçlarda, çok az masraf ve gayretle, çok büyük zarar vermek mümkün olabilmektedir. (Broadhurst, 2006: 410; Özcan, 2004: 329. Geleneksel suçluluğa nazaran bu özelliğin yarattığı neticeler açısından bkz. Brenner S. W., 2004: 10 vd.)

Siber suçların ekonomik sonuçları, gerek birtakım programların çalınması veya yok edilmesi, veritabanının çökmesi, gerekse kredi kartı dolandırıcılığı, banka hesaplarının boşaltılması vb. olsun, çoğu zaman ağır zararlar biçiminde olmakta, oluşan zararlar ve artan güvenlik harcamaları milyarlarca doları bulabilmektedir. (Tulum, 2006:54-55; Ayrıca Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS) tarafından yapılan ve siber suçların dünya ekonomisine zararının 400 milyar dolardan fazla olduğunu ortaya koyan araştırma için bkz. “Net Losses:Estimating the Global Cost of Cybercrime”, Economic Impact Of Cybercrime II, Center for Strategic and International Studies, 2014, s. 2. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>)

Elektronik ortamda işlenen çocuk pornografisi, cinsel istismar, taciz, şantaj gibi ahlak suçlarında görüldüğü gibi, manevi zararlar da söz konusu olabilmektedir. (Turhan, 2006: 109; Ahlak suçları hakkında daha fazla bilgi için bkz. (Kutub, 2013:2 vd. ; Özkan, 2011)

Günümüzde işlenmekte olan siber suçların çoğu genellikle internet aracılığıyla gerçekleştirilmektedir. Gerek bilgisayar korsanlarının (hacker) yetkisiz giriş eylemleri yahut sistem kırıcıların (cracker) sisteme kötü niyetle sızarak verilere zarar vermeleri veya verileri değiştirmeleri gerekse de zararlı ve casus programlar (spyware, vandalware: virüs, truva atı, solucan, mantık bombası, istem dışı alınan elektronik postalar (spam), bilgi ve veri aldatmacası (data diddling) vs. vasıtasıyla girilen eylemler siber suçların önemli, sık rastlanan örneklerini teşkil etmektedir. (Siber suç işleme yöntemleri (modus operandi) ile ilgili geniş bilgi için bkz. (ed. Çakır & Kılıç, *Güncel Tehdit: Siber Suçlar*,(2014): 27-35; Turhan, 2006: 47-57; Nacar, 2010: 8-11; Pallı, 2008: 52-67;)

C. Siber Suç Türleri ve Nitelikleri

Siber suçların tasnifine ilişkin farklı yaklaşımlar bulunmaktadır. (Ulusal doktrinde siber suçların tasnifi için bkz. Yazıcıoğlu, 1997:143 vd.; Özcan, 2004: 305-307; Ergün, 2008: 27 vd.; Özen & Baştürk, 2011:90) Literatüre bakıldığında “bilgisayar sistemleri vasıtasıyla işlenen klasik suçlar” ve “bilgisayar sistemlerine yönelik suçlar” şeklindeki (Karagülmez, 2011:44; İnanıcı, 1996:514) genel tasnifin yanında, verilere yönelik suçlar (verilerin durdurulması, değiştirilmesi, hırsızlığı), bilişim ağlarına yönelik suçlar (bilişim sisteminin işlevlerini yerine getirmesinin engellenmesi) ve sanal tecavüz (Ergün, 2008: 29-31; en-Neccar,

2009: 23) şeklindeki sınıflandırmaya ve biraz daha detaylı olarak “kimlik hırsızlığı,” “çevrim içi taciz,” “yetkisiz ve izinsiz erişim,” “dolandırıcılık” ve “verilere yönelik suçlar” şeklinde (Çakır & Kılıç, 2014: 22-26) tasniflere rastlamak mümkündür.

Tasniflerdeki bu farklılık, bir yönüyle teknolojinin sürekli gelişmesine ve her geçen gün biraz daha fazla insan hayatına girmesine, bunun sonucunda yeni ihlal tiplerinin ortaya çıkmasına, dolayısıyla sabit bir ayırım yapılmasının zorluğuna diğer yönüyle de yapılacak tasnifin kullanım amacına bağlanılabilir.

Nitekim Avrupa Konseyi Siber Suç Sözleşmesi’ne göre siber suçlar; bilgisayar veri sistemlerinin gizliliği, bütünlüğü ve kullanımına ilişkin suçlar,(yasadışı erişim, verilere ve sistemlere müdahale) bilgisayarlarla ilişkili suçlar,(sanal sahtecilik ve dolandırıcılık) içerik itibarıyla suçlar (cinsel istismar) ve fikri mülkiyet haklarının ihlali ile ilgili suçlar şeklinde sınıflandırılmıştır. (Şehitoğlu, 2005: 31; (Özkan T. , 2006: 69-70; Nacar, 2010: 12-13; (<http://conventions.coe.int/treaty/en/treaties/html/185.htm>, 2001)

Diğer bir görüşe göre siber suçları beş grup altında toplamak mümkündür: (Yazıcıoğlu, 1997:150; (Kurt, 2005: 69; ; (Türkî, 2011:29; (el-Beâdî, 2012: 6)

1. Bilgisayar sistem ve ağlarına hakkı olmadan girmek,
2. Hak sahibinin izni olmaksızın konulmuş olan emniyet tedbirlerini aşmak suretiyle bilgisayar veri ve programları silmek, bozmak, yok etmek,
3. Bilgisayarların işlemlerini engellemek amacıyla bilgisayar ve sistemlerini tahrip etmek, silmek.
4. Hukuk dışı olarak iletişime müdahale etmek,
5. Menfaat temin etmek için ticari sırları izin almadan veya hukuken bir hak olmaksızın ifşa etmek veya tevzi etmek.

Başka bir görüşe ise Siber suçlar; (Sagir, 2013: 44-54)

1. Mala yönelik işlenen suçlar, (dolandırıcılık, sahtecilik veya zimmete para geçirilmesi, bilişim sistemine girme, engelleme, bozma, verileri yok etme veya değiştirme, fikri mülkiyet hakkı ihlalleri, siber kumar ve bahisler vb.) (Bkz. el-Mehami, 2002:11-12; Suveyr, 2011:32-33; el-Halife, 2004:43; Sagir, 2013:44-49; Ergün, 2008: 39-40. Ayrıca bkz. Kocabey, 2004: 35-70; Murat Yılmaz, 2005)
2. Kişilere yönelik işlenen suçlar, (özel hayatın gizliliğini ihlal, kimlik hırsızlığı, hakaret, iftira vb.) (Geniş Bilgi için bkz. Civelek, 2011; Zorlu, 2010; Karimi & Korkmaz, 2013; Suveyr, 2011: 32-33; Ergün, 2008: 57-74)
3. Devlet ve kamu düzenine karşı işlenen suçlar (internet üzerinden yayınlar yapan, fon transferleri gerçekleştiren organize terör suçları vb.) (Beceni, 2007; Sagir, 2013: 54-59)

II. SİBER HIRSIZLIK SUÇU

Suç işleme niyetindeki bazı birey ve grupların teknolojiyi hem araç hem de hedef olarak kullanması; siber suçların günümüz modern toplumlarının önemli sorunlarından biri haline gelmesini sağlamış, bu ise siber suçların cezalandırılmasına ilişkin farklı şekillerde de olsa hukuk ve ceza mevzuatlarında düzenlemeler yapılmasına, çeşitli şekillerde cezai müeyyideler ortaya konmasına neden olmuştur.

Nitekim Suudi Arabistan, İran, Pakistan, Birleşik Arap Emirlikleri, Umman gibi birçok İslam ülkesi de siber suçları İslami bir bakış açısıyla hukuki mevzuatlarında ele almıştır. (En-Naim, 2013; Sajedi & Ariani, 2014; Aldurra, 2013; Crystal, 2001; Maghaireh, 2008)

Hukuk sistemlerinin bu konuya ilişkin ilgili suçlara öngördüğü cezalar farklılık arz ettiği için biz bu araştırmamızda önce siber hırsızlık örnekleminde modern hukukta öngörülen cezaları, daha sonra da İslam hukukçularının takdir ettiği cezaları ele almak istiyoruz. Hangi davranışın suç sayıldığını doğru tespit edebilmek için de suçun tanım ve unsurlarını kısaca hatırlatmakta fayda görüyoruz.

A. SUÇUN TANIMI VE MAHİYETİ

Siber hırsızlık; bir bütün olarak, siber uzay ortamının kullanılması yoluyla gerçekleştirilen bilgi hırsızlığı, -bilgisayar yazılımlarını da kapsar biçimde- para veya mal hırsızlığı ile hizmet hırsızlığı fiillerini de içine alan mülkiyete karşı işlenmiş suçlardandır. (Brenner W. , 2001:9-10; Sınar, 2001:71; eş-Şeşrî, 2012: 34)

Temelde “hırsızlık suçu”, kişinin mülkiyet hakkına yapılan haksız bir fiildir. Bu fiil ile başkasına ait taşınabilir bir mal, sahibinin rızası olmaksızın faydalanmak kastı ile bulunduğu yerden alınmakta, dolayısıyla kişinin malvarlığında bir azalma gerçekleşirken, fail, kendisi veya bir başkası lehine haksız bir yarar, zenginleşme sağlamaktadır. (Eker H. , 2014: 10-12; 5237 sayılı Türk Ceza Kanunu, 141. maddede, hırsızlığı, bir kimsenin “*zilyedinin rızası olmadan, başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla, bulunduğu yerden alması*” olarak tanımlamaktadır. (Bkz. Ekinci & Esen, 2005:4) İslam hukukunda da hırsızlık; “*başkasına ait bir malın mülk edinme kasdıyla muhafaza edildiği yerden gizlice alınması*” şeklinde tanımlanmaktadır. (Bkz.. İbnü'l-Hümmam, ty.: V, 354; İbn Nüceym, 1311: V,154; Bilmen, 1985: III, 261; Züreyr, 1980:4; Bardakoğlu, 1998:385; Menekşe, 1998: 20)

Nitekim siber hırsızlık da klasik suçların neden olduğu zararların yanısıra ayrıca ciddi ekonomik zararlara yol açmakta ve bireysel bilgi hakkına zarar vermektedir.

Geçmişte hırsızlığa konu olarak sadece fiziksel özellik taşıyan mallar (ayn) ele alınırken, günümüzde teknolojinin gelişmesiyle birlikte bu durum daha da değişmiştir. Artık insanlar bilişim sistemlerini kullanarak alışveriş yapmakta, kişi veya kurumlar arasında çeşitli bilgi, kaynak ve para transferleri gerçekleştirmektedir. Ayrıca fertler veya çeşitli kurum ve kuruluşlar, iktisadi değeri yüksek olan ve kendileri için hayati önem arz eden birçok bilgi, tasarım ve programlarını sanal ortamlarda gizlemektedir. Gayrı meşru yollardan bu bilgi, tasarım ve programlardan faydalanmak isteyenler, çeşitli yollarla güvenlik sistemlerini aşmakta ve sahibinin rızası hilafına bu bilgi veya programları çalabilmektedir.

Nitekim günümüz bankaları ve finans kurumları, kişisel verilerin gizliliğinin korunması ve finansal işlemlerin internet üzerinde güvenli bir şekilde gerçekleştirilmesi, internet bankacılığında yapılan işlemlerin, işleme taraf olmayan üçüncü kişilerin eline geçmemesi ve bilgi transferinin güvenli bir şekilde yapılması için Elektronik Kimlik Belgesi, SET (Güvenli Elektronik İşlemler Protokolü), SSL (Güvenli Yuva Katmanı Protokolü) ve Elektronik imza gibi elektronik güvenlik sistemleri kullanarak mudi ve hissedarlardan oluşan banka müşterilerine ait varlıkları korumaya çalışmaktadır. (Çakır & Kılıç, 2014:98) Bu sistemlerin mümkün olan en güvenli sistemler olduğu ve itibarlarını korumak ve sızmalar karşısında meydana gelebilecek korkunç zararlardan korunmak maksadıyla, gerekli güvenlik önlemlerinin alındığı ve sürekli güncellendiği de varsayılmaktadır.

Ancak alınan tüm bu güvenlik tedbirlerine rağmen bankaların bilgi sistemlerine yine de sızmalar gerçekleşmektedir. Sızmalar, kötücül (malware) ve casus (spyware) yazılımlar (keylogger, Screenlogger, spyware vb.), istenilmeyen e-posta (spam) ve oltalama (phishing), yemleme, (pharming) gibi metodlarla yapılmaktadır. (Baş, 2015:33; Eralp, 2012:69-93)

Ağa bağlı bir bankanın bilişim sistemine girilerek kredi kartı şifrelerinin çalınması, haksız olarak elde edilen banka kartı ve şifresi ile ATM’den para çekilmesi, mudilere ait banka hesaplarının failin kendisine veya bir başka hesaba aktarılması gibi suçların sonuçları, adi hırsızlık suçlarının sonuçlarından farklıdır. Hatta daha zararlı, daha tehlikeli ve mücadele edilmesi daha da zordur. (Ergün, 2008: 125-126)

B. Siber Hırsızlık Çeşitleri

Siber hırsızlık suçları çok çeşitlilik arz etmektedir. Zimmete geçirmeden endüstri casusluğuna; intihal/ telif hakları, eser hırsızlığından bilimsel korsanlığa ve hatta kimlik hırsızlığına kadar varabilen çeşitli suçlar işlenebilmektedir:

1. Zimmete Geçirme (Embezzlement)

Zimmet suçu, görevi kötüye kullanma suçunun özel olarak düzenlenmiş bir çeşididir. Suçun faili, kamusal faaliyette bulunan kamu görevlisidir. Suçun maddi unsuru, kamu görevlisinin zilyetliğindeki veya koruma ve gözetimi altındaki malı kendisinin veya başkasının zimmetine geçirmesidir. (Gülşen, 2011:141; Volkan Aslan, 2013:44)

2. Endüstri Casusluğu (Corporate/Industrial Espionage)

Endüstri casusluğu; ekonomik kayıp vermek ya da yasal olmayan bir ekonomik avantaj sağlamak niyetiyle yetkisi ya da herhangi bir yasal sebebi olmaksızın uygun olmayan yollarla bir ticari sırrın elde edilmesi, kullanımı, transferi ya da ifşa edilmesidir. (Boğa, 2011:30)

3. İntihal/Eser Hırsızlığı (Plagiarism)

İntihal; başkalarının fikir, yazı ve çalışmalarını çalarak, aldığı kişilere gereken şekilde atıf yapmadan kendisinin gibi göstermektir. (Uçak & Birinci, 2008: 191)

4. Bilimsel Korsanlık (Piracy)

Korsanlık; fikri mülkiyet korumasına konu olan yazılım, müzik, film, kitap vb. herhangi bir nesnenin izinsiz olarak kaydedilmesi, çoğaltılması, umuma iletilmesidir. (Kırcı, 2004:57)

5. Kimlik Hırsızlığı (Identity Theft)

Bir başkasına ait kişisel bilgilerin yetkisiz olarak kullanılması suretiyle işlenen hırsızlık yöntemidir. Kredi kartı ve internet bankacılığı bilgileri, şifre ve parolalar, elektronik posta ve diğer önemli kişisel bilgiler bir başkası tarafından çıkar sağlamak amacıyla kullanılmaktadır. (Civelek, 2011:36; Turhan, 2006:162)

C. SİBER HIRSIZLIK SUÇUNUN UNSURLARI:

Suç, “kanunun cezalandırdığı fiil” şeklinde tanımlandığı gibi, (Türk Hukuk Lügati , 1991: 303; Yılmaz, 2005:824) “*yapılması yasaklanan ve karşılığında ceza öngörülen bir fiili yapmak veya terki yasaklanan ve terk edilmesi halinde ceza öngörülen bir fiili terk etmektir.*” (Suçun, benimsenen felsefi görüşe ya da suçun genel unsurları teorisi bakımından varılan neticeye göre değişik şekillerde tanımlanmasına ilişkin örnekler için bkz. (Boynukalın, 2009: XXXVII, 454) veya “*Allah Teâlâ'nın had veya ta'zîr cezalarıyla cezalandırdığı hukuki yasaklar*” (Udeh, 1992: I,66; keza benzer tarifler için bkz. Ebû Zehra, ts.:24; Karaman,

1987: I, 147) şeklinde de tanımlanmıştır.

Günümüz ceza hukukunda da suç: “*Sorumlu bir kimse tarafından olumlu veya olumsuz bir hareketle meydana getirilen ve ceza tehdidini taşıyan bir kanunda yer alan tarife uygun bulunan hukuka aykırı fiil*” (Dönmezer & Erman, 1994: I, 311; Gözübüyük, 1988: 4) şeklinde tanımlanmıştır.

Her suçta olduğu gibi, siber hırsızlıkta da öngörülen cezanın uygulanabilmesi için bir takım unsurların bulunması gerekli görülmüştür.

Bir eylem ve davranışın suç olarak nitelendirilebilmesi için genel olarak bu unsurları taşıması gerekir. Bu unsurlardan herhangi birinin yokluğu durumunda, söz konusu fiil ve davranış hukuken suç kapsamında değerlendirilmez. (Udeh, 1992: I, 111; Ebû Zehra, ts.: 168; Yiğit, 2012:29)

Hukukçular suç sayılacak davranışın şu dört unsuru taşıması gerektiğini ifade etmişlerdir ki, (Udeh, 1992.:I,142-149; Dönmezer & Erman, 1994: I, 310-311; Önder, 1992:151-154; Turhan, 2006:33. Ayrıca detay bilgi için bkz. Yiğit, 2012:29-37; Esen, 2006:41-53; Akalın, 2013:50-72) bunları şu şekilde ifade edebiliriz:

1. Kanûni Unsur (Tipiklik):

İşlenen fiilin -suçta kanunîlik ilkesinin zorunlu bir sonucu olarak- ceza kanununda suç olarak tanımlanması ve tanımda gösterilen şekilde gerçekleşmiş olması gerekir. “Suçun kanûniliği prensibi” şeklinde de dile getirilen bu unsur, ceza hukukunda “Kanunsuz suç ve ceza olmaz” ilkesinin temel dayanağını teşkil etmektedir. Kanûnilik ilkesi; kanun koyucu tarafından, suç olarak belirtilmiş fiil ve sözlerin icra edilmesi durumunda, hukuken sorumluluğu olan şahsa uygulanacak cezanın açıklanması şeklinde tanımlanabilir. (Dönmezer & Erman, 1994; I,21; Erem, 1991:I,75; İçel & Donay, 1993:73)

2. Maddi Unsur :

Hukukun, sorumlu kabul ettiği herhangi bir şahıstan, yasaklanmış bir fiil veya sözün, fert ya da topluma zarar verecek şekilde sadır olması, suçun maddi unsurunu oluşturur. (Udeh, 1992.: I, 342; Dönmezer & Erman, 1994: I, 379)

Suç olarak nitelendirilen söz veya fiillerin faillerine ceza verilebilmesi için, kişinin suç sayılan bir eyleminin olması ve bu eylemle doğan sonuç arasında bir illiyet (nedensellik) bağının bulunması gerekir. (Bkz. Udeh, 1992: I, 347; Karaman, 1987: I, 148; Dönmezer & Erman, 1994: I, 379)

a) Malın gizlice alınması:

Gizlice almaktan maksat, hırsızın, mağdûrun evindeki veya koruması altındaki bir malı izni ve rızası olmaksızın alıp götürmesidir. Buna göre, alıp götürme

mal sahibinin huzurunda veya bilgisi altında olursa, fiil hırsızlık olarak nitelendirilmez. Bu unsur, hırsızlık suçunu *gasp*, *âriyet*(ödünç),ya da *vedîa* (emanet) olarak alınan malın geri verilmemesi gibi yine mala yönelik diğer fiillerden ayırmaktadır. Dolayısıyla malın gizlice alınmasının şart koşulmasının tabii bir sonucu olarak zorbalıkla, emaneti altındaki malı *gasp* etmek veya insanların gözü önünde kapıp-kaçma suretiyle gerçekleşen eylemler, hırsızlık suçu kapsamında değerlendirilmez ve bu tür eylemlerde bulunanlara hırsızlık için öngörülen ceza uygulanmaz. (Serahsi, 1983: , IX, 160 ;Kâsânî, 1986: VII, 65; İbn Kudâme, ts. : X, 240; Züreyr, 1980:49)

Gizlice alma şartının tamamlanması için hırsızın malı muhafaza edildiği yerden alması, malın mağdurun mülkünün sınırları dışına çıkarılması, ayrıca malın hırsızın zilyedliğine geçmiş olması gibi şartlar aranır da hangi durumlarda bu şartların gerçekleşmiş sayılacağı fakihler arasında tartışmalıdır. Meselâ bir eve hırsızlık kastiyle girip de suçüstü yakalanan kimsenin eylemi teşebbüs seviyesinde kaldığından çoğunluğa göre had değil ta'zîr cezası gerekir. Hanefiler, gizlice alma şartının gerçekleşmesi için malın bulunduğu yerden alınmasını, yani mâlikin mülkünden çıkmasını yeterli görmeyip fiilen hırsızın mülk ve tasarruf alanına girmesini diğer bir deyişle somut ve fiziki olarak eline geçmiş olmasını gerekli görür. (Serahsî, 1983; X,147; Kâsânî, 1986: VII,65; İbnü'l-Hümmam, ts.: V,384; Kubeyşî, 1971:67-68) Diğer mezhep fakihleri ise malın, sahibinin zilyedliğinden çıkmasıyla hükmen hırsızın zilyedliğine geçeceği görüşünde olduğundan bu durumda had cezasından yanadırlar. (Şirazî, 1959-1960: II,280; İbn Kudâme, ts.: X, 259)

Malı bizzat alma, tahıl ambarını delip buğdayı dışarı akıtma gibi doğrudan filler ile malı bir hayvanın sırtına yükleyip veya akarsuya atıp arazi dışına çıkmasını sağlama gibi dolaylı fiiller arasında fark gözetilmez. Ancak hırsız malı bulunduğu yerde telef ederse bu eylem hırsızlık değil haksız fiil olarak nitelendirilir. (Kâsânî, 1974: VII, 68-69; İbnü'l-Hümmam, ts.: V,356; Udeh, 1992: II, 536-537; İbn Rüşd, 1985: II, 376)

Dolayısıyla siber hırsızlıkta da söz konusu suçun teşekkülü için malın mağdurun mülkünün sınırları dışına çıkarılması, ayrıca malın hırsızın zilyedliğine geçmiş olması şartı da önemli bir yer tutar. Ancak malda mutlaka failin fiili bir hâkimiyet kurmuş olması da şart değildir. Örneğin, paranın kendi hesabına havale edilmiş olması yeterlidir; paranın çekilmiş olması da gerekmez. (Özbek, 2002:1034)

b) Malın mütekavvim olması:

Hırsızlığa konu olan şeyin, “mal” olması, hırsızlık suçunun oluşumunda önemli yer tutan unsurlardan birisini teşkil etmektedir. Çalınan şeyin hukuken

hem mal hem mütekavim sayılması, genelde bütün akitlerde ve hukuki işlemlerde aranan bir şartın konuya uyarlanmış şeklini ifade eder.

İslâm hukukçuları, bir şeyin mal kabul edilebilmesi için o şeyin insanlar tarafından mal edinilmesinin âdet haline getirilmiş olmasını, mütekavim olabilmesi için de o şeyden faydalanmanın imkan dâhilinde bulunmasını gerekli görürler. Buna göre insanların örflerinde, “mal” kabul edilen ve mülk için biriktirilen şeyler, “mal” olarak değerlendirilir. (Kâsânî, 1986: VII, 67; İbn Kudâme, ts. : X,245; İbn Rüşd, 1985: II, 376; Bilmen, 1985: III,266; Bardakoğlu, 1998: 386)

“Mütekavim mal” ifadesi, özellikle Hanefi fakihlerinin kullandığı bir terim olup diğer fakihler genelde “muhterem” veya “kıymetli mal” ifadesine yer verirler. Belirtilen nitelikleri taşıyan mallar, İslâm hukukunda haklara konu olur. Buna karşılık kendilerinden faydalanmanın şer’an caiz ve serbest olmadığı gayri mütekavim mallar haklara konu teşkil etmediği için mülkiyeti de korunmaz, gasp veya telef edilirlerse tazmin edilmez. (Bardakoğlu, 1998: XVII, 386; Kubeysî, 1971: 132)

Bu itibarla mülkiyet ifade eden ve alım satıma konu olan her tür mütekavim malın, sahibinin rızası hilafına korunduğu veya saklı bulunduğu yerden alınması ise hırsızlık suçunu oluşturur. (Kâsânî, 1986: VII, 69; İbnü’l-Hümmam, ts.: V,368; Şirazî, 1959-1960: II, 280; İbn Kudâme, ts. : X/241-142)

Siber hırsızlık suçu ise mal almaya dayalıdır. Mal terimi sadece para, mücevher, giysi gibi maddi şeyleri değil elektrik, dijital veriler gibi fiziksel varlığı olmayan şeyleri de kapsar. (Sınar, 2001:72; Turhan, 2006:33; Özpençe & Özpençe, 2011)

Bu itibarla hırsızlık da manevi içeriğe sahip maddi bir bilginin, yani manetize kaset veya CD’lerin, flash belleğin, verilerin aktarıldığı kabloların, lisanslı yazılımların ve maddi değere sahip bilişim varlıklarının üzerinde meydana gelmektedir. (el-Mezmumî, 2008: 60; Dülger, 2004:90; Türkî, 2011: 96)

Hırsızın kopyalanan bilgileri asıl sahibinden çalarak kendi mülkiyetine geçirmesi, bilgiye saldırmasıdır. Çünkü hırsızın asıl amacı bu kasetleri çalmak değil, kasetin içindeki bilgileri çalmaktır. Bunun sonucunda da malın çalınması meydana gelmektedir. (Türkî, 2011:96-97)

c) Malın başkasının mülkiyeti altında bulunması:

Hırsızlık suçunun oluşumu için, çalınan malın, hırsızın mülkiyetinde veya mülkiyet iddiasında bulunabileceği bir konum ve nitelikte olmaması gerekir. (Udeh, 1992: II,588) Nitekim İslâm hukukçuları, ödünç, rehin veya kiraya vermiş olduğu bir malı, korunduğu yerden mal sahibinin gizlice alması durumunda

kendisine ceza uygulanmayacağını ifade etmişlerdir. Çünkü hırsızlığa konu olan malın mülkiyeti, çalan şahsa aittir. (Kâsânî, 1986: VII, 70; İbnü'l-Hümmam, ts.: V, 160; Bilmen, 1985:III,268) Aynı şekilde ortaklığın söz konusu olduğu bir malın, ortaklardan herhangi birisi tarafından çalınması, babanın çocuğuna, usul ve furûun, karı kocanın birbirine ait malı çalması başka tür müeyyideler gerektirse de belirtilen gerekçe nedeniyle fakihlerin çoğunluğuna göre haddi gerektiren bir suç olarak görülmez. (Kâsânî, 1986: VII, 70; İbnü'l-Hümmam, ts.: V,139; Bardakoğlu, 1998:386)

Bir siber suç failinin, siber uzay ortamını kullanarak kendi bilgisayarından bir finans kuruluşunun sistemine girdiğini ve bu finans kuruluşunun fonlarında bulunan paraları kendisine ait hesaplara geçirdiğini düşünürsek, siber suçun faili başkasına ait olduğunu bildiği parayı hukuka aykırı olarak kendi fiili hâkimiyet alanına geçirmekte ve o paraya hukuken sahip olan kişileri zarara uğratmaktadır. Dolayısıyla mal başkasının mülkiyetindedir. (Turhan, 2006:34)

d) Malın Menkul ve Koruma(Hırz) Altında Olması:

Hırsızlık suçunun oluşmasında malın “hırz” altında (mahrûz) iken alınmış olması şartı da önemli bir yer tutar. Bir eylemin hırsızlık sayılabilmesi için alma eyleminin koruma bölgesinde gerçekleşmesi ve çalınan malın koruma alanından dışarıya çıkarılması, dolayısıyla taşınabilir(menkul) olması şarttır. (Udeh, 1992, II, 543)

Nitekim failin, bir kişinin bilişim sisteminde kayıtlı programını bir CD'ye kaydederek bunu kendi bilgisayarına zilyedinin rızası dışında aktarması da hırsızlık suçunu oluşturur. (Ergün, 2008:123-124) Ancak şu var ki, bilgisayarda var olan verilerin bir başka yere gönderilmesi veya değiştirilmesi suretiyle hukuka aykırı bir yarar sağlanması; verilerin hala mağdurun sisteminde kalması ve ortada taşınır bir mal (somut bir nesne) bulunmaması sebebiyle hırsızlık suçu söz konusu olmayacaktır. Kişinin rızası dışında, failin kendisine veya bir başkasına yarar sağlamak amacıyla hareket edip kişinin eşya üzerindeki egemenliğine bilişim sistemi aracılığıyla son verilmesi eylemiyle bu suç gerçekleşmektedir. (Dülger, 2004:290; Ekinci & Esen, 2005:60)

Hırsızlık suçunun oluşumu için çalınan malın, muhafaza altında (muhrez) olması da gerekli görülmüştür. Buna göre muhafaza altında olmayan bir malın çalınması durumunda, hırsızlık cezası uygulanmaz. Hırzın (koruma) ölçüsünü örf belirler. Örf'e göre bir malın muhafaza altında olduğu varsayılıyorsa, bu şart gerçekleşmiş kabul edilir. (Hırz (malın muhafaza altında olması) şartı hakkında geniş bilgi için bkz. İbnü'l-Hümmam, ts.: V,141; İbn Kudâme, ts. : X, 249; Züreyr, 1980:25; Bilmen, 1985:III,362; Menekşe, 1998: 28-33; Akalın, 2006:90-101)

Nitekim bir siber suç failinin sahibinin izni olmaksızın siber uzay ortamını kullanıp kendi bilgisayarından kişi veya kurumların bilgisayar sistemlerine sızarak, buradaki çeşitli güvenlik tedbirleriyle de koruma altında olan iktisadi değer taşıyan ve alım satıma konu olan her türlü veri ve programları alması, hırsızlık suçunu oluşturur.

Buna göre malın korunan yerden bir internet ağına aktarılması, korunduğu yerden çıkarılması sayılır. Bu ise hırsızlık suçunun temel rükunlarından biridir. (Akalin, 2013:118; Türkî, 2011:97)

Ayrıca çeşitli banka ve finans kurumlarında internet koruma sistemleri ile korunan mudilere ait hesaplardan, failin bilişim sistemlerini kullanılarak kendisine veya bir başkasına ait hesaba para aktarması da siber hırsızlık kapsamındadır. (Dülger, 2004: 257; Kurt, 2005:184; Sınar, 2001:73; Ergün, 2008:37-38) Çünkü bu durumda da sahibinin rızası ve bilgisi dışında başkasına ait paranın çalınması, hukuka aykırı olarak kendi fiili hâkimiyet alanına geçirilmesi söz konusudur. (Akalin, 2013:117-118)

e) Çalınan Malın Belli Bir Değerde Olması:

Hırsızlık suçunun unsurlarından biri de çalınan malın belli bir değerde olmasıdır. İslâm hukukçuları, bu konuda nisab şartını ilke olarak benimseyip nisab miktarını da geleneksel teamüle uyararak altın veya gümüş para (dinar ve dirhem) cinsinden belirlemekle birlikte Hz. Peygamberden rivayet edilen hadisler ve uygulamalar arasında farklılıklar bulunması sebebiyle farklı görüşlere sahip olmuşlardır.

Hanefilere göre, el kesme cezası için gerekli miktar, on dirhem (yaklaşık 30 gr) gümüş veya bir dinar (4.25 gr) altın ya da bunların değerindeki maldır. (İbnü'l-Hümmam, ts.: V, 121; İbn Rüşd, 1985: II, 374) Çoğunluğu temsil eden Şâfîî, Malikî ve Hanbelî mezheplerine göre ise, hırsızlıkta nisap miktarı, altında çeyrek dinar (1/4 =1,112 gr) altın veya üç dirhem (8.125 gr) gümüş ya da bunların değerindeki maldır. İbnü'l-Kayyim değişen para değerleri karşısında her zaman uyacak bir ölçü getirmektedir. Buna göre hırsızlık konusu olan malın asgari değeri bir ailenin bir günlük yiyecek bedelidir. (Ebû Zehre, ts.:133-134; İbn Kudâme, ts. : X, 241; İbn Rüşd, 1985: II, 373; ; Avvâ, 2006: 221)

Teknolojinin gelişmesiyle de ortaya birçok yeni hırsızlık türü çıkmıştır. Nitekim bunlardan biri olan siber hırsızlık suçunda da çalınanın iktisadi değerinin hırsızlık suçunda aranan değer limitine (nisab) ulaşması durumunda hırsıza had uygulanır. (Akalin, 2013:118; Kubeyşî, 1971:132)

3. Manevi Unsur (Kusurluluk):

Bir fiilin suç sayılabilmesi için fiille birlikte iradenin de bulunması, kısaca fiilin iradî olması, yani hukuka ve yasaya aykırı olan fiille, failin kusurlu iradesinin de katılmış olması gerekir.

Bütün suçlarda olduğu gibi hırsızlık suçunda da fâilin; suç işleme kastını taşıması, ayrıca bu kastın hukuken geçerliliğinin bulunması cezalandırma için gerekli en önemli unsurdur.

Kasıt; bir kimsenin bir fiili bilerek ve isteyerek işlemesi olduğundan hırsızın da eylemini böyle bir bilinç ve istekle gerçekleştirmesi, yani başkasına ait olduğunu bildiği bir malı sahiplenme (temellük) maksadıyla almış olması şartı aranır.

Hırsızlık suçunda bu genel kastın dışında başkasına ait malın mülk edinme maksadıyla alınması da şarttır. Aksi halde hırsızlık suçu teşekkül etmez. Meselâ failin bir malı kendi malı veya sahipsiz olduğu zannıyla ya da kullandıktan sonra geri verme, tehlikeden koruma amacıyla alması durumunda suç kastı bulunmadığı için, faile ceza tatbik edilmez. (Udeh, 1992: I, 403, II, 608; Bardakoğlu, 1998: 386. Nitekim Mecelle'nin 2.maddesinde de "*Bir işten maksat ne ise hüküm ona göredir.*" denilmektedir.)

Suç kastının varlığından söz edebilmemiz için fâilin, akıllı, ergen ve serbest iradeye sahip olması gerekmektedir. (Serahsî, 1983: IX, 189; Kâsânî, 1986: VII,67; Şirazî, 1959-1960: II, 278; Udeh, 1992: II, 609) Sayılan nitelikleri taşımayan şahıslara, işledikleri hırsızlık fiilinden dolayı, ceza uygulanmaz. Ancak, çaldıkları malı tazmin etmekle yükümlü tutulurlar. (Serahsî, 1983: IX, 140; Kâsânî, 1986: VII,79; Udeh, 1992: II, 610)

Siber hırsızlık failinin amacı da kendisine veya bir başkasına mali kazanç sağlamak ya da mağdura ciddi kayıplar vermektir.

4. Hukuka aykırılık:

Fiilin yalnızca ceza hukukuyla değil bütün hukuk düzeniyle çatışma halinde bulunmasıdır. Yani kısaca, hukuk düzeninin izin vermediği bir fiilin işlenmesidir. Hukuka aykırılık, davranışın ceza hukuku kuralında tanımlanan suç tipine uygun düşmesi, bununla birlikte onu hukuka uygun hale getiren ve dolayısıyla suç olmaktan çıkararak hukuka uygunluk sebebinin bulunmaması durumunda açığa çıkmaktadır. İslam ceza hukukunda hukuka uygunluk sebepleri; kanun hükmünün ve yetkili merciin emrinin yerine getirilmesi, meşrû müdafâ, zorunluluk hali, hakkın kullanılması ve ilgilinin rızasıdır. Hukuka uygunluk sebepleri fakihler tarafından daha çok ibâha eksenli kavramlarla işlenmiştir. (Ergün, 2008:5;

Akalın, 2006: 48; Boynuakalın, Suç, 2009: 436;. Ayrıca geniş bilgi için bkz. Yıldız K. , 2009)

Her suçun oluşmasında esas olduğu üzere siber suçlarda da kesin olan o ki, “hukuka aykırılık unsuru” suçun oluşmasının bir koşuludur. Bu itibarla bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirmiştir. (Taşkın, 2008:30-31; Mahmutoğlu, 2013: 862)

Klasik anlamda hırsızlık suçunun oluşabilmesi için gerekli olan bu unsurlar siber hırsızlık suçunun gerçekleşmesi ve ceza sorumluluğunu doğurabilmesi açısından da uygulanabilir niteliktedir.

Bu itibarla bir suçun elektronik ortam içerisinde işlenebilme imkânı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçlara siber suçlar denir.

Siber suçun gerçekleşmesi için failin bu suç unsurlarını gerçekleştirmesi, yani bilişim sistemine izinsiz girmesi, eylemi isteyerek yapması, sisteme girme ve kalmanın yanında bunun hukuka aykırı olarak işlenmesi gerekmektedir. (Ziya Mustafa Osman, 2010: 72-79, 85-87)

D) Siber Hırsızlık Suçunun Kovuşturulması ve Delillendirilmesi

Hırsızlık suçunun klasik literatürde had suçları grubunda yer alması ve Allah hakkına taalluk eden bir suç olarak nitelendirilmesi, kural olarak bu suçun takibinin şikâyete bağlı olmamasını ve suçlunun da kamu adına yargılanmasını gerektirir. Ancak hırsızlık suçu netice itibarıyla bir şahsın malına karşı işlendiğinden çoğunluğunu Hanefî ve Şâfiîler’in ve bir kısım Hanbelîler’in teşkil ettiği fakihler bu suçun yargılanmasını, malı çalınan veya hakkı ihlâl edilen kişinin davacı olmasına bağlamayı tercih etmişlerdir.

Mal sahibinin, çalınan malı hırsıza hibe etmesi, hırsızın çaldığı malda hak iddiasında bulunması gibi, bazı özel durumların bulunabileceği ihtimalinden hareketle, hırsızlık suçunda şikâyet şartı getirilmiştir. Başta Mâlikîler ve Ahmed b. Hanbel olmak üzere diğer fakihler ise, hırsızlık suçu kamu hakkının baskın olduğu bir suçtur, bu yüzden malı çalınan şahsın dava açması şart değildir. (Geniş bilgi için bkz. Kâsânî, 1986: VII, 83; İbn Kudâme, ts. : X, 294; Menekşe, 1998:35-41.)

Siber suçlar da takibi şikâyete bağlı olan suçlardır. Yani suçun cezaî yaptırımının sağlanabilmesi, ilgili suç hakkındaki adlî işlemlerin başlayabilmesi için ilgili makamlara bu suçun bildirilmesi gerekmektedir. (Köse & Köse, 2015)

Günümüzde adliyelere intikal eden siber suç sayısının az olmasının ve böylelikle suçun kovuşturulmamasının temel sebebi; bir çok suç mağdurunun su-

çun farkında olmaması ve şikayette bulunmaması, suçun mağduru olan kurumların ve büyük şirketlerin ise kamuoyunda duyulması halinde güven ve prestij kaybına uğrayacakları endişesiyle şikayetçi olmamalarıdır. (Ergün, 2008:132)

Suçun ispatı, davanın karara bağlanması prosedürünün önemli bir parçasını teşkil eder. İslâm hukukunda hırsızlık suçunun tespitinde, günümüz ceza hukukundaki her şeyin delil olabilmesi ve bütün delillerin hâkim tarafından serbestçe değerlendirilmesi manasında olan vicdanî delil sisteminin aksine kanunî deliller esas alınmış, ağır cezayı gerektiren had cezalarının ispatı daha zor şartlara bağlanmıştır. Doktrinde ve uygulamada kişilerin kural olarak borçsuz ve suçsuz oluşu esas alındığından suçun işlendiği kesinlikle ispat edilmedikçe kişinin cezalandırılmaması ilkesi hâkim olmuştur. (Bayındır, 1986: 75, 124-126, 141-142.; Bardakoğlu, Hırsızlık, 1998: 389. Nitekim Mecelle'de bu prensip "Be-raeti zimmet asıldır" diye özetlenmektedir. (Bkz. Mecelle, md.8))

İslâm muhâkeme hukukunda ispat yükü kural olarak davacıya aittir ve bu yargılama hukukunda genel bir ilke olmuştur. (Bkz. *Mecelle*, md. 76.) Bu sebeple klasik doktrinde yerleşik prosedüre göre hırsızlık suçu ya beyyine (delil) ya da hırsızlık yapan mükellef bir şahsın suçunu kendiliğinden veya yapılan isnat üzerine itiraf etmesi şeklindeki ikrar yoluyla ispatlanabilmektedir.

Siber suçlarda, klasik suç anlayışından farklı olarak servis sağlayıcılar, içerik sağlayıcılar, site sahibi gibi birbiriyle bağlantılı pek çok süje suçun faili olabilmektedir. Sanal ortamda bu süjelerin gerçek kimliklerini çoğu zaman gizlemeleri nedeniyle gerçek kimliklerini elde etmenin pek kolay olmadığı bilinen bir gerçektir. Ayrıca internet ortamının sınır ve mesafe tanımayan nitelikte olması sebebiyle failerin bulunmasında da zorluk olması, fail bulunsa dahi devletlerarasındaki farklı usul uygulamaları bulunması suçun kovuşturulmasını çoğu zaman imkânsız kılmaktadır. (Ergün, 2008:43-44)

Siber suçlarda, suç bilinen usullerin dışında çok daha hızlı, teknik, kolay ve dikkatlerden uzak bir şekilde işlenebilmekte, hem de suçlunun kimliğinin ve suç alanının tespit edilmesi zorlaşmaktadır. Yine suç tespit edilse bile suçta kullanılan araçlardan faile ulaşılması, fail belirlense bile yakalanması, fail yakalanırsa bile kişinin uğradığı zararın veya suça konu zararlı içeriğin web ortamından tamamen kaldırılması, alınan veya yayılmış üçüncü dördüncü taraflardaki kopyaların silinmesi, yok edilmesi mümkün olmamaktadır. (Yazıcıoğlu, 1997: 150; Değirmenci, 2002:75; Özcan, 2004: 326-327; Turhan, 2006:47; Ergün, 2008:43; Suveyr, 2011:12; Sagir, 2013:9)

Siber suçu ortaya çıkarmaya yarayacak delillerin türü ve formatı, bir de bunları elde etme yöntemleri geleneksel suçlara nazaran farklıdır (Özen & Baş-türk, 2011:91).

Siber suçları diğer suçlardan ayıran temel özelliklerden birisi, toplanan delillerin klasik delil yerine daha çok dijital delil olmasıdır. Her ne kadar siber suçlarda da parmak izi toplama, DNA testi yapma, olay yeri inceleme, grafolojik incelemeler gibi eskiden beri var olan klasik deliller ve delil toplama yöntemleri kullanılsa da siber suçlar açısından bu deliller yan deliller olarak değerlendirilecek, esaslı ve önemli deliller her zaman için dijital deliller olacaktır. (Yetim, 2014:184; Al-A'ali , 2007)

Ancak delilleri elde etmek zor olduğu gibi, bunları mahkemeler nezdinde kabul görecektir şekilde, mevcut usûli kurallara uygun olarak toplamak da ayrıca bir meseledir. (Önok, 2013:1235; Choo, 2008:286 vd.)

İnternette yapılan işlemler, IP numarasının öğrenilmesi ve daha sonra bu numaradan internet bağlantısı yapılan telefonun ve dolayısıyla mekânın tespit edilmesiyle bir anlamda takip edilebilmektedir. (Eralp, Bilişim Suçlusuna Giden Yol – İp, 2004)

Siber suçların çok uluslu ve sınır ötesi suçlar olması itibarıyla deliller ancak işbirliği ve yardımlaşma ile toplanabilecektir. Bu durumda da birden fazla ülkenin polis teşkilatları, kriminal laboratuvarları ve ceza usul yasaları devreye girecektir. Toplanan delillerin hukuka uygun delil olarak değerlendirilebilmesi için, ilgili ülke ceza usul yasalarının hukuki düzlemde insan haklarını düzenleyen uluslararası bir kısım sözleşmelere uygun olması gerekecektir.

Siber suç delillerinin “adli bilişim” adı verilen, “potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan” uygulamalarla (Berber, 2004: 39; Karagülmez, 2011: 379 vd.; Çakır & Sert, 2011) ortaya konması, dijital delillerin derlenip adli makamlara sunulması, korunması; bu suçları soruşturacak personelin çok ciddi bir uzmanlığa sahip olmasını gerektirmektedir. (Uçkan & Beceni, 2004: 423; Tulum, 2006:95-97; Önok, 2013:1235)

D. SİBER HIRSIZLIĞIN CEZASI

Gerek İslam hukukunda, gerekse tarihten günümüze düzenlenen hukuk sistemlerinde hırsızlık suçuna mutlaka belirli müeyyideler konulmuştur. Bilim ve teknolojinin ilerlemesi sonucu günümüzde hırsızlığa konu olan mal ve hizmetler geçmişe göre daha değişmiş ve gelişmiştir. Özellikle bilişim ve iletişim alanında yaşanan gelişmeler, fiziki özelliğe sahip olmasa da mülkiyet ifade eden yeni mal türlerinin ortaya çıkmasına sebep olmuştur. Teknolojinin gelişmesiyle ortaya çıkan bu yeni hırsızlık türlerinde yöntem, teknik ve araçlar değişse de yapılan fiil yine bir çalma eylemidir.

İşte bu bölümde, bilişim alanındaki hukuki ihlallerden biri olan, sanal ortamda da çeşitli suçların işlenmesini sağlayan siber hırsızlığa ilişkin cezai yaptırımlar

rimlar İslam hukuku ve modern hukuk bağlamında ele alınmış, hukuk sistemlerinin söz konusu suçla ilişkin öngördüğü cezalar irdelenmeye çalışılmıştır.

I- MODERN HUKUKTA SİBER HIRSIZLIK ve CEZASI

Modern hukuk doktrininde bilişim alanındaki hukuki ihlallerin cezalandırılmasına yönelik çeşitli ülke mevzuatlarında yeni bir takım düzenlemeler veya değişiklikler olmuştur.

Bu düzenlemelerde de temelde üç ayrı yöntem benimsenmiştir: (Eker Ö. U., 2006:108-109)

a. Ceza kanunlarına bilişim suçlarına yönelik ayrıca özel hükümler eklenmesi,

b. Mevzuatlarda hali hazırda yer almakta olan geleneksel suç tiplerinin yeniden tanımlanması, daha doğrusu geleneksel suç tiplerinin tariflerinin/tanımlarının genişletilmesi yahut mevcut hükümlere yeni fiillerin eklenmesi,

c. Söz konusu olguyu düzenleyen ayrı ve özel kanunlar çıkartılması.

T.C.K Anayasası ve T.C.K hükümleri çerçevesinde siber suçları değerlendirdiğimiz zaman kısaca şunları söyleyebiliriz:

Öncelikle siber suçlar, esas olarak “bilişim alanında suçlar” ve özel hayata ve hayatın gizli alanına karşı suçlar” bölümünde düzenlenmiştir. Bunlar bilişim sistemi aracılığıyla işlenebilen, özellikle bilişim sistemleri kullanılmadan işlenebilmeleri sınırlı olan suçlardır.

Yeni düzenlenen T.C.K. ile birlikte bilişim sistemleri kullanılarak gerçekleştirilen hırsızlık suçları nitelikli hırsızlık suçlarından sayılmış ve bu suçlara, basit hırsızlığa göre daha ağır cezalar öngörülmüştür. Nitekim TCK 142/2. fıkrasının ‘e’ bendinde; “*Hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde üç yıldan yedi yıla kadar hapis cezasına hükmolunur*” ifadesi yer alır. Ayrıca yine bu sistemlerin kullanılması suretiyle siber suç işleyenlerle ilgili hükümler, 5237 sayılı yeni Türk Ceza Kanunu’nun “Topluma Karşı Suçlar” kısmının onuncu bölümünde “Bilişim Alanında Suçlar” başlığı altında, T.C.K. ’nun 243 ilâ 246. maddeleri arasında yer almıştır. Buna göre, bilişim sistemlerine hukuka aykırı olarak giren, sistemi engelleyen, bozan, değiştiren ya da haksız çıkar sağlamak için kullananlar hakkında gerekli görülen hapis ve para cezalarına yer verilmiştir.

5846 Sayılı Fikir ve Sanat Eserleri Kanunu’nun 2. maddesinde; “bilgisayar programlarının koruma altına alınması” konusu, (Taşkın, 2008:33) 71. maddesinde; “manevi, mali veya bağlantılı haklara tecavüz” konusu düzenlenmiş, 5070 sayılı Elektronik İmza Kanunu’nda ise; “imza oluşturma verilerinin izinsiz kullanılması” suçu düzenlenmiştir.

Doğrudan bilişim suçu sayılmayan fakat bilişim vasıta kılınarak işlenen “haberleşmenin gizliliğini ihlal”, “kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, “özel hayatın gizliliğini ihlal”, “kişisel verilerin kaydedilmesi ve izinsiz olarak ele geçirilmesi”, “müstehcenlik suçu” gibi suçlarda bilişim vasıta kılınarak işlenmesi durumunda ise ayrıca bir düzenleme yapılmaksızın TCK’daki düzenlemeler yeterli görülmüştür.

Yine, yeni TCK’nın ikinci kısmı olan kişilere karşı suçların onuncu bölümünde, “Mal varlığına Karşı Suçlar” başlığı altında 142. maddenin 2. fıkrasının (e) bendindeki nitelikli hırsızlık ile 157 ve 158. maddelerdeki dolandırıcılık suçunun nitelikli dolandırıcılık olarak bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde cezanın ağırlaştırıcı sebebi olacağı vurgulanmıştır. (Ergün, 2008: 83-104; Ketizmen, 2008:144; Çakır & Kılıç, 2014):182-194)

Modern hukukta, kullanıcıların sanal kimliklerine ilişkin suçlar (Örneğin; facebook veya twitter gibi sosyal medya hesaplarının çalınması, ilgili hesaplara zarar verilmesi ya da fotoğraf, video gibi verilerin çalınması, ilgili verilerin izinsiz kullanılması; banka hesaplarının çalınması); dijital olarak depolanmış verilerde sahtekârlık ve söz konusu verilerin değiştirilmesi, silinmesi, bilgisayar virüslerinin ve diğer zararlı yazılım unsurlarının (Örneğin; Spam, Worm gibi tehdit oluşturan unsurlar) dağıtılması – bulaştırılması, bilgi teknolojileri sistemlerine yönelik saldırılar ile diğer siber suçlarda (hukuka ve genel ahlâka aykırı verilerin bulundurulması, Örneğin; çocuk pornografisi ya da sanal ortamdaki telif haklarının ihlali) ihlal şekline göre tazminat (adli para) ve hapis cezaları öngörülmüştür. (Geniş bilgi için bkz. Ergün, 2008: 83-129.)

II- İSLAM HUKUKUNDA SİBER HIRSIZLIK ve CEZASI

A. Siber Hırsızlık Cezasının Hukuki Dayanağı

İslâm hukuku doktrinde bugünkü tabirle doğrudan “siber hırsızlık” veya bunu dolaylı olarak ifade eden bir başka kavram bulunmamaktadır.

Günümüz fıkıh araştırmacıları ilmî, teknik ve teknolojik gelişmeler karşısında ortaya çıkan, içinde bulunduğumuz ve fiilen yaşadığımız güncel hayatın getirdiği problemlerden biri olan siber suçlara yönelik, çeşitli ayetlerdeki ve hadislerdeki ifadelerden, dinin genel ilke ve amaçları (makâsıdu’ş-şerîa) doğrultusunda, geçmiş dönemlerde fıkıh bilginlerinin benzer olayları çözerken benimsedikleri prensip ve yöntemlerden de yararlanarak çözümler üretmeye çalışmışlardır.

İslam ceza hukuku yaptırımlarında suçun cezalandırılmasında gözetilen temel amaç; genelde suçun açıktan işlenmesine ve yayılmasına engel olarak içtîmâi vicdanı ve yapıyı korumak, özelde ise suçu önlemek, suçluyu te'dib ve islah

etmektir. Bundan dolayı suçluya verilecek cezanın toplumun hukukunu ve ortak değerlerini koruması, suçun işlenmesine ve tekrarına engel olması, suçluyu uslandırması, maşerî vicdanı tatmin edip mağdurun intikam hissini dindirecek miktar ve şekilde olması esastır. (Ebû Zehre, 1998: 27; Avvâ, 2006:91-99; (İbn Âşûr, ts.:515-516; Dağcı, 1996:33-34; Karaman, 1987:l, 152-153; Bardakoğlu, Ceza, 1993: 472)

İslam hukukunda, gerek internet üzerinden yapılan yayınlarla ve gerekse hukuk dışı girişimlerle bireylerin hedef alınan malvarlıkları ile şahsiyet haklarının korunması İslam teşrî'inin ana gayeleri arasında sayılmaktadır. Zira toplumun ve toplumun bir ferdi olan insanın varlığını koruyup devam ettirebilmesi için haksız saldırılara hukuk düzeniyle karşı konulması kaçınılmazdır. Böylece "hak" ve "hürriyet" şeklinde tanımlanabilecek bazı değerlerin varlığı anlamlı hale gelebilecektir. İslam hukukunda ise bu hak ve hürriyetler, "maksat" ya da "maslahat" adı verilen değerlerin korunması bağlamında ele alınmıştır. (Şâtîbî, 1990: II,7; Zekiyüddin Şa'ban, 1990:413 vd; Yavuz, 2006)

"Zarûrât-ı hamse" şeklinde de ifade edilen bu değerler; canın, neslin, aklın, malın ve dinin korunmasıdır. (Söz konusu beş temel hak için bkz. Şâtîbî, 1990:II, 9; Şa'ban, 1990:414; Bardakoğlu, Ceza, 1993: 472; İbn Âşûr, ts.: 151; Büyükbaş, 2013: 146-147)

Nitekim siber suçların doğrudan bilgisayar sistemlerine ya da dolaylı olarak kişinin mülküne yani bu beş önemli değerden birine verdiği zarar, İslam hukukçuları tarafından meselenin hükmü belirlenirken hareket noktası olarak kabul edilmiştir. (Maghaireh, 2008:342-343; es-Sened, 2004: 306; el-Hadimi, 2006: 32-39; 95- 176.)

Yine bu bağlamda siber suçlar ele alınırken, fıkhîta yerleşik hala gelmiş bazı külli/genel kurallardan da yararlanıldığı görülür. (Maghaireh, 2008: 342-343) En çok başvurulan fıkıh kuralları ise şunlardır:

"Bir işten maksat ne ise hüküm ona göredir."(İnsanların gerek sözlü gerekse fiili iş ve tasarruflarının hukuki sonuçları ve hükümleri, kişinin fiil ve tasarrufları yaparken taşıdığı amaca bağlı olarak değişir. (Ahmed Cevdet Paşa, Açıklamalı Mecelle : (Mecelle-i ahkam-ı adliye), 1979, md. 2)

"Şek ile yakîn zail olmaz."(Kesin olarak bilinen bir durum veya hüküm, şüphe ile ortadan kalkmaz. Bir kişinin cezalandırılabilmesi için de suçluluğunun kesin olarak ispat edilmesi gerekir. Bkz. Mecelle., md.4)

"Zarar izale olunur."(İslam hukukunda temel ilke, kimsenin zarara uğratılmaması, buna rağmen başkasına zarar verilmiş ise mağdurun uğradığı zararın, zarara sebebiyet veren fail tarafından karşılanmasıdır. Bkz. Mecelle., md.20)

Yine bu kapsamda; konut dokunulmazlığına ilişkin olarak evlere izinsiz girilmemesinin emredilmesi; ("*...Erdemlilik asla evlere arkalarından gelip gir-*

meniz değildir; fakat erdemlilik kişinin Allah’a saygılı olmasıdır. Evlere kapılardan gelin; Allah’a saygılı olun ki kurtuluşa eresiniz.” (Bakara Suresi, 2 /189), “Ey iman edenler! Başkalarının evlerine ev sahiplerinden izin alıp onlara selâm vermeden girmeyin. Bu davranış sizin için daha hayırlıdır. Düşünüp anlayasınız diye size böyle öğüt veriliyor. ” (Nur Suresi, 24/27-29); “izin istemek gözden dolayı (yani gözün evin mahremiyetini görmesini önlemek için)meşru kılınmıştır.” (Buhari, “İsti’zan”, 11; Müslim, “Edeb”, 40,41; Tirmizi, “İsti’zan”, 17) “Bir kimsenin kendisine izin verilmeden başkalarının evinin içine bakması yasaktır.” (Ebu Davud, “Edeb”, 136.) Ayrıca geniş bilgi bkz. Kahraman, 2008:137-184.) yazılı ve sözlü haberleşmenin gizliliğiyle ilgili emir ve nehiyeler; (“Kardeşinin yazılı metnine onun izni olmadan bakan ancak ateşe bakmış olur.” (Ebu Dâvud, “Tefriu' ebvabi'l-vitr”, 23); “İnsanların duyulmasından hoşlanmadıkları ya da duyulmasından çekindikleri konuşmalarına kulak kabartan kişinin kıyamet günü kulağına kurşun dökülür.” (Buhârî, “Ta'bir”, 45; Tirmizî, “Libâs”, 19). insanların bilinmesine rıza göstermeyecekleri gizli durumlarını, (Gizliliğin ölçüsü olarak Hz. Peygamber “Bir kimse konuşurken, başkasının işitmemesi arzusuyla etrafına bakınırsa, o şey gizli sayılır.” (Ebu Davud, “Edeb”, 32; Tirmizî, “Birr”, 39) ölçüsünü verir. Ayrıca bkz. Tirmizî, “İstizân”, 16;”Edeb”, 76; Buhârî, “Tabirü'r-rüyâ”, 45; “İstizân”, 45; Müslim, “Selâm”, 36.) ayıplarını ve kusurlarını merak edip izini sürme, araştırıp ortaya dökme çabaları olan suizan, sövme ve hakaret etme, (şetm ve tahkir), söz götürüp getirme (koğuculuk/nemime)”, tecessüs ve gıybette dair önleyici ve uyarıcı talimatlar,(“Ey diliyle inanıp kalbine iman girmeyenler! Müslümanlara eziyet (gıybet) etmeyin ve onların gizli tarafını araştırmayın. Müslüman kardeşinin gizlisini araştıranın Allah da gizlisini araştırır. Allah, kimin gizli yanını araştırırsa, evinin içinde bile olsa onu herkese karşı mahcup ve rezil rüsvay eder.” (Ebû Dâvud, “Edeb”, 35; Tirmizî, “Birr”, 85) ahlaki yönlendirmeler (Zan, kusur ve ayıpları ifşa, alay, haset, düşmanlık beslemek, ihanet, zulüm, tahkir, tezyif vb. kötülüklerden kaçınmaya dair çok sayıda ahlaki yönlendirmeler için örnek olarak bkz. Hucurât, 49/12; Hümeze, 104/1-2; Buhârî, “Mezâlim”, 4; “Nikah”, 45; “Edeb”, 57, 58; “Ferâiz”, 2; Müslim, “Birr”, 21, 58; Ebû Dâvud, “Edeb”, 39, 40, 56; Tirmizî, “Birr”, 18, “Büyü”, 38; Ebû Davud, “Büyü' (İcare)”, 79), bilgisayar kullanımına ilişkin etik kurallar (Mason, 1986; Masum, 2013) bu hususta konulan çerçevenin tamamlayıcı öğeleridir.

Nitekim Modern Ceza hukukunda siber suçlara yönelik kanun maddeleri ile İslam hukukunun temel ilkeleri karşılaştırıldığında (Nitekim Mansur el-Ali de makalesinde Teksas Bilgisayar Suçları ile Kur’an ayetleri ve hadislerin benzer bir şekilde karşılaştırmasını yapar. Bkz.Al-A'ali , 2007) ortaya şöyle bir tablo çıkmaktadır:

Modern ceza hukukunda, sahibinin izni olmaksızın bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girilmesi ve orada kalmaya de-

vam edilmesi suç olarak düzenlenmiştir. (Dülger, 2004: 211) İslam hukukunda da sahibinin rızası olmaksızın kişisel bilgileri ihtiva eden verilerin bir başkasına verilmesi, özel hayatın mahremiyetinin ihlal edilmesi suç sayılmış ve bu; güvenin zedelenmesi, gizliliğin ihlali olarak nitelenmiştir. Bu itibarla elektronik ortamda da mahremiyet korunarak başkasının bilgisayarında depolanmış kişisel dosyalara erişim yasaklanmıştır. (es-Sened, 2004: 304-306; Al-A`ali, 2007)

Nitekim bu bağlamda İslam hukukçuları da şahsiyet haklarının ihlalinin bir parçası kabul ettikleri bu tür suçları cezalandırmışlar, yer, zaman, şahıs ve ihlal şekline göre de cezanın şekil ve miktarını belirlemişlerdir. (Hira, 2014: 86; Kahraman, 2008: 215; Akgündüz, 2011: 412.)

B. Siber Hırsızlık Cezasının İnfazı

Hırsızlık; İslam ceza hukukunun had, kısas-diyet ve ta'zîr şeklindeki üçlü ayırımının (İslam ceza hukukundaki bu üçlü ayırım için bkz. Bardakoğlu, Ceza, 1993; Avvâ, 2006: 151 vd. ; Yiğit, 2012: 161, 167-175.) had grubunda yer alır. Özellikle Hanefi literatüründe bazen hırsızlığın ikiye ayrılıp eşkıyalık, silahlı gasp, soygun, yağma, yol kesme ve terör suçuna "büyük hırsızlık" (es-serikatü'l-kübra), basit hırsızlığa da "küçük hırsızlık" (es-serikatü's-suğra) denilmektedir.

Siber hırsızlık suçunun had gerektiren küçük hırsızlık kapsamında mı, yoksa ihtilâs (özel bir koruma altında bulunmayan menkul bir malı, sahibinin ya da yetkili kimsenin rızâsı olmadan ve zor kullanmadan hile ve el çabukluğu ile alıp kaçmak. Bkz. Kaya, 2000) kapsamında mı olduğunu ve İslam hukukunun buna yönelik uygulama boyutunu anlamak için; şifre, bilgisayar ve internet koruması gibi elektronik güvenlik ekipmanlarının bir mal sahipliği olup olmadığının belirlenmesi gerekir.

Siber hırsızlık ya cari hesaplarla oynama ya da hesaplar arası transfer işlemleri ile gerçekleşir ki bu da kişinin bankadaki malvarlığına yönelik bir suçtur. Buradan alınan herhangi bir şey, had gerektiren hırsızlık kapsamındadır. Çünkü bankadaki para, koruma altındaki (hırz) bir maldır ve failin parayı mağdurun hesabından kendi hesabına aktarmasıyla cezası had olan hırsızlık suçu oluşmuştur.

İhtilâs ise failin mali zimmetinde olumlu bir artış sağlamak amacıyla, internet üzerinden ticari işlemlerle ilgili gerçek dışı bilgilerin kullanılması veya mevcut bilgilerin değiştirilmesi veya silinmesiyle olur. (Türkî, 2011:96-109; Abdülhalîm, 2000:148)

Banka kartlarına yönelik saldırı durumunda da aynı hüküm geçerlidir. Bu ise birçok yöntemle gerçekleşir.

a. Casusluk Yöntemi:

İster bilinen casus yazılımlar kullanmak, ister mağdurun bilgisayarına sızmak veya onun veri alışverişi için kullandığı iletişimi sabote ederek olsun, aşılması zor güçlü koruma önlemleri aşılmak suretiyle gerçekleşen hırsızlık, haddi gerektiren bir hırsızlıktır. (Geniş Bilgi için bkz. (Türkî, 2011:90; Canbek & Sağıroğlu, 2007)

b. Aldatma Yöntemi:

Bu, meşhur web sitelerine benzeyen sahte siteler yapılması, müşterinin bu sitelere girmesi, bilgilerini vermesi, hackerlerin bunları alması ve kendi çıkarları için kullanması şeklinde olur. Mağdurun aşırı ihmalkâr davranması ve emin olmadığı bir yere bilgilerini girmesinden dolayı da bu gibi bir durumda had cezası uygulanmaz.

Hukukta, başkalarına ait kredi kart şifrelerini ele geçirmek maksadıyla, matematiksel ve istatistiksel denklemlere dayalı yöntemler kullanılarak kart bilgilerinin ifşa edilmesi ve meşru amaçlarla kullanılması halinde de, bu durum kartı veren tarafın güvenlik zafiyetine işaret eder ve o takdirde kuvvetli şüphe nedeniyle had cezası düşürülerek ta’zîr ile cezalandırılır.

Yine saldırı anlaşılmaksızın, mağdurun kullandığı cihaz aracılığıyla gizli şifrelerin ele geçirilmesi durumunda da bir kesinlik yoktur. Çünkü mağdur, gizli şifrelerini cihazda bırakarak hata etmiş, saldırgan da şifreyi sahipliğine almıştır ki bunda şüphe vardır ve cezası ta’zîrdir. (Bkz. Türkî, 2011: 99, 111-112)

Bilişim sistemini bozma, verileri yok etme veya değiştirmeye yönelik sisteme virüs bulaştırma, verileri izinsiz kopyalama, çoğaltma, dağıtma, te’lif haklarının ihlali ta’zîr cezasını gerektirir. (en-Nâhî, 1982; el-Halife, 2004: 114-133, 199)

C. Cezanın Düşmesi

İslam hukukunda hırsızlığın cezası son derece ağır olmakla birlikte İslam hukukçuları suçun oluşmasını ve cezanın uygulanmasını çok sıkı şartlara bağlamış, bu şartlardan birinin bulunmaması veya cezanın infazına engel bir durumun ortaya çıkması durumunda had cezasının düşmesi ilkesini benimsemiş. bunlara ilaveten toplumda kişileri hırsızlık suçunu işlemeye iten sebeplerin de en aza indirilmesi yönünde bir dizi tedbirden söz etmişlerdir.

Had kapsamında bir hırsızlık eyleminden bahsedebilmek için suçlu, çalınan mal ve çalma eylemiyle ilgili bazı şartlar aranır. Bunlar da çalan kimsenin (sârik) mükellef olup suç işleme kastının bulunması, çalınan malın (mesrûk) bütünüy-

le başkasına ait olması, çalınan şeyin hukuki- mali bir değer (nisab) taşıması, malın gizlice alınmış olması, çalınan malın koruma (hırsz) altında olması gerekmektedir. (Geniş bilgi için bkz. Menekşe, 1998: 23-34; Akalın, 2013:25-32; Türkî, 2011:45-52)

Bilgisayar yoluyla işlenen siber hırsızlığa had uygulanabilmesi için de suçun bu unsurlarını taşıması gerekir. Şayet unsurlar tam oluşmamış, ya da suçun unsurlarında ve ispatında herhangi bir şüphe ve tereddüt bulunması veya infaz öncesi bu kabil bir eksiklik ortaya çıkması gibi sebeplerle kanuni ceza uygulanmıyorsa suçluya ta'zîr cezası verilir. (es-Sened, 2004: 336. Ayrıca geniş bilgi için bkz. (Cello, 1990:II,11; Yiğit, 2012:118-123; Başoğlu, 2011)

Netice olarak siber hırsızlık suçlarına şer'î bir cezanın uygulanabilmesi için, öncelikle bilgisayar vasıtasıyla nakit varlıklara yönelik hırsızlık ve saldırının nasıl gerçekleştiğinin bilinmesi ve adi hırsızlık unsurları ve şartları ile bir mukayese yapılması gerekir.

SONUÇ

Fert ve toplum açısından sosyal ve hukuki bağlamda önemli sonuçları olan “Siber Hırsızlık” Örneğinde İslâm Hukukunda Siber Suçlar ve Cezası” konulu araştırmamızda varmış olduğumuz sonuçları şöyle özetlemek mümkündür:

1) Tüm dünyada günlük hayatın bir parçası haline gelen internet teknolojisi, kişiler arası arkadaşlık ilişkilerinden bankacılık işlemlerine, sağlık sektöründen ulusal güvenliğe kadar tüm alanlarda etkin bir şekilde kullanılmaktadır. Yapılan işlemlerin gerçekleştiği alan sanal bir dünya olsa da yapılan işlemlerin sonuçlarının son derece gerçek olduğu bu teknolojiye olan bağımlılık hiç kuşkusuz bireylerin hayatlarına büyük kolaylıklar getirmekle beraber aynı bireylerin maruz kalabilecekleri riskleri de artırmıştır.

Öyle ki teknolojinin kolaylaştırarak sunduğu bu altyapı suçların işlenmesinde kolaylık, suçun konusu olabilecek nesnelere çeşitlilik ve insanların birçok aktivitelerini elektronik ortam üzerine aktarması ile geniş bir platformda birçok hukuki yararın ihlal edilmesine açık bir ortam yaratılmasına da neden olmuştur. Teknolojideki hızlı gelişmenin oluşturduğu süreç değişimleri ve bilişim sistemlerinin mevcut süreçlere entegrasyonu, suç işleme niyetindeki bazı birey ve grupların teknolojiyi hem araç hem de hedef olarak kullanmasına yol açmıştır.

Nitekim bu kapsamda “bilişim suçları”, “dijital suçlar”, “internet suçları”, “yüksek teknoloji suçları” vs. gibi farklı farklı isimlendirilse de her geçen gün gelişen ve değişen siber suçlar günümüz modern toplumlarının önemli sorunlarından biri olarak günlük yaşamımızı tehdit eder hale gelmiştir.

2) Siber suç; sınır tanımayan, çözümü için işbirliği gerektiren, bilgisayar teknolojilerinin kötüye kullanıldığı, ulusal ve kamu güvenliğinin tehlikeye düşürüldüğü, bireyin esenlik ve ahlaki değerlerinin tehdit edildiği sanal alanda gerçekleştirilen bir suçtur.

3) Siber suç, bir bilişim sistemine izinsiz ve hukuka aykırı olarak girilmesi ve sonrasında yapılan bir eylemdir. Bu suçta hedef; bir kişi olabileceği gibi, kişinin mal varlığı veya bir sistemin kendisi de olabilir.

4) Günümüzde teknolojinin ilerlemesi ile birlikte, fertler ve kurumlar birçok hizmetlerini, bilişim sistemleri üzerinden gerçekleştirmekte, banka hesap takiplerini, çeşitli bilgi, kaynak ve para transferlerini hep bu sistemler üzerinden yapmaktadır. Ayrıca gerek ferdi gerekse kurumsal noktada birçok kişi, çok özel bilgilerini de bu sistemlerde saklamaktadır. İşte bu noktada özel güvenlik sistemlerinin bir şekilde devre dışı bırakılarak, sahibinin rızası hilafına bu para, bilgi ve veriler çalınabilmektedir. Ayrıca banka ve kredi kartlarının kullanılmasıyla gerçekleştirilen hırsızlık suçları da buna örnek verilebilir. Gayrı meşru yollardan kart bilgilerini ya da kartları eline geçiren kişiler, sahibinin rızası olmaksızın banka hesaplarına girip yüklü miktarlarda para çalabilmektedir. Dolayısıyla kişilere ve onların malvarlığına yönelik işlenen bu suçların cezalandırılmasına ilişkin hukuk ve ceza mevzuatlarında farklı şekillerde de olsa düzenlemeler yapılmış, çeşitli şekillerde cezai müeyyideler ortaya konmuştur.

5) İslam hukukunda da, gerek internet üzerinden yapılan yayınlarla ve gerekse hukuk dışı girişimlerle bireylerin hedef alınan malvarlıkları ile şahsiyet haklarının korunması, İslam teşri’inin ana gayeleri arasında sayılmaktadır.

6) İnternet kullanımının yaygınlaşmasıyla birlikte ortaya çıkan hak ihlallerini ve hak edilmeyen mağduriyetleri önlemenin en iyi yolu, hukukla birlikte ahlak eğitime de önem verilmesidir. Bir eylemin kötülüğünü vicdanında kabul etmemiş bir insanın onu işlememesi için hukuki ve cezai müeyyidelerin yeterli olamayacağı aşikârdır. Bu nedenle İslam, bu konuyu öncelikle ve prensip olarak iman ve ahlaka bağlamış, gerektiğinde de hukuki ve cezai müeyyideleri önermiştir.

7) Siber hırsızlık için öngörülen ceza; işlenen suçun ağırlığına denk, ibret verici yönü bulunan, hem hırsızlığa teşebbüs ve niyet eden kimseyi caydıracak, ıslah edecek, hem de toplumu bu yönde uyuracak ve gerekli tedbirleri almaya zorlayacak nitelikte bir cezadır. Öte yandan suça ceza uygulamak amaç değil belki son çaredir. Önemli olan siber hırsızlığı besleyen veya kamçılایan, kişileri bu suçu işlemeye teşvik eden sosyal dengesizlik, iktisadi ve manevi sıkıntılar, intikam alma duygusu, ihtiras, ahlaki çöküntü gibi nedenleri ortadan kaldırmak, sanal riskleri, dijital kaosları azaltacak tedbirleri almaktır. Şartlar iyileştirildikten ve gerekli tedbirler alındıktan sonra işlenen suçun cezalandırılması da adaletin

gereği ve İslam'ın toplum düzenini ve hakların himayesini sağlamadaki kararlılığının bir parçasıdır.

8) Siber hırsızlık cezasının had ya da ta'zîr olmasının belirlenmesi, cezanın infazı açısından önem arz etmektedir. Zira, had olarak kabul edildiğinde, cezanın şekli ve infazı hususunda yorum ve takdir hakkı kullanma yetkisi sınırlandırılırken; ta'zîr olması halinde bu hakkın daha geniş olarak kullanılabilme imkanı bulunmaktadır. Bir başka ifadeyle, söz konusu cezanın ta'zîr olarak nitelendirilmesi halinde, bu cezaya sebep olan şeyin suç olarak nitelendirilip nitelendirilmemesi, bu suçun kamu düzeni ile olan ilişkisi yoruma ve içtihadı açık olacaktır. Yoruma ve içtihadı açık olan bir suçun cezasının da aynı vasfı taşıması kaçınılmazdır. Nitekim günümüzde bazı İslâm ülkelerinin, özellikle bu cezayı şekil ve uygulama yönünden farklı biçimlerde kanunlaştırmaları, bu cezanın ta'zîr, yani yorum ve içtihadı elverişli olma vasfından kaynaklanmaktadır.

Notlar

- (*) Dr., DİB., Bilgi Yönetimi ve İletişim Daire Bşk.
omer.menekse@diyanet.gov.tr

Kaynaklar

- Abdülhalîm, R. M. (2000). *Cerâimü'l-İ'tida ale'l-Eşhâs ve'l-İnternet*. Kahire: Dârü'n-Nehdati'l-Arabiyye.
- Ahmed Cevdet Paşa. (1979). *Açıklamalı Mecelle : (Mecelle-i Ahkam-ı Adliye)*, yay. haz. Ali Himmet Berki. İstanbul: Hikmet Yayınları.
- Akalın, A. (2006). *İslam Ceza Hukukunda Hırsızlık Suçu ve Çalınan Mal İle İlgili İhtilaflar*. Ankara: Ankara Üniv. Sosyal Bilimler Enst. Temel İslam Bilimleri, İslam Hukuku Anabilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Akalın, A. (2013). İslam Hukuku Açısından Suçun Unsurları. *e-Şarkiyat İlmi Araştırmalar Dergisi*(10), s. 50-72.
- Akbulut, B. (1999). *Türk Ceza Hukukunda Bilişim Suçları*. Konya: Selçuk Üniv. Sosyal Bilimler Enst. Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı (Yayımlanmamış Doktora Tezi).
- Akbulut, B. B. (2000). Bilişim Suçları. *Selçuk Üniv. Hukuk Fak. Dergisi (Milenyum Armağanı)*, 8(1-2), 545-555.
- Akgündüz, A. (2011). *Islamic Public Law (Documents on Practice From The Ottoman Archives)*. Rotterdam: Iur Press.
- Al-A`ali, M. (2007). Computer Crime and the Law from an Islamic Point of View. *Journal of Applied Sciences*(7), s. 1558-1565.
- Al-A'ali, M. (2007). Cybercrime and the Law: An Islamic View. *Webology*, IV(3). 07 24, 2015 tarihinde <http://www.webology.org/2007/v4n3/a46.html> adresinden alındı
- Aldurra, F. A. (2013). *Cybercrime and Penal Code: A Comparative. Study between United Arab Emirates and Japan (Doktora Tezi)*. Japonya: Fukuoka Üniv.
- Avvâ, M. S. (2006). *Fî Usûli'n-Nizâmî'l-Cinâî'l-İslâmî*. Kahire: Dârü'l-Meârif.

- Bardakoğlu, A. (1993). Ceza. *Türkiye Diyanet Vakfı İslam Ansiklopedisi (DİA)* (Cilt VII, s. 470-478). İstanbul: Türkiye Diyanet Vakfı Yayınları.
- Bardakoğlu, A. (1998). Hırsızlık. *Diyanet Vakfı İslam Ansiklopedisi(DİA)* (Cilt XVII, s. 384-396). İstanbul: Türkiye Diyanet Vakfı Yayınları.
- Baş, E. (2015). *Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu*. Ankara: Yetkin Yayınları.
- Başoğlu, T. (2011). Ta'zir. *Diyanet Vakfı İslam Ansiklopedisi (DİA)* (Cilt XL, s. 198-202). İstanbul: Türkiye Diyanet Vakfı Yayınları.
- Bayındır, A. (1986). *İslâm Muhâkeme Hukuku: (Osmanlı Devri Uygulaması)*. İstanbul: İslami İlimler Araştırma Vakfı Yayınları.
- Beceni, Y. (2007). Siber Suçlar (Cyber Crimes) ve Bilişim Etiği. 9 16, 2015 tarihinde <https://savcibey55.wordpress.com/2007/06/03/siber-suclar-cyber-crimes-ve-bilisim-etigi> adresinden alındı
- Berber, L. K. (2004). *Adli Bilişim (Computer Forensic)*. Ankara: Yetkin Basım Yayın Dağıtım A.Ş.
- Bilmen, Ö. N. (1985). *Hukûkî İslâmîyye ve İstılahatı Fıkhîyye Kamusu*. İstanbul: Bilmen Yayınevi.
- Boğa, U. (2011). *Bilişim Suçlarıyla Mücadele Yöntemleri (Uzmanlık Tezi)*. Ankara: Radyo Ve Televizyon Üst Kurulu.
- Boynukalın, M. (2009). Suç. *Türkiye Diyanet Vakfı İslam Ansiklopedisi (DİA)* (Cilt XXXVII, s. 453-457). İstanbul: Türkiye Diyanet Vakfı Yayınları.
- Brenner, W. (2001). Is There Such a Thing as "Virtual Crime? *Berkeley Journal of Criminal Law, IV*(1). 07 13, 2015 tarihinde <http://scholarship.law.berkeley.edu/bjcl/vol4/iss1/3> adresinden alındı
- Brenner, W. S. (2004). Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement? *Rutgers Computer and Technology Law Journal, XXX*(1), s. 1-104. 09 13, 2015 tarihinde <https://www.defcon.org/images/defcon-11/dc-11-presentations/dc-11-Brenner-Susan/dc-11-brenner.doc> adresinden alındı
- Broadhurst, R. (2006). Developments in the Global Law Enforcement of Cyber-Crime. *Policing: An International Journal of Police Strategies & Management, XXIX*(3), s. 408-433.
- Büyükbaş, N. (2013). İslam Ceza Hukukunda Cezalandırma ve Maslahatların Korunması Arasındaki İlişki. *Erciyes Üniv. Sosyal Bilimler Ens. Dergisi*(34), s. 144-170.
- Canbek, G., & Sağiroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniv. Mühendislik Mimarlık. Fak. Dergisi, XXII*(1), s. 121-136.
- Cello, D. Ş. (1990). *İstifâü'l-Ukûbatü'l-Haddiyye: Dirase Mukarene fi'l-Fıkhî'l-İslâmî, ve'l-Kanunî'l-Vaz'i*. Riyad: el-Merkezü'l-Arabi li'd-Dirasatü'l-Emniyye ve't-Tedrib.
- Choo, K.-K. R. (2008, Eylül 1). Organised Crime Groups in Cyberspace: a Typology. *Trends Organ Crim, XI*(3), s. 270- 295. <https://tr.scribd.com/doc/44570634> adresinden alındı
- Civelek, D. Y. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi*. Bilgi Toplumunu Dairesi Başkanlığı (Uzmanlık Tezi).
- Crystal, J. (2001). Criminal Justice in the Middle East. *Journal of Criminal Justice, XXIX*(6), 469-482.
- Çakır, H., & Kılıç, M. S. (2014). *Güncel Tehdit: Siber Suçlar*. Ankara: Seçkin Yayıncılık.
- Çakır, H., & Sert, E. (2011). Bilişim Suçları ve Delillendirme Süreci, Örgütlü Suçlar ve Yeni Trendler, Uluslararası Terörizm ve Sınırtaşın Suçlar Sempozyumu (UTSAS 2010) Seçilmiş Bildirileri. (s. 143-170). Ankara: Polis Akademisi Yayınları.
- Dağcı, Ş. (1996). *İslam Ceza Hukukunda Şahıslara Karşı Müessir Fiiller*. Ankara : Diyanet İşleri Başkanlığı Yayınları.

- Değirmenci, O. (2002). *Bilişim Suçları*. İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü (Yayımlanmamış Yüksek Lisans Tezi).
- Dönmezer, S., & Erman, S. (1994). *Nazari ve Tatbiki Ceza Hukuku Genel Kısım*. İstanbul: Beta Basım Yayım Dağıtım.
- Dursun, H. (1998). Bilgisayar ile İlgili Suçlar. *Yargıtay Dergisi*, XXIII(3), s. 334-339.
- Dülger, M. V. (2004). *Bilişim Suçları*. Ankara: Seçkin Yayıncılık.
- Ebû Zehre, M. (ts.). *el-Ukûbe : el-Cerime ve'l-Ukûbe fi'l-Fikhi'l-İslâmî*. Kahire: Dârü'l-Fikri'l-Arabi.
- Eker, H. (2014.). *Açıklamalı-İçtihatlı Hırsızlık Suçları*. İstanbul : Legal Kitabevi.
- Eker, Ö. U. (2006). Türk Ceza Hukuku'nda Bilişim Suçları: Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu. *Türkiye Barolar Birliği Dergisi*(62), s. 101-131.
- Ekinci, M., & Esen, S. (2005). *Anlatımlı ve Gereğçeli 5237 Sayılı Türk Ceza Kanununda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar*. Ankara: Adalet Yayınevi.
- el-Beâdî, Ş. A. (23-25 Eylül 2012). Deâva el-Cerâimi'l- Elektronik ve Deâva İsbatiha fi't-Teşriati'l-Arabiyye, beyne'l-Vaki' ve'l-Me'mûl. Hartum: el-Mü'temirü's-sâli li rüesâi'l-mehâkimi'l-ulyâ bi'd-düveli'l-arabiyye.
- el-Hadimî, N. M. (2006). *el-İnternet ve Makasidü's-Şeria ve Usulihı ve Kavâ'idihı*. Riyad: Mektebetü'r-Rüşd.
- el-Halife, M. b. (2004). *Cerâimü'l-Hâsibü'l-Âli ve Ukûbetüha fi'l-Fikhi'l-İslâmî ve'n-Nizami, (Cerîmetü İstinsah Beramic Hasibi'l-âli ve Bey'ihı ve İntaci'l- Firûsat ve Neşriha)*. Riyad: Camiatu Nayifi'l-Arabiyye li'l-Ulumi'l-Emniyye = Naif Arab Universty for Security Sciences.
- el-Mehami, Y. A. (2002). *Cerâimü'l-Kompiter ve'l-İnternet*. Abu Dabi,. <http://faculty.ksu.edu.sa/6955/Documents/الانترنت/المقالات/جرام الكمبيوتر والانترنت.docx> adresinden alındı
- el-Mezmumî, M. b. (1428/2008). *Cerîmetü'l-İ'tidâ ale'l-Emvâl an Tariki'l- Hasibi'l-âli Dirase Kanuni Mukarene bi'l- Fikhi'l-İslami (Bitirme Tezi)*. Cidde: Camiatü'l-Melik Abdülaziz,.
- en-Nâhî, S. (1982). Çağdaş Mevzu Hukuklara ve İslam Hukukuna Göre Telif Hakkı (çev. Şener, Abdulkadir). *Ankara Üniv. İlahiyat Fak. Dergisi*, XXV(1), s. 237-295.
- en-Naim, B. M.-A. (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. *Information and Knowledge Management*, 3(2), 14-19. <http://www.iiste.org/Journals/index.php/IKM/article/viewFile/9642/9758> adresinden alındı
- en-Neccar, U. A. (2009). *Cerâimü'l-Hâsibü'l-âli fi'l-Fikhi'l-İslâmî*. Gazze: el-Camiatü'l-İslamiyye ; Külliyyetü's-Şeria ve'l-Kanun (Yüksek Lisans Tezi) .
- Eralp, Ö. (2004, Mart). *Bilişim Suçlusuna Giden Yol – İp*. Ekim 3, 2015 tarihinde http://www.turkhukuksitesi.com/makale_166.htm adresinden alındı
- Eralp, Ö. (2012). *İnternet Bankacılığı ve Kredi Kartı Dolandırıcılığının Teknik, Hukuki ve Cezai Boyutu*. Ankara: Adalet Yayınevi.
- Erem, F. (1991, Ekim). Bilgisayar Suçları ve Türk Ceza Kanunu. *Yargıtay Dergisi*(4), s. 436-444.
- Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum*. Ankara: Adalet Yayınevi.
- Esen, H. (2006). *İslam'da Suç ve Ceza: İslam Hukukunda Cezai Sorumluluk*. İstanbul: Akademi Yayınları.
- es-Sened, A. b. (2004). *el-Ahkâmü'l-Fikhiyye li't-Teamülati'l-Elektroniiyye : el-Hasibü'l-ali ve Şebeke'l-Ma'lumat (el-İnternet)*. Beyrut: Dârü'l-Varrak.

- eş-Şeşri, D. A. (2012, Mart 30). el-Cerâimü'l-Elektroniyye Zidde'l-Mülkiyyeti ve'l-Müctemai. <http://www.abhathoo.net.ma/content/view/pdf/19572> adresinden alındı
- Gercke, M. (2011). *Understanding Cybercrime: A Guide For Developing Countries*. Geneva: International Telecommunications Union Publication.
- Gözübüyük, A. P. (1988). *Türk Ceza Kanunu Şerhi*. İstanbul: Kazancı Yayınları.
- Grabosky, P. (2007). Requirements of Prosecution Services to Deal with Cyber Crime. *Crime Law and Social Change*, XLVII(4), 201-223.
- Gülşen, T. (2011). *Zimmet Suçu*. Ankara: Ankara Üniv. Sosyal Bilimler Enst. Kamu Hukuku (Ceza Ve Ceza Usul Hukuku) Anabilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Hira, A. (2014). Özel Hayatın Korunması: Türk Ceza Kanununda Özel Hayata ve Hayatın Gizli Alanına Karşı İşlenen Suçlarla İlgili Düzenlemenin İslam Hukuku ile Mukayesesi. *Kafkas Üniv. Sosyal Bilimler Enst. Dergisi*(13), s. 75-102.
- <http://conventions.coe.int/treaty/en/treaties/html/185.htm>. (2001).
- <http://www.startimes.com/?t=33677893>. (tarih yok). 12 01, 2015 tarihinde alındı
- https://ar.wikipedia.org/wiki/الْكَتْرُونِيَّة_جْرِيْمَة. (tarih yok). 12 01, 2015 tarihinde alındı
- İbn Âşûr, M. T. (ts.). *Makâsîdü's-Şeriatil-İslâmiyye*. Amman: Dârü'n-Nefâis.
- İbn Kudâme, E. M. (1972). *el-Mugni*. Beyrut: Dârü'l-Fikri'l-Arabi.
- İbn Nuceym, Z. Z. (1311). *el-Bahrü'r-Raik Şerhu Kenzi'd-Dekaik*. Kahire: el-Matbaatü'l-İlmiyye.
- İbn Rüşd, E.-V. M. (1985). *Bidayetü'l-Müctehid ve Nihayetü'L-Muktesid*. İstanbul: Çağrı Yayınları.
- İbnü'l-Hümmam, K. M. (ty.). *Şerhu Fethü'l-Kadir*. Beyrut: Dârü'l-Fikr.
- İçel, K., & Donay, S. (1993). *Ceza Hukuku*. İstanbul: Beta Basım Yayın.
- Illar, D. J. (2010). Cyber Fatwās and Classical Islamic Jurisprudence. *The John Marshall Journal of Information Technology & Privacy Law*, XXVII(4), s. 577-592.
- İnanıcı, H. (1996). Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü. *İstanbul Barosu Dergisi*, LXX(7-8-9), s. 508-537.
- Kahraman, A. (2008). *İslam Hukuk ve Ahlak İlkeleri Işığında Özel Hayatın Gizliliği (Mahremiyet)*. Ankara: Ebabel Yayınları.
- Karagülmez, A. (2011). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. Ankara: Seçkin Yayınevi.
- Karaman, H. (1987). *Mukayeseli İslam Hukuku*. İstanbul: Nesil Yayınları.
- Karimi, O., & Korkmaz, A. (2013). Kişisel Verilerin Korunması. *18.Türkiye'de İnternet Konferansı-net-tr'13 İstanbul Üniversitesi, 9-11 Aralık*. İstanbul. <http://inet-tr.org.tr/inetconf18/bildiri/63-uzun.doc> adresinden alındı
- Kâsânî, A. E. (1986). *Bedâiu's-Sanâi' fî Tertîbi's-Şerâi'*. Beyrût: Dârü'l-Kütübi'l-İlmiyye.
- Kaya, A. (2000). İhtilas. *Türkiye Diyanet Vakfı İslam Ansiklopedisi (DİA)* (Cilt XXI, s. 570-571). İstanbul: Türkiye Diyanet Vakfı Yayınları.
- Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yayıncılık.
- Kırcı, N. B. (2004). Korsan Üretim, Türkiye ve Dünyadaki Gelişmeler. *Ankara Barosu Dergisi*(3), s. 55-68.
- Kocabey, D. (2004). *İnternette Fikri Hakların Korunması*. Ankara: Ankara Üniv. Sosyal Bil. Enst.(Yayımlanmamış Yüksek Lisans Tezi).
- Köse, U., & Köse, U. (2015, 10 3). *Siber Suçlara Karşı Türk Hukukundaki Cezaî Yaptırımların Yeterliliği*. <http://inet-tr.org.tr/inetconf18/bildiri/36.pdf> adresinden alındı

- Kubeyî. (1971). *Ahkâmu's-Serika fî Şeriatî'l-İslamiyye ve'l-Kanun*. Bağdad.
- Kurt, L. (2005). *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*. Ankara: Seçkin Yayıncılık.
- Kutub, M. A. (2013). *Mevkîfü's-Şeriatî'l-İslamiyye, min Ceraimi'l-ahlak abra'l-* internet. Bahreyn: Merkezü'l-İlâm el-Emniyye. <http://www.policemc.gov.bh/reports/2013/October/1-10-2013/635162236055071268.pdf> adresinden alındı
- Maghaireh, A. (2008, July-December). Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cyber crime? *International Journal of Cyber Criminology (IJCC)*, II(2), s. 337-345.
- Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. *İÜHFİM*, LXXI(1), s. 855-889.
- Mancuso, S. (2007). Consumer Protection in E-commerce Transactions: a First Comparison Between European Law and Islamic Law. *Journal of International Commercial Law and Technology*, II(1), s. 1-8.
- Mason, O. R. (1986). Four Ethical Issues of Information Age. *MIS Quarterly*, X(1), s. 5-12.
- Masum, A. K. (2013). Ethical Issues in Computer use: A Study from Islamic Perspective. *Global Journal of Computer Science and Technology Interdisciplinary*, XIII(2).
- Menekşe, Ö. (1998). *XVII ve XVIII. Yüzyılda Osmanlı'da Hırsızlık Suçu ve Cezası*. İstanbul: Marmara Üniv. Sosyal Bilimler Enst. İslam Hukuku Ana Bilim Dalı (Yayımlanmamış Doktora Tezi).
- Minşavi, M. A. (1423). *Cerâimü'l-İnternet min Manzuri's-Şer'i ve Kanunî*. Mekke. 07 14, 2015 tarihinde <http://www.khayma.com/education-technology/Study33.htm> adresinden alındı
- Muhd Rosydi, B., & Marjan, B. (2003). Using Information and Communication Technology (ICT) to Disseminate the Understanding of Islamic Jurisprudence (Fiqh) and Juridical Opinion (Fatwa) : A View of Ismail et al. 18 Technologist. *In Seminar on Understanding Islam Through Techno-Da'ei*, (s. 1-28). Kuala Lumpur.
- Murat Yılmaz. (2005). Teknik Açıdan İnternet ve Telif Hakkı. *Türk Kütüphaneciliği*, XIX(1), 128-138.
- Nacar, F. B. (2010). *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları*. Ankara: Atılım Üniv. Sosyal Bilimler Enst. Avrupa Birliği Anabilim Dalı (Yüksek Lisans Tezi).
- Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact Of Cybercrime II, Center for Strategic and International Studies*. (2014, June). Aralık 02, 2015 tarihinde <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> adresinden alındı
- Norazlina, Z., Fauziah, O., & Siti Hartini, M. (2004). E-Commerce from an Islamic Perspective. *Electronic Commerce Research and Applications*, III(3), s. 280-293.
- Osman, Z. M. (2010). *es-Serikatü'l-Elektroniyye: Dirasetün Fıkhiyyetün (Yüksek Lisans Tezi)*. Ürdün: Câmîatü'l-Yermük, Külliyyetü's-Şeria ve'd-Dirâsati'l-İslamiyye.
- Önder, A. (1992). *Ceza Hukuku Dersleri*. İstanbul : Filiz Kitabevi.
- Önok, M. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (Prof. Dr. Nur Centel'e Armağan)*, XIX(2), 1229-1269.
- Özbek, V. Ö. (2002). İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları. *Doğuz Eylül Üniv. Hukuk Fak. Dergisi*, IV(1), s. 101-158.

- Özcan, M. (2004). *Siber Terörizm ve Ulusal Güvenlik, İnternet ve Hukuk*. (M. Y. derleyen: Atamer.) İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Özen, M., & Baştürk, İ. (2011). *Bilişim-İnternet ve Ceza Hukuku (Temel Hak ve Özgürlükler Bağlamında)*. Ankara : Adalet Yayınevi.
- Özkan, H. (17-19 Kasım 2011). Siber Alanda İşlenen Cinsel Taciz Suçu, 2.Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı., (s. 97–109). İzmir.
- Özkan, T. (2006). *Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi*. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü (Yüksek Lisans Tezi).
- Özpençe, Ö., & Özpençe, A. İ. (2011). Dijital Kamusal Mal ve Dijitalizm . *Uluslararası 9. Bilgi, Ekonomi ve Yönetim Kongresi Bildirileri, 23-25 Haziran 2011*, (s. 1470-1481). Saraybosna-Bosna Hersek.
- Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Kayseri: Erciyes Üniv. Sosyal Bilimler Enst., Kamu Hukuku Anabilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Pocar, F. (2004). New Challenges for International Rules Against Cyber-Crime. *European Journal of Crime, Criminal Law and Criminal Justice*, X(1), s. 27-37.
- Sagir, Y. (2013). *el-Cerimetü'l-Mürtekebe abra'l-İnternet*. Tizi Ouzou: Câmîatü Mevlûd Mameri, Külliyyetü'l-Hukuk ve'l-ULûmi's-Siyasiyye.
- Sajedi, F., & Ariani, M. G. (2014). Cyber-Crimes in Iran: Definition and Analysis . I. C.-C. Security. Kuala Lumpur, Malaysia. <http://www.academia.edu/9346464> adresinden alındı
- Serahsi, Ş. (1983). *el-Mebsût*. İstanbul: Çağrı Yayınları.
- Shuriye, A. O., & Ajala, M. T. (2014). Islam and the Cyber World". *Journal of Educational and Social Research*, 4(6), s. 513-520.
- Sinar, H. (2001). *İnternet ve Ceza Hukuku*. İstanbul: Beta Yayınevi.
- Suveyr, S. (2011). *el-Ceraimü'l-Ma'lumatiyye*. Câmîatu Ebi Bekr Bel Kâyed,Külliyyetü'l-Hukuk ve'l-ULûmi's-Siyasiyye.
- Sürer, M. (2014). *Siber Suçlar Üzerine Bir Araştırma AfyonKarahisar Örneği*. Afyon: Afyon Kocatepe Üniv. Fen Bilimleri Enst., İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Şa'ban, Z. (1990). *İslâm Hukuk İlminin Esasları (trc. İ. Kafi Dönmez)* . Ankara: Türkiye Diyanet Vakfı Yayınları.
- Şâtıbî. (1990). *el-Muvâfakât fî Usûli's-Şerî'a (İslami İlimler Metodolojisi) trc. Mehmet Erdoğan*. İstanbul: İz Yayıncılık.
- Şehitoğlu, O. (2005). *Bilgisayar ve Ağ Üzerinden İşlenen Siber Suçlarla Müdahalenin Hukuksal ve Güvenlik Boyutu*. Ankara: Kara Harp Okulu Savunma Bilimleri Enst. Güvenlik Bilimleri Ana Bilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Şirazî, E. İ. (1959-1960). *el-Mühezzebe fî Fıkhi'l-İmam eş-Şafii*. Kahire: Mustafa el-Babi el-Halebi.
- Tanılır, M. N. (2002). *İnternet Suçları ve Bireysel Mahremiyet*. Ankara: Liberte Yayınları.
- Taşkın, Ş. C. (2008). *Bilişim Suçları* . İstanbul: Beta Yayınevi.
- Tiedemann, K. (1975). Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi. (Ç. F. Yenisey.) *İÜHFM, XLI(1-2)*, s. 319-332.
- Tulum, İ. (2006). *Bilişim Suçları ile Mücadele*. Isparta: Süleyman Demirel Üniv. Sosyal Bilimler Enst. Kamu Yönetimi Anabilim Dalı (Yayımlanmamış Yüksek Lisans Tezi).
- Turhan, O. (2006). *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)*. Ankara: Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği.

- Türk Hukuk Lugatı*. (1991). Ankara: Başbakanlık Basımevi.
- Türkî, b. A. (2011). *es-Serikatü'l-Elektroniyye, Beyne'l-Haddi ve't-Ta'zîr, Dirase Ta'siliyye Mukarene Tatbikiyye*. Riyad: Camiatü Naif el-Arabiyye li'l-ulûmi'l-Emniyye (Yüksek Lisans Tezi).
- Uçak, N. Ö., & Birinci, H. G. (2008). Bilimsel Etik ve İntihal. *Türk Kütüphaneciliği, XXII(2)*, s. 187-204.
- Uçkan, Ö., & Beceni, Y. (2004). *Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Udeh, A. (1992). *et-Teşriü'l-Cinaıyyü'l-İslâmî: Mukaranen bi'l-Kanuni'l-Vaz'î*. Beyrut: Müessesetü'r-Risâle.
- Volkan Aslan. (2013). Zimmet Suçu. *İÜHFİM, LXXI(1)*, s. 43-66.
- Yavuz, Y. V. (2006). Maksadi Yorum. *İslam Hukuku Araştırmaları Dergisi*,(8), s. 41-78.
- Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları – Kriminolojik, Sosyolojik ve Hukukî Boyutlarıyla*. İstanbul: Alfa Yayınları.
- Yenidünya, A. C., & Olgun, D. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. Ankara: Legal Yayıncılık.
- Yenisey, F. (2002). İnternet Suçlarının Yeni İşleniş Biçimleri. *Uluslararası İnternet Hukuku Sempozyumu 21 -22 Mayıs 2001*, (s. 447-450). İzmir.
- Yeşil, S., & Alkan, M. (2007). İnternet Yönetişimi ve İçerik Düzenlemeleri. XII. 'Türkiye'de İnternet' Konferansı 8-10 Kasım 2007, (s. 128-135). Ankara.
- Yetim, S. (2014, Nisan). Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi. *V(17)*, s. 177-230.
- Yiğit, Y. (2012). *İslam Ceza Hukuku hükümlerinin Yürürlülüğü*. Ankara: Sistem Ofset Yayıncılık.
- Yıldız, K. (2009). Hukuka Aykırılık Kavramının Fıkıh İlmi Açısından Değerlendirilmesi. *İslam Hukuku Araştırmaları Dergisi*(13), s. 305-312.
- Yıldız, S. (2007). Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi. *Selçuk Üniv. Sosyal Bilimler Enst. Dergisi*(17), s. 609-623.
- Yılmaz, E. (2005). *Hukuk Sözlüğü*. Ankara: Yetkin Yayınları.
- Yücel, M. (1992). Bilişim Suçları. *Ankara Barosu Dergisi*(4), s. 505-512.
- Zakir, A., & Gürsel, Ö. (2010). *Bilişim Hukuku*. İstanbul: Türkiye Bankalar Birliği.
- Zorlu, S. (2010). *İnternet Yoluyla Kişilik Haklarının İhlali ve Korunması*. Konya: Selçuk Üniv. Sosyal Bil. Enst. Özel Hukuk Ana Bilim Dalı, (Yayımlanmamış Yüksek Lisans Tezi).
- Züreyr, H. B. (1980). *Mükafahatu Cerimeti's-Serika fi'l-İslâm*. Riyad: Mektebetü'l-Maârif.