

BÖLÜM 8

BİLİŞİM HUKUKU VE KİŞİSEL VERİLERİN KORUNMASI

ANAHTAR KAVRAMLAR

Bilişim Sistemleri, Kişisel Veri, Bilişim Suç ve Cezaları, Kişisel Verilerin Korunması, Kişisel Veri Suç ve Cezaları



ÖĞRENME HEDEFLERİ

-  1 Kişisel verilerin işlenmesinde veri sorumluları
-  2 Veri sorumlularının yükümlülükleri
-  3 Kişisel verilerin hukuka aykırı şekilde işlenmesi halinde mevzuatın düzenlediği idari yaptırımların öğrenilmesi hedeflenmiştir.
-  4 Bilişim ve bilişim sistemi kavramlarının mevzuatımızda tanımı ile bilişim hukukunun, hukuk dalları arasındaki yeri
-  5 Bilişim hukukunun kapsadığı alan ve faaliyetler, bilişim hukukunun kapsamı.

GİRİŞ

Bir canlı türü olarak insanın binlerce yıldır süren tarihsel gelişimi ve değişiminde

ateşin, yazının, sayma sisteminin, takvimin, tekerleğin ve daha birçok keşfin önemli yeri vardır. Tarımsal üretimin keşfi, avcı-toplayıcılıktan yerleşik hayata geçişe, dolayısıyla insanların toplu olarak bir arada yaşamaya başlamasına yol açmıştır. Yerleşik olarak bir arada yaşamaya başlayan insanlar arasında yeni ilişkiler ve anlaşmazlıklar doğmuş, daha önce var olmayan ve günümüzde insanın insan olmaktan doğan temel haklarına yenileri eklenmiştir. Yine insanlar arasında işbölümü zamanla yaygınlaşmış, bir arada yaşayan insanların oluşturduğu toplumda bireyler ve topluluklar arasındaki ilişkilerin, mülkiyete dayalı üretim ilişkilerinin, iktidar (devlet/ yöneten) ile yönetilen arasındaki ilişkinin ve toplum düzeyinin korunmasına ihtiyaç duyulmuştur. Hukuk düzeni bu ihtiyaçlardan ortaya çıkmış ve insanlığın gelişimine paralel olarak gelişen dinamik bir alan olarak varlığını sürdürmektedir.

İnternet ve bilişim sistemlerinin kamusal ve özel alanda yaygınlaşarak, çok çeşitli biçimdeki kullanım alanı dolayısıyla, bu alanda ortaya çıkacak hukuka aykırılıkların önüne geçecek hukuki düzenlemeler yapılmasına ihtiyaç duyulmuştur. Bu nedenle, bilişim sistemlerinin kendi güvenliğine yönelik olarak ve bilişim sistemlerinin araç olarak kötüye kullanılması yoluyla işlenebilecek suçlara yönelik düzenlemeler yapılmıştır. Bununla birlikte yine bilişim ve ağ sistemleri yoluyla elde edilen, saklanan, iletilen kişisel verilerin de korunmasına yönelik veri sorumlularının uyması gereken kurallar düzenlenmiştir. Diğer yandan elektronik ortamda ticarete ilişkin olarak düzenlemeler yapılmış, yine elektronik ortamda üretilen veya kullanılan fikir ve sanat eserlerine ilişkin olarak düzenlemeler yapılmıştır.



1. BİLİŞİM HUKUKUNUN KAPSAMI

Teknolojideki gelişmelerle bilgi elektronik ortama taşınmıştır. Bununla birlikte iletişim, ekonomik faaliyetler, devletin bireyle olan ilişkilerindeki bürokratik faaliyetler de elektronik ortamda sürdürülmeye başlanmıştır. İnsanlık tarihinde tarım devrimi ve sanayi devriminden sonra mikroelektronik ve iletişim olanaklarının artan gelişme hızıyla ivme kazanan, bilgisayar gücünün evlerimizde gündelik yaşamımıza değin girmeyle, bilişim toplumu olarak adlandırılan yeni bir yaşam ve toplum düzeni ortaya çıkmıştır (KÖKSAL, 2003). Bilişim teriminin birçok tanımı yapılmaktadır. Bilişim, elektronik sistemlerin tamamını içeren bir üst terimdir. Bilişim, kısaca, bilgi ve teknolojinin birlikte kullanılarak üretilen sonuçlar olarak tarif edilebilir. Ya da daha geniş ve farklı olarak; teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve özellikle elektronik aletler aracılığıyla düzenli bir biçimde işlenmeyi öngören bir bilimdir. Bir diğer tabirle, her türlü bilgi ve verinin elektronik bilgi işlem araçlarıyla işlenmesini ve değerlendirme tekniklerini konu alan bilim şeklinde de tanımlanabilmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2019).

Bir başka tanıma göre bilişim; insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimidir (Türk Dil Kurumu , 2023) .

Bu tanımlardan yola çıkarak, bilişimin elektronik makineler aracılığıyla ekonomik ve toplumsal alanda iletişimle ve bilginin işlenmesiyle ilgili bilim dalı olarak kabul edildiği söylenebilir. Bilişimi sağlayan her türlü elektronik araç, bilişim aracı olarak kabul edilir.

Yürürlükteki kanunlarda bilişim kavramına rastlamış değiliz. Buna karşın bilişim sistemi kanunda olmasa da ikincil mevzuat niteliğinde olan yönetmelikte tanımlanmış durumdadır. Bunun anlamı, bilişim sistemine yönelik veya bilişim sisteminin araç olarak kullanılması yoluyla işlenebilecek suçlarda, bilişim sisteminden ne anlaşılması gerektiğini göstermektedir. Bu anlamda bilişim sistemi kavramı mevzuatta tanımlanmış durumdadır. Bu tanıma göre “bilişim sistemi”; bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemdir (Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik, 2011).

Kitabın bu bölümünde bilişim sistemi kavramı dijital ortamı kapsayan tüm unsurları kapsayacak şekilde kullanılacaktır. Bilişim hukuku terimi de esasen bilişimin tüm unsurlarını içeren genel bir kavramdır. Böylece okuyucu için daha anlaşılır bir şekilde konu aktarılmaya çalışılacaktır.

Bilişim hukuku terimi önceleri bilişim suç ve cezalarıyla sınırlı olarak, kamu hukukunun alt dalı olan ceza hukukunun bir dalı olarak görünmekteydi. Sonradan elektronik ticaret, elektronik imza, elektronik haberleşme, elektronik paralar, yapay zekâ gibi konular da bilişim hukukunun alt başlıkları olarak incelenmeye başlanmış ve özel hukuk dalı olarak konumlanmıştır. Artık günümüzde bilgisayar, cep telefonları, internet yayıncılığı, sosyal medya, elektronik ticaret, elektronik haberleşme, elektronik imza, yapay zekâ, elektronik paralar ve bilişim suçları başta olmak üzere, bilişim sistemleri aracılığıyla yürütülen her türlü legal ve illegal faaliyet bilişim hukukunun konusunu oluşturmaktadır (EKİCİ, 2023).

2. KİŞİSEL VERİLER HUKUKU

Veri, bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge; muta (I), data, done olarak tanımlanmaktadır (Türk Dil Kurumu, 2023). Veri sözcüğünün içerdiği en önemli özellik, bir bilgi içeriyor olmasıdır (EKİCİ, 2023). Bilişim hukuku açısından ise veri; bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak tanımlanabilir (DÜLGER, 2023). Bilişim hukuku açısından veri olarak kabul edilecek bilgilerin bilişim sistemleri tarafından bir işleme tabi tutulabilir olması, ondan sonuç çıkarılabilir olması ve saklanabilir olması gerekmektedir (EKİCİ, 2023).

Bilişim hukuku kapsamında son yıllarda “kişisel veri” ve büyük veri” veri hukukunun önemli kısımları olmuştur (EKİCİ, 2023). Büyük veri, geleneksel ya da klasik veri işleme yöntemleri ile değerlendirilemeyecek kadar çok büyük hacimli, oldukça kompleks, hızlı değişebilen ve çok zayıf yapılandırılmış büyük miktardaki veriyi ifade etmektedir (TURAN, 2023, s. 295).

Kişisel Verilerin Korunması

Kişisel veri normlar hiyerarşisine göre en üst norm olan ve ülkemizin de taraf olduğu İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme (Avrupa İnsan Hakları Sözleşmesi)’nin 8. Maddesi ile koruma altına alınmıştır. Bu maddeye göre;

Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörölmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması

için gerekli bir tedbir olması durumunda söz konusu olabilir. “ (İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme, 1950)

Bu düzenleme uyarınca kişisel veriler, özel hayata saygı hakkı kapsamında sayılmaktadır. Bu nedenle de temel insan hakları arasındadır.

Kişisel veriler, 1982 Anayasasının 20’nci maddesinin 3’üncü fıkrası ile “*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 öngörölen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir*” hükmü ile koruma altına alınmıştır. Anayasanın bu düzenlemesi uyarınca 2016 yılında Kişisel Verilerin Korunması Kanunu (KVKK) TBMM’de kabul edilmiş ve Resmî Gazetede yayımlanarak yürürlüğe girmiştir.

Kişisel veri kavramı, bizzat kanun koyucu tarafından 6698 sayılı KVKK’nun 3’üncü maddesinin 1’inci fıkrasının (d) bendinde; *kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi* olarak tanımlanmıştır. (6698 Sayılı Kişisel Verilerin Korunması Kanunu, 2016) Bu tanım uyarınca, bilginin kişisel veri sayılabilmesi için gereken ilk koşul, bir bilginin gerçek kişiye ait olmasıdır. Bu nedenle tüzel kişilere ait bilgiler KVKK anlamında kişisel veri sayılmayacaktır. Kanuni tanımından yola çıkılarak bilginin kişisel veri sayılması için aranan diğer koşul, bilginin; kimliği belirli veya belirlenebilir bir gerçek kişiye ait olmasıdır. İkinci unsur, kimliği belirli veya belirlenebilir olmadıkça, yani anonim hale getirildiğinde, bu bilginin kişisel veri olmadığı anlamını taşımaktadır. Anonim hale getirme yine kanun tarafından tanımlanmıştır. Buna göre, kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette

kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi, kişisel verilerin anonim hale getirilmesidir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

Bir bilginin kişisel veri olabilmesi ve KVKK kapsamında sayılması için gereken ilk koşul olan bilginin bir gerçek kişiye ait olması unsuru, gerçek kişinin hukuki tanımının aktarılmasını da zorunlu kılmaktadır. Kişiler hukuku, Türk Medeni Kanunu'nda düzenlenmiştir (Türk Medeni Kanunu , 2001). Kanun'un 28. Maddesine göre; kişilik, çocuğun sağ olarak tamamıyla doğduğu anda başlar ve ölümle sona erer. Çocuk hak ehliyetini, sağ doğmak koşuluyla, ana rahmine düştüğü andan başlayarak elde eder. Hak ehliyeti kavramı da yine aynı kanunda, haklara ve borçlara sahip olmak olarak tanımlanmıştır. Bu nedenle, çocuğun sağ olarak tamamıyla doğma koşulu gerçekleştiğinde, kişisel verinin çocuğun ana rahmine düştüğü andan itibaren koruma altında olduğu söylenebilir. Böylece bir bilginin kişisel veri olarak KVKK'nun kapsamında olması, çocuğun ana rahmine düştüğü andan itibaren başlayarak, kişiliğin sona erdiği ölümle sona erer.

Kişisel Verilerin Korunması Kanunu ile, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere, kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amaçlanmıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Kişisel verilerin korunmasının mahremiyetten daha geniş bir anlamı ve koruma alanı olduğu söylenmektedir. Buna göre, verilerin korunması ile mahremiyetin, yani özel hayatın gizliliğinin yanında, ifade özgürlüğü, din ve vicdan özgürlüğü, bilginin serbest akımı, birey özgürlüğü, kendi kaderini tayin etme gibi hakların da korunduğu belirtilmektedir (TURAN, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2021). Bu haklar, tıpkı özel hayatın gizliliği hakkı gibi, temel insan hakları arasındadır. Bu nedenle, kişisel ve

rilerin korunması, sadece bireyin özel hayatının gizliliği hakkını değil, bundan daha geniş olarak ifade özgürlüğü başta olmak üzere bazı başka temel hakların korunmasını da sağlar.

Bu açıklamalardan sonra KVKK'nun amaçları kısaca;

- Kişisel verilerin işlenmesinde, kişilerin temel hak ve özgürlüklerini korumak,
- Kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek (disiplin altına almak),
- Kişilerin mahremiyetini korumak (özel hayatın gizliliği),
- Kişisel veri güvenliğini sağlamak olarak sayılabilir (Kişisel Verileri Koruma Kurumu, 2019).

Kanunun kapsamında ise, verileri işlenen gerçek kişiler ile verileri işleyenler bulunmaktadır. Kanunda tüzel kişilere ait verilerin kişisel veri olarak kabul edilmediğine bir kez daha vurgu yapmak gerekir. Verileri işleyenler ise ya gerçek kişilerdir ya da tüzel kişilerdir. Verilerin işlenmesi otomatik olabileceği gibi, veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yolla işleyen tüzel kişiler bulunmaktadır. Veri kayıt sistemi Kanunda, *kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi* olarak tanımlanmıştır. Bu bakımdan, verilerin kurumsal ve kişisel veri olarak sınıflandırıldığına, kanunun kişisel verilerin korunmasına yönelik düzenlemeler içerdiği söylenebilir. Ancak, kurumlar nezdinde bulunan kişisel verilerin de olduğu tüm veriler, kurumlar açısından kurumsal veri olarak nitelendirilmekte olduğundan, kurumsal verilerin de kişisel veriler gibi korunması kurumsal yapılar açısından önem taşımaktadır (TURAN, Karşılaştırmalı Hukukta Kişisel Verilerin Korunması, 2021).

Verilerin kurumsal veri/kişisel veri olarak sınıflandırılmasının yanında, kişisel veriler de kendi içinde kişisel veriler/ özel nitelikli kişisel veriler olarak sınıflandırılabilir. Bu ayrıma göre,

bazı kişisel veriler, diğerlerine göre daha özel niteliktedir ve farklı bir koruma ihtiyacı içindedir. Kanun da kişisel veriler içinde bazı verileri özel nitelikli kişisel veri sayarak, bu verilerin işlenmesini diğerlerine göre başka koşullara tabi tutmuştur. KVKK'nun 6'ncı maddesinin 1'inci fıkrasında kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veri olarak sayılmıştır.

Kanun, kişisel verilerin KVKK ya da başka kanunlarda öngörülen usul ve esaslara uygun olarak işlenebileceğini düzenlemiştir. Bu anlamda kişisel verilerin işlenmesi; "kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem" olarak tanımlanmıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Bu tanımdan yol çıkarak, kişisel verilerin işlenmesinin, bir kişisel veriyi elde etmekle başlayıp bu veri üzerindeki her türlü işlemi kapsadığı söylenebilir. Bu nedenle, kişisel verilerin elde edilmesinde mevzuatın aradığı yükümlülükleri yerine getirmek, veri işleyen sorumluluğunu sona erdirmes. Veri elde edildiği andan itibaren üzerinde gerçekleşen her türlü işlemde de KVKK'nun düzenlediği şartların gerçekleşmesi sağlanmalıdır.

Kişisel verilerin hangi şartlarda işlenebileceği ve kişisel verilerin işlenmesine ilişkin genel ilkeler de yine KVKK tarafından düzenlenmiştir. Buna göre, genel kural olarak kişisel verilerin ilgili kişilerin açık rızası olmadan işlenemeyeceği

düzenlenmiştir. Kanun, açık rızayı *belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza* olarak tanımlamıştır (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Açık rıza, 6698 sayılı Kanun'da hem özel nitelikli kişisel veriler hem de özel nitelikli olmayan kişisel veriler bakımından hukuka uygunluk sebebi olarak öngörülmüştür (<https://www.kvkk.gov.tr/>). Kanunda ayrıca, kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği ve aktarılmayacağı, özel nitelikli kişisel verilerin ilgili kişinin açık rızası olmadan işlenemeyeceği düzenlenmiştir. Açık rıza; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır. Açık rızanın yazılı olarak alınması şart olmayıp elektronik ortamda alınması da mümkündür (<https://www.kvkk.gov.tr/>).

Kişisel verilerin işlenmesinde ilgili kişinin açık rızasının aranmayacağı istisnalar da düzenlenmiştir. Buna göre;

- a) Kanunlarda açıkça öngörülmesi,
- b) Fiili imkânsızlık/rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması zorunluluğu,
- c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- d) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- e) İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
- g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun

meşru menfaatleri için veri işlenmesinin zorunlu olması,

durumlarından her biri için ilgili kişinin açık rızası olmadan kişisel verilerin işlenmesi mümkündür. Bu istisnalar dışında ise, kişisel verilerin işlenmesinde ilgili kişinin açık rızasının alınması zorunludur.

Özel nitelikli kişisel verilerin işlenmesinde açık rıza aranmayacak durumlar ise şunlardır: Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Kanunlarda öngörülen haller dışında, yine bu veriler de açık rıza olmaksızın işlenemez.

Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

Özel nitelikli kişisel verilerin işlenmesiyle ilgili olarak kanun, Kişisel Verileri Koruma Kurulu (Kurul) tarafından belirlenen önlemlerin alınması şartını düzenlemiştir. Kurul'un 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı ile özel nitelikli kişisel verilerin işlenmesinde verileri işleyen veri sorumlusuna ek yükümlülükler getirmiştir. Bu yükümlülükler arasında özel nitelikli kişisel verilerin işlendiği elektronik ortamların;

a) Verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,

b) Kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,

c) Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,

d) Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

e) Verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

f) Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması gerekmektedir.

Kişisel Verileri Koruma Kurumu tarafından tüm kişisel verilere yönelik olarak ayrıca, Kişisel Veri Güvenliği Rehberinde kişisel verilerin korunmasına yönelik alınması gereken idari ve teknik önlemler yer almaktadır (<https://www.kvkk.gov.tr/>).

KVKK'nda kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi veri sorumlusu olarak tanımlanmıştır. Veri sorumlusu, kişisel verilerin işlenme amaç ve araçlarını belirleyen gerçek ya da tüzel kişidir. Bunun dışında Kanun'un öngördüğü veri kayıt sisteminin kurulması ve yönetilmesi sorumluluğu da veri sorumlusuna aittir.

Kişisel veriler; ancak açık ve meşru amaçlar için, işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olarak, işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek şartlarıyla, hukuka ve dürüstlük kuralına uygun olarak, doğru ve gerektiğinde güncel olarak işlenebilir. Bu ilkeler, kişisel verilerin işlenebilmesinde veri sorumlularının uyması gereken ilkelerdir.

Kanun tarafından gerçek kişilere, veri sorumlusuna karşı bazı başvuru hakları tanınmıştır.

Buna göre ilgili kişi kişisel verisinin işlenip işlenmediğini öğrenme, işlenmişse buna ilişkin bilgi talep etme hakkına sahiptir. Bunun dışında ilgili kişi, veri sorumlusuna kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme, yurt içi ve yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri öğrenme, kişisel verileri yanlış veya eksik işlenmiş ise bunların düzeltilmesini isteme haklarına sahiptir.

3. VERİ SORUMLULARININ YÜKÜMLÜLÜKLERİ VE İDARİ YAPTIRIMLAR

Kişisel verilerin korunmasıyla ilgili kanuni düzenleme olan 6098 sayılı Kanun, ilgili kişisel verilerin elde edilmesiyle başlayan verilerin işlenmesi sürecine yönelik kuralları düzenlediği gibi, verilerin muhafazasını, işlenme amacı ortadan kalktığında silinme, yok edilme ya da anonim hale getirilmesini, ilgili kişisel verinin doğru ve güncel bilgiler içermemesi halinde bunların düzeltilmesine yönelik kuralları da koymuştur. Bu anlamda, veri sorumlusuna yönelik olarak öngörülen yükümlülüklerin ihlali halinde bazı idari para cezaları da düzenlemiştir.

Kabahat kavramı, 5326 sayılı 30.03.2005 tarihli Kabahatler Kanunu'nun 2'nci maddesinde; *kanunun, karşılığında idarî yaptırım uygulanmasını öngördüğü haksızlık* şeklinde tanımlanmıştır. Bu tanıma göre KVKK'nda aykırılıklar ve karşılığında idari para cezaları düzenlenmiştir. Bu nedenle, özellikle Türk Ceza Kanunu'nda düzenlenen bilişim suç ve cezalarına ilişkin bilişim suçlarından ayrı olarak, KVKK'na aykırılıklar kabahat şeklinde düzenlenmiştir. KVKK'nun ihlali bu anlamda kabahat fiilini oluştururken, kabahatin cezalandırılması ise idari para cezaları şeklinde düzenlenmiştir.

KVKK'nun 10'uncu maddesine göre veri sorumlusu ya da yetkilendirdiği kişi tarafından, kişisel verileri işlenecek olan ilgili kişiye, kişisel verilerin elde edilmesi sırasında veri sorumlu-

İlgili kişi, KVKK'na uygun olarak kişisel verilerinin işlenmiş olması halinde dahi, işlenmesini gerektiren sebeplerin ortadan kalkması halinde veri sorumlusuna işlenen kişisel verilerinin silinmesi, yok edilmesi ya da anonim hale getirilmesi için başvuruda bulunma hakkına sahiptir. İşlenme sebepleri ortadan kalktığında, verileri işleyen veri sorumlusu da herhangi bir talep beklemeksizin bu verileri silmeli, yok etmeli ya da anonim hale getirmelidir (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016).

sunun ve varsa temsilcisinin kimliği, kişisel verilerin hangi amaçla işleneceği, kimlere hangi amaçla işlenen kişisel verilerin aktarılacağı, kişisel verilerin hangi yolla toplanacağı ve kişisel verilerin işlenmesinin hukuki sebebini ve ilgili kişinin veri sorumlusuna başvurma hakkı olduğu konusunda aydınlatılması gerekmektedir. Söz konusu aydınlatma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında idari para cezası uygulanır.

Her şeyden önce veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini önlemekle yükümlü tutulmuştur (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Kanun, kişisel verilerin işlenmesinde özellikle "hukuka aykırı" terimini tercih etmiştir. Bu kavram yerine doğrudan KVKK'na atıf yaparak "kanuna aykırı" terimini de kullanabilirdi. Bu durumda hukuka aykırılık ile kanuna aykırılık kavramlarının aynı şeyi ifade etmediğini belirtmek isteriz.

Hukuka aykırılık kavramı, kanunla ya da herhangi bir mevzuat düzenlemesiyle sınırlı olmayan, hukukun genel ve evrensel ilkelerini de kapsayan en geniş anlamdadır. Bunun anlamı kanunda öngörülen işleme şartları sağlanmış olsa dahi, işlenmek istenen amacın sınırlarını aşacak şekilde ve ölçüsüz olarak amacı aşan verilerin işlenmemesi gerektiğidir. Örneğin, bir spor salonu müşterilerinin giriş-çıkış kontrolünü biyometrik veri olan parmak izi taranması yoluyla yapılması,

amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan kişisel verilerin işlenmesinden kaçınılmasını gerektirdiği, ölçülülük ilkesi gereği veri işlemenin amacı gerçekleştirecek ölçüde olması gerektiği, amacı aşan ölçüde çok veri elde etmenin, ilgili kişi aydınlatılsa ve açık rızası olsa dahi meşru bir amaca hizmet etmeyeceği sebebiyle hukuka aykırıdır.

Veri sorumlusunun ikinci yükümlülüğü, kişisel verilere hukuka aykırı olarak erişilmesini önlemektir. Bu nedenle veri sorumlusu, hukuka uygun şekilde işlediği kişisel verileri hem kurum içinde hem de dışarıdan gelebilecek olası siber saldırılara karşı korumakla yükümlüdür. Yine veri sorumlusunun bir diğer yükümlülüğü kişisel verilerin muhafazasını sağlamaktır. Veri sorumlusu bu yükümlülüklerini yerine getirmek için her türlü teknik ve idari tedbirleri almak zorundadır.

Veri sorumlusu ile veri sorumlusu tarafından görevlendirilen, veri sorumlu adına veri işleyen gerçek ya da tüzel kişiler, görevlerinden ayrıldıktan sonra dahi işlenen verileri kanun amacı dışında kullanamaz ve başkasına açıklayamazlar. Veri sorumlusu, yukarıda açıklanan verilerin güvenliğine ilişkin tedbirleri almaması halinde idari para cezası ile cezalandırılır.

Kişisel verisinin işlenip işlenmediği, işlendiyse bunun kanuna uygun olup olmadığı, üçüncü kişilere aktarılıp aktarılmadığı, verilerin işlenmesi amacının gerekliliği ortadan kalktıktan sonra silinip silinmediği (veya anonim hale getirilip getirilmediği ya da yok edilip edilmediği) gibi hususlarda ilgili kişi, veri sorumlusuna başvuru hakkına sahiptir. Veri sorumlusu bu talebi en geç otuz gün içinde cevaplandırmakla yükümlüdür. Başvuru konusu bir talep niteliğindeyse, veri sorumlusu tarafından başvurunun reddi, verilen yanıtın yetersiz bulunması veya süresinde cevap verilmemesi hallerinde Kişisel Verileri Koruma Kuruluna şikâyet hakkına sahiptir. Kişisel verilerin hukuka aykırı olarak işlenmesi nedeniyle ilgili kişiler, şikâyet hakkının yanında ayrıca uğ-

radıkları zarara karşılık tazminat talep etme hakları da mevcuttur (6698 Sayılı Kişisel Verilerin Korunması Kanunu , 2016). Şikâyet sonucunda Kurul tarafından ihlal tespit edildiğinde, veri sorumlusu tarafından en geç otuz gün içinde ihlalin ve hukuka aykırılığın giderilmesine karar verilir. Bu süre içinde hukuka aykırılık giderilmediği takdirde, veri sorumlusu idari para cezası ile cezalandırılır.

Kanun tarafından veri sorumlusu hakkında düzenlenen yükümlülöklere uyulmaması halinde düzenlenen idari para cezasının yanında, aydınlatma, veri güvenliği, Kurul tarafından verilen hukuka aykırılık nedeniyle ihlal kararının yerine getirilmemesi eylemlerinin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre disiplin soruşturması açılacağı düzenlenmiştir. Ayrıca bu kamu görevlilerinin, görevi ihmal veya görevi kötüye kullanma suçlarından sorumluluğu doğabilecektir.

Yukarıda açıklandığı üzere, veri hukukunun idari ve birazdan görüleceği üzere cezai yaptırımlar öngörerek Anayasal düzeyde koruma sağladığı kişisel verilerin korunması, pozitif hukuk kurallarıyla veri işleyen gerçek ve tüzel kişiler için uyulması gereken kuralları belirlemiştir. Ancak, kişisel verilerin hukuka aykırı olarak işlenmesi, veri güvenliğinin sağlanması, işlendikleri amaç ortadan kalktıktan sonra silinmesi ya da anonim hale getirilmesi ile verilerin üçüncü kişilere hukuka aykırı olarak aktarılması yükümlülükleri, veri sorumlusunun yetkilendirdiği veri işleyen kişiler için de geçerlidir. Bu anlamda, özellikle bilgi işlem alanında çalışan kişilerin, kişisel verilerin korunmasıyla ilgili yükümlülükleri bilmesi ve gerektiğinde veri sorumlusunun alması gereken önlemler hakkında farkındalık yaratması faydalı olacaktır.

4. BİLİŞİM SUÇLARI

Bilişim suçu kavramının mevzuatta tanımı yapılmamıştır. Buna karşın öğretide üzerinde fikir birliğine varılmayan birçok tanım bulunmaktadır (DÜLGER, 2023). Öğretide bilişim suçlarının dar ve geniş anlamda iki tanımı bulunmaktadır. Bu tanımlara göre, geniş anlamda bilişim suçu, bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her tür suç olarak tanımlanmıştır (DÜLGER, 2023).

Bu tanımın ifade ettiği husus, dar anlamda bilişim suçunun yanında, bir suçun bilişim sistemlerinin araç olarak kullanılarak işlenmesi halinde, bu suçun bilişim suçu olarak kabul edilmiştir. Örneğin Türk Ceza Kanunu'nun (TCK) 157. Maddesinde "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası verilir." şeklinde düzenlenen dolandırıcılık suçunun hareket unsuru yani eylem, hileli davranışlarla bir kimseyi aldatmaktır. Hilenin şekli önemli değildir. Bu yönüyle suçun serbest hareketli bir suç olduğu söylenebilir (Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAŞIZ, 2022). Suçun hareket unsuru olan hileli davranışların şekli önemli olmadığından, bilişim sistemleri yoluyla işlenmesi zorunluluğu yoktur. Ancak TCK'nın 158'inci maddesinin 1'inci fıkrasının (f)

bendinde dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi halinde üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası verileceği düzenlenmiştir (5237 Sayılı Türk Ceza Kanunu, 2004). Görüldüğü gibi dolandırıcılık suçu esasında bilişim suçu olmamakla birlikte, bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi halinde geniş anlamda bilişim suçu sayılabilir.

Türk Ceza Kanunu'nda düzenlenen hırsızlık, dolandırıcılık, kumar oynanması için yer ve imkân sağlama suçları bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi halinde daha fazla ceza verilmesini gerektiren nitelikli hal kapsamındadır. Israrlı takip suçu açısından ise, bilişim sistemlerinin kullanılması yoluyla ısrarlı şekilde tema kurmaya çalışma suçun kanuni unsuru arasında sayılmıştır. Bütün bu suçlarla birlikte, hakaret, tehdit, şantaj gibi birçok suç bilişim araçları kullanılarak işlenebilir. Sayılan tüm bu suçlar, geniş anlamda bilişim suçları arasındadır.

Dar anlamda bilişim suçu ise verilere, bilişim sistemlerine, işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suçlardır. Dar anlamda bilişim suçları Türk Ceza Kanunu'nun "bilişim alanında suçlar" ve "özel hayata ve hayatın gizli alanına karşı suçlar" bölümünde düzenlenmiştir (DÜLGER, 2023).

4.1. Bilişim Sistemine Girme Suçu (TCK m. 243)

Maddenin birinci fıkrasında "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.*" düzenlemesi mevcuttur.

Kanuni düzenleme uyarınca, bilişim sistemine kasten hukuka aykırı olarak girilmesi ya da sisteme hukuka uygun girilmiş olmasına rağmen bu hukuka uygunluk durumu sona erdikten sonra kasten sistemde kalınması suç olarak düzenlenmiştir. Suçun oluşması için hukuka aykırı şekilde

girilen veya hukuka aykırı olarak kalınan bilişim sisteminden verilerin ele geçirilmesi gerekmez. Öğretide bu suç tipinin bu tür eylemlerin önüne geçilmesinde tek başına yeterli olmadığı, bilişim sistemlerine yönelik yetkisiz girişlerin önüne geçilmesi için bilişim sistemlerinin korunmasının yanında, sisteme yetkisiz giriş ve veri ele geçirmeyi sağlayan yazılımların üretilmesi ve yayılmasının suç olarak düzenlenmesi gerektiği savunulmaktadır (DÜLGER, 2023).

Maddenin üçüncü fıkrasında “*Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur*” düzenlemesi mevcuttur. Bu hükme göre, sistemin içerdiği verilerin silinmesi ya da değiştirilmesi kastı olmadığı halde, sırf hukuka aykırı olarak bilişim sistemine girme ya da hukuka aykırı olarak sistemde kalma eylemi nedeniyle verilerin silinmesi ya da değişmesi durumu halinde daha fazla cezaya hükmolunacağı düzenlenmiştir. Öğretide failin bu fıkra nedeniyle sorumlu tutulması için verilerin silinmesi ya da yok edilmesinde en azından taksirle hareket etmiş olması gerektiği ifade edilmektedir.

Maddenin dördüncü fıkrasında ise “*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmek için teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*” hükmü düzenlenmiştir. Buna göre, bilişim sistemine hukuka aykırı olarak girilmemesine rağmen, bilişim sisteminin kendisi ya da birden fazla bilişim sistem arasındaki veri alışverişini teknik araçla hukuka aykırı olarak izlemek suç olarak düzenlenmiştir. Burada esasında bilişim sistemine girme başlığı altında olsa da farklı bir suç olan, İngilizcesi “interface” olan “araya girme” eyleminin suç olarak düzenlendiği ifade edilmektedir (DÜLGER, 2023).

4.1. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)

Maddenin ilk fıkrası “*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*” şeklinde düzenlenerek, bilişim sisteminin çok geniş ve önemli alanlarda kullanıldığı gözetilerek işleyişin kasten engellenmesi ya da bozulması suç olarak düzenlenmiştir. Örneğin, kişiye ait sosyal medya hesabının şifresinin bir başkası tarafından değiştirilmesi halinde burada tanımlanan bilişim sisteminin işleyişinin engellenmesi suçunun oluştuğu söylenebilir. Söz konusu suçun teknik destek sorumlusunun kasten bir virüs saldırısına karşı sistemi savunmasız bırakması halinde ihmali davranışla işlenmesi de mümkündür (DÜLGER, 2023). Ancak aynı durumda, aşağıda görüleceği üzere, hesap sahibinin kendi sosyal medya hesabına şifresi başkası tarafından değiştirildiği için girememesi nedeniyle bilişim sistemindeki verilerin erişilmez kılınması da söz konusu olabilir.

Maddenin ikinci fıkrasında “*Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*” düzenlemesi ile bilişim sistemi içerisindeki verilerin kasten bozulması, yok edilmesi, erişilmez kılınması, sisteme

hukuka aykırı ve yetkisiz şekilde veri yerleştirilmesi eylemlerinin yanında sistemde var olan verilerin başka bir yere nakledilmesi eylemleri suç olarak düzenlenmiştir. Bu suçun da teknik destek sorumlusunun ihmali hareketiyle işlenmesi mümkündür. Bu nedenlerle, kurum ve kuruluşlarda bilişim güvenliğinden sorumlu çalışanların bilişim sistemlerinin siber saldırılara karşı görev tanımları dâhilindeki işlerini kasten yapmayarak bilişim sistemlerinin güvenliğini sağlamamaları halinde söz konusu suçları ihmalen işledikleri ve bu nedenle sorumlu oldukları kabul edilebilir.

Maddenin üçüncü fıkrasında ilk iki fıkroda tanımlanan eylemlerin işlendiği bilişim sistemlerinin banka, kredi kurumu, kamu kurum veya kuruluşuna ait olmasının daha fazla cezaya hükmüleceği “*Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır*” şeklinde düzenlenmiştir.

Maddenin son fıkrasında ise, ilk üç fıkroda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması halinde, failin iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılacağı düzenlenmiştir.

4.2. Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK m. 245)

Kanun koyucu banka ve kredi kartlarıyla işlenebilecek bilişim sistemleri alanındaki suçları ayrı bir madde ile düzenlemiştir. Buna düzenlemeye göre, kanun koyucu, başkasına ait banka veya kredi kartının ele geçirilip, sahibinin rızası olmadan kullanılması yoluyla yarar sağlanması eylemini üç yıldan altı yıla kadar hapis cezası ve beşbin gün adli para cezası ile yaptırıma tabi tutmuştur. Aynı maddenin diğer fıkralarında, baş-

kalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi eylemleri üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile yaptırıma tabi tutulmuş, sahte kartların kullanarak yarar sağlanması eylemi ise dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası yaptırımına tabi tutulmuştur.

4.3. Yasak Cihaz veya Programlar (TCK m. 245/A)

“Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.”

Kanunun bu maddesinde, bir cihazın, yazılımın, programın, şifre ya da her türlü güvenlik kodunun bilişim alanında düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılarak işlenebilen diğer suçların işlenmesi amacıyla yapılması veya oluşturulması durumunda madde- de sayılan eylemleri yaptırıma tabi tutulmuştur.

5. KİŞİSEL VERİLERE İLİŞKİN SUÇLAR

Kişisel Verilerin Korunması Kanununun 17'nci maddesinde kişisel verilere ilişkin suçlar bakımından TCK'nın 135 ila 140'ıncı maddelerinde düzenlenen hükümlerin uygulanacağını düzenlemiştir. Buna göre, kişisel verilerin hukuka aykırı olarak kaydedilmesi, verilerin hukuka aykırı olarak ele geçirilmesi, yayılması, başkasına verilmesi; verilerin saklanması gereken süreden sonra yok edilmemesi suçları mevcuttur. Kişisel veriler, gelişen teknoloji ile yaygın biçimde bilişim sistemleri aracılığıyla işlenmekte olduğundan,

bu alanda düzenlenen suçlar ve cezalar hakkında okuyucuya bilgi verilmesi yararlı görülmüştür. Ancak unutulmamalıdır ki, kişisel veriler yalnızca bilişim sistemleri aracılığı ile işlenmez. Bu durumda artık bilişim hukukunun kapsamı dışına çıkmış olur. Bilişim sistemi aracılığı ile işlenmesinde de kişisel verilerin işlenmesine dair KVKK'ndaki uygunluk unsurları geçerli olacaktır. Aynı zamanda TCK'nın 135-140 maddelerinden failin sorumlu olması için, verinin bilişim sistemleri aracılığı ile işlenmesi şart değildir.

5.1. Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)

“Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sen-

dikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.”

KVKK'nda düzenlenen hukuka uygunluk şartları oluşmadan kişisel verilerin kaydedilmesi hapis cezası ile yaptırıma tabi tutulmuştur. Madde-

nin ikinci fıkrasında sayılan ve KVKK’nda da özel nitelikli kişisel veri olarak sayılan kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal

bağlantılarına ilişkin kişisel verilerin hukuka aykırı olarak işlenmesi halinde birinci fıkradaki ceza miktarının yarı oranında artırılacağı düzenlenmiştir.

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

“Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Suçun konusunun, Ceza Muhakemesi Kanununun 236’ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır.”

Bu maddenin birinci fıkrasında kişisel verilerin hukuka aykırı olarak bir başkasına aktarılması ya da bir başkasının kişisel verileri hukuka aykırı olarak ele geçirmesi suçu düzenlenmiştir. Maddenin ikinci fıkrasında ise, maddede sayılan

eylemlerin cinsel saldırı ve cinsel istismar mağdurlarının ceza soruşturması evresindeki kayda alınan beyan ve görüntüleri hakkında işlenmesi halinde, daha fazla cezaya hükmolunacağı düzenlenmiştir.

TCK’nun 135 ve 136’ncı maddelerinde düzenlenen suçların kamu görevlisi tarafından görevinin verdiği yetki kötüye kullanılmak suretiyle veya belirli bir meslek ve sanatın sağladığı kolaylıktan faydalanmak suretiyle işlenmesi halinde daha fazla cezaya hükmolunacağı ise 137’nci maddede ayrıca düzenlenmiştir.

5.3. Verileri Yok Etmeme (TCK m 138)

“Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.”

Maddenin ilk fıkrası, hukuka uygun olarak işlenen verilerin ya doğrudan kanunun silinme zamanını düzenlemesi ya da işleme amacının ortadan kalkması halinde verilerinin silinmesiyle yükümlü olanların bu yükümlülüklerini yerine getirmemesini suç olarak düzenlemiştir. Buradaki amaç daha önce hukuka uygun olarak ve meşru bir amaçla işlenen kişisel verilerin sonsuza kadar saklanması kişisel verilerin ve özel hayatın gizliliğinin ihlal olasılığının artmasıdır.

KVKK’nun 17’nci maddesinde KVKK’nun 7’nci maddesine aykırı olarak kişisel verileri silmeyen

ya da anonim hale getirmeyenlerin ise TCK’nun 138’inci maddesine göre cezalandırılacağı hükmü düzenlenmiştir.

Öğretide yok etme kavramının, imha kavramı kapsamında, yok etme, silme ve anonim hale getirme unsurlarından oluştuğu ifade edilmektedir (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022). Buna göre, silime veya yok etme yerine, verinin anonim hale getirmesi durumunda suçun oluşmayacağı kabul edilmelidir.

Kanundaki düzenleme uyarınca suçun, ya ilgili kanunlarda verilerin kim tarafından silineceği düzenlenmişse bu kişi ya da KVKK’da düzenlenen veri sorumlusu tarafından işlenebileceği ifade edilmektedir (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022).

Maddenin ikinci fıkrasında ise bir suç soruşturması ya da kovuşturması sırasında Ceza Muhakemesi Kanununa göre mağdur ya da sanıktan elde edilen bazı kişisel verilerin imha edilmeme-

si halinde cezanın daha ağır şekilde uygulanacağı düzenlenmiştir. Örneğin genetik inceleme verilerinin, iletişimin, gizli soruşturmacının elde ettiği suçla ilgili olmayan kişisel verilerin, teknik araçla izleme ses ve görüntü kaydı ile oluşan verilerden suçla ilgili olmayanların imha edilmesi gerekirken bunun yapılmaması halinde madde- nin ikinci fıkrası uygulanacaktır. Bu durumlar- da suçun faili, verilerin imhasıyla ilgili yükümlü

kılınan kamu görevlisi olup, Ceza Muhakemesi Kanununa göre genellikle cumhuriyet savcısı olacaktır (Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA, 2022).

Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verile- ri yok etmeme hariç olmak üzere bu bölümdeki diğer suçların soruşturması ve kovuşturmasının mağdurun şikâyetine bağlıdır.

6. SONUÇ

Bilişim sistemlerinin gelişmesi, bilginin bilişim sistemlerinde işlenmesinin yaygın hale gelmesi sonucunda bilişim hukuku alanı doğmuş ve bu alan gelişmeye devam etmektedir. Bilişim sis- temlerinin güvenliğini sağlamak, içerdiği çok sayıda kişisel verinin yanında kullanıldığı alana göre özel hayatın gizli mahrem kalması gereken bilgilerle beraber, ekonomik alanda örneğin ban- kacılık bilgilerini de içermektedir. İşte bu geniş kapsamlı ve korunmadığı zaman kötüye kullanı- mı çok olumsuz sonuçlar doğurması olası veri- lerin işlendiği bilişim sistemlerinin güvenliğini koruma gerekliliği, mevzuatımızda da bu alanın hem idari yaptırımla hem de adli ceza ile yaptırı- ma tabi tutulmasına sebep olmuştur.

Veri güvenliğinden sorumlu kişilerin yanın- da, bilişim sistemlerine yasal olmayan erişim- lerin de engellenmesi gerekmekte olduğundan, bilişim sistemlerine ilişkin alanlarda faaliyet gösteren bireylerin ve kurumların hangi haller- de sorumlu olacağı giriş seviyesinde anlatılmaya çalışılmıştır. Giriş bölümünde ifade edildiği üze- re internet yayıncılığı, sosyal medya, elektronik ticaret, elektronik haberleşme, elektronik imza, yapay zekâ, elektronik paralarla ilgili faaliyetler de bilişim hukukunun kapsamı içinde kalmakta ancak bu çalışmanın konusunu oluşturmamak- tadır. Bu anlamda ön lisans seviyesinde temel bilgiler içeren bu çalışmanın öğrencilere faydalı olacağını umarım.

BÖLÜM ÖZETİ

Teknolojik gelişmeler sayesinde günümüz dünyasında bilişim araçları ve internet çok yaygın kullanım alanına sahiptir. Bu yapı iletişimden ekonomik faaliyetlere, veri üretme-saklama-yaymadan elektronik resmi belge oluşturmaya kadar, bununla da sınırlı olmayan ve daha birçok alanı etkileyen, değiştiren ve dönüştüren büyük etkilere sahiptir. Bilişimde yaşanan gelişmeler, geniş etki alanında yarattığı faydanın yanında riskler de barındırmaktadır. Bu riskler iki başlık altında incelenebilir. Bunlardan ilki, doğrudan bilişim araçlarının taşıdığı risklerdir. Diğer bir anlatımla bilişim sistemlerine yetkisiz ve kötü niyetli girilmesiyle başlayan ve çeşitlenen risklerdir. Diğer ise, bir takım hukuka aykırı fiillerin, bilişim sistemlerinin araç olarak kullanılması yoluyla işlenmesi sonucunda ortaya çıkması olası risklerdir. Bu durumda ya hukuka aykırı fiilin işlenebilmesinin kolaylaşmış olabileceği ya da failin kimliğini daha kolay gizleyebileceği gibi durumlar bilişim sistemleri ve internet ağının taşıdığı kendine özgü risklerdir. Bilişim hukuku kavramı, önceleri bu gibi suç ve cezaların belirlendiği, ceza hukukuyla ilgili olarak kamu hukuku alanında anılmıştır. Bilişim sistemleri, bilişim araçları ve internetin kullanım alanı hem kamu kurum ve kuruluşlarını hem de gerçek ya da tüzel kişiler arasındaki hukuki iş ve işlemleri geniş anlamda etkilemiştir. Bilişim sistemleri, araçları ve internet yoluyla örneğin bankacılık işlemleri yapılabilen, nüfus kayıtlarına erişilebilen, ıslak imza ile aynı anlama gelen elektronik imzalı belge oluşturulabilen, sağlık verileri işlenirken, kamu kurumlarına idari başvurular yapılabilen, dava açılabilen, kamu kurumları yetki alanı içindeki tüm bilgi ve belgeleri üretip saklayabilmektedir. Ayrıca yapay zekâ, kripto varlıklar gibi unsurlar bilişim hukukunun özel hukuk alanında da anılmasına ve gelişmesine sebep olmuştur. Bilişim hukukunun geniş kapsamı karşısında, kitabın bu bölümünde özellikle bilişim hukukunun bir alt dalı olarak sayılabilecek olan “veri hukuku” konusuna değinilecek, bilişim hukukunun diğer alt dalları hakkında genel bilgiler verilecek, bilişim suç ve cezaları ile kişisel verilere ilişkin suç ve cezalar hakkında açıklamalar yapılacaktır.

GÖZDEN GEÇİRELİM

1. Bilişim sistemlerinin yaygın olarak kullanımının beraberinde getirdiği riskleri düşünelim.
2. Kişisel verilerin hukuk düzeni tarafından hangi yollarla korunduğunu düşünelim.
3. Kişisel verilerin hukuka uygun olarak işlenme koşullarını biliyor musunuz?
4. Ağ ve veri güvenliğinin önemini bilişim suçları kapsamında düşünelim.
5. Kişisel verilerin korunmasında, veri sorumlusunun yükümlülüklerini gözden geçirelim.
6. Bilişim sistemine girme, sistemi engelleme, verileri yok etme ve değiştirmenin suç olduğunu, bu nedenle veri ve ağ güvenliğinin önemini kavrayalım.

Kaynakça

5237 Sayılı Türk Ceza Kanunu. (2004).

6698 Sayılı Kişisel Verilerin Korunması Kanunu . (2016, Nisan 7). *Kabul Tarihi: 24.03.2016*. Resmi Gazete, S.29677.

Bilgi Teknolojileri ve İletişim Kurumu. (2019). *Bilişim Hukuku ve Bilişim Suçu*. Ekim 15, 2023 tarihinde Bilgi Teknolojileri ve İletişim Kurumu Resmi Web Sayfası: <https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu> adresinden alındı.

Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik. (2011, Eylül 20). Sayı: 28060: Resmi Gazete.

DÜLGER, M. V. (2023). *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık.

EKİCİ, Ş. (2023). *Bilişim ve Teknoloji Hukuku*. Ankara: Seçkin.

<https://www.kvkk.gov.tr/>. (tarih yok). Ekim 22, 2023 tarihinde Kişisel Verileri Koruma Kurumu Resmi Web Sitesi: <https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf> adresinden alındı

İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme. (1950, Kasım 4). Roma.

- Kişisel Verileri Koruma Kurumu. (2019). *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*. Ekim 22, 2023 tarihinde Kişisel Verileri Koruma Kurumu Resmi Web Sitesi: <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF> adresinden alındı
- KÖKSAL, A. (2003). *Bilişim Devrimi, Küreselleşme ve Uygarlıklar Çatışması Ortamında Kimliğini Arayan Türkiye*. Ekim 15, 2023 tarihinde Prof. Dr. Aydın KÖKSAL Kişisel Web Sitesi: <https://www.aydinkoksal.gen.tr/shared/dosyalar/yayinlar/yayin-194-2003.pdf> adresinden alındı
- Rıza SAKA, Ramazan ÇAĞLAYAN, Mahmut KOCA. (2022). *Avrupa Birliği Hukuku, İdare Hukuku ve Ceza Hukuku Açısından Kişisel Verilerin İmhası*. Seçkin Yayıncılık .
- TURAN, M. (2021). *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması*. Seçkin .
- TURAN, M. (2023). *Bilişim Hukuku*. Seçkin.
- Türk Dil Kurumu . (2023). *Türk Dil Kurumu Sözlükleri*. Ekim 15, 2023 tarihinde Güncel Türkçe Sözlük: <https://sozluk.gov.tr/> adresinden alındı
- Türk Medeni Kanunu . (2001). Resmi Gazete .
- Veli Özer ÖZBEK, Koray DOĞAN, Pınar BACAKSIZ. (2022). *Türk Ceza Hukuku Özel Hükümler*. Seçkin Yayıncılık.