Bilişim Suçları İle Mücadelede Karşılaşılan Sorunlar

Baki Yiğit ÇAKMAKKAYA [1] **Teoman AKPINAR [2]**

[1]C.Savcısı, yigitcakmakkaya@gmail.com, Sorumlu Yazar

[2]Doç.Dr., takpinar@nku.edu.tr

Özet: İnternet kullanımı insanlar için önemli faydalar sağlarken eğitim, kültür, sanat, iletişim ve diğer tüm alanlarda insanların bilgiye erişimini de kolaylaştırmış ve hızlandırmıştır. Ancak internet yoluyla yapılan yayınlarda kişilerin veya kurumların haklarının ihlal edilmesi, suç işlenmesi de söz konusu olabilmektedir. Bilişim yoluyla işlenen suçlar 5237 Sayılı Türk Ceza Kanunu'nda düzenlenirken internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yolu ile işlenen suçlarla mücadele edilmesi 5651 Sayılı yasa ile hukukumuza girmiştir. Bilgisayar teknolojilerinin süratli gelişimi karşısında ilgili yasaların uygulanmasında sorunlarla karşılaşılmaktadır. Anılan sorunları uluslararası anlaşmalardan kaynaklanan eksiklikler, yasal düzenlemelerdeki yetersizlikler, uygulayıcıların niteliklerinden kaynaklanan sorunlar ve teknik problemler olarak dört başlık altında değerlendirmek mümkündür. İnternet ortamında yapılan ihlallerin giderilmesi hukuka uygun davranılmasının sağlanması ile internet ortamında işlenen suçlar ile etkin mücadele edilerek kamu düzeni ve şahıs haklarının daha ileri seviyede korunabilmesi amacıyla yapılabileceklere dair önerilerimiz çalışmada yer almaktadır.

Anahtar Kelimeler: suç, internet, ceza hukuku, 5651 Sayılı Kanun, internet hukuku, yasa uygulayıcıları

Problems Encountered On Fight Against Cyber Crimes

Abstract: Internet use has facilitated and expedited people's access to information in the fields of education, culture, art, communication and other while providing significant benefits. However, any publishing via Internet can violate individuals' or institutions' rights and lead to committing an illegal act. Cyber crimes are regulated under the Turkish Criminal Code no 5237, while regulation of publications on Internet and fight against offences committed through such publications have been included in the Turkish legal system with the Act no 5651. When implementing relevant laws, problems are encountered as result of rapid improvements in computer technologies. The aforesaid problems can be handled under four headings, namely deficiencies arising from international agreements, deficiencies in legislative regulations, problems stemming from qualification of the executives and technical problems. This study contains our proposals on actions to be taken aiming the elimination of violations on Internet, ensuring compliance with law and further protection of public order and individual rights more effectively by fighting offences committed on the Internet.

Key words: offence, Internet, criminal law, Act no 5651, Internet law, legislation officers

GİRİŞ

Bilgi teknolojilerindeki hızlı gelişme bilgisayar ve internet kullanımını artırırken bu alanda kötüye kullanımları ve hukuk ihlallerini de beraberinde getirmiştir. Kişilik haklarının ihlalini doğuran, tehdit, taciz suçları, hakaret suçları yanında kamu düzenini ciddi anlamda bozan suçlar da kullanıcı sayısına bağlı olarak artmaktadır. İnternetin hukuki normlara uygun olarak kullanılabilmesi için kullanıcıların yasalara uymaya özen göstermesi gerekmektedir. Yasalara uymayı reddeden kişiler için ise hukuki yaptırımların uygulanması çağdaş hukukta bir gerekliliktir. Yasaları uygulayan hukukçuların yasalara uymayanlara gerekli cezayı verebilmesi için " Suçta ve Cezada Kanunilik İlkesi " gereği, kanunlarda bu konularda ilgili düzenlemelerin yapılmış olması gerekmektedir. Braman'a göre; herkesin yararı gözetilerek oluşturulacak olan bir İnternet siyasasında: İnternete erişim, İçeriğe erişim, Fikri mülkiyet hakları, Özel hayatın gizliliği/mahremiyet gibi dört temel unsurun dikkate alınması gerekmektedir (Braman 2011'den akt.,Özdemir, 2015:85). Proaktif adli yaklaşımla bilişim yoluyla yapılan maddi ve manevi zararlara engel olmak ve suç işleyen kişileri cezalandırabilmek için hukuki düzenlemelerin yeterli ve tam olması ve bu kurallara uyulmasının sağlanması için uygulamada eksiklik bulunmaması gerekmektedir (Henkoğlu ve Uçak, 2012:379). Ülkemizde bilişim suçları ile ilgili genel hükümler 5237 Sayılı TCK'da yer alırken, suç teşkil eden içeriğin çıkarılması, ve bilişim yoluyla işlenen suçlarda teknik konuların düzenlenmesi 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da yer almaktadır. Anılan kanun internete dair yürürlükte olan temel kanundur. 5651 Sayılı Kanun, her ne kadar internet üzerinden yapılan ve suç teşkil

edebilecek yayınlara ilişkin çeşitli düzenlemeler içermekte ise de, özellikle kişilik haklarının korunması, suç teşkil eden içeriğin yayından kaldırılmasına dair karar alınması süreci, alınan kararın uygulanması konularında yetersiz kalmaktadır. Yine TCK'da yer alan suçların delillerinin toplanması, faillerinin tespit edilmesi ve cezalandırılması hususlarında da uygulamada ciddi aksaklıklar ile karşılaşılmaktadır. Çalışmamızda öncelikle, bilişim suçları konusundaki yasal düzenlemeler başlığı altında Türk Ceza Kanunu ve 5651 Sayılı Kanun ile yapılan düzenlemelere yer verilmiş; daha sonra ise bilişim suçları ile mücadelede uygulamada yaşanan sorunlar başlığı altında uluslararası antlaşmalardan kaynaklanan eksiklikler, ulusal yasalardaki boşluklar ve infaz sorunları, yasa uygulayıcılarından kaynaklanan sorunlar ve teknik sorunlar incelenmiştir.

1. Bilişim Suçları Konusundaki Yasal Düzenlemeler

1.1. Türk Ceza Kanununda (5237 Sayılı) Bilişim Yoluyla İşlenen Suçlar

Teknolojik cihazlar yardımı ile internet ortamında işlenen suçları bilişim suçları olarak adlandırabiliriz. Bilişim alanında işlenen suçlar; bilişim sistemlerine karşı işlenen suçlar ve bilişim sistemleri ile işlenen suçlar olarak iki gruba ayrılabilir. İlk durumda, bilişim sistemlerinde bulunan bilgilerin karakteristiği yani; gizliliği, bütünlüğü ya da erişilebilirliği hedef olmaktadır. Bilişim sistemi tarafından sağlanan hizmetler, depolanan, alınan ve gönderilen veriler ya da donanım olarak ifade edilen kurban bilgisayarlar zarar görmektedir. Servis Dışı bırakma (Denial of Service- DoS) saldırıları bu gruba örnek verilebilir. İkinci durumda yer alan suçlar ise; siber terörizm, çocuk pornografisi, nitelikli dolandırıcılık, fikri mülkiyet hakları ihlalleri ve yasadışı maddelerin çevrimiçi satışı gibi suçlardır. Bilişim suçları; TCK 5273'ün 10. Maddesinde yer alan "Bilişim Alanında İşlenen Suçlar" başlığının 243, 244 ve 245'inci maddelerinde ele alınmaktadır (Gönen, 2016:230). TCK, Md.243'te*, Bilişim sistemine girme* başlığı altında, "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir" hükmü yer almaktadır. Yine aynı maddede, "Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır (Md.243/4)" hükmüne yer verilmiştir. *TCK,* Md.244'te, *Sistemi engelleme, bozma, verileri yok etme veya değiştirme başlığın altında* "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. 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 cezalandırılır. Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunacağı" ifade edilmiştir. *TCK, Md.245'te ise Banka veya kredi kartlarının kötüye kullanılması* başlığın altında "Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır" hükmüne yer verilmiştir.

İlave olarak, 5237 Sayılı Türk Ceza Kanunu'nun ikinci kısmı olan kişilere karşı suçların, dokuzuncu bölümünde, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında; "kişisel verilerin kaydedilmesi (Md.135)", "kişisel verileri hukuka aykırı olarak verme ve ele geçirme (Md.136)" ve "verileri yok etme (Md.138)" suçları konularında düzenlemeler yapılmıştır. TCK'nın ikinci kısmı olan kişilere karşı suçların onuncu bölümünde, "Mal varlığına Karşı Suçlar" başlığı altında madde 142 ile hırsızlık suçunun nitelikli hali olarak bilişim sistemlerinin kullanılması yolu ile hırsızlık ve madde 158 de dolandırıcılık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde nitelikli dolandırıcılık olarak tanımlanarak cezanın ağırlaştırıcı sebebi olacağı vurgulanmıştır. TCK'nın ikinci kısmındaki yedinci bölümü olan "hürriyete karşı olan suçlar" altında madde 124 teki "haberleşmenin engellenmesi", aynı kısmın sekizinci bölümü olan "şerefe karşı suçlar" başlığı altında madde 125 deki "hakaret", aynı kısmın, dokuzuncu bölümünde, "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında madde 132 deki "Haberleşmenin gizliliğinin ihlali" ile madde 133 deki "kişiler arasındaki konuşmaların

dinlenmesi – kaydedilmesi" suçları ve topluma karşı işlenen suçlar kısmının yedinci bölümünde ise "Genel ahlaka karşı işlenen suçlar" adı altına madde 226 da yer alan "müstehcenlik suçu" da bilişim suçu olarak adlandırılmamış olsalar da bilişim vasıtası ile işlenebilecek suçlardandır.

1.2. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yolu İle İşlenen Suçlarla Mücadele Edilmesi Hakkında 5651 Sayılı Kanun

5651 Sayılı Kanun diğer tüm kanunlarda olduğu gibi toplumsal ihtiyaçlar nedeniyle ortaya çıkmıştır. 4 Mayıs 2007 tarihinde 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" adıyla internet konusunda temel yasa çıkarılmıştır. 23 Mayıs 2007 tarihinde de Resmi Gazete'de yayımlanmıştır. Kanun'un uygulama yetkisi Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) verilmiştir ve yürütme, Kurum bünyesinde bulunan Telekomünikasyon İletişim Başkanlığı'na (TİB) bağlı İnternet Daire Başkanlığı tarafından başlatılmıştır (Gök, 2012:17).

5651 sayılı Yasanın çıkarılmasının iki amacı bulunmaktadır. Birincisi; İnternet'in önemli aktörlerinden olan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını belirlemektir. Diğer amaç ise; İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir (https://birimler.dpu.edu.tr/app/views/panel/ckfinder/userfiles/2/files/mevzuatlar/5651_Say_l__Kanun.pdf , Erişim Tarihi (E.T.) 29.09.2018).

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 1 inci maddesinde Kanun'un amaç ve kapsamı ifade edilmiştir: " İçerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir ". Bu kanunla elektronik ortamda çocuğa, gençliğe ve aileye yönelik ağır ve vahim nitelikteki saldırıların önlenmesi hedeflenmiştir. 5651 Sayılı Kanun'a 06.02.2014 yılında 9/A maddesi eklenmiştir. Bu madde ile İnternet ortamında yer alan ve özel hayatı ihlal eden bir içerik nedeniyle söz konusu İnternet sitesine erişim engelleme imkânı getirilmiştir. 5651 Sayılı Kanun, Anayasamızın, özel olarak korunmasını öngördüğü, başta aile, çocuklar ve gençler olmak üzere belirli sosyal kesimlere yönelik suçların kolayca işlenmesini önlemeyi hedefleyen özel nitelikli bir kanundur (Kılınç, 2016:584).

Bu yasa özellikle suç teşkil eden içeriğin engellemesi konusunu düzenlemeye çalışmıştır. 5651 Sayılı Kanun kapsamında erişim engellemeyi dört ana başlık altında inceleyebiliriz; Bunlar; 8. maddede yer alan katalog suçların işlenmesi, 8/A maddesi uyarınca Milli Güvenlik, Kamu Düzeni gerekçesi, 9.maddesi uyarınca kişilik haklarının ihlal edilmesi durumu, 9/A Maddesi uyarınca özel hayatın gizliliğinin ihlal edilmesidir.

Erişimin engellenmesi konusunda 8.madde kapsamındaki engellemeler Telekomünikasyon İletişim Başkanlığı (TİB) tarafından 9. madde kapsamındaki engellemeler ise Erişim Sağlayıcıları Birliği tarafından yerine getirilmektedir. İlgili yasada suç teşkil eden Erişimi engelleme; alan adından, IP adresinden, URL erişiminden yapılarak kullanıcıların herhangi bir yayına erişmesini engellemeye çalışmaktır. Bu çabaların yüzde yüz başarı sağlayacağını söylemek doğru olmayacaktır, kesin çözüm içeriğin kaldırılmasıdır. Uygulamada 5651 Sayılı Yasa'nın uygulamasında ciddi sorunlar yaşanmaktadır.

2. Bilişim Suçları İle Mücadelede Uygulamada Yaşanan Sorunlar

Bilişim suçlarının diğer suçlardan bazı temel farkları bulunmaktadır: Zaman, mekan veya yer ile sınırlı olmadan bu suçlar meydana gelmekte ayrıca, suç ülke sınırlarını aşabilmekte, tespiti ve delillerin toplanması oldukça güç olmakta, delil elde etmek üst düzey teknik bilgi gerektirmekte ve bu suçlar sürekli biçimde mevzuatın yeterliliğini sorgulatan, biçimsel ve niteliksel değişimlere uğramaktadır.

2.1. Uluslararası Antlaşmalardan Kaynaklanan Eksiklikler

Bilişim suçlarıyla mücadele etmek bakımından en önemli husus, uluslararası adli yardımlaşmadır. Adli yardımlaşma konusunda uluslararası anlaşmaların yetersiz olmasının yanı sıra adli yardımlaşma konusunda prosedürün ülkemizde yeterince süratli işletilmemesi de önemli bir sorundur. İnternet sitelerinin Türkiye temsilciliği olmaması sebebiyle uyar kaldır yöntemi ve mahkeme kararlarının uygulanması da kolay olmamaktadır. Özgürlük ve

suç arasındaki dengede ülkelerin farklı yaklaşımı da üzerinde tartışılması gereken hususlardandır. Ülkeler özgürlük anlayışları iddiası ile başka ülkelerde yayınlanan içeriğin kaldırılması ve suç delillerinin ilgilere teslimi konusunda kayıtsız kalabilmektedirler. Anılan siteler yurtdışından tüm Dünya'ya yayın yapsa da yayınlandıkları ülkenin hukukunu da gözetmelidirler. Bunun için ikili anlaşmalar yapılmalıdır. ICANN (Internet Corporation for Assigned Names and Numbers / İnternet Tahsisli Sayılar ve İsimler Kurumu), uluslararası düzeyde organize olmuş, İnternet Protokolü (IP) adresi alanı tahsisi, protokol tanıtıcı ataması, genel (gTLD) ve ülke kodu (ccTLD) Üst Düzey Alan ismi sistemi yönetimi ve kök sunucu sistemi yönetimi işlevlerinden sorumlu kâr amacı gütmeyen bir kurumdur. Başka bir deyişle, ICANN İnternet'teki alan adları için denetleyici kurumdur.

ICANN, bugün dünya genelinde farklı İnternet Servis Sağlayıcıları (ISP'ler) arasında var olduğumuz global internet dediğimiz şey üzerinden, kamu şebekesi kullanımı için diğer tüm IP adres aralıklarını ayırmıştır. ICANN, alan adı sistemi (DNS) dahil olmak üzere, İnternet'in temel teknik öğelerinin bazılarının koordinasyonu için politikalar geliştirmeye yönelik küresel bir forumdur. ICANN, internetin temel teknik unsurlarının kamu yararına olan koordinasyon politikalarını oluşturmak için bir araya gelerek, etkilenen paydaşlarla birlikte mutabakat temelinde çalışır. (https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en, E.T.30.09.2018; https://archive.icann.org/tr/turkish.html, E.T.26.09.2018).

ICANN gibi uluslararası kuruluşlar internet içeriğinin denetlenmesi değil daha çok alan adlarının düzenlenmesi ve bu konudaki ihtilafları takip etmektedirler. Bu tür kuruluşların suç ile etkin mücadele için diğer ülkelere destek vermesi veya bu tür kuruluşların benzerlerinin uluslararası alana dahil edilmesi gerekmektedir.

Türkiye'de temsilcilikleri olmayan siteler aracılığı ile yoğun hak ihlali yapılması halinde bu siteler, temsilcilik açana kadar kapatılmalıdır.

2.2. Ulusal Yasalardaki Eksikliklerden Kaynaklanan Sorunlar

5651 Sayılı Yasa'nın sınırlı sayıda suç için erişimin engellenmesi hususunu C.Savcısının takibine bıraktığı hakaret, iftira, tehdit veya başkaca konularda düzenleme yapmadığı kamu görevlilerine hakaret ve kişilik haklarının ihlali halinde ise özel hukuk yaklaşımı ile konunun takibini mağdura bıraktığı gibi bir izlenim oluşmaktadır. Oysa hukukumuzda kamu görevlisine hakaret, gibi suçlar da re'sen soruşturulan suçlardandır. Bu suçlarda delil toplama ve suçluya ulaşma yanında suç teşkil eden kayıtların imhası da önem kazanmaktadır. Örneğin, maddi olarak mektupla hakaret suçunda ilgili mektup C.Savcılığının emanet biriminde delil olarak saklanır ve yazan kişiye veya kendisine yazılan kişiye teslim edilmez. Ayrıca, bir internet sitesi ile kişiye hakaret edilmiş ise bu sitenin kapatılması ve suç delillerinin saklanması nasıl yapılacaktır? Ya da suç içeren bir siteye erişim sağlayıcı veya içerik sağlayıcı izin vermiyor ise girmek ve erişimi engellemek mümkün müdür? Yani, maddi hukukta suçluyu ve delilleri aramak için bir eve arama kararı ile girilebiliyor iken suç işlenen bir sitenin o alanına içerik ve yer sağlayıcının rızası olmadan mahkeme kararı ile girmek mümkün müdür? Kullanıcı adı ve parola bilgilerinin elde edilmesi için sistemin yönetici paneline mahkeme kararı ile çilingir olarak tabir edebileceğimiz "kali Linux" ve benzeri programlarla girilmesi mümkün müdür? Anılan hususlar tartışılması ve neticeye bağlanması gereken hususlardır.

2.3. Yasa Uygulayıcılarından Kaynaklanan Sorunlar

Bilişim suçları alanında işlenen suçlar yeni bir suçluluk türü olduğu ve sürekli farklı yol ve yöntemler kullanarak güncellendiği halde ceza adaleti sisteminin uygulayıcıları, konuya hakim değildir. Emniyet teşkilatında siber suçlarla mücadele birimi kurulması ve adliyelerde bilişim suçları büroları bulunmasına rağmen görevliler bilişim suçları konusunda nitelikli eğitim almamaktadırlar. Soruşturmalar kolluğa havale edilmekte, matbu kararlar ile bilişim suçları, Kovuşturmaya Yer Olmadığı Kararı (KYOK-Takipsizlik) kararları ile sonuçlandırılmaktadır. Bilişimle ilgili tüm işler kolluk tarafından takip edildiğinden kolluğun bunları zamanında inceleyip, savcılığa vermesi mümkün değildir. Açık kaynak incelemeleri gibi temel konular dahi kolluğa havale edilmekte, kolluğu ait siber suçlarla mücadele birimlerinin ağır iş yükü göz ardı edilmektedir. Bilişim konusundaki ihtilaflar sadece soruşturma değil kovuşturma aşamasında da aynı akıbete uğramakta bu konuda yetkili mahkemeler bulunmadığı gibi uygulamacılar da ayrı bir eğitime sahip bulunmamaktadırlar. Yine BTK ve TİB görevlileri de yeterli eğitime sahip değildirler.

2.4. Teknik Sorunlar

Diğer bir sorun ise https uzantılı alan adlarının kapatılamamasıdır. Anılan husus erişim sağlayıcılar birliğinin internet sitesinde de yer almaktadır. Bu konuda teknik olarak çalışma yapılması ve çözüme kavuşturulması gerekmektedir. İnternet protokolü, bilgisayarlar ve ağ cihazları arasında iletişimi sağlamak amacıyla standart olarak kabul edilmiş kurallar dizisidir. Bu kurallar dizisi, temel olarak verinin ağ üzerinden ne şekilde paketleneceğini ve iletilen veride hata olup olmadığının nasıl denetleneceğini belirlemektedir. Ağ kavramının ortaya çıkmasından günümüze kadar geçen sürede farklı amaçlar için birçok protokol geliştirilmiştir. Bunlardan en yaygın olanları "http" ve "https" protokolleridir. Http; "Hyper Text Transfer Protocol" (Hiper Metin Transferi Protokolü) kelimelerinin baş harflerinden oluşan bir kısaltmadır. http, web üzerinden iletişim kurallarını tanımlayan bir protokoldür. Bir adrese bağlanmak istediğimizde belli bir sunucuda bulunan bir metni indirmek isteriz. Bu durumda web sitelerine ait metin ve görsellere erişebilmemiz için "http" protokolü ile bir talepte bulunmuş oluruz. Web sitelerinin adreslerinin başında da bu protokole bağlı olduklarını ifade etmek için "http" ifadesi yer alır. http, İnternette sunucular (server) ve son kullanıcılar (client) arasında bilgilerin nasıl aktarılacağına dair kurallar ve yöntemleri düzenleyen bir sistemdir. İnternet sitesine bağlanmaya çalışıldığında, adresin başına bu yazılmasa da tarayıcı bunu otomatik olarak ekler, çünkü sunuculardan web sitelerine ait bilgileri indirebilmek için, «http» protokolü ile bir istekte bulunulması gerekmektedir. **Https; "Hyper Text Transfer Protocol Secure** ise " (Hiper Metin Transferi Protokolü-Güvenli) kelimelerinin baş harflerinden oluşan bir kısaltmadır. Hypertext, bir web sitesinin kod veya eklenti gerektirmeyen, metin, tablo veya resim gibi içeriklerini açıklar. Secure, http ve ssl/tls protokollerinin birleşimini temsil eder. Bu protokoller İnternette gezinme dışında e-postalar, anında mesajlaşma gibi içeriğin de şifrelenmesinde kullanılır. Yani https, İnternet sitelerinin düz metin ile kurduğu iletişimin güvenliği artırmak amacıyla şifrelenmesi demektir. Sosyal ağların popüler hale gelmesiyle birlikte İnternet ortamında daha fazla sayıda kişisel veri, şifresiz olarak gönderilmeye başlanmıştır. Bu durum ise özel hayat ihlallerini arttırmaktadır. İnternet adreslerinin https protokolünü kullanmaları durumunda şifreli olduğundan URL den erişimin engellenmesi tedbirinin uygulanması teknik olarak mümkün olamamaktadır. Başka bir ifadeyle, https protokolü kullanan İnternet sitelerine yalnızca alan adından erişim engelleme işlemi tesis edilebilmektedir. https protokolü, ilk başta güvenlik özelliği nedeniyle, ödeme işlemleri, elektronik postalar ve hassas bilgi sistemlerinde kullanılmıştır. Ancak 2000'li yılların başından itibaren İnternet siteleri de bu protokolü kullanmaya başlamıştır. Bu protokolün kullanımı her geçen gün artmaktadır. Bunun anlamı ise, İnternet ortamındaki yayınlarda içeriğe URL erişim engelleme işleminin işlevini yitirmesidir. Dolayısıyla bu protokolü kullanan bir İnternet sitesi söz konusu içeriği kaldırmadığı takdirde ancak tamamen kapatılma yöntemi ile yayından kaldırılabilecektir (Kılınç,2016:608-610).

SONUÇ

Bilgi teknolojilerinde yaşanan süratli gelişim internet kullanımını yoğunlaştırırken bu alanda işlenen suçlarda artışı ve anılan suçlarla mücadele zorunluluğunu da beraberinde getirmiştir. Bilişim alanında işlenen suçlar ile mücadele etmek diğer suç tiplerine nazaran çok daha zordur; Bilişim alanında işlenen suçlarla mücadelede karşılaşılan zorluklar uluslararası anlaşmalar ve yasalardan kaynaklanan eksiklikler, teknik sorunlar, uygulayıcıların niteliğinden kaynaklanan sorunlar olarak özetlenebilir. Bilişim suçlarının mukayeseli hukukta ortak tanımı olmadığı gibi, mevcut tanımlar da net değildir. Maddi ceza hukuku bakımından gözlemlenen farklılıklar, etkili bir adli yardımlaşmayı da engellemektedir. Bu nedenle, siber suçlara dair maddi ceza kurallarının yeknesaklaştırılması önemlidir. Mevzuat güncellenmeyip, klasik suç tipleri, bilişim teknolojisinin ortaya çıkardığı suçluluk türlerine uygulanmak istendiğinde, faili cezalandırmak her zaman mümkün olmamaktadır. Kaldı ki, hızla gelişen teknoloji, siber suçların yeni görünüm şekillerini ortaya çıkarmakta, bu da, yeni düzenlemeler yapan devletler açısından dâhi, mevcut yasal çerçevenin aynı hızla değiştirilmesini ve geliştirilmesini gerektirmektedir. Siber suçlarla, mücadele ve de adli işbirliği, zaman ve masraf anlamına gelmektedir. Bu noktada Adalet Bakanlığının adli istinabe yazışmalarını daha süratli yapabilmesi için teknikler geliştirmesi uygulamalarını güncellemesi gerekmektedir. Bu noktada tebligatlar v.s. konusunda elektronik ortamdan daha fazla yararlanması yazışmaları süratli hale getirmesi mümkündür. Bilişim teknolojileri süratle gelişmekte olduğundan ceza kanunlarında tanımlanmamış yeni suç tipleri ortaya

çıkmaktadır. Ceza hukukunda suçun kanunda yazılı tanıma uyması şeklinde izah edilen tipiklik ilkesinin gerçekleşmemesi halinde suçun failine ceza verilemeyeceğinden yeni suç tipleri karşısında yeni yasal düzenlemeler gerekmekte, yeni suç tipinin tespiti ile yasalaştırılması ise zaman almaktadır. Bu sebeple yasaların hızlı şekilde çıkarılması için üst seviyede eğitim almış nitelikli bilişim komisyonu aracılığı ile çalışmalar yürütülmelidir. Örnekle açıklamak gerekirse Bu konuda TCK, CMK ve 5651 Sayılı Yasa bilişim yasası birbirinden ayrı ve kopuk kopuk hazırlanmıştır. 5651 Sayılı Yasa'da kamu düzenini bozucu kamu görevlilerine hakaret gibi içeriğin internetten çıkarılması kişilik haklarına müdahale kapsamında değerlendirilerek ilgilinin mahkemeden mağdur tarafından karar alması gibi kamu düzenini bozucu olay soruşturması ile bağdaşmayan yöntemlere dayanmaktadır. Uygulayıcılar da kamu adına resen yürütülmesi gereken soruşturma ile kişisel hakların ihlalini konuya hakim olmamaları yanı sıra iş yoğunluğunu gerekçe göstererek aynı kapsamda değerlendirmektedirler. Bilişim alanındaki yasalar tek çatı altında toplanmalı, cezalar suçların soruşturulma usulleri, delil toplama yöntemleri ve erişimin engellenmesi konuları tekrar gözden geçirilmelidir. Anılan yasada uluslararası anlaşmalara da atıfta bulunulmalıdır. Yasa hazırlama sürecinde hukukçular, bilgisayar mühendisleri, kolluk yetkileri, sivil toplum kuruluşu yetkilileri bir araya gelmelidir. Yine hakim savcı ve avukatların bilişim suçları konusunda uzmanlaşması sağlanmalı bunun için hukuki konular yanında teknik konularda da eğitim almaları sağlanmalıdır. Bilişim teknolojisi günlük hatta anlık olarak değişmektedir. Yeni donanım cihazları, yeni virüsler, yeni sızma teknikleri geliştirilirken yasaların stabil kalması düşünülemez. Bu konuda anılan yasaları güncelleyecek ve yeniliklere uyduracak bir çalışma grubu sürekli bulundurulmalıdır.

Adliyelerde görev yapan bilişim suçlarının araştırılması ve yargılamasından sorumlu savcıların ve hakimlerin bilişim tekniği ve hukuku hakkında temel bilgiye sahip olmaları ve bilgilerini sürekli güncellemeleri ile bilişim suçları ile etkin mücadele yapılması mümkün olabilecektir. Hukuk fakültelerinde sadece bir yarıyıl bilişim derslerinin okutulması günümüz koşullarında yetersiz kalmaktadır. Bilgisayar derslerinin saati ve AKTS kredisi artırılmalı, çeşitlendirilmeli ve bilgisayar kullanımının farklı alanlarında seçmeli dersler açılarak, gerekirse yan dal alınması temin edilerek hukukçulara bilişim teknolojileri alanında okul yıllarından itibaren uzmanlaşma olanağı verilmelidir. Yine bilişim avukatlığı ünvanının kullanılması için en az bir yıl anılan konuda eğitim alma şartı getirilmeli, suç türüne göre aile ve sosyal politikalar bakanlığı ve ilgili diğer bakanlıkların bilişim suçlarının mağdurlarına yönelik avukat ataması hukuki yardım yapması için gerekli çalışmalar yapılmalıdır.

Nitelikli soruşturmalar için hukuk ve ceza Mahkemeleri'nde bilişim uzmanı istihdam edilmelidir. Bilişim soruşturma ve yargılamalarını yürüten katiplerinin de ayrı olması daha uygun olacaktır. Hatta ayrı bilişim mahkemeleri oluşturulmalı ve bu mahkemelerde; teknik konularda bilgisi olan, hukuk eğitiminin yanında bilişim konusunda yüksek lisans-doktora eğitimi almış, hakim ve savcılar çalıştırılmalıdır. Zira, Bilişim uzmanlık gerektiren teknik bir konu olduğu için bilirkişiye sorulacak sorulan dahi bilgi ve uzmanlığa dayalı olduğu günümüzün gerçeğidir.

Bilişim ile görevli mahkemeler kurulması gerektiği gibi savcılık bilişim büroları ve kurulacak bilişim mahkemelerine zabıt katibi alınırken adaylar genel katip alım sınavından ayrı bir sınava tabi tutulmalıdırlar. Hakim ve savcılar eğitim merkezlerinden itibaren özel eğitim alarak uzmanlaşmalı, mesleki eğitimler ile tüm çalışanlar bilgilerini yenilemelidirler. Bilişim bürolarında daha teknik konular için bilişim uzmanları da görev yapmalıdır. Bilişim çağı olarak adlandırılan günümüzde anılan konuda yargılamanın unsuru olan kişilerin alımları ve yetiştirilmelerinde ayrı bir yöntem izlenmesi anılan suç türleriyle etkin mücadele edilmesinde önemli bir unsur olarak karşımıza çıkmaktadır. Bütün bunların hayata geçirilmesi için öncelikle özellikle büyükşehir C.Savcılıkları ve Mahkemelerinin HSK müfettişlerince yapılan teftişlerinde ortaya konan bilişim suçlarının takibi ile ilgili eleştirileri, ilgili yerdeki yöneticilere, hakimler savcılar kurulu ve adalet bakanlığının ilgili birimlerine tebliğ edilmeli, yine BTK ve diğer kurumlarda yapılacak çalışmalar da bir araya getirilerek akademisyenler ulusal ve uluslararası hukuk uygulayıcıları ve meclis çalışma grubu ile bir araya gelerek çözüm üretmelidirler. Yine BTK ve TİB deki görevlilerde nitelikli eğitim almalı ve denetimleri iyi yapılmalıdır.

KAYNAKÇA

Aydoğan, Tan.(2009).5651 Sayılı Yasaya Göre Erişim Engellemeleri,

Https://Hukuksokagi.Com/Kaynak/5651-Sayili-Yasaya-Gore-Erisim-Engellemeleri/ , E.T.06.09.2018.

BTK, Bilgi Teknolojileri ve İletişim Kurumu, https://slideplayer.biz.tr/slide/12852567/, E.T.

06.09.2018.

Canata, Fatih.(2016). 5651 Sayılı Kanun Kapsamında İnternet Düzenlemeleri ve Düşünce-

İfade Özgürlüğü Üzerine Bir Değerlendirme, Türk Kütüphaneciliği 30, 2, 185-205.

Gök, M.S.(2012).5651 Sayılı Kanun ve Bilgi Güvenliği İlişkisi Mehmet Salih Gök, İstanbul

Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Yüksek Lisans Programı, Ekonomi Hukuku.

Gönen, S; Ulus, H.İ ve Yılmaz, E.N.(2016).Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme, Bilişim Teknolojileri Dergisi, Cilt: 9, Sayı: 3.

Henkoğlu, T. ve Uçak, N.Ö.(2012). Elektronik Bilgi Güvenliğinin Sağlanması İle İlgili Hukuki ve Etik Sorumluluklar, Bilgi Dünyası, 2012, 13 (2) 377-396.

Kılınç, Doğan.(2016).5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve

Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması, Gazi Üniversitesi Hukuk Fakültesi Dergisi C. XX, Y.

Önok, Http://Dergipark.Gov.Tr/Download/İssue-File/517, s.1232, E.T.13.09.2018.

Özdemir, Y.D.(2015). İnternet Siyasası Oluşturma ve 5651 Sayılı İnternet Yasası'na Eleştirel Bir

Bakış, Ankara Üniversitesi iletişim Fakültesi (ilef) Dergisi, 2(2), 81-103.

https://birimler.dpu.edu.tr/app/views/panel/ckfinder/userfiles/2/files/mevzuatlar/5651_Say_l__Kanun.pdf , Erişim Tarihi (E.T.) 29.09.2018.

https://www.icann.org/resources/pages/cctlds-21-2012-02-25-en, E.T.30.09.2018.