www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 2, Sayı: 1

Geliş: 11.06.2020
Kabul: 29.06.2020

Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu (TCK Md. 136)

Hasan, Sınar
Altınbaş Üniversitesi/Hukuk Fakültesi/Kamu Hukuku Bölümü/Ceza ve Ceza Muhakemesi Hukuku ABD, İstanbul, Türkiye, hasan.sinar@altinbas.edu.tr
ORCID: https://orcid.org/0000-0002-7554-1528

ÖZ
Kişisel verilerin korunması günümüzde tüm gelişmiş hukuk sistemlerinin gündeminde olan bir konudur ve bu amaçla çok çeşitli yasal düzenleme çalışmaları yapılmaktadır. Bu kapsamda, Türk hukukunda 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda (TCK) kişisel verilerin ceza normlarıyla korunması için yeni suç tipleri ihdas edilmiştir. Bu çalışmanın konusunu oluşturan kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu (TCK md. 136) da bu kapsamda yer alır. Bununla birlikte, Türk hukukunda 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yürürlüğe girmesi ile kişisel verilerin korunmasında yeni bir aşamaya gelinmiştir. Bu çalışmada, esas itibarıyla TCK md. 136'da yer alan suç tipinin yapısal unsurları ele alınacaktır. Ayrıca sonuç bölümünde, kişisel verilerin ceza normlarıyla korunmasının günümüzdeki gerekliliği konusu da değerlendirilecektir.

Anahtar Kelimeler: Kişisel Veri, Hukuka Aykırı, Verme, Yayma, Ele Geçirme, Suç

The Offence of Unlawfully Giving, Disseminating or Obtaining of Personal Data (TPC Art. 136)

ABSTRACT
The protection of personal data is in the agenda of all contemporary legal systems and several legislations have carried out within this aim. In this context, new offences created for the protection of personal data with criminal provisions in Turkish Penal Code (TPC) Numbered 5237 which enacted in 2005. The offence of unlawfully giving, disseminating or obtaining of personal data (TPC Art. 136) which is the subject of this study is also a part of these criminal provisions. However, the legal protection of personal data reached to a new era in Turkish law, after entering in force of The Protection of Personal Data Act Numbered 6698 in 2016. In this study, basically, the legal elements of the offence designed in TPC Art. 136 will be examined. Moreover, the necessity of the criminal protection of personal data will be evaluated in the conclusion part.

Keywords: Personal Data, Unlawful, Giving, Disseminating, Obtaining, Offence.

Atıf Gösterme Sınar, H. (2020). Kişisel Verileri Hukuka Aykırı Olarak Verme, Yayma Veya Ele Geçirme Suçu (TCK md. 136), *Kişisel Verileri Koruma Dergisi. 2*(1), 33-62.

GİRİŞ

Kişisel verilerin hukuk düzeni tarafından himaye gören bir hukuksal değer olarak kabul edilmesi bazı gelişmiş ülkelerde göreceli olarak uzunca bir geçmişe sahip olsa da; bilişim teknolojilerindeki gelişmelere paralel olarak kişisel verilerin gerek elde edilmesine gerekse işlenmesine ve paylaşılmasına ilişkin süreçlerin olağanüstü hız kazanması ve bu itibarla kişisel verilerin evrensel düzeyde asimetrik biçimde yayılması, kişisel verilerin korunması gerekliliğinin tüm dünyada tartışılmasına yol açmıştır. Bu konuda ulusal üstü düzeyde 1981 tarihli 108 sayılı Avrupa Konseyi Sözleşmesi ile ulusal üstü düzeyde yeni bir açılım yaratan ve ardından Avrupa Birliği'nin 1995 tarihli (95/46/AT) sayılı Yönergesi ile ilerleyen süreç, 2016 yılında 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü ile yeni bir aşamaya taşınmıştır. Ulusal düzeyde ise uzunca bir hazırlık sürecinin sonucunda 2016 yılında spesifik olarak kişisel verilerin korunması konusuna özgülenmiş bir özel kanun olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) yürürlüğe girmiştir.

Kişisel verilerin korunması teknik boyutu bir hayli ağırlıklı olan ve disiplinler arası niteliği ağır basan yeni bir alandır ve bu itibarla pek çok hukuk dalı ile doğrudan ilişkilidir. Ancak kişisel verilerin korunmasının ceza hukukuyla olan ilişkisine, diğer hukuk dallarıyla olan ilişkisinden daha farklı bir parantez açmak gerekir. Çünkü Türk hukuku yönünden kişisel verilerin hukuk düzeni tarafından himaye görmesi noktasında ceza hukukunun pozitif ayrışan bir özelliği vardır. Şöyle ki, Türk ceza hukuku mevzuatına ilişkin olarak 21. yüzyılın ilk yıllarında ortaya çıkan yeniden kodifikasyon hareketi kapsamında 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nda (TCK), kişisel verilerin korunmasına ilişkin spesifik suç tipleri (TCK md. 135-139) ihdas edilmiş bulunmaktadır. Bilindiği üzere, ceza hukukunda *ultima ratio* prensibi geçerlidir ve bu prensip uyarınca, ceza hukuku ancak toplumsal düzenin sürdürülebilmesi için korunması zorunlu bulunan hukuksal değerleri konu alır ve bu hukuksal değerler yönünden diğer hukuk dallarıyla sağlanan korumanın yetersiz kalması durumunda devreye girerek bunları ceza normu ile düzenlemek suretiyle himaye eder. Bu durumda, kişisel verilerin özel bir kanun ile düzenlenmesinden yıllar önce, ceza kanunu tarafından bir hukuksal değer olarak kabul edilerek spesifik suç tipleri ile himaye altına alınmış olması, kanun koyucunun vizyoner bir bakış açısıyla kişisel verilerin korunmasına verdiği önemi vurgulaması bakımından fevkalade değerlidir. Bununla birlikte, kişisel verilerin toplumsal yaşamdaki ağırlığının artmasıyla birlikte bu konuda ihdas edilmiş olan spesifik düzenleme olan KVKK'nın yarattığı farkındalık bir bütün olarak değerlendirildiğinde; bugün artık kişisel verilerin ceza kanunu tarafından aynı şekilde himaye görmeye devam etmesinin mi yoksa ceza kanununun bu alandan tamamen çekilerek, kişisel verilerin himayesi görevinin tümüyle KVKK tarafından gerçekleştirilmesinin mi daha yararlı olacağı hususlarının süreç içerisinde bilimsel zeminde tartışmaya açılmasında yarar olduğu düşüncesindeyiz.

İnceleme konumuzu oluşturan, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu ise teknolojik ilerlemelerin etkisiyle, kişisel verilerin birçok farklı amaç ile çok çeşitli kişi ve kuruluşlara çok kolaylıkla ulaştırılabildiği gerçeğini dikkate alarak, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi fiillerinin cezalandırılmasını amaçlamaktadır. Bu çalışmada, TCK md. 136'da düzenlenmiş olan bu suç tipinin yapısal unsurlarının, uygulamadan örnekler ışığında incelenmesi ve suç tipinin uygulanmasıyla ilişkili hukuksal sorunların irdelenerek çözüm önerilerinin ortaya konulması yoluna gidilecektir.

KORUNAN HUKUKİ YARAR

Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçuyla korunan hukuksal yararın tespitindeki ilk olarak normlar hiyerarşisinin gereklerine uygun olarak normlar piramidinin en üst basamağında yer alan Anayasa'dan yola çıkılmalıdır. Çünkü normlar hiyerarşisinin en üst basamağında yer alan Anayasa hükümleri, alt basamaklarda yer alan tüm yasal düzenlemeler açısından bağlayıcı bir nitelik taşır ve bu düzenlemelerin Anayasa'da belirtilen hususlara aykırı bir hüküm içermesi mümkün değildir. Bu açıdan özellikle temel hak ve özgürlüklere ilişkin anayasal düzeyde bir düzenlemenin yapılmış olması hukuk düzeninin öngördüğü en yüksek güvence ile koruma sağlanması anlamını taşır.

1982 Anayasası'nın "*Kişinin Hak ve Ödevleri"*ni düzenleyen 2. kısmının 20. maddesi *"Özel Hayatın Gizliliği"* başlığını taşır ve bu başlık altında kişinin özel hayatı ve aile hayatı temel haklar arasında sayılmıştır. Buna karşın, 1982 Anayasası'nın orijinal şeklinde kişisel verilerin korunmasının bağımsız bir hak kategorisi olarak temel haklar arasında düzenlenmesi söz konusu değildir. Bu nedenle, belirtilen süreçte kişisel verilerin Anayasa'da düzenlenen insan onuru ve kişilik hakkı kapsamında korunduğu düşüncesi kabul edildiği gibi özel hayatın gizliliği ve korunması hakkı kapsamında himaye edildiği düşüncesi de ileri sürülmüştür (Şimşek, 2008; Yaşar, Gökcan ve Artuç, 2014).

Bununla birlikte, bilişim teknolojisindeki gelişmelerin kişisel verilerin toplumsal yaşamdaki önemini ve ağırlığını artırması ile birlikte, kişisel verilere yönelen müdahalelerin düzenlenmesi ve sınırlanması noktasında anayasal düzeyde bir himayenin gerekliliği ortaya çıkmıştır. Bu durumun neticesi olarak ise, 07.05.2010 tarihinde 5982 sayılı Kanun'un 2. maddesiyle, Anayasa'nın "*Özel Hayatın Gizliliği*" başlığını taşıyan 20. maddesine spesifik olarak kişisel verilerin korunması hakkını düzenleyen aşağıdaki fıkra eklenmiştir:

"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, Bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar, kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Kişisel verilere anayasal düzeyde koruma sağlayan bu düzenlemenin gerekçesinde ise Anayasada kişisel verilerin korunmasına yönelik dolaylı hükümler bulunmakla birlikte, mukayeseli hukukta ve tarafı olduğumuz uluslararası belgelerde de kişisel verilerin korunmasının önemle vurgulandığı ve bu maddeyle herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak teminat altına alındığı ifade edilmiştir.

Şu hâlde 2010 Anayasa değişikliği ile getirilen bu düzenleme ile kişisel verilerin korunması hakkı her ne kadar özel hayatın gizliliği altında düzenlenmiş olsa da, anayasal düzeyde tanınmış ve teminat altına alınmış bir hak olma özelliği kazanmıştır (Kama Işık, 2020).

Bu verilerin ışığında TCK md. 136'da düzenlenen suç tipi ile korunan hukuksal yararı tekrar ele aldığımızda, kişisel verilerin korunması hakkını ayrı ve bağımsız bir hak kategorisi olarak değerlendirmeyen görüşlere iştirak etmenin artık mümkün olmadığı düşüncesindeyiz. Bu çerçevede, öğretide ortaya konulduğu üzere, TCK md. 136 ile özel hayatın gizliliği veya korunması hakkının korunduğunu veya bu suç ile korunan hukuksal yararın genel kişilik hakkı ile bağlantılı olarak ele alınması gerektiğini ya da bu suç ile korunan yararın mülkiyet hakkı ve iletişim hakkı yönünden değerlendirilmesi yönündeki görüşlere katılamıyoruz (Özbek, Doğan, Bacaksız ve Tepe, 2017; Yaşar, Gökcan ve Artuç, 2014; İtişgen, 2015; Bayraktar ve ark., 2018).

Gerçekten 2010 yılında yapılan anayasa değişikliği ile kişisel verilerin korunması hakkı anayasal güvence altına alınırken bir özgürlük olarak değil ancak bir hak alanı olarak düzenlenmiştir. Diğer bir ifadeyle, bir dokunulmazlığı ifade eden özgürlük olarak değil ancak bir talep edilebilirliği ifade eden hak alanı olarak düzenlenmiş olması, veri ilgilisine kişisel verilerine ilişkin olarak bilgilendirilme, verilere erişme, verilerin hatalı olması durumunda düzeltilmesini isteme, gerektiğinde silinmesini isteme ve hangi amaçla işlendiğinin öğrenilmesi gibi çok geniş bir yelpazede talepte bulunabilme ayrıcalığını getirmiştir (Tanör ve Yüzbaşıoğlu, 2012). Bunun yanı sıra veri işleme koşullarının da düzenlenerek kişisel verilerin korunması hakkına ilişkin düzenlemelerin kanunla yapılması esasının öngörülmesi, kişisel verileri kamu otoritelerinin keyfi ve ölçüsüz müdahalelerine karşı koruma altına alınmış bulunmaktadır (Dülger, 2020). Görüldüğü üzere, bu anayasal koruma mekanizmasının sonrasında artık kişisel verilerin korunması alanı, her ne kadar iletişim hakkı, kişilik hakkı ve bilhassa özel hayatın gizliliğinin korunması hakkı ile olan yakın ilişkisi yadsınamaz olsa da; artık bunlardan ayrı bir hak kategorisi oluşturmaktadır ve giderek kendine özgü dinamikleri olan bir bağımsız bir disiplin olma yolunda ilerlemektedir. Keza öğretide kişisel verilerin korunması hakkı; bilim ve teknolojinin olası kötüye kullanılmalarına karşı insanı korumayı amaçlayan dördüncü kuşak haklar içerisinde değerlendirilmeye başlanmıştır (Uygun, 2015). Bu açıdan, teknolojik gelişmelerin katkısıyla modern toplumsal yaşamda giderek ön plana çıkan kişisel verilerin korunması alanının, kişilik hakkının ya da özel hayatın gizliliği ve korunması hakkından giderek ayrıştığı ve bu anlamda belirtilen hak kategorilerinin korunmasın ilişkin mekanizmaların, kişisel verilerin korunması alanındaki gereksinime yanıt veremedikleri tespit edilebilir. Bu anlamda söz gelimi KVKK kapsamında düzenlenmiş bulunan alenileştirilmiş kişisel verilerin ya da kamusal alanda elde edilmiş kişisel verilerin, kişilik hakkı ile izahı mümkün bulunmadığı gibi, bu gibi kişisel verilerin özel hayatın gizliliği ve korunması hakkının getirdiği koruma alanının da açıkça dışında kaldığı belirlenebilir. Ancak bu tarz durumların da bireyin kişisel verileri üzerindeki hâkimiyet alanına dâhil olmaları nedeniyle, kişisel verilerin korunması hakkı kapsamında bu hakka ilişkin tüm gereksinimleri aynı şemsiye altında toplayabilen özgün bir koruma mekanizmasının tanınmasına gereksinim bulunmaktadır (Börekçi, 2019).

Şu halde sonuç olarak, bugün için TCK md.136'da düzenlenen suç tipi ile korunan hukuksal yarar, anayasal düzeyde güvence altına alınmış bağımsız bir hak kategorisi olan kişisel verilerin korunması hakkıdır. Burada ayrıca belirtilmesi gereken bir husus ise bu suç tipi ile yalnızca kişisel verilerin kendisinin değil ancak bilhassa verme ve yayma şeklindeki hareket biçimleri ile ifade edilen, kişisel verilerin işlenmesi hususunun özel olarak düzenlenmiş ve koruma altına alınmış olmasıdır.

Nihayet belirtelim ki, kişisel verilerin korunması hakkı bağlamında gerek inceleme konumuzu oluşturan TCK md.136 ve gerekse ceza kanununda kişisel verileri korumaya yönelmiş diğer suçlar yönünden, bu şekilde bir hukuksal yararın sahiplenilmesi, aslında felsefi bir bakış açısıyla, modern insanın teknolojik ilerleme karşısında kendisini koruma içgüdüsünün hayata geçirilmesi anlamını taşımaktadır. Çünkü içinde yaşadığımız modern dünyada, bireyin artık teknolojik gelişmeleri ve bu gelişmelerin yarattığı bilgi toplumunu reddetme gibi bir imkânı olmadığı gibi, kendisini bu süreçte azade kılmayı seçme gibi bir lüksü de bulunmamaktadır. Oysa teknolojik bilgi toplumunda, bireylerin kişisel verileri geniş bir yelpazeye yayılmış çok çeşitli merkezler tarafından sürekli ve çok boyutlu bir tehdidin altındadır (Dülger, 2020). Kişisel verilerin çok boyutlu, etkin ve etkili bir biçimde toplanabilmesi, işlenebilmesi ve yayılabilmesi imkânını yaratan bu teknolojik tehdit sürecinde, adeta kuşatılmış bir biçimde sürekli izlenildiğini ve gözetlendiğini hisseden insanın verebileceği en doğal ve meşru tepki, kendi mahrem yaşam alanını korumaya çalışmaktır. İşte, inceleme konumuzu oluşturan TCK md.136 ve kişisel verilerin korunmasına özgülenmiş diğer suç tiplerinin ihdas edilmesi suretiyle, esas itibarıyla bireyin kendi mahremiyetini imkân ölçüsünde koruyarak modern toplumsal yaşam içerisindeki varlığını huzur içerisinde devam ettirebilmesi amaçlanmaktadır.

SUÇUN YAPISAL UNSURLARI

Suçun yapısal unsurları, bütün suçlar bakımından ortak olan ve bulunmadıkları zaman suçun oluşmasını engelleyen, genel nitelikteki unsurlardır. Bununla birlikte, bir suçun genel ve kurucu unsurlarının nelerden ibaret olduğu ya da diğer bir ifadeyle suçun hangi yapısal unsurlardan müteşekkil olduğu hususu konusunda ceza hukuku öğretisinde bir görüş birliği bulunmamaktadır. Bu görüş ayrılığı, suçun yapısal unsurların kaça ayrılarak incelenmesi noktasında ortaya çıktığı gibi; suçun aynı sayıda unsurdan oluştuğunu kabul eden yazarlar arasında da, bu unsurlara verilen anlam konusunda bir mutabakatın oluşturulabilmesi de mümkün olmamıştır. Bu açıdan suçun yapısal unsurlarının gerek sayısı gerekse anlam ve içeriği yazardan yazara değişkenlik gösterir (Artuk, Gökcen, Alşahin ve Çakır, 2017).

Bu açıdan, geçmişteki suç tipi incelemelerimizde olduğu gibi, inceleme konumuzu oluşturan suç tipi yönünden de yapısal unsurların, maddi unsurlar, manevi unsurlar ve hukuka aykırılık şeklindeki üçlü ayrıma uygun bir biçimde incelenmesi yöntemi tercih edilmiştir.

Maddi Unsurlar

Suçun Konusu

Suçun konusu, kanuni tipe uygun hareketin üzerinde gerçekleştirildiği maddi şeydir (Özbek, Doğan, Bacaksız ve Tepe, 2016). Kişisel verileri hukuka aykırı olarak verme, yayma ve ele geçirme suçunun konusu da, kişisel verilerdir.

Normatif düzeyde ele aldığımızda, ilk olarak 108 sayılı Avrupa Konseyi Sözleşmesi'nde (AKS) kişisel veri kavramı "kimliği belirli veya belirlenebilir gerçek kişi hakkındaki tüm bilgiler" olarak tanımlanmıştır (m. 2/1-a). Avrupa İnsan Hakları Sözleşmesi'nde ve 1982 Anayasası'nda kişisel verilere ilişkin bir tanım bulunmamasına karşın, gerek Avrupa İnsan hakları Mahkemesi (AİHM) içtihatlarında, gerekse Anayasa Mahkemesi (AYM) bireysel başvuru kararlarında, kişisel verilerin, 108 sayılı AKS'deki tanım ile uyumlu bir biçimde tanımlandığı ifade edilebilir (Börekçi, 2019).

Bu bakımdan ulusal düzenlemelere geçmeden önce konunun kapsamının anlaşılması bakımından Avrupa İnsan Hakları Mahkemesinin kişisel verilere yaklaşımına değinilmesi de yerinde olacaktır. Avrupa İnsan Hakları Mahkemesi de kişisel verilere yönelik olarak teknolojinin getirdiği tehditlere karşı kayıtsız kalmamış ve kişisel verilerin devlet tarafından kişinin rızası dışında veya rızası olsa dahi belirli ölçütlere aykırı olarak toplanmasının veya saklanmasının özel hayat kapsamında değerlendirileceğini belirtmiştir (Kilkelly, 2007; Tezcan, Erdem, Sancakdar ve Önok, 2014; Salihpaşaoğlu, 2013). Keza Mahkeme'ye göre, bir kişinin özel yaşamına ilişkin bilgilerin kaydedilmesi 8. madde kapsamında olup bilgilerin kullanılmasına gerek dahi yoktur (Case of Amann v. Switzerland, App. No: 27798/95). Yine Mahkeme; devletin - tıpkı özel hayat gibi - kişisel verilere ilişkin olarak hem negatif (Leander v. Switzerland, App. No: 9248/81) hem de pozitif yükümlülüklerinin (Gaskin v. United Kingdom, App. No: 10454/83; M.G. v. United Kingdom, App. No: 39393/98) bulunduğunu ve bu yükümlülüklere aykırı olarak gerçekleştirilen keyfi müdahalelerin 8. maddeyi ihlal anlamı taşıyacağını belirtmiştir (Aktaş, 2017).

Mahkeme önüne gelen bazı somut olayları, "kişisel veri" kapsamında değerlendirmiş ve bir nevi kavramın içerisini içtihatları ile zenginleştirmiştir. Buna göre Mahkeme; cinsiyet, doğum yeri, medeni hal gibi bilgilerin zorla toplandığı nüfus sayımlarını ve aile kayıtlarını (Case of X. v. United Kingdom, App. No: 9072/82; Godelli v. Italy, App. No: 33783/09), parmak izleri ve DNA profillerini (Case of S. and Marper v. The United Kingdom, App. No: 30562/04 and 30566/04; Case of M.K. V. France, App. No: 19522/09), tıbbi verileri (Case of Z. v. Finland; App. No: 22009/93; M.S. v. Sweden, App. No:

20837/92; Case of Y.Y. v. Russia, App. No: 40378/06; P. and S. v. Poland, App. No: 57375/08; L.H. v. Latvia, App. No: 52019/07; Case of L. L. v. France, App. No: 7508/02; Case of I. v. Finland, App. No: 20511/03, Case of Radu V. The Republic Of Moldova, App. No: 50073/07; Mitkus v. Latvia, App. No: 7259/03), iletişim numaralarını (Case of X v United Kingdom, App. No: 9072/82), telefon görüşmelerinin izlenmesini ve saklanmasını (Malone v. United Kingdom, App. No: 8691/79; Case of Amann v. Switzerland, App, No: 27798/95; Case Of Bărbulescu V. Romania, App. No: 61496/08), kamuya açık alanlarda görüntü yakalayan kameralarda yer alan görüntüleri (Peck v. United Kingdom, App. No: 44647/98; Köpke v. Germany, App. No: 420/07), dini veya ailevi bilgilerini (Tsavachidis v. Greece, App. No: 28802/95; Fernandez Martinez v. Spain, App. No: 56030/07), mahkûmların ziyaretleri sırasında yakınları ile görüşmelerinin kayda alınmasını (Wise v. Fransa, App. No: 71611/01; Szuluk v. The United Kingdom, App. No: 36936/05), polis tarafından tutulan kayıtları (Case of Murray v. United Kingdom, App. No: 14310/88; P. G. and J. G. v. United Kingdom, App. No: 44787/98; Case of Szabó And Vıssy V. Hungary, App. No: 37138/14; Case of Rotaru v Romania, App. No: 28341/95; M.M. V. The United Kingdom, App. No: 24029/07. Shimovolos v. Russia, App. No: 30194/09), mahkemede delil olarak sunulan belgeleri (Panteleyenko v. Ukraine, App. No: 11901/02; Apostu v. Romania, App. No: 22765/12) kişisel veri kapsamında değerlendirmiştir (Kosta, 2013).

Ulusal düzeyde ise 6698 sayılı KVKK'da (md. 3/2b-d) ise, yine AKS ve AİHM içtihatları ile paralel olarak kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. KVKK'daki tanım çerçevesinde kişisel veri kavramından yalnızca bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin olarak teşhis edilebilmesini sağlayan bilgilerin değil; ancak aynı zamanda fizikî, ailevî, ekonomik, sosyal ve sair özelliklerine ilişkin bilgilerin de kişisel veri olarak kabul edildiği sonucuna ulaşılır.

Kişisel verilerin kapsamına ilişkin olarak KVKK'nın madde gerekçesinde de, özetle; kişinin fizikî, ekonomik, kültürel veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm hallerin bu kapsamda olduğu ifade edilmiştir. Nitekim gerekçede isim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi verilerin belirli veya belirlenebilir kılma özelliklerinin bulunması nedeniyle kişisel veriler oldukları belirtilmiştir (Çekin, 2019).

Kişisel veri kavramının ceza hukukunda yorumlanmasına ilişkin olarak her ne kadar 5237 sayılı TCK, Türk hukukunda kişisel verilerin korunmasına ilişkin kanun düzeyindeki ilk metin olma özelliğini gösterse de, TCK'nın tanımlar başlıklı 6. maddesinde bir kişisel veri tanımına yer verilmemiştir. Buna karşın, TCK md.135'de düzenlenen kişisel verilerin kaydedilmesi suçunun gerekçesinde bir tanım yer almış ve kişisel veri "gerçek kişiyle ilgili her türlü bilgi" olarak tanımlanmıştır.

İnceleme konumuzu oluşturan TCK md.136'ya ilişkin olarak, suçun konusunu oluşturan kişisel verinin maddede açıkça tanımlanmamış olması ve -KVKK'nın yürürlüğe girmesinden önceki süreçte 108 sayılı AKS'de yer alan - "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" şeklindeki tanım esas alınarak uygulama yapılmasının belirlilik ilkesini ihlal ettiği gerekçesiyle, Anayasaya aykırılık başvurusu yapılmıştır. Bu başvuruyu inceleyen Anayasa Mahkemesi, özetle, teknolojik gelişmelere bağlı olarak sürekli gelişen kişisel veri kapsamına giren tüm verilerin kanun koyucu tarafından önceden öngörülmesinin ve tek tek sayılmasının mümkün olmadığı, ancak bu kavramın çerçevesinin ulusal, uluslararası mevzuat ile yargı içtihatları tespit edilmiş olması nedeniyle belirlilik ilkesine aykırılık oluşturmadığı ve ayrıca bu maddenin kanuni tanımında gerek tipe uygun eylemin ve gerekse uygulanacak yaptırımın açıkça düzenlenmiş bulunduğu gerekçeleriyle, TCK md.136 düzenlemesini Anayasa'ya aykırı bulmamıştır (AYM Kararı, E. 2015/32, K. 2015/102, T. 12.11.2015, Resmî Gazete 02.12.2015, Sy: 29550). Bu kararın bir yansıması olarak Yargıtay da; "Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı

bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir" şeklindeki müstakar içtihatları ile kişisel verilere ilişkin genel bir çerçeve oluşturma yoluna gitmiştir (Y. 15. CD., E. 2019/8797, K. 2019/15711, T. 26.12.2019; Y. 12. CD., E. 2018/8466, K. 2019/9054, T. 18.09.2019; Y. 12. CD., E. 2018/8144, K. 2019/8317, T. 10.07.2019). Keza Yargıtay Ceza Genel Kurulu da TCK'nın 135 ve 136. maddelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerde sadece sır niteliğinde kişisel verilerin korunacağına ilişkin bir hükmün bulunmaması ve aksine 135. maddenin gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri olarak kabul edilmesi gerektiğini belirtmiştir (YCGK., E. 2012/1510, K. 2014/331, T. 17.06.2014).

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu düzenleyen TCK md.136'nın madde başlığında "verileri" terimini kullanan kanun koyucunun, madde içeriğinde suçun konusu olarak "kişisel verileri" terimini kullanması kanun yapma tekniği açısından doğru olmamıştır. Çünkü veri ve kişisel veri birbirinden farklı anlama sahip kavramlardır. Veri, bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan okuyup tekrar işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgidir (Dülger, 2018). Buna karşın, yukarıda değinildiği üzere, verinin bir gerçek kişiyle ilgili olması ve onun kimliğini belirli veya belirlenebilir kılması halinde ise kişisel veri söz konusu olur. Bu nedenle, TCK md.136'daki suçun konusunun kişisel veriler olduğu göz önüne alınarak madde başlığındaki terimin de, "kişisel veri" şeklinde düzeltilerek yeknesaklık sağlanması hem kanun yapma tekniği açısından hem de kanunilik ilkesinin gereklerine uyulabilmesi yönünden daha doğru olacaktır (Çekin, 2019; Korkmaz, 2019).

Bununla bağlantılı olarak, tüzel kişiye ait olan verilerin veya gerçek kişiye ait olmakla birlikte gerçek kişinin tek başına üzerinde tasarrufta bulunabilmesi mümkün olmayan, ticari sır kavramı kapsamına giren verilerin bir başka kişiye verilmesi, yayılması veya başka kişi tarafından ele geçirilmesi durumunda, bu veriler TCK md.136'daki suçun konusunu oluşturmadığı için söz konusu suç da oluşmaz. Ancak bu durumda, tüm yasal koşullarının gerçekleşmesi kaydıyla, TCK md.239'da düzenlenen ticarî sır, bankacılık veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması suçunun oluşması söz konusu olabilir (Kangal, 2019; Özbek, Doğan, Bacaksız ve Tepe, 2017).

Bu başlık altında son olarak, TCK md.136'daki suçun konusunu oluşturan kişisel veri ile kişisel materyal arasındaki farklılığa da değinmek gerekir. Kişisel materyal, kişisel veriyi elde etmekte yararlanılan ancak tek başına bir gerçek kişiyi belirlenebilir kılmaya elverişli olmayan her türlü materyal olarak tanımlanabilir. Bu açıdan, söz gelimi insan kanı bir kişisel materyaldir ancak bir kişisel veri değildir. Çünkü kan kuşkusuz bir kişiye aittir ancak tek başına belirli bir kişiyi teşhis etmeye yeterli değildir; bu kişisel materyalin kişisel veriye dönüşebilmesi için üzerinde çalışılması ya da daha somut bir ifadeyle birtakım tıbbi testlere ve karşılaştırma işlemlerine konu edilmesi gerekir. Şu halde, bu kan üzerinde belirtilen test ve karşılaştırma işlemleri yapıldıktan sonra ulaşılan bilgi bir kişisel veri niteliği taşıyacaktır (Börekçi, 2019). Bu itibarla, bu işlemler yapılmadan önce henüz ham bir kişisel materyal olan kan üzerinde gerçekleştirilecek hukuka aykırı verme, yayma veya ele geçirme işlemleri TCK md.136'daki suçu oluşturmaz. Buna karşın, bir kez o kişisel materyalin bir gerçek kişi ile ilişkilendirilebilmesini ya da daha doğru bir deyişle kişisel materyalin bir gerçek kişiyi belirlenebilir kılmasını sağlayacak işlemlerin gerçekleştirilmesiyle birlikte ortaya çıkan bilgiler bir kişisel veri niteliği taşır ve TCK md.136'daki suçun kapsamında mütalaa olunur.

Fail

TCK md.37'de fail, suçun kanuni tipinde belirlenen fiili gerçekleştiren kişi olarak belirlenmiştir. Suçun kanuni tanımında herhangi bir kimse tarafından işlenebileceği belirtilen suçlara *"genel suçlar"* ya da *"herkes tarafından işlenebilen suçlar"* denilir. TCK'da düzenlenmiş olan suçların çoğunluğu, kural olarak herkes tarafından işlenebilir suçlardan oluşmaktadır (Artuk, Gökcen, Alşahin ve Çakır, 2017).

İnceleme konumuzu oluşturan TCK md.136'da düzenlenen suç tipinin kanuni tanımında da, bu suçun faili, kişisel verileri hukuka aykırı olarak veren, yayan veya ele geçiren kişi şeklinde düzenlenmiştir. Bu itibarla, TCK md.136'da düzenlenen suç tipi de fail yönünden özellik gösteren bir suç tipi değildir ve herkes bu suçun faili olabilir (Korkmaz, 2019).

Buna karşılık, "özgü *(mahsus)* suç" olarak bilinen bazı suçlarda ise fail ancak belirli nitelikleri haiz veya özel bir yükümlülük altında bulunan kişiler olabilir. Bu açıdan, suçun temel şeklinin gerçekleşmesi için failde özel niteliklerin arandığı suçlara "gerçek özgü suçlar"; buna karşın temel şeklinin herkes tarafından işlenebildiği, fakat nitelikli halinin ise yalnızca kanuni tanımda belirtildiği şekilde özel niteliklere sahip kişiler tarafından gerçekleştirildiği suçlara ise "görünüşte özgü suçlar ismi verilir (Artuk, Gökcen, Alşahin ve Çakır, 2017). TCK md.136'da kişisel verileri verme, yayma ve ele geçirme suçunun temel şekli herkes tarafından işlenebilen bir suç olarak belirlenmiş iken, TCK md.137/1-a'da ise bu suçu da kapsayan "görünüşte özgü suç" biçiminde bir nitelikli hal düzenlenmiştir (Hafızoğulları ve Özen, 2010). Buna göre, TCK md.136'daki suçun bir kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmesi halinde cezanın yarı oranında arttırılır.

Diğer yandan, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesinin bir tüzel kişiliğin faaliyeti biçiminde icra edilmesi durumunda, tüzel kişinin bu suçun faili olup olmayacağı da belirlenmelidir. Bu konuda, ceza sorumluluğunun şahsiliği ilkesini düzenleyen TCK md.20'de tüzel kişilerin suç faili olamayacağı hususundaki açık düzenlemenin zorunlu bir sonucu olarak, bu suç tüzel kişiliğin yararına veya faaliyeti kapsamında işlenmiş olsa bile, tüzel kişi fail olarak kabul edilemez ve tüzel kişi hakkında ceza yaptırımı uygulanamaz. Bununla birlikte, TCK md 20'deki genel düzenlemenin yanı sıra, kişisel verilere karşı işlenen suçları da kapsar biçimde tüzel kişilere ilişkin özel bir düzenleme getiren TCK md.140 uyarınca, bu suçların tüzel kişiliğin yararına veya faaliyeti kapsamında işlenmesi olması dolayısıyla, ilgili tüzel kişi hakkında bunlara özgü güvenlik tedbirleri uygulanabilir.

Mağdur

Her suçun bir faili olduğu gibi, mutlaka bir mağduru da vardır, bu itibarla mağdursuz suçtan söz edilebilmesi mümkün değildir. Suçun mağduru, suç ile ihlal edilen varlık veya değerin sahibi olan gerçek kişidir. Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun mağduru da, kişisel verinin ilgili bulunduğu kişidir. Burada önemli olan husus, mağdur sıfatının oluşması yönünden mutlaka bir bilişim sistemine kaydedilmiş olan kişisel verinin maliki veya zilyedi olmanın gerekli olmamasıdır; bilakis, hukuka aykırı olarak verilen, yayılan veya ele geçirilen kişisel verinin bir birey ile ilgili olması, mağdur sıfatının gerçekleşmesi için yeterlidir (Dülger, 2020). Bu itibarla, bu suç tipi mağdur yönünden herhangi bir özellik göstermez ve herkes bu suçun mağduru olabilir. Bununla birlikte, faile ilişkin olarak değinildiği üzere, mağdur yönünden de tüzel kişilerin bu suçun mağduru olup olamayacağı hususu bir sorun olarak ortaya çıkar. Bu noktada, ceza hukuku öğretisinde egemen bulunan ve bizim de katıldığımız görüşe göre, bir suçun mağduru yalnızca gerçek kişiler olabilir; tüzel kişiler ve kurumlar ise suçun mağduru değil ancak suçtan zarar gören olabilirler. Suçtan zarar gören, suçun mağdurundan daha geniş bir kavram olarak, suç ile ihlal edilen varlık veya değerin doğrudan sahibi olan kişiyi değil; ancak suçun işlenmesiyle hukuken korunan menfaatleri doğrudan veya dolaylı olarak ihlal edilenleri ifade eder. Bu bağlamda, devleti bir hak süjesi olarak kabul etmek suretiyle, devlet tüzel kişiliğinin suç mağduru olabileceği düşüncesi de artık çağdaş ceza hukukunda geçerliliğini yitirmiş bulunmaktadır. Buna göre, çağdaş hukuk sistemlerinde hak süjesi yalnızca bireylerdir ve suç mağduru bazı suçlarda belirli kişi veya kişiler olarak belirlenebildiği gibi, böyle bir belirlemenin yapılamadığı

mağduru belirli olmayan diğer bazı suçlarda da toplumu oluşturan tüm bireylerin, kısaca herkesin suçun mağduru olduğu kabul edilmektedir (Katoğlu, 2012).

Bu açıklamalar ışığında, tüzel kişilerin TCK md.136'daki suçun mağduru olarak kabul edilemeyecekleri sonucuna ulaşmak gerekmektedir. Ancak bu sonuca ulaşmanın yegâne gerekçesi, çağdaş ceza hukukunun yukarıda değinilen genel prensipleri değil; ancak aynı zamanda bizatihi KVKK düzenlemesi de bizi aynı sonuca götürmektedir. Şöyle ki, KVKK'da kişisel verinin tanımının yapıldığı 3/1-d uyarınca kişisel veri, kimliği belirli veya belirlenebilir "*gerçek kişiye*" ilişkin her türlü bilgi olarak tanımlanmaktadır. Şu hâlde, KVKK, kişisel veriyi yalnızca gerçek kişilere özgülemiş olduğu için, tüzel kişilere ait kişisel verilerden söz edilemez ve dolayısıyla kişisel verisi olmayan tüzel kişiler, TCK md.136'daki suçun mağduru da olamazlar. Nitekim bu görüş uygulama tarafından da benimsenmiş olup Yargıtay'ın da; "*Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından ... gerçek kişiye ait her türlü bilginin anlaşılması gerektiği nazara alındığında ... şikayetçi ... A.Ş.nin, sanığa yüklenen verileri hukuka aykırı olarak verme veya ele geçirme suçunun mağduru olmadığı ve suçtan doğrudan zarar görmemesi sebebiyle davaya katılma hakkının bulunmadığı gözetilmeksizin…*" (Y. 12. CD, E. 2017/1636, K. 2018/3978, T. 4.4.2018), "*şirkete ait mali bilgilerin ve programların "kişisel veri" olarak kabul edilemeyeceği de gözetilmeden, yasal olmayan ve dosya kapsamına uygun düşmeyen yetersiz gerekçelerle, sanığın mahkumiyetine karar verilmesi…*" (Y. 12. CD:, E: 2013/10672, K: 2013/15772, T. 10.06.2013) şeklindeki içtihatlarında tüzel kişilerin suç mağduru olamayacağı açıkça ortaya konulmuştur.

Hareket

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunda hareket unsuruna ilişkin ilk belirtilmesi gereken husus, bu suçun bir sırf (salt) hareket suçu olarak düzenlenmiş olmasıdır (Yaşar, Gökcan ve Artuç, 2014; İtişgen, 2015). Diğer bir deyişle, suçun kanuni tanımında belirtilen hareketlerden birinin yapılmasıyla birlikte, kanuni tipin ihlali tamamlanır ve ayrıca bir neticenin gerçekleşmesi aranmaz. Buna paralel olarak, suçun kanuni tanımında yalnızca bu suçu oluşturan hareketlerin gösterilmesi ile yetinildiği ve ayrıca bir zarar neticesi öngörülmediği için bu suç aynı zamanda bir soyut tehlike suçudur ve bu suç tanımında yer alan hareketlerin yapılması ile birlikte suç tamamlanır (Dülger, 2020). Ayrıca, davranış normun suçun hangi hareketler ile işlenebileceği açıkça gösterildiği için bu suç bir bağlı hareketli suç olma özelliği taşır. Hareketin şekli açısından ise, suçun işlenebilmesi mutlak biçimde aktif, icrai bir davranışta bulunması gerekli kıldığı için, icrai hareketle işlenebilen bir suçtur.

Bunun yanı sıra, TCK md.136'daki suç, bir seçimlik hareketli suç olma özelliği gösterir. Buna göre, suçun kanuni tanımında belirlenmiş kişisel verileri hukuka aykırı olarak "bir başkasına vermek", "yaymak" ve "ele geçirmek" şeklindeki hareketlerden birinin gerçekleştirilmesiyle suç oluşur. Failin, bu seçimlik hareketlerden birden fazlasını veya hepsini birlikte gerçekleştirmiş olması durumunda ise bu durum birden fazla suçun bulunduğuna işaret etmez. Bu tarz bir durumda ortada yine tek bir suç vardır ancak bu ihtimalde fail hakkında tayin edilecek ceza belirlenirken TCK md.61'de cezaların belirlenmesine ilişkin esaslar göz önünde bulundurularak alt sınırdan ayrılınması veya üst hadden ceza verilmesi yoluna gidilebilir (Artuk, Gökcen, Alşahin ve Çakır, 2017; Hafızoğulları ve Özen, 2010).

Aşağıda, bu suçta düzenlenen seçimlik hareketler sırasıyla kısaca ortaya konulacaktır.

Kişisel Verileri Bir Başkasına Vermek

Kişisel verilerin bir başkasına verilmesi, suçun tipik hareketlerinden ilkini oluşturmaktadır. Sözlük anlamıyla vermek; *"üzerinde, elinde veya yakınında olan bir şeyi birisine eriştirmek, iletmek"* olarak tanımlanır (Türk Dil Kurumu, t.y.). Buradaki vermek ibaresi de kişisel verinin bir başkasına

aktarılmasını, ulaştırılmasını ifade eder. Bu açıdan söz gelimi, başkası tarafından cinsel amaçlı olarak rahatsız edileceğini bilmesine karşın, mağdura ait cep telefonu numarasının üçüncü bir kişiye verilmesi halinde, TCK md.136 kapsamında kişisel verilerin bir başkasına verme hareketi işlenmiş olur (Börekçi, 2019).

Keza Yargıtay'ın; "*Sanık ... ile arkadaşı olan diğer sanık ...'ın cinsel taciz suçundan beraatlerine ilişkin hükümlerin temyiz edilmeksizin kesinleştiği, temyizin kapsamının; sanık ... hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan kurulan beraat hükmü ile sınırlı olduğu belirlenerek yapılan incelemede:*

Soruşturma evresinde katılana ait cep telefonu numarasını kimseye vermediğini ifade eden sanık ...'in, kovuşturma evresinde, arkadaşı N.'ın köyde borcu olanların telefon numaralarını istemesi nedeniyle katılana ait cep telefonu numarasını arkadaşına verdiğine dair ilk ifadesiyle çelişen tutarsız savunmalarına itibar edilemeyeceği ve arkadaşı olan N.'ın da evini ve adresini bildiği katılanla doğrudan iletişim kurmak yerine 2012 yılından beri tahsil etmediği 90,00 TL'lik borcun ödenmesi için katılanı iki yıl sonra aynı gün birden fazla defa telefonla aramasının hayatın olağan akışına uygun düşmediği gözetildiğinde, sanık ...'in, katılana ait GSM numarasını arkadaşına vermesini gerektiren makul, meşru ve mantıklı bir sebep bulunmaması nedeniyle katılanın rızası dışında hareket ettiğinin açıkça anlaşılması karşısında,

Sanık ...'in, kişisel veri niteliğindeki katılana ait cep telefonu numarasını kaydedilmiş haliyle ve hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle arkadaşına vermesi şeklinde sübut bulan eyleminden dolayı TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine karar verilmesi gerekirken…" şeklindeki kararı verme hareketinin işlenişine örnek teşkil etmektedir (Y. 12. CD., E. 2018/8466, K. 2019/9054, T. 18.09.2019).

Kişisel verinin bir başkası tarafından öğrenilebilir kılınması ile suç tamamlanır. Bu aktarma işlemi ise birçok değişik şekillerde işlenebilir, aktarımın yöntemi ve biçimi konusunda herhangi bir sınırlama mevcut değildir. Buna göre kişisel verileri başkasına vermek, kişisel verileri içeren bilgi veya belgeleri fiziksel olarak (yazılı bir kâğıt veya defter, dosya, CD, USB, hafıza kartı veya başkaca bir taşınabilir bellek biçimi ile) bir başkasına ulaştırmak şeklinde olabileceği gibi, bir iletişim aracı (faks, e-posta, sms, WhatsApp, sosyal medya araçlarındaki doğrudan mesaj (DM) vb. iletim imkânları) ile veya bulut bilişim (Clouding) sistemleri gibi yollarla da gerçekleştirilebilir (Kangal, 2019; Soyaslan, 2012). Bu bakımdan Yargıtay'ın; "*Oluşa ve dosya kapsamına göre: katılan N.'in bilgisi ve rızası dışında, ona ait olduğunu belirttiği cep telefonu ve evde kurulu telefon numaraları ile msn adresini yazıp, üçüncü kişilere, katılan N. tarafından oluşturulmuş gibi tanışma ve görüşme isteğini içerir elektronik posta gönderen sanığın, verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlediği…*" (Y. 12. CD., E. 2012/25427, K. 2013/15774, T. 10.06.2013); "*sanığın, katılan ve dava dışı eski eşi Ş. arasında gerçekleşen arama kaydı dökümlerini katılanın akrabalarına göndermesi eyleminde, arama kaydı dökümlerini, katılanın ve dava dışı Ş.'nin yaptıkları aramalarla kendilerini arayan numaralara dair tarih, saat ve süre bilgilerini içermesi ve bu iki kişi arasında gerçekleşen konuşma veya mesajlaşma içeriklerine dair bilgi bulunmaması karşısında, sanığın eyleminin haberleşmenin gizliliğini ihlal suçunu değil, T.C.K.nın 136/1. maddesinde düzenlenen, verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu gözetilmeden suçun vasfında yanılgıya düşülerek yazılı şekilde karar verilmesi…*" (Y. 12. CD., E: 2014/22994, K. 2015/2630, T. 16.02.2015); "*şikayetçi ...'ün kendisine ait kişisel veri niteliğindeki banka hesap hareketlerine dair dökümün bilgisi dışında şüpheli ...'e verildiğini ve şüpheli ... tarafından da rızası dışında delil olarak kullanıldığını iddia etmesine, şüpheli ...'in ... Tic. Ltd. Şirketi yetkilisi sıfatı ile şikayetçi ... hakkında güveni kötüye kullanma, hırsızlık ve dolandırıcılık suçlarını işlediğinden bahisle vekili aracılığıyla Cumhuriyet Başsavcılığı nezdinde suç duyurusunda bulunduğu esnada dilekçe ekinde şikayetçiye ait şahsi hesaba dair hesap hareketliliklerini gösterir belgenin delil olarak ibraz edilmesine, şikayetçiye ait hesap hareketinin telefonla yapılan talep üzerine düzenlenip*

şüpheli ...'nın müdür olarak görev yaptığı şube tarafından şikayetçinin sistemde kayıtlı olan çalıştığı firmaya ait faks numarasına gönderildiğinin ... Bankası ... Şubesi'nin 11.06.2012 tarihli cevabi yazısı ile bildirilmesine göre, şüpheliler ... ve ... haklarında 5237 Sayılı Türk Ceza Kanunu'nun 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçundan soruşturma yapılması için yeterli delil bulunduğu" (Y. 12. CD., E. 2016/9332, K. 2016/13355, T. 14.12.2016) şeklindeki kararları hareketin farklı biçimlerde ortaya çıkma hallerine örnek olarak gösterilebilir.

Buna karşın, kişisel verilerin özellikle sosyal medya ve bulut bilişim sistemlerindeki iletimi, somut bir kişinin değil ancak çok sayıdaki başka kişilerin de ulaşabileceği şekilde gerçekleştirilmiş ise bu takdirde yayma şeklindeki seçimlik hareketin gerçekleştiğini ifade etmek gerekir.

Öğretide bir görüş, kişisel verileri bir başkasına vermek şeklindeki hareket biçiminin yalnızca o kişisel veriyi elinde bulunduran kişiler tarafından işlenebileceği ve failin egemenlik alanında bulunmayan kişisel verilerin başkasına verilemeyeceğini savunmakla birlikte bizim de katıldığımız diğer görüş ise günümüzde teknolojik gelişmelerin failin kendi aktif egemenlik alanının dışında kalan verileri de başkalarına aktarabilmesinin mümkün olduğunu kabul etmektedir (Sert, 2019; Korkmaz, 2019; Hafızoğulları ve Özen, 2010). Gerçekten, bugün için söz gelimi failin bulut bilişim üzerinden faaliyet gösteren belirli veri tabanlarında bulunan kişisel verileri aktarmak için üçüncü bir kişiyle anlaşması üzerine, bu anlaşma doğrultusunda tasarlamış olduğu bir bilgisayar virüsünün bu veri tabanlarına sızmasını sağlaması ve bu virüs tarafından veri tabanlarında ele geçirilen kişisel verilerin üçüncü kişiye aktarılması pekâlâ mümkün bulunmaktadır (Börekçi, 2019). Bu durumda, failin gerek virüsün bulut bilişim veri tabanları üzerindeki kişisel verilere yönelik saldırısını icra ettiği esnada gerekse kişisel verileri üçüncü kişiye aktarımı esnasında, o kişisel verileri elinde bulundurması veya onlar üzerinde bir aktif hâkimiyeti söz konusu değildir. Kaldı ki, makine öğrenme yeteneğini haiz, yapay zekâlı algoritmaların hızla geliştiği bir teknolojik ortamda bu örnektekine benzer hukuka aykırı faaliyetlerin bu algoritmalar tarafından çok daha karmaşık yöntemler ile gerçekleştirilebilmesi de gayet beklenebilir bir durumdur. Bu itibarla, kişisel verileri bir başkasına vermek şeklindeki hareket biçiminin uygulanması için bu kişisel verilerin failin aktif egemenlik alanı içerisinde bulunması zorunlu bir unsur değildir. Buna karşın, suçun oluşması için kişisel verilerin, aktarımın yapıldığı muhatap kişinin -Kanun'un ifadesiyle bir başkasının- aktif egemenlik alanına girmiş olması gerekir. Bu kişinin, kişisel verilerin içeriğini öğrenmiş olması ise zorunlu değildir. Hatta kişisel verilerin aktarıldığı bu muhatap kişi, bu kişisel verilerin içeriğini kavrayabilecek durumda veya düzeyde olmada dahi, yine de suç oluşacaktır. Çünkü burada suçun oluşumu yönünden önemli olan, kişisel verinin aktarımı ile birlikte, aktarılan kişinin bu kişisel verilerin içeriğini öğrenme olanağının sağlanmış olmasıdır (Akdağ, 2013).

Failin mağdura ait kişisel verileri verdiği kişi, bir gerçek kişi olabileceği gibi, bir tüzel kişi de olabilir (Dülger, 2016; Kangal, 2019; Sert, 2019). Bununla birlikte, kişisel verileri bir başkasına veren failin, bu verileri hukuka uygun bir biçimde mi elinde bulundurduğu yoksa hukuka aykırı bir biçimde mi ele geçirmiş olduğu hususunun, suçun oluşması yönünden bir etkisi yoktur. Keza Yargıtay da; "*Sanık ... tarafından mağdureye ait kişisel veri niteliğindeki resimlerin rızası dahilinde çekilerek aktarıldığı hafıza kartının kaybedilmesinin ardından söz konusu kartı bulan sanık ...'dan aldıkları karttaki resimleri hukuka aykırı şekilde temin eden sanıklar ... ile ...'nin eylemlerinin hem özel hayatın gizliliğini ihlal hem de verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturup, 5237 Sayılı TCK'nın 44. maddesinde düzenlenen fikri içtima kuralı gereğince daha ağır yaptırım içeren aynı Kanunun 136. maddesinde düzenlenen suçu oluşturduğu gözetilerek hükümler kurulması gerekirken suç vasfının tayininde yanılgıya düşülerek özel hayatın gizliliğini ihlal suçundan mahkumiyetlerine karar verilmesi…*" (Y. 14. CD., E. 2019/5596, K. 2019/13580, T. 24.12.2019) şeklindeki yakın tarihli bir kararında bu hususu ifade etmiştir. Yalnızca, fail eğer bir başkasına verdiği bu kişisel verileri hukuka aykırı olarak ele geçirmiş ise bu davranış TCK md.136'da düzenlenen bir diğer seçimlik hareketi oluşturduğu için bu hareketten dolayı ayrıca ceza verilemez ancak birden fazla seçimlik hareketi birlikte gerçekleştirmiş olan failin bu durumu, yukarıda değinildiği üzere, TCK md.61 uyarınca cezanın tayininde göz önünde bulundurulur.

Kişisel Verileri Yaymak

Kişisel verilerin yayılması, suçun tipik hareketlerinden ikincisini oluşturur. Sözlük anlamıyla yaymak *"birçok kimseye duyurmak"* olarak tanımlanır (Türk Dil Kurumu Güncel Türkçe Sözlük, t.y.). Kişisel verilerin hukuka aykırı olarak yayılması ise bu verilerin çok sayıda kişiye duyurulması anlamını taşır ve bu yönüyle ilk seçimlik hareket olan vermeye göre çok daha yoğun ve etki alanı çok daha geniş bir hareket biçimi olma özelliği taşır (Karagülmez, 2013). Bu açıdan söz gelimi, mağdura ait kişisel verinin üçüncü bir kişiye elektronik posta veya Whatsapp mobil iletişim sistemi üzerinden gönderilmesi vermek iken aynı kişisel verinin çok sayıda insanın ulaşabileceği bir sosyal paylaşım sitesine konulması ise yaymak olarak nitelenir (İtişgen, 2015).

Nitekim Yargıtay da; "*Oluşa ve dosya kapsamına göre; ceza hâkimi olarak görev yapan katılanlar... ve ... tarafından, sanık ... hakkında farklı suçlardan dolayı mahkumiyet kararları verilmesi sebebiyle her iki katılana tepki duyan sanık ...'ın, katılan ...'ın eşi ile yan yana ve katılan ...'in yalnız başına günlük kıyafetleriyle poz vermiş şekilde çektirdikleri fotoğraflarını, katılanların kendi adlarına başka internet sitelerinde (facebook-twitter gibi) açmış oldukları hesaplarından ele geçirip, bu fotoğrafları, slayt gösterisi şeklinde ve duygusal fon müziği eşliğinde, "... adliyesinin yasak aşkı" başlığı altında, katılanların arasında gayriresmi bir ilişki varmış algısı doğuracak biçimde, youtube adlı video paylaşım sitesinde yayımladığı kabulüne konu olayda,*

Katılanlar tarafından internet ortamında yayımlanan ve katılanların kamuya açık alanlarda günlük kıyafetleriyle poz vermiş şekilde çektirdikleri resimleri, katılanların başkalarının görmesini ve bilmesini istemeyecekleri özel yaşam alanlarına dair görüntü olarak kabul edilemeyeceğinden, katılanların kişisel veri niteliğindeki resimlerini, hukuka uygunluk nedenlerinin bulunmaması sebebiyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle yayımlayan sanığın eyleminin, TCK'nın 136/1. maddesinde tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden…" (Y. 12. CD., E. 2015/11703, K. 2017/870, T. 08.02.2017); "*…sanıkların sahibi olduğu özel hastanede hastane müdürü ve başhekim olarak görev yapan, hastanenin aynı zamanda ortağı olan ortopedi doktoru katılan ...'in, anılan hastaneden ve ortaklıktan ayrılmasına rağmen hastaneye ait internet sitesinde yer alan reklam filmlerinde, hastanenin başhekimi ve ortopedi uzmanı olduğuna dair açıklamalarla beraber rızası olmaksızın görüntülerinin yayımlanmaya devam ettiği iddia ve kabulüne konu olayda; Katılan tarafından kaldırılması istenilmesine ve bu konuda daha önce şikayette bulunulmasına rağmen reklam filmlerini aynı şekilde yayımlamaya devam ederek, katılanın kişisel veri niteliğindeki görüntüsünü hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle başkalarının görgüsüne sunmaya devam eden sanıkların sübut bulan eylemlerinden dolayı TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet kararı verilmesi gerektiği gözetilmeksizin…*" Y. Y. 12. CD., E. 2018/8144, K. 2019/8317, T. 10.07.2019) şeklinde verdiği kararlarla bu hususu vurgulamıştır (Benzer kararlar için Y. 12. CD., E. 2017/3721, K. 2018/5256, T. 08.05.2018; Y. 12. CD., E. 2017/5654, K. 2018/2911, T. 14.03.2018).

Bu örneğin ve kararın da ortaya koyduğu üzere, yayma biçimindeki seçimlik hareket herhangi bir usul veya şekil kuralına bağlı değildir ve çok çeşitli şekillerde gerçekleştirilebilir (Soyaslan, 2012). Mağdura ait olan kişisel verinin söz gelimi; mektupla birden çok kişiye yazılı şekilde gönderilmesi, yine birden çok kişiye elektronik postayla ya da CD, USB, hafıza kartı vb. ortamında taşınabilir bellek ile gönderilmesi, bir web sitesine ya da sosyal paylaşım sitesine konulması, yayma hareketi kapsamında yer alan davranışlardır. Özellikle günümüzde hemen hemen herkesin hayatının bir parçası olan sosyal paylaşım sitelerinin durumu üzerinde biraz durmak gerekmektedir. Bu bakımdan kişisel verilerin hukuka aykırı olarak yayılması noktasında en sık karşılaşılan durum fail ya da faillerin sahte hesaplar açarak mağdurların fotoğraflarının, isim soy isimlerinin ya da telefon numaralarının bu hesaplarda kullanılmasıdır. Yargıtay da bu durumlarda kişinin günlük yaşamına dair özel hayatı kapsamında

kalmayan kişisel verilerinin hukuka aykırı olarak bu tür hesaplarda kullanılmasını TCK m. 136/1 kapsamında değerlendirilmesi gerektiğine ilişkin olarak müstakar içtihat oluşturmuştur (Aktaş, 2017): "*Mağdurun kendi facebook hesabındaki profil resminin, onun başkaları tarafından görülmesini ve bilinmesini istemeyeceği özel yaşam alanına ilişkin bir görüntü olarak kabul edilemeyeceği; ancak, mağdurun kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle Ktü 2. El Eşya, Yardımlaşma, Haberleşme ve Duyuru Platformunda yayımlayan sanığın, iddianamede tarif edilen ve yapılan yargılama sonunda sübut bulan eyleminin TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu…*" (Y. 12. CD., E. 2019/532, K. 2019/10827, T. 13.11.2019); "*Sanık ...'ün, mağdur ... ile aralarındaki arkadaşlık ilişkisi sona erdikten sonra, mağdur ...'nin adını ve soyadını taşıyan sahte facebook hesabı açıp, bu hesap üzerinden, mağdur ...'nin günlük kıyafetleriyle poz vermiş şekilde çektirdiği resimlerini ve adı geçen mağdurun babası olan diğer mağdur ...'ın aktif kullanımında olan cep telefonu numarasını farklı zamanlarda yayımlaması eylemlerinden dolayı verileri hukuka aykırı olarak verme veya ele geçirme suçundan mağdur sayısınca iki ayrı mahkumiyet hükmü kurulması gerekirken, aynı suçun mağdurlara karşı tek bir fiille işlendiğine ve TCK'nın 43/2. madde ve fıkrasının koşullarının oluştuğuna dair dosya kapsamına uygun düşmeyen yetersiz gerekçelerle sanık hakkında TCK'nın 136/1. madde ve fıkrası uyarınca tek bir mahkumiyet hükmü kurulması…*" (Y. 12. CD., E. 2018/8366, K. 2019/8625, T. 11.09.2019); "*İkrar içeren savunmaya ve dosya kapsamına göre; sanığın, katılan facebook hesabında yayınladığı resimleri ve katılana ait cep telefonu numarasını kendi facebook hesabında yayınlaması şeklinde eyleminin TCK'nın 136/1. madde ve fıkrasında düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğu ve sanık hakkında bu suçtan mahkumiyete karar verilmesi gerektiği gözetilmeden, delillerin takdirinde ve suç vasfında yanılgıya düşülerek yazılı şekilde özel hayatın gizliliğini ihlal suçundan sanığın beraatine karar verilmesi…*" (Y. 12. CD., E. 2018/8221, K. 2019/6189, T. 15.05.2019); "*Şikayetçinin babasına ait facebook adresinde daha önce yayınladığı sadece baş ve yüz kısmını gösteren resmi, şikayetçinin başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin bir görüntü olarak kabul edilemeyeceğinden, şikayetçinin kişisel veri niteliğindeki resmini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle internet sitesinde şikayetçi adına oluşturduğu sahte hesapta profil resmi olarak kullanan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı gözetilmeden…*" (Y. 12. CD., E. 2018/8198, K. 2019/6187, T. 15.05.2019); "*Dosya kapsamına göre, sanığın, mağdurun fotoğrafını mağdur adına açtığı sahte facebook hesabında yayınlaması şeklinde sübutu kabul edilen eyleminin, mağdurun gündelik elbiseler ile poz vermiş ve baş bölgesi ile vücudunun bir kısmını gösteren fotoğrafı ile ad ve soyadının kişisel veri niteliğinde olması karşısında sanık hakkında TCK 136/1. madde ve fıkrasında düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması gerekirken, delillerin takdirinde hataya düşülerek yasal ve yeterli gerekçe gösterilmeden aynı Kanunun 134/2. maddesinde düzenlenen özel hayatın gizliliğini ihlal suçundan yazılı şekilde mahkumiyete karar verilmesi, kanuna aykırı…*" (Y. 12. CD., E. 2017/7385, K. 2018/3977, T. 04.04.2018)

Yayma hareketine konu olan kişisel verinin içeriğinin, kamuya açık bir alanda kayıt altına alınan ses veya görüntülerden ibaret olması durumunda, bu kayıtların yayılmasının TCK md.136'daki suçu oluşması yönünden irdelenmesi gerekir. Öğretide, bu tarz bir durumda da, fiilin suç niteliğinin değişmeyeceği ileri sürülmüşse de; kanımızca bu görüşe biraz ihtiyatla yaklaşmak gerekir (Akdağ, 2013). Şöyle ki, günümüzde gerek mobil iletişim araçlarıyla yüksek çözünürlüklü resim ve videolar üretebilme ve paylaşabilmeye ilişkin teknolojinin hızla gelişmesi ve buna paralel olarak görsel paylaşım sitelerinin popülerliğinin artması ile birlikte, kamuya açık alanlarda resim çekme, ses ve görüntü kaydı yapmak geniş kitleler tarafından benimsenen, çok yaygın bir davranış biçimi halini almıştır. Özellikle, insanların kendi resim ve videolarını özçekim *(selfie)* yapmak suretiyle tespit ederek, bu resim ve görüntülerini sosyal paylaşım siteleri üzerinden paylaşmaları adeta günlük hayatın olağan bir parçasına dönüşmüştür. Üstelik bu durum yalnızca tiyatro, konser, festivaller gibi insanların yığın halinde bulunduğu etkinlik alanlarıyla sınırlı değildir ve günlük yaşamın sürdürüldüğü her yerde devam

etmektedir. Toplumda kamuya açık alanlarda bu denli yaygın bir şekilde sürdürülen bu resim ve video paylaşımları esnasında, kişilerin kendi görüntülerinin yanı sıra, başka kişilere ait görüntüleri de paylaşmaları halinde, bu tarz bir davranışın otomatik olarak TCK md.136'daki suçu oluşturacağını ileri sürebilmek, kanımızca mümkün değildir. Çünkü öncelikle, bu gibi paylaşımlarda bulunan kişiler çoğu kez yapmış oldukları bu davranışın bir suç oluşturduğunu bilmeden hareket etmektedirler ki; bu tarz bir durumda, kişinin içine düşmüş olduğu bu durumun TCK md.30/4 uyarınca haksızlık yanılgısı kapsamında irdelenmesi ve bir hataya düşmüşlerse bile bu hatanın kaçınılmaz olup olmadığı hususu, her somut vakıada irdelenmelidir (Börekçi, 2019). Ayrıca, aşağıda irdeleneceği üzere, suçun manevi unsuru yönünden kişisel verilerin hukuka aykırı olarak yayılması yalnızca kasten işlenebilen bir suç olarak düzenlendiği için kendi resim ve görüntüleri ile birlikte, kişisel veri kapsamında yer alan başkalarına ait resim ve görüntüleri de paylaşan failin, bu başkalarına ait kişisel verileri yayma hareketi bilerek ve isteyerek gerçekleştirmiş olup olmadığı hususunun da ayrıca irdelenmesi gerekmektedir. Bu nedenle, kamuya açık alanda, başkalarına ait resim ve görüntülerin yayılması halinde, failin ancak işlediği fiilin haksızlık oluşturduğu konusunda kaçınılmaz bir hataya düşmemiş olması ve ayrıca bu resim ve görüntülerin yayılması hareketini bilerek ve isteyerek gerçekleştirdiğinin sabit olması durumunda, TCK md.136 uyarınca sorumlu tutulması mümkün olabilecektir.

Fail tarafından yayılan kişisel verinin içeriğinin başkaları tarafından fiilen öğrenilmiş olup olmaması, suçun oluşması yönünden herhangi bir önem taşımaz. Burada önemli olan husus, failin gerçekleştirmiş olduğu bu yayma hareketi ile mağdura ait kişisel verilerin içeriğinin birden fazla kişi tarafından öğrenilebilmesi olanağının sağlanmış olmasıdır (Dülger, 2016; Kangal, 2019, Korkma, 2019). Keza, failin yaymış olduğu kişisel verileri, hukuka uygun bir şekilde mi elinde bulundurduğu yoksa hukuka aykırı olarak mı ele geçirdiği hususu da suçun oluşumu yönünden önemsizdir. Söz gelimi, sosyal medya platformuna kişinin rızası ile yüklediği fotoğraf, o platformun kullanıcıları açısından ulaşılabilir nitelikte olup birçok kişi tarafından görülme ve kaydetme imkânı sunabilir, ancak kişinin kendi fotoğrafını paylaşması onun rızası dışında başkaları tarafından da yayınlanabileceği anlamına gelmez. Nitekim Yargıtay da buna benzer bir olayda; "*Bu açıklamalar ışığında incelenen dosya kapsamına ve ikrar içeren savunmaya göre; sanığın, bir dönem internet üzerinden tanışıp arkadaş olduğu katılanın daha önce kendi facebook hesabında paylaştığı resimleri, katılan ile tartışmaları sebebiyle katılan adına açtığı sahte facebook hesabından katılanın rızası dışında yayınladığı iddia edilen olayda, katılanın gündelik kıyafetler ile kamuya açık alanda çekilmiş ve kişisel veri niteliğindeki resimlerini daha önce kendi facebook hesabında yayımlamasının bu resimlerin kişisel veri olma özelliğini değiştirmeyeceği gibi üçüncü kişilere katılanın rızası dışında yayınlama hakkı da tanımayacağı gözetilmeden sanık hakkında verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyetine karar verilmesi gerekirken delillerin takdirinde yanılgıya düşülerek yazılı şekilde sanığın beraatine karar verilmesi…*" şeklindeki gerekçeyle TCK m. 136'da yer alan suçun oluştuğunu ifade etmiştir (Y. 12. CD., E. 2017/2960, K. 2018/1541, T. 14.02.2018).

Bununla birlikte, fail yaymış olduğu bu kişisel verileri hukuka aykırı olarak ele geçirmiş ise yukarıda da belirttiğimiz üzere bu durumda aynı suçun iki farklı seçimlik hareketini gerçekleştirmiş olacağı için bu hareketi nedeniyle ayrıca cezalandırılmaz. Bunun yerine, bu durum TCK md.61 uyarınca cezanın tayininde göz önünde bulundurulur.

Bu konuda değinilmesi gereken ilginç bir husus, TCK md.136'nın içeriğindeki üç seçimlik hareketten birini oluşturan yayma hareketine, madde başlığında yer verilmemiş olmasıdır. Kanun yapma tekniği açısından çok sorunlu olan ve sehven yapılan bir hata olduğunu düşündüğümüz bu durumun mutlaka düzeltilmesi gerekmektedir

Kişisel Verileri Ele Geçirmek

Kişisel verilerin ele geçirilmesi, suçun tipik hareketlerinin üçüncüsüdür. Sözlük anlamıyla ele geçirmek *"yakalamak, sahibi olmak ve gizlenmek istenen bir şeyi elde etmek"* şeklinde tanımlanır (Türk Dil

Kurumu Güncel Türkçe Sözlük, t.y.). Kişisel verileri hukuka aykırı olarak ele geçirmek, failin mağdura ait kişisel verileri kendine aktarması veya fiilî egemenlik alanına dâhil etmesi şeklinde gerçekleşir. Görüldüğü üzere ele geçirmek seçimlik hareketinde, önceki iki seçimlik hareketten farklı olarak fail tarafından bir başkasına kişisel veri aktarımı yapılması söz konusu değildir.

Kişisel verilerin ele geçirilmesi, bir başkasına ait kişisel veriler üzerinde tasarruf yetkisine sahip olmamasına rağmen, bu kişisel verilerin üzerinde tasarruf edilebilecek şekilde edinilmesi anlamını taşır. Yargı içtihatlarına yansıyan bir örnekle açıklamak gerekirse, trafikte araçla seyir halinde iken kendisini sıkıştıran mağdurun araç plakasını, trafik şube müdürlüğünde görevli polis memuru arkadaşı aracılığıyla sorgulatan ve bu şekilde araç sahibinin kimlik bilgilerine ulaşan failin bu davranışın, kişisel verilerin hukuka aykırı olarak ele geçirilmesidir (Y. 12. CD, E. 2018/636, K. 2018/6140, T. 30.5.2018). Bu örnekte, polis memurunun davranışı ise, yine TCK md. 136 kapsamında kişisel verilerin hukuka aykırı olarak verilmesidir (Börekçi, 2019; Yaşar, Gökcan ve Artuç, 2014).

Keza Yargıtay Ceza Genel Kurulu da somut olayda; "*Kişisel verilerin ele geçirilmesi" seçimlik hareketi ise; kişisel verilerin kayıtlı olduğu belgelerin alınması ya da kayıtlı olduğu bilişim sisteminden ele geçirilmesi vb... şekillerde gerçekleştirilebilecektir. Ele geçirme fiili, başkasının hakimiyeti altında bulunan bir kişisel verinin, failin hakimiyeti altına girmesi ile gerçekleşmiş olacaktır… Kendisi ve eşi de memur olan sanığın, yapacakları şikayete konu olmak üzere eşi ile aynı işyerinde ebe olarak çalışan katılanın doğum belgesini hastaneden alarak, il sağlık müdürlüğüne verdikleri şikayet dilekçesinin ekinde sunmaları şeklinde gerçekleşen somut olayda, katılana ait doğum belgesinin kişisel veri olması, memur olarak çalışan sanığın başkasına ait bilgileri içeren bir belgeyi velev ki yapacağı şikayet başvurusuna konu olsa dahi almasının hukuka aykırı olacağını bilebilecek durumda bulunması, suça konu doğum belgesini şikayet dilekçesine eklemek suretiyle burada yer alan ve kişisel veri niteliğinde bulunan bilgilerin katılanın rızası dışında başkalarınca öğrenilmesine neden olunması hususları birlikte değerlendirildiğinde, sanığın eylemi TCK'nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme ve yayma suçunu oluşturmaktadır*." şeklindeki kararı ile kişisel verilerin ele geçirilmesinden ne anlaşılması gerektiğini ortaya koymuştur (YCGK., E. 2012/12-1514, K. 2014/312, T. 10.6.2014).

Yukarıdaki örnekte ve Yargıtay kararında da vurgulandığı üzere, ele geçirme hareketine konu olan kişisel veriler, genellikle normal koşullarda ulaşılabilir bir alanda bulunmayan kişisel verilerdir (Akdağ, 2013; Kangal, 2019). Ancak, normalde ulaşılabilir olan verilerin ele geçirilmesi de pekâlâ mümkündür. Failin, normal koşullarda ulaşabildiği veya egemenlik alanı içerisinde yer alan verileri hukuka aykırı bir biçimde kendine aktarması durumunda da bir ele geçirmeden söz etmek gerekir. Bu açıdan söz gelimi, yüksek gelir grubuna yönelik villalardan oluşan büyük bir site inşa eden bir inşaat şirketinin satış departmanı müdürünün, şirket bilgisayarından ulaşabildiği potansiyel müşteri portföyünün kimlik ve iletişim bilgilerini bir USB taşınabilir bellek aracılığıyla evindeki şahsi bilgisayarına aktarması da TCK md.136 kapsamında bir ele geçirmedir. Nitekim Yargıtay; sanığın şirkette bilgi teknolojileri müdürü olarak çalıştığı esnada katılan şirketin müşterilerine ait bilgileri, evindeki bilgisayara aktarmasını verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğunu ifade etmiştir (Y. 15. CD., E. 2013/612, K. 2014/14715, T. 16.9.2014).

Ele geçirme hareketi, diğer seçimlik hareketlerde olduğu gibi, birçok değişik şekilde gerçekleştirilebilir (Soyaslan, 2012). Buna göre, kişisel verilerin yazılı olduğu belgenin veya kayıtlı olduğu CD, USB, hafıza kartı vb. cismani materyallerin fiilen bir yerden alınması veya kişisel verinin kayıtlı olduğu bilişim sistemine ulaşılarak sistemdeki verilerin kopyalanması veya başka bir ortama gönderilmesi halinde, ele geçirme hareketinden söz edilecektir (Taşkın, 2008). Ele geçirmenin mutlaka fizikî bir nitelik taşıması da gerekli değildir. Bu kapsamda, yukarıdaki örnekte, inşaat şirketinin müşteri portföyündeki kişilerin kimlik ve iletişim bilgilerinin, açık bırakılan şirket bilgisayarından okunarak öğrenilmesi de ele geçirme kapsamındadır. Buna karşılık, Yargıtay ise yakın tarihli bir kararında; "*Bu noktada belirtmek gerekir ki, kişisel verilerin, üzerinde yazılı olduğu belgenin bulunduğu yerden*

alınması ya da kaydedilmiş haliyle başka bir nesne üzerine taşınarak (örneğin; yazının başka bir kağıt, defter vb. nesne üzerine geçirilmesi, taşınabilir belleğe veya CD'ye aktarılması gibi işlemlerle) sabitlenmesi, böylece istenildiğinde tekrar kullanılabilmesi olanağını sağlayan her türlü faaliyet, kişisel verileri "ele geçirme" kapsamında değerlendirilebilir ise de, kişisel verilerin kaydedilmeden önce öğrenilmesi, hafızada tutulan kişisel verilerin başkalarına açıklanması, kişisel verilere salt duyu organları aracılığıyla vakıf olunması, ancak TCK'nın 134. maddesinin 1. fıkrasının 1. cümlesinde düzenlenen özel hayatın gizliliğini ihlal suçu kapsamında değerlendirilebilir." şeklindeki gerekçesiyle aksi yönde bir karar vermiştir (Y. 12. CD., E. 2017/12083, K. 2018/2539, T. 07.03.2018).

Kişisel verilerin ele geçirilmesi çok çeşitli nedenlerle gerçekleştirilebilen bir hareket olmakla birlikte, bunların içerisinde en sık rastlanılanı, kimlik hırsızlığı veya kimlik dolandırıcılığı amacıyla kişisel verilerin ele geçirilmesidir (İtişgen, 2015). Bunların her ikisinde de bir kişinin kimlik bilgileri şeklindeki kişisel verileri hukuka aykırı olarak ele geçirilir ve çoğunlukla haksız ekonomik kazanç elde etme maksadıyla çeşitli hırsızlık, dolandırıcılık, yağma ve bilişim sistemine yetkisiz girme gibi suç teşkil eden fiillere ilişkin işlemlerde kullanılır (Kangal, 2019). Kimlik hırsızlığı veya dolandırıcılığı ile birlikte, mağdurun kredi kartı bilgilerinin kullanılması şeklinde bir suistimalin ortaya çıkması durumunda, TCK md.136'nın yanı sıra, bu konuya özgü spesifik bir düzenleme olan banka veya kredi kartlarının kötüye kullanılması suçuna (TCK md.245) ilişkin hükümler de uygulanır.

Keza Yargıtay pek çok kararında bu hususu ifade etmiştir: "*…sanıklarla kart kopyalamak üzere anlaşıp karşılığında menfaat elde ettiği anlaşılan sanığın eyleminin, çalıştığı restauranta gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmekten ibaret olduğu diğer sanıkların sahte kart üretmek ve bu kartları kullanmak suçlarına iştirak ettiğine dair dosya kapsamında delil bulunmadığı anlaşılmakla, eyleminin TCK.nun 136. maddesinde düzenlenen birden fazla kişiye ait kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğu gözetilmeden…*" (Y. 8. CD., E. 2017/15706, K. 2018/866, T. 31.01.2018); "*Sanıkların, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmek için ATM cihazına yerleştirdikleri düzenek ve hafıza kartında herhangi bir bilgi bulunup bulunmadığı araştırılıp, bilgi bulunması halinde eylemlerinin TCK.nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırma ile yazılı şekilde aynı Kanun'un 245/2. ve 35. maddeleri uyarınca hükümler kurulması…*" (Y. 8. CD., E. 2016/12565, K. 2017/12892, T. 20.11.2017); "*…mağdurlara ait kart bilgileri kopyalayarak bir kart oluşturdukları ya da kart oluşturulma eylemine iştirak ettiklerine dair delil elde edilemeyen sanıkların kart bilgilerinin kopyalanması sonrasında ele geçirilen bilgilerle yurtdışında gerçekleşen para çekim işlemlerine iştirak ettiklerine dair de bir delil elde edilemediği ve eylemlerinin mağdur sayısınca TCK.nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme suçunu oluşturduğu…*" (Y. 8. CD., E. 2018/509, K. 2019/15371, T. 19.12.2019); "*…suça konu kredi kartları gerçeğe aykırı olarak üretilen banka sayısınca TCK.nun 245/2. maddesiyle ve aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda aynı Kanun'un 43. maddesinin uygulanması, bu kartların kullanılması halinde ise, banka sayısınca TCK.nun 245/3. maddesiyle aynı bankaya ait birden fazla kart ile veya bir kart ile değişik zamanlarda para çekilmesi veya harcama yapılması halinde ise TCK.nun 43. maddesi uyarınca uygulama yapılması, harcama yapılmadan kartların bloke olması halinde TCK.nun 245/3 maddesine teşebbüs suçundan uygulama yapılması gerektiği, mağdurlara ait kart bilgileri kopyalanarak bir kart oluşturulmaması halinde ise ele geçirilen kopyalama cihazında bilgi bulunması halinde eyleminin mağdur sayısınca TCK.nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırma ile yazılı şekilde hüküm kurulması…*" (Y. 8. CD., E. E. 2018/6171, K. 2018/10436, T. 8.10.2018).

Nitelikli Haller

Ceza normunda bir suçun temel şekli tanımlanır. Ancak, suçun temel şekline ilave olarak, izlenen suç siyaseti gereğince gerçekleştirilen eylemin daha ağır veya daha hafif sayılan niteliğini belirleyen ve böylelikle cezanın artırılması veya eksiltilmesini gerektiren nitelikli hallere de yer verilebilir (Artuk, Gökcen, Alşahin ve Çakır, 2017). Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçuna ilişkin olarak, 7188 sayılı Kanun ile TCK md.136'ya eklenen 2. fıkra ile *"suçun konusunun CMK'nın 5. ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler olması"* bir nitelikli hal olarak belirlenmiştir.

Bunun yanı sıra, TCK md.137'de, bu suçun *"kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle"* veya *"belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle"* işlenmesi halleri, suçun diğer nitelikli halleri olarak düzenlenmiştir. Bu her üç hal de, cezayı ağırlaştıran birer nitelikli hal olup TCK md. 136/2'deki nitelikli halin varlığı cezayı *"bir kat"* artırırken; TCK md. 137'deki nitelikli hallerin varlığında ise ceza *"yarı oranında"* artırılır. Buna karşın, TCK md. 136'ya ilişkin olarak Kanun'da cezayı azaltan bir nitelikli hal ise bulunmamaktadır.

Suçun Konusunun CMK md. 236'nın 5. ve 6. Fıkraları Uyarınca Kayda Alınan Beyan ve Görüntüler Olması

Kişisel verileri hukuka aykırı olarak verme yayma veya ele geçirme suçunun orijinal şeklinde bulunmayan bu nitelikli hal, Yargı Reformu 1. Paketi olarak da bilinen 31.10.2019 tarih ve 7188 sayılı Kanun'un 17. maddesi ile TCK md.136'ya 2. fıkra olarak eklenmiştir.

Bu nitelikli halde belirtilen CMK md.236/5. ve 6. fıkralar ise, yine 7188 sayılı Kanun ile getirilmiştir ve öz itibarıyla, cinsel saldırı ile çocukların cinsel istismarı suçlarının mağdurlarının dinlenilmesine ilişkin esasları yeniden düzenlemektedir.

Buna göre, TCK md.103/2'de düzenlenen *(çocukların nitelikli cinsel istismarı)* suçunun mağduru olan çocukların soruşturma evresindeki beyanları, bu çocuklara yönelik hizmet veren merkezlerde Cumhuriyet savcısının nezaretinde uzmanlar aracılığıyla alınır. Mağdur çocuğun beyan ve görüntüleri kayda alınır. Kovuşturma evresinde ise ancak maddi gerçeğin ortaya çıkarılması açısından mağdur çocuğun beyanının alınması veya başkaca bir işlem yapılmasında zorunluluk bulunması hâlinde bu işlem, mahkeme veya görevlendireceği naip hâkim tarafından bu merkezlerde uzmanlar aracılığıyla yerine getirilir. Mağdur çocuk yargı çevresi ve mülkî sınırlara bakılmaksızın en yakın merkeze götürülmek suretiyle bu fıkrada belirtilen işlemler yerine getirilir.

TCK md.102/2'de düzenlenen *(nitelikli cinsel saldırı)* suçunun mağdurlarının soruşturma evresindeki beyanları bakımından da, yukarıdaki paragraftaki esaslar uygulanır. Ancak, beyan ve görüntülerin kayda alınmasında mağdurun rızası aranır.

Buna göre, TCK md 136'ya eklenen 2. fıkra ile kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun konusunun, çocukların cinsel istismarı veya nitelikli cinsel saldırı suçlarının mağdurlarının soruşturma evresinde kayıt altına alınan beyan ve görüntüleri olması durumunda, fail hakkında uygulanacak olan ceza bir kat artırılacaktır. Böylece, düzenlemenin gerekçesinde de belirtildiği üzere, cinsel istismar ve cinsel saldırı suçunun mağdurlarının örselenmelerinin engellenmesi ve korunmaları amacıyla soruşturma ve gerekiyorsa kovuşturma aşamasında ifade ve beyanların kayıt altına alınması esası getirilmekte ve TCK md.136 kapsamında gerçekleştirilecek ihlallerin, burada belirtilen nitelikteki kayıtları konu alması halinde failin daha ağır şekilde cezalandırılması öngörülmektedir.

Suçun Kamu Görevlisi Tarafından Görevinin Verdiği Yetki Kötüye Kullanılmak Suretiyle İşlenmesi

TCK md.136'daki suça ilişkin ilk nitelikli hal, kamu görevlisinin görevini kötüye kullanarak başkalarının kişisel verilerini hukuka aykırı olarak ele geçirmesi veya bu verileri hukuka uygun olarak elinde bulundurmak ile birlikte, hukuka aykırı olarak başkalarına vermesi veya yayması şeklinde ortaya çıkar (TCK md.137/1-a).

Bu nitelikli halin gerçekleşmesi için öncelikle failin bir kamu görevlisi olması gerekir. Kamu görevlisi kavramı, Ceza Kanunu'nun "Tanımlar" başlıklı 6. maddesinde *"kamusal faaliyetin yürütülmesine atama veya seçilme yoluyla ya da herhangi bir surette sürekli, süreli veya geçici olarak katılan kişi"* olarak tanımlanmıştır (TCK md. 6/1-c). Madde gerekçesinde, bir kişinin Ceza Kanunu anlamında kamu görevlisi olarak kabul edilebilmesi için yürütmekte olduğu faaliyete ilişkin olarak maaş, ücret veya benzeri bir maddi karşılık alıp almamasının kamu görevlisi sıfatına bir etkisinin bulunmadığı ve kişinin yürüttüğü faaliyetin kamusal bir nitelik taşıması halinde Ceza Kanunu uygulamasında kamu görevlisi olarak kabul edileceği belirlenmiştir. Bu nitelikli halin uygulanması kamu görevlisi olmayı zorunlu kıldığı için, burada bir görünüşte özgü suç söz konusudur (Börekçi, 2019; İtişgen, 2015).

Bununla birlikte, bu nitelikli halin uygulanabilmesi için failin yalnızca kamu görevlisi olması yeterli değildir (Yaşar, Gökcan ve Artuç, 2014). Bunun yanında, failin kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme şeklindeki hareketi, kamu görevinin vermiş olduğu yetkiyi kötüye kullanmak suretiyle gerçekleştirmiş olması gerekir. Eğer kamu görevlisinin yetkilerini kötüye kullanması kapsamında değilse söz konusu nitelikli uygulanmayacaktır: "*Sanığın trafikte kendisini sıkıştırdığını iddia ettiği mağdura ait aracın plakasını polis memuru olan tanığı arayıp sorgulattığı ve mağdurun kimlik bilgilerini vermesini sağladığı şeklinde sübutu kabul edilen eylemi sebebiyle polis memuru olan tanığın mağdurun kimlik bilgilerini vermesinin görevinin sağladığı yetkiyi kötüye kullanması kapsamında olmadığı gözetilmeden sanık hakkında TCK 137/1-a. madde ve fıkrası gereğince artırım yapılarak sanık hakkında fazla ceza tayini… bozmayı gerektirmiş olup…*" (Y. 12. CD., E. 2018/636, K. 2018/6140, 30.05.2018).

Burada belirlenen görevinin vermiş olduğu yetkiyi kötüye kullanma ibaresinin, TCK md.257'de düzenlenen görevi kötüye kullanma suçun özel bir görünümü olarak kabul edilmelidir (Korkmaz, 2019). Bu açıdan burada da tıpkı görevi kötüye kullanma suçunda olduğu gibi, görevin gereklerine aykırılık arandığı için kişisel verilere ilişkin gerçekleştirilen bu ihlalin kamu görevlisinin görevine ilişkin olması ve aynı zamanda kamu görevlisinin bu konuda bir yetkisinin de bulunması gerekir. Eğer bu ihlal fiili, kamu görevlisinin görev ve yetki alanına girmiyor ise bu nitelikli halin uygulanması mümkün olmaz. Bu nedenle, kamu görevlisinin görev ve yetki alanı kişisel verilerle ilgili olarak, söz gelimi bu kişisel verileri elde etmeye, kaydetmeye ya da işlemeye elverişli bir nitelik taşımalı ya da en azından kamu görevlisi görevinin verdiği yetkinin bir gereği olarak başkasına ait kişisel verilere ulaşabilir durumda olmalıdır (Kangal, 2019). Nitekim İzmir Bölge Adliye Mahkemesi'nin 10. Ceza Dairesi de, "*Olay tarihinde Sosyal Güvenlik İl Müdürlüğünde sosyal güvenlik denetmen yardımcısı olarak görev yapan şüphelinin yetkileri çerçevesinde erişmemesi gereken bilgi ve belgelerden uzak durmayarak, yönetmelikte belirtilen görev-yetki ve sorumluluklarına, bilgi güvenliği kurallarına aykırı olarak makul bir iş gerekçesi olmadan kurumun bilişim sistemine girerek Türkiye Cumhuriyeti Cumhurbaşkanının çocuklarının kişisel bilgilerini sorgulaması şeklinde anlatılan eylemin suçtan zarar gören kişiler yönünden ayrı ayrı temel suç tanımı TCK'nın 136/1. maddesinde düzenlenen "Verileri hukuka aykırı olarak verme veya ele geçirme" suçunun, eylemlerin kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmekle TCK'nın 137/1-a maddesinde düzenlenen nitelikli halini oluşturduğu…*" şeklindeki gerekçesiyle somut olayda nitelikli halin oluştuğunu ifade etmiştir (İzmir BAM, 10. CD., E. 2017/1122, K. 2017/1114, T. 05.07.2017).

Kamu görevlisinin görevinin verdiği yetkinin gereklerini ne zaman kötüye kullandığının belirlenmesinde, bu alana özgü idari mevzuat ile birlikte KVKK hükümleri birlikte ele alınmalıdır. Kişisel verilerin korunması konusunda, kamu görevlilerini kapsar anlamda, uyulması gereken esaslar yönünden özellikle KVKK'daki düzenlemeler hem yol gösterici hem de bağlayıcıdır. Diğer bir ifadeyle, kişisel verilerin korunmasına ilişkin KVKK'daki kurallar hem kamu hem de özel sektöre yönelik olduğu için, tüm kamu kurum ve kuruluşları ile buralarda faaliyet gösteren kamu görevlileri bu kurallara uymak durumundadır (Börekçi, 2019). Bununla birlikte bu genel kurala, KVKK md. 28'de kişisel verilerin;

- kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarı faaliyetler kapsamında veya
- soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercilerinin faaliyetleri sırasına işlenmesi,

hallerine ilişkin bir istisna getirilmiş ve kişisel verilerin bu belirtilen faaliyetler kapsamında işlenmesi halinde, KVKK hükümlerinin uygulanmayacağı belirlenmiştir. Bu istisnanın geçerli olmadığı yegâne durum ise, önleyici faaliyetler ve soruşturma işlemleri kapsamında kişisel veri işlendiği takdirde dahi veri sorumlusunun aydınlatma yükümlülüğü ve ilgili kişinin zararın giderilmesini talep etme hakkı bulunmasıdır (KVKK md.28/2-a).

Suçun Belirli Bir Meslek ve Sanatın Sağladığı Kolaylıktan Yararlanmak Suretiyle İşlenmesi

TCK md.136'daki suça ilişkin ikinci nitelikli hal, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesinin, belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesidir (TCK md.137/1-b).

Maddenin yazımında her ne kadar *"meslek ve sanatın sağladığı kolaylıktan yararlanmak*"tan söz edilirken arada "ve" bağlacı kullanılmış ise de kişinin bu suçtaki kişisel veriler ihlalini gerçekleştirirken hem mesleğinden hem de icra ettiği bir sanattan yararlanmış olması, gerçekleşmesi neredeyse olanaksız olan bir durumdur. Bu nedenle, amaca uygun şekilde yorum yapılarak buradaki bağlacın *"veya"* şeklinde anlaşılması ve bunlardan birinin sağlamış olduğu kolaylıktan yararlanarak kişisel veri ihlalini gerçekleştirmiş olması, nitelikli halin uygulanması gerekir (Gültekin, 2012).

Meslek, sözlük anlamı ile *"belli bir eğitim ile kazanılan sistemli bilgi ve becerilere dayalı, insanlara yararlı mal üretmek, hizmet vermek ve karşılığında para kazanmak için yapılan, kuralları belirlenmiş iş"* şeklinde tanımlanır (Türk Dil Kurumu Güncel Türkçe Sözlük, t.y.). Sanat ise, bu hükmün uygulanması için elverişli olan sözlük anlamıyla *"bir şey yapmada gösterilen ustalık"* şeklinde tanımlanır (Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/ adresinden 18.05.2020 tarihinden alınmıştır). Bu açıdan, kanımızca sanat teriminin günlük yaşamda daha ziyade tasarıma dayalı bir yaratıcılığı ve farklı anlatım yeteneğini ifade eden diğer anlam biçimleriyle kullanıldığı için kanun koyucunun burada sanat yerimi yerine *"insanların maddeye dayanan gereksinimlerini karşılamak için yapılan, öğrenimle birlikte deneyim, beceri, ustalık gerektiren iş"* olarak tanımlanan (Türk Dil Kurumu Güncel Türkçe Sözlük, https://sozluk.gov.tr/ adresinden 18.05.2020 tarihinden alınmıştır) *"zanaat"* terimini kullanması daha yerinde bir tercih olurdu (Özbek, 2008). Bu nedenle, buradaki sanat ifadesini zanaat olarak yorumlamak, amaca uygun olacaktır. Failin meşgul olduğu meslek veya zanaatın icrasını kural olarak belirli bir ücret veya kazanç karşılığında gerçekleştirmesi gerekmekle birlikte; bu işler öğrenme, deneme veya benzeri bir amaç ile geçici şekilde ücretsiz olarak da yürütülebilir. Meslek veya zanaatın bağımsız olarak mı yoksa bir iş veya hizmet sözleşmesi çerçevesinde bağlı olarak mı yürütüldüğü hususu ise nitelikli halin uygulanması yönünden önem taşımaz (Kangal, 2019).

Bu nitelikli halin uygulanabilmesi için, failin icra ettiği meslek veya zanaatın kişisel verilerin verilmesi, yayılması veya ele geçirilmesi yönünden ona bir kolaylık sağlamaya elverişli olması ve failin bu

kolaylıktan yararlanmak suretiyle kişisel veri ihlalini gerçekleştirmiş olması gerekir (Özbek, Doğan, Bacaksız ve Tepe, 2017; Soyaslan, 2012). Buradaki kolaylık sağlamadan anlaşılması gereken husus ise hiç kuşkusuz meslek veya zanaatın icrası ile suçun işleniş biçimi arasında bir nedensellik ilişkisinin bulunmasıdır (Özbek, Doğan, Bacaksız ve Tepe, 2017; Börekçi, 2019). Örneğin, bir polis memurunun PVSK md.4 uyarınca durdurma ve kimlik sorma yetkisi kapsamındaki gerçekleştirilen yasal denetim faaliyeti esnasında kimlik bilgilerini öğrendiği bir kişiye ait kimlik belgesindeki kişisel verilerin resmini çekerek telefonuna kaydetmesi veya evlere yemek siparişi götüren motosikletli kuryenin bu yolla telefon numarasını öğrendiği kişiyi mesaj veya arama yoluyla rahatsız etmesi örneklerinde, bu nitelikli hal uygulama alanı bulur. Özel hayatın gizliliğini ihlal suçu kapsamında kalsa da Yargıtay; mağdurun, doktor olarak çalıştığı özel hastanede farklı kadınlarla cinsel ilişkiye girdiği esnada gizlice kaydettiği görüntüleri bilgisayarına depoladığı ve 2010 yılı içerisinde arızalanan bilgisayarının tamiri için sanığın çalışmakta olduğu firmayla anlaştığı, sanığın mağdura ait bilgisayarı tamir ederken, mağdurun cinsel içerikli görüntülerini fark edip kişisel hard diskine bu görüntüleri kopyaladığı ve adı geçen sanığın firmadan ayrıldığı 2012 yılında, arkadaşları olan diğer sanıklar ile fikir ve eylem birliği içerisinde hareket ederek, mağdurdan görüntüleri iade etme karşılığında para talep edip aksi takdirde görüntüleri yayacakları tehdidiyle mağdura şantaj yaptığı olayda özel hayatın gizliliğini ihlal suçunun yanı sıra 137/1-b hükmünü de ağırlaştırıcı sebep olarak uygulamıştır (Y. 12. CD., E. 2015/5128, K. 2016/10207, T. 15.06.2016). Bu bakımdan benzer bir husus 136/1 durumunda da gündeme gelebilecektir.

Manevi Unsurlar

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, kasten işlenebilen bir suçtur (Hafızoğulları ve Özen, 2010). Buna göre, failin mağdura ait kişisel verileri bir başkasına verdiğini, yaydığını veya ele geçirdiğini bilerek ve isteyerek hareket etmiş olması, suçun oluşması için yeterlidir. Kanun'da suçun işlenmesi esnasında herhangi bir saik, amaç veya maksatla hareket edilmiş olması aranmadığı için, bu suç genel kast ile işlenebilen bir suçtur, ayrıca bir özel kastın varlığı aranmaz. Yine Kanun'da suçun taksirle işlenebileceğine ilişkin bir düzenleme bulunmadığı için, bu suçun taksirle işlenebilmesi de mümkün değildir (Korkmaz, 2019).

Buna karşın, failin bu suçun kanuni tanımında yer alan hareketleri olası kastla gerçekleştirmiş olması hususu ise tartışmalıdır. Bu konuda bir görüş, failin, mağdura ait olduğunu öngördüğü kişisel verileri, bu durumu kabullenerek bir başkasına vermesi, yayması veya ele geçirmesi durumunda, bu suçun olası kastla da işlenebileceğini kabul etmektedir (Özbek, Doğan, Bacaksız ve Tepe, 2017). Yine fail mağdura ait kişisel verileri üzerinde gerçekleştirmiş olduğu ihlalin, bu verileri başka kişiler tarafından ulaşılabilir hale getireceğini veya bu verilerin başka kişilerin eline geçebileceğini öngörmüş olmasına karşın, bu durumu kabullenerek hareket etmiş ise yine olası kastla işlenen bir suçtan söz edilir (Kangal, 2019).

Buna karşılık, TCK md. 136'da "hukuka aykırılı olarak" şeklinde belirtilen özel hukuka aykırılık düzenlemesine manevi unsur yönünden sonuç bağlayan diğer görüş ise suçun kanuni tanımındaki bu düzenlemenin faildeki özel hukuka aykırılık bilinci bulunması gerektiğine işaret ettiğini ve bu itibarla bu suçun yalnızca doğrudan kast ile işlenebileceğini belirtmektedir (Yaşar, Gökcan ve Artuç, 2014).

Keza Yargıtay da vermiş olduğu bir kararda kişisel veri kapsamındaki bilgiyi verme veya yayma açısından failin hukuka aykırılık bilinci taşıması gerektiğine hükmetmiştir: "*Aksi kanıtlanamayan savunmaya ve dosya kapsamına göre; katılan ... tarafından, resmi nikahlı eşi olan sanık ...'ün olumsuz tutum ve davranışlarından dolayı evlilik birliğinin ve müşterek hayatın çekilmez hale geldiği iddiasıyla açılan boşanma davasının reddine ilişkin kararın temyiz aşamasında olduğu ve tarafların halen evli oldukları dönemde, katılanın etrafındaki ortak tanıdıklarına evli olmadığını söylediğini işiten ve katılanın kendisini bekar olarak tanıtıp katılanla onun işyeri arkadaşı olan tanık ... arasında duygusal birliktelik başladığını öğrenen sanığın, katılanla halen evli olduklarını göstermek amacıyla, Karatay Nüfus Müdürlüğünden temin ettiği, eşi ve müşterek çocuklarının da nüfus bilgilerini içeren kendisine*

ait nüfus kayıt örneğini, katılanın işyeri arkadaşları olan tanıklar ... ve ...'ya, facebook adlı sosyal paylaşım sitesindeki hesapları üzerinden mesaj olarak gönderdiği olayda,

Eşinin sergilediği davranışlardan dolayı onuru zedelenen ve katılanla beraber olma düşüncesini taşıyan kadınlar tarafından katılanın bekar olmayıp halen kendisi ile evli olduğunun öğrenilmesini isteyen sanığın, aile birliğini koruma amacını taşıyan eylemlerinde hukuka aykırı hareket ettiği bilinciyle davrandığı kabul edilemeyeceğinden, sanığın üzerine atılı verileri hukuka aykırı olarak verme veya ele geçirme suçundan dolayı beraatine dair yerel mahkemenin kararında bir isabetsizlik görülmemiştir." Y. 12. CD., E. 2015/10438, K. 2016/12933, T. 23.11.2016).

İncelediğimiz suç tipinin gerçekleşebilmesi için failin suçunu konusunu oluşturan kişisel verilerin, kimliği belirli veya belirlenebilir bir gerçek kişiye ait bir bilgi olduğunu bilerek hareket etmiş olması gerekir. Failin suçun konusuna ilişkin olarak bir bilgisizlik veya yetersiz bilgi ile hareket etmiş ya da daha somut bir deyişle bir başkasına verdiği, yaydığı veya ele geçirdiği bilginin bir kişisel veri olduğunu bilmeden hareket etmiş ise bu durumda TCK md. 30/1 uyarınca suçun kanuni tanımında maddi unsurlarında hataya düşmüştür. Bu tarz bir hata, failin kastını ortadan kaldırır. Örneğin, bir şirkette insan kaynakları uzmanı olarak çalışan failin, yüksek lisans başvurusunda bulunduğu üniversiteye başvuru evrakı kapsamında kendi özgeçmişini göndermesi gerekirken yanlışlıkla şirketine iş başvurusunda bulunmuş bir adayın özgeçmişini göndermesi halinde, suçun konusuna ilişkin olarak hataya düşülmesi söz konusudur. Bu durumda failin zihninden geçen, tasavvur ettiği ile gerçek durum birbirinden farklıdır. Ancak olayın failin tasavvur ettiği şekilde gerçekleşmesi ya da diğer ifadeyle kendisine ait özgeçmişi üniversiteye göndermiş olması durumunda, bu hareketi TCK md. 136 kapsamında suç teşkil etmeyeceği için failin düşmüş olduğu hata esaslı bir hatadır ve somut vakıada düşmüş olduğu bu hatadan yararlanır. Bu noktada, TCK md. 30/1 kapsamında bir hata mevcut olduğu için bu hataya ilişkin herhangi bir kaçınılmazlık değerlendirmesi de yapılmayacaktır (Börekçi, 2019). Nihayet burada failin, taksirle hataya düşmüş olmasının da herhangi bir önemi yoktur; zira fail, objektif özen yükümlülüğünü ihlal etmek suretiyle, gerekli dikkat ve özeni göstermediği için hataya düşmüş olsa bile TCK md. 136'daki suçun taksirli şekli kanunda düzenlenmediği için bu taksirli davranışından dolayı sorumlu tutulabilmesi mümkün değildir.

Hukuka Aykırılık Unsuru

Hukuka aykırılık, fail tarafından işlenen ve kanuni tanıma uygun bulunan fiile hukuk düzeni tarafından cevaz verilmemesidir. Bu şekildeki bir fiil yalnızca ceza hukuku ile değil ancak; hukuk düzeninin tümü ile bir çelişki ve çatışma içerisinde demektir (Katoğlu, 2003; Artuk, Gökcen, Alşahin ve Çakır, 2017). TCK md. 136'daki suçun oluşabilmesi için de işlenen fiilin hukuka aykırı olması zorunludur. Bununla birlikte, TCK md. 136'da düzenlenen suçun kanuni tanımında –tıpkı kişisel verilerin hukuka aykırı olarak kaydedilmesine ilişkin TCK md. 135'deki suç tipinde olduğu gibi ayrıca "hukuka aykırı olarak" ibaresine yer verilmiştir. Fail tarafından işlenen bir fiilin suçun kanuni tanımına uygun yani tipe uygun olması, kural olarak o fiilin hukuka aykırı olduğu hususunda bir karine teşkil eder (Özbek, Doğan, Bacaksız ve Tepe, 2016). Bu nedenle, hukuka aykırılığın kanuni tipte açıkça dile getirilmesi gerekli değildir; hukuka aykırılık o fiilin hukuk düzeniyle çatışma içerisinde olması nedeniyle zaten kendiliğinden mevcuttur. Bununla birlikte, inceleme konumuzu oluşturan TCK md. 136'da olduğu gibi, bazı suçlarda hukuka aykırılığa suçun kanuni tanımında açıkça yer verilmesi halinde, "hukuka özel aykırılık" olarak isimlendirilen bir durum ortaya çıkar. Buna göre, hukuka aykırılığın kanunda özel olarak zikredilmiş olduğu buradaki gibi ifadeler, suç tipinin bütününün değerlendirilmesiyle ilgiliyse, bu takdirde bu durum, fiilin genelini değerlendiren unsurlar öğretisi uyarınca yalnızca hukuka aykırılığın suçun genel bir unsuru olduğuna işaret eden ve kanun koyucunun hâkimi hukuka uygunluk sebebinin varlığını araştırmaya yönelttiği bir belirlemeden ibarettir. Buna karşın, hukuka aykırılığın kanunda özel olarak zikredilmiş olması, münferit bir unsurun sıfatı olarak kullanılmış ise bu halde suç tipine ait bir unsur olarak değerlendirilir (Artuk, Gökcen, Alşahin ve Çakır, 2017). Bu durumda, failin suç tipine dâhil

olan bu sıfatı da bilerek ve isteyerek hareket etmiş olması ya da diğer bir anlatımla kastının hukuka özel aykırılığı da kapsaması gerekir (Koca ve Üzülmez, 2018).

Bu bilgiler ışığında, TCK md. 136'daki hukuka özel aykırılık ifadesi, suç tipine ilişkin herhangi bir maddi unsurunu tanımlamamakta ancak fiilin genelini değerlendirmek suretiyle, bir bütün olarak hukuka uygun olup olmadığına ilişkin bir belirlemede bulunmaktadır. Bu nedenle, TCK md. 136'daki "hukuka aykırı olarak" ibaresi suç tipinin maddi unsurlarına dâhil olmayıp fiilin bir bütün olarak hukuka uygun olup olmadığına ya da diğer deyişle fiilin genelini değerlendiren bir unsur niteliği taşımaktadır. Buna göre, kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesine ilişkin kanuni tanımda yer alan hukuka aykırılık, suç tipine ait münferit bir unsurun sıfatı olarak kullanılmamıştır, suçun maddi unsuruna dâhil bir unsur değildir (Kangal, 2019).

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunda, TCK'nın genel hükümlerinde düzenlenen hukuka uygunluk nedenlerinin yanında KVKK md. 5'te düzenlenen hukuka uygunluk nedenlerinin de uygulanması mümkündür. Ancak 2016 yılında sonraki kanun olarak yürürlüğe giren KVKK ile TCK'nın genel hükümlerindeki hukuka uygunluk nedenlerine ilave birtakım koşulların öngörüldüğü belirlenebilir. Bu itibarla, TCK ile KVKK arasında bir genel norm-özel norm ilişkisinden söz etmek yanlış olmaz. Bu ilişkinin kurulmasının mümkün olmadığı hukuka uygunluk nedenleri ise KVKK'da düzenlenmiş olmalarına karşın, TCK'da bir karşılıkları bulunmayan, "alenileştirme" ve "meşru menfaat" şeklindeki hukuka uygunluk nedenleridir (Börekçi, 2019). Aşağıda önce TCK md. 136 yönünden, TCK ve KVKK uyarınca uygulanabilir olan hukuka uygunluk nedenlerine, sonrasında ise yine bu suç açısından KVKK'ya özgü olarak düzenlenmiş olan iki hukuka uygunluk nedenine kısaca değinilecektir.

Bu konuda değinilmesi gereken ilk hukuka uygunluk nedeni, TCK md. 24/1'de "*kanunun hükmünü yerine getiren kimseye ceza verilmez*" şeklinde düzenlenmiştir. Buna göre, bir kanun hükmünün yerine getirilmesi kişisel verilerin bir başkasına verilmesi yayılması veya ele geçirilmesi fiillerini hukuka uygun hale getirebilir. KVKK'nın kişisel verilerin işlenme şartları başlıklı 5. maddesinde, kanunlarda açıkça öngörülmesi halinde kişisel veriler ilgili kişinin açık rızası aranmaksızın işlenebileceği düzenlenmiştir (KVKK md. 5/2-a). Yine KVKK'nın özel nitelikli verilerin işlenme şartlarını düzenleyen 6. maddesinde ise bu maddede sayılan sağlık ve cinsel hayat dışındaki özel nitelikli verilerin, kanunlarda öngörülen hallerde ilgilinin açık rızası olmaksızın işlenebilmesi imkânı getirilmiştir (KVKK md. 6/3) (Sert, 2019).

TCK md. 136'da düzenlenen suç tipi yönünden, kanun hükmünün yerine getirilmesi hukuka uygunluk nedeninin kapsamına girecek yasal düzenlemelere örnek olarak Adli Sicil Kanunu gösterilebilir. Adli Sicil Kanunu'na göre kural olarak adli sicil ve arşiv bilgileri gizlidir ve görevlilerce başkalarına açıklanamaz. Ancak aynı Kanun'un 7. 8. ve. 10. maddelerinde, kişinin özel nitelikli kişisel verisi olan ceza mahkûmiyetini içeren adli sicil bilgilerinin, kullanılış amacı belirtilmek suretiyle kamu kurum ve kuruluşlarına verilebilmesi yetkisi düzenlenmektedir. Bu nedenle, belirtilen hükümlere dayanarak bir kişinin ceza mahkûmiyeti kayıtlarını elde eden kamu kurumu yetkililerinin bu davranışı, kanun hükmünü yerine getirme hukuka uygunluk nedeni kapsamında yer aldığı için TCK md. 136'daki suçu oluşturmaz.

Bu konuda diğer bir örnek olarak Ceza Muhakemesi Kanunu (CMK) gösterilebilir. CMK md. 75, 76 ve 78'de düzenlenen beden muayenesi, biyolojik örnek alınması ve moleküler genetik incelemesi şeklindeki delil elde etme araçlarının işletilmesi suretiyle her biri birer özel nitelikli kişisel veri olan sağlık, cinsel hayat ve genetik verilere ulaşılabilmektedir. Bununla birlikte, bu özel nitelikli kişisel verilerin elde edilmesi işlemi bir ceza soruşturması veya kovuşturması faaliyetine bağlı olarak yürütüldüğü için TCK md. 136'daki suçu oluşturmaz. Bu konuda kapsamlı bir mevzuat incelemesi yapıldığında Umumi Hıfzıssıhha Kanunu (md. 57,104,113), Avukatlık Kanunu (md. 46/2) ve Kimlik Bildirme Kanunu (Ek md. 1) gibi çok çeşitli kanunlarda, kişisel verilerin verilmesi, yayılması veya ele

geçirilmesi fiillerinin suç niteliğini ortadan kaldıran hukuka uygunluk nedenlerinin düzenlendiği tespit edilebilir (Börekçi, 2019).

TCK md. 136 yönünden uygulanabilecek diğer bir hukuka uygunluk nedeni olan "ilgilinin rızası" TCK md. 26/2'de "kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez" biçiminde düzenlenmiştir. Bu düzenleme uyarınca, ceza hukuku açısından ilgilinin rızası şeklindeki hukuka uygunluk nedeninin uygulanabilmesi için kişinin rıza gösterilecek hak üzerinde mutlak surette tasarruf yetkisinin bulunması, rıza gösterme ehliyetine sahip olması ve rızasını bir davranış ile açıklaması, biçiminde özetlenebilen koşulların birlikte gerçekleşmiş olması gerekir (Artuk, Gökcen, Alşahin ve Çakır, 2017). İncelediğimiz suç tipi bu koşullar yönünden ele alındığında, ilk olarak belirtilmelidir ki, kişisel veri ilgilinin üzerinde mutlak surette tasarruf edebileceği haklar arasında yer alır. Şu hâlde kişisel verilerin sahibinin, bu verilerin bir başkasına verilmesine, yayılmasına veya ele geçirilmesine rıza göstermesi halinde, bu rızanın varlığı TCK md. 26/2 uyarınca, fiili hukuka uygun hale getirir. Bu açıdan ani bir kalp rahatsızlığı ile hastaneye kaldırılan bir siyasetçinin, tedavi altına alındıktan sonra, hastane yönetiminin sağlık durumuyla ilgili kamuoyuna açıklama yapmasına rıza göstermesi, bu kapsamda yer alır (Aydın, 2013; Kangal, 2019). KVKK sisteminde ise rıza kavramı, TCK'daki düzenlemeden farklılaşmaktadır. Buna göre, KVKK'da, "ilgilinin rızası" veya "rıza" kavramı yerine "açık rıza" kavramına yer verilmiştir. Açık rıza, Kanun'da "belirli bir konuya ilişkin bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza" biçiminde tanımlanmıştır (KVKK md. 3/1-a) (Dülger, 2020). Bu tanımın da ortaya koyduğu üzere, TCK'da düzenlenen ilgilinin rızası için gerekli bulunan 3 koşuldan, rıza gösterilecek hak üzerinde mutlak tasarruf yetkisinin bulunması ve rıza gösterme ehliyetine sahip olunması şeklindeki ilk iki koşul, KVKK'daki açık rıza için de geçerli bulunmaktadır. Bu açıdan KVKK'daki açık rızanın, TCK'daki ilgilinin rızasından ayrıştığı husus ise rızanın bir davranış ile açıklanmasına ilişkin son koşula ilişkin ortaya çıkar. Çünkü açık rızanın açıklanış biçimi ile ilgilinin rızasının açıklanış biçimi birbirinden farklılık arz eder (Börekçi, 2019).

Şöyle ki, TCK anlamında rızanın açıklanması açık veya örtülü bir biçimde gerçekleştirilebileceği halde, KVKK anlamında açık rıza kavramı ise gerek kanundaki tanımı ve gerekse lafzı itibarıyla örtülü bir rıza açıklaması şeklinde gerçekleştirilmeye elverişli değildir (Dülger, 2020; aksi görüş Çekin, 2019). Nitekim KVKK md. 19 uyarınca veri koruma otoritesi olarak kurulmuş olan Kişisel Verileri Koruma Kurumu'nun hazırlamış olduğu Açık Rıza Rehberi'nde de ülkemizde özel nitelikli olan veya olmayan, her türlü kişisel verinin işlenmesi için açık rızaya ihtiyaç bulunduğu vurgulanmıştır (Kişisel Verileri Koruma Kurumu, t.y.). Bu itibarla, TCK md. 136'da yer alan suçun konusunu oluşturan kişisel veriler yönünden örtülü rızanın varlığı, hiçbir biçimde bir hukuka uygunluk nedeni olarak kabul edilemez (Börekçi, 2019).

Diğer yandan KVKK'daki tanım uyarınca, açık rıza bilgilendirmeye dayalı olması yönünden de TCK md. 26/2'deki ilgilinin rızasından ayrılır. Bilgilendirmeye dayalı açık rıza, veri sorumlusunun, ilgili kişiden rıza talebinde bulunurken veya ilgili kişi rıza açıklamasında bulunurken hangi verilerin, hangi konuya ilişkin olarak işleneceği, rıza beyanının niteliği ve sonuçları, geri alınıp alınmayacağı hususlarında bilgilendirilmiş olmayı zorunlu kılar. Diğer bir ifadeyle, bilgilendirmeye dayalı açık rıza için ilk olarak, kişisel veriler üzerinde gerçekleştirilecek bütün faaliyetlere ilişkin olarak kapsamlı, sarih ve anlaşılır bir bilgilendirmenin yapılmış olması ve bunun yanı sıra bu bilgilendirme işleminin kişisel verilerin işlenmesinden önce veya en geç veri işleme faaliyetinin gerçekleştirildiği esnada yapılmış olması gerekir (Dülger, 2020). Bu nedenle, belirtilen bu yükümlülüklere riayet edilmeksizin kişisel veriler üzerinde TCK md. 136 kapsamında gerçekleştirilecek tasarrufların hiçbiri, buradaki hukuka uygunluk nedeninden yararlanamazlar.

TCK md. 136 yönünden uygulanabilecek başkaca bir hukuka uygunluk nedeni olan hakkın kullanılması, TCK md. 26/1'de "hakkını kullanan kimseye ceza verilmez" şeklinde düzenlenmiştir. Hakkın kullanılması hukuka uygunluk nedeninin yasal mevzuat içerisinde geniş bir yelpazede ve çok farklı

görünüş biçimlerinin bulunduğu tespit edilebilir (Artuk, Gökcen, Alşahin ve Çakır, 2017). Kişisel verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesine ilişkin olarak ise hakkın kullanılması hukuka uygunluk nedeni ilk olarak dilekçe hakkı kapsamında ortaya çıkabilir. Bu kapsamda, söz gelimi Cumhuriyet Başsavcılığına verilen bir şikâyet dilekçesinde şikâyet edilen kişinin adı, soyadı, adresi, telefon numarası şeklindeki kişisel verilerinin yer alması örneğinde olduğu gibi, yargısal veya idarî mercilere yapılan yazılı başvuruların başkalarının kişisel verilerini içermesi durumunda, bu durum, dilekçe hakkının kullanılmasıdır ve hakkın kullanılması hukuka uygunluk nedeni kapsamında yer aldığı için, fiil hukuka uygundur. Bununla paralel olarak, kişisel veri niteliğindeki bilgi ve belgelerin ilgili mercilere, iddia ve savunma hakkı (1982 Anayasası md.36/1, TCK md.128) kapsamında verilmesi veya yayılması hallerinde de, yine hakkın kullanılması şeklindeki hukuka uygunluk nedeni söz konusu olur. Bunun yanı sıra, kişisel verilere ilişkin TCK md.136 kapsamındaki tasarrufların, yine bir hakkın kullanılması biçimi olan basının haber verme hakkı çerçevesinde hukuka uygun hale gelebilmesi de mümkündür. Bu konuda özellikle magazin basını örneğinde gibi, işin mahiyeti gereği kişilerin özel hayatıyla ilgili olarak yapılan yayınların çoğu kez kişisel verileri de içermesi kaçınılmaz bir durumdur. Bu nedenle, kişisel verilerin bu şekilde yayılması faaliyetinin hukuka uygun olabilmesi için haber verme hakkının koşullarını oluşturan gerçeklik, güncellik, kamu yararı ve toplumsal ilgi ile düşünce ve ifade arasında düşünsel bağlılık ve güncellik sınırları içerisinde gerçekleştirilmiş bulunması gerekir (Dönmezer ve Bayraktar, 2016; Kangal, 2019). Nihayet bunların yanı sıra, ifade özgürlüğü (AY md.25-26) ile sanat özgürlüğü kapsamında yapılan bilimsel araştırmalarda da kişisel verilerin verilmiş, yayılmış veya ele geçirilmiş olması, hakkın kullanılması hukuka uygunluk nedeni kapsamında değerlendirilmelidir.

Bu noktada, TCK'da düzenlenmemiş olmakla birlikte, KVKK'da yer alan ve TCK md.136 yönünden uygulanabilir olan hukuka uygunluk nedenleri olan "alenileştirme" ve "meşru menfaat"e de kısaca değinmek gerekir.

Kişisel verilerin ilgili kişi tarafından alenileştirilmesi, KVKK kapsamında bir hukuka uygunluk nedeni olarak düzenlenmiştir (KVKK md.5/2-d ve 28/2-b). Buna göre, kişisel verilerini kendi özgür iradesiyle alenileştirmek suretiyle, kişi artık bu kişisel verileri üzerinde egemenliğinden kısmen de olsa vazgeçmiş olduğunu ortaya koymaktadır, dolayısıyla artık bu durumda korunması gereken bir menfaatin bulunduğundan söz edilemez (Yücedağ, 2017). Ancak bu hukuka uygunluk nedeni yalnızca genel nitelikteki kişisel verileri için söz konusu olup KVKK md. 6'da düzenlenen özel nitelikli kişisel veriler yönünden geçerli değildir.

Alenileştirmeden anlaşılması gereken, kişisel verilerin belirsiz kişi tarafından erişilebilir hale getirilmiş olmasıdır. Örneğin kişinin kendi resmini veya videosunu söz gelimi Instagram hesabında yayınlamış olması bir alenileştirmedir. Bununla birlikte, alenileştirme halinde kişisel veri üzerindeki egemenlik tümüyle değil ancak; kısmî şekilde ortaya kalkar. Diğer bir ifadeyle, bir kimsenin kişisel verisini alenileştirmiş olması, bu alenileştirmeye konu kişisel verilerin her türlü amaç ve yöntemle işlenebileceği anlamına gelmez. Bu çerçevede, alenileştirilmiş olan kişisel veriyi işleyen veri sorumlusunun KVKK'dan doğan bazı yükümlülükleri varlığını muhafaza etmektedir. Bunlar, veri sorumlusunun aydınlatma yükümlülüğü ile ilgili kişinin zararını giderme yükümlülüğü biçiminde ortaya çıkar (Börekçi, 2019).

KVKK kapsamında düzenlenen diğer bir hukuka uygunluk nedeni ise kişisel verilerin, veri sorumlusunun meşru menfaatleri doğrultusunda işlenmesidir (KVKK md. 5/2-f). Buna göre, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlemenin zorunlu olması, bir hukuka uygunluk nedenidir. Meşru menfaat, hukuk düzeni içerisinde cevaz verilen her türlü hukuki, iktisadi ya da kişisel menfaati ifade eder. Ancak, bu menfaatin soyut amaçlardan çok somut bir kullanım ya da işleme amacına yönelik olması gerekir (Çekin, 2019). Meşru menfaatin geniş yorumlanması durumunda kişisel verilerin korunması hakkına zarar verilebileceği ya da veri sorumlusunun meşru menfaatin sağladığı alan içerisinde haklarını kötüye kullanabilecekleri ileri

sürülerek meşru menfaat kavramına ilişkin olarak dar yorum ilkesinin geçerli olması gerektiği ve bu yola ancak son çare olarak başvurulması gerektiği ifade edilmiştir (Dülger, 2020). Bu yorumla paralel olarak ikinci koşul ise bahse konu meşru menfaate ulaşılabilmesi bakımından kişisel veri işlenmesinin zorunluluk arz etmesidir. Nihayet son olarak, veri sorumlusu ile kişisel verileri işlenen ilgili kişi arasında menfaat dengesinin hakkaniyetli bir biçimde gözetilmesi ve bu doğrultuda veri işleme faaliyeti ile ilgili kişinin temel hak ve özgürlüklerine zarar verilmemesi gerekir (Çekin, 2019). Bu kapsamda örneğin; bir işletmenin iş yeri güvenliğini sağlamak için ziyaretçilerin kimlik bilgilerini kaydetmesi, güvenlik kameraları ile ziyaretçilerin ve çalışanların kişisel verilerini işlemesi, meşru menfaat hukuka uygunluk nedenini oluşturur (Dülger, 2020).

SUÇUN ÖZEL OLUŞUM BİÇİMLERİ

Teşebbüs

Kişisel verileri hukuka aykırı aykırı olarak verme, yayma veya ele geçirme suçu, hareketi incelerken de değinildiği üzere, bir sırf hareket suçudur. Bu itibarla verme, yayma veya ele geçirme şeklindeki hareket biçimlerinden birinin gerçekleştirilmesi ile birlikte suç oluşur; ayrıca bir neticenin gerçekleşmesi aranmaz. Bu nedenle prensip olarak, bu suç teşebbüse elverişli bir nitelik taşımaz. Ancak suçun icra hareketlerinin parçalara bölünebilmesi ve bu hareketlerin failin elinde olmayan nedenler ile tamamlanamamış olması durumunda, teşebbüs hükümlerinin uygulanması mümkün olabilir (Soyaslan, 2012; İtişgen, 2015; Sert, 2019; Kangal, 2019). Yine de bu olasılığın yalnızca hukuka uygun olarak ele geçirilmiş kişisel verilerin bir başkasına verilmesi veya yayılması yönünden geçerli olabileceği belirtilmelidir. Çünkü eğer bu kişisel veriler önceden hukuka aykırı olarak ele geçirilmişlerse zaten bu ele geçirme hareketi ile suç tamamlanmış olacağı için sonraki verme veya yayma hareketleri yönünden teşebbüse elverişlilik söz konusu olmaz.

TCK md.136'daki suçun failinin, bir bilişim sistemindeki kişisel verileri hukuka aykırı olarak ele geçirmek için suçun icra hareketlerine başladıktan sonra, bilişim sistemine girmiş olmasına karşın, buradaki kişisel verilerin içeriğini öğrenmeden kendi isteğiyle icra hareketlerine devam etmekten imtina etmesi durumunda, TCK md.36 uyarınca gönüllü vazgeçme hükümlerinin uygulanması söz konusu olabilir. Bu tarz bir durumda fail, kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüsten değil ancak o zamana kadar gerçekleştirdiği fiil TCK md.243 uyarınca bilişim sistemine yetkisiz girme suçunu oluşturduğu için tamamlanmış olan bu suçtan dolayı sorumlu olacaktır (Akdağ, 2013; Korkmaz, 2019).

İştirak

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, iştirak müessesesi yönünden özellik gösteren bir suç tipi değildir; suça iştirakin her şeklinin gerçekleşmesi mümkündür.

Bu suçta düzenlenen seçimlik hareketlerin farklı kişiler tarafından farklı zaman dilimlerinde gerçekleştirilmiş olması durumunda, tek bir suça iştirak edilmesinden ziyade, birden fazla suçun işlenmesi olasılığı bulunur. Buna karşın, bu seçimlik hareketler failler arasında önceden anlaşmaya dayalı bir suç işleme kararı kapsamında ortaya çıkmış ise bu takdirde suça iştirak hükümleri uygulanabilir. Örneğin, faillerden birisi mağdura ait kişisel verileri elde ettikten sonra, önceden anlaştıkları şekilde diğer faile göndermiş ve diğer fail de bu kişisel verileri yaymış ise bu durumda suça iştirakten söz edilebilir. Ancak aynı silsile, aralarında bir anlaşma olmaksızın gerçekleşmiş ise birlikte suç işleme kararının bulunmaması nedeniyle, her failin fiili ayrı bir suç teşkil edecektir (Korkmaz, 2019).

İştirak halinde işlenen kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunun faillerden birisinin, görevinin verdiği yetkiyi kötüye kullanan bir kamu görevlisi olması (TCK md.137/1) veya belirli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle fiili işlemiş olması durumunda, bir görünüşte özgü suç ortaya çıkar. Bu tarz bir durumda, kişisel verilerin verilmesi, yayılması veya ele geçirilmesi fiillerine iştirak eden fakat bu şekilde bir özel faillik sıfatına sahip bulunmayan diğer suç ortakları ise TCK md.40/2 uyarınca azmettiren veya yardım eden sıfatıyla cezalandırılacaklardır.

İçtima

Kişisel verileri hukuka aykırı olarak, yayma veya ele geçirme suçunun TCK md. 42 uyarınca bir bileşik suç biçiminde ortaya çıkması söz konusu olabilir. Bu durumda, TCK md. 136'daki suçu oluşturan hareket biçimlerinin, bir başka suçun unsuru veya cezayı ağırlaştıran bir nitelikli hali olarak ortaya çıkması durumunda, TCK md. 136'dan dolayı ayrıca bir ceza verilmez. Bu kapsamda söz gelimi bir restoranda garson olarak çalışan failin ödemeyi kredi kartı ile yapan müşterinin kredi kartı bilgilerini kopyaladıktan sonra, mağdurun banka hesaplarıyla ilişkilendirerek sahte banka veya kredi kartları üretmesi durumunda, bu fail TCK md. 245/2 uyarınca cezalandırılır. Buna karşın, bu tarz bir durumda, kişisel verilerin hukuka aykırı olarak geçirilmiş olması TCK md. 245/2'de düzenlenen suçun zorunlu bir unsurunu oluşturduğu için bir bileşik suç ilişkisi ortaya çıkar ve fail ayrıca TCK md. 136'daki suçtan dolayı cezalandırılmaz (Kangal, 2019). Nitekim Yargıtay da; "Gerçek kartların manyetik şerit bilgilerini kopyalamak, şifrelerini elde etmek ve elde etmiş oldukları kart bilgilerini beyaz kart tabir edilen kartlar ile değişik amaçlarla ellerinde bulunan diğer kartlara encoder cihazı aracılığı ile kopyalayıp, bankada bulunan hesaplarla ilişkilendirerek sahte kart üretme eylemin kül halinde TCK md. 245/2. maddesine uyduğu gözetilmeden, ayrıca TCK'nın 136. maddesiyle cezalandırılmasına karar verilmesi…" kararıyla bu hususa işaret etmiştir (Y. 8. C.D., E. 2016/6350, K. 2016/8725, T. 30.06.2016).

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu zincirleme şekilde de işlenebilir. Buna göre, aynı kişiye ait bulunan kişisel verilerin, aynı suç işleme kararının kapsamında olarak değişik zamanlarda başkaca kişilere verilmiş, yayılmış veya ele geçirilmiş ise, TCK md. 43/1 uyarınca zincirleme suç hükümleri uygulanır (İtişgen, 2015). Buna göre, bu kapsamdaki fiiller hakkında tek bir ceza uygulanır ancak verilecek olan bu ceza dörtte birden dörtte üçüne kadar arttırılacaktır. Zincirleme suç hükümlerinin uygulanması için, kişisel verilerin aynı nitelikte olması aranmaz. Bu kapsamda, bir sosyal paylaşım sitesinde, fail tarafından aynı kişinin önce resminin daha sonra ise kimlik bilgilerinin paylaşılması durumunda, zincirleme suç hükümleri uyarınca artırılmış tek bir ceza uygulanacaktır (Korkmaz, 2019; Kangal, 2019). Bu durumda mağdura ait kişisel verilerin bu sosyal paylaşım sisteminde yayınlanmaya devam ettiği sürece, işlenen suçun kesintisiz (mütemadi) şekilde işlenmekte olduğu kabul edilmeli ve bu süreçte suç fiilinin ancak bahse konu paylaşımın yayından kaldırılması ile bittiği ve zamanaşımının başlangıcı gibi sonuçların da ancak bu andan itibaren doğmuş sayılacağı esası benimsenmelidir (Korkmaz, 2019).

TCK sisteminde kişisel verilerin verilmesi, yayılması veya ele geçirilmesi şeklindeki hareket biçimleri ile doğrudan ilişkili bulunan bazı suç tipleri bulunmaktadır ve bu suçlar ile TCK md. 136 arasında suçların içtimaına ilişkin olasılıkların kısaca ortaya konulması gerekmektedir.

Bu çerçevede ilk olarak, TCK md. 136 ile aynı bölümde düzenlenmiş olan özel hayata ve hayatın gizli alanına karşı suçlar ele alınmalıdır. TCK md. 132'de düzenlenen haberleşmenin gizliliği ihlal suçu kapsamında, kişiler arasındaki haberleşme içeriklerinin ifşa edilmesi (md. 132/2) ile kendisiyle yapılan haberleşmelerin içeriğinin diğer tarafın rızası olmaksızın hukuka aykırı olarak ifşa edilmesi (Md. 132/3) fiilleri ele alındığında, bu her iki hüküm yönünden suçun konusunu oluşturan "ifşa edilen haberleşme içeriklerinin", başkasına veya diğer tarafa ait kişisel verileri içermesi çoğu kez kuvvetle muhtemeldir. Bu tarz bir durumda, bu ifşa hareketi, TCK md. 132 ile birlikte TCK md. 136'daki suçun oluşmasına da sebebiyet verecektir. Bu tarz bir durumda, fail tek bir fiil ile Kanun'da düzenlenmiş bulunan birden fazla

hükmü ihlal etmiş olacağı için TCK md. 44 uyarınca "Farklı neviden fikri içtima" hükümlerinin uygulanması gerekir (Artuk, Gökcen, Alşahin ve Çakır, 2017). Diğer bir deyişle, işlediği fiil nedeniyle birden fazla farklı suçun (TCK md. 132 ve TCK md. 136'da yer alan suçların) oluşmasına sebebiyet veren fail, işlediği bu suçlardan daha ağır cezayı gerektiren suç olan TCK md. 136 uyarınca cezalandırılacaktır.

Benzer bir ifşa faaliyeti TCK md. 133/3'de kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçuna ilişkin olarak düzenlenmiş olup bu suç ile TCK md. 136 uyarınca da benzer bir içtima ilişkisi ortaya çıkabilir. Buna göre, kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verilerin hukuka aykırı olarak ifşa edilmesi durumunda, ifşa edilen bu verilerin içeriğinde başkasının veya diğer tarafın kişisel verilerinin yer alması hem TCK md. 133/3 hem de TCK md. 136 hükümlerinin uygulanmasını gerekli kılar. Ancak bu tarz bir durumda da, fail tek hareketle Kanun'daki birden fazla suçun oluşmasına sebebiyet verdiği için yine "farklı neviden fikri içtima" hükümlerinin uygulanması söz konusu olur. Bununla birlikte, bu kez, TCK md. 133/3'de yer alan suç ile TCK md. 136'daki suçun alt sınırları aynı olmasına karşın, TCK md. 133/3'deki suçun üst sınırı daha yüksek olduğu için fail daha ağır olarak kabul edilen bu suç uyarınca cezalandırılacaktır.

TCK md. 134'de düzenlenen özel hayatın gizliliğini ihlal suçu ise özel hayata ve hayatın gizli alanına karşı suçlar içerisinde torba hüküm olarak nitelendirilen bir suç tipidir (Zafer, 2014). Bu itibarla, özel hayatı ve hayatın gizli alanını koruyan suç tipleri ile TCK md. 134 arasında bir özel norm-genel norm ilişkisi bulunmaktadır. Diğer bir ifadeyle, somut vakıada, özel norm niteliğini taşıyan suç tipinde TCK md. 134'ün unsurlarına ilave olarak yer alan diğer koşullar gerçekleşmiş ise, bu özel norma ilişkin hükümler uygulanacaktır. Buna göre, hukuka aykırı olarak verilen, yayılan veya ele geçirilen bilgi veya belgelerin kişisel veri niteliğinde olması durumunda artık genel norm olan TCK md. 134 değil ancak bu konuda özel norm olan TCK md. 136 uygulanacaktır (Akyürek, 2014). Ancak kişisel veri niteliği taşımayan bilgi veya belgeler ya da TCK md. 134/2'deki ses veya görüntü kayıtları yönünden ise TCK md. 134'deki genel norm uygulanacaktır. Bu konudaki diğer bir görüş ise kişinin özel hayatına ilişkin bir ses veya görüntünün TCK md. 134 kapsamında cezalandırılması gerektiği yönündedir (Yaşar, Gökcan ve Artuç, 2014). Yargıtay içtihatlarında da benimsenen bu görüşe göre, TCK md. 136 hükmünün uygulanabilmesi için ancak "özel hayata ilişkin olma" kriterinin dışında kalan, diğer bir ifadeyle TCK md. 134'ün uygulanma kabiliyeti bulunmayan, kişisel veriler hakkında söz konusu olabilir: "*Sanığın, mağdura ait facebook hesabından ele geçirdiği mağdurun günlük kıyafetleriyle poz vermiş şekilde çektirdiği resimlerini, aynı sitede mağdur adına açtığı sahte hesap üzerinden, mağdurun rızasına aykırı şekilde yayımladığı olayda; Mağdura ait facebook hesabında mağdur tarafından yayımlanan ve mağdurun günlük kıyafetleriyle poz vermiş şekilde çektirdiği resimleri, mağdurun başkalarının görmesini ve bilmesini istemeyeceği özel yaşam alanına ilişkin görüntü olarak kabul edilemeyeceğinden, mağdurun kişisel veri niteliğindeki resimlerini, hukuka uygunluk nedenlerinin bulunmaması nedeniyle hukuka aykırı olduğunda tereddüt bulunmayan bir yöntemle facebook adlı sosyal paylaşım sitesi üzerinden yayımlayan sanığın eyleminin, TCK'nın 136/1. madde ve fıkrasında tanımlanan verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna dair yerel mahkemenin kabulünde dosya kapsamına göre bir isabetsizlik görülmemiştir.*" (Y. 12. C.D. E:2018/7939 – K: 2019/640, T: 16.01.2019). Yine bir diğer görüş ise tek bir fiil ile TCK md. 134 ile TCK md. 136 hükümleri birlikte ihlal edildiğinde, TCK md. 44 uyarınca farklı neviden fikri içtima kuralları kapsamında daha ağır olan suçun cezasının verilmesi gerektiğini savunmaktadır (Börekçi, 2019).

Bu konuda son olarak, TCK md. 136 ile bilişim sistemine hukuka aykırı olarak girme fiilini düzenleyen TCK md. 243 arasındaki ilişkiye değinmek gerekir. Çünkü teknolojik gelişmelerin etkisiyle, kişisel veriler giderek artan şekilde bilişim sistemlerine kaydedilmekte ve bilişim sistemlerinde bulundurulmaktadır. Bu nedenle, bugün TCK md. 136 kapsamında özellikle kişisel verilerin hukuka aykırı olarak ele geçirilmesi şeklindeki seçimlik hareketin bilişim sistemleri üzerinden gerçekleştirildiği ve dolayısıyla aynı zamanda TCK md. 243'deki suçun da gerçekleştiği ifade edilebilir. Bununla birlikte,

TCK md. 243, TCK md. 136 açısından bir "geçit suçu" niteliği taşımaz. Çünkü geçit suçundan söz edebilmek için bulunması gereken, bir suçun işlenmeden öteki suçun işlenmesinin imkânsız olması ve bu her iki suçun aynı hukuksal yararı korumaya yönelmiş olması koşulları, burada mevcut bulunmamaktadır. Diğer yandan, bilişim sistemine hukuka aykırı olarak girmek (TCK md 243) ile o bilişim sistemindeki kişisel verileri hukuka aykırı olarak ele geçirmek (TCK md. 136) zamansal olarak da birbirinden ayrı ve bağımsız iki fiili ifade eder. Bu nedenle, bir bilişim sistemine girerek, o sistemin içindeki kişisel verileri hukuka aykırı olarak ele geçiren fail, gerçek içtima kuralları uyarınca, hem TCK md 243 hem de TCK md 136'dan dolayı ayrı ayrı cezalandırılacaktır (Dülger, 2020; Kangal, 2019).

YAPTIRIM DÜZENİ VE MUHAKEME USULÜ

Kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu, hapis cezasını gerektiren bir suç olarak benimsenmiştir ve bu suç için bir adlî para cezası öngörülmemiştir.

Buna göre, kişisel verileri hukuka aykırı olarak veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Nitelikli unsurlar yönünden, ilk olarak 7188 sayılı Kanun ile TCK md. 136'ya eklenen 2. fıkraya göre, suçun konusunun CMK md. 236/5.ve 6. fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.

TCK md. 137'de düzenlenmiş olan, suçun kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek veya sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmiş olması halinde ise verilecek ceza yarı oranında artırılır.

Buna karşın, 5809 sayılı Elektronik Haberleşme Kanunu'nun 63/3. maddesi uyarınca, kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme biçimindeki seçimlik hareketlerin, elektronik haberleşme hizmeti vermek üzere yetkilendirilmiş bulunan işletmecilerin personeli tarafından işlenmesi halinde, TCK md. 137'ye göre yapılacak artırım bir kat oranında gerçekleşecektir.

TCK md. 140 uyarınca, kişisel verilerin korunmasına ilişkin diğer suç tiplerinde olduğu gibi, TCK 136'daki suç yönünden de, bu suçun işlenmesi dolayısıyla tüzel kişi yararına bir haksız menfaatin sağlanmış olması durumunda, TCK md. 60 uyarınca tüzel kişilere özgü güvenlik tedbirleri uygulanabilir.

Özel hayata ve hayatın gizli alanına karşı işlenen suçlar her ne kadar kural olarak şikâyete bağlı suçlar şeklinde düzenlenmiş ise de TCK md. 139'daki açık düzenleme ile kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçu bu kuralın istisnaları arasında sayıldığı için, bu suçla ilgili olarak bir şikâyet koşulu aranmaz ve Cumhuriyet Başsavcılığı tarafından resen soruşturma yapılır. Buna karşın, suçun TCK md. 137/1-a kapsamında bir kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak suretiyle işlenmiş olması, bahse konu kamu görevlisi hakkında soruşturma yapılabilmesi için 4483 sayılı Memurlar ve Diğer Kamu Görevlilerinin Yargılanması Hakkında Kanun (Md. 32/1) uyarınca, yetkili merciden soruşturma izni alınması gereklidir.

Suçun soruşturulması şikâyete bağlı olmadığı ve ayrıca bu suça CMK md. 253'de sayılan suçlar arasında yer verilmediği için uzlaştırma hükümlerine tâbi değildir.

TCK md. 136'daki suç için görevli mahkeme, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ve Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 1. maddesi uyarınca, Asliye Ceza Mahkemesidir.

SONUÇ

Kişisel veriler 21. yüzyılın ilk çeyreğinde dünya üzerindeki en önemli ekonomik değer kaynağı haline gelmiş bulunmaktadır. Bilişim ve iletişim teknolojisindeki gelişmeler, kişisel verilerin gerek elde edilmesini, gerek kaydedilerek saklanmasını ve gerekse her şekilde işlenmesini fevkalade kolaylaştırmıştır. Bugün için yapay zekâ ve makine öğrenmesi alanındaki gelişmelerin özellikle büyük veri üzerinde yaşamın her alanında çok boyutlu kullanılmaya elverişli bir veri analizini mümkün kılması, insan zihninin algoritmik sınırlarını aşan yeni ve heyecan verici bir veri evrenine kapı aralamaktadır.

Ancak tüm bu gelişmeler bireyin kişisel verileri bağlamında özel hayatı ve mahremiyeti konusunda çok ciddi tehdit ve tehlikeleri de birlikte getirdiği için tüm dünyada bireylerin kişisel verilerinin korunmasına ilişkin gerekli hukuksal altyapının geliştirilmesi için çalışmalar yapılmaktadır.

Kişisel verilerin ceza normları ile korunması bu kapsamdaki çalışmaların önemli bir parçasıdır ve nitekim Türk hukukunda da, inceleme konumuzu oluşturan kişisel verileri hukuka aykırı olarak verme, yayma veya ele geçirme suçunu da kapsayan ceza normları yürürlüğe konulmuştur. Bununla birlikte, artık günümüzde kişisel verilerin korunması tüm gelişmiş ülkelerde bir veri otoritesinin denetimi çerçevesinde, kendine özgü kuralları ve işleyişi olan özgün bir koruma mekanizmasını gerekli kılan ve bağımsız bir hukuk dalı olmaya evrilen alan olma özelliği taşımaktadır. Türk hukukunda 2016 yılında yürürlüğe giren 6698 sayılı KVKK ve bu Kanun ile oluşturulan veri koruma otoritesi olan Kişisel Verileri Koruma Kurumu ile bu alanda yeni bir aşamaya gelinmiştir. Bu aşama ile artık yapılması gereken, kişisel verilerin korunmasına ilişkin farkındalığın artırılması ve bu anlamda kişisel verileri işleyen gerçek ve tüzel kişilerin KVKK kapsamındaki yükümlülükleri ile uymaları gereken usul ve esasları benimseyerek tüm bu kuralları içselleştirmelerinin sağlanmasıdır.

Bu nedenle KVKK sonrası süreçte, kişisel verilerin korunması için TCK'da düzenlenmiş olan suç tiplerinin ceza hukukunun son çare olma (ultima ratio) özelliği ile uyumunu yitirdiğini ve aksine, kişisel verilere ilişkin ihlallerde refleks olarak ceza silahına başvurmanın, KVKK mekanizmasının benimsenmesi ve içselleştirilmesi sürecine olumsuz bir etkisi olduğu düşüncesindeyiz. Bu nedenle, TCK'da kişisel verilerin korunmasına ilişkin diğer suçlarla birlikte TCK md. 136'da düzenlenen suçun da, idari ceza hukuku alanına kaydırılması gerektiğini sonucuna ulaşmış bulunuyoruz. Bu şekilde, TCK'da kişisel verilere ilişkin öngörülmüş olan ihlal biçimlerinin KVKK kapsamında veri otoritesi tarafından karar verilecek caydırıcı ve etkili birer idari yaptırım ile karşılanmasının, KVKK sistemine de büyük güç kazandıracağını ifade etmek yerinde olacaktır.

KAYNAKLAR

Akdağ, H. (2013). *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması*. Ankara: Adalet Yayınevi.

Aktaş, B. (2017). *İnsan Hakları Avrupa Mahkemesi ve Yargıtay Kararları Açısından Özel Hayatın Gizliliğini İhlal Suçu*. İstanbul: Der Yayınları.

Akyürek, G. (2014). *Özel Hayatın Gizliliğini İhlal Suçu*. Ankara: Seçkin Yayınevi.

Artuk, M. E., Gökcen A., Alşahin M., ve Çakır K. (2017). *Ceza Hukuku Genel Hükümler*. Ankara: Adalet Yayınevi.

Aydın, N. (2013). Tıp Ceza Hukukunda Verileri hukuka Aykırı Olarak Verme ve Ele Geçirme Suçu (TCK md. 136). *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, C: 21 (2).

Bayraktar, K., Kiziroğlu, S. K., Yıldız, A. K., Zafer, H., Retornaz, E. A., Akyürek, G., Evik, A. H., Sınar, H., Altunç, S., İnceoğlu, Aytekin A., Erman, R. B. ve Eroğlu, F. (2018). *Özel Ceza Hukuku*: *Hürriyete, Şerefe, Özel Hayata, Hayatın Gizliliği Alanına Karşı Suçlar*. İstanbul: On İki Levha Yayınevi.

Börekçi, E. B. (2019). *Kişisel Verileri Verme, Yayma veya Ele Geçirme Suçu*. İstanbul: Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

Çekin, M. S. (2019). *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayınevi.

Dönmezer, S. ve Bayraktar, K. (2016). *Basın Hukuku*. İstanbul: Beta Yayınevi.

Dülger, M. V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* (3/2).

Dülger, M. V. (2018). *Bilişim Suçları ve İnternet İletişim Hukuku*, Ankara: Seçkin Yayınevi.

Dülger, M. V. (2020). *Kişisel Verilerin Korunması Hukuku*. İstanbul: Hukuk Akademisi Yayınları.

Gültekin, N. M. (2012). *Kişisel Verilerin Ceza Hukuku yönünden Korunması*. İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

Hafızoğulları, Z. ve Özen, M. (2010). *Ceza Hukuku Özel Hükümler-Kişilere Karşı Suçlar*. Ankara: Us-A Yayınevi.

İtişgen, R. (2015). Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu. *Türkiye Adalet Akademisi Dergisi* (23).

Kama Işık, S. (2020). *Avrupa Veri Koruma Hukukuna Anayasal Bir Bakış*. İstanbul: On İki Levha Yayınevi.

Kangal, Z. T. (2019). *Kişisel Verilerin Ceza ve Kabahatler Hukukunda Korunması*. İstanbul: On İki Levha Yayınevi.

Karagülmez, A. (2013). *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*. Ankara: Seçkin Yayınevi.

Katoğlu, T. (2003). *Ceza Hukukunda Hukuka Aykırılık*. Ankara: Seçkin Yayınevi.

Katoğlu, T. (2012). Ceza Hukukunda Suçun Mağduru Kavramının Sınırları. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 61(2).

Kilkelly, U. (2007). The right to respect for private and family life (A guide to the implemantation of Article 8 of the European Convention on Human Rights). *Human Rights Handbooks* (No: 1).

Kişisel Verileri Koruma Kurumu. (t.y.). Açık Rıza Rehberi. Kişisel Verileri Koruma Kurumu. https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf adresinden 20.05.2020 tarihinde alınmıştır.

Koca, M. ve Üzülmez, İ. (2018). *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayınevi.

Korkmaz, İ. (2019). *Kişisel Verilerin Ceza Hukuku Kapsamında Korunması*. Ankara: Seçkin Yayınevi.

Kosta, V. (2013). *Fundamental Rights In EU Internal Market Legislation, Modern Studies In European Law*. Florence: European University Institute.

Özbek, V. Ö., Doğan K., Bacaksız P. ve Tepe İ. (2017). *Türk Ceza Hukuku Özel Hükümler*. Ankara: Seçkin Yayınevi.

Özbek, V. Ö., Doğan K., Bacaksız P. ve Tepe İ. (2016). *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Yayınevi.

Salihpaşaoğlu, Y. (2013). Özel Hayatın Kapsamı: Avrupa İnsan Hakları Mahkemesi İçtihatları Işığında Bir Değerlendirme. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, C. XVII (3).

Sert, Ş. (2019). *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*. Ankara: Seçkin Yayınevi.

Soyaslan, D. (2012). *Ceza Hukuku Özel Hükümler*. Ankara: Yetkin Yayınevi.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. İstanbul: Beta Yayınevi.

Tanör, B. ve Yüzbaşıoğlu, N. (2012). *1982 Anayasasına Göre Türk Anayasa Hukuku*. İstanbul: Beta Yayınevi.

Taşkın, Ş. C. (2008). *Bilişim Suçları*. Bursa: Beta.

Tezcan, D., Erdem, R. M., Sancakdar, O., ve Önok, R. M. (2014). *İnsan Hakları El Kitabı*. Ankara: Seçkin Yayınevi.

Türk Dil Kurumu Güncel Türkçe Sözlük. (t.y.). https://sozluk.gov.tr/ adresinden 18.05.2020 tarihinde alınmıştır.

Uygun, O. (2015). *Devlet Teorisi*. İstanbul: On İki Levha Yayıncılık.

Yaşar, O., Gökcan, H. T. ve Artuç, M. (2014). *Yorumlu-Uygulamalı Türk Ceza Kanunu (III).* Ankara: Yetkin Yayıncılık.

Yücedağ, N. (2017). Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 75(2).

Zafer, H. (2017). *Özel Hayatın ve Hayatın Gizli Alanının Ceza Hukukuyla Korunması (TCK md. 132-134)*. İstanbul: Beta Yayınevi.