Siber Suçlara Karşı Türk Hukukundaki Cezaî Yaptırımların Yeterliği

Umut Köse[1], Utku Köse[2]

[1] Anadolu Üniversitesi, Hukuk Fakültesi, Eskişehir

[2] Uşak Üniversitesi, Bilgi İşlem Daire Başkanlığı, Uşak

umuthukuk03@hotmail.com, utku.kose@usak.edu.tr

Özet: Bu çalışmanın amacı, özellikle ülkemizde yaygın olarak karşılaşılan siber suçlara karşı, mağdurların hukukî yaptırımlar anlamında nasıl korunduğunu ortaya koymak ve yine bu bağlamda; Türk hukukundaki mevcut cezaî yaptırımların yeterliği konusuna eğilmektir. Bilindiği üzere; bilgisayar ve iletişim teknolojilerinde ortaya çıkan yeni gelişmeler ve değişimler, daha etkin ve dolayısıyla tehlikeli siber suçların ortaya çıkmasına; hatta işe koşulan eski yaklaşım, yöntem ve tekniklerin yerini daha gelişmiş olanlara bırakmasına sebep olmaktadır. Bütün bu gelişmeler, hukukî anlamdaki güvencelerin ve sonuç itibariyle cezaî yaptırımların güncelliğinin sürekli sorgulanması gerekliliğini ortaya çıkarmaktadır. Açıklamalar kapsamında bu çalışma, mevcut durumun kısaca değerlendirilmesi adına bir referans niteliğinde kaleme alınmıştır.

Anahtar Sözcükler: Siber Suçlar, Bilişim Suçları, Türk Hukuku, Cezaî Yaptırımlar, Takibi Şikâyete Bağlı Suçlar.

Competency of Criminal Sanctions of Turkish Law against Cyber-Crimes

Abstract: The objective of this study is to discuss about how aggrieved people are protected against cyber-crimes; in the sense of law sanctions and evaluate current criminal sanctions from the related perspective. As it is known; improvements and developments in computer and information technologies cause more effective and more dangerous cyber-crimes to be appeared; even enable older approach, method, and techniques to give their place to the more advanced ones. All of these progresses make it necessary to evaluate always timeliness of assurances in the context of law, and so criminal sanctions. In the sense of the related explanations, this work has been written as a reference for evaluating the current situation briefly.

Keywords: Cyber-Crimes, IT Crimes, Turkish Law, Criminal Sanctions, Crimes Tracked after Complaint.

1. Giriş

Bilgisayar ve iletişim teknolojilerindeki gelişmeler, günlük hayatımızı kolaylaştırdığı gibi; sanal ortamda çeşitli suçların gerçekleşmesine sebep de olmaktadır. Bu durumun başlıca sebebi, teknolojinin insan hayatını pratikleştirmesi ve bilgiye erişim ya da bilgiyi yayma konusunda ortaya çıkardığı; karşı konulamaz yaklaşımlardır. Geçmiş süreci ele aldığımızda; kimlik bilgilerimizden, kişisel anlamda kritik değerdeki bilgilere ve hatta sahip olduğumuz maddi varlıklara kadar birçok önemli değerin sayısal sistemler kapsamında depolanmadığı dikkat çekmektedir. Söz konusu zaman diliminde yine bu varlıklara karşı ortaya çıkan çeşitli suçlar olmasına karşın; ilgili değerlerin "veri" olarak sayısal sistemlerde – bilgisayarda depolanmaya başlaması; sanal ortamda ortaya çıkan ve çeşitleri zaman içerisinde hızla artan suçların gelişmesine neden olmuştur. Her ne kadar kritik değerdeki bilgi ve varlıkların sanal ortamda temsil edilmesi, günümüz koşulları anlamında zorunluluk haline gelmiş olsa da; siber suçlar (bilişim suçları) olarak adlandırabileceğimiz suçlarla karşı karşıya kalınmasına engel olmamaktadır.

İfade edilen suçlara karşı kişilerin korunması adına; zamanla çeşitli güvenlik yaklaşımları, yöntemleri ve teknikleri geliştirilmiş; kişilerin bu güvenlik tabanlı unsurlara ilişkin olarak bilgilendirilmesi ve böylece siber suçların azaltılması konusunda genel bir çerçeve oluşturulması yoluna gidilmiştir. Ancak güvenlik tabanlı unsurlar ne kadar yaygın izlenirse izlensin; siber suçlar karşısında mağdur durumuna düşen kişiler de varlığı sürekli surette korumaktadır. Bu noktada dikkat edilmesi gereken husus; suçların ortaya çıkması durumunda mağdur kişilerin hukukî anlamda nasıl korunduğu ve yine mevcut cezaî yaptırımların bu korumayı sağlamak adına ne kadar güncel, etkin ve yeterli olduğunu düşünmektir. Kısacası, güvenlik tabanlı yaklaşım, yöntem ve tekniklerin geliştirilmesinin yanında, hukukî anlamda ne gibi korunma yollarına ve haklarına sahip olduğumu bilmek, önemli bir konudur.

Açıklamalar paralelinde bu çalışmanın amacı; özellikle ülkemizde yaygın olarak karşılaşılan siber suçlara karşı, mağdurların hukukî yaptırımlar anlamında nasıl korunduğunu ortaya koymak ve yine bu bağlamda; Türk hukukundaki mevcut cezaî yaptırımların yeterliği konusuna eğilmektir. Bilindiği üzere; bilgisayar ve iletişim teknolojilerinde ortaya çıkan yeni gelişmeler ve değişimler, daha etkin ve dolayısıyla tehlikeli siber suçların ortaya çıkmasına; hatta işe koşulan eski yaklaşım, yöntem ve tekniklerin yerini daha gelişmiş olanlara bırakmasına sebep olmaktadır. Bütün bu gelişmeler, hukukî anlamdaki güvencelerin ve sonuç itibariyle cezaî yaptırımların güncelliğinin sürekli sorgulanması gerekliliğini ortaya çıkarmaktadır. Nitelik bağlamında bu çalışma, mevcut durumun kısaca değerlendirilmesi adına güncel bir referanstır.

Konu kapsamında, çalışmanın ilerleyen bölümleri şu şekille şekillendirilmiştir: Bir sonraki bölüm altında siber suç kavramının ne olduğu, ilgili kavramın kapsamı ve ülkemizde yayın durumdaki siber suçlara değinilmiştir. Ardından, üçüncü bölüm altında; söz konusu siber suçlar karşısında Türk Hukuku kapsamındaki temel cezaî yaptırımların neler olduğuna odaklanılmış ve bu bölümü takiben, dördüncü bölüm altında; açıklanan yaptırımların yeterliği konusunda değerlendirmelere yer verilmiştir. Çalışma "Sonuçlar ve Öneriler" bölümü altındaki açıklamalarla birlikte sona erdirilmiştir.

2. Siber Suç Kavramı, Kapsamı ve Türkiye'de Yaygın Durumdaki Siber Suçlar

Günümüzde teknolojinin gelişmesiyle orantılı olarak bilişim sistemleri kullanılarak işlenen suçlarda da artış yaşanmaktadır. Siber suç, suçun fail ya da failleri tarafından bilişim

sistemi kullanılarak başka bir bilişim sisteminin güvenliğini, buna bağlı verileri ya da kullanıcısına yönelik işlenen suçtur [1]. Tanımda bahsettiğimiz bilişim sistemleri, 5237 sayılı TCK'nın (Türk Ceza Kanunu) 243. maddesinin gerekçesine göre "…verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir" şeklinde tanımlanmıştır [2]. Siber suçlar genel olarak, bilişim sistemi aracılığıyla başka bir bilişim sistemine yönelik olarak işlenebilir. Bunun dışında diğer iletişim araçlarıyla (telefon, faks… vb.) işlenen suçlar (örneğin; telefonla aldatarak veri hırsızlığı) niteliği itibariyle bilişim sistemi sayılamayacağından; siber suçlar kapsamında da yer almamaktadır. Siber suçlar genel olarak; 5237 sayılı TCK'nın Onuncu Bölümü'nde 243 ile 246. maddeler arasında düzenlenmiştir. Ayrıca 5651 sayılı Kanun ve 5846 sayılı FSEK'in (Fikir ve Sanat Eserleri Kanunu) ilgili maddelerinde ve diğer kanunlarda çeşitli siber suçlar tanımlanmıştır [2].

Siber suçlar takibi şikâyete bağlı olan suçlardır. Yani suçun cezaî yaptırımının sağlanabilmesi için ilgili makamlara bu suç bildirilmelidir. Aksi takdirde bu suç hakkındaki adlî işlemler başlamayacaktır. Takibi şikâyete bağlı olan suçlar da şikâyet süresinde yapılmalıdır. Şikâyet süresi, siber suçun faili ve bu suçun fiilinin öğrenilmesinden itibaren altı aydır. Şikâyet süresinde yapılmadığı takdirde, işlenen siber suçun soruşturulması ve kovuşturulması yapılamamaktadır [3].

Ceza hukukunun suçun kanunîliği ve kanunsuz suç ve ceza olmaz ilkeleri doğrultusunda Türk hukukundaki yaygın olarak işlenen siber suçları şu şekilde sıralayabiliriz [4]:

- 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.

- Diğer siber suçlar (Örneğin; çocuk pornografisi ya da sanal ortamdaki telif haklarının ihlali).

Söz konusu siber suçlara karşı, bu suçların mağduru durumundaki kişilerin, hukukî açıdan izleyebilecekleri çözüm yollarını ve bu bağlamdaki cezaî yaptırımları kısaca ifade etmemiz, konu kapsamı açısından yerinde bir yaklaşım olacaktır.

3. Siber Suçlara Karşı Türk Hukukundaki Cezaî Yaptırımlar

Bir önceki bölüm altında da ifade edilen; Türkiye'de yaygın durumdaki siber suçlar karşısında, hukukî bağlamda izlenecek işlem adımlarını ve ilgili cezai yaptırımları şöyle açıklamak mümkündür:

Kullanıcıların sanal kimliklerine ilişkin suçlar: Gerek ülkemizde, gerekse dünya çapında işlenen en yaygın siber suçlardan birisi, kullanıcıların Internet ya da daha genel anlamda dijital ortamdaki sanal kimliklerinin çalınması ya da kötüye kullanılması doğrultusunda ortaya çıkmaktadır. Bu tarz siber suçları kısaca sanal kimliklere ilişkin suçlar olarak ifade etmemiz mümkündür. Daha detaylı olarak ilgili suçlar, -özellikle

günümüzde oldukça sık karşılaşılan- banka veya kredi hesaplarının kötüye kullanılması olacağı gibi, Internet ortamındaki Facebook benzeri sosyal medya platformlarında kullanılan kimliklerin (profil) çalınması ve kötüye kullanılması şeklinde ortaya çıkabilmektedir. Bu noktada; sanal kimliklerin çalınması, kullanıcıların farkına varamadıkları casus yazılımlar ile (Örneğin; keylogger yazılımları) yapılabildiği gibi, donanımsal ve yazılımsal açıklardan faydalanarak ya da kişiler üzerinde sosyal mühendislik yaklaşımları uygulanarak da yerine getirilebilmektedir.

Daha önce de bahsedildiği üzere, takibi şikâyete bağlı olan suçlardan olan bu tarz siber suçlara karşı çeşitli adımların izlenmesi, sonuca ulaşma noktasında kişilere faydalı olmaktadır. Bu bağlamda, burada bahsi geçen sanal kimliğe ilişkin suçlara karşı etkili ve sağlıklı çözüm elde etmek adına şu adımların izlenmesinde fayda bulunmaktadır [1]:

- Güvenli bir bilgisayardan ilgili hesabın kurtarılması denenmeli; eğer kurtarma işlemi başarılı olmazsa, hesabın olduğu Web sitesinin ilgili birimlerine şikâyette bulunulmalıdır.

- Adli işlem yapılabilmesi için şahsi müracaat yapılması şarttır. Bu noktada; işlemin eksiksiz başlaması için, ilgili emniyet şubelerinde ya da savcılıkta temin edilebilecek örnek müracaat formu doldurulmalıdır (Söz konusu form, ilgili emniyet müdürlüğünün Web sitesinden de elde edilebilmektedir).

- Form el yazısıyla doldurup imzalandıktan sonra; form ile birlikte suçun işlendiği yerdeki polis merkez amirliğine, Cumhuriyet Başsavcılığı'na ya da Siber Suçlarla Mücadele Şube Müdürlüğü'ne müracaat edilmelidir.

Bu suçu işleyen kişi TCK'nın 243. maddesine göre 1 yıla kadar hapis veya adli para cezası ile cezalandırılmaktadır. Ek olarak; bilgisayar sistemindeki verilerinin silinmesi ya da değiştirilmesi halinde ise, suçun faili için bu suçun cezası altı aydan iki yıla kadar hapis cezasıyla sonuçlanmaktadır [3].

Açıklanan siber suç, banka veya kredi hesaplarının kötüye kullanılması yönünde ise; siber suçu işleyen kişi, 5237 sayılı TCK'nın 245. Maddesi hükümlerince cezalandırılmaktadır. Böyle bir suçla karşılaşılması hâlinde yapılması gerekenleri ise kısaca şu şekilde sıralayabiliriz [1]:

- İlgili banka ile görüşüp şüpheli görülen harcamanın / harcamaların ekstresi temin edilerek, kişiye ait olmayan harcamalar belirlenmeli; gerekirse bağlı doküman çıktıları elde edilmelidir.

- İşlemin eksiksiz başlaması için hazırlanan örnek müracaat formu elde edilip, el yazısıyla doldurulmalı ve imzalanmalıdır. Ardından, ilgili form ile suçun işlendiği yerden sorumlu polis merkez amirliğine, Cumhuriyet Başsavcılığı'na ya da Siber Suçlarla Mücadele Şube Müdürlüğü'ne müracaat edilmelidir.

Ancak bu suçun işlenmesinde dikkat edilmesi gereken bir husus vardır. Bu husus, 5237 sayılı TCK'nın 245. Maddesinin 4. fıkrasında düzenlenmiştir. Buna göre; banka veya kredi hesaplarının kötüye kullanılması suçu, haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecedeki kayın hısımlarından birinin veya evlat edinen veya evlatlığın, aynı konutta beraber yaşayan kardeşlerden birinin zararına işlenmesi hâlinde ilgili akrabaya ceza hükmolunamayacaktır. Yani bu suçun faili bu fıkradaki sayılan kişilerden birisi ise, hakkında bu suç için cezaî işlem yapılamayacaktır [3].

Dijital olarak depolanmış verilerde sahtekârlık ve söz konusu verilerin değiştirilmesi, silinmesi: Bu suçun işlenebilmesi için, başka bir bilgisayardan, hedef bilgisayardaki verilerden hareketle sahtekârlık veya bu verilerin değiştirilip silinmesi yaklaşımı izlenmiş olmalıdır. Örneğin; bir bilgisayara başka bir bilgisayar kullanıcısı, uzaktan erişip kullanabilmiş ve sonuç olarak bilgisayar verileri kendisine kopyalamış ya da silmiş ise şu hususlara dikkat edilmelidir [1]:

- Öncelikli olarak suça maruz kalan bilgisayara format atılmamalı ya da herhangi bir işlem yapılmamalıdır.

- Daha önce de ifade edilmiş olduğu gibi; örnek müracaat formu el yazısıyla doldurup imzalanmalı ve form ile birlikte suçun işlendiği yerden sorumlu polis merkez amirliğine, Cumhuriyet Başsavcılığı'na ya da Siber Suçlarla Mücadele Şube Müdürlüğü'ne müracaat edilmelidir.

Bu suçu işleyenler hakkında TCK'nın 244. Maddesinin 2. fıkrasına göre 6 aydan 3 yıla kadar hapis cezası ile ortaya çıkmaktadır. Suçun banka veya kredi kurumlarına karşı işlenmesi hâlinde suçun cezası yarı oranında artırılmaktadır [3].

Bilgisayar virüslerinin ve diğer zararlı unsurların dağıtılması – bulaştırılması: Bir bilgisayara, Internet'ten indirilen dosyalar ya da başka bir yerden kopyalanmış dosyalar aracılığıyla virüs yazılımı bulaşabilmektedir. Ancak buna benzer unsurların bilgisayara bulaşmış olması, suçun oluşması için yeterli değildir. Bu zararlı unsurların suç oluşturabilmesi için, bilgisayarda kanundaki yazılı neticeleri doğuracak fiillerin gerçekleşmesi gerekmektedir.

Örneğin, bilgisayara bir Worm (solucan) zararlı yazılımı bulaştıktan sonra, bilgisayardaki verilerde bir zarar oluşmuyor ya da kişiye yönelik herhangi bir problem ortaya çıkmıyor; sadece bilgisayarın performansında yavaşlama söz konusu ise; bu durum bir siber suç olmayacaktır. Ancak, bilgisayarın işleyişi engelleniyorsa, siber suç işlenmiş olacak (TCK m.244/f.1) [3] ve bu nedenle ilgili makamlara başvurarak, gerekli adlî işlemlerin başlatılmasının önü açılmış olacaktır.

Bilgi teknolojileri sistemlerine yönelik saldırılar: Bu siber suç türü, doğrudan bilgisayara karşı işlenen ve seçimlik hareketli bir suç olup, TCK'nın ilgili maddelerinde nitelikli hâlleriyle birlikte düzenlenmiştir. Buna göre:

- 5237 sayılı TCK'nın 244. Maddesinin 1. fıkrasına göre, bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılmaktadır [3].

- TCK'nın 244. Maddesinin 2. fıkrasına göre, bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılmaktadır [3].

- TCK'nın 244. Maddesinin 3. fıkrasına göre, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılmaktadır [3].

- TCK'nın 244. Maddesinin 4. fıkrasına göre, bilgi teknoloji sistemlerine yönelik saldırı fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş

bin güne kadar adlî para cezasına hükmolunmaktadır [3].

Söz konusu suçla karşılaşılması hâlinde, mağdurların, daha önceki alt-başlıklar kapsamında ifade edilen suç türlerinde izlenen adımları uygulamaları gerekmektedir [1].

Diğer siber suçlar: Diğer siber suçlardan başlıca hukuka ve genel ahlâka aykırı verilerin bulundurulması suçuna değinilmelidir. Bu bağlamda, ilgili verilerin bulundurulması ve yayınlanması durumunda; TCK m.226'da düzenlenmiş olan "müstehcenlik suçu" işlenmiş olacaktır [3].

Böyle bir siber suç ile karşılaşıldığı takdirde, ilgili suçun ihbar edilmesi gerekmektedir. Ancak suçu işleyen kişiye karşı etkili bir çözüme ulaşılması için şu adımların takip edilmesi gerekmektedir [1]:

- Müstehcen – pornografik içeriğin olduğu Web sayfasının ekran görüntüsü alınmalı,
- Tespit edilen; örneğin çocuk pornografisi görüntüsü yer alan Web sayfasının adres bilgisi not alınmalı,
- İşlemin eksiksiz başlaması için hazırlanan örnek müracaat formu elle doldurulup imzalanmalı ve formda, şikâyet edilecek Web sitesinin – sayfasının adresini eksiksiz belirtmeye dikkat edilmelidir.
- Aynı zamanda, ilgili Web sitesini – sayfasını Telekomünikasyon İletişim Başkanlığı İnternet Bilgi İhbar Merkezi'nin; "ihbarweb.org.tr" Web adresine ya da bulunulan yerdeki Siber Suçlar Şube Müdürlüğü'nün ihbar hattı adresine Web site – sayfa adres bilgisi ve ekran görüntüsü ile ihbar etmek mümkündür [1].

İfade edilen çözüm – işlem adımları ve ilgili cezaî yaptırımlar bağlamında düşünüldüğünde, hukukî süreçlere sıklıkla konu olan bazı problemler de ortaya çıkabilmektedir. Söz konusu bu problemler; ilgili hukukî yaklaşımların yeterliği çerçevesinde birtakım değerlendirmeler yapılması gerektiğini, bizlere anlatmaktadır.

4. Yeterliğe Dair Bazı Değerlendirmeler

Bir önceki bölüm altında ifade edilen cezaî yaptırımların yeterliğine dair yapılacak değerlendirmeler; özellikle günümüz siber suçları bağlamında söz konusu olabilecek açıkların ya da dikkat edilmesi gereken temel durumların kısaca ortaya konulması adına önemlidir. Buna göre, "yeterliğe dair değerlendirmeler" yaklaşımı altında ifade edebileceğimiz bazı hususlar şunlardır:

- Özellikle 5237 sayılı TCK'nın, siber suçlarını sadece dört madde olarak düzenlemesi; her geçen gün gelişen teknoloji ve ortaya çıkan yeni tehditler düşünüldüğünde, yeni oluşan siber suçların suçun kanunîlik ilkesi kapsamında cezasız kalmasına yol açabilmektedir. Buna göre, siber suçlarıyla mücadelede alınması gereken önlemler bağlamında; ceza hukuku normlarıyla bu konuyla ilgili kamu düzenin ihlali olarak görülen eylemlerin suç tipi olarak tanımlanması, siber suçların kapsam ve niteliği ayrıntılı bir şekilde açıklanması ve gerekli yasal düzenlemelerin yapılması, açıkların ortadan kaldırılması adına etkili olacaktır [5].
- Uygulama aşamasında, işlenen bir siber suçun faili, siber suçların nitelikli hâlleri ayrıntılı düzenlenmediği ve sadece takdiri indirim nedenleriyle (faile uygulanarak yapılan yargılama sonunda hükmolunan ceza, iki yıl veya daha az süreli hapis cezası

olduğu için), "hükmün açıklanmasının geri bırakılması" kararı verilerek (5271 sayılı CMK m.231'e göre) [6] gerektiğinden daha az ceza alabilmektedir. Bu durum, mevcut kanunların işlenen suçun cezasının belirlenmesinde yetersiz olmasından kaynaklanmaktadır. Bu nedenle daha detaylı düzenlemelerin, ilgili kanunlar altında gerçekleştirilmesi son derece önemlidir.

- Daha önce bahsettiğimiz; 5237 sayılı TCK'nın 245. Maddesinin 4. Fıkrasında belirtilen kişilere karşı banka veya kredi hesaplarının kötüye kullanılması suçu işlenmesi hâlinde ilgili akrabaya ceza hükmolunamayacağı durumu [3], işlenen pek çok siber suçun cezasız kalmasına yol açabilmektedir. Hâlbuki siber suçlar, ilgili fıkradaki kişilere karşı daha kolay işlenebilmektedir. Bu bağlamda, gerekli önlemlerin ilgili hukuksal yaklaşımlar dâhilinde alınması gerekmektedir.

- Siber suçları kovuşturan birimlerin, değişen veya yeni ortaya çıkan şartlara karşı uyumlu olmaları adına, devamlı surette eğitim süreçlerine tabi tutulmaları önemlidir. Buna göre; özellikle hâkimlerin, polislerin ve savcıların, ilgili siber suçlarının niteliği ve delillerin elde edilmesi; ya da analiz, karar gibi faktörler açısından etkin eğitim süreçleri dâhilinde olması gerekmektedir [5].

5. Sonuçlar ve Öneriler

Siber suçlar, ne kadar etkin önlemler alınırsa anılsın; sayısal sistemlerin – bilgisayar sistemlerinin veri işletimi ve düzenlenmesi konusunda işe koştuğu yaklaşımlar bünyesinde ortaya çıkan çeşitli açıkların değerlendirilmesi suretiyle geliştirilmeye devam etmektedir. Bunun yanında, sosyal mühendislik adı verdiğimiz; insan faktörünün zaaflarını hedef alan yaklaşımlar da, bilişim suçlarının işlenmesi yönünde zincirin zayıf halkası niteliğinde olan kişilerin sosyal yönden kötü amaçlar doğrultusunda kullanılmasına neden olmaktadır. Siber suçları kapsamındaki bütün yaklaşım, yöntem ve teknikler; hukukî anlamda çeşitli güvenceler ve çeşitli yaptırımlar ise cezasız kalmamasına rağmen; yine hukukî anlamdaki çeşitli açıkların kullanılmasına da engel olamamaktadır.

Çalışma içerisinde ifade edilen hukukî durum; Türk hukukunun güncelliği konusunda çeşitli değerlendirmelerde bulunmamıza ve bu yönde bazı önerilerin de dolaylı yönden sunulmasına sebep olmuştur. Bu noktada bütün hukukî açıkların ve yaptırımlar konusundaki kötüye kullanım yönlerinin ortadan kaldırılması adına; daha genel çapta bazı önerilerde bulunmamız mümkündür. Söz konusu önerileri kısaca şu şekilde ifade edebiliriz:

- Çalışmadan ve söz konusu incelemelerden – değerlendirmelerden çıkacak en önemli ders; teknolojideki gelişmeler paralelinde gelişimine devam eden siber suçlara karşı, hukuksal düzenlemelerde de eş zamanlı hızda gelişmelere gidilmesi gerekliliğidir. Teknolojik gelişmeler ne kadar hızlı olursa olsun; hukukî kapsamdaki gelişmelerin de bu doğrultuda hızlı yerine getirilmesi gerekmektedir. Bu bağlamda, gerekli düzenleme ve güncellemelerin takibini daha etkin yapacak; hukukçu, akademisyen gibi konusunda etkin kişilerin yer aldığı ilgili birimlerin kurulması önerilebilir.

- Değerlendirmelerde ifade bulmuş olan en önemli unsurlardan birisi olan "eğitim" faktörü, siber suçlara

karşı gerekli düzenlemelerin yapılması, önlemlerin alınması ve hatta mağdur duruma düşme potansiyeli olan kişilerin bilinçli hale getirilmesi doğrultusunda son derece önemlidir. Unutulmamalıdır ki; siber suçlara karşı bilinçli durumda olan kişiler; söz konusu suçların önlenmesi ve azaltılması yönünde anahtar rol oynayacaktır.

- Hukuksal düzenlemelerin gerçekleştirilmesi noktasında önerilebilecek diğer bir unsur da; uluslararası platformdaki hukuksal gelişmelerin ve düzenlemelerin de takibinin iyi yapılması gerekliliğidir. Her ne kadar bir noktadan sonra gerekli düzenlemelerin ülkemiz sınırları dâhilimdeki değişken durumlara göre gerçekleştirilmesi daha iyi olsa da; küresel bağlamdaki gelişmelerin takipçisi olunması da etkin ve hızlı düzenlenmelerin yapılması ve gerekli önlemlerin alınması adına oldukça yararlı olacaktır.

Kaynaklar

[1] İstanbul Siber Suçlarla Mücadele Şube Müdürlüğü: http://sibersuclar.iem.gov.tr/siber_suclari.html, 2013.

[2] 5237 sayılı Türk Ceza Kanunu Gerekçesi: www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc, 2013.

[3] 5237 sayılı Türk Ceza Kanunu, Beta Yayınları, 2013.

[4] Evik V., Sınar H., Erman B., Kurt G., 'Bilişim Hukuku', Güncel Hukuk Dergisi, 2013, s. 17-18.

[5] Keçeci, O, 'Siber Suçlar ve Siber Terörizm': http://www.academia.edu/2333087/Siber_Suclar_ve_Terorizm, 2012.

[6] Centel N., Zafer H., Çakmut Ö., 5271 sayılı Ceza Muhakemesi Kanunu, 2013.