SOSYAL MEDYADA İŞLENEN SUÇ TİPLERİ VE SUÇLULARIN TESPİTİ

Gürkan Özocak (Avukat, LL.M.)

ÖZET

Bilişim teknolojilerindeki gelişimle beraber, toplum hayatında 'sosyal medya' olarak adlandırılan sosyal ağ ve paylaşım sitelerinin yeri gün geçtikçe arttığından, bu mecraların insanlar bakımından sosyalleşme platformu olmasının yanı sıra, sosyolojik bir olgu olan suçların da alanı haline gelmesi kaçınılmaz olmuştur. Sosyal medya alanlarında işlenen suçlar hem TCK m. 243-246'da düzenlenen ve teknik olarak 'bilişim suçu' olarak tanımlanan suçlar, hem de bilişim sistemleri aracılığıyla işlenen klasik suçlar olarak ortaya çıkabilmektedir. Bu suçlar işleniş yöntemleri açısından diğer suçlardan farklılık arzettiği gibi, suçluların tespiti ve delillere ulaşma gibi muhakeme sorunları bakımından da kendine has niteliğe sahiptirler.

ANAHTAR KELİMELER

Sosyal medya, bilişim suçları, İnternet suçları, elektronik delil.

I. GİRİŞ

Son yıllarda, bilişim ve telekomünikasyon teknolojilerindeki gelişmelere de paralel olarak, insanların birbirleriyle iletişim kurma kanalı, hatta sosyalleşme yolu olarak daha çok İnterneti tercih etmeye başlamaları ile beraber, sosyal medya ve sosyal ağlar gerek sosyolojik, gerekse hukuki olarak toplum hayatının önemli bir parçası haline geldi. İnternette yayın yapan ve kullanıcılarının artık yüz milyonları bulduğu sosyal ağlar, sosyal paylaşım siteleri ve İnternet sözlükleri, sosyal hayatın bizzat kendisine tekabül eder hale geldiğinden, hukuki olmasının yanı sıra sosyolojik birer olgu olan suçların da çok farklı tezahürlerine sosyal medyada rastlamak mümkün hale geldi.

Sosyal medya üzerinden işlenen suçlar, günlük somut hayattan farklı olarak, maddi varlığı bulunmayan soyut ortamlar üzerinde gerçekleştiğinden, bunların işlenme yolları ve suçluların tespiti yöntemleri farklılık arzetmektedir. Bu itibarla, bu tür suçların ayrı bir değerlendirmeye tutulmasında, bu yöntemlerin tasnifi ve konunun daha iyi anlaşılması bakımından fayda bulunmaktadır. Ancak, sosyal medya üzerinden işlenen suçların incelenmesine geçmeden önce, bu suçlar da esasen *"bilişim*

suçları" başlığı altında değerlendirildiğinden, bilişim suçlarından bahsetmek gerekmektedir.

II. BİLİŞİM SUÇLARI

Doktrinde kimi zaman birbirinin yerine de sıkça kullanılan *"bilişim suçları"* veya *"bilgisayar suçları"* ile ilgili ortak bir tanımlama yapılamamış, birçok yazar bu suçlara kendince bir sınır çizmiştir (**Bozdoğan Akbulut**, 2000: 550). Çalışmamızın kapsamı bakımından bu tartışmaların tamamını buraya alamamakla birlikte[1], son tahlilde bilişim suçları, verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yönelik olarak veya onları araç olarak kullanarak icra edilen haksız eylemler olarak tanımlanabilir (**Kurt**, 2005: 53; **Özen/Baştürk**, 2011: 90-91).

Bugün, bilişim suçlarını "*bilişim sistemleri aracılığıyla işlenen suçlar*" ve "*bilişim alanındaki suçlar*" olarak ikiye ayırmak mümkündür. İlk gruptaki suçlar "*geleneksel*" ya da "*klasik*" suçlar olarak tanımlanan, ancak bir bilişim sistemi aracılığıyla işlenen suçlardır. Örneğin; e-posta yoluyla işlenen tehdit veya hakaret suçu, yine bilgisayar veya İnternet siteleri üzerinden işlenen cinsel taciz, halkı kin ve düşmanlığa tahrik etme gibi suçlar bu grupta sayılabilir. Teknolojik imkanların müthiş bir hızla artması ve gelişmesi ile birlikte, artık insan öldürme suçuna kadar her suç bilişim yoluyla işlenebileceği için, bu gruptaki suçların sınırını belirlemek mümkün değildir (**Özdilek**, 2006: 112).

İkinci gruptaki suçlar ise, kanunda sınırlı sayıda düzenlenen ve ilk gruptaki suçlara göre teknik özellikler arzeden suçlardır. 5237 sy. TCK'da da bu suçlar, 243 ila 246. maddeler arasında, "*Bilişim Alanında Suçlar*" başlığıyla düzenlenmiştir[2].

Sosyal medya üzerinde işlenen suçlar, her iki grup suçun kapsamına da girmektedir. Gerçekten de, örneğin, bir kimsenin bir sosyal paylaşım sitesi hesabı

[1] Terimle ilgili tartışmalar için bkz. **Ketizmen**, 2008: 32-54; **Kurt**, 2005: 49-53; **Sınar**, 2001: 69-78.

[2] Bunlara, kanun tarafından sınırlı sayıda öngörüldükleri için "*dar anlamda bilişim suçları*" da denilmektedir. Bkz. **Özen/Baştürk**, 2011: 113.

şifresinin kırılarak hesabına yetkisiz bir biçimde girilmesi durumunda ikinci grup olan *"bilişim alanında suç"* (TCK m. 243) söz konusu olacakken, buna karşın, sosyal paylaşım sitesindeki bir hesap üzerinden bir kimseye hakaret edilmesi durumunda, ilk grup olan klasik ya da geleneksel suçlardan olan hakaret suçunun (TCK m. 125) bilişim sistemleri aracılığıyla işlenmesinden bahsetmek gerekecektir.

TCK m. 243-246 arasında düzenlenen ikinci grup suçlar ayrı ve ayrıntılı teknik değerlendirmeleri içerdiğinden, çalışmamızın kapsamını çok genişletmemek adına, bu suçlardan kısaca bahsedip, esasen ilk grup klasik suçların bilişim sistemleri aracılığıyla işlenmesi ve bu durumlarda suçluların tespitine ilişkin ceza muhakemesi hükümleri konularına değineceğiz.

III. SOSYAL MEDYA ÜZERİNDE İŞLENEN SUÇ TİPLERİ

Son yılların adeta 'moda' tabiri haline gelen sosyal medyayı, bireylerin İnternet üzerinden birbiriyle yapmış olduğu diyalog ve paylaşımların bütünü olarak tanımlamak mümkündür. Sosyal ağlar, bloglar, mikro bloglar, sohbet siteleri, forumlar ve İnternet sözlükleri gibi kişilerin birbirleriyle iletişim kurmasını ve bilgi paylaşmasını sağlayan İnternet siteleri ve uygulamalar sosyal medya kapsamında sayılmaktadır. Bunlar bazen iki kişinin birbiriyle yapmış olduğu sohbetler gibi mikro ölçekte paylaşımlardan oluşsa da, İnternet ortamının sınırsız zenginliğinden kaynaklı olarak, paylaşılan bir bilgi veya içeriğin saniyeler içerisinde binlerce, hatta milyonlarca insana ulaşması mümkün hale gelebilmektedir.

Bu nedenle, bu sosyal mecra üzerinde işlenen suçlar, işlenme yöntemlerinin farklılığının yanında, yaratmış olduğu etki nedeniyle de özellik arzetmektedir.

A. BİLİŞİM ALANINDA İŞLENEN SUÇLAR

5237 sayılı TCK'nun 243 – 246. maddeleri arasında 'Bilişim Alanında Suçlar' başlığı altında düzenlenen suçlar, klasik suçların aksine, sadece bilişim vasıtasıyla işlenen suçlar değil, aynı zamanda bütün hareket ve neticenin de bilişim alanında doğduğu suçlardır. Bahsi geçen suçları tasnif edecek olursak, TCK, "Bilişim Alanında Suçlar"ı şu şekilde sınıflandırmaktadır: "*Yetkisiz Erişim", "Sisteme Müdahale",*

"Veriye Müdahale (Değiştirme, Bozma, Yok Etme, Erişilmez Kılma)", "Bilişim Sistemleri Aracılığıyla Yarar Sağlama" ve *"Banka ve Kredi Kartlarının Kötüye Kullanımı*".

Bu suçların gerek hukuki gerekse teknik açıdan ayrı ayrı incelemesine girmek çalışmamızın kapsamını açacağından, konunun yalnızca sosyal medya ile bağlantısı üzerinde duracağız[3]. Bilişim suçlarının, sosyal medya üzerinde en sık görünen şekli, "şifre kırma" olarak da adlandırılan hacking yöntemiyle, TCK m. 243/1'de düzenlenen yetkisiz erişim suçudur. Kanun *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimse"*nin bu suçu işleyeceğini söylemektedir. Örneğin, bir kimsenin bir sosyal paylaşım sitesindeki hesabının şifresinin kırılarak sistemine girilmesi ve burada kalınması durumunda, TCK m. 243'te düzenlenen yetkisiz erişim suçu oluşacaktır.

TCK m. 244'ün düzenlemesi ise şu şekildedir: *"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."* Buradaki "engellemek" "*bir şeyin gerçekleşmesini veya yapılmasını önlemek*"; "bozmak" ise "*bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek*" olarak anlamak gerekmektedir (**Ketizmen**, 2008: 129). Bilişim sisteminin engellenmesi veya bozulması ve veriye müdahale şeklinde adlandırılan bu suçun da sosyal medya üzerinde işlendiği görülmektedir.

Hükmün ilk fıkrasındaki fiil, İnternet sitelerinin işleyişinin engellenmesi şeklinde meydana gelmektedir. Örneğin, bir sosyal paylaşım sitesine yapılan DoS veya DDoS saldırısı ile site çalışamaz hale getirilebilir ve kullanıcıların bu siteye girişleri engellenebilir[4]. Bu durumda, "*bir bilişim sisteminin işleyişini engelleyen*"

[3] Bu suçların hukuki ve teknik anlamda detaylı açıklama ve değerlendirmeleri için bkz. **Ketizmen**, 2008: 67 vd.; **Kurt**, 2005: 146 vd.; **Parlar**, 2011: 15 vd.

[4] Bilişim alanında en çok görülen siber saldırıların başında DoS *(Denial of Service)* ve DDoS *(Distributed Denial of Service)* saldırıları gelmektedir. DoS saldırısı, kısaca, belli bir sunucunun belli bir şekilde hizmet bekleyen kullanıcılara hizmet verememesini sağlamak amacıyla, o bilgisayarın işlem yapmasını engellemek, bir başka deyişle hedef bilgisayarı bilişim sisteminin içerisine girmeksizin

failin TCK m. 244/1 dolayısıyla sorumluluğundan bahsetmek gerekecektir.

TCK m. 244/2 ise, kullanıcı bazlı bakıldığında, sosyal medyada ihlal edildiğine daha sık rastlanan bir hükümdür. Örneğin, bir kimsenin bir sosyal ağ hesabına giren fail, bu hesapta bulunan bazı içerikleri (*mesajları, paylaşımları, iletileri vs.*) silmesi halinde, "sistemdeki verilerin yok edilmesi" fiilini gerçekleştirdiğinden, TCK m. 244/2'den sorumlu olacaktır. Aynı şekilde, hukuka uygun veya aykırı bir biçimde girmiş olduğu sosyal ağ hesabına bir içerik yerleştiren fail "*sisteme veri yerleştirdiği*" yahut girmiş olduğu hesaptaki bazı verilere ulaşım iznini kaldıran ya da bu verilere şifre koyan fail "*verileri erişilmez kıldığı*" için, yine TCK m. 244/2'nin maddi unsurunu gerçekleştirmiş olacaktır.

Burada tartışma konusu olabilecek husus, örneğin, bir kişinin bir sosyal paylaşım sitesindeki hesabına giren fail, buradaki mevcut içeriklere hiç dokunmaksızın, bu hesap üzerinden bir başka kimseye bir ileti gönderdiğinde yahut benzer bir biçimde bir kişinin bir İnternet sözlüğündeki hesabına giren fail, bu hesap üzerinden bir ileti (*entry*) paylaştığında, bunun TCK m. 244/2 bağlamında suç oluşturup oluşturmayacağı hususudur. Ancak bunun belirlenebilmesi için, önce 'veri' kavramının açıklanması gerekmektedir.

Öğretide, "*veri*" (*data*), "*enformasyon*" (*information*) ve "*bilgi*" (*knowledge*) deyimleri arasındaki ilişki tartışmalı bir alanı oluşturur. Ancak bu üç terimin birbirinden ayrılması gerekir. Zira, ister elektronik ister elektronik olmayan ortamlarda tutulmuş olsun, veri yalnızca bilgi, olgu ya da sayıların ham hali olarak düşünülürse, bu verinin insanlara anlamlı gelen bir enformasyona dönüştürülmesi gerekir. Bu bağlamda, anlamlı bir biçime sokularak kullanılabilir hale gelen verilere bilgi denilmektedir. Dolayısıyla bilgi, bir üst aşamayı ifade eder. Ne var ki, dilimizde özellikle bilgi ve veri birbiriyle eş anlamda kullanılmaktadır. Bu nedenle, bu terimler arasındaki tartışmaların detayına girmeksizin söyleyebiliriz ki, veri "*bilgi,*

---

kilitlemektir. DoS işlemi, birden çok sayıda bilgisayar üzerinden yapıldığında, yani "dağıtılmış" (*distributed*) bir şekilde gerçekleştirildiğinde ise ortaya DDoS saldırısı çıkmaktadır. DoS ve DDoS saldırıları ve bunların teknik açıklaması ve hukuki niteliği hakkında detaylı bilgi için bkz. **Özocak**, 2012: s. 24 vd.

data/(bilişim açısından) olgu, kavram ve komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"ni ifade etmektedir (**Küzeci**, 2010: 9-11). Nitekim, konu bakımından önem arzeden "kişisel veri" de 2008 yılından beri tasarı halinde bekleyen ve halen yürürlüğe girmemiş olan 'Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı'nın 3. maddesinde 'kişisel veri' "*Belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgiler*" şeklinde tanımlanmaktadır.

Bu bağlamda, yukarıdaki örneğe bakıldığında, bir kimsenin Facebook, Twitter vb. sosyal paylaşım sitelerinde yazmış olduğu iletiler yahut göndermiş olduğu mesajlar veya Ekşisözlük gibi İnternet sözlüklerinde girmiş olduğu iletilerin (*entry*ler) birer veri niteliğinde olduğu kuşkusuzdur. O halde, failin bir kişinin bu sosyal ağlardaki hesaplarından birine girip, o hesapta bir ileti paylaşması, "*sisteme veri yerleştirme*" olarak kabul edilmeli ve fail TCK m. 244/2'den sorumlu tutulmalıdır.

Şüphesiz ki, buna benzer durumlarda, failin ceza sorumluluğu olup olmadığı belirlenirken, işlenen fiilin, Kanundaki düzenlemeyle birebir örtüştüğünün mutlak bir biçimde tespiti gerekir. Zira, tipiklik, her şeyden evvel, bir fiilin görünümünü, adeta resmini ifade eder (**Keyman**, 1980: 59). Ceza hukukunda "tipiklik" fiilin cezalandırılması için zorunludur. Tipik fiil, iradi olması nedeniyle bir insana atfedilebilen, münferit kanuni bir soyut tipin içine yerleştirilebilen, yani bu kanuni düzenlemenin bütün özelliklerini bünyesinde taşıyan objektif unsurların tamamına tekabül eder (**Keyman**, 1988: 121 vd.). Bu nedenle, failin fiilinden cezalandırılması için, kanunda tanımı yapılan tipik fiil ile örtüşmesi gerekmektedir (**Toroslu**, 2012: 96). Örneğin, failin hesap sahibinin hesabından başka bir yere mesaj atması durumunda, bunun "var olan verilerin başka yere gönderilmesi" olarak düşünülmesi mümkün değildir. Zira, kanuni tipte suçun oluşabilmesi için ortada "*var olan bir veri*"nin bulunması ve bunun "*başka bir yere gönderilmesi*" şartı aranmıştır. Böyle bir örnekte, fail başka bir yere gönderdiği veriyi kendisi yarattığından ve sistemdeki var olan bir veri üzerinde herhangi bir müdahalede bulunmadığından, fiili bu açıdan tipik olmayacak ve fail *"var olan verilerin başka bir yere gönderilmesi"* bakımından sorumlu tutulamayacaktır. Ancak, örneğin mağdurun Facebook hesabına girerek buradaki mağdur tarafından yazılmış bir iletiyi yahut mağdurun hesabında yer alan kişisel bilgilerini bir başka yere gönderen veya başka bir yerde paylaşan failin fiili

"*tipik fiil*" olduğundan bu kapsama girecektir.

B. BİLİŞİM SİSTEMLERİ ARACILIĞIYLA İŞLENEN SUÇLAR

Bilişim teknolojilerinin yalnızca suç işlemenin bir aracı olarak kullanıldığı düşünüldüğünde, pek çok klasik ya da geleneksel suçun bilişim sistemleri aracılığıyla işlendiği görülebilir. Bu yüzden, teknik olarak "bilişim suçu" olan, yani hem bilişim sistemleri aracılığıyla işlenen, hem de sonuçları doğrudan bilişim alanında ortaya çıkan ve yukarıda değinilen suçların dışında, bu suçların ayrı bir başlık altında incelenmesi yerinde olacaktır (**Akıncı/Alıç/Er**, 2003: 175).

Gelişen teknoloji ile beraber her suçun bilişim sistemleri aracılığıyla işlenmesi söz konusu olabilir. Öyle ki, örneğin, kalp rahatsızlığı olduğu bilinen bir kimsenin bilgisayarına kurulacak bir programla, korkutma yoluyla kalp krizi geçirmesini sağlayarak insan öldürme suçunun dahi bilişim sistemleri aracılığıyla işlenebileceği düşünüldüğünde, bu suçlar bakımından herhangi bir sınır konulması mümkün değildir. Bu nedenle, ceza kanunlarında düzenlenen her suç bilişim sistemleri aracılığıyla işlenebilir.

Biz, çalışmamızın kapsamına bağlı kalmak amacıyla, sosyal medyada görülmesi mümkün her suçtan değil, yalnızca bu mecrada sıkça görülen klasik suçlardan bahsedeceğiz.

1) Hakaret ve Tehdit (TCK m. 125 ve 106)

Sosyal medyada en sık rastlanan suçların başında hakaret ve tehdit suçları gelmektedir. Hakaret suçu TCK'nun 125. Maddesinde "*Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden ya da yakıştırmalarda bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırmak*", Tehdit suçu ise TCK'nun 106. Maddesinde "*Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit etmek*" biçiminde düzenlenmektedir.

Genel olarak, hakaret suçu ile, kişinin hukuk düzeni tarafından "şeref varlığı" adı altında korunan toplumdaki sosyal değerlerine ve itibarına saygı gösterilmesinin sağlanması ve zarar verilmesinin önlenmesi (**Tarhan**, 2007: 276); tehdit suçu ile ise, kişilerin bağımsız karar alma, özgürce düşünüp hareket edebilme yetisinin ve insana özgü bu mekanizmanın sekteye uğramadan işleyebilmesinin sağlanması amaçlanmaktadır (**Tarhan**, 2007: 28).

Bu iki suç, birbirinden ayrı ve farklı hukuki konulara sahip suçlar olmakla beraber, sosyal medyada genelde aynı fiil içerisinde ihlal edildiklerinden, çalışmamızda aynı başlıkta incelenmektedir. Gerçekten de, son yıllarda verilen yargı kararlarına bakıldığında, sosyal medya üzerinden, özellikle de Facebook ve Twitter gibi neredeyse herkesin kullanmakta olduğu sosyal ağlar üzerinden işlenen suçların, çok büyük bir çoğunluğu hakaret ve tehdit suçlarıdır.

Şüphesiz ki, sözlü, yazılı veya görsel şekilde işlenen klasik hakaret ve tehdit suçları gibi, sosyal medya üzerinden işlenen hakaret ve tehdit suçları da, tipik fiilde belirtilen unsurları taşıdıkları sürece, bu hükümlere göre cezalandırılacaktır. Ancak, burada farklılık arzeden ilk husus, eğer fail tehdit suçunu sosyal medya üzerinden kendini tanınmayacak bir hale sokarak işlerse, örneğin, sahte isimle bir Facebook ya da Twitter hesabı açarak bir kişiyi ölümle tehdit ederse, bu fiil tıpkı imzasız bir mektup gibi değerlendirilecek ve failin cezası TCK m. 106/2(b)'deki "*Kişinin kendisini tanınmayacak bir hâle koyması suretiyle...*" düzenlemesi nedeniyle, ağırlaştırılacaktır. Bu suçların klasik hakaret ve tehdit suçlarından farklılık arzeden ikinci özelliği ise suçluların tespiti ile ilgili olup, buna çalışmamızın sonraki bölümlerinde değineceğiz.

Özellikle hakaret suçu bakımından değinilmesi gereken bir husus da, fiilin TCK'da belirtilen bazı suçlardaki özel kasıtla işlenmesi halidir. Örneğin, kişi bir sosyal ağdaki hesabı üzerinden cumhurbaşkanına hakaret ediyor yahut kanun koyucunun korunacak değer açısından özel önem yüklediği Türklüğü, Cumhuriyeti veya Devletin kurum ve kuruluşlarını aşağılıyorsa (**Yalçın Sancar**, 2006: 69 vd.), burada artık TCK m. 125'den değil, özel düzenleme söz konusu olduğu için TCK m. 299 veya 301'den ceza sorumluluğu doğacaktır (**Tarhan**, 2007: 276).

2) Kişisel Verilerin Hukuka Aykırı Kaydedilmesi ve Yayılması (TCK m. 135-136)

Sosyal medyada sık görülen suç tiplerin birisi de kişisel verilerin hukuka aykırı kaydedilmesi ve yayılması suçlarıdır. Tipik fiillerin düzenlendiği TCK m. 135 "*Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir. Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır*", TCK m. 136 ise "*Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır*" hükümlerini ihtiva etmektedir.

Burada ilk dikkat edilmesi gereken husus, Kanun koyucu 135. Maddenin ilk fıkrasında kişisel verilerin hukuka aykırı olarak kaydedilmesini ararken, ikinci fıkrada hukuka aykırı kayıt şartını aramamıştır. Bu durumda, siyasi, felsefi veya dini görüşlere yahut ırksal kökenlere ilişkin verilerin kaydedilmesinde hukuka aykırı kayıt şartı aranmayacak, bunların kayıtları her halükarda suça vücut verecektir (**Küzeci**, 2010: 288).

Sosyal paylaşım sitelerinde kişilerin isim, kimlik bilgileri, cep telefonu numaraları, fotoğrafları gibi kişisel verilerinin rızaları dışında kaydedilmesi veya yayılması, şüphesiz ki bu suçlara vücut verilmektedir. Ancak burada şunu belirtmek gerekir ki, kişiler Facebook, Twitter vb. herkesin görebileceği sosyal ağlarda fotoğraf veya saklamaya gerek duymadıkları kişisel bilgilerini yayınladıklarından, bunların kaydedilmesi TCK m. 135 anlamında suç oluşturmayacaktır. Ne var ki, kendi rızasıyla fotoğraflarını veya kişisel bilgilerini bu mecralarda paylaşan kişilerin bu rızası, söz konusu kişisel verilerin yayılmasını kapsamadığından, kaydedilen bu fotoğraf ve bilgilerin, veri sahibinin rızası dışında paylaşılması TCK m. 136 anlamında "*kişisel verilerin hukuka aykırı yayılması*" suçuna vücut verecektir.

Bu bağlamda, söz konusu suçun sık görülen türlerinden birisi de, sosyal ağlarda başkasının adına hesap açmak fiilidir. Facebook, Twitter gibi İnternet sitelerinde, başkalarının adına hesap açıldığı herkesçe bilinmektedir. Eğer bir kimse,

başka bir kişinin ayırt edici bilgileriyle veya fotoğrafını kullanarak, o kişi adına bir hesap açarsa, bu fiil hiç şüphe yok ki kişisel verilerin hukuka aykırı yayılması olacak ve fail, TCK m. 136 dolayısıyla sorumlu olacaktır.

3) Özel Hayatın Gizliliğini İhlal (TCK m. 134)

TCK'nun 134. maddesi uyarınca, "*Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır… Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*."

Buna göre, bir sosyal medya ortamında kişilerin özel hayatın gizliliği ihlal edilirse, örneğin, bir kimseye ait özel görüşmeler yayınlanır yahut o kimsenin özel hayatına ilişkin özel bilgiler paylaşılırsa, fail TCK m. 134/1 uyarınca sorumlu olacaktır.

Maddenin ikinci fıkrasında ise, suçun ağırlaştırıcı hali düzenlenmiş ve özel hayata ilişkin görüntü veya seslerin ifşasında, cezanın ağırlaştırılacağı ifade edilmiştir. Burada tartışılması gereken; bir kimsenin özel hayatına ilişkin bir fotoğrafı bir sosyal ağda paylaşıldığında, fail TCK m. 136'dan dolayı mı, yoksa 134/2'den dolayı mı cezalandırılacaktır? Burada ceza hukukundaki fikri içtima kavramı gündeme gelmektedir. TCK m. 44 uyarınca "*İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır*." Gerçekten de, failin dış dünyadaki hareketi tek fiil ise, yani tek bir davranış ve tek bir maddi sonuçtan oluşuyorsa, ancak buna karşın bu fiil ile soyut normlar dünyasında iki ihlal meydana gelmiş, bir başka deyişle iki ayrı ceza hükmü ihlal edilmişse, bu durumda fail her iki suçtan dolayı değil, bu iki suçtan daha ağır olanı ile cezalandırılır (**Toroslu**, 2012: 342-343; **Centel/Çakmut/Zafer**, 2006: 478 vd.; **Öztürk/Erdem**, 2012: 338-339). Böyle bir durumda, fail sosyal ağ üzerinden mağdurun özel hayatına ilişkin fotoğraflarını paylaşırsa, fiili hem TCK m. 136 anlamında *"kişisel verilerin yayılması",* hem de TCK m. 134/2 anlamında *"özel hayatın gizliliğini ihlal"* olacağından ve ortada bir fikri içtima söz konusu olacağından, faile daha ağır ceza öngören TCK m. 134/2 uyarınca ceza verilecektir.

4) Haberleşmenin Gizliliğini İhlal (TCK m. 132)

TCK'nun 132. Maddesi, kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesini ve haberleşme içeriklerinin hukuka aykırı olarak, yani tarafların rızası dışında ifşa edilmesini suç olarak saymıştır. Örneğin, TCK m. 244'e ilişkin açıklamalarda bulunurken verdiğimiz örnek olayda, bir kimsenin sosyal ağ hesabına giren failin, o kimsenin hesabından başkalarına mesaj gönderdiği varsayımına dayanmıştık. Böyle bir durumda, fail, hesabına giriş yaptığı mağdurun hesabında bulunan ve başkalarıyla yaptığı görüşmeleri içeren mesajları başka bir yere gönderir veya paylaşırsa, TCK m. 132'den dolayı sorumlu tutulacaktır.

TCK'nun 132. Maddesi hükmü, kişinin kendisiyle yapılan haberleşmenin içeriğinin diğer tarafın rızası olmaksızın ifşa edilmesini de suç olarak düzenlemiştir. O halde, yalnızca karşı tarafın üçüncü kişilerle yapmış olduğu görüşmelerin değil, bizatihi fail ile yatığı görüşmelerin yayılması da suçtur. Yani, örneğin, sosyal ağ hesabından bir kimseyle mesajlaşan fail, eğer bu mesaj içeriklerini karşı tarafın rızası olmaksızın yayınlar ya da paylaşırsa, bu durumda TCK m. 132/3 dolayısıyla cezalandırılacaktır.

5) Cinsel Taciz (TCK m. 105)

Sosyal medyada sık görülen suçlardan birisi de cinsel tacizdir. Suçu düzenleyen TCK m. 105, cinsel taciz suçu için failin fiziksel temasını aramamış, mağduru "*cinsel amaçlı olarak taciz etmek*" davranışını suç için yeterli görmüştür. Bu itibarla, sosyal ağ üzerinden, bir kimseye karşı cinsel içerikli sözler söylemek veya bu amaçla görseller paylaşmak gibi fiiller, TCK m. 105 bağlamında cinsel taciz suçuna vücut verecektir.

6) Müstehcenlik ya da Çocuk Pornografisi (TCK m. 226)

TCK 226. maddesi, gerek çocukları müstehcen görüntü, ses ya da yazıya maruz bırakmayı, gerekse de müstehcen görüntü, ses ya da yazı içeren ürünlerde çocukları kullanmayı suç olarak tanımlamıştır.

Müstehcenlik, daha çok bilinen adıyla çocuk pornografisi, bütün Dünyada kararlılıkla üzerine gidilen ve devletlerin suçlulukla mücadele başlıklarının en üstünde bulunan bir suçtur. Sosyal medya da bu suçun sıkça işlendiği mecralardan biridir. Zira, bilişim teknolojisinin gelişmesi ve artık çocukların da küçük yaştan itibaren bilgisayarlara aşina olmasından dolayı, çok erken yaşta iyi düzeyde bilgisayar kullanabilir hale gelmeleri ile birlikte, sosyal ağlarda hesap açmaktadırlar. Bu bağlamda, sosyal ağlarda çocuklarla iletişime geçen yetişkinlerin, çocuklara müstehcen görüntüler göstermeleri yahut çocukları müstehcen ses veya yazılara maruz bırakmaları durumunda, bu suç meydana gelecektir.

IV. SOSYAL MEDYADA İŞLENEN SUÇLULARIN TESPİTİ

Sosyal medyada işlenen suçlar, bilişim sistemleri üzerinden işlendiğinden, bu suçlara ilişkin delillerin toplanması ve suçluların tespiti de özellik arzetmektedir. Bu bağlamda, özellik arzeden durumların izahı amacıyla, bilgisayarlarda arama ve el koyma tedbiri ile uluslararası adli istinabe başlıklarına değineceğiz.

A. CEZA MUHAKEMESİNDE BİLGİSAYARLARDA ARAMA VE EL KOYMA TEDBİRİ

Sosyal medyada işlenen bir suç, ister TCK'da bilişim alanında suçlar arasında düzenlenmiş bir bilişim suçu, ister bilişim sistemleri aracılığıyla işlenen klasik bir suç olsun, elde edilecek deliller bilişim sistemleri üzerinde yer aldığından, elektronik delillerin toplanması rejimine tabi olacaktır.

Elektronik deliller (*e-delil*), "*bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir*." (**Keser Berber**, 2004: 46) Elektronik delillerin *latent*, yani gizil yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirir. Çünkü içerdiği bilgiler yalnızca insanın duyu organları ile algılanamaz. Örneğin olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani nicel gözlem yapılmalıdır.

Buna karşın elektronik delillerin içerisindeki dijital verileri anlayabilmek için ise mutlaka bir uzman tarafından, alet ve cihazlar ile nicel gözlemler yapılmalıdır. Çünkü genellikle makine dili ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır (**Say**, 2006: 29).

Ceza muhakemesi hukukunda, elektronik delillerin toplanması, bir başka deyişle bilgisayarlarda yapılacak delil araştırması Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenmiştir. Buna göre "*Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*" Şu unutulmamalıdır ki, delil araştırmasının bu aşamasında CMK tarafından öngörülen usule eksiksiz bir biçimde uyulması delillerin hukuki olması ve ceza yargılamasında verilecek hükme esas teşkil edebilmesi açısından son derece önemlidir (**Özocak**, 2011: 36).

Bu hüküm uyarınca bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bununla beraber bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. İstenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır[5].

Sosyal medyada işlenen suçlarda da deliller bilgisayar üzerinde yer aldığından, CMK m. 134 uyarınca işlem yapılmalı, ancak koruma tedbiri uygulanırken yasal düzenlemenin getirdiği sınırlara özen gösterilmeli ve kanunun

[5] Bu düzenlemeyle ilgili daha detaylı açıklama ve uygulamada yaşanan sorunlar hakkında bilgi için bkz. **Özbek ve Diğerleri**, 2012: 377 vd.; **Özocak**, 2011: 37 vd.

zorunlu saydığı ilkeler çerçevesinde bilgisayarda arama ve el koyma işlemi gerçekleştirilmelidir.

B. ULUSLARARASI ADLİ İSTİNABE

Çalışmamızın konusunu oluşturan suçların üzerinde işlendiği sosyal medya mecralarının büyük çoğunluğu yurt dışı menşeli ve tüm dünyadan giriş yapılan Facebook, YouTube, Twitter gibi İnternet siteleridir. Bu İnternet sitelerinin bağlı olduğu şirketlerin (Facebook Inc., Google Inc., Twitter Inc.) merkezleri yurt dışında bulunduğundan ve Türkiye'de resmi bir irtibat merkezleri bulunmadığından, bu siteler üzerinden bir suç işlendiğinde, suçlulara nasıl ulaşılacağı uygulamada ciddi anlamda sorun yaratmaktadır. Zira, suç işlenmesi halinde Türk adli makamlarında suçu işleyen hesaba giriş yapan IP adreslerine ulaşılamamakta, bunlara ulaşılması için yurt dışındaki şirket merkezleriyle iletişime geçilmesi gerekmekte, adli makamlar da bu hususla ilgili gerekli özeni göstermemektedir. Öyle ki, uygulamada, bu sosyal ağlar üzerinden işlenen suçlarda, suçluların tespiti için şirket merkezleriyle iletişime geçileceği yerde, "*İnternet sitesinin merkezi yurt dışında olduğundan suçun yurt dışında işlendiği*" yahut "*Faillere ulaşmanın mümkün olmadığı"* veya *"delil yetersizliği*" gibi gerekçelerle takipsizlik ya da beraat kararları verilmektedir.

Oysa, ceza hukukunu ilgilendiren fiillerde, eğer tespit edilecek suçlulara veya delillere ilişkin bilgiler yurt dışındaysa, bununla ilgili gidilecek kurum uluslararası adli istinabedir. Hukukta kural olarak, her mahkemenin bir yargı çevresi vardır ve mahkemeler yalnızca bu yargı çevresi içindeki işleri yapabilirler. Ancak mahkemeler kendi yargı sınırları dışında kalan bir iş yapmak zorunda kaldıklarında, bu sınırların dışına çıkamayacaklarından, o işlemin yapılacağı yargı çevresindeki adli makamlardan hukuki yardım isterler. İşte bu hukuki yardıma istinabe adı verilir (**Pekcanıtez/Atalay/Özekes**, 2011: 103).

Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün B.03.0.UİG.0.00.00.06/010.06.02/7-1 sayılı yazısıyla yayınlanan 01.03.2008 tarih ve 69/1 sayılı "Cezai İşlere İlişkin Uluslararası İşbirliğinde Adli Makamlarımızca Dikkat Edilmesi Gereken Hususlar" Hakkındaki Genelge uyarınca, yurtdışında yerleşik bir tüzel kişiden ceza hukukuna ilişkin bir soruşturma kapsamında yargı makamları

tarafından bilgi temini taleplerinin mümkün olduğu düzenlenmiştir. Suçların işlendiği büyük sosyal ağlarının sahibi şirketlerin çoğunluğunun yerleşim yerleri ABD olduğundan, bilgi temini talebi yapılacak olan ABD ile Türkiye Cumhuriyeti arasında imzalanan, TBMM tarafından 8.10.1980 tarih ve 2312 sayılı Kanunla onaylanan ve 20.11.1980 tarih ve 17166 sayılı Resmi Gazete'de yayımlanan 'Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adlî Yardım Antlaşması'nın hükümlerine göre de, yargı makamları aracılığıyla ABD'de yerleşik tüzel kişilerden bilgi talebinde bulunulması mümkündür.

Bu bağlamda, sosyal medya mecralarında işlenen suçlarda savcılık veya mahkemeler, yurt dışı merkezli İnternet siteleri kullanıcılarının kimliklerini tespit edebilmek yahut buralardan delil toplamak için, uluslararası adli istinabe yolunu kullanmaları gerekmektedir.

V. SONUÇ

Sosyal medya ortamında işlenen suçları, ceza kanunlarında yer alan ancak İnternet ortamında işlenişleri bakımından farklılık arzeden hakaret, tehdit, müstehcenlik gibi klasik suçların yanı sıra, yalnızca İnternet ortamında işlenmesi mümkün olan bilişim suçları olarak ikiye ayırmak mümkündür. Sosyal medya mecralarında sık rastlanan bu her iki suç grubunda da, çoğu kez fail kimliğini gizlemekte ve böylece suçun mağdur bakımından vahametini artmakta, ayrıca failin yakalanması da güçleşmektedir. İşte, bu suçları diğer suçlardan ayıran belki de en önemli özellik, faillerinin tespitinin kendine has bir nitelik arzetmesi ve bu tespitte kullanılacak yasal ve teknik yöntemlerle ilgili sorunlardır. Teknik yöntemlerle ilgili sorunlar, daha çok delil tespiti ve suçlu takibi yapan personelin kimi zaman nicelik kimi zamansa nicelik olarak yetersizliği noktasında düğümlenirken; yasal sorunlar CMK m. 134 bağlamında elektronik delillerin toplanmasında kanuni şartlara uyulmaması, kanuna aykırı delil elde edilmesi, uluslararası alanda yapılacak IP tespiti ya da başka delil elde etme yolları için düzenlenen yasa ve yönetmeliklerle getirilen uluslararası adli istinabe gibi kurumların mahkemelerce veya savcılıklarca bilinmemesi yahut doğru bir biçimde uygulanmaması gibi başlıklarda toplanabilir. Ancak, bütün bu sorunların tespit edilip ortaya konulması yeterli olmamakta; nitelikli

ve sayıca fazla teknik personel yetiştirilmesi, suçlulukla mücadele ve adli bilişim yöntemlerinin geliştirilmesi, kanuna uygun delil toplanması hususunda kolluk kuvvetinin bilgilendirilmesi ve bilişim ihtisas mahkemelerinin kurulması tartışmaları gibi çözüm başlıkları halen güncelliğini ve gerekliliğini korumaktadır.

VI. KAYNAKÇA

AKINCI, Hatice / ALIÇ, A. Emre / ER, Cüneyd; *"Türk Ceza Kanunu ve Bilişim Suçları"*, İnternet ve Hukuk, İstanbul, 2004.

BOZDOĞAN AKBULUT, Berrin; "*Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Sayı 1-2, C. 8, Konya, 2000.

CENTEL, Nur / ÇAKMUT, Özlem / ZAFER, Hamide; Türk Ceza Hukukuna Giriş, İstanbul, 2006.

KESER BERBER, Leyla; Adli Bilişim, Ankara, 2004.

KETİZMEN, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

KEYMAN, Selahattin; "Cürmi Fiilin Yapısal Unsuru Olarak Hareket", AÜHF Dergisi, C. 40, S. 1-4, Ankara, 1988.

KEYMAN, Selahattin; "Tipiklik ve Ceza Hukuku", AÜHF Dergisi, C. 37, S. 1-4, Ankara, 1980.

KURT, Levent; Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

KÜZECİ, Elif; Kişisel Verilerin Korunması, Ankara, 2010.

ÖZBEK, Veli Özer / KANBUR, M. Nihat / DOĞAN, Koray / BACAKSIZ, Pınar / TEPE, İlker; Ceza Muhakemesi Hukuku, Ankara, 2012.

ÖZEN, Muharrem/BAŞTÜRK, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

ÖZDİLEK, Ali Osman; Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006.

ÖZOCAK, Gürkan; "*Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması*", 2. Uluslararası Bilişim Hukuku Kurultayı Bildiri Kitabı, İzmir, 2011.

ÖZOCAK, Gürkan; "*DDoS Saldırısı ve Failin Cezai Sorumluluğu*", Bilişim 2012 – 29. Uluslararası Bilişim Kurultayı Bildiriler Kitabı, Ankara, 2012.

ÖZTÜRK, Bahri / ERDEM, Mustafa Ruhan; Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, Ankara, 2012.

PARLAR, Ali; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2011.

PEKCANITEZ, Hakan / ATALAY, Oğuz / ÖZEKES, Muhammet; Medeni Usul Hukuku, Ankara, 2011.

SAY, Kubilay; Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara, 2006. (Yayımlanmamış Yüksek Lisans Tezi)

SINAR, Hasan; İnternet ve Ceza Hukuku, İstanbul, 2001.

TARHAN, Emine Ülker; Yeni Türk Ceza Yasasında Tehdit ve Hakaret Suçları, Ankara, 2007.

TOROSLU, Nevzat; Ceza Hukuku Genel Kısım, Ankara, 2012.

YALÇIN SANCAR, Türkan; Alenen Tahkir ve Tezyif Suçları, Ankara, 2007.