

# SOSYAL MEDYADA SUÇ İŞLENMESİ

\*Hilal ÇALIK

## Sosyal Medya Nedir ?

Sosyal medya, kullanıcılar tarafından oluşturulan bilginin basit, anlık ve çift taraflı olarak paylaşılmasını ve ulaşılmasını sağlayan yeni bir medya biçimidir.

We Are Social-Digital in 2016'ya göre günde ortalama 2 saat 32 dakikamızı sosyal medyada geçirmekteyiz. Dünya üzerinde 3,419 milyar insan internete bağlanıyor, 2,307 milyar kullanıcı aktif olarak sosyal medyada yer alıyor. 3,790 milyar mobil cihaz kullanıcısının 1,968 milyarı ise sosyal medyayı mobil cihazlar üzerinden kullanıyor.

Peki bu kadar sık kullandığımız sosyal medya hesaplarında yaptığımız paylaşımların hukuka uygun olup olmadığını hiç düşünüyor muyuz ?

5237 Sayılı Türk Ceza Kanunu'nda yer alan ve Facebook, Twitter, Instagram, Youtube, Snapchat, Periscope gibi sosyal medya araçlarıyla, Whatsapp, Skype, Facetime, Tango gibi iletişim araçlarıyla, gmail, hotmail, yahoo gibi e-posta araçlarıyla veya swarm, foursquare gibi yer bildirim araçlarıyla, google plus, blogger, wordpress gibi yayın araçlarıyla internet üzerinden işlenebilecek başlıca suçlar şunlardır:

Cinsel Taciz (m 105)

Tehdit (m 106)

Şantaj (m 107)

Nefret ve Ayırmıcılık (m 122)

Kişilerin Huzur ve Sükununu Bozma (m 123)

Haberleşmenin Engellenmesi (m 124)

Hakaret (m 125)

Haberleşmenin Gizliliğini İhlal (m 132)

Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (m 133)

Özel Hayatın Gizliliğini İhlal (m 134)

Kişisel Verilerin Kaydedilmesi (m 135)

Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (m 136)

Nitelikli Dolandırıcılık (m 158)

Halkı Kin ve Düşmanlığa Tahrik veya Aşağılama (m 216)

Hayasızca Hareketler (m 225)

Müstehcenlik (m 225)

Kumar Oynanması İçin Yer ve İmkan Sağlama (m 228)

Suç Delillerini Yok Etme, Gizleme veya Değiştirme (m 281)

TCK Onuncu Bölümde Yer Alan Bilişim Suçları

Bilişim Sistemine Girme (m 243)

Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (m 244)

Banka veya Kredi Kartlarının Kötüye Kullanılması (m 245)

Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması (m 246)

## **UYGULAMADA SIK KARŞILAŞILAN SUÇLAR**

### **CİNSEL TACİZ**

Kanuni tanımdan anlaşılacağı üzere cinsel taciz suçunda önemli unsurlardan bir tanesi vücut bütünlüğünün ihlal edilmemesidir. Bu bağlamda sosyal medya üzerinden gönderilen cinsel içerikli iletiler, görseller veya karşılıklı görüntülü konuşma sırasında sergilenen eylemlerle cinsel taciz suçunun işlenmesi mümkündür.

Sözü edilen suç sırf hareket suçu olmakla beraber, hareketin kısımlara bölünebildiği oranda teşebbüsten bahsetmek mümkün olacaktır. Buna göre, sosyal medya platformları üzerinden görüntülü konuşma sırasında, cinsel amaçlı bir eylem gerçekleştirme niyetiyle hareketine başlayan kişinin veya cinsel içerikli iletinin gönderildiği sırada internet bağlantısının kopması, bilgisayarın bozulması vb. durumlarda hareketinin teşebbüs aşamasında kaldığını söylemek doğru olacaktır.

### **TEHDİT**

Günümüzde tehdit suçu sadece yüzyüze değil, Whatsapp, Viber, Tango, Wechat, Line, Skype gibi anlık mesajlaşma programları vasıtasıyla resim ya da ileti göndermek suretiyle olabileceği gibi Facebook, Twitter, Instagram gibi sosyal medya platformlarından yapılan paylaşımlar ya da iletiler vasıtasıyla da olabilir. Ancak tehdidin internet ortamında olmasıyla gerçek hayatta olması arasında bir fark yoktur. Her durumda tehdidin niteliği ve ağırlaştırıcı sebep içerip içermediği önemlidir. İnternet ortamında işlenen tehdit suçlarının gerçek hayatta işlenen tehdit suçlarından cezai yaptırım açısından farkı yoktur.

Ancak suçun ispatı noktasında büyük bir fark vardır. Soruşturma esnasında işin ciddiye bindiğini farkedene fail tehdit içeren iletisini ya da paylaşımını silmek suretiyle suçun ispatını engelleyebilir. Bu açıdan bakıldığında soruşturma sırasında bir bilişim avukatıyla çalışılması

hayati öneme haizdir. Bilişim avukatına ek olarak, ispatı mümkün kılabilmek için tehdit içeren unsurun ekran görüntüsünün (screenshot) alınması gerekmektedir.

## **HAKARET**

Ceza hukuku; kişiyi onur, şeref ve haysiyetine karşı fiillere karşı korumaktadır. Her ne gerekçe ile olursa olsun bir kimsenin başka bir kimseyi aşağılamak hakkı yoktur. Aşağılamak, sövme şeklinde gerçekleşebileceği gibi somut bir fiilin isnadı şeklinde de olabilir. Böylelikle herhangi bir kimseyi sosyal medya araçları (facebook, twitter vs.) vasıtasıyla aşağılamak suç oluşturacaktır.

Aşağılama hareketi şayet bir kimsenin uygunsuz fotoğraflarını yayınlamak veya örneğin bir partide aşırı alkol alıp kustuğu bir videosunu aşağılamak amacı ile Youtube'da paylaşmak şeklinde gerçekleştiyse hem hakaret hem de 'özel hayatın gizliliğini ihlal' suçu oluşacaktır ve fikri içtima kuralları uygulanacaktır.

Haber siteleri bakımından suçu ve faili değerlendirmek için öncelikle içerik ve yer sağlayıcı sükeleri önem taşımaktadır. İçerik ve yer sağlayıcı kavramları 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da düzenlenmiştir

5651 sayılı kanuna göre İçerik Sağlayıcı; İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, deęiştiren ve sağlayan gerçek veya tüzel kişiler olarak tanımlanmış ve internet ortamında kullanıma sunduęu her türlü içerikten sorumlu olacak şekilde, Yer Sağlayıcı ise; Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler olarak tanımlanmış ve yer sağladığı içerięi kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü kılınmayacak şekilde düzenlenmiştir.

Haber siteleri düzenledikleri ve yayınladıkları haberler bakımından içerik sağlayıcı olarak, sosyal medyayla entegre şekilde kullanıma sundukları yorum araçları bakımından ise yer sağlayıcı olarak nitelendirilmektedirler.

Yayımlanan haberlere yapılan yorumlarda sosyal medya aracılığı ile hakaret suçunu işleyenler bakımından haber sitelerinin cezai bir sorumluluęu bulunmamakta, cezai sorumluluk suçta şahsiliik ilkesi gereęi tamamıyla eylemi gerçekleştiren kişiye aittir.

Hakaret suçunun klasik hali ani suç olarak deęerlendirilmektedir. Ancak suçun internet sitesi veya sosyal medyada işlenmesi halinde kesintisiz bir suçtan bahsetmek mümkün olacaktır. Bu durumda eylem devam ettięi sürece her an 6 aylık şikayet süresi baştan başlayacaktır.

Hakaret suçu kapsamında soruşturulan ve şikayete konu eylem ve söylemler kime yöneldiğine göre deęerlendirilmelidir. Şöyle ki, toplum içerisinde belirli tanınmışlık seviyesinde bulunan ve topluma mal olmuş kişilerle, politikacı ile siyasetçiler bakımından daha esnek deęerlendirme yapılmaktadır. Kişilerin buldukları konum dolayısıyla eleştirilmesi gerekebilir veya bu konum nedeniyle politik söylemlerde bulunabilirler. Tüm bu

söylem ve eleştiriler sıradan vatandaşa söylenmiş söz veya sıradan vatandaşın söylediği söz olarak değerlendirilemez.

Bu durumda politikacıların, siyasetçilerin, devlet adamlarının, topluma mal olmuş kişilerin bazı eleştirilere hatta ağır eleştirilere konumları gereği katlanma yükümlülüğü bulunmaktadır. Yargıtay Ceza Genel Kurulu 20.03.2007 tarih, 2007/4-65E., 2007/70K. sayılı kararında ilkel olarak bazı ölçütlere yer vermiştir. Bu ölçütlerin yer alması durumunda hakaret suçunun oluşmadığı, eleştiri sınırları içinde kaldığı belirtilmiştir.

Bu ölçütler ise;

- ✘ Eleştiriye konu haberin veya olayın gerçek ve güncel olması
- ✘ Açıklanmasında kamunun ilgi ve yararının bulunması
- ✘ Açıklanış şekli ile konusu arasında düşünsel bir bağ bulunması
- ✘ Açıklamalarda küçültücü sözlerin kullanılmamasıdır.

Yargıtay 4. Ceza Dairesi 28.01.2014 tarih, 2012/16551 E., 2014/2237 K., sayılı kararında vatandaşın kurul üyelerine yazdığı dilekçedeki “Anayasa, Kanunlar, Yönetmelikler, yargı hukuk hak anlamayan kıyakçı gaspçı zihniyetli icraatçılar hesabını iyi biliyorlar ya sonrası bu bağlamda görevim ülkeme aileme, özürülere, inançlarıma hizmet vermek doğrultusundan konuyu TC makamlarına arz ederim” sözlerini tartışmıştır. Kararda Anayasa’nın 24 ile 30. maddelerine ve İHAS 9 ve 10. maddelerine atıf yaparak dilekçede belirtilen sözlerin sanığın haksızlığa uğradığı kanısıyla yazdığı, eleştiri ve yakınma boyutunda kaldığı belirtilmiştir.

## **HABERLEŞMENİN GİZLİLİĞİNİ İHLAL**

Aleni olmayan telefon konuşmalarını ilgilinin rızası olmadan dinlemek TCK’ya göre suçtur. TCK m 132’de düzenlenmiş bulunan bu suç tipinde sadece telefon dinlemek değil, kişiler arasındaki her türlü haberleşmenin (mektup, telgraf, -e posta, 3.kişilere kapalı olan facebook ve sohbet odası konuşmaları vs.) içeriğinin öğrenilmesi cezai yaptırım altına alınmıştır.

Özel kanunlarda (PVSK, Jandarma Teşkilat, Görev ve Yetkileri Kanunu vs.) yer alan ‘önleme amaçlı dinleme’ hükümleri ve CMK m 135 gereği usulunce yapılan dinlemeler dışında, kişiler arasındaki haberleşmenin gizliliğinin ihlali kanunumuz tarafından suç kabul edilmektedir.

Haberleşme gizliliğinin dinlemek veya okumak suretiyle ihlali suçun basit halini oluştururken, haberleşme içeriklerinin ayrıca kayda alınması durumunda suçun nitelikli hali oluşmaktadır.

Haberleşme içeriğinin hukuka aykırı olarak ifşası ise ayrı bir suç olarak düzenlenmiştir. Kişinin kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa etmesi de ayrıca suç olarak düzenlenmiştir.

Bununla birlikte kamuya mal olmuş kişiler bakımından yayın yasağı getirilmemiş olmak ve soruşturmanın gizliliğinin ihlal edilmemesi kaydıyla basın-yayın özgürlüğü kapsamında gazetecilik mesleğinin icrası kapsamında hukuka uygun yapılan haberler bu kapsamda suç olarak nitelendirilmeyecektir.

Delil elde edilmesine yönelik olarak dinleme ve kayıt altına almaları hukuka uygun gören mahkeme kararları vardır. Yargıtay Ceza Genel Kurulu da ‘kişinin kendisine karşı işlenmekte olan bir suçla ilgili olarak, bir daha kanıt elde etme olanağının bulunmadığı ve yetkili makamlara başvurma imkanının olmadığı ani gelişen durumlarda karşı tarafla yaptığı konuşmaları kayda alması halinin hukuka uygun olduğunun kabulü zorunludur. Aksi takdirde kanıtların kaybolması ve bir daha elde edilmemesi söz konusudur.’ gerekçesiyle bu kayıtları hukuka uygun görmüştür.

## **ÖZEL HAYATIN GİZLİLİĞİNİ İHLAL**

Öğretide baskın görüşe göre, kişinin hayatı üç alana ayrılmaktadır: gizli hayat, mahrem hayat ve kamuya açık hayat.

TCK m 134 ile ‘gizli yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının saptanması ve kaydedilmesi’ cezalandırılmaktadır.

‘Anonimleşme’ söz konusu olduğunda fotoğraf ve video kaydı kullanılabilir. Örneğin; öğrencileri ile fotoğraf çektiren bir öğretmen, söz konusu fotoğrafın internette paylaşılması durumunda özel hayatının gizliliğinin ihlal edildiğini iddia edemeyecektir.

Bunun dışında basın mensuplarına açıklama yapan veya görüntü veren kişinin bunların yayınlanmasına zımnen izin verdiği; kamuya mal olmuş kişilerin özel hayatlarının bir kısmından gönüllü olarak feragat ettikleri kabul edilir.

Kamuoyunun bilgilendirilme hakkı kapsamında örneğin bir bakanın gayrimeşru ilişkisine ait görüntülerin haber niteliğinde hazırlanıp yayınlanması durumunda basın mesleğinin icrası kapsamında eylem hukuka uygun kabul edilir.

## **NİTELİKLİ DOLANDIRICILIK**

Örneğin başkasının adına sahte Facebook profili oluşturarak, namına hareket ettiği arkadaşlarından, kendini profil sahibi kişiymiş gibi tanıtarak para, kontör veya farklı maddi istemlerde bulunması nitelikli dolandırıcılık suçunu oluşturacaktır.

## **KİŞİSEL VERİLERİN KAYDEDİLMESİ**

Bu suç genellikle, kişisel veri havuzları oluşturma ve bu havuzları reklam şirketlerine satma eylemleri şeklinde karşımıza çıkmaktadır. Ayrıca internette forum bilgilerinin 3.kişiler ile paylaşılması halinde de bu suç oluşacaktır.

## **VERİLERİ HUKUKA AYKIRI OLARAK VERME**

Çoğu işlemde istenen nüfus cüzdanı fotokopileri hassas veriler barındırmaktadır. Bu bilgilerin 3.kişilerle hukuka aykırı olarak paylaşılması halinde suç oluşur. Ayrıca kişisel verilerin hukuka aykırı olarak ‘belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle’ bir başkasına verilmesi halinde ceza artırılarak verilecektir. Örneğin bir GSM operatörü bayininin hat açtırma işlemi için eline geçen kimlik fotokopisini 3.kişiler ile paylaşması halinde TCK m 137/1-b bağlamında ‘verileri hukuka aykırı olarak verme’ suçu oluşur.

## **HAYASIZCA HAREKETLER**

TCK’da teşhirciliğin ne olduğu açıklanmamaktadır. Teşhircilik hareketlerinin ne olduğuna örf-adetler, gelenekler dikkate alınarak somut olayın özelliklerine ve günün koşullarına göre hakim-mahkeme tarafından karar verilmelidir. Maddenin gerekçesi teşhircilik eylemlerindeki alenilik şartının fiziki olmasının zorunlu mu olduğu yoksa siber ortamda yapılmasının yeterli mi olduğuna cevap vermemektedir.

Öğretideki baskın görüş, teşhircilik suçunun siber ortamlarda işlenmesinin mümkün olduğu yönündedir. Teşhircilik suçu 3 şekilde işlenebilir. 1.si TCK m 105/2-e kapsamında cinsel taciz suçunun teşhir suretiyle işlenmesi, 2.si TCK m 226/2 kapsamında internet ortamında yayınlanan müstehcen görüntü/pornografik içeriğin teşhir içermesi ve 3.sü bunlar dışında kalan siber ortamdaki teşhircilik eylemleridir.

Online teşhircilikte, teşhire konu görüntünün sahibine ait olması ve görüntü sahibinin bizzat kendisi veya bilgisi dahilinde diğer kişilerce paylaşılması gerekmektedir. Örneğin; herkese açık profil resmine kendi tenasül organının fotoğrafını koyan kişi online teşhircilik suçunu işlemiş olacaktır. Buna karşın herhangi bir cinsel uzvun görüntüsünün internette paylaşılması halinde bu suç değil diğer şartları mevcutsa TCK m 226 kapsamında müstehcenlik suçu oluşacaktır.

## **KUMAR OYNANMASI İÇİN YER VE İMKAN SAĞLAMA**

TCK kapsamında kumar oynamak değil kumar oynanması için yer ve imkan sağlamak suçtur. Kumar oynamak Kabahatler Kanunu m 34’te yer alır.

İnternet ortamında kumar oynatmanın suç sayılabilmesi için 3 koşul aranmalıdır. 1.si oyunun siber ortamda oynatılması kazanç kastı ile icra edilmeli, 2.si kar ve zarar talihe bağlı olmalı, 3.sü oynatılan oyundaki kar ve zararın maddi bir değeri olmalıdır.

## **SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME**

Şifre hırsızlığında, şifre kırmak konusunda başvuru en basit yöntem; şifresi kırılacak kişinin doğum tarihi, yaşadığı yer, evcil hayvanının adı gibi ilk akla gelen kombinasyonları denemektir. Bu tarz basit kombinasyonların denenmesi usulü ile şifrenin bulunması suç değildir.

Son dönemde sıklıkla başvuru alan şifre ele geçirme yöntemi ‘sahteform (fakeform)’dur. Bu yöntemde göre; kişiler şifrelerini girmeleri için yanıltıcı sayfalara yönlendirilmekte ve kişilerin şifrelerini kendi eliyle girmesi sağlanmaktadır. Burada kişiler şifrelerini rızaları ile girseler de neye rıza gösterdiklerini bilmediklerinden hukuka uygunluktan söz edilememektedir.

Şifrenin ele geçirilmesi değil, bilişim sistemi olarak kabul edilen sosyal ağ hesaplarına sahibinin rızası bulunmadan giriş yapılarak, belli bir süre bu hesabın kullanılması, hesaptaki kişisel verilerin hukuka aykırı olarak kaydedilmesi, hesabın aracı olarak kullanılmasıyla hakaret, tehdit, cinsel taciz gibi suçların işlenmesi gibi eylemler suç oluşturmaktadır.

Yargıtay da, Facebook, MSN şifrelerinin eşe geçirilerek değiştirilmesini, hesabı bilişim sistemi olarak nitelendirerek asıl hesap sahibinin bilişim sistemine erişiminin engellenmesi olarak değerlendirerek TCK m 244/2 kapsamında suç olarak değerlendirmiştir.

### **SUÇ OLARAK KABUL EDİLMEYEN EYLEMLER**

Hackerlık faaliyetlerinin bir çoğu bahsi geçen hükümlerden (TCK m 243-244) en az birini ihlal etmektedir. Buna karşın beyaz şapkalı hacker denilen ve bilgisayar/işletim/sunucu gibi bilişim sistemlerinin güvenliğini sağlamak amaçlı siber saldırı öncesi önlemler alan kişiler ise siber saldırılara karşı savunmanın zorunlu ve orantılı olması şartıyla karşılık verdiklerinde meşru müdafaa hükümlerinden yararlanabileceklerdir.

Örneğin; DDOS (Distributed-Denial-of-Service) saldırısını engellemek amacıyla saldırıyı gerçekleştiren veya gönüllü köle (zombie) bilişim sistemlerine karşı DDOS saldırısı yapılabilecektir.

Olası siber saldırıları önlemek amacıyla yazılım geliştirilmesi de suç teşkil etmemektedir. Örneğin; film şirketleri, orijinal DVD filmlerin kopyalanmasını önlemek amacıyla, kopyalama girişimi sırasında bilişim sistemine bulaşan virüsleri orijinal film DVD’lerine koymaktadırlar. DVD kabında gerekli uyarıların yapılması ve bilişim sisteminin tümüne maddi boyutları karşılanamayacak ölçüde zarar verilmemesi koşuluyla, film şirketlerinin bu savunma hareketi meşru müdafaa kapsamında değerlendirilebilir.