Araştırma Makalesi | **Research Article** **ÇÜHAD 2022/2** | **e-ISSN:** 2822-4809

YARGITAY KARARLARI IŞIĞINDA DİJİTAL FLÖRT ŞİDDETİ TEŞKİL EDEN YÖNTEMLERDEN DOĞAN CEZA SORUMLULUĞU•

Criminal Responsibility Arising from Methods that constitute Digital Dating Violence in the Light of Turkish Supreme Court Decisions

Mehmet Emre YILDIZ*

ÖZ

Flört şiddeti, flört ilişkisinde bulunan partnere karşı gerçekleştirilen fiziksel, cinsel, psikolojik ve ekonomik zarara neden olan herhangi bir davranışı ifade etmektedir. Günümüzde bilgi iletişim teknolojilerinin gelişmesi ve internet kullanımının artması ile birlikte flört şiddeti teşkil eden davranışlar bilişim alanına taşınmıştır. Flört şiddetinin bir türü olan "dijital flört şiddeti" kavramı, dijital teknolojileri kullanan flört partnerini kontrol etme, tehdit etme veya ona baskı yapma gibi eylemleri içeren davranışlar için kullanılan genel bir kavramdır. Dijital flört şiddeti teşkil eden yöntemlerin ilgili kişiye fiziksel, cinsel, psikolojik ve ekonomik yönden zarar vermesi konunun ceza hukuku alanında da tartışılması gerekliliğini ortaya koymaktadır. Dijital flört şiddeti teşkil eden yöntemlerin uygulanması ceza hukuku ile korunan farklı hukuki değerleri ihlal edebilecektir. Bu nedenle çalışmada özellikle dijital flört şiddeti yöntemlerinin özelliği, ceza hukuku açısından sonuçları ve Türk Ceza Kanununda hangi suçları oluşturacağı Yargıtay' ın vermiş olduğu kararlar ışığında tartışılmaya çalışılmıştır.

Anahtar Kelimeler: Flört şiddeti, Yakın partner şiddeti, Hesap ele geçirme, Kişisel verileri paylaşma, Cinsel içerikli mesajlaşma, Cinsel içerikli şantaj, İntikam pornosu, siber cinsel uşaklaştırma, Sahte cinsel içerikli görüntü üretme.

• **Gönderi**: 19.08.2022 - **Kabul**: 24.09.2022 | **Received**: 19.08.2022 - **Accepted**: 24.09.2022.

* Arş. Gör. Dr., Çukurova Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, Adana, Türkiye ✉ yildizmehmetemre@gmail.com • ORCİD 0000-0001-9969-7730.

Atıf Şekli / **Cite As**: YILDIZ, Mehmet Emre (2022). Yargıtay Kararları Işığında Dijital Flört Şiddeti Teşkil Eden Yöntemlerden Doğan Ceza Sorumluluğu. ÇÜHAD, (2), 93-143.

İntihal / **Plagiarism**: Bu makale bir intihal engelleme yazılımı aracılığıyla denetlenmiş ve en az iki hakem incelemesinden geçmiştir. / This article has been checked via a plagiarism prevention software and reviewed by at least two referees.

ABSTRACT

Dating violence refers to any behavior that causes physical, sexual, psychological and economic harm to the partner in a dating relationship. Today, with the development of information and communication Technologies and the increase in the usage of Internet, behaviors that constitute dating violence have begun to be carried out in cyber space. The concept of "digital dating violence", which is a type of dating violence, is a general concept of using behaviors that include actions such as controllinf, threatening or putting pressure on the dating partner using digital technologies. The fact that the methods which constitute digital dating violence physically, sexually, psychologically and economically harm to the person concerned reveals the necessity of discussing the issue in the field of criminal law. The execution of methods that constitute digital dating violence may violate different legal values protected by criminal law. Therefore, in this study, especially the characteristics of digital dating violence methods, their consequences in terms of criminal law and which crimes they will constitute in the Turkish Penal Code have been tried to be discussed in the light of the decisions of Turkish Supreme Court.

Keywords: Dating violence, Intimate partner violence, Account take over, Sharing personal data (doxing), Sexting, Sextortion, Revenge porn, Cyber sexual grooming, Deepfake.

GİRİŞ

Günümüzde bilgi iletişim teknolojileri alanındaki gelişmelerle birlikte yakın partner/flört şiddetinin bir türü olan dijital flört şiddeti kavramı ön plana çıkmaktadır. Dijital flört şiddeti kavramı genel olarak dijital teknolojileri kullanan flört partnerini kontrol etme, tehdit etme veya ona baskı yapma gibi eylemleri içeren davranışlar için kullanılan şemsiye bir kavramdır. Dijital flört şiddeti kavramı, her ne kadar tüm dijital (sanal) platformlarda gerçekleştirilen şiddet eylemlerini ifade eden kapsayıcı bir kavram olsa da, günümüzde sosyal medyanın yoğun kullanımı nedeniyle söz konusu eylemlerin sosyal medya üzerinden gerçekleştirilmesi konunun her birey için önemini daha da artırmaktadır. Nitekim Toplumsal Bilgi ve İletişim Derneği tarafından 2021 yılında yapılan Türkiye' de Dijital Şiddet Araştırmasına göre, dijital şiddet eylemlerinin en çok gerçekleştirildiği platformlar sosyal medya platformlarıdır (Instagram %53, Facebook %35, Twitter %19) Ülkemiz açısından sosyal medya kullanımının yoğunluğu da dikkate alınırsa, dijital şiddet yöntemlerinin gün geçtikçe artan uygulaması ve bu yöntemlerin yaratmış olduğu olumsuz etkiler konunun yakından incelenmesini gerektirmektedir.

Dijital şiddet yöntemleri sanal ortamlarda flört partnerini kontrol etme ve ona baskı kurma eylemleri, flört partnerinin itibarına zarar verici davranışlar, flört partnerinin ekonomik istismarına yol açacak davranışlar, flört partneri ile ilgili görüntü ya da yazıya dayalı cinsel

şiddet davranışları ya da çocukların cinsel sömürüsü amacıyla sanal ortamların kullanılması gibi çok değişik yöntemleri içerisinde barındırabilmektedir. Bu yöntemlerin çeşitliliği eylemi gerçekleştiren failin ceza hukuku açısından sorumluluğu açısından da farklı suç tiplerini gündeme getirmektedir. 5237 sayılı TCK' da söz konusu bu yöntemleri cezalandıran genel bir düzenleme bulunmamaktadır. Bu nedenle fail tarafından kullanılan yöntemin türüne göre bilişim alanında suçlar (TCK m. 243-245/A), haberleşmenin gizliliğini ihlal suçu (TCK m. 132), özel hayatın gizliliğini ihlal suçu (TCK m. 134), cinsel dokunulmazlığa karşı suçlar (TCK m. 102-105), bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu (TCK m. 158/1-f), tehdit ve şantaj suçu (TCK m. 106-107), müstehcenlik suçu (TCK m. 226), kişilerin huzur ve sükununu bozma suçu (TCK m. 123) ve hakaret suçu (TCK m. 125) gibi değişik suçlar oluşabilecektir. Çalışmada öncelikle dijital flört şiddeti kavramı, daha sonra ise bu kavram içerisinde değerlendirilen suç teşkil eden eylemler ve bunlardan doğan ceza sorumluluğu Yargıtay kararları ışığında incelenmeye çalışılacaktır.

I. DİJİTAL FLÖRT ŞİDDETİ KAVRAMI

Dijital flört şiddeti kavramının ne ifade ettiğinin anlaşılabilmesi için öncelikle kavramın içerisinde barındırdığı sözcüklerin anlamlarının ortaya konulması gerekmektedir. "Dijital", "flört" ve "şiddet" sözcüklerinin birleşiminden oluşan "dijital flört şiddeti" kavramı, içerisinde barındırmış olduğu sözcükler temelinde değerlendirildiğinde, bu kavramın en yalın şekilde dijital (sanal) ortamda gerçekleşen flört şiddeti teşkil eden yöntemleri karşılamak için oluşturulmuş olduğu anlaşılmaktadır.

Türk Dil Kurumu' nun sözlüğüne bakıldığında "dijital" kelimesi, sıfat olarak "*Verileri bir ekran üzerinde elektronik olarak gösteren*" ya da isim olarak "*Verilerin bir ekran üzerinde elektronik olarak gösterilmesi*" olarak tanımlanmaktadır[1]. Bilişim terimleri sözlüğündeki diğer bir tanıma göre[2] ise "dijital", "*Ses, görüntü, bilgisayar verisi ya da diğer bilgiler için işlemleri yapmak veya ikilik (sıfır veya bir) sinyalleri iletmek için voltaj, frekans, genlik, zaman vb. ayrık değişkenleri kullanan bir yöntem*"dir. Her ne kadar belirtilen teknik anlamdaki tanımlamalar olsa da, dijital flört şiddeti kavramının içeriğindeki "dijital" sözcüğü ile anlatılmak istenen,

1 Bkz. Türk Dil Kurumu Güncek Türkçe Sözlük, https://sozluk.gov.tr/ (Erişim Tarihi: 10.05.2022).

2 ERALP, s. 48.

"flört şiddeti" teşkil edebilecek davranışların siber/sanal[3] ya da bilişim[4] alanı[5] olarak adlandırılan ortamda işlenmesidir.

Flört şiddeti kavramı, flört (duygusal ilişki[6]) içinde bulunan kişilerden birisi tarafından uygulanan şiddet anlamına gelmektedir. Bu bakımdan nelerin "şiddet" olarak kabul edildiği önem arz eden bir konudur. Şiddet, Dünya Sağlık Örgütü (WHO) tarafından "*fiziksel güç veya iktidarın kasıtlı bir tehdit veya gerçeklik biçiminde bir başkasına uygulanması sonucunda maruz kalan kişide yaralanma, ölüm ve psikolojik zarara yol açması ya da açma olasılığı bulunması*" durumu olarak tanımlanmaktadır[7]. Bu tanımda "fiziksel güç" kavramı yanında "iktidar" kavramına da yer verilmesi, tehdit ya da yıldırma örneklerinde olduğu gibi, şiddet içeren eylemlerin bir iktidar ilişkisinden kaynaklanan eylemleri de içerecek şekilde geleneksel şiddet anlayışını genişletmesi sonucunu doğurmaktadır[8]. İktidar kullanımı ("*use of power*"), daha bariz şiddet içeren eylemlerin icrasına ek olarak hareketsiz kalma ya da ihmali eylemleri de içermektedir[9]. Böylece "fiziksel güç veya iktidar kullanımı" kavramı, ihmali ve her türlü fiziksel, cinsel ve psikolojik istismarın yanı sıra intihar ve kişinin kendi istismarına yol açan diğer eylemleri içermektedir[10]. Şiddet tipolojisine bakıldığında şiddet, kendine yönelik (*self-directed*), kişilerarası (*interpersonal*) ve kollektif şiddet türleri olarak ayırıma tabi tutulmaktadır. Flört şiddeti, bu ayırımda kişilerarası şiddet grubuna dâhil olmaktadır. Buna göre flört şiddeti, partnere karşı gerçekleştirilen fiziksel, cinsel, psikolojik ve yoksunluk ya da ihmali eylemler şeklinde gerçekleşebilmektedir[11]. Uluslararası literatürde flört şiddeti kavramı ile

---

3 Siber terimi, İng. "*Cyber*" sözcüğünün Türkçe karşılığı olarak kullanılmakta ise de, uluslararası hukuk metinlerinin resmi Türkçe çevirilerinde İng. "*Cyber*" sözcüğü "sanal ortam" olarak çevrilmektedir. Bkz. Sanal Ortamlarda İşlenen Suçlar Sözleşmesi, Budapeşte, (23.11.2001) (R.G., T. 09.08.2014, S. 29083).

4 "*Bilişim*" sözcüğü, güncel Türkçe sözlükte "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" şeklinde tanımlanmıştır. Bkz. Türk Dil Kurumu Güncek Türkçe Sözlük, https://sozluk.gov.tr/ (Erişim Tarihi: 10.05.2022).

5 Bilişim alanı, verilerin işlenmesini, saklanmasını, işlenilen verilerin aktarılmasını ve bunların teknolojilerini ifade eden bir kavramdır. Bilişim alanı kavramı, bilgisayar kavramını da içine alan daha üst bir kavramdır. Bkz. AKBULUT, s. 110.

6 "*Flört*" sözcüğü, güncel Türkçe sözlükte, "*Kadınla erkek arasındaki duygusal ilişki*" ve "*Birbirine duygusal ilgi duyan kadın ve erkek*" olarak tanımlanmaktadır. Bkz. Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/ (Erişim Tarihi: 10.05.2022). Başka bir tanıma göre flört; sosyal etkileşim içeren ve ilişkiye devam ya da sonlandırma niyetiyle eylemlerde bulunulan, daha sonra bir tarafın ya da iki tarafın isteğiyle sonlandırılan ya da resmi bir ilişkiyle (evlilik, nişanlılık, birlikte yaşama) devam eden bir ilişki türüdür. Bkz. AVŞAR BALDAN, AKIŞ, s. 41.

7 POLAT, s. 15-16; WORLD HEALTH ORGANIZATION (WHO), World report on violence and health, s. 5.

8 WHO, World report on violence and health, s. 5.

9 WHO, World report on violence and health, s. 5.

10 WHO, World report on violence and health, s. 5.

11 WHO, World report on violence and health, s. 6.

benzer şekilde yakın partner şiddeti (İng. *intimate partner violence*) kavramının da kullanıldığı görülmektedir. Yakın partner şiddeti, yakın bir ilişki içindeki kişilere fiziksel, psikolojik veya cinsel zarara neden olan herhangi bir davranışı ifade etmektedir[12]. Uygulanan şiddet tipine göre sınıflandırma yapıldığında yakın partner şiddeti fiziksel şiddet, cinsel şiddet, duygusal şiddet, ekonomik şiddet ve siber şiddet[13] olarak alt başlıklara ayırılmaktadır[14]. Yakın partner şiddeti teşkil eden yöntemler fiziksel travma, psikolojik travma/stres ya da korku ve kontrol sonucunu doğuran yöntemleri içermektedir[15]. Flört şiddetinin, yakın partner şiddetinin bir alt tipi olduğu ve evli olmayan kişiler arasında görüldüğü belirtilmektedir[16]. Yakın partner şiddeti birçok ilişki türünü içine alan bir tanımlamadır. Dünya Sağlık Örgütü (DSÖ) 2013 yılında yayınladığı raporda, yakın partner şiddetinin resmi ilişkileri (evlilik) ve resmi olmayan ilişkileri (flört ilişkisi, evlilik dışı seksüel birliktelik) kapsayan bir terim olduğunu vurgulamıştır[17].

Dijital flört şiddeti (İng. *digital dating violence*), flört içindeki partnerler arasında yazışma (mesajlaşma), sosyal medya ve benzeri çevrimiçi ortamlar aracılığıyla gerçekleşen fiziksel, cinsel, ekonomik veya psikolojik/duygusal şiddet anlamına gelmektedir. Bu terim aynı zamanda teknolojinin kolaylaştırdığı şiddet olarak da bilinmektedir[18]. Dijital flört şiddeti, dijital flört istismarı (İng. *digital dating abuse*) olarak da anılmaktadır. Dijital flört şiddeti ya da istismarı, dijital teknolojileri kullanan flört partnerini kontrol etme, baskı yapma veya tehdit etme eylemlerini içeren davranışlar için kullanılan şemsiye bir kavramdır. Dijital teknolojiler sosyal medya, online oyunlar, multimedya, akıllı telefonlar ya da interneti içermektedir[19].

Dijital flört şiddetinin yaygın örnekleri, zorbalık etmek (sindirmek-*bully*), taciz etmek, gizlice takip etmek ya da tehdit etmek için mesajlaşmak ve sosyal ağları kötüye kullanmaktır.

12 WHO, World report on violence and health, s. 89.

13 Siber şiddet eylemleri iki temel bilişim teknolojisi aracıyla yapılmaktadır. Bunlardan ilki kişisel bilgisayar yoluyla saldırganın tekrarlı olarak anında mesaj, müstehcen taciz mesajı, iftira içeren mesaj göndermesi ya da internet sitesi hazırlayarak bunları yayınlamasıdır. İkincisi ise kurbana rahatsız edici mesajların cep telefonu yoluyla iletilmesidir. Ayrıca son dönemde kişiler arasında değişik video ve görsel materyallerin paylaşılması, sohbet edilmesi, sanal oyunların oynanabiliyor olması nedeni ile kişisel web siteleri, bloglar ve sosyal paylaşım siteleri daha popüler olmaktadır. Siber şiddet eylemi ciddi boyutlarda olabilecek, psikolojik, duygusal ve sosyal zararlar yaratmaktadır. Bkz. POLAT, s. 33-34.

14 POLAT, s. 17.

15 WORLD HEALTH ORGANIZATION (WHO), Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence, s. 8.

16 AVŞAR BALDAN, AKIŞ, s. 41.

17 AVŞAR BALDAN, AKIŞ, s. 41.

18 BRITISH COLUMBIA SOCIETY OF TRANSITION HOUSES, s. 1.

19 HINDUJA, PATCHIN, s. 2.

Genellikle bu davranışlar online olarak işlenen sözlü ya da duygusal istismara yol açan davranışlar olmaktadır.

Dijital flört şiddeti ile siber zorbalık (İng. *cyberbullying*) arasında teknolojik yöntemler içerme, büyük çoğunlukla bilenen akranlar arasında gerçekleştirilme, duygusal, psikolojik, fiziksel ve davranışsal sonuçları olma ve her ikisinin de kontrol ve baskı aracı olma gibi benzerlikler olduğu ifade edilmektedir. Bu nedenle dijital flört şiddetinin aslında siber zorbalığın bir şekli olduğu belirtilmektedir[20]. Ancak her iki kavram arasındaki farklılık bulunmaktadır. Siber zorbalık birbirini sevmeyen ve birlikte olmak istemeyen bireyler arasında meydana gelme eğilimindeyken, dijital flört şiddeti en azından belirli düzeyde birbirine ilgi duyan iki kişi arasında gerçekleşmektedir[21].

Dijital flört şiddeti, yüz yüze flört şiddeti ile bazı benzerlikler paylaşmaktadır. Çünkü her iki durum da hakaret, küçük düşürme, tehdit, izleme, duygusal manipülasyon ve partnerin sosyal ilişkilerini kontrol etme gibi farklı psikolojik saldırganlık türlerini içermektedir[22]. Bazı yazarlar dijital flört şiddeti yöntemlerini de içerir şekilde altı farklı şiddet içeren siber davranış tanımlamıştır. Bunlar psikolojik/duygusal şiddet, tehdit içeren yorumlar, utandırıcı/küçük düşürücü davranışlar, taciz veya sürekli temas kurma yoluyla denetim, cinsel taciz veya zorlama ve takip etme veya kontrol etme olarak belirtilmektedir[23].

Belirtilen özellikleri dikkate alındığında farklı sınıflandırmalara tabi tutulabilirse de ceza hukuku açısından önem arz eden dijital flört şiddeti teşkil eden yöntemler şu beş ana başlık altında toplanabilir:

1. *Sanal ortamda flört partnerini kontrol etme ve ona baskı kurmaya yönelik davranışlar* (Flört partnerine ait sanal ortamda kimlik doğrulamada kullanılan şifrelerin ele geçirilmesi (*yetkisiz erişim*) ya da hesapların ele geçirilmesi (=*account take over*), flört partnerinin çevrimiçi (*online*) faaliyetlerinin hukuka aykırı olarak takip edilmesi "siber takip", sanal

20 HINDUJA, PATCHIN, s. 3. Siber zorbalar bireysel veya grup halinde, bilgi ve iletişim teknolojileri aracılığıyla düşmanlık ve korkutma amaçlı iletileri (resim veya mesaj) kasıtlı, ısrarlı ve düzenli bir şekilde gönderirler. Bkz. DÜLGER, s. 123. Öğretide *Aksoy Retornaz* ise, siber zorbalığın siber tacizin bir türü olduğunu belirtmektedir. Yazara göre siber taciz ise zarar verme amacıyla yapılan, siber alanda tekrarlayan ve olumsuz özellikteki, asimetrik güç dengesinin söz konusu olduğu, bir bireye yönelmiş olan ve bir sosyal grup çerçevesinde gerçekleşen bir davranışın olması gerektiğini belirtmektedir. Ancak yazar eylemlerin her zaman belli bir sosyal grup içinde gerçekleşmeyebileceğini de vurgulamaktadır. Bkz. AKSOY RETORNAZ, s. 9-10, 21, 23.

21 HINDUJA, PATCHIN, s. 3.

22 RODRIGUEZ-DEARRIBA, NOCENTINI, MENESINI, SANCHEZ-JIMENEZ, s. 1.

23 RODRIGUEZ-DEARRIBA, NOCENTINI, MENESINI, SANCHEZ-JIMENEZ, s. 1.

ortamdaki yazışmalarının kontrol edilmesi ya da ifşası, sanal ortamda dijital kanallar üzerinden ısrarlı şekilde mesaj göndermek vb.)

2. *Sanal ortamda flört partnerinin itibarına zarar verici davranışlar* (Sanal ortamda flört partneri adına sahte profil ya da hesap oluşturma, hukuka aykırı olarak ele geçirilen hesaplardan hesabın gerçek sahibi adına utanç verici veya suç oluşturan paylaşımlarda bulunma, sanal ortamlarda flört partnerine ait kişisel verilerin hukuka aykırı olarak yayınlanması/yayılması "*doxing*" vb.)

3. *Sanal ortamda flört partnerinin finansal istismarına yol açacak davranışlar* (Sanal ortamda hukuka aykırı olarak ele geçirilen flört partnerine ait hesap üzerinden hesabın gerçek sahibinin arkadaş listesinde yer alan kişilere hileli mesajlar yollayarak maddi menfaat temin etme, sanal ortamda flört partnerinin finansal kimlik bilgilerini (internet bankacılığı ya da kredi kartı bilgileri vb.) kullanarak haksız yarar sağlama, flört partnerinin sanal ortamda içerik üretmek suretiyle kazanç sağladığı hesaplara erişimin engellenmesi suretiyle flört partnerine finansal zarar verme (örn. sosyal medyadan kazanç sağlayan hesabın gerçek sahibinin hukuka aykırı olarak hesaba erişimini engelleme veya hesabı kapatma vb.))

4. *Sanal ortamda flört partnerine ait cinsel içerikli görüntülerin rıza dışı paylaşılması, sahte olarak üretilmesi ya da bu görüntülerin paylaşılması tehdidi, flört partnerine rıza dışı cinsel içerikli yazı ya da görüntü yollama* (flört partnerine ait özel resimlerin ya da videoların sanal ortamda rıza dışı paylaşılması örn. "*intikam pornosu*" ya da bu görüntülerin paylaşılması tehdidi/şantajı "*sextortion*", flört partneri ile ilgili olarak sahte cinsel içerikli görüntü üretme ve paylaşma "*deepfake*", sanal ortamda flört partnerine rıza dışı cinsel içerikli yazı ya da görüntü yollama "*sexting*")

5. *Cinsel sömürü amacıyla sanal ortamda çocuklarla flört ilişkisi veya cinsel temas kurmaya yönelik davranışlar* (siber cinsel uşaklaştırma "*cyber sexual grooming*")

II. DİJİTAL FLÖRT ŞİDDETİ TEŞKİL EDEN YÖNTEMLERİN GÖRÜNÜM (ORTAYA ÇIKMA) BİÇİMLERİ

A. Sanal Ortamda Flört Partnerini Kontrol Etme ve Ona Baskı Kurmaya Yönelik Davranışlar

Sanal ortamda flört partnerini kontrol etme ve ona baskı kurmaya yönelik davranışlar çeşitli şekillerde gerçekleştirilebilmektedir. Bu davranışlar flört partnerine ait sanal ortamda kimlik doğrulamada kullanılan şifrelerin ele geçirilmesi, bilişim sistemine hukuka aykırı girme

(*yetkisiz erişim*) ya da hesapların ele geçirilmesi (=*account take over*) yöntemlerini içerebilmektedir. Bu yöntemleri içeren davranışların flört partneri tarafından gerçekleştirilmesi halinde TCK çerçevesinde değişik suç tiplerinin gündeme geleceği söylenebilir.

Sanal ortamda flört partnerini kontrol etme yöntemlerinin başında, flört partnerinin kullanmış olduğu online servisler ya da sosyal medya hesaplarında kullanmış olduğu şifrelerin ele geçirilmesi yer almaktadır. Bu şifrelerin ele geçirilmesiyle birlikte, sanal ortamlarda flört partnerinin kendi hesabında gerçekleştirmiş olduğu hareketler ya da başkaları ile yazışmaları kontrol altına alınabilmektedir. Bu durum genellikle flört partnerinin kullanmış olduğu bilgisayar ya da diğer bilişim sistemlerine zararlı yazılımlar (=*malware*) yüklenmesi suretiyle gerçekleştirilmektedir. Esasen zararlı yazılımlar virüsler, Truva atları (*trojan horse*), solucanlar (*worms*), casus yazılımlar (*spyware*), tuş ve ekran kaydediciler (*keylogger*, *screenlogger*) gibi çok çeşitlilik arz etse de, flört şiddeti açısından flört partnerinin şifrelerinin ele geçirilmesi açısından tuş ve ekran kaydedici programlar ön plana çıkmaktadır. Tuş kaydediciler (*keylogger*), kullanıcının klavye kullanarak girdiği bilgileri yakalayıp, tutan ve bunları saldırgana gönderen casus yazılımlardır[24]. Bu yazılım bilgisayar klavyesinden basılan tüm tuş hareketlerini göstermekte ve bunları log.txt dosyasına kaydetmektedir[25]. Ekran kaydedici programlar da tuş kaydedici programlar ile benzer şekilde çalışmaktadır.

Ekran kaydedici programlar, tuş kaydedici yazılımlara karşı koyabilmek amacıyla "sanal klavye (*virtual keyboard*)" kullanan kişilerin şifrelerinin ele geçirilmesi amacıyla oluşturulmuştur. Ekran kaydedici (*screenlogger*) yazılımlar tuş kaydedicilerden farklı olarak, kullanıcının klavye hareketlerini kaydetmek ve bunları saldırgana göndermek yerine, kullanıcının ekran üzerindeki fare ile tıklamış olduğu görüntülerin resmini çekerek bunları kaydeder ve bu verileri saldırgana gönderir. Bir başka deyişle bu yazılımların temel işlevi, bilgisayar ekranındaki görüntüleri milisaniye bazında kaydederek kullanıcıların fare ile girmiş olduğu hassas bilgileri saldırgana göndermektir[26].

Flört ilişkisi içinde söz konusu yazılımların partner tarafından kullanılması, genellikle sosyal medyaya girilen ve ortak kullanılan bir bilgisayara bu yazılımların yüklenmesi ya da casus yazılımın önceden yüklendiği cihazların partnere hediye edilmesi yoluyla söz konusu olmaktadır.

24 CANBERK, SAĞIROĞLU, s. 126.

25 YAZICIOĞLU, s. 71.

26 YAZICIOĞLU, s. 72.

Flört partnerinin kullanmış olduğu bilgisayar, bilgisayar özellikli cihazlar ya da bilişim sistemine yukarıda belirtilen yazılımların kullanılması suretiyle hukuka aykırı olarak girilmesi eyleminde, ceza sorumluluğunun nasıl belirleneceği önem arz etmektedir. 5237 sayılı TCK çerçevesinde bakıldığında bir bilişim sistemine hukuka aykırı olarak girilmesini içeren eylemler TCK' nın İkinci Kitap (*Özel Hükümler*) içerisinde "Topluma Karşı Suçlar" isimli üçüncü kısmının, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde m. 243' te düzenlenmiştir. Aynı şekilde bir bilişim sisteminin tamamına ya da bir bölümüne hukuka aykırı olarak erişim eylemlerinin suç olarak tanımlanması yükümlülüğünü de içeren 23.11.2001 tarihli Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesine Türkiye taraftır[27]. Sözleşmenin II. Bölümü, Kısım 1 (Maddî Ceza Hukuku), Başlık 1 (Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar) m. 2' de[28] "*Yasadışı Erişim*" suçuna yer verilmiştir.

Flört partnerinin TCK m. 243 anlamında bilişim sistemine hukuka aykırı olarak girmesinden söz edilebilmesi için, öncelikle ortada duygusal ilişki içindeki diğer tarafın "yetkili" olarak kullanmış olduğu bir "*bilişim sistemi*"nin bulunması gerekmektedir. "*Bilişim sistemi*" kavramı, TCK m. 243 ve 244'te madde metninde kullanılmakla birlikte, bu kavramın tanımına kanun metninde yer verilmemiştir. Ancak söz konusu bu kavram 243. maddenin gerekçesinde, "…*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir*…" şeklinde tanımlanmıştır. Bilişim sistemine ilişkin bir diğer tanım Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik m. 3/1-b'de yer almaktadır. Bu düzenlemeye göre bilişim sistemi, "*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi*" ifade etmektedir. Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi madde 1'de ise, "bilgisayar sistemi" teriminin tanımı yapılmıştır. Bu tanıma göre bilgisayar sistemi, "…*bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya*

27 Türkiye Cumhuriyeti bu sözleşmeyi 10 Kasım 2010 tarihinde Strazburg' da imzalamış, imzalanan sözleşme 6533 sayılı "*Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun*" ile onaylayarak uygun bulmuştur. R.G., T. 02.05.2014, S. 28988.

28 "*Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir*". Bkz. Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi Resmi Çevirisi, Türkiye Büyük Millet Meclisi, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, s. 14 (https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, Erişim Tarihi: 11.04.2022).

birbiriyle bağlantılı veya ilgili bir grup cihazı"[29] ifade etmektedir. Görüleceği üzere, bilişim sistemi kavramı, bilgisayar ile eş anlamlı bir kavram değildir. Bilişim sistemi "bilgisayar"a göre daha geniş bir kavramdır[30]. Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetini gerçekleştirmesine karşın "bilişim sistemi", hem verilerin işlenmesi hem de verilerin aktarılmasını kapsar. Ancak bilişim sistemi, bir bilgisayarın varlığını gerekli kılmaktadır[31].

Flört partneri tarafından kontrol ya da baskı amacıyla duygusal ilişki yaşanılan diğer kişinin kullanmış olduğu bilgisayar ya da diğer bilişim sistemi kapsamına giren cihazlara zararlı yazılım yüklenmesi suretiyle bilişim sistemine hukuka aykırı girilmesi eylemleri TCK m. 243/1'de yer alan "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme*" suçunu oluşturacaktır. Flört partneri bu kapsamda, kontrol ve baskı amacıyla ilişkinin diğer tarafında olan kişinin örn. mail adreslerine, sosyal medya hesaplarına hukuka aykırı olarak girebilir. TCK m. 243'teki suçun işlenebilmesi için kanun metninde failin herhangi bir saik ile hareket etmesi aranmadığından, bu suçun işlenebilmesi için failin genel kastı yani bilişim

---

29 Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi Resmi Çevirisi, Türkiye Büyük Millet Meclisi, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, s. 13 (https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, Erişim Tarihi: 11.04.2022).

30 Aynı yönde KOCA, s. 92; AKBULUT, s. 125. *Akbulut*' a göre bilişim sistemleri, bilginin toplanmasında, işlenmesinde, depolanmasında, ağlar aracılığıyla bir yerden bir yere iletilip kullanıcıların hizmetine sunulmasında kullanılan iletişim ve bilgisayarlar dâhil bütün teknolojileri kapsayan bir kavramdır. Bkz. AKBULUT, s. 124-125. *Ketizmen* ise, bilişim sistemini de kapsar şekilde "*enformasyon sistemi*" kavramından söz etmektedir. Yazara göre, "*enformasyon sistemi*", enformasyonun toplanmasını, adlandırılmasını, düzenlenmesini dönüştürülmesini, saklanmasını ve iletilmesini mümkün kılan sistemlerdir. Bkz. KETİZMEN, s. 11.

31 *Tezcan/Erdem/Önok* haklı olarak, akıllı telefonlar örneğinde olduğu gibi, verileri işleme ve aktarma özelliğine sahip olan cihazların da TCK m. 243' ün uygulama alanı içerisinde olduğunu belirtmektedir. Bkz. TEZCAN, ERDEM, ÖNOK, s. 1150. Yargıtay da akıllı telefonların TCK m. 243'te belirtilen "bilişim sistemi" kapsamında değerlendirilmesi gerektiğine vurgu yapmaktadır: "…*Somut olayda; katılanın cep telefonundan çekilmediği halde sanığın; "Sen Hacer'i değil, parayı seviyorsun..., kızım seninle görüşmez, bırak kızımın peşini, dolanma peşinde, seni uyarıyorum, Hacer'in seninle işi olmaz, bir daha bir araya gelmeniz ben hayattayken imkansız..." şeklindeki mesajı oluşturduğu ve telefonuna geldiği iddiasıyla boşanma dava dosyasında delil olarak ibraz ettiğinden bahisle açılan davada, sanık suçlamayı kabul etmemiş, bilirkişi raporunda ise iletişim detaylarında suça konu mesajlaşmaya dair kayıt bulunmadığı, ancak cep telefonlarına özel yazılımlar yüklenerek veya internet vasıtasıyla mesaj oluşturulabileceği belirtilerek mesaj çekilen ve mesaj alan cep telefonlarının incelenip, iletişim kayıtlarıyla karşılaştırılması gerektiğinin bildirilmesi karşısında, cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtları ile karşılaştırılmak suretiyle program yükleme veya internetten gönderme şeklinde suça konu mesaj gönderilip gönderilmediğinin araştırılması, sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken, cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,…Yasaya aykırı*…" Y. 8. CD., T. 18.03.2015, E. 2014/30037, K. 2015/14023 (Kazancı İçtihat Programı).

sistemine hukuka aykırı olarak girildiğinin bilinmesi ve bu yöndeki istemi yeterlidir. Yargıtay da kararlarını bu yönde vermektedir[32].

Şimdiye kadar yapılan açıklamalar flört partnerinin sadece bilişim sistemine hukuka aykırı bir şekilde girmesi eylemi için geçerlidir. Bu kapsamda flört partnerinin söz konusu eylemlerde bilişim sisteminin işleyişine ya da bilişim sisteminde var olan verilere[33] müdahalesi söz konusu değildir. Ancak flört partnerinin duygusal ilişki içinde olduğu diğer kişinin yetkili olduğu bilişim sistemine girmekle yetinmeyip, aynı zamanda bilişim sisteminde var olan verilere müdahale teşkil eden eylemleri gerçekleştirmesi durumunda ceza sorumluluğunun nasıl belirleneceği önem arz etmektedir. Flört partnerinin bilişim sistemine girmekte kullandığı şifreleri ele geçiren kişinin, sisteme girmeye gerçekte yetkili olan flört partnerinin sisteme erişimini engellemek amacıyla, kullanılan mail adresini (kullanıcı adını) ya da şifreyi değiştirmesi durumunda TCK m. 244/2'de yer alan "*Bilişim sistemindeki verileri erişilmez*

---

32 "*…sanığın savunmasında, katılanla evli olduğu dönemde mail adreslerinin şifrelerini bilmesi sebebiyle mail adreslerine girdiğini, mail adreslerinin şifrelerini kırmadığı ve değiştirmediğini beyan ettiği, sanığın kullandığı bilgisayar üzerinde yapılan inceleme sonrası düzenlenen bilirkişi raporlarında da, sanığın, katılana ait mail adreslerine girdiğinin tespit edildiği, ancak üçüncü kişilerle yazışma yaptığına dair kayıtlara rastlanmadığının bildirildiği dikkate alındığında, sanığın aksi kanıtlanamayan savunmaları ve tüm dosya kapsamı birlikte değerlendirildiğinde, sanığın, katılana ait iki farklı mail adreslerine izinsiz olarak girme eyleminin sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu değil, TCK'nın 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturduğu gözetilmeden suçun vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması hatalıdır*." Y. 12. CD., T. 22.06.2016, E. 2015/9555, K. 2016/10731 (Kazancı İçtihat Programı); "*…Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı elektronik posta adresine rızası dışında birçok kez girdiği olayda, sanığın, bu şekildeki eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu ve mahkemenin hükmün gerekçesinde de eylem bu şekilde kabul edildiği halde, sanık hakkında bilişim sistemine girme suçu yerine, TCK'nın 244. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan hüküm kurulmak suretiyle sanık hakkında fazla ceza tayini,…Kanuna aykırı olup…*" Y. 12. CD., T. 13.01.2016, E. 2015/15933, K. 2016/277 (Kazancı İçtihat Programı).

33 Veri, TCK m. 243' ün gerekçesinde bilişim sistemi içindeki soyut unsurlar şeklinde açıklanmaktadır. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 2/1-k' ya göre veri, "*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*" ifade etmektedir. *Dülger*' e göre veri, bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgidir. Bkz. DÜLGER, s. 80. *Koca*' ya göre veri, bilgilerin belirli bir formata dönüştürülmüş şeklidir. Bu bağlamda bir bilişim sisteminde saklanan yazı, resim, web sayfası tasarımı ve rakam gibi bilgiler veri olarak kabul edilmelidir. KOCA, s. 94. *Akbulut*' a göre, veri sisteme girilen, sistemde işlenen ve saklanan her türlü değeri ifade etmektedir. Yazara göre, programlar da veri kavramı içindedir. Bkz. AKBULUT, s. 188. Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi madde 1'de ise, "*bilgisayar verisi*" teriminin tanımı yapılmıştır. Bu tanıma göre bilgisayar verisi, "*bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini*" ifade eder. Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi Resmi Çevirisi, Türkiye Büyük Millet Meclisi, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, s. 13 (https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, Erişim Tarihi: 11.04.2022).

kılma" suçu gündeme gelmektedir[34]. Bu durum hesabın ele geçirilmesi olarak da ifade edilebilecektir (=*account take over*). TCK m. 244/2' de yer alan verilerin erişilmez kılınması, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup, burada veri içerik bakımından bütünlüğünü korumaktadır. Erişilmez kılmada ne verinin içeriği değiştirilmekte, ne yok edilmekte, ne de silinmektedir[35]. Verilere ulaşmak için mevcut olan bağın ortadan kaldırılması durumunda da verileri erişilmez kılma vardır[36]. Yargıtay da kişinin kullanmış olduğu sanal servisler, sosyal medya hesapları gibi kullanıcı adı, mail adresi ya da şifre gerektiren platformlarda, bu unsurların değiştirilmesi suretiyle yetkili kullanıcının sisteme erişiminin engellenmesini bu yönde değerlendirmiştir[37].

Flört partnerinin bilişim sistemine hukuka aykırı olarak girmesi ile ilgili olarak değerlendirilmesi gereken diğer bir husus da gerçek hesap sahibi kişinin 3. kişiler ile yapmış

---

34 Bu durumda tüketen norm-tüketilen norm ilişkisi gereği faile ayrıca TCK m. 243'ten dolayı ceza verilmeyeceği belirtilmektedir. Bkz. TEZCAN, ERDEM, ÖNOK, s. 1160. *Koca/Üzülmez*' e göre, bir bilişim sistemindeki verileri değiştirmek isteyen fail, bu suçun icra hareketlerini gerçekleştirirken sisteme de girmektedir ve dolayısıyla m. 243' ü de ihlal etmektedir. Bu durumda tek fiille birden fazla kanun hükmü ihlal edildiğinden farklı neviden fikri içtima (m. 44) ilişkisinin varlığı kabul edilmelidir. Bkz. KOCA, ÜZÜLMEZ, s. 874-875.

35 DÜLGER, s. 343; GÖKCAN, ARTUÇ, Cilt 5, s. 8154.

36 AKBULUT, s. 199.

37 "*Suça sürüklenen çocuğun mağdura ait kelebek_zulal@hotmail.com isimli facebook adresine izinsiz şekilde girdikten sonra mağdurun hesabında ekli kişilere hakaret içerikli mesajlar gönderdiği ve mağdurun facebook hesabı giriş şifresini değiştirdiği iddia edilmesi şeklinde eylemin TCK.nın 244/2. maddesinden tanımlanan suçu oluşturacağı ve suç tarihi itibariyle 15 yaşını doldurup 18 yaşını doldurmayan suça sürüklenen çocuğa yüklenen suçun Yasa maddesinde öngörülen cezasının türü ve üst sınırı itibariyle 5237 sayılı TCK.nın 66/1-e ve 66/2. maddelerinde belirlenen 5 yıl 4 aylık, asli zamanaşımı süresinin, zamanaşımını kesen son usulü işlem olan 04.03.2015 tarihli savunmasından temyiz inceleme tarihine kadar gerçekleştiği anlaşılmış ve Cumhuriyet Savcısının temyiz itirazları bu nedenle yerinde görülmekle hükmün 5320 sayılı Yasanın 8/1. maddesi gereğince uygulanması gereken 1412 sayılı CMUK.nın 321. maddesi uyarınca BOZULMASINA…*" Y. 8. CD., T. 22.02.2021, E. 2020/7839, K. 2021/2596; "*…sanık ...'ın, kız arkadaşı olan mağdur ... ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdura ait facebook hesabının önceden bildiği internet şifresini, onun bilgisi ve rızası dışında değiştirerek, hakkı bulunmadığı halde giriş yaptığı mağdurun facebook hesabında, beraber oldukları dönemde mağdurun bilgisi dahilinde kaydettiği cinsel içerikli görüntülerini yayımlayıp, mağdurun facebook hesabına erişimini engellemesi biçiminde sübut bulan eylemlerinin TCK'nın 244/2. maddesindeki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve aynı Kanun'un 134/2. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçlarını oluşturduğuna dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir*." Y. 12. CD., T. 24.05.2017, E. 2015/13308, K. 2017/4272 (Kazancı İçtihat Programı); "*Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK. nun 244/2. madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde yasal ve yeterli olmayan gerekçeyle beraatına hükmolunması,…Yasaya aykırı…*" Y. 8. CD., T. 23.06.2014, E. 2013/771, K. 2014/15833 (Kazancı İçtihat Programı); "*Sanığın oluşa uygun sübut bulan katılanın bilişim sistemine girişi sırasında kullandığı elektronik posta adresini değiştirip, katılanın sistemdeki kendisine ait kısma erişimini engellemek biçimindeki eyleminin, TCK'nın 244/2. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturacağı ve anılan madde gereğince sanığın cezalandırılmasına karar verildiği halde, kararın gerekçesinde, "... sanığın eyleminin TCK 244/1 maddesindeki suçu oluşturduğu kanaati ile sanığa eylemine uyan suçtan ceza verilmiş..." ibarelerine yer verilerek, gerekçeyle hükmün karıştırılması,…*" Y. 12. CD., T. 18.11.2013, E. 2013/2454, K. 2013/25865 (Kazancı İçtihat Programı).

olduğu yazışmaların içeriğinin öğrenilmesi ve bu içeriklerin ifşası eylemlerinde ceza sorumluluğunun nasıl belirleneceğidir. Bu durumda "*Haberleşmenin gizliliğini ihlal*" suçuna ilişkin, TCK m. 132/1 ve 2 düzenlemeleri gündeme gelecektir. Yargıtay' a göre haberleşmenin içeriğine ilişkin bilgilerin değil de, örneğin arama kayıtlarının öğrenilmesi durumunda "kişisel verileri hukuka aykırı olarak ele geçirme" suçu oluşacaktır[38].

Kanımızca flört partnerinin bilişim sistemine hukuka aykırı girmesi eylemi, salt duygusal ilişki yaşadığı kişinin 3. kişilerle yaptıkları mesajlaşma içeriklerini öğrenmek amacıyla gerçekleştirmesi durumunda, tek fiil ile TCK m. 243 (Bilişim sistemine hukuka aykırı girme) ve TCK m. 132/1 (Haberleşme gizliliğini ihlal) suçlarının oluşumuna sebebiyet verdiğinden farklı neviden fikri içtima hükmü (TCK m. 44) uygulanacaktır. Bu durumda failin sadece cezası ağır olan TCK m. 132/1'den dolayı sorumlu tutulması gerekmektedir. Bu görüşün ileri sürülmesinin nedeni TCK m. 243' te seçimlik hareketlerden birisinin "bilişim sisteminde kalmaya devam etme" olarak belirtilmiş olmasıdır. Belirtilen durumda fail sisteme hukuka aykırı olarak erişmekle yetinmemiş aynı zamanda sistemin gerçek kullanıcısının 3. kişilerle yapmış olduğu haberleşme niteliğindeki yazışmaları okuyarak (öğrenerek), haberleşme gizliliğini ihlal etmiştir. "Bilişim sisteminin bütününde veya bir kısmında hukuka aykırı olarak kalmaya devam etme" hareketi bakımından suç kesintisiz (mütemadi) suç özelliğinde olduğundan[39], işlenmeye devam eden fiil ile birden fazla farklı suçun oluşmasına sebebiyet verilmiştir (TCK m. 44)[40].

Mesaj (haberleşme) içeriklerinin ifşa edilmesi halinde ise farklı sonuca varmak gerekecektir. Zira ifşa etme eylemi ile bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme veya orada kalmaya devam etme fiilleri tek fiil olarak değerlendirilemez. Bu durumda gerçek içtima ilişkisi uygulanarak faile hem TCK m. 243/1' den hem de TCK m.

38 "*…dosya kapsamına ve ikrar içeren savunmaya göre; katılan ile bir dönem duygusal birliktelik yaşayan sanığın, katılanın hazırlandığı sırada katılanın rızası dışında cep telefonunu alarak arama kayıtlarına baktığı iddiasına konu olayda; TCK'nın 132/1. madde ve fıkrasındaki suçun konusunun, haberleşme içeriği olup söz konusu suçun, belirli kişiler arasındaki haberleşme içeriğinin hukuka aykırı biçimde öğrenilmesiyle oluşacağı, haberleşmenin gizliliğinden söz edebilmek için, kişiler arasında haberleşme olarak isimlendirilebilecek bir iletişimin olması, en az iki kişi arasında bir haberleşme vasıtası olması (telefon, mektup, e-posta vb.) ve tarafların bu haberleşmeyi gizlilik önlemlerini alarak yapması gerektiği, katılanın, kim ile, ne zaman, hangi sıklıkla, hangi süreyle görüştüğüne ilişkin bilgiler kişisel veri kapsamında olup haberleşme olarak nitelendirilemeyeceği anlaşıldığından, katılana ait kişisel veri kapsamındaki arama kayıtlarına katılanın rızası dışında bakarak içeriğine vakıf olan sanık hakkında TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği gözetilmeden, delillerin takdirinde ve hukuki nitelendirmede yanılgıya düşülerek yazılı şekilde haberleşmenin gizliliğini ihlal suçundan beraat hükmü kurulması,…*" Y. 12. CD., T. 10.04.2019, E. 2018/8152, K. 2019/4886.

39 Aynı yönde TEZCAN, ERDEM, ÖNOK, s. 1152; AKBULUT, s. 128; GÖKCAN, ARTUÇ, Cilt 5, s. 8131.

40 Aynı yönde KOCA, ÜZÜLMEZ, s. 860.

132/2' den ceza verilmesi gerekmektedir. Yargıtay benzer durumda failin TCK m. 132' de düzenlenen haberleşme gizliliğini ihlal suçundan sorumlu olduğuna karar vermiştir[41].

Bilişim sistemine hukuka aykırı olarak girme eylemi, tuş kaydedici ya da ekran kaydedici örneklerinde olduğu gibi bilgisayar programı[42] olarak kabul edilen zararlı bir yazılım aracılığıyla gerçekleştiriliyorsa, failin bu yazılımları imal etmesi, bir başkasından satın alması ya da kabul etmesi durumunda ayrıca TCK m. 245/A' da yer alan suçtan[43] (*Yasak cihaz veya programlar*) cezalandırılması gerekmektedir.

B. Sanal Ortamda Flört Partnerinin İtibarına Zarar Verici Davranışlar

Flört partnerinden intikam almak ve ona zarar vermek için yapılan itibara zarar verici davranış şekillerinden ilki kişinin adı soyadı, adresi, telefon numarası gibi kişisel bilgilerini rızasına aykırı olarak itibarına zarar verici internet sitelerinde (örn. eskort sitelerinde) paylaşmaktır.

Sanal ortamda başkasına ait kişisel bilgilerin o kişiyi aşağılamak (küçük düşürmek), tehdit etmek, sindirmek ya da cezalandırmak için rızaya aykırı şekilde 3. kişilerle bilinçli olarak paylaşılması, internette herkesin görebileceği hale getirilmesi öğretide "*doxing*" yöntemi olarak adlandırılmaktadır[44]. Bir tanıma göre "*doxing*", kötü niyetli bir tarafın, diğer tarafı kimlik olarak tanımlayan bilgilerini, bir başka deyişle hassas bilgilerini ifşa etmek suretiyle diğer tarafa zarar verdiği çevrimiçi istismardır[45]. Bu kapsamda "*doxing*", mağdura ait özel bilgilerin çevrimiçi olarak herkesin erişimine sunulması, bu bilgilerin herkesçe erişilebilir hale getirilmesini ifade etmektedir[46]. "*Doxing*" terim olarak, 90'lı yıllarda yasadışı hacker kültüründe bir intikam

41 "*…Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre, sanığın, katılanın doğrudan internet adresleri üzerinden gerçekleştirdiği ikili sohbet görüşmelerine ilişkin elektronik iletileri içerir yazılarını, birlikte kullandıkları bilgisayara yüklediği casus program aracılığıyla ele geçirip, onun bilgisi ve rızası dışında, aralarında görülmekte olan boşanma davası dosyasına 7.12.2009 tarihinde metin halinde sunduğu iddiasına konu olayda, 5237 TCK' nın 132. Maddesinde düzenlenen haberleşmenin gizliliğini ihlal suçu (şikâyete tabidir)…*" Y. 12. CD., T. 1.7.2013, E. 9548, K. 17899 (Aktaran DÜLGER, s. 541-542).

42 Casus yazılımlar da bilgisayar programı olarak kabul edilmektedir. Casus yazılım, hedefin bilgisayar faaliyetlerini gizlice izlemesi için özel olarak yapılmış program olarak tanımlanmaktadır. Bkz. ERALP, s. 36.

43 Söz konusu düzenleme 24.03.2016 tarihinde 6698 sayılı Kanunun 30. maddesi ile TCK' ya eklenmiştir. Bu düzenlemenin TCK madde metnine eklenmesinin nedeni, Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi m. 6' da yer alan "Cihazların kötüye kullanımı" yükümlülüklerin yerine getirilmesidir. Aynı yönde görüş için bkz. GÖKCAN, ARTUÇ, Cilt 5, s. 8216.

44 DOUGLAS, s. 199.

45 SNYDER, DOERFLER, KANICH, MCCOY, s. 432.

46 SNYDER, DOERFLER, KANICH, MCCOY, s. 432.

biçimi olan kişilerin kimliğini ortaya çıkarmayı ve ifşa etmeyi içeren "belgeleri düşürme" veya "dox düşürme" ifadelerinden gelmektedir[47].

Douglas' a göre[48], "*doxing*" yönteminin üç türü bulunmaktadır. Bunlar; 1. Anonimliği sona erdiren doxing (*Deanonymization*), 2. Hedef gösteren doxing (*Targeting*) ve 3. Gayrimeşrulaştıran doxing (*Delegitimization*) olarak belirtilebilir. Anonimliği sona erdiren doxing (*Deanonymization*) türünde, kişi ile ilgili herhangi bir kimlik bilgisi ifşa edilir ya da açığa vurulur. Böylece kişi anonimliğini kaybetmektedir. Örn. herhangi bir takma ad kullanan kişinin yasal kimliğinin ortaya çıkarılması[49]. Hedef gösteren doxing (*Targeting*) türünde kişiye ulaşılmasına izin veren fiziksel olarak bulunduğu yerin ifşa edilmesi ya da açığa vurulması söz konusudur. Böylece kişi gizliliğini, bulunduğu yerin belirsiz olması özelliğini kaybeder. Örn. Kişinin ev adresi bilgisinin herkes tarafından erişilebilir hale getirilmesi. Gayrimeşrulaştıran doxing (*Delegitimization*) türünde ise, kişinin kredibilitesine, itibarına ya da karakterine zarar verme amacıyla kişisel bilgilerin ifşası söz konusudur. Örn. Sözde ahlaksız faaliyetlerin kanıtının internette herkesin erişimine sunulması.

TCK çerçevesinde bakıldığında belirlenebilir bir kişiye ait olan ev adresi, cep telefonu numarası, meslek ve kariyer bilgileri vb. bilgiler kişisel veri olarak değerlendirilmektedir[50]. 108 sayılı Avrupa Konseyi Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi (Strazburg, 28.01.1981) m. 2' ye göre "*kişisel veriler*", "*kimliği belirli veya belirlenebilir bir gerçek kişi ("ilgili kişi") hakkındaki tüm bilgileri*" ifade etmektedir. Aynı tanım 6698 sayılı Kişisel Verilerin Korunması Kanunu m. 3/1-d' de de yer almaktadır. Bu çerçevede flört partneri tarafından söz konusu özellikteki kişisel verilerin hukuka aykırı olarak

47 DOUGLAS, s. 200; AKSOY RETORNAZ, s. 19.

48 DOUGLAS, s. 204.

49 Kanımızca bir kişinin tanımadığı kişiler tarafından kendisine herhangi bir iletişim aracı ile doğrudan ulaşılamaması da anonimlik içerisinde değerlendirilmelidir. Bu nedenle kişinin cep telefonu numarasının internette herkes tarafından erişilebilir hale getirilmesi de anonimliği sona erdiren doxing (*Deanonymization*) içerisinde değerlendirilmelidir.

50 Yargıtay Ceza Genel Kurulu da söz konusu bilgileri "kişisel veri" olarak değerlendirmektedir: "…*Kişinin; Türkiye Cumhuriyeti kimlik numarası, adı, soyadı, doğum tarihi, doğum yeri, nüfusa kayıtlı olunan yer (İl, İlçe, mahalle veya köy), anne adı, baba adı, medeni hal (Evli, bekâr, boşanmış), cilt ve aile sıra no, kan grubu evlenme tarihi, boşanma tarihi ve mahkeme kararı özet bilgileri, ad-soyad veya diğer kayıt düzeltmeleri, vatandaşlıktan çıkarılma bilgileri, evlatlık ilişkisi, adres, din, bitirilen okullar (ilk-orta-yüksek), hastalıklar, hastalıklar ile ilgili tahlil sonuçları (DNA bilgileri), mali durum (servet, alınan ücretler), ahlaki eğilimler, zaaflar, çevre ile ilişkiler, hatıra, anı ve günlükle ilgili defterindeki bilgiler, siyasi görüş (oy verdiği partiler, üye olduğu dernekler), alışkanlıkları, sevdiği kitaplar veya gazeteler, alışveriş eğilimleri, vergi numarası, e posta adresi, banka bilgileri, bilgisayarının IP numarası, emeklilik ve kurum sicil numarası, aldığı ödüller, parmak izi, avuç içi izleri, mektupları, yazılar, kitaplar. telefon numaraları, mesajları, fiziki kimliği (boy, kilo, engellilik durumu, ten rengi, göz rengi, saç rengi ve şekli, sesi, genel görünüm, ayak ve beden numarası) ve çok daha fazla bilgi kişisel veri kapsamında değerlendirilebilecektir*." YCGK., T. 10.06.2014, E. 2012/1514, K. 2014/312.

sanal ortamlarda paylaşılması durumunda TCK m. 136' da düzenlenen "*kişisel verilerin hukuka aykırı olarak yayılması*" suçunu oluşturacaktır. Yayma, bir kimsenin elindeki bir şeyi birden fazla kimsenin bilgisine sunması, birden fazla kimseye vermesi, ulaştırması olarak anlaşılmaktadır[51]. Bu kapsamda duygusal ilişki yaşaması sonucunda kurmuş olduğu yakınlık nedeniyle elde etmiş olduğu kişisel verileri sanal ortamda belirsiz sayıda kişilerle hukuka aykırı olarak paylaşan kişinin eylemi "*kişisel verilerin hukuka aykırı olarak yayılması*" suçunu oluşturacaktır. Yargıtay da kişiye ait resminin ve telefon bilgisinin[52] ya da kişinin oturduğu evin dış cepheden fotoğrafının[53] hukuka aykırı olarak sanal ortamda paylaşılmasının TCK m. 136 çerçevesinde suç olduğunu vurgulamıştır.

Sanal ortamda flört partnerinin itibarına zarar verici davranış şekillerinin bir diğeri de, flört partnerinin adı, fotoğrafı, mesleği ya da diğer kişisel verilerini kullanarak sosyal medya gibi platformlarda sahte profiller oluşturmak ve onun adına itibara zarar verici paylaşımlarda bulunmaktır. Bu durumda fail sahte hesaplar yoluyla flört partnerinin yakın çevresi ile iletişime

---

51 GÖKCAN, ARTUÇ, Cilt 3, s. 4933. Yargıtay Ceza Genel Kurulu "kişisel verileri yayma" hareketini şu şekilde açıklamaktadır: "*'Kişisel verileri yayma' seçimlik hareketi de çeşitli şekillerde gerçekleştirilebilecektir; internet üzerindeki bir web sitesinde kişisel verileri yayınlamak, birçok kişiye elektronik posta ile ya da telefondan kısa mesajla göndermek, yazılı ya da görsel medyada yayınlamak gibi... Türk Dil Kurumu Büyük Türkçe Sözlüğünde 'yaymak'; 'birçok kimseye duyurmak, çevreye dağılmasına sebep olmak' olarak açıklanmıştır*." YCGK., T. 10.06.2014, E. 2012/1514, K. 2014/312.

52 "*Dosya kapsamına göre mağdurun adını ve soyadını kullanarak açtığı sahte ... hesabında, mağdura ait telefon numarasını yayımlayan ve mağdur tarafından yazılmış algısı doğuracak cinsel içerikli paylaşımlarda bulunan hükümlü ...'ün eyleminin 5237 sayılı TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden,…*" Yargıtay 8. CD., E. 2020/4113, K. 2021/20067, T. 02.11.2021 ; "*Daha önce mağdurun bilgisi ve rızası dahilinde yayımlandığı anlaşılan mağdurun günlük kıyafetleriyle poz vermiş şekilde çektirdiği resimleri, mağdurun başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin görüntüler olarak kabul edilemeyeceğinden, mağdurun kişisel veri niteliğindeki resimlerini ve cep telefonu numarasını, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle yayımlayan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/2. madde ve fıkrasında düzenlenen görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi,…"* Y. 12. CD., T. 23.12.2020, E. 2020/2234, K. 2020/7459.

53 "*…sanığın, bir dönem duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu mağdurenin, adı, soyadı, mezun olduğu okul bilgileri, ikamet ettiği eve ait adres bilgileri ile birlikte, mağdurenin günlük hayatta çekilmiş fotoğrafı ile oturduğu eve ait dış cepheden çekilmiş fotoğrafları, mağdure tarafından arkadaşlıklarına son verilmesine tepki olarak ve mağdurenin bilgisi ve rızası dışında, "facebook" adlı sosyal paylaşım sitesinde yayınladığı olayla ilgili olarak, mağdurenin, aktif kullanımında olan, herkes tarafından bilinmeyen veya kolaylıkla ulaşılması ve bilinmesi mümkün olmayan, ancak sınırlı bir çevre ile paylaştığı adres bilgilerini, adı, soyadı, kendisine ve oturduğu eve ait fotoğrafı ile birlikte rızası dışında, başkalarının bilgisine sunan sanığın eyleminin TCK'nın 136/1. maddesindeki "Verileri hukuka aykırı olarak verme veya ele geçirme" suçunu oluşturacağı, mahkemece suç vasfında yanılgıya düşülerek, sanığın yazılı şekilde TCK'nın 134/2. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkumiyetine karar verilmiş ise de, sanığın sübut bulan eyleminin soruşturulmasının ve kovuşturulmasının şikayete bağlı olmadığı, bu yönüyle sanık hakkında kurulan hükmün, usul ve yasaya uygun olduğu anlaşılmakla, sanığın eyleminin şikayete tabi olduğu ve şikayet yokluğu nedeniyle davanın düşürülmesi gerektiği gerekçesiyle, bu suç yönünden kurulan hükme ilişkin kanun yararına bozma talebinin REDDİNE,…*." Y. 12. CD., T. 10.02.2014, E. 2013/30406, K. 2014/2980.

girerek ve etkileşimde bulunarak onu tanıyanlar gözünde küçük düşürmeye çalışmaktadır. Bu durum sahte hesaplar vasıtasıyla gerçekleştirilen paylaşımlar (örn. pornografik içeriklerin paylaşılması) ya da sanal ortamlarda gerçekleştirilen faaliyetler (örn. terör propagandası içeren bir gönderinin beğenilmesi) yoluyla gerçekleşebilmektedir.

Flört partnerinin adı soyadı, fotoğrafı ve diğer şahsına ait bilgilerin kullanılarak sahte sosyal medya hesabı açılması durumunda kanımızca TCK m. 136' da yer alan "*kişisel verilerin hukuka aykırı olarak yayılması*" suçu oluşacaktır. Kişinin fotoğrafını, ad-soyad bilgisini kendi isteğiyle sanal ortamda herkesin erişimine imkân verecek şekilde daha önce paylaşmış olması onun söz konusu bilgilerinin hukuka aykırı olarak sahte sosyal medya hesabı açılmasına rıza göstermiş olduğu şeklinde yorumlanamaz. Yargıtay bir kararında fail tarafından başkasına ait resim ve ad-soyad kullanılarak salt sosyal medya hesabı açılmasını suç olarak değerlendirmemiştir[54]. Yargıtay vermiş olduğu diğer kararlarında ise başkasına ait resmin sosyal medya hesabından paylaşılması şeklindeki eylemin TCK m. 136' da yer alan suçu oluşturduğu yönünde kararlar vermiştir[55]. Çalışmada daha önce belirtildiği üzere, Yargıtay 2021 tarihli bir kararında başkasının adını ve soyadını kullanarak sahte sosyal medya hesabı

54 "*… Katılanla aynı üniversitede çalışan sanık tarafından katılanın resmi ile ad ve soyadı kullanılarak facebook sayfası açmaktan ibaret eyleminde, sayfada yer alan bilgiler de nazara alındığında eylemin cezai yaptırımı gerektirecek içeriği bulundurmadığı gözetilmeksizin beraati yerine özel hayatın gizliliğini ihlalden mahkumiyetine karar verilmesi, …Bozmayı gerektirmekle*…" Y. 12. CD., T. 04.04.2012, E. 2011/12220, K. 2012/9228 (Kazancı İçtihat Programı).

55 "*Mağdurun kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle "Nesrin Hülya Ezgi" adlı facebook hesabı üzerinden başkalarının görgüsüne sunan sanık hakkında, genel kastla işlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı mahkumiyet kararı verilmesine dair yerel mahkemenin kabulünde bir isabetsizlik görülmemiştir*." Y. 12. CD., T. 12.04.2017, E. 2015/13248, K. 2017/3108; "*Sanık ... ile mağdur ... arasında erkek arkadaşı meselesinden kaynaklanan husumet bulunduğu dönemde, sanık ...'in, mağdura ait twitter hesabında mağdur tarafından paylaşılıp, kısa süre sonra kaldırılan ve mağdurun belden yukarısında giysisi olup, bacakları görüntülenen ayna karşısında poz vermiş şekilde çektirdiği fotoğrafını, 26.02.2013 tarihinde, "'Ahh gonlum kirik ayna' Ama yaa bu tweettr daha neler gorucek:))))) hahah" ibareleri ile birlikte kendi internet hesabında yayımlayarak, mağdurun yarı çıplak fotoğrafını rızasına aykırı şekilde başkalarının görgüsüne sunup, TCK'nın 134/2. madde ve fıkrasındaki görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçunu işlediğinin iddia edildiği olayda; Mağdura ait twitter hesabında mağdur tarafından paylaşılan mağdurun poz vermiş şekilde çektirdiği fotoğrafın, mağdurun başkalarının görmesini ve bilmesini istemeyeceği özel hayatına ilişkin görüntü olarak kabul edilemeyeceği; ancak, mağdurun özel yaşam alanına ilişkin olmayan kişisel veri niteliğindeki fotoğrafını, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle kendi internet hesabında yayımlayan sanık hakkında, iddianamede tarif edilen eyleminden dolayı TCK'nın 136/1. madde ve fıkrasının uygulanması ihtimaline binaen ek savunma hakkı tanındığı da nazara alınıp, verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması gerekirken, "...katılanın bahse konu fotoğrafının herkese açık şekilde sosyal paylaşım sitesindeki sayfasında paylaştığı, katılanın herhangi bir kısıtlama yapmaması nedeniyle bu şekilde paylaştığı fotoğrafının başkaları tarafından görülmesinden ve paylaşılmasından rahatsızlık duymadığı, bu nedenle bahse konu fotoğrafın alınmasının ve yorum yapılmasının yüklenen suçu oluşturmayacağı..." biçimindeki yasal ve yeterli olmayan gerekçelere dayalı olarak yazılı şekilde beraat hükmü kurulması,…*" Y. 12. CD., T. 06.10.2021, E. 2020/2426, K. 2021/6589.

açılması ve bu hesaptan kişiye ait telefon numarasının paylaşılmasını TCK m. 136/1 kapsamında değerlendirmiştir. Söz konusu 2021 tarihli kararda fail, başkası adına sahte bir sosyal medya hesabı açmış, adına sahte hesap açtığı kişinin ev telefonu numarasını ve cinsel içerikli mesajları bu hesaptan paylaşmıştır[56]. Kanımızca somut olayda TCK m. 136/1 (kişisel verilerin hukuka aykırı yayılması) yanında, cinsel içerikli mesajlar paylaşılması algısı yaratıldığından, bir başka deyişle somut olgu isnadında bulunulduğundan TCK m. 125' de yer alan hakaret suçu da oluşmaktadır. Nitekim Yargıtay benzer nitelikteki bir olay hakkında vermiş olduğu daha eski tarihli bir kararında fail hakkında hem TCK m. 136/1' de yer alan suçtan hem de TCK m. 125'te yer alan suçtan ceza verilmesi gerektiğine hükmetmiştir[57].

Flört partnerinin duygusal ilişki yaşamış olduğu kişi adına sahte oluşturmuş olduğu sosyal medya hesabından, terör örgütü propagandası teşkil edebilecek içerikler paylaşması durumunda olduğu gibi, intikam almak amacıyla suç teşkil eden paylaşım yapılması durumunda ceza sorumluluğunun belirlenmesi önem arz etmektedir. Kanımızca bu durumda failin kastına bakılarak ceza sorumluluğu belirlenmelidir. Failin ceza sorumluluğu içeriği paylaşmasındaki kastının suç teşkil eden diğer suçları işlemek mi (örn. terör örgütü propagandası yapmak mı),

---

56 "*Dosya kapsamına göre; somut olayda sanığın, müştekinin adına sosyal medya hesabı açarak cinsel içerikli mesajlar ve müştekiye ait ev telefonu numarasını paylaşması şeklinde gerçekleşen eylemin, 5237 sayılı Türk Ceza Kanunu'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan ceza tayin edilmesinde isabet görülmediğinden bahisle 5271 sayılı CMK.nın 309. maddesi uyarınca anılan kararın bozulması lüzumu Yüksek Adalet Bakanlığı Ceza İşleri Genel Müdürlüğünün 11.05.2020 gün ve 2020/4092 sayılı kanun yararına bozma istemine atfen Yargıtay Cumhuriyet Başsavcılığının 04.06.2020 gün ve KYB/2020-48938 sayılı ihbarnamesi ile dairemize tevdii kılınmakla incelendi…Dosya kapsamına göre mağdurun adını ve soyadını kullanarak açtığı sahte ... hesabında, mağdura ait telefon numarasını yayımlayan ve mağdur tarafından yazılmış algısı doğuracak cinsel içerikli paylaşımlarda bulunan hükümlü …'ün eyleminin 5237 sayılı TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden, suç vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması, Yasaya aykırı…*" Y. 8. CD., T. 02.11.2021, E. 2020/4113, K. 2021/20067.

57 "*Oluşa ve dosya kapsamına göre; sanık Hakan'ın, bir süre cinsel yakınlık boyutuna varacak düzeyde arkadaşlık ilişkisi içerisinde olduğu katılan Banu tarafından arkadaşlıklarına son verilmesine tepki olarak, facebook adlı sosyal paylaşım sitesinde üyelik işlemleri yapıp, katılan adına oluşturduğu sahte hesapta, katılanın rızası dahilinde çekilmiş resmini, profil fotoğrafı olarak kullandığı ve bu hesap üzerinden başka kişilere ait müstehcen görüntüleri yayınladığı iddia ve kabulüne konu olayda,...Katılanın başını ve yüzünü gösteren, günlük kıyafetleriyle poz vermiş şekilde çektirdiği resminin, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte olmaması karşısında, katılanın resmini, isim ve soy ismiyle birlikte hukuka aykırı olarak yayınlayan sanığın TCK'nın 136. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması; ayrıca, oluşturduğu sahte hesapta, katılan tarafından yayınlanıyor algısı doğuracak şekilde cinsel içerikli görüntülere yer vererek, katılanın, onur, şeref ve saygınlığını rencide eden sanığın TCK'nın 125. maddesinde düzenlenen hakaret suçundan mahkumiyetine karar verilmesi gerekirken, suç vasfında yanılgıya düşülerek, yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/2. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkumiyet hükmü kurulması,… Bozmayı gerektirmiş olup,…*" Y. 12. CD., T. 20.05.2014, E. 2013/22544, K. 2014/12128.

yoksa ilişki yaşamış olduğu kişinin şeref ve haysiyetine zarar vermek mi olduğu dış dünyaya yansıyan hareketlerinden tespit edilerek belirlenmelidir.

C. Sanal Ortamda Flört Partnerinin Finansal İstismarına Yol Açacak Davranışlar

Sanal ortamlarda flört partnerinin finansal istismarına yol açacak davranışlar çeşitli şekillerde gerçekleştirilebilmektedir. Bunlardan ilki, flört partnerine ait sosyal medya hesaplarını hukuka aykırı olarak ele geçiren ya da flört partneri adına sahte hesap oluşturan failin, flört partnerinin yakınları ile iletişimini sağlayan bu dijital kanallar vasıtasıyla (örn. sosyal medya hesabı üzerinden) hileli davranışlarda bulunarak maddi menfaat temin etmesidir. Bu durumda fail bilişim sistemlerini kullanmak suretiyle hileli davranışlar gerçekleştirmekte, bu hileli davranışlar sonucunda flört partnerinin yakınlarını aldatmakta ve onların zararına olarak kendisine maddi yarar sağlamaktadır. TCK çerçevesinde değerlendirildiğinde bilişim sistemlerinin kullanılması suretiyle hileli davranışlarla gerçek kişilerin aldatılması ve onların zararına olarak yarar sağlanması eylemleri TCK m. 158/1-f' de düzenlenen "*bilişim sistemlerinin kullanılması suretiyle dolandırıcılık*" suçunu oluşturacaktır[58]. Yargıtay' ın da haklı olarak belirttiği üzere, internet de çeşitli bilişim sistemlerinin birbirine bağlı olduğu ağlar bütünü olması sebebiyle münhasıran bir bilişim sistemi olarak kabul edilmektedir[59]. Bu nedenle internetteki içeriklerin aynı anda birçok kişiye ulaşmasındaki çabukluk ve sağladığı kolaylık nedenleriyle dolandırıcılık suçunda internetin araç olarak kullanılabileceğinin ve bu durumlarda TCK m. 158/1-f'de yer alan suçun oluşacağının söylenmesi gerekmektedir[60].

---

58 *Tezcan/Erdem/Önok'* a göre, kişilerin sosyal medyadaki hesaplarını *hack*' lemek suretiyle, listesinde kayıtlı bulunan kullanıcılarla o kişiymiş gibi temas kurarak onlardan maddi menfaat temin edilmesi durumunda TCK m. 158/1-f' de yer alan bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu oluşmaktadır. Bkz. TEZCAN, ERDEM, ÖNOK, s. 896. Öğretide *Dülger* de aynı yönde görüş bildirmektedir. Yazara göre, failin bir kişiye ait sosyal medya (MSN Messenger, Facebook vb.) ya da elektronik posta giriş şifrelerini ele geçirerek, şifresini ele geçirdiği kişilerin arkadaşlarına kendisini profil sahibi gibi tanıtıp para istemesi ya da belli bir telefona kontör yüklenmesini talep etmesi ve istemlerini kabul ettirmesi suretiyle yarar sağlaması durumunda TCK m. 158/1-f' de yer alan bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu oluşmaktadır. Bkz. DÜLGER, s. 529. Madde gerekçesine bakıldığında bu nitelikli hale yer verilmesinin nedeni, "*…Bilişim sistemlerinin…araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır*" şeklinde açıklanmıştır.

59 YCGK, T. 11.6.2013, E. 2013/15-239, K. 2013/432 (Kazancı içtihat programı).

60 "*Bilişim sistemlerinin aynı anda birçok kişiye ulaşmasındaki çabukluk ve sağladığı kolaylığa dayanarak 'www.sahibinden.com' adlı internet sitesinde emsallerine göre fiyatını ucuz göstererek araç satışı için ilan veren sanığın, bu ilanı görüp kendisini arayan şikayetçiden kapora adı altında 250 Lira alması şeklinde gerçekleşen olayda; sanığın bilişim sistemini araç olarak kullanmak suretiyle suçu işlediği anlaşılmakla, eylemin TCK'nun 158. maddesinin 1. fıkrasının (f) bendinde düzenlenmiş olan nitelikli dolandırıcılık suçunu oluşturduğu kabul edilmelidir*." YCGK, T. 11.6.2013, E. 2013/15-239, K. 2013/432 (Kazancı içtihat programı); "*Bilişim sistemlerinin aynı anda birçok kişiye ulaşmasındaki çabukluk ve sağladığı kolaylığa dayanarak internet sitesinden R…Şirketler Topluluğu isimli işyeri adına HP marka dizüstü bilgisayarların satışı için ilan veren sanıkların, Giresun'da ikamet eden ve ilanı görerek bildirdikleri telefon numarasını aradıktan sonra hesaplarına para aktaran şikayetçiye sözde alışverişe konu bilgisayarı göndermemeleri şeklinde gerçekleşen olayda; bilişim sisteminin araç olarak kullanılması suretiyle gerçekleştirilen eylemlerin*

Fail tarafından bilişim sistemlerinin kullanılması suretiyle gerçekleştirilen hileli davranışlar çeşitli şekillerde gerçekleştirilebilmektedir. Failin, internette hesabını ele geçirdiği flört partnerinin yakınları ile sanki hesabın gerçek sahibiymiş gibi mesajlaşma suretiyle borç isteme, hattına kontör yüklenmesini isteme vb. şekillerde maddi menfaat temin edebilecektir. Yargıtay da söz konusu eylemleri TCK m. 158/1-f' de düzenlenen bilişim sistemlerinin kullanılması suretiyle dolandırıcılık olarak değerlendirmektedir[61].

Flört partnerinin sanal ortamda finansal istismarına yol açacak davranış şekillerinden bir diğeri ise, flört partnerinin sanal ortamda finansal işlemler gerçekleştirebilmek için kullanmış olduğu finansal kimlik bilgilerini (örn. internet bankacılığı ya da kredi kartı bilgileri vb.) kullanarak haksız yarar sağlama davranışıdır. İnternet bankacılığında, müşterilere uygulanan kimlik doğrulama mekanizmasında genellikle birbirinden bağımsız en az iki bileşen bulunmaktadır. Bu iki bileşen müşterinin "bildiği", müşterinin "sahip olduğu" veya müşterinin "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmaktadır[62]. Kişi bu bilgileri kullanarak internet üzerinden bankacılık işlemleri yapabildiği alana, yani banka bilişim sistemine giriş yapmaktadır[63]. Hukuka aykırı bir şekilde ele geçirdiği internet bankacılığına giriş bilgilerini kullanarak, finansal işlemler yapılabilen banka bilişim sistemine giren fail,

TCK'nun 158. maddesinin 1. fıkrasının (f) bendi uyarınca nitelikli dolandırıcılık suçunu oluşturduğu kabul edilmelidir." YCGK., T. 02.04.2013, E. 2012/15-1293, K. 2013/111 **(**Kazancı içtihat programı).

61 "*…Sanığın, katılanın facebook hesabını kullandığı sırada, katılanın arkadaşı olan B.. H.. E..'in facebook hesabını bir şekilde ele geçirerek katılana mesaj gönderdiğini, internet banka hesabı kullanıp kullanmadığını sorduğu, kullandığını öğrenince de kendisinden iade etmek şartıyla 450,00 TL para istediği, katılanın Akbank internet bankacılığı aracılığıyla sanığın vermiş olduğu ... numaralı GSM hattına 450,00 TL para gönderdiğini, daha sonra B..H.. E..'in facebook sayfasının dondurulduğunu görünce şüphelendiği ve bankadan yaptığı araştırmada gönderdiği paranın 9 dakika sonra Antalya Kumluca'da bulunan ATM'den çekildiğini öğrendiği, B..'yi aradığında facebook hesabının çalındığını söylediği, ATM güvenlik kamera kayıtlarının temin edilerek emanete alındığı, havalenin yapıldığı ... numaralı GSM hattının sanık M..'un annesi F.. Ç.. adına kayıtlı olup sanığın gözaltına alındığı 25/12/2012 tarihinde yapılan üst aramasında suça konu hattın sanığın cep telefonuna takılı halde üzerinde bulunduğu olayda, nitelikli dolandırıcılık suçunun oluştuğu yönündeki kabulde bir isabetsizlik görülmemiştir…*" Y. 15. CD., T. 01.07.2013, E. 2013/14846, K. 2013/12178; "*…Şikayetçi ile eşinin internet ortamında MSN'de iletişim yaptıkları sırada müştekinin eşine ait elektronik posta adresine ait şifreyi bir şekilde elde edip şikayetçi ile sanki eşiymiş gibi görüşmeye devam ederek onu kandırıp cep telefonu için kontör isteyip şikayetçinin MSN'den gönderdiği kontörleri satmak suretiyle haksız yarar sağlayan sanığın eyleminin bilişim sisteminin araç olarak kullanılması suretiyle 5237 sayılı TCK'nın 158/1-f maddesindeki dolandırıcılık suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi,…*" Y. 11. CD., T. 18.03.2010, E. 2007/5408, K. 2010/3253.

62 BDDK tarafından çıkarılan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ' de (R.G. T. 14.09.2007, S. 26643) böyle bir yükümlülük mevcut iken, daha sonra bu tebliğ yürürlükten kaldırılmıştır (R.G. T. 15.03.2020, S. 31069).

63 Bankalar, mevduat sahiplerinin hesaplarına internet bankacılığı yolu ile yetkisiz kişilerce erişilememesi için değişik güvenlik uygulamaları kullanmaktadırlar. Bunlardan bazıları sanal klavye kullanımı, erişimde veya işlem yapılabilmesi için tek kullanımlık parolalar, erişim için IP kısıtlamalarıdır. Her ne kadar bu güvenlik uygulamaları kullanılsa da, banka müşterisinin internet bankacılığını kullandığı bilgisayarda konuşlanmış, key logger (tuş kaydedici) ve screen logger (ekran kaydedici) adlı kötü yazılımlar sayesinde gerek güvenli şifre gerekse sanal klavye uygulamaları, 3. kişilerin başkasına ait banka hesaplarına yetkisiz erişimini engelleyememektedir. Bkz. YILDIZ, Banka veya Kredi Kartları, s. 52, dp. 155.

gerçekte yetkili olan kişinin zararına olacak şekilde değişik finansal işlemler gerçekleştirebilecektir. Bunlar; kişinin banka hesaplarından kendisine ya da 3. kişi hesabına hukuka aykırı havale yapmak, kişinin hesabındaki ekonomik değerlerle kendine ait faturaları ödemek ya da kontör yüklemek, kişinin kredi kartı bilgilerini öğrenerek bu kredi kartları ile online alışveriş yapmak, kişi adına sahte sanal kart üretip bu kart ile alışveriş yapmak vb. şekillerde gerçekleşebilecektir. Failin söz konusu eylemlerden doğan ceza sorumluluğu TCK çerçevesinde farklı olabilecektir.

Hukuka aykırı olarak girmiş olduğu flört partnerinin internet bankacılığı bilişim sisteminde, flört partnerine ait banka hesaplarından kendisine ya da 3. kişi hesabına hukuka aykırı havale yapmak eylemi konusunda, her ne kadar öğretide haklı olarak hırsızlık suçunun konusu oluşturan "taşınabilir mal" unsurunun bulunmaması nedeniyle TCK m. 244/4'te yer alan suçun (bilişim sisteminde var olan verilere müdahale suretiyle yarar sağlama) oluştuğu belirtilmişse de[64], Yargıtay Ceza Genel Kurulu TCK m. 142/2-e' de düzenlenen "*bilişim sistemlerinin kullanılması suretiyle hırsızlık*" suçunun oluştuğuna karar vermiştir[65].

Yetkisiz olarak flört partnerinin internet bankacılığı hesabına girdikten sonra flört partnerinin kredi kartı bilgilerinin (kredi kartı numarası, kart güvenlik kodu vb.) kullanılması suretiyle finansal işlemler gerçekleştirilmesi de söz konusu olabilecektir. Bu durumda TCK m. 245/1'de yer alan gerçek banka veya kredi kartlarının kötüye kullanılması suçu oluşacaktır. Bu gibi durumlarda finansal işlemler gerçekleştirmek için sadece kredi kartı bilgilerinin kullanılması yeterli olduğundan, banka veya kredi kartlarının kötüye kullanılması suçunun işlenmesi yüz yüze gerçekleştirilen işlemlerden daha kolaydır[66]. Öğretide finansal işlemlerde kredi kartı fiziki olarak kullanılmadan, sadece kredi kartına ait bilgilerin kullanılması durumunda TCK m. 244/4'te yer alan suçun oluşacağı savunulmaktadır[67]. Kanımızca 5464 sayılı Kanunda kredi kartı tanımının fiziki varlığı bulunmayan kart numarasını da kapsar şekilde

64 YILDIZ, İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi, s. 129-150. Aynı yönde görüşte olan *Tezcan/Erdem/Önok*' a göre, failin mağdurun internet hesabına girerek oradan kendi hesabına aktarma yapması durumunda malın bulunduğu yerden alınması değil, yalnızca verinin yer değiştirmesi söz konusu olduğu için, TCK m. 244/4' ün uygulanması gerekmektedir. Bkz. TEZCAN, ERDEM, ÖNOK, s. 766. Öğretide *Akbulut*, internet üzerinden başka birinin hesabına girerek başkasının hesabına para aktarma eylemini, verileri değiştirmek suretiyle hırsızlık olarak TCK m. 142/2-e çerçevesinde değerlendirmektedir. Bkz. AKBULUT, s. 222.

65 "*Sanığın; firari diğer sanık ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, banka şubesindeki hesabından 10.750 YTL' yi, kendi adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylem, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunu oluşturur*." YCGK., T. 17.11.2009, E. 2009/11-193, K. 2009/268.

66 YILDIZ, Banka veya Kredi Kartları, s. 189.

67 TEZCAN, ERDEM, ÖNOK, s. 1183.

yapılması nedeniyle, bu durumda TCK m. 245/1'de yer alan suç oluşacaktır. Yargıtay da kararlarını bu yönde vermektedir[68].

Yetkisiz olarak flört partnerinin internet bankacılığı hesabına girdikten sonra fail tarafından sanal kart üretilmesi, üretilmiş olan sanal kart ile alışveriş yapılması durumunda ise failin ceza sorumluluğunun ne şekilde belirleneceği önem arz etmektedir. Yargıtay' a göre, ortada gerçek bir banka veya kredi kartı bulunmadığı için, başka deyişle sanal kart teşkil eden başkaca kredi kartı numaraları oluşturulduğundan TCK m. 245/1 değil, TCK m. 245/2 ve 3 gündeme gelecektir. Yargıtay söz konusu olayda TCK m. 245/2 (sahte kart üretme) ve TCK m. 245/3 (sahte kartları kullanarak yarar sağlama) suçlarının oluştuğuna hükmetmiştir[69].

Nihayet flört partnerinin finansal istismarına yol açan diğer bir yöntem de sosyal medya hesapları (örn. Youtube) vasıtasıyla gelir elde eden flört partnerinin hesabı ele geçirildikten sonra, şifrelerinin değiştirilmesi ya da hesaplarının kapatılmasıdır. Bu şekilde flört partnerinin bu hesaplara erişmesinin engellenmesi suretiyle ekonomik zarara uğratılması söz konusu olmaktadır. Bu durumda daha önce de belirtildiği üzere TCK m. 244/2'de yer alan "bilişim sisteminde var olan verilerin erişilmez kılınması" suçu oluşacaktır. Burada fail eylemi ile kendisi veya başkası adına herhangi bir haksız çıkar sağlamadığı için TCK m. 244/4'de yer alan suç oluşmayacaktır.

---

68 "*…sanıklar Ergin, Erkan ve Elveda'nın yakınana ait kredi kartı numarasını kullanarak bilişim sistemi üzerinden kontör satın alması ve aynı sistem üzerinden başkalarına kontörlerin satılması eylemleri nedeniyle dava açıldığının anlaşılması karşısında; fiilin 5237 sayılı TCK'nın 245/1 ve 43. maddelerinde öngörülen zincirleme suretiyle banka ve kredi kartlarının kötüye kullanılması suçunu oluşturacağı ve eylemde sahte oluşturulmuş veya üzerinde sahtecilik yapılmış bir banka veya kredi kartından söz edilemeyeceği gözetilmeden, aynı maddenin 3. fıkrası ile uygulama yapılması,…yasaya aykırı…olduğundan …hükmün…bozulmasına*" Y. 11. CD., T. 17.09.2008, E. 2008/12914, K. 2008/8887 (YKD., C. 35, S. 5, Mayıs 2009, s. 999) "*Oluşa, mağdurun beyanına, sanıkların savunmalarına ve tüm dosya kapsamına göre; suç tarihinde mağdur ...'in ... nolu telefonunu ... numaralı telefondan aranarak kemer, cüzdan ve kol saati kazandınız demek suretiyle arandığı, yaklaşık yarım saat sonra bu defa... nolu hattan arandığı, mağdurdan adres teyidi için aradıklarını beyan ederek kredi kartının ilk dört hanesinden sonrasını söylemesini istedikleri, mağdurunda inanarak söylenen numaraları verdiği, sanığın TEB'e ait kredi kartından üç defa da toplam 1.047 TL para çekimini gerçekleştirdiğinin anlaşıldığı olayda, sanıkların iştirak halinde hareket ederek mağdurun iradesini etkisiz kılarak kredi kartı bilgilerini ele geçirerek alışveriş yaptıkları, mağdurun aynı ürünleri 2 defa almasının hayatın olağan akışına uygun olmadığı, sanıkların, mağdura ait kredi kartındaki harcamalarının mağdurun rızası dışında yapıldığının anlaşılması karşısında; sanıkların eylemlerinin TCK.nun 245/1. maddesinde tanımlı banka veya kredi kartlarının kötüye kullanılması suçunu oluşturacağı gözetilmeden, yazılı şekilde hükümler kurulması,…*" Y. 8. CD., T. 14.01.2019, E. 2018/8157, K. 2019/457; Aynı yönde bkz. Y. 11. CD., T. 13.10.2010, E. 2010/7788, K. 2010/11083 (Kazancı içtihat programı); Y. 11. CD., T. 24.11.2009, E. 2007/849, K. 2009/14539 (Kazancı içtihat programı).

69 "*Sanığın; sahte sanal kredi kartı oluşturup, bu kredi kartıyla değişik zamanlarda harcama yapmaktan ibaret eylemlerinin TCK.nun 245/2. ve 245/3., 43. maddelerine uyan suçları oluşturduğu gözetilmeden, eylemler kül halinde değerlendirilerek yazılı biçimde hüküm kurulması aleyhe temyiz olmadığından bozma nedeni yapılmamıştır.*" Y. 8. CD., T. 29.09.2014, E. 2014/3533, K. 2014/21275 (YILDIZ, Banka veya Kredi Kartları, s. 266, dp. 65)

D. Sanal Ortamda Flört Partnerine Ait Cinsel İçerikli Görüntülerin Rıza Dışı Paylaşılması, Sahte Olarak Üretilmesi ya da Bu Görüntülerin Paylaşılması Tehdidi, Flört Partnerine Rıza Dışı Cinsel İçerikli Yazı ya da Görüntü Yollama

1. Cinsel İçerikli Şantaj (*Sextortion*) ve İntikam Pornosu (*Revenge Porn*)

Cinsel içerikli şantaj (*sextortion*) kavramının tanımının ne olduğu konusunda bir uzlaşının olmadığı söylenebilir[70]. Cinsel içerikli şantajın tanımıyla ilgili benimsenin iki ayrı yaklaşım bulunmaktadır. Bunlar: (1) cinsel içerikli şantaj, bir failin mağdurdan zorla bir şey elde etmek için kurbanın cinsellik içeren özel görüntülerini paylaşmakla tehdit etmesidir, 2) cinsel içerikli şantaj, özel cinsel görüntüleri paylaşma ya da başka bir biçimde zarar verme tehdidiyle bir mağdurun bir faile cinsel içerikli materyallerini göndermeye zorlanmasıdır[71]. Bu iki yaklaşımı da kapsayan en yalın tanımıyla cinsel içerikli şantaj (*sextortion*), cinsel içerikli görseller kullanılarak yapılan şantajdır[72].

Cinsel içerikli şantaj, faillerin genellikle maruz kalan kişinin internet ortamındaki yaşamında "arkadaş olarak var olan" kimseler arasında olması nedeniyle günümüzde çoğunlukla güncel kalmayı başarmaktadır. Bu durum faillerin kırılgan konumdaki bu kişilere ve arkadaş çevresine saldırmasını kolaylaştırmaktadır. Mağdur, failin daha fazla görüntü yollaması ya da belirli bir isteği yerine getirmesi (örn. ekonomik menfaat, cinsel ilişki vs.) yönündeki talebi karşılamayı reddettiğinde, görüntülerinin ailesine veya arkadaşlarına gönderileceği yönünde tehdit edilmektedir. Bu durum yalnızca çocuklar ve gençler açısından değil, yetişkinler açısından da geçerli olabilmektedir[73].

"Cinsel içerikli şantaj (*sextortion*)" ve "intikam pornosu (*revenge porn*)[74]" kavramları teorik olarak bazen birbiri ile karıştırılabilmektedir. Söz konusu bu kavramlar genellikle birbiriyle bağlantılı olmakla birlikte eş anlamlı değildir. Daha az kullanılan ve daha doğru bir şekilde "rıza dışı pornografi[75]" olarak adlandırılan intikam pornosu, bir kurbanın pornografik

---

70 CARLTON, s. 180.

71 CARLTON, s. 180.

72 WEBB, s. 82.

73 WEBB, s. 83.

74 İntikam pornosu (*revenge porn*), "*bir veya daha fazla kişinin cinsel içerikli fotoğraf, video veya resminin, başka bir ifadeyle görüntüsünün ilgililerin rızası olmadan çevrimiçi paylaşılmasını ifade etmek için kullanılan bir terimdir*". "Revenge porn", "*çoğunlukla bir ilişki esnasında fotoğraf veya video elde eden eski bir eş ya da sevgilinin mağduru aşağılamak veya korkutmak amacıyla cinsel içerikli materyali çevrimiçi iletmesi olarak da tanımlanabilir. Bu davranışı gerçekleştiren kişi, her zaman eski eş ya da sevgili de olmayabilir*" Bkz. AKSOY RETORNAZ, s. 27, 28.

75 Rıza dışı pornografi, kişilerin kendilerini kimin çıplak göreceğine karar vermesini engelleyerek cinsel mahremiyeti ihlal eder. Bu açıdan kişinin kendi bedeni üzerindeki "denetiminin" yok edilmesi anlamına

materyallerinin rızası dışında paylaşılarak yayılmasıdır[76]. Bu iki kavram arasında birbirine karıştırılmalarına neden olan bağlantı, şantajın mağdur kendisinden talep edilen bir şeye razı olmadığında mağdura karşı intikam pornosu suçu işlenmesi tehdidinin söz konusu olmasıdır[77]. Hem cinsel içerikli şantaj hem de intikam pornosu cinsellikle bağlantılı internet suçlarıdır. Ancak intikam pornosunun aksine, susmaya (sessiz kalmaya) zorlama, cinsel içerikli şantajın başarıya ulaşmasında çok önemli bir rol oynamaktadır. Şantaj faili, mağdurun özel materyallerini elinde bulunduruyorsa, bunu hemen yayınlamayacaktır; çünkü burada amaç genellikle farklı cinsel içerikli materyal veya ekonomik kazanç elde etmektir. Mağdurun sessizliği ve utanç verici bir konuma düşmekten korkması failin bu amaca ulaşması için çok önemlidir. Buna karşılık, intikam pornosunda suçlunun amacı mağdurun cinsel materyalini yayınlamaktır ve mağdurun sessizliği bu amaca ulaşmada önemli bir rol oynamaz[78].

Cinsel şantaja konu olan mağdurun cinsel içerikli görüntüleri fail tarafından çeşitli yollarla ele geçirilmiş ya da elde bulunduruluyor olabilir. Bu görüntüler duygusal ilişki yaşanılan kişinin rızası ile kaydedilmiş ya da faile istenilerek yollanmış olabileceği gibi, mağdur aldatılarak ele geçirilmiş, gizli olarak rıza dışı kaydedilmiş ya da mağdura ait bilişim sistemlerine müdahale suretiyle yani bilişim suçları yoluyla ele geçirilmiş olabilecektir. TCK' ya göre, görüntülerin ele geçirilme şekline göre farklı suç tiplerinin gündeme geleceği söylenmelidir.

Cinsel içerikli görüntülerin kullanılması suretiyle gerçekleştirilen şantaj suçu ile ilgili olarak üç aşamanın söz konusu olduğu söylenebilir. Bunlar; 1. Cinsel içerikli görüntünün ele geçirilmesi, 2. Cinsel içerikli görüntünün mağdur tarafından istenilen şeyin yapılmaması durumunda 3. kişilerle paylaşılması tehdidi (şantaj) ve 3. İstenilenin yapılmaması durumunda cinsel içerikli görüntülerin 3. kişilerle paylaşılması aşamalarıdır. Bu aşamalar ile ilgili olarak ceza sorumluluğu açısından ilk belirtilmesi gereken husus, görüntülerin ele geçirilmesi fiili ile bu görüntülerin yayılması tehdidi (şantaj) ya da bu görüntülerin mağdurun istenilen şeyi yapmaması durumunda gerçekten de paylaşılması (yayılması) fiillerinin farklı fiiller olduğu hususudur. Bu durumda fail söz konusu oluşabilecek suçlar nedeniyle gerçek içtima gereği ayrı

gelmektedir. Herkesin görmesi amacıyla yayınlanan çıplak fotoğraflar, insanları cinsel organlarına ve göğüslerine indirgemektedir. Bkz. CITRON, s. 1918.

76 CARLTON, s. 181. *Aksoy Retornaz*' a göre, cinsel içerikli görüntülerin ifşası, yayılması veya erişilebilir kılınması eylemleri özel hayata ve hayatın gizli alanına karşı suçlar arasında özel suç tipi olarak düzenlenmesi gerekmektedir. Bu nedenle yazar "*revenge porn*" yerine "cinsel içerikli görüntülerin rızaya aykırı olarak ifşası" ifadesinin kullanılması gerektiğini belirtmektedir. Bkz. AKSOY RETORNAZ, s. 31, 142.

77 CARLTON, s. 181.

78 CARLTON, s. 182.

ayrı cezalandırılacaktır. Cinsel içerikli görüntüler flört ilişkisi içinde flört partnerinin rızasıyla ya da rıza dışı/gizli kaydedilme yoluyla[79] failin elinde bulunuyor olabilecektir. Cinsel içerikli görüntülerin kaydedilmesine yönelik rıza her ne kadar bu görüntülerin üretilmesi ya da bulundurulmasına yönelik olsa da bu görüntülerin 3. kişilerle paylaşılmasını içermediğinden söz konusu görüntülerin paylaşılması durumunda failin fiilini hukuka uygun hale getirmeyecektir[80]. Bu nedenle flört partnerinin rızasına dayalı da olsa edinilmiş ya da üretilmiş olan cinsel içerikli görüntülerin 3. kişilerle paylaşılması durumunda özel hayatın gizliliğini ihlal suçu (TCK m. 134/2) oluşacaktır[81]. Zira yetişkin bir kişinin cinsel içerikli görüntülerinin kaydedilmesine göstermiş olduğu rıza, sadece bu görüntülerin üretilmesi ve bulundurulması fiillerinin hukuka aykırılığını ortadan kaldırır. Yargıtay haklı olarak cinsel içerikli görüntülerin henüz 3. kişilerle paylaşım olmaksızın bulundurulmasında, görüntünün ilgilinin rızası ile kaydedilip kaydedilmediğinin araştırılması gerekliliğini vurgulamaktadır[82]. Yargıtay' a göre bu araştırma yapılırken çekimin başlangıcı, devamı ve sona ermesi sırasında çekim cihazının bulunduğu yer ile mağdur arasındaki mesafe, mağdurun çalışır vaziyetteki çekim cihazının varlığından haberdar olup olmadığı, çekimi fark ettiği izlenimini uyandıracak bir davranışının olup olmadığı, çekim yapan cihaza ısrarla bakıp bakmadığı ve odaklanıp odaklanmadığı gibi hususlar bilirkişi aracılığıyla incelenecektir[83].

---

79 Kişiler arasında cinsel ilişki rızaya dayanıyor olsa dahi, bu cinsel birlikteliğin gizli olarak rıza dışı kayıt altına alınması durumunda özel hayatın gizliliğini ihlal suçu oluşacaktır. Nitekim Yargıtay da bu yönde karar vermektedir: "Sanık ...'un, mağdur ...'la fiili livata şeklinde karşılıklı rızaya dayanan cinsel ilişki anlarını, mağdurun bilgisi dışında, gizli kamera ile kaydetmesi biçiminde sübut bulan eyleminin, TCK'nın 134/1. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçunu oluşturduğuna dair yerel mahkemenin kabulünde dosya kapsamına göre bir isabetsizlik görülmemiştir." Y. 12. CD., T. 25.04.2018, E. 2017/10639, K. 2018/4829.

80 "*Sanık ...'in, mağdur ...'le cinsel ilişkiye girdiği esnada onun bilgisi dahilinde çektiği çıplak fotoğrafları, mağdurun rızası olmaksızın başkalarına göndererek, görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçunu işlediğinin iddia edildiği olayda*…" Y. 12. CD., T. 13.01.2021, E. 2019/5035, K. 2021/215.

81 "*Sanığın, katılan ile arkadaşlıklarını sürdürdükleri sırada çektirdikleri özel fotoğrafları facebook adlı internet sitesinde yayınlaması şeklinde gerçekleşen ve mahkemece de bu şekilde kabul edilen olayda TCK'nın 134/2. madde ve fıkrasındaki görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan dolayı mahkumiyet hükmü kurulması gerektiği gözetilmeden, sanık hakkında TCK'nın 134/1. maddesi uyarınca hüküm kurulmuş ise de aleyhe temyiz olmadığından bozma nedeni yapılamayacağı,…*" Y. 4. CD., T. 23.11.2021, E. 2019/5408, K. 2021/27352.

82 "*Sanığın, katılan ile arkadaşlık yaptığı dönemde yaşadıkları cinsel birliktelik anını kayda alarak katılanın özel hayatının gizliliğini ihlal ettiği iddia edilen olayda; adli emanette kayıtlı flash bellek ve telefondaki cinsel içerikli görüntülerin tamamı, bilişim uzmanı olan üç kişilik bilirkişi heyetine inceletilip, görüntülerin katılanın bilgisi dahilinde kaydedilip kaydedilmediği hususlarını denetime olanak verecek şekilde açıklayan rapor düzenlettirilmesi, sonucuna göre de sanığın hukuki durumunun belirlenmesi gerektiği gözetilmeden eksik incelemeyle mahkumiyet kararı verilmesi,…Kanuna aykırı,…Hükmün Bozulmasına,…*" Y. 4. CD., T. 09.11.2021, E. 2019/2286, K. 2021/26683.

83 "*Soruşturma evresinde Kayseri Emniyet Müdürlüğü Siber Suçlarla Mücadele Şube Müdürlüğü Adli Bilişim Büro Amirliğinin hazırladığı 14.01.2014 tarihli inceleme raporunda, sanığa ait cep telefonunda mağdurla ilgili 25 adet resim tespit edildiğinin belirtilmesi ve söz konusu görüntülerin aktarıldığı CD'nin adli emanete*

Cinsel içerikli görüntülerin ele geçirilmesi yöntemlerinden bir diğeri ise, mağdurun bilgisayarına fail tarafından zararlı bir yazılım yollanması suretiyle görüntülerin ele geçirilmesidir. Bu görüntüler mağdurun bilgisayarında halihazırda kayıtlı olan görüntüler olabileceği gibi mağdurun bilgisayarındaki kamera sisteminin zararlı yazılım tarafından aktif hale getirmesi suretiyle kaydedilmiş görüntüler de olabilecektir. Söz konusu durumda tek fiil ile hem özel hayatın gizliliğini ihlal suçu hem de bilişim sisteminde var olan verilerin başka yere gönderilmesi (TCK m. 244/2) ya da bilişim sisteminin işleyişinin bozulması (TCK m. 244/1) suçu oluşacaktır. Fail farklı neviden fikri içtima ilişkisi nedeniyle bu suçlardan en ağır olanından cezalandırılacaktır (TCK m. 44).

Yine uygulamada sıklıkla rastlanılan ve Yargıtay kararlarına konu olan durumlardan birisi mağdurun özel görüntülerinin gizli kamera[84] kullanmak suretiyle giyinme odasında[85], tuvalette[86], etek altına tutmak suretiyle[87] ya da kişi aldatılarak[88] alınmasıdır. Bu gibi durumlarda

alınmış olması karşısında, adli emanete alınan CD'de yer alan mağdura ait görüntüler bir bilirkişiye inceletilip, çekimin başlangıcı, devamı ve sona ermesi sırasında çekim cihazının bulunduğu yer ile mağdur arasındaki mesafeye, tarafların konumuna ve tespit edilebilen durumlarına göre, mağdurun çalışır vaziyetteki çekim cihazının varlığından haberdar olup olmadığı, çekimi fark ettiği izlenimini uyandıracak bir davranışının bulunup bulunmadığı, çekim yapan cihaza ısrarla bakıp bakmadığı ve odaklanıp odaklanmadığı, özetle görüntülerinin bilgisi dahilinde kaydedilip kaydedilmediği ile hangi tarihlerde kaydedildiği hususlarını denetime olanak verecek şekilde açıklayan rapor düzenlettirilmesi, toplanan tüm deliller birlikte değerlendirilerek, iddia ve savunmanın doğruluk derecesi açıklığa kavuşturulduktan sonra sanığın hukuki durumunun takdir ve tayini gerekirken, çekimin mağdurun rızasıyla yapıldığına dair savunmanın aksine delil elde edilemediğinden bahisle eksik incelemeye dayalı olarak beraat kararı verilmesi,…" Y. 12. CD., T. 02.12.2020, E. 2020/941, K. 2020/6656; aynı yönde Y. 4. CD., T. 09.11.2021, E. 2019/2286, K. 2021/26683.

84 Y. 12. CD., T. 10.03.2021, E. 2019/4532, K. 2021/2455.

85 Y. 12. CD., T. 12.12.2018, E. 2018/4715, K. 2018/12017.

86 İşyeri tuvaletine gizli kamera yerleştirilmesi için bkz. Y. 12. CD., T. 27.03.2019, E. 2019/1025, K. 2019/4186; Y. 12. CD., T. 04.11.2020, E. 2019/3021, K. 2020/5690; Y. 12. CD., T. 16.12.2020, E. 2019/10514, K. 2020/7154; Y. 12. CD., T. 16.05.2018, E. 2017/12179, K. 2018/5551.

87 "*…sanığın, yaşı küçük mağdurların haberleri olmadan etek altı görüntülerini cep telefonuna kaydetmesi şeklindeki eylemlerinin, mağduru sayısınca TCK'nın 226/3. maddesinin ilk cümlesindeki müstehcen görüntülerin üretilmesinde çocukların kullanılması suçunu oluşturduğu gözetilmeden, suç vasfında yanılgıya düşerek TCK'nın 134. maddesindeki özel hayatın gizliliğini ihlâl suçundan açılan davada, şikayet yokluğu gerekçesiyle düşme kararı verilmesi,…*" Y. 4. CD., T. 22.12.2021, E. 2021/31435, K. 2021/29897.

88 Gerçekleşmiş bir olayda mağdura bir öğrenci dizisinde rol alacağını ve yönetmenin fiziğini görmesi gerektiği yalanı söylenmiş ve mahrem görüntülerinin kaydı sağlanmıştır: "*sanık ...'ın, işlettiği markete müşteri olarak gelmesinden dolayı tanıdığı 14 yaşındaki mağdur ...'a facebook sosyal paylaşım sitesi üzerinden "..." ismi ile arkadaşlık isteği göndererek, kendisini dizi yapımcısı olarak tanıtıp, kandırdığı mağduru, bir öğrenci dizisinde rol alacağına ve bu amaçla bir kadın yönetmenle görüşeceğine inandırdıktan bir süre sonra, kadın ismiyle açtığı facebook hesabından gönderdiği mesajlarla kadın yönetmen algısı oluşturup, MSN'de kamerasını açmaya ikna ettiği mağdura, dizide oynayabilmesi için fiziğini görmesi gerektiğini ifade etmesinin ve bu yöndeki ısrarının ardından, bir kadınla iletişim kurduğunu zanneden mağdurun üst kısmındaki tüm giysileri ile altındaki pantolonunu çıkarmasını ve yalnızca alt iç çamaşırı kalacak şekilde soyunmasını sağlayıp, aynı zamanda mağdura ait yarı çıplak görüntüyü cep telefonuna kaydettiği olayda; Ayrıntıları Yargıtay Ceza Genel Kurulunun 24.03.2015 tarihli, 2014/14-603-2015/66 sayılı kararında da vurgulandığı üzere; 14 yaşındaki mağdurun fiziksel mahremiyetine ilişkin yarı çıplak görüntüsünü cep telefonu ile kaydeden sanığın cinsel arzu ve isteklerini tatmin maksadına yönelik eylemlerinde, TCK'nın 134/1. madde ve fıkrasında tanımlanan görüntü veya seslerin kayda alınması suretiyle özel hayatın gizliliğini*

da henüz fail tarafından yetişkin bir kişiye ait bu görüntülerin paylaşılması tehdidi (şantaj) gerçekleştirilmemişse, sadece özel hayatın gizliliğini ihlal suçu oluşacaktır. Etek altı görüntülerinin ya da giyinme kabini veya tuvaletlerde kişilerin mahrem yerlerinin gizlice kayıt edilmesi fiilinin çocuklara karşı gerçekleşmesi durumunda ise özel hayatın gizliliğini ihlal suçu değil, müstehcenlik (TCK m. 226/3) suçu oluşacaktır[89].

Cinsel içerikli görüntülerin fail tarafından ele geçirilmesi ya da elde bulundurulması sonrasında, bu görüntülerin istenilen şeyin yapılmaması durumunda fail tarafından paylaşılması tehdidi şantaj suçunu oluşturacaktır. Burada fail mağdurun şeref ve saygınlığına zarar verecek görüntüleri açıklamak tehdidi ile mağduru kendisine veya bir başkasına herhangi bir çıkar sağlamaya zorlamaktadır (TCK m. 107/2). Yargıtay kararlarına yansıyan olaylarda da görüldüğü üzere bu çıkar ekonomik olabileceği gibi manevi nitelikte de olabilir. Örneğin,

ihlal ve aynı Kanunun 105/1. madde ve fıkrasında düzenlenen cinsel taciz suçlarının yanı sıra toplumun sahip olduğu ortak ar ve haya duygularını, yerleşik edep kurallarını incitici ve genel ahlâka aykırı nitelikteki müstehcen görüntüyü içeren ürünün üretiminde 18 yaşından küçük mağdur çocuğun yer almasından dolayı TCK'nın 226/3-1. madde, fıkra ve cümlesinde tanımlanan müstehcenlik suçunun da oluştuğu gözetilerek, sanığın, TCK'nın 44. maddesi gereğince daha ağır cezayı gerektiren müstehcenlik suçundan cezalandırılması gerekirken, mağdurun yaşı ve kaydedilen görüntünün özellikleri dikkate alınmaksızın, eylem sadece görüntü veya seslerin kayda alınması suretiyle özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilerek, sanığın TCK'nın 134/1. madde ve fıkrası gereğince mahkumiyetine dair yazılı şekilde karar verilmesi,…" Y. 12. CD., T. 04.11.2020, E. 2020/2239, K. 2020/5688.

89 "*Dairemizce de benimsenen Yargıtay Ceza Genel Kurulu'nun 24.03.2015 tarihli ve 2014/14-603 Esas, 2015/66 Karar sayılı ilamında vurgulandığı üzere TCK'nın 226/3-1.cümlesindeki suçun oluşumu için önemli olan bir çocuğun müstehcen ürün üretiminde kullanılması olup, bu düzenlemede, suçun oluşumu için müstehcen görüntülerin profesyonel olarak hazırlanması aranmamakta, müstehcen ürünlerin şekli şartları ya da bu ürünlerin üretiliş biçimi ve amaçları konusunda bir sınırlama getirilmemektedir. Ayrıca suçun unsurlarının oluşması bakımından müstehcen ürünlerin izlenmesi, izlettirilmesi, satılması ve dağıtılması gibi bir zorunluluk da söz konusu değildir. Bu mahiyetteki müstehcen ürünlerin hiç izlenmemiş olması ya da bireysel amaç için üretilmiş olması da sonucu değiştirmeyecektir.…sanığın, yaşı küçük mağdurların haberleri olmadan etek altı görüntülerini cep telefonuna kaydetmesi şeklindeki eylemlerinin, mağduru sayısınca TCK'nın 226/3. maddesinin ilk cümlesindeki müstehcen görüntülerin üretilmesinde çocukların kullanılması suçunu oluşturduğu gözetilmeden, suç vasfında yanılgıya düşerek TCK'nın 134. maddesindeki özel hayatın gizliliğini ihlâl suçundan açılan davada, şikayet yokluğu gerekçesiyle düşme kararı verilmesi,…*" Y. 4. CD., T. 22.12.2021, E. 2021/31435, K. 2021/29897; Aynı yönde Y. 12. CD., T. 21.03.2018, E. 2017/5846, K. 2018/3217; Y. 18. CD., T. 13.03.2018, E. 2015/45221, K. 2018/3497.

arkadaşlığı ve ilişkiyi devam ettirme[90], ekonomik çıkar sağlama (para isteme)[91] ya da birliktelik yaşama[92] gibi çıkarlar söz konusu olabilmektedir.

Nihayet cinsel içerikli şantaj sonrasında fail tarafından istenilen şeyin yapılmaması durumunda mağdurun cinsel içerikli görüntülerinin 3. kişilerle paylaşılması halinde özel hayatın gizliliğini ihlal suçu (TCK m. 134/2) oluşacaktır[93].

2. Flört Partneri ile İlgili Olarak Sahte Cinsel İçerikli Görüntü Üretme ve Paylaşma: "*Deepfake*"

Deepfake teknolojisi kişilerin yüzlerini dijital olarak bir başkasının yüzüne yerleştirerek (montajlayarak) rıza dışı porno görüntüler üretilmesini sağlayan teknolojinin adıdır[94]. Günümüzde makine öğrenimi teknolojileri, insanların yüzlerinin ve seslerinin gerçek pornografiye monte edildiği "deep-fake (sahte)" cinsel içerikli videoların üretilmesi için kullanılmaktadır. Deep-fake teknolojisi, dijital bütün üzerinden kimlik oluşturulmasını sağlar. Sonuç olarak çürütülmesi giderek zorlaşan gerçekçi görünen video veya ses kayıtları oluşturulmaktadır[95].

Günümüzde dijital alanda cinsel mahremiyetin ihlali yöntemleri[96] arasında yer alan deepfake teknolojisi ile üretilmiş videolar, teknoloji uzmanları tarafından intikam pornosunun geleceği olarak belirtilmektedirler[97]. Cinsel mahremiyet, insan iradesinin ve cinsel özerkliğin

---

90 "*olayda, mağdur ...'nın görüntülerinin sanıkta olduğunun tespit edildiği, sanık tarafından mağdureye gönderilen mesaj içeriklerinde ise "... bu görüntülerin herkes tarafından izlensin..." şeklinde beyanlarda bulunarak görüntüleri yayacağını belirtip şantaj yoluyla arkadaşlığını ve ilişkiyi devam ettirmeye çalışarak yarar sağlamaya çalıştığı anlaşılmakla, sanığın bir yarar sağlamak amacıyla değil mağdurla arkadaşlığının devam etmesi amacıyla bu mesajları yazdığı şeklinde dosya içeriğine uymayan ve yerinde olmayan gerekçe ile şantaj suçundan yazılı şekilde hüküm tesisi,…*" Y. 4. CD., T. 21.10.2020, E. 2016/17882, K. 2020/13039; Y. 12. CD., T. 13.01.2021, E. 2019/5035, K. 2021/215; Y. 12. CD., T. 27.01.2021, E. 2020/871, K. 2021/736.

91 Y. 15. CD., T. 17.03.2020, E. 2017/30219, K. 2021/3104; Y. 4. CD., T. 10.06.2021, E. 2018/4386, K. 2021/18918; Y. 4. CD., T. 20.01.2021, E. 2017/19680, K. 2021/1644; Y. 4. CD., T. 18.01.2021, E. 2017/21718, K. 2021/1217.

92 Y. 4. CD., T. 25.11.2020, E. 2017/18626, K. 2020/18067.

93 Aynı yönde Y. 4. CD., T. 09.11.2021, E. 2019/2286, K. 2021/26683; Y. 12. CD., T. 10.03.2021, E. 2019/4532, K. 2021/2455.

94 WILKERSON, s. 329; Benzer bir tanıma göre "*Deepfake*", "*eldeki verilerden derin öğrenme tekniği kullanılarak, gerçek olmamasına rağmen gerçeğe çok yakın görüntü, video ve ses biçimindeki içeriklerin üretilmesi faaliyeti ve bu faaliyet sonucu üretilen içeriklerin*" genel adıdır. Bkz. BABAYİĞİT, s. 655. Yazara göre terim, "*derin öğrenme teknolojisinin kullanımıyla sahte içerik oluşturma*", "*derin öğrenme teknolojisinin kullanımıyla oluşturulan sahte içerik*", "*ileri sahtecilik*", "*derin taklit*", "*derin hile*", "*derin sahtecilik*" ve "*dip düzmece*" gibi ifadelerle Türkçe' ye çevrilebilir. Bkz. BABAYİĞİT, s. 656-657, dp. 3.

95 CITRON, s. 1921.

96 Öğretide cinsel mahremiyetin dijital alanda ihlali yöntemleri şu şekilde ayırılmaktadır: 1. Dijital röntgencilik, 2. Etek altı fotoğraflar, 3. Cinsel içerikli şantaj (*sextortion*), 4. Rıza dışı pornografi ve 5. Deep-fake seks videoları. Bkz. CITRON, s. 1908.

97 WILKERSON, s. 329.

uygulanması için esas niteliğinde bir ilkedir. Bireylerin mahrem yaşamlarının sınırlarını belirlemelerini sağlar. Cinsel mahremiyet ile bireyler, çıplak bedenlerinin görüldüğü, kaydedildiği, fotoğraflandığı veya sergilendiği kapsamları belirler. Bu anlamda kişiler mahrem bilgilerinin ne ölçüde ifşa edileceğine, yayınlanacağına veya gösterileceğine kendileri karar vermelidir. Başka birine cinsel yönelimi, cinsiyeti veya cinsel geçmişi hakkında bilgi verme ya da vermeme ancak kendi tasarruflarında kalması gereken bir konudur[98].

Deep-fake ile üretilmiş cinsel içerikli videolar, mahrem görüntülerin rıza dışı ifşa edilmesinden farklıdır; çünkü aslında bir mağdurun gerçek çıplak vücudunu göstermemektedir. Yayınlanan kişilerin gerçek genital bölgelerini ya da mahrem kalması gerekli vücut bölgelerini göstermese dahi deepfake videoları yine de insanların cinsel ve mahrem kimliklerinin kontrolünü ele geçirmektedir[99]. Rıza dışı pornografi gibi, deep-fake videoları da insanların cinselliği üzerinde hâkimiyet kurarak, rızaları olmaksızın bu kimliklerini başkalarına teşhir eder[100]. Bireyleri genitale, göğüslere, kalçalara ve anüslere indirgeyerek bireyin kendi eseri olmayan bir cinsel kimlik yaratırlar. Bu anlamda cinsel içerikli deep-fake videoları, insanların mahrem kimliklerini yalnızca kendilerinin paylaşabilecekleri veya paylaşmama iradesi gösterebilecekleri algısının bir ihlalidir[101]. Teknoloji temelli gerçekleştirilen bu sahte videolar, flört ilişkisi içinde olan ya da öncesinde flört ilişkisi yaşamış kişiler için dijital şiddet uygulama aracı haline gelebilmektedir[102].

Deep-fake videoları üretme fiillerinin Amerika' nın bazı eyaletlerinde suç olarak cezalandırılmış olduğu söylenebilir. Örn. Kalifornia Ceza Kanununun "Sahte Kimlik ve Hileler" başlıklı 8. Bölümü § 528.5(a)'ya göre, bir kişiye zarar vermek, korkutmak, tehdit etmek ya da dolandırmak amacıyla bilerek bir internet sitesinde ya da Internet sitesi aracılığıyla veya herhangi bir elektronik yolla gerçek bir kişinin kimliğine bürünmek (onu taklit etmek) suç olarak düzenlenmiştir[103].

98 CITRON, s. 1882.

99 CITRON, s. 1921.

100 CITRON, s. 1921.

101 CITRON, s. 1921.

102 Eski yakın partnerler de deep-fake yöntemine maruz kalabilmektedir. Bir Reddit kullanıcısının, şu soruyu sorduğu aktarılmaktadır: "Eski kız arkadaşımla bir porno videosu yapmak istiyorum. Onunla çektiğim yüksek kaliteli bir videom yok ama bir sürü iyi kalite fotoğrafım var." Bir Discord kullanıcısı ise, liseye birlikte gittiği bir kızın Instagram ve Facebook hesaplarından alınan yaklaşık 380 fotoğrafını kullanarak "oldukça iyi" bir video yaptığını açıklamıştır. Bkz. CITRON, s. 1922.

103 https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=8.&article= (Erişim Tarihi: 10.08.2022).

Fail tarafından deepfake teknolojisi ile üretilen cinsel içerikli görüntülerin yaratılması ve yaratılan görüntülerin sanal ortamlarda paylaşılması gibi fiillerden doğan ceza sorumluluğunun belirlenmesi önem arz etmektedir. Öğretide haklı olarak deepfake yöntemi ile gerçeğe yakın bir görüntünün üretilebilmesi için, yüzü ve sesi cinsel içerikli bir görüntüye eklenecek olan kişinin gerçek fotoğraflarına ve ses kayıtlarına ilişkin olabildiğince fazla verinin toplanmış olması gerektiği belirtilmektedir[104]. Bu kapsamda kişinin özellikle gerçek fotoğraflarının elde edilme şekli failin ceza sorumluluğunun belirlenmesinde yol gösterici olacaktır. Kişinin deepfake teknolojisi ile sahte video üretmekte kullanılacak fotoğrafları, gündelik yaşamını sürdürürken fail tarafından gizlice çekilmişse, bu durum mağdurun özel hayatının gizliliğini ihlal ettiğinden TCK m. 134/1' de yer alan özel hayatın gizliliğini ihlal suçu oluşacaktır[105]. Mağdurun özel hayatına ilişkin fotoğrafı ya da sesini içeren kayıtlar, "kişisel veri" olma özelliğine sahip olsa da, bu nitelikteki kişisel verilerin kaydedilmesi ya da ifşası gibi fiiller özel olarak TCK m. 134/1 ve 2' de düzenlendiğinden bu fiiller nedeniyle TCK m. 135 ve 136' da yer alan kişisel verilerin kaydedilmesi ya da yayılması suçu oluşmayacaktır[106]. Yargıtay mağdurun daha önce rızası ile yayımladığı fotoğraflar ile ilgili bir kararında, özel hayat ile ilgili olarak "*mağdurun başkalarının görmesini ve bilmesini istemeyeceği*" fotoğraf vurgusunu yaparak, bu nitelikte olmayan fotoğrafların ele geçirilmesi ya da verilmesi fiillerini TCK m. 136' da yer alan kişisel verileri hukuka aykırı olarak verme ya da ele geçirme suçu olarak değerlendirmiştir[107]. Belirtilen şekilde özel hayata ilişkin öğeler içermeyen fotoğrafların fail

---

104 BABAYİĞİT, s. 667.

105 "*…Mağdur …'in bindiği halk otobüsündeki tekli yolcu koltuğunda oturan Suriye uyruklu sanık …'ın, kamera fonksiyonunu aktif hale getirdiği cep telefonunun çekim yönünü, yakınında ve ayakta duran 19 yaşındaki mağdura doğru odaklayarak, mağdurun bilgisi dışında fotoğraflarını çektiği esnada, aynı otobüste yolcu olarak bulunan tanık Aslı'nın mağduru uyarmasının ve durumun kolluğa ihbar edilmesinin ardından, sanığa ait cep telefonununda mağdurun arkadan görüntülendiği 4 adet fotoğrafın tespit edildiği iddialarına dayalı olarak sanık hakkında TCK'nın 134/1. maddesindeki görüntü veya seslerin kayda alınması suretiyle özel hayatın gizliliğini ihlal suçundan kamu davası açıldığı olayda*…" Y. 12. CD., T. 10.03.2021, E. 2019/10269, K. 2021/2454.

106 Yargıtay da kararlarını aynı yönde vermektedir: "*…bir özel hayat görüntüsü ya da sesinin, "kişisel veri" olduğunda kuşku bulunmamakta ise de, kişinin özel hayatına ilişkin görüntüsü ya da sesinin, bilgisi dışında, resim çekme veya kaydetme özelliğine sahip aletle belli bir elektronik, dijital, manyetik yere sabitlenmesi TCK'nın 134/1. madde ve fıkrasının 2. cümlesinde; rızası dışında ifşa edilmesi, yani; yayılması, açığa vurulması, afişe edilmesi, ilan edilmesi, kamuoyuna duyurulması, aleniyet kazandırılması, özetle; içeriğini öğrenme yetkisi bulunmayan kişi veya kişilerin bilgisine sunulması TCK'nın 134/2. madde ve fıkrasında özel hayatın gizliliğini ihlal suçu kapsamında düzenlendiğinden, kişinin özel hayatına ilişkin görüntüsü ya da sesi, yasal anlamda, TCK'nın 136/1. madde ve fıkrası kapsamında kişisel veri olarak değerlendirilemez*." Y. 4. CD., T. 11.03.2021, E. 2020/11581, K. 2021/8890.

107 "*Daha önce mağdurun bilgisi ve rızası dahilinde yayımlandığı anlaşılan mağdurun günlük kıyafetleriyle poz vermiş şekilde çektirdiği resimleri, mağdurun başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin görüntüler olarak kabul edilemeyeceğinden, mağdurun kişisel veri niteliğindeki resimlerini ve cep telefonu numarasını, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle yayımlayan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında*

tarafından ele geçirilmesi durumunda kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçu oluşacaktır.

Deepfake yöntemi ile cinsel içerikli görüntü üretmek için belirli bir bilgisayar programının kullanılması durumunda her ne kadar TCK m. 245/A' da düzenlenen yasak cihaz veya program bulundurma suçu akıllara gelse de, söz konusu suçta belirtilen hareketin ancak bilişim alanında işlenen suçlar ya da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen suçların işlenmesi için gerçekleştirilmesinin aranması nedeniyle TCK m. 245/A' da yer alan suç oluşmaz[108]. Nitekim fail deepfake ile sahte görüntüleri üreten programı bilişim suçlarını işlemek için değil, dijital şiddet teşkil eden cinsel şantaj, hakaret ve benzeri suçları işlemek için kullanmakta ve bulundurmaktadır.

Deepfake yöntemi ile üzerinde mağdurun yüzünün montajlanacağı müstehcen görselde çocuk, temsili çocuk görüntüleri veya çocuk gibi görünen kişiler varsa ya da şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlar mevcutsa, görselin niteliğine göre müstehcenlik suçu (TCK m. 226/3-4) oluşacaktır. Bu görsellerin orijinal halinin bulundurulması zaten başlı başına müstehcenlik suçunu oluşturacağından, deepfake ile sahte üretilen görselin ayrıca bulundurulması önem arz etmeyecektir.

Kanımızca deepfake yöntemi ile cinsel içerikli görüntülere 3. kişilerde gerçek algısı yaratacak şekilde bir kişinin fotoğrafının ve ses kaydının montajlanması ve bu görüntülerin sanal ortamda (Internet, sosyal medya vb.) paylaşılması durumunda, bu kişiye karşı kişinin şeref ve haysiyetine saldırı teşkil eden "cinsel içerikli görüntüde yer aldığı" somut fiili ve olgusu isnat edilmiş olacaktır[109]. Bu durumda TCK m. 125/4'te yer alan alenen hakaret suçu oluşacaktır[110]. Ancak bu fiil yukarıda da belirtildiği üzere aynı zamanda kişisel verilerin hukuka aykırı olarak yayılması suçunu oluşturduğundan farklı neviden fikri içtima ilişkisi gereği cezalandırma en ağır ceza gerektiren suçtan, yani kişisel verileri hukuka aykırı olarak yayma

tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden,…" Y. 12. CD., T. 23.12.2020, E. 2020/2234, K. 2020/7459.

108 Aynı yönde BABAYİĞİT, s. 666.

109 Öğretide bu durumda yeni bir suç tipi olarak cinsel içerikli görüntüleri rızaya aykırı olarak ifşa etme, yayma, erişilebilir kılma veya üretme suçunun düzenlenmesi gerektiği ve "*deepfake*" teknolojisi aracılığıyla üretilen cinsel içerikli görüntülerin bu suçun konusunu oluşturduğu savunulmaktadır. Bkz. AKSOY RETORNAZ, s. 102, 115-116. Yazarın önerdiği yeni suç tipine göre "*deepfake*" yoluyla sahte oluşturulan görseller, cinsel içerikli görüntülerin üretilmesi seçimlik hareketini oluşturmaktadır. Ayrıca yazarın önermiş olduğu suç tipinde failin çocuk olması halinde soruşturma ve kovuşturma yapılması şikayete bağlı tutulmuştur. Bkz. AKSOY RETORNAZ, s. 142-143.

110 Aynı yönde BABAYİĞİT, s. 671.

suçundan (TCK m. 136) gerçekleştirilecektir. Yargıtay bir kararında benzer yaklaşımla önceden duygusal ilişki yaşadığı bir kişinin ismini ve fotoğrafını profil resmi olarak kullanıp, oluşturduğu sahte sosyal medya hesabından cinsel içerikli paylaşımlar gerçekleştirilmesi fiilini hakaret suçu kapsamında değerlendirmiştir[111]. Burada tartışılması gereken bir başka husus ise, failin deepfake yöntemi ile mağdurun fotoğrafını ve sesini montajlayıp ürettiği cinsel içerikli görüntüyü henüz paylaşamadan yakalanmış olmasıdır. Kanımızca bu durumda huzurda ya da gıyapta hakaret teşkil edebilecek bir saldırıya yönelik bir fiil bulunmadığından hakaret suçu oluşmayacaktır. Bu durumda sadece sahte videoda kullanılan fotoğraf, ses kaydı gibi kişisel veri teşkil eden unsurlardan dolayı kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçu (TCK m. 136) oluşacaktır.

3. Sanal Ortamda Flört Partnerine Rıza Dışı Cinsel İçerikli Yazı ya da Görüntü Yollama: "*Sexting*"

Cinsel içerikli mesajlaşma (*sexting*), cep telefonları veya internet üzerinden çıplak veya yarı çıplak fotoğraflar dâhil olmak üzere müstehcen mesajlar ve görüntülerin gönderilmesi veya paylaşılması olarak tanımlanmaktadır[112]. Amerikan Ulusal Kayıp ve İstismara Uğrayan Çocuklar Merkezi' ne (*NCMC*) göre bu adlandırma, "*gençlerin cinsel içerikli mesajlar yazması, kendilerinin veya akran grubundaki diğer bireylerin müstehcen fotoğraflarını çekerek, bu fotoğrafları ve/veya mesajları akranlarına iletmesini tarif etmektedir*"[113]. Ancak günümüzde

111 "*…sanık Hakan'ın, bir süre cinsel yakınlık boyutuna varacak düzeyde arkadaşlık ilişkisi içerisinde olduğu katılan Banu tarafından arkadaşlıklarına son verilmesine tepki olarak, facebook adlı sosyal paylaşım sitesinde üyelik işlemleri yapıp, katılan adına oluşturduğu sahte hesapta, katılanın rızası dahilinde çekilmiş resmini, profil fotoğrafı olarak kullandığı ve bu hesap üzerinden başka kişilere ait müstehcen görüntüleri yayınladığı iddia ve kabulüne konu olayda, Katılanın başını ve yüzünü gösteren, günlük kıyafetleriyle poz vermiş şekilde çektirdiği resminin, özel yaşam alanına ilişkin ve özel hayatının gizliliğini ihlal edecek nitelikte olmaması karşısında, katılanın resmini, isim ve soy ismiyle birlikte hukuka aykırı olarak yayınlayan sanığın TCK'nın 136. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan cezalandırılması; ayrıca, oluşturduğu sahte hesapta, katılan tarafından yayınlanıyor algısı doğuracak şekilde cinsel içerikli görüntülere yer vererek, katılanın, onur, şeref ve saygınlığını rencide eden sanığın TCK'nın 125. maddesinde düzenlenen hakaret suçundan mahkumiyetine karar verilmesi gerekirken, suç vasfında yanılgıya düşülerek, yasal ve yeterli olmayan gerekçelerle sanık hakkında TCK'nın 134/2. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkumiyet hükmü kurulması,… Bozmayı gerektirmiş olup,…*" Y. 12. CD., T. 20.05.2014, E. 2013/22544, K. 2014/12128.

112 SWEENY, s. 103. 'Cinsel içerikli mesajlaşma (*sexting*)' teriminin ilk adlandırma açısından geçmişte Kanadalı bir haber basını olan The Globe and Mail' in 2004 yılında ünlü futbolcu David Beckham ve asistanı arasındaki müstehcen metin mesajlarının tanımlandığı haberlere dayandığı belirtilmektedir. Bkz. MINOR, s. 309. Ayrıca bazılarına göre cinsel içerikli mesajlaşma (*sexting*) terimi Birleşik Krallık basınının ortaya attığı bir kavramdır. Diğer kişilere göre ise, terim önceleri cep telefonları üzerinden yazı temelli cinsel yazışmaları işaret etmekteyken, günümüzde cinsel içerikli fotoğrafların gönderilmesi olarak kullanılmaktadır. Bkz. GILLESPIE, s. 624. Öğretide müstehcen yazışmaların sadece cep telefonları ile yapılmasının "sexting" olarak ifade edildiği tanımlamalar da bulunmaktadır. Bkz. WEBB, s. 80. "Sexting" teriminin gençler ve ebeveynleri açısından tanımlamaları için bkz. MULDAVIN, s. 431-434.

113 WEBB, s. 80.

cinsel içerikli mesajlaşma (*sexting*) kavramı gençler arasındaki mesajlaşma ile sınırlı bir kavram olarak değil, yetişkinler de dâhil olmak üzere tüm kişiler arasındaki cinsel içerikli mesajlaşmaları kapsar şekilde kullanılmaktadır[114]. Dikkat edilecek olursa cinsel içerikli mesajlaşmada söz konusu olan cinsel içerikler (yazışma, görseller), gönderen kişinin kendi kendine üretmiş olduğu içerikler de olabilecektir. Bu anlamda kişi kendi üretmiş olduğu cinsel içerikteki metini ya da çıplak, yarı çıplak veya cinsel davranış içeren görseli duygusal ilişki yaşadığı kişiye "özel mesaj ya da fotoğraf" olarak göndermektedir[115]. Öğretide kişinin kendisini temsil eden cinsel içeriği, videoyu veya fotoğrafı paylaşması durumu "*birincil 'sexting'*" olarak adlandırılmaktadır[116]. Başka bir kişinin ilettiği veya ürettiği cinsel içerikli materyalin aktarılarak materyalin yayılmasına neden olunması ise "*ikincil 'sexting'*" olarak adlandırılmaktadır[117].

Dijital medya çağında, reşit olmayanlar arasında cinsel içerikli mesajlaşma büyük ölçüde sosyal etkileşim biçimi haline geldiğinden, bu kişiler arasındaki cinsel içerikli mesajlaşmaların suç soruşturması ya da kovuşturması konusu olması potansiyelinin de arttığı söylenebilecektir. Bir araştırmaya göre gençlerin en az yüzde yirmisinin çıplak veya yarı çıplak fotoğraf ve videolarını gönderip paylaştığı söylenmektedir[118]. Özellikle cinsel içerikli mesajlaşmaya konu olan yazışmalar ya da görüntülerin siber zorbalıkta, cinsel içerikli şantajda ya da flört istismarında kullanılabilmesi, içeriğin sanal ortamda uzun süreler kalabilmesi bu eylemlerin çocuklar üzerinde ciddi psikolojik zarara yol açmasına neden olabilmektedir[119].

ABD' de Arkansas, Connecticut, Florida, Louisiana, New Jersey, Rhode Island, Güney Dakota, Vermont ve Batı Virginia dâhil birkaç eyalet "cinsel içerikli mesajlaşma" ile ilgili bir hükmü kanunlarına eklemiştir[120].

Florida' nın cinsel içerikli mesajlaşma yasası, cinsel siber taciz kapsamında bir başkasının kasıtlı ve kötü niyetli cinsel siber tacizi olduğunu belirtmektedir. "*Cinsel siber taciz, ciddi bir duygusal sıkıntıya neden olma niyetiyle, meşru bir amaç olmaksızın müstehcen bir görüntü yayınlamak anlamına gelir*."[121]

114 GILLESPIE, s. 624; AKSOY RETORNAZ, s. 17.
115 GILLESPIE, s. 624.
116 AKSOY RETORNAZ, s. 17.
117 AKSOY RETORNAZ, s. 18.
118 MINOR, s. 310.
119 MULDAVIN, s. 444 vd.
120 MINOR, s. 318-319.
121 MINOR, s. 319.

Çocuğun cinsel anlamda sömürüsünün önlenmesi için birçok ülke cinsel içerikli görüntülerde çocuğun kullanılmasını, bu içerikli görüntülerin üretilmesi, paylaşılması ya da bulundurulması gibi eylemleri ulusal mevzuatlarında suç olarak düzenlemiştir. Bu durum da cinsel içerikli mesajlaşma eylemlerine konu olan yazışma ve görsellerin çocuk pornografisi olarak cezalandırılabilir eylemler şeklinde değerlendirilmesine yol açmaktadır. Örneğin ABD' de on yedi yaşında birisinin kendisinin müstehcen bir fotoğrafını çekmesi ve bunu kimse ile paylaşmaması durumunda dahi çocuk pornografisi üretme ya da bulundurma eyleminden suçlu bulunabileceği belirtilmektedir[122]. ABD' nin Pensilvanya eyaleti Ceza Kanununun "Cinsel içerikli görüntülerin küçük tarafından iletilmesi" başlıklı § 6321/(a)/1'e göre, kendisinin cinsel içerikli görüntüsünü içeren elektronik iletişimi bilerek ileten, yayan, yayınlayan ya da dağıtan küçük suç işlemiş sayılmaktadır[123]. Aynı Kanun § 6321/(a)/2'ye göre ise, küçük bilerek 12 yaşında veya daha büyük bir küçüğün cinsel içerikli görüntüsünü bulundurur ya da bilerek görüntülerse suç işlemiş sayılmaktadır. Söz konusu Kanunun "Tanımlar" başlıklı § 6321/(g)'ye göre, küçük on sekiz yaşının altındaki kişileri belirtmektedir.

Birleşik Krallık' ta Çocukların Korunması Kanunu 1978, bölüm 1, 1/a'ya göre, bir çocuğun herhangi açık saçık fotoğrafının ya da sözde/sahte/düzmece fotoğrafının alınması, alınmasına müsaade edilmesi ya da üretilmesi suç olarak düzenlenmiştir. Aynı Kanun 1/b'ye göre aynı görsellerin yayılması ya da gösterilmesi, 1/c'ye göre başkaları tarafından yayılması ya da gösterilmesi amacıyla bu görsellerin bulundurulması, 1/d'ye göre reklam veren tarafından bu görsellerin yayıldığı, gösterildiği şeklinde anlaşılacak şekilde reklamın yayınlanması ya da yayınlanmasına neden olunması suç olarak düzenlenmiştir[124]. Bu eylemler çerçevesinde söz konusu Kanun dikkate alındığında İngiltere ve Galler ülkelerinde bir gencin kendi cinsel içerikli görüntülerini alması ve bunu bir başkasına yollaması durumunda potansiyel olarak belirtilen suç çerçevesinde suçlu sayılması riski bulunduğu belirtilmektedir[125]. Bu durum ise gençlerin cinsel kimliklerini ifade etme özgürlüğünün olup olmadığı tartışmalarını Avrupa İnsan Hakları

122 SWEENY, s. 105.

123 https://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=63&sctn=21&subsctn=0 (Erişim Tarihi: 29.07.2022).

124 https://www.legislation.gov.uk/ukpga/1978/37 (Erişim Tarihi: 29.07.2022).

125 GILLESPIE, s. 631.

Sözleşmesi m. 10 (ifade özgürlüğü)[126] ve m. 8 (özel hayata saygı hakkı)[127] çerçevesinde gündeme getirmektedir[128].

Cinsel içerikli mesajlaşma daha çok on sekiz yaş altı kişilerin, yani çocukların söz konusu olduğu durumlarda ceza hukuku açısından ön plana çıkmaktadır. Zira yetişkin kişilerin duygusal ilişki içinde olduğu kişi ile karşılıklı rıza çerçevesinde cinsel içerikli görüşmesi ya da görüntü yollaması, gönderilen içeriğin TCK m. 226 "Müstehcenlik" suçu ile korunan hukuksal değeri ihlal etmemesi şartıyla suç teşkil etmemektedir. Bu durum bireyin kişiliği ile sıkı sıkıya bağlantılı olan cinsel mahremiyeti ve cinsel özerkliği[129] konusunda tasarrufta bulunma yetkisinin bir sonucudur. Yetişkin kişilerin tasarruf etme yetkisinin bulunduğu cinsel mahremiyet ve cinsel özerklik konusunda çocukların tasarrufta bulunma hakkının olup olmadığı ya da bu hak varsa çocuğun bu hakka ilişkin hangi sınırlar içinde tasarrufta bulunabileceği konusu tartışmaları beraberinde getirmektedir[130]. Bu sınır çocuklar arasındaki cinsel içerikli mesajlaşma ("*sexting*") eylemlerinin "çocuk pornografisi" çerçevesinde "müstehcenlik" suçu, özel hayatın gizliliği ya da diğer cinsel suçları oluşturup oluşturmayacağı tartışmasında belirleyici nitelikte olacaktır.

İlk olarak kendi hazırlamış olduğu mesaj ya da kendi görselini kullandığı içerikleri diğer bir çocuğa yollayan çocuk failin eyleminde cinsel taciz suçunun çocuklara karşı işlenmesi suçunun oluşup oluşmadığının incelenmesi gerekir. Cinsel taciz suçunun oluşabilmesi için cinsel saldırı boyutuna varmayan, cinsel yönden "*ahlak temizliğine aykırı olarak*" mağduru rahatsız eden herhangi bir cinsel davranışın bulunması gerekmektedir[131]. Yargıtay, cinsel saldırı boyutuna varma eşiğine ilişkin değerlendirmenin bedensel (fiziki) temas olup olmamasına göre

126 Çocuk pornografisi yasalarından daha az cezayı gerektirse dahi gençler arasındaki cinsel içerikli mesajlaşmayı suç sayan yasaların ifade özgürlüğünü kısıtlayan anayasaya aykırı uygulamalar olduğu belirtilmektedir. Bkz. SWEENY, s. 105.

127 Dudgeon v Birleşik Krallık (Başvuru No: 7525/76, 22.10.1981), AİHM Kararına göre cinsel kimlik, m. 8 (özel hayata saygı hakkı) kapsamında görüldüğünden bu madde çerçevesinde tartışılmıştır. Bkz. GILLESPIE, s. 634-635.

128 GILLESPIE, s. 631.

129 Cinsel özgürlüğün tasarruf edilebilir nitelikte olması nedeniyle mağdurun rızasının hukuka aykırılığı ortadan kaldıracağı yönünde görüş için bkz. TEZCAN, ERDEM, ÖNOK, s. 497. Aynı yönde bkz. KOCA, ÜZÜLMEZ, s. 333.

130 Bu tartışmaya YCGK kararına konu bir olayda da vurgu yapılmaktadır: *"...Burada uyuşmazlığın sağlıklı bir hukuki zemine oturtulabilmesi için çocukların çıplak bedenlerine ait görüntüler de dahil olmak üzere özel hayatlarına ilişkin olarak her türlü konuda mutlak surette tasarruf özgürlüklerinin bulunup bulunmadığının, dolayısıyla da bu konudaki rızalarının geçerli olup olmadığının belirlenmesi zorunluluğu doğmaktadır*." YCGK., T. 10.06.2014, E. 2013/551, K. 2014/311.

131 Madde gerekçesine göre, "*Cinsel taciz, kişinin vücut dokunulmazlığının ihlâli niteliği taşımayan cinsel davranışlarla gerçekleştirilebilir. Cinsel taciz, cinsel yönden, ahlâk temizliğine aykırı olarak mağdurun rahatsız edilmesinden ibarettir*."

yapılacağını istikrarlı bir şekilde kararlarında belirtmiştir[132]. Ayrıca Yargıtay Ceza Genel Kuruluna göre[133], "…*Eylemin cinsel amaçla işlenip işlenmediği ya da hangi fiilin cinsel taciz suçunu oluşturacağı belirlenirken sosyal hayatın gerekleri, tarafların konumları ile aralarındaki ilişki gözetilmeli*"dir ve "…*şikâyetçi ve sanık arasındaki yaş farkı, sanığın medeni durumu ve taraflar arasındaki sosyal ilişki*…" gibi unsurlar da dikkate alınmalıdır. Karşılıklı iki çocuğun rızaya dayalı cinsel içerikli mesaj göndermesi durumunda bedensel temas içeren bir davranışın bulunmadığı açıksa da, bu eylemin muhatap çocuğu rahatsız edici bir davranış olup olmadığı tartışılması gereken bir sorundur. Zira Yargıtay da karşılıklı mesajlaşma ya da görüşmelerde "taciz rahatsız etme" unsurunun ne şekilde oluştuğunun tespit edilmesi gerektiğini vurgulamaktadır[134].

Konu esasen çocuğun cinsel özgürlüğü hakkında tasarrufta bulunma yeteneğinin sınırlarının ne olduğu ile ilgilidir. Türk ceza hukuku sisteminde TCK m. 103 (çocukların cinsel istismarı) ve TCK m. 104 (reşit olmayanla cinsel ilişki) düzenlemeleri dikkate alındığında 15 yaşını doldurmuş bir çocuğun cinsel ilişki boyutuna varmamak koşuluyla cinsel özgürlüğü konusunda tasarruf yeteneğinin bulunduğu söylenebilir[135]. Bu açıdan cinsel içerikli bir mesajı ya da cinsel içerikli kendi görüntüsünü karşılıklı rıza ile yollayan ya da benzer içerikteki mesajı alan 15 yaşını doldurmuş çocukların gerçekleştirmiş oldukları eylemlerde cinsel taciz suçu oluşmayacaktır. Ancak bu içeriklerin 15 yaşını doldurmamış çocuğa gönderilmesi durumunda kanımızca içeriğin objektif olarak "rahatsız edici" biçimde nitelendirilmesi ve cinsel taciz suçunun oluştuğunun kabul edilmesi gerekmektedir. Örneğin 16 yaşında bir çocuğun kendi müstehcen görüntüsünü alıp, bu görüntüyü 14 yaşındaki arkadaşına onun rızası ile de olsa göndermesi, cinsel açıdan "rahatsız edici" davranış olarak kabul edilmeli ve cinsel taciz suçunun oluştuğu sonucuna varılmalıdır[136]. 14 yaşında bir çocuğun kendi müstehcen

---

132 Y. 14. CD., T. 17.11.2020, E. 2016/4987, K. 2020/5046; Y. 14. CD., T. 12.10.2020, E. 2016/3632, K. 2020/3936; Y. 14. CD., T. 09.12.2019, E. 2016/5777, K. 2019/13122.

133 YCGK., T. 04.12.2018, E. 2017/244, K. 2018/601.

134 "…*katılan …'a cinsel içerikli mesajlar attığının iddia olunması, sanığın savunmalarında suçları kabul etmeyip katılan ile duygusal arkadaşlık yaptığını ve kendisinin attığı mesajlara karşılık olarak mesajlar aldığını ifade etmesi ve dosya içerisinde yer alan katılanın HTS kayıtlarında, suç tarihinde karşılıklı olarak çok sayıda mesaj atılıp alındığının ve katılanın sanığı toplamda 4 kez telefonla arayıp uzun süreler konuştuğunun anlaşılması karşısında, bu hususlar değerlendirilmeden, "taciz rahatsız etme" öğesinin nasıl oluştuğu tespit edilmeden, eksik inceleme ve yetersiz gerekçe ile TCK'nın 105/1.maddesi uyarınca sanık hakkında cinsel taciz suçundan hükümlülük kararı verilmesi*,…" Y. 4. CD., T. 19.10.2017, E. 2016/11510, K. 2017/22787.

135 TEZCAN, ERDEM, ÖNOK, s. 474. Aynı yönde YCGK. T. 10.06.2014, E. 2013/551, K. 2014/311.

136 "*Sanığın, internet üzerinden irtibat kurduğu 14 yaşındaki mağdureyle cinsel içerikli yazışmalar yaptığı, ona cinsel ilişki teklif ettiği olayda; mevcut hâliyle bedensel temas içermeyen eylemlerin zincirleme şekilde cinsel taciz suçunu oluşturduğu gözetilmeden*,…" Y. 6. CD., T. 19.02.2020, E. 2017/1556, K. 2020/722.

görüntüsünü alıp, bu görüntüyü 16 yaşındaki arkadaşına onun rızası ile de olsa göndermesi durumunda ise cinsel taciz suçunun oluşmadığı sonucuna varmak gerekecektir. Aynı değerlendirme "özel hayatın gizliliği suçu" açısından da yapılabilir. Nitekim Yargıtay Ceza Genel Kurulu bir kararında 15 yaşından küçük çocuğun çıplak bedeninin çocuğun rızası ile alınması durumunda, mağdurun üzerinde mutlak tasarrufta bulunabileceği bir hakkın bulunmadığına vurgu yapmıştır[137]. Söz konusu olayda ayrıca 14 yaşındaki bir çocuğun müstehcen fotoğrafının üretilmesi ve bulundurulması eylemleri açısından TCK m. 226 "müstehcenlik" suçunun tartışılması gerekmektedir. Bu eylem nedeniyle şayet müstehcenlik suçunun da oluştuğu söylenebilirse, belirtilen suçlar ile müstehcenlik suçu farklı neviden fikri içtima ilişkisine girecektir.

Belirtilen tartışmalar da dikkate alındığında 15 yaşından küçük bir çocuğun herhangi bir çıplak fotoğrafının ya da cinsel ilişkisini içeren bir görselin üretilmesi durumunda müstehcenlik suçunun oluşup oluşmadığının üzerinde durulması gerekmektedir. TCK m. 226/3' te müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların, temsili çocuk görüntülerinin veya çocuk gibi görünen kişilerin kullanılması suç olarak düzenlenmiştir. TCK m. 226/3, 2. cümleye göre aynı nitelikteki ürünlerin ülkeye sokulması, çoğaltılması, satışa arz edilmesi, satılması, nakledilmesi, depolanması veya bulundurulması eylemleri de suç olarak düzenlenmiştir. Müstehcenlik suçu ile korunan hukuksal değer[138] ve suçun TCK sistematiğinde "Topluma Karşı Suçlar" kısmının "Genel Ahlaka Karşı Suçlar" bölümünde düzenlenmesi dikkate alındığında bu suçta çocuğun belirtilen eylemlere rızasının eylemi hukuka uygun hale getirmeyeceği söylenmelidir. Benzer sonuca içeriğini kendisinin oluşturduğu "müstehcenlik" teşkil eden ürünü bizzat kendisi üreten 15 yaşını doldurmamış çocuk açısından da ulaşılması gerekmektedir. Müstehcenlik suçunun mağduru toplumu oluşturan tüm bireyler olduğu için[139],

---

137 "*…Sanığın suç tarihinde cinsel ilişkiye girdiği 15 yaşından küçük mağdurenin çıplak bedenini kendi rızası dahilinde cep telefonu kamerasıyla çekip kaydetmesi eyleminde, mağdurenin rızası hukuken üzerinde mutlak surette tasarruf edebileceği bir hakka ilişkin olmadığından hukuka uygunluk nedeni olarak kabul edilemeyecektir. Dolayısıyla 15 yaşından küçük mağdurenin rızasıyla bile gerçekleştirilmiş olsa bu eylem TCK'nun 134/1. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçunu oluşturmakta olup sanığın cinsel ilişki sırasında mağdurenin bedenini görüyor olması da, ulaşılan bu sonucu değiştirmeyecektir*." YCGK., T. 10.06.2014, E. 2013/551, K. 2014/311.

138 Öğretide bu suçla korunan hukuksal değerin, "*genel ahlakın korunması bağlamında müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocuk cinselliğinin istismarının, açıkçası çocuğun seks aracı, cinsel nesne olarak kullanılmasının, kısacası 'çocuk pornografisinin' önlenmesine ilişkin ferdi-kamusal yarar*" olduğu belirtilmektedir. HAFIZOĞULLARI, ÖZEN, s. 341. Diğer bir görüş ise, bu suçla korunanın çocuk hakları olduğu ve bu nedenle suçla çocuğun korunmasının amaçlandığı söylenmektedir. Bu görüşe göre, çocuğun pornografik bir ürünün ya da benzer bir fiilin konusu olmasının da engellenmek istenmiştir. Diğer taraftan çocuğun cinsel istismara karşı korunması da sağlanmak istenmiştir. Suç ile çocuğun korunması amacıyla aynı zamanda genel ahlak da korunmaya çalışılmaktadır. Bkz. ÖZBEK, s. 118-121.

139 *Hafızoğulları/Özen*' e göre, bu suçun mağduru kanunen genel ahlakı korumakla görevli kılınan kamu idareleri yanında, cinsel nesne olarak kullanılan çocuk veya çocuklardır. Bkz. HAFIZOĞULLARI, ÖZEN,

15 yaşını doldurmayan çocuğun kendisine ait müstehcen içeriği üretmesi durumunda fail ile mağdur sıfatının aynı kişide birleşmesi durumu söz konusu olmayacaktır[140]. TCK m. 226/3' deki düzenlemeye bakıldığında müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların, temsili çocuk görüntülerinin veya çocuk gibi görünen kişilerin kullanılması yasaklanmıştır. Çocuk kavramı, TCK m. 6/1-b' de henüz onsekiz yaşını doldurmamış kişi olarak tanımlanmıştır. O halde 17 yaşındaki bir çocuğun kendi telefonu ile müstehcen nitelikteki kendi fotoğrafını oluşturması/yaratması/meydana getirmesi bu suç tanımına uyacaktır. Söz konusu bu eylemin çocuk pornografisi ile eşdeğer tutulması ve ceza hukuku yönünden aynı sonuca bağlanması kanımızca yerinde değildir. 17 yaşındaki çocuğun eyleminde Yargıtay kararlarında da vurgu yapılan toplumun ortak edep ve ahlak temizliğine yönelik açık bir saldırı niteliği olmadığı, özellikle çocukların bu davranışın zararlı etkilerinden korunmasının gerekmemesi nedeniyle suçun oluşmadığının söylenmesi gerekmektedir[141]. 17 yaşındaki bir çocuğun kendine ait müstehcen içerikli bir fotoğrafı ürettikten sonra, bu fotoğrafı duygusal ilişki yaşadığı flört partnerine yollaması durumunda bu kişi de belirtilen nitelikteki ürünü bulundurduğu için TCK m. 226/3, 2. cümledeki suçu işlemiş sayılacaktır. Kanımızca bu durumda ilgili fotoğrafı bulunduran kişinin eyleminin de çocuk pornografisi bulundurma eylemi ile eşdeğer tutulması yerinde olmayacaktır[142].

Çocuğun kendi cinsel içerikli görüntüsünü üretmesi ve bu görüntüyü kendi gibi bir başka çocukla paylaşması eylemlerinin "müstehcenlik suçu" çerçevesinde cezalandırılmaması gerekliliği Avrupa Konseyi Çocukların Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi (*Lanzarote Sözleşmesi*) Komitesi tarafından da dile getirilmiştir[143]. Komiteye göre, "sexting" konusunda çocuğun yüksek yararının her zaman göz önünde tutulması

s. 341. *Gökcan/Artuç*' a göre, bu suçun mağduru 18 yaşını tamamlamamış kimseler olan çocuklardır. Bkz. GÖKCAN, ARTUÇ, Cilt 5, s. 7525.

140 Aynı yönde bkz. ÖZBEK, s. 124.

141 Ancak Yargıtay 15 yaşını doldurmuş çocuklara ait çıplak görüntülerin de TCK m. 226/3' deki müstehcenlik suçunun konusunu oluşturabileceğini belirtmektedir: "*…suça sürüklenen çocuk …'den ele geçen görüntülere ilişkin bilirkişi raporunda, 16 yaşında olan katılan …'a ait cinsel içerikli fotoğraflar olduğunun belirtilmesi karşısında, iddianamede suça sürüklenen çocuk …'nin yaşı büyük ve soruşturması ayrı yürütülen …, mağdure … çıplak görüntülerini almasını ve kendisine vermesini söylediği, yaşı büyük … 'ın bu görüntüleri … isteği ile çektiği ve çıplak görüntüleri … telefonuna gönderdiği şeklinde anlatılan eyleminin TCK'nın 226/3. maddesinin ilk cümlesinde tanımlanan müstehcenlik suçunu oluşturduğu, özel hayatın gizliliğinin ihlali suçundan açılan davada değişen bu suç vasfı nedeniyle müstehcenlik suçundan ek savunma hakkı tanınarak yargılamaya devamla hüküm kurulması gerektiği gözetilmeden, özel hayatın gizliliğinin ihlali suçundan beraat kararı verilmesi,…*" Y. 18. CD., T. 15.11.2018, E. 2018/6751, K. 2018/15084.

142 Bu haksız sonucun önüne geçebilmek için, öğretide yeni suç tipi olarak düzenlenmesi gerekli olan "*Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme*" suçunun çocuk fail tarafından işlenmesi durumunda suçun şikâyete tabi olması gerektiği önerilmiştir. Bkz. AKSOY RETORNAZ, s. 142-143.

143 AKSOY RETORNAZ, s. 53.

gerekmektedir. Bu nedenle çocukların sadece özel kullanımları için kendileri tarafından cinsel içerikli görüntülerin oluşturulması, paylaşılması ve bulundurulmasının "çocuk pornografisi üretimi, bulundurulması, sunulması, dağıtılması, iletilmesi, tedarik edilmesi veya bilerek erişim sağlanması" anlamına gelmediğinin altının çizilmesi gerekmektedir. Komiteye göre, cinsel içerikli görüntüler çocuklar tarafından oluşturulduğunda, çoğu durumda bu çocukların manipülasyon veya zorlamaya maruz kalmış mağdurlar olduğu göz önünde bulundurularak bu çocukları cezalandırmak yerine, bu tür davranışların sonuçları konusunda eğitmeye ve kendilerini nasıl koruyacaklarını öğretmeye odaklanılmalıdır. Çocuklar gizli kalması amaçlanan cinsel görüntüleri ve videoları bilerek ifşa ederlerse, yalnızca son çare olarak "çocuk pornografisi" ile ilgili kasten işlenen suçlar nedeniyle işlem yapılmalı ve zararlı davranışların giderilmesine yönelik eğitim ve tedavi amaçlı tedbirler uygulanmalıdır[144].

Salt çıplak ya da yarı çıplak fotoğrafın başlı başına "müstehcen" sayılıp sayılmayacağı tartışması[145] bir tarafa bırakılacak olunursa, Yargıtay kararlarında çocuğun etek altı görüntülerinin alınması[146], çıplak fotoğraflarının şantajla ele geçirilmesi[147], sosyal medyadan arkadaşlık kurarak üst kısmı çıplak fotoğrafını göndermesinin sağlanması[148], MSN' de görüntülü sohbet yaptıkları esnada çocuğun kıyafetini yukarıya doğru kaldırmasını sağlayarak göğüslerini gösteren fotoğraflarının gizlice çekilmesi[149], cep telefonu ile tamamen çıplak ve

144 Aktaran AKSOY RETORNAZ, s. 53.

145 Öğretide çıplaklığın her zaman müstehcen nitelikte olmayacağı belirtilmektedir. *Hafizoğulları/Özen*' e göre, çocukların çağın eğitsel gereklerine uygun olarak cinsellik karşısında korunması hariç; iğrenç, tiksindirici, aşağılayıcı, ayırımcı olmadıkça ve insanlığın kazanımı evrensel insani değerleri zedelemedikçe, hangi form altında olursa olsun, cinselliğin her türlü ifadesinin bir yasağın konusu yapılmaması, yani müstehcen sayılmaması gerekir. Bkz. HAFIZOĞULLARI, ÖZEN, s. 329. Müstehcenlik "*topluma hakim olan ortak edep duygularının incitilmesi, her ne suretle olursa olsun edep ve ahlak temizliğine saldırılması şeklinde ortaya çıkmakta ve cinsel arzuları tatmine yönelen ve cinselliği tahrik ve istismar eden davranışlarla belirlenmektedir*". Bu tanım uyarınca "çıplaklık" her zaman müstehcen nitelikte değildir. Tartışmalar için bkz. AKSOY RETORNAZ, s. 94-95; ÖZBEK, s. 45-53; GÖKCAN, ARTUÇ, Cilt 5, s. 7528-7530. Yargıtay' a göre, "…*Müstehcenlik normatif bir kavram olup toplumdan topluma değiştiği gibi aynı toplum içinde toplumsal değerlere bağlı olarak da değişikliğe uğramaktadır. Bu kavramın varlığının tespitinde, toplumun belli bir kesiminde kabul edilen değer yargıları değil, toplumun genelinin ve demokratik toplum düzenine ilişkin davranış kurallarının esas alınması gerekir.*
Buna göre suça konu ürünün toplumun ortak edep ve ahlak temizliğine yönelik açık bir saldırı niteliğinde olup olmadığı, özellikle çocukların bu davranışın zararlı etkilerinden korunması gerekip gerekmediği tespit edilip objektif olarak müstehcen olup olmadığı belirlenmelidir…." YCGK., T. 24.03.2015, E. 2014/603, K. 2015/66; "…*suça konu ürünün toplumun ortak edep ve ahlak temizliğine yönelik açık bir saldırı niteliğinde olup olmadığı, özellikle çocukların bu davranışın zararlı etkilerinden korunması gerekip gerekmediği tespit edilip objektif olarak müstehcen olup olmadığı belirlenmelidir. Müstehcenlikte kamu yararına, genel ahlak ile sağlığa aykırılık ve tecavüz hâli vardır dolayısıyla cezai önlem ve yaptırım kamu düzeni ve yararı için zorunludur*." YCGK., T. 25.06.2020, E. 2018/461, K. 2020/323.

146 Y. 4. CD., T. 22.12.2021, E. 2021/31435, K. 2021/29897.

147 Y. 4. CD., T. 22.12.2021, E. 2021/14728, K. 2021/29898.

148 Y. 4. CD., T. 15.12.2021, E. 2021/32664, K. 2021/29357.

149 Y. 12. CD., T. 13.10.2021, E. 2021/5277, K. 2021/6888.

cinsel organı da görüntülenen fotoğraflarının kaydedilmesi[150], cinsel ilişki esnasında görüntülerin kaydedilmesi[151], banyoda çıplak görüntülerinin cep telefonuyla çekerek CD' ye kaydedilmesi[152] gibi durumlarda müstehcenlik suçunun oluşacağı belirtilmektedir.

E. Cinsel Sömürü Amacıyla Sanal Ortamda Çocuklarla Flört İlişkisi veya Cinsel Temas Kurmaya Yönelik Davranışlar (Siber Cinsel Uşaklaştırma: "*Cyber Sexual Grooming*")

Günümüzde internetin yaygınlaşması ile birlikte özellikle sosyal medya ve bilişim alanı, henüz kendi cinsel mahremiyeti ve cinsel özerkliği konusunda yeterince olgunlaşmamış çocukların cinsel sömürü amacıyla kullanılabileceği bir alan haline gelmiştir. Sanal alanın gerçek dünyadan bu konuda daha tehlikeli olmasının nedeni, bu alanın kullanıcılara gerçek kimliklerini ve yaşları gibi kişisel özelliklerini gizleyebildikleri elverişli bir anonimlik sağlamasıdır. Bu tehlikelerin başında bilişim alanında gerçekleştirilen çocuklarla flört ilişkisi veya cinsel temas kurmaya yönelik davranışları içeren bir üst kavram olan siber cinsel uşaklaştırma (İng. *cyber sexual grooming*) gelmektedir. Literatürde belirtilen davranışların içerdiği yöntemleri ifade etmek bakımından değişik kavramların kullanıldığı görülmektedir. Bunlar; "çocuğun cinsel yönden uşaklaştırılması (*child sex grooming*)[153]", "cinsel uşaklaştırma (*sexual grooming*)[154]", "siber cinsel uşaklaştırma (*cyber sexual grooming*)[155]" kavramlarıdır. Kavramın ifade ettiği yöntem ve eylemlere bakıldığında İngilizce "*groom*" kelimesinin uşak olarak çevrilmesi mümkün olduğu gibi, bir kişinin bir iş için yetiştirilmesi ya da hazırlanması anlamına gelen İngilizce (*groom someone for a job*) ifadesindeki anlamıyla da çevrilmesi mümkündür. Zira bu kavramın ve içermiş olduğu yöntemlerin özünde çocuğun cinsel istismar ya da cinsel anlamda sömürülmesi için hazırlanması yer almaktadır[156].

"Çocuğun uşaklaştırılması (*child grooming*)", cinsel suç faillerinin çocuklarla cinsel sömürü içeren ilişkiyi dikkatli bir biçimde başlatma ve sürdürme sürecini tanımlamak için

150 Y. 12. CD., T. 07.07.2021, E. 2021/1557, K. 2021/5658.

151 Y. 4. CD., T. 04.03.2021, E. 2020/18348, K. 2021/7822.

152 Y. 14. CD., T. 23.12.2020, E. 2016/4160, K. 2020/6274.

153 AKHTAR, s. 167 vd.

154 MOHAN, LEE, s. 96 vd.

155 DONICA, CHEW, MAJEED, s. 40 vd.

156 Nitekim öğretide cinsel uşaklaştırma (*sexual grooming*), bir failin cinsel anlamda istismar amacıyla aşama aşama (kademeli olarak) bir kişinin ya da organizasyonun güvenini kazandığı bir hazırlık süreci olarak tanımlanmaktadır. Bkz. POLLACK, MACIVER, s. 161. Bu tanımdan da anlaşılacağı üzere kavramın odak noktası cinsel istismara hazırlık sürecidir.

kullanılan bir terimdir[157]. Uşaklaştırmada bir yetişkin tarafından küçük çocuk ile arkadaş olunması ve suç teşkil eden cinsel temasta bulunmak için çocuğun koymuş olduğu engellemeleri azaltmak amacıyla onunla duygusal bağlantı tesis etme söz konusudur[158]. Bir başka deyişle çocuğun uşaklaştırılmasında, gelecekte çocuğun istismarını gerçekleştirmek veya çocuğa pornografi sunmak örneğinde olduğu gibi diğer yollar aracılığıyla çocuğun cinsel istismarına zemin hazırlamak amacıyla fail ile çocuk arasında güveni içeren istikrarlı ve güvenilir bir ilişkinin tesis edilmesi söz konusudur[159]. Uşaklaştırma çevrimiçi ya da yüz yüze (fiziksel) gerçekleştirilebilir[160]. Olağandışı vakalarda fail tehdit ve fiziksel gücü de çocuğun istismarında kullanabilmektedir[161].

Uşaklaştırma süreci çeşitli aşamaları içermektedir. Bu aşamalar; mağduru seçme aşaması, arkadaşlık ve ilişki-şekillendirme aşaması, sınırın ortadan kalkması (özel olma)/izolasyon aşaması ve son olarak cinselleştirme ve kontrolü sürdürme aşaması olarak belirtilebilir[162]. Uşaklaştırma, fail tarafından kullanılan bilinçli, kasıtlı ve dikkatli bir biçimde yürütülen bir yaklaşımdır. Uşaklaştırmanın amacı, cinsel istismara olanak sağlamak ve bunu gizli tutmaktır. Uşaklaştırma süreci, failin cinsel istismara hazırlık aşamasında kullandığı çeşitli yöntemleri kapsar. Ayrıca yöntemler, suça maruz kalanın suça ortak edilmesini ve gizliliğini sağlayarak taciz ilişkisinin sürdürülmesine destek olur[163]. Yöntemler neticesinde çocuğun güveninin sağlanması çocuğun istismar edilmesini kolaylaştırıcı bir etki sağlar[164]. Failin uşaklaştırma yöntemlerinde sağladığı başarı, çocuğun cinsel temasını yetkili otoritelere bildirmemesine de neden olmaktadır. Bu durum da faillerin eylemleri karşılığında cezai herhangi bir yaptırıma maruz kalmadan uzaklaşmasını sağlamaktadır[165].

Çocukların cinsel anlamda istismar edilmesinde internet ya da bilişim alanının aracı olarak kullanılması ve bu alanlarda çocukların birer cinsel obje haline getirilmesi suretiyle cinsel sömürüsünün yapılması uluslararası boyutta engellenmesi gereken bir tehlikedir. Bu

157 KNOLL, s. 374. Amerika Birleşik Devletleri Adalet Bakanlığı Cinsel Suçluları Sorgulama, İzleme, Yakalama, Kaydetme ve Takip Etme Bürosu (*SMART*)' na göre uşaklaştırma (*grooming*), bir çocuğa erişim sağlamak ve onunla yalnız kalmaya zaman kazanmak amacıyla çocuk ve çocuğun etrafındaki yetişkinler ile güven inşa etmeyi kapsayan suçluların kullandığı yöntemdir. Bkz. POLLACK, MACIVER, s. 161.

158 CHETOSKY, s. 4.

159 EZIONI, s. 2.

160 EZIONI, s. 2.

161 POLLACK, MACIVER, s. 161.

162 DONICA, CHEW, MAJEED, s. 44-45; CHETOSKY, s. 4, dp.16.

163 KNOLL, s. 374.

164 CHETOSKY, s. 5.

165 CHETOSKY, s. 5.

kapsamda siber uşaklaştırma yöntemlerinin suç olarak kabul edilmesi gerekliliği *Avrupa Konseyi Çocukların Cinsel Sömürü ve İstismara Karşı Korunması Sözleşmesi*[166]' nin "*Çocukların Cinsel Amaçlar İçin Teşvik Edilmesi*" başlıklı 23. maddesinde düzenlenmiştir. Bu düzenlemeye göre: "*Taraflardan her biri, 18. Maddenin 2. Fıkrasının uygulanmasında belirlenen yaşa*[167] *ulaşmamış bir çocuğa, bilgi ve iletişim teknolojileri yoluyla bir yetişkinin, 18. Maddenin 1a*[168] *fıkrası veya 20. Maddenin 1a*[169] *fıkrası uyarınca belirlenen suçlardan herhangi birini işlemek amacıyla kasten buluşma teklifinde bulunmasını, bu teklifi takiben söz konusu buluşmayla sonuçlanacak icra hareketlerinin gerçekleşmesi halinde, suç olarak düzenlemek için gereken yasal ve diğer tedbirleri alır*."

Karşılaştırmalı hukuka bakıldığında Birleşik Krallık (U.K.) Cinsel Suçlar Kanunu 2003, "*Çocuk ile cinsel iletişim*" başlıklı 15A bölümünde, siber uşaklaştırma yöntemlerini kapsar şekilde bir suça yer verilmiştir. Bu düzenlemeye göre [15A/(1)][170], "*18 yaşında ya da daha büyük (A) kişisi şayet,*

(a) cinsel tatmin elde etmek amacıyla A, kasten (bilerek) diğer kişi (B) ile iletişim kurarsa,

(b) iletişim cinsel nitelikte ise ya da B' yi (A ya da bir başkası) ile cinsel nitelikte iletişime geçmeyi teşvik etmeyi amaçlıyorsa,

(c) B 16 yaşının altındaysa ve A, B' nin 16 veya daha büyük bir yaşta olduğuna kabul edilebilir şekilde inanmıyorsa suç işlemiş olur." Singapur Ceza Kanununda (1871)[171] ise, cinsel uşaklaştırma, özel olarak çocukların yaş aralığı dikkate alınarak düzenlenmiştir. Kanunun 376E maddesinde "16 yaşından küçük çocukların cinsel uşaklaştırılması", 376EA maddesinde "16 yaşından büyük olan fakat 18 yaşından küçük olan çocukların sömürücü cinsel

166 Sözleşme 25.11.2010 tarihli ve 6084 sayılı Kanunla onaylanmıştır. Sözleşmenin resmi çevirisi için bkz. R.G., T. 10.09.2011, S. 28050.

167 Sözleşme m. 18/2: "*Yukarıdaki 1. fıkra amacına uygun olarak, taraflardan her biri bir çocukla cinsel faaliyette bulunmanın yasak olduğu yaş alt sınırına karar verir*".

168 Sözleşme m.18/1a'ya göre bu suçlar, kasten işlenen yasal olarak cinsel erginlik yaşına gelmemiş bir çocukla cinsel faaliyetlerde bulunmak, zor/güç/tehdit kullanarak çocukla cinsel faaliyetlerde bulunma, çocuk üzerinde güven, yetki veya etki gerektiren mevkii kullanarak çocuğun istismarı ve zihinsel veya fiziksel özürlülüğü veya bağımlılığı sebebiyle çocuğun savunmasız durumundan yararlanarak istismar suçlarıdır.

169 Sözleşme m.20/1a' ya göre bu suçlar çocuk pornografisi üretimi, teklifi veya sağlanması, çocuk pornografisi dağıtımı veya yayınlanması, kendisi veya başkası için çocuk pornografisi temin etme, çocuk pornografisine sahip olma ve bilgi ve iletişim teknolojileri yoluyla bilerek çocuk pornografisine erişim sağlama suçlarıdır.

170 Cinsel Suçlar Kanunu 2003 (*Sexual Offences Act 2003*) bkz. https://www.legislation.gov.uk/ukpga/2003/42/section/15A (Erişim Tarihi: 10.08.2022).

171 Singapur Ceza Kanunu için bkz. Singapur Devlet İnternet Sayfası (https://sso.agc.gov.sg/, Erişim Tarihi: 10.08.2022).

uşaklaştırılması", 376EB maddesinde "16 yaşından küçük çocukla cinsel iletişime geçme", 376EC maddesinde "16 yaşından büyük olan fakat 18 yaşından küçük olan çocuklarla sömürücü cinsel iletişime geçme" suçlarının düzenlendiği görülmektedir.

TCK açısından bakıldığında çocuğun cinsel uşaklaştırılması yöntemlerinin sanal ortamda kullanılması durumunda failin ceza sorumluluğu farklı suç tipleri ile ilişkilendirilebilecektir. Öncelikle çocuklara karşı cinsel istismar suçu işlemek ya da çıplak fotoğraf göndermesini sağlamakta olduğu gibi cinsel sömürü teşkil edebilecek davranışlara zorlamak için failin çocuk ile sanal ortamlarda arkadaşlık kurması ya da mesajlaşması eylemleri değerlendirilmelidir. Zira siber uşaklaştırma için failin öncelikle çocukla yakınlık kurması ve güven ilişkisi tesis etmesi gerekmektedir. Kanımızca çocuk ile sanal ortamda arkadaşlık etme ve mesajlaşma eylemleri iki açıdan incelenmelidir. Bunlar; çocuk ile cinsel içerikli olmayan görüşmeler ve cinsel içerikli görüşmelerdir.

Amacı cinsel istismar suçunu işlemek olan fail ileride çocuk ile fiziki ortamda buluşmak amacıyla çocukla sanal ortamda (internette) cinsel içerikli olmayan şekilde mesajlaşabilir, görüşebilir, arkadaşlık edebilir, yakınlık ve güven tesis ettikten sonra buluşma teklifinde bulunabilir. Bu gibi eylemlerde cinsel taciz ya da cinsel istismar suçuna teşebbüs etme suçunun oluşup oluşmadığının incelenmesi gerekmektedir. Cinsel istismar suçu açısından bakıldığında TCK m. 103/1-a' da on beş yaşını tamamlamamış veya tamamlamış olmakla birlikte fiilin hukuki anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen "*her türlü cinsel davranış*" cinsel istismar olarak tanımlanmıştır. Acaba fail tarafından güven tesis edilmesi amacıyla çocuk ile gerçekleştirilen yazışmada herhangi bir cinsel içerik olmasa da tek başına yazışma eylemi, çocuğun güveni sağlandıktan sonra buluşma teklif edilmesi ya da fiziken çocukla buluşulması eylemleri "cinsel davranış" olarak kabul edilecek midir? Çalışmanın önceki başlıklarında belirtildiği üzere Yargıtay cinsel istismar suçunun oluşması için gerekli olan cinsel davranışların çocuğun "*vücut dokunulmazlığını*" da ihlal etmiş olmasını aramaktadır. Bu bakımdan bedensel (fiziki) temas içermeyen eylemlerde cinsel istismar suçunun oluşmadığının söylenmesi gerekecektir. Bu noktada sorulması gereken diğer bir soru ise, failin çocukla sanal ortamda cinsel içerikli olmayan yazışması, görüşmesi, ona buluşma teklif etmesi ya da onunla buluşması eylemleri, çocuğun vücut bütünlüğünü ihlal eden bedensel temasa yönelik olmaları sebebiyle cinsel istismar suçunun icra hareketi olarak değerlendirilebilir mi? TCK m. 35' e göre suça teşebbüsten söz edilebilmesi için failin işlemeyi kastettiği suçu elverişli hareketlerle doğrudan doğruya icraya başlaması, fakat elinde olmayan sebeplerle suçu tamamlayamaması gerekmektedir. Dikkat edilecek olursa TCK' da suça

teşebbüs konusunda failin suçu işleme iradesinin açıkça ortaya çıkmış olmasının icra hareketlerinin başlamış olduğunun kabulü için tek başına yeterli olduğu sübjektif teori benimsenmemiştir. TCK m. 35 düzenlemesine bakıldığında objektif teorinin benimsenmiş olduğu görülmektedir. Buna göre suç tipinde belirtilen hareketlerin ve bu hareketlerle zorunlu bağlantı ilişkisi içindeki hareketlerin fail tarafından gerçekleştirilmesi durumunda suçun icrasına başlandığı kabul edilecektir. Bu kapsamda olmayan hareketler ise, kanunun özel olarak suç olarak düzenlememesi durumunda cezalandırılmayan, suçun icrasını kolaylaştıran hazırlık hareketi niteliğindedir. Bu açıklamalar ışığında değerlendirildiğinde iradesi ileride çocuk istismarı suçunu işlemek olan failin çocuk ile cinsel içerikte olmayan yazışması, görüşmesi, buluşma teklifinde bulunması[172] ya da buluşması çocuğun cinsel istismarı suçu açısından hazırlık hareketi niteliğindedir. Yargıtay da kararlarını bu yönde vermektedir[173]. Yargıtay çocuğun kolundan tutularak çekiştirildiği olaylarda bedensel temas olması durumunda dahi, bu

172 "*…sanığın, çocuğun basit cinsel istismarı suçunu, bir suç işleme kararının icrası kapsamında değişik zamanlarda birden fazla işlemediği, sanığın ilk eylemi gerçekleştirdikten sonra başka bir gün mağduru yanına çağırmasına karşılık mağdurun gitmemesi şeklindeki eylemin, belirtilen suçun icra hareketi olarak değerlendirilemeyeceği gözetilmeden, koşulları oluşmadığı halde sanığın cezasının TCK'nın 43/1. maddesi gereğince arttırılması suretiyle fazla ceza tayini,..*" Y. 14. CD., T. 24.03.2016, E. 2016/236, K. 2016/2925.

173 "*…Olay günü sanığın, lojmanın bahçesinde oynayan altı yaşındaki mağdureyi yanına çağırmasının ardından ağlayarak binaya girdiğini görünce takip ettiği ve bu sırada fiziksel bir temasta bulunmadan çevreden gelenlerce yakalandığı tüm dosya kapsamından anlaşılmakla, bu haliyle atılı suçun icrasına henüz başlanmayıp, bu ana kadar ki eylemlerin hazırlık hareketleri aşamasında kaldığı gözetilerek sanığın beraati yerine yazılı şekilde mahkumiyetine karar verilmesi, Kanuna aykırı, sanık müdafisinin temyiz itirazları bu itibarla yerinde görüldüğünden,…*" Y. 14. CD., T. 20.01.2021, E. 2016/8493, K. 2021/343; "*…sanığın mağdureye söylediği cinsel içerikli sözleri müteakip odadan ayrılmasının ardından anılan sözlerden dolayı cinsel saldırıya uğrayacağı korkusuna kapılan mağdurenin kendisini balkonlu odaya kapatarak balkona çıkmasından sonra kapalı kapının zorlanması üzerine sanığın kendisine saldıracağından emin olarak balkon korkuluklarına iyice yaslandığı ve sanık ile tanık ... beyanıyla sabit olduğu üzere tanık ... içeri girip müdahale etmek istediği sırada mağdurenin aşağıya düşmesinden ibaret eylemde, gerek cinsel sözlerin sarf edildiği odadan sanığın ayrılmasına kadar geçen süre içinde, gerekse mağdurenin balkona çıkmasından sonraki süreçte mağdureye yönelik cinsel içerikli sözler söylediği sabit olan sanığın nitelikli cinsel saldırı suçunun hazırlık hareketlerini aşacak mahiyet ve derecede olmak üzere atılı suçun icrai hareketlerine başladığına dair cezalandırılmasına yeter, her türlü şüpheden uzak, kesin ve inandırıcı delil bulunmadığı ve mevcut haliyle eylemin cinsel taciz suçu kapsamında kaldığı gözetilerek bu suçtan hüküm kurulması yerine suç vasfının tayininde yanılgıya düşülerek yazılı şekilde beden veya ruh sağlığını bozacak şekilde nitelikli cinsel saldırı suçuna teşebbüsten mahkumiyet kararı verilmesi,…*" Y. 14. CD., T. 05.04.2017, E. 2017/428, K. 2017/1822; "*…mağdurenin suç tarihinde kardeşiyle birlikte yolda yürüdüğü sırada karşılarına çıkan sanığın, mağdureye yaşını ve adını sorduktan sonra kolundan tutarak çalılıklara sürüklediği, mağdurenin bağırıp çığlık atması ve tanık ...'nın yardım istemesi nedeniyle olay yerine gelen insanların olduğunu görmesi üzerine sanığın mağdureyi bırakarak olay yerinden kaçması şeklinde gerçekleşen olayda, sanık hakkında her ne kadar çocuğun basit cinsel istismarı suçuna teşebbüsten mahkûmiyet hükmü kurulmuş ise de, sanığın o aşamaya kadar çocuğun cinsel istismarı suçunu işlemeye yönelik kastını ortaya koyan herhangi bir söz veya davranışta bulunmadığı, mevcut haliyle eylemlerin cinsel istismar suçuna hazırlık hareketleri niteliği taşıdığı anlaşıldığından çocuğun basit cinsel istismarı suçundan beraati yerine yazılı şekilde mahkûmiyetine karar verilmesi,…*" Y. 14. CD., T. 24.05.2016, E. 2016/2110, K. 2016/5048.

temasın cinsel arzuları tatmin etmeye yönelik hareketlere başlanmış sayılmayacağına hükmetmiştir[174].

Çocuk ile sanal ortamda (internette) cinsel içerikli yazışma yapılması, görüşülmesi ve ardından buluşma teklifinde bulunulması ya da buluşulması durumunda failin ceza sorumluluğu ise farklılık arz edecektir. Ancak failin belirtilen eylemlerden doğan ceza sorumluluğu çocuğa karşı işlenen cinsel taciz suçu ve müstehcenlik suçu çerçevesinde çalışmanın cinsel içerikli yazışma (*sexting*) başlığı altında tartışıldığından burada sadece belirtilmekte yetinilecektir.

SONUÇ

Flört şiddeti, flört ilişkisinde bulunan partnere karşı gerçekleştirilen fiziksel, cinsel, psikolojik ve ekonomik zarara neden olan herhangi bir davranışı ifade etmektedir. Günümüzde bilgi iletişim teknolojilerinin gelişmesi ve internet kullanımının artması ile birlikte flört şiddeti teşkil eden davranışlar bilişim alanına taşınmıştır. Flört şiddetinin bir türü olan "dijital flört şiddeti" kavramı, dijital teknolojileri kullanan flört partnerini kontrol etme, tehdit etme veya ona baskı yapma gibi eylemleri içeren davranışlar için kullanılan genel bir kavramdır. Bu kavram kökeni itibariyle ceza hukukuna ait bir kavram değildir. Ancak dijital flört şiddeti kavramının içerisinde barındırmış olduğu yöntemlere bakıldığında, bu yöntemlerin ceza hukuku ile korunan birçok hukuksal değeri ihlal eden davranışı içerdiği görülmektedir. Bu nedenle ceza sorumluluğunun belirlenmesinde flört ilişkisi içindeki kişinin gerçekleştirmiş

174 "*…Bu eylemin 5237 sayılı TCK'nın 103/1. maddesinde düzenlenen çocuğun basit cinsel istismarı suçunun hazırlık hareketleri niteliği taşıdığı ve henüz cinsel arzuları tatmin etmeye yönelik hareketlere başlanmadığı gözetilmeden, sanık hakkında kişiyi hürriyetinden yoksun kılmaya teşebbüs niteliğindeki eylemi nedeniyle ayrıca çocuğun basit cinsel istismarı suçundan da mahkûmiyet hükmü kurulması,…" Y. 14. CD., T. 24.05.2016, E. 2014/5228, K. 2016/5025; Benzer yönde "…"…sanığın mağdura cinsel ilişki teklif etmesinin cinsel taciz suçunu oluşturduğu, mağdurun reddetmesi üzerine onu kolundan tutup içeri çekmesi eyleminin ise sanığın pasif durumda kalarak gerçekleştirmek istediği cinsel ilişki suçuna hazırlık hareketi sayılıp bu haliyle eylemin açılmış bir dava bulunmayan kişiyi hürriyetinden yoksun kılma suçuna teşebbüsü oluşturacağı gözetilmeden,…*" Y. 14. CD., T. 10.02.2015, E. 2013/5668, K. 2015/916; "*…sanığın kendisine yaklaşıp ben seni tanıyorum, ben de sizin gibi Malatyalıyım diyerek, elinden tutup ileride bulunan halı sahanın diğer tarafına doğru çekmeye çalıştığını, yaklaşık bir metre kadar kendisini çektiğini, kendisinin elini geri çekmesinden sonra kızım sen hasta mısın diyerek tekrar elini tuttuğunu, kendisinin durumdan rahatsız olarak yürümeye devam ettiğini, sanığın arkadan kendisine sahilde çay bahçem var, oraya yalnız gel, başkalarının haberi olmasın, çay bahçesinde kimse olmadığı zaman gel dediğini' ifade etmesi karşısında sanığın eyleminin cinsel istismar suçu açısından hazırlık hareketleri boyutunda kaldığı, cinsel istismar suçunun icra hareketlerine başlanmadığı, ancak cinsel istismar suçu açısından hazırlık hareketi boyutunda olan bu eylemlerden sanığın mağdureyi elinden ve kolundan tutarak istediği yere götürmek istemesi ve bu şekilde mağdureyi bir metre kadar çekiştirmesi eyleminin 5237 sayılı TCK.nın 109/2, 109/3-f, 109/5 ve 35. maddelerinde düzenlenen kişiyi hürriyetinden yoksun kılmaya teşebbüs suçunu oluşturacağı gözetilmeksizin TCK.nın 103/1. maddesi uyarınca hüküm kurulması,…*" Y. 14. CD., T. 27.06.2012, E. 2011/3748, K. 2012/7356.

olduğu yöntemin niteliğine göre, TCK' da ilgili suç tipi çerçevesinde inceleme yapılması gerekmektedir.

Ceza hukuku açısından önem arz eden dijital flört şiddeti teşkil eden yöntemler beş ana başlık altında toplanabilir. Bunlar; 1. *Sanal ortamda flört partnerini kontrol etme ve ona baskı kurmaya yönelik davranışlar*, 2. *Sanal ortamda flört partnerinin itibarına zarar verici davranışlar*, 3. *Sanal ortamda flört partnerinin finansal istismarına yol açacak davranışlar*, 4. *Sanal ortamda flört partnerine ait cinsel içerikli görüntülerin rıza dışı paylaşılması, sahte olarak üretilmesi ya da bu görüntülerin paylaşılması tehdidi, flört partnerine rıza dışı cinsel içerikli yazı ya da görüntü yollama*, 5. *Cinsel sömürü amacıyla sanal ortamda çocuklarla flört ilişkisi veya cinsel temas kurmaya yönelik davranışlar* olarak belirtilebilir.

Dijital flört şiddeti yöntemleri içerisinde sanal ortamda gerçekleştirilen cinsel içerikli yazışma ve görüntülerin rıza dışı paylaşılması, bu materyallerin şantaj ya da korkutma aracı olarak kullanılması gibi yöntemler ön plana çıkmaktadır. Özellikle cinsel içerikli mesajlaşmaya konu olan yazışmalar ya da görüntülerin siber zorbalıkta, cinsel içerikli şantajda ya da flört istismarında kullanılabilmesi, içeriğin sanal ortamda uzun süre kalabilmesi bu eylemlerin çocuklar üzerinde ciddi psikolojik zarara yol açmasına neden olmaktadır. Bu nedenle bu gibi durumlarda özellikle çocuk faillerin cezalandırılmasından çok, belirtilen zararların oluşmasının engellenmesi için çocuklarda farkındalık yaratılması gerekmektedir. Bu kapsamda özellikle çocukların cinsel mahremiyet konusunda bilinçlenmesi ve henüz ceza hukuku devreye girmeden belirtilen zararların ortaya çıkmasının engellenmesi gerekmektedir.

Dijital flört şiddeti yöntemleri içerisinde önemi nedeniyle özellikle belirtilmesi gereken diğer bir yöntem ise çocuğun siber uşaklaştırılmasıdır. Bu yöntemde fail ileride çocuğun cinsel istismarını gerçekleştirmek ya da çocuğun kendisine ait müstehcen görüntüyü üretip yollaması için sanal ortamda onun güvenini kazanmaya çalışmaktadır. Belirtilen amaca ulaşmak için fail tarafından gerçekleştirilen çocuk ile cinsel içerikli olmayan görüşmeler, buluşma teklifinde bulunma ve buluşma eylemi TCK m. 103 çocukların cinsel istismarı suçu açısından cezalandırılmayan hazırlık hareketi niteliğindeki davranışlardır. Söz konusu bu eylemler bazı ülkeler tarafından suç oluşturacak şekilde özel olarak düzenlenmiştir. Ulusal mevzuatımız açısından da belirtilen eylemlerin suç haline getirilmesi tartışılabilecektir. Ancak cinsel içerikli olmayan görüşmelerde ya da çocuk ile buluşma teklif edilmesi gibi davranışlarda failin cinsel istismar amacının mevcudiyeti, failin dış dünyaya yansıyan hareketleri ile açıkça ortaya konulması gerekmektedir. Bu durumun ortaya konulmasının güçlüğü karşısında ceza hukukunun son çare olma özelliği de dikkate alındığında, esas olanın çocukların bu gibi

durumlarda daha bilinçli davranabilmesi ve ailelerin internet kullanan çocuklar üzerinde gerekli gözetim ve kontrolü yerine getirebilmesi gerekliliğidir.

KAYNAKÇA

AKBULUT, B. (2017). Bilişim Alanında Suçlar (2. b.). Ankara.

AKSOY RETORNAZ, E. E. (2021). Bir Siber Taciz Biçimi: Cinsel İçerikli Görüntüleri Rızaya Aykırı Olarak İfşa Etme, Yayma, Erişilebilir Kılma veya Üretme Suçu (Revenge Porn ve Deep Fake). İstanbul.

AKHTAR, Z. (2014). Child Sex Grooming: 'Culture' Crime, Racial Stereotyping and the Environment". European Journal of Crime, Criminal Law and Criminal Justice, 22 (2), 167-196.

AVŞAR BALDAN, G., AKIŞ, N. (2017). Flört Şiddeti. Uludağ Üniversitesi Tıp Fakültesi Dergisi, 43 (1), 41-44.

BABAYİĞİT, B. (2021). Deepfake'in Ceza Hukuku Bakımından Değerlendirilmesi ve De Lege Ferenda Öneriler. Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 25 (4), 655-703.

BRITISH COLUMBIA SOCIETY OF TRANSITION HOUSES (2021). Responding to Teen Digital Dating Violence: BC Anti-Violence Worker Surwey Results (Technology Safety Project).

CANBERK, G., SAĞIROĞLU, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22 (1), 121-136.

CARLTON, A. (2020). Sextortion: The Hybrid "Cyber-Sex" Crime, North Carolina Journal of Law & Technology, 21 (3), 177-215.

CHETOSKY, K. K. (2019). Minnesota v. Muccio: The Constitutionality of Minnesota's Sexual Grooming Law. Northwestern University Law Review Online, 114, 1-22.

CITRON, D. K. (2019). Sexual Privacy. Yale Law Journal, 128(7), 1870-1961.

DONICA, T. L. H., CHEW, W. X., MAJEED, K. (2015). Understanding the behavioral aspects of cyber sexual grooming: Implications for law enforcement. International Journal of Police Science & Management, 17(1), 40-49.

DOUGLAS, D. M. (2016). Doxing: a conceptual analysis. Ethics and Information Technology, 18, 199-210.

DÜLGER M. V. (2022). Bilişim Suçları ve İnternet İletişim Hukuku (9. b.). Ankara.

ERALP, Ö. (2007). Hukukçular İçin Bilişim Terimleri Sözlüğü. Ankara.

EZIONI, L. (2020). The Crime of Grooming. Child and Family Law Journal, 8 (1), 1-18.

GILLESPIE, A. A. (2013). Adolescents, Sexting and Human Rights. Human Rights Law Review, 13 (4), 623-644.

GÖKCAN H. T., ARTUÇ M. (2021). Yorumlu-Uygulamalı Türk Ceza Kanunu Şerhi (Cilt 1-6). Ankara.

HAFIZOĞULLARI, Z., ÖZEN, M. (2017). Türk Ceza Hukuku Özel Hükümler: Topluma Karşı Suçlar. Ankara.

HINDUJA, S., PATCHIN, J. W.. Digital Dating Abuse: A Brief Guide for Educators and Parents. Cyberbullying Research Center, (cyberbullying.org, Erişim Tarihi: 10.04.2022).

KETİZMEN, M.(2008). Türk Ceza Hukukunda Bilişim Suçları. Ankara.

KNOLL, J. (2010). Teacher Sexual Misconduct: Grooming Patterns and Female Offenders. Journal of Child Sexual Abuse, 19 (4), 371-386.

KOCA, M. (2009). Hukukumuzda TCK'nun 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını. Ankara.

KOCA, M., ÜZÜLMEZ İ. (2019). Türk Ceza Hukuku Özel Hükümler (6. b.). Ankara.

MINOR, A. D. (2016). Sexting Prosecutions: Teenagers and Child Pornography Laws. Howard Law Journal, 60 (1), 309-324.

MOHAN, S. C., LEE Y. (2020). Sexual Grooming as an Offence in Singapore. Singapore Academy of Law Journal, 32 (1), 96-123.

MULDAVIN, K. (2019). Cruel to be kind: The societal response to technology and youth sexual expression. Lewis & Clark Law Review, 23 (1), 425-463.

ÖZBEK, V. (2009). Müstehcenlik Suçu (TCK m. 226). Ankara.

POLAT, O. (2016). Şiddet. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 22 (1), 15-34.

POLLACK, D., MACIVER, A. (2015). Understanding Sexual Grooming in Child Abuse Cases. Child Law Practice. 34 (11), 161-168.

RODRIGUEZ-DEARRIBA, M.L., NOCENTINI, A. L., MENESINI, E., SANCHEZ-JIMENEZ, V. (2021). Dimensions and measures of cyber dating violence in adolescents: A systematic review. Aggression and Violent Behavior, 58, 1-10.

SNYDER, P., DOERFLER, P., KANICH, C., MCCOY, D. (2017). Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. IMC (Internet Measurement Conference), November 1-3. London.

SWEENY, J. (2012). Sexting and Freedom of Expression: A Comparative Approach. Kentucky Law Journal, 102 (1), 103-146.

TEZCAN, D., ERDEM, M. R., ÖNOK, R. M. (2020). Teorik ve Pratik Ceza Özel Hukuku (18 b.). Ankara.

WEBB, T. (2013-2014). The Brave New World of Cyber Crime Investigation and Prosecution. Nexus: Chapman's Journal of Law and Policy, 19, 77-86.

WILKERSON, J. J. (2021). Revenge Porn: State Laws, Constitutional Challenges, and the Progress of Federal Legislation. University of Louisville Law Review, 60 (2), 301-330.

WORLD HEALTH ORGANIZATION (WHO) (2002). World report on violence and health. (Etienne G. Krug, Linda L. Dahlberg, James A. Mercy, Anthony B. Zwi and Rafael Lozano, Düzenleyenler) Geneva.

WORLD HEALTH ORGANIZATION (WHO) (2013). Global and regional estimates of violence against women: prevalence and health effects of intimate partner violence and non-partner sexual violence. Geneva.

YAZICIOĞLU, R. Y. (2009). Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi. 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını. Ankara.

YILDIZ, M. E. (2015). Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu. Ankara.

YILDIZ, M. E. (2010). İnternet Bankacılığı Hakkında Yargıtay'ın 17.11.2009 Tarih, 2009/11-193 Esas Sayılı Kararının İncelenmesi. Ceza Hukuku Dergisi, 14 (5), 129-150.

İnternet Kaynakları

Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi Resmi Çevirisi, Türkiye Büyük Millet Meclisi, Yasama Dönemi: 24, Yasama Yılı: 3, Sıra Sayısı: 380, (https://www5.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf, Erişim Tarihi: 11.04.2022).

Birleşik Krallık Cinsel Suçlar Kanunu 2003 (*Sexual Offences Act 2003*) https://www.legislation.gov.uk/ukpga/2003/42/section/15A (Erişim Tarihi: 10.08.2022).

Birleşik Krallık Çocukların Korunması Kanunu 1978 (https://www.legislation.gov.uk/ukpga/1978/37 (Erişim Tarihi: 29.07.2022).

Kalifornia Ceza Kanunu https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=8.&article= (Erişim Tarihi: 10.08.2022).

Pensilvanya Ceza Kanunu https://www.legis.state.pa.us/cfdocs/legis/LI/consCheck.cfm?txtType=HTM&ttl=18&div=0&chpt=63&sctn=21&subsctn=0 (Erişim Tarihi: 29.07.2022).

Singapur Ceza Kanunu Singapur Devlet İnternet Sayfası (https://sso.agc.gov.sg/, Erişim Tarihi: 10.08.2022).

Yargıtay Kararları (https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/) – Çalışmada alıntı kaynağı belirtilmeyen tüm kararlara Yargıtay Başkanlığı web sitesinden erişilmiştir.