

ÜNİTE 1

BİLİŞİM
VE
BİLİŞİM HUKUKUNUN
TEMEL KAVRAMLARI

Arş. Gör. Mustafa Can DAĞLI

ANAHTAR KAVRAMLAR

Bilişim
Veri
İnternet
Bulut bilişim

BİLİŞİM VE BİLİŞİM HUKUKUNUN TEMEL KAVRAMLARI

ÖĞRENME HEDEFLERİ

- 1 Bilişim, veri, enformasyon ve bilgi kavramlarını ayırt etmek.
- 2 Bilişim hukukunun kapsamını öğrenmek.
- 3 Bilgisayar donanımının ve programlarının hukuki niteliğini öğrenmek.
- 4 Ağ ve internet hakkında bilgi sahibi olmak.
- 5 Web kavramını öğrenmek.
- 6 Türkiye'de internetin nasıl yönetildiğini öğrenmek.
- 7 Türk hukukuna göre internet ortamında yer alan sùjeleri öğrenmek.
- 8 Bulut bilişim konusunda bilgi sahibi olmak.

GİRİŞ



Bilgi, günümüzde insanlar tarafından belirli teknolojik aygıtlar kullanılarak toplanmakta, işlenmekte ve aktarılmaktadır. Bir diğer deyişle teknolojinin getirdiği olumlu gelişmeler sayesinde bilginin aktarımı gittikçe kolaylaşmakta ve hızlanmaktadır. Bu aktarım bugün çoğunlukla bilişim sistemleri kullanılarak sağlanmaktadır.

Teknolojinin getirdiği bu olumlu sonucun yanında bazı olumsuz sonuçlar da doğmaktadır. Bunların başında hukuki sorunlar yer almaktadır. Zira teknoloji, insanların eylem alanını genişletmekte, geçmişe kıyasla bazı fiillerin gerçekleşmesini daha kolay hale getirmekte ya da geçmişte hiç yapılamayacak işlemleri mümkün kılmaktadır. Buna bağlı olarak kişiler arasında çıkar çatışmaları doğabilmektedir. Böylece bireylerin birbirleriyle ve kamu kuruluşları ile olan ilişkilerini düzenleme ihtiyacı doğabilmektedir. Bu ihtiyaç ise doğrudan hukuk bilimini ilgilendirmektedir.

Bilim ve teknolojinin gelişmesiyle, klasik hukuk kuralları yetersiz kalmaya başlamış, yeni hukuki kavramlar ve kurumlara ihtiyaç duyulmuştur. Böylece bilişim hukuku, söz konusu ihtiyacı gidermek için hukuki incelemeleri bünyesinde barındıran yeni ve bağımsız bir hukuk dalı olarak karşımıza çıkmaktadır.

“Bilişim”, “Veri”, “Enformasyon” ve “Bilgi” Kavramları

Bilişim hukukunun kapsamını belirleyebilmek için öncelikle bilişim kavramının ne anlam ifade ettiğini incelemek gerekir. Bilişim kavramı, Fransızca karşılığı olan “enformatik” kavramı ile aynı anlamı ifade etmektedir. Bilişimle ilgili doktrinde çeşitli tanımlamalara rastlamak mümkündür. Bahsi geçen tanımlardan birisi bilişimi, “bilginin elektronik araçlar kullanılarak otomatik olarak işlenmesi süreci” olarak tanımlamaktadır. Başka bir tanıma göre, bilgi ve bilgisayar bilimine dayanan bilişim kavramı “bilgiyi çalıştırma, öğrenme, bilme ve işleme” şeklinde tanımlanmaktadır.

Bilişim kavramını tanımlayabilmek için “veri”, “enformasyon” ve “bilgi” kavramlarını da açıklamak gerekmektedir. Bu kavramlar günlük hayatta sıklıkla birbirinin yerine kullanılsa da birbirlerinden farklı anlamlar taşımaktadır. “Veriler”, işlenerek enformasyona dönüştürülene kadar hiç veya çok az değeri bulunan ham olgular veya gözlemlerdir. Bir başka ifadeyle “veri”, nesnelerin, olayların ve bunların çevrelerinin özelliklerini temsil eden sembollerdir. Veriler ölçüm, deney, gözlem gibi araştırma yöntemleri vasıtasıyla elde edilmektedir. “Enformasyon” ise yaygın olarak; anlamlı bir hale gelmesi için işlenen veri, belirli bir amaç için işlenen veri, alıcısı tarafından yorumlanan ve anlaşılan veri şeklinde tanımlanmaktadır. Enformasyon özellikle bilgisayarlar vasıtasıyla verilerin analiz edilmesi sonucu elde edilir. Son olarak “bilgi” ise, bireyin algısı, tecrübeleri, sezgileri ve analitik becerileri gibi özgün yeteneklerini, sahip olduğu enformasyon ile birleştirmesidir. Bilgi, enformasyonun talimatlara dönüştürülmesini mümkün kılmaktadır. Bilgi ya ona sahip bir kişiden iletişim yoluyla ya da tecrübeden çıkarılarak elde edilir ve her iki halde de bilginin kazanımı öğrenmedir. Veri kavramından bilgi kavramına doğru gildikçe insan girdileri, anlamlandırılabilirlik artmakta, bilgisayar girdileri ve programlanabilirlik ise azalmaktadır.

Veri kavramına değinmişken, bu kitapta ayrıntılı olarak ele alınan “kişisel veri” kavramına da kısaca değinmek gerekir. Kişisel veri, 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), m. 3/1 d bendinde; “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi” ifade edecek şekilde tanımlanmıştır. Veri kavramının kapsamı çok geniş iken, kişisel veri kavramı yalnızca kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi kapsamına almaktadır.

Veri ile ilişkili bir başka kavram ise “büyük veri” (big data) kavramıdır. Doktrinde “büyük veri”, büyük bir hızla artan, veri çeşitliliğinin fazla olduğu yüksek hacimli veri topluluğu olarak tanımlanmaktadır. Büyük veri, verilerin sınıflandırılarak kişilerin kullanım alışkanlıkları, arz talep dengesi gibi unsurlara ilişkin bilgi verdiği için ticari hayat bakımından önemli görülmektedir. Günümüzde reklamcılık sektöründe büyük verinin sıklıkla kullanıldığı bilinmektedir.

Yukarıda anlatılanlar ışığında “bilişim”; veri, enformasyon veya bilginin özellikle elektronik araçlarla işlenmesi, değerlendirilmesi, saklanması ve aktarılması gibi süreçlerin tamamını inceleyen bilim dalıdır. “Bilişim hukuku” ise bu süreçleri düzenleyen kurallar ve ilkeler bütünüdür. Yukarıda bahsedilenler ışığında bilişim hukuku, veri, enformasyon veya bilginin özellikle elektronik araçlarla işlenmesi, değerlendirilmesi, saklanması ve aktarılması gibi faaliyetlerin tamamını düzenleyen hukuk dalı olarak tanımlanabilir.

Bilişim Hukukunun Kapsamı

Kıta Avrupası hukuk sisteminde ve Türk Hukukunda, hukuk öğreniminin kolaylaştırılması adına hukuk bilimi iki alana ayrılarak incelenmektedir. Bu alanlar kamu hukuku ve özel hukuk alanlarıdır. Kamu hukuku kapsamında, anayasa hukuku, ceza ve ceza muhakemesi hukuku, idare hukuku, milletlerarası hukuk; özel hukuk kapsamında, medeni hukuk, borçlar hukuku, ticaret hukuku, uluslararası özel hukuk, fıkri mülkiyet hukuku gibi hukuk dalları yer almaktadır.

Bilişim ve teknoloji hukuku ise kapsamının genişliği itibarıyla hem kamu hukuku hem özel hukuk dallarıyla ilişki içerisindedir. Zira bilişim hukuku; medeni hukuk, medeni usul hukuku, eşya hukuku, borçlar hukuku, tüketici hukuku, ticaret hukuku, fikri mülkiyet hukuku gibi özel hukuk alanlarıyla ve idare hukuku, ceza hukuku, anayasa hukuku gibi kamu hukuku alanlarıyla doğrudan ilişki içerisindedir. Bu bağlamda bilişim hukuku, geleneksel kamu hukuku, özel hukuku ayırımına uymamaktadır. Bilişim hukukunun disiplinler arası bir hukuk dalı olduğunu belirtmek mümkündür.

Bilişim hukukunun kapsamını, sınırlayıcı bir tanımla belirlemek, hızla gelişen teknoloji ve alanın dinamik yapısı nedeniyle mümkün değildir. Bununla birlikte, bilişim hukuku alanında çalışma yapılan güncel konu başlıklarına değinmek mümkündür. Bilişim hukukunun kapsamında genel olarak, bilişim suçları (ceza hukuku), adli bilişim, elektronik ticaret hukuku, kişisel verilerin korunması hukuku, elektronik haberleşme hukuku, internet hukuku gibi hukuk dalları yer almaktadır. Ayrıca bilişim hukuku kapsamında, siber güvenlik hukuku, yapay zekâ, makine öğrenmesi, robotik, blokzincir, kripto varlıklar, akıllı sözleşmeler, oyun ve e-spor, metaverse, bulut bilişim, NFT, dijital fikri ve sınai haklar, dijital tüketici hukuku, elektronik ticaretin vergilendirilmesi, elektronik imza gibi konular incelenmektedir. Bu alanlar sınırlı bir biçimde sayılmamış olup, teknolojinin gelişmesiyle söz konusu alanların değişmesi ve bunlara yeni alanların eklenmesi mümkündür.

Bilişim Sistemi

5237 sayılı Türk Ceza Kanunu'nun (TCK) 243. maddesinin gerekçesine göre, bilişim sistemi; “verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler” olarak tanımlanmıştır. Yargıtay da birçok kararında bu tanımlı benimsemiştir.

TCK m. 243'ün gerekçesinde belirtilen “manyetik sistemler” ifadesi, bilişim sistemi tanımını sınırlandırdığı için haklı olarak eleştirilmektedir. Aynı maddenin gerekçesindeki, “otomatik işlemlere tabi tutma” ifadesi de bilişim sistemi kavramının kapsamını daraltmaktadır.



EK BİLGİ

Avrupa Konseyi Siber Suç Sözleşmesi Bölüm 1, Madde 1 “Bilgisayar sistemi, bir veya daha fazlasının bir program uyarınca otomatik veri işleme faaliyetinde bulunduğu herhangi bir cihaz veya birbirine bağlı veya ilişkili cihazlar topluluğudur.” şeklindedir.

Bilişim sistemi, verileri bilgisayar veya bilgisayar gibi belirli bir mantık dahilinde çalışan elektronik cihazlarla işleyen, değerlendiren, aktaran, depolayan araçların bütünüdür. Bilgisayarlar bir bilişim sistemidir; ancak, bilişim sistemi bilgisayardan daha geniş bir kavramdır.

Bilgisayar

“Bilgisayar”, içerisinde geçici veya kalıcı olarak kayıtlı bulunan talimatlar dizisine göre veri işleyen, depolayan, hesaplama yapan, verileri görüntüleyen elektronik bir cihazdır. Doktrinde bilgisayara ilişkin birçok tanım yer almaktadır. Bu tanımlar arasında en isabetli olanlardan birine göre, “bilgisayar”, üzerine yüklenen yazılımlar aracılığıyla, verileri depolayan, işleyen, değerlendiren, sonuçlar üreten ve bu sonuçları kullanıcıya sunan, veri iletişimini sağlayan cihazdır.

Bilgisayarın temel çalışma mantığı, belirli yazılımlar vasıtasıyla, girdi olarak adlandırılan verileri belirli bir işleme tabi tutarak çıktı olarak adlandırılan verileri üretmektir. Bir bilgisayarın çalışabilmesi için belirli donanımlara ve yazılımlara ihtiyaç duyulmaktadır.

Bilgisayar birden çok elektronik cihazın bağlantılı halde bulunduğu bir sistemdir. Bilgisayarı oluşturan, maddi varlığı olan her türlü parça bilgisayar donanımı olarak adlandırılmaktadır. Bilgisayarda yapılacak işlemlere ilişkin yönergeler ise yazılım olarak adlandırılmaktadır. Donanımın aksine yazılımların belirli bir maddi varlığı bulunmamaktadır.

Yazılım

En basit haliyle “yazılım”, bilgisayarda yapılacak işlemlerin talimatlar bütünüdür. Doktrinde “yazılım” kavramına ilişkin birden çok tanım yer almaktadır. Katıldığımız daha ayrıntılı bir görüşe göre yazılım, bilgisayardan beklenen bir işlemin yapılması için verileri işleyen ve bunlardan sonuçlar çıkaran, belirli algoritmalar içeren komut dizisidir.

Yazılımlar veya bilgisayar programları temelde “işletim sistemi yazılımları” ve “uygulama yazılımları” olmak üzere ikiye ayrılarak incelenebilir. Doktrinde yazılım terimi, bilgisayar programlarını da kapsayacak şekilde yararlanılan bir üst başlık olarak kullanılmaktadır.

İşletim Sistemi Yazılımı: Bilgisayarın kontrolü işlevini üstlenen, bilgisayarın yönetimini sağlayan, diğer tüm programların ve donanımın çalışmasını sağlayan yazılımlara işletim sistemi denilmektedir. Bilgisayarın düzgün bir biçimde çalışabilmesi için ve bilgisayara diğer yazılımların yüklenebilmesi için işletim sistemi gereklidir. Bugün itibarıyla en yaygın kullanılan işletim sistemi yazılımları *Microsoft Windows, Mac OS X ve Linux* yazılımlarıdır.

Uygulama Yazılımı: Kullanıcının talebi doğrultusunda, belirli görevleri yerine getirmek üzere girdiler üzerinde işlem yaparak çıktılar elde edilmesini sağlayan yazılımlara bilgisayar programı, uygulama programı veya uygulama yazılımı denilmektedir. Uygulama programları işletim sistemi üzerine kurularak çalışır. Cep telefonlarında kullanılan “*application*” veya “*app*” olarak adlandırılan uygulamalar da birer uygulama yazılımıdır. İnternet tarayıcıları (web browser), e- posta uygulamaları, kelime işlemci programları (örneğin, Microsoft Word), veri işleme programları (örneğin, Microsoft Excel), diğer ofis yazılımları ve oyun yazılımları bilgisayar programlarına örnek olarak verilebilir.

Bilgisayarın Temel Bileşenleri

Bilgisayarın temel bileşenleri; anakart, işlemci, RAM, hard disk, güç kaynağı, ekran kartı, klavye, fare gibi donanımlardan ibarettir. Anakart, işlemci, RAM, hard disk, güç kaynağı, ekran kartı gibi donanımlar, bu cihazları muhafaza eden bilgisayar kasası içerisinde yer alırlar. Bir bilgisayar üzerinde bu sayılan donanımlardan daha fazlası bulunabileceği gibi, bilgisayarın işlevlerini yerine getirebilmesi için gerekli olan temel donanımlar bu sayılanlardır. Burada sayılan tüm donanımın yukarıda belirtildiği üzere maddi bir varlığının bulunduğunu hatırlatmak gerekir.

Dış Donanım Birimleri

Kullanıcının bilgisayara veri aktarmasını, komut vermesini sağlayan, bilgisayarda işlenen verilerin sonuçlarının iletimini sağlayan ve anakarta bağlanan donanım birimleri dış donanım birimleri olarak adlandırılmaktadır. Dış donanım birimleri girdi ve çıktı birimleri olmak üzere ikiye ayrılır.

Girdi Birimleri

Dışarıdan bilgisayara veri aktarımını sağlama amacıyla kullanılan donanımlara girdi birimleri denilmektedir. Klavye, fare, tarayıcı, mikrofon gibi cihazlar girdi birimleridir.

Klavye (*keyboard*), üzerinde harf, rakam, simge ve özel fonksiyon tuşlarının bulunduğu, bilgisayara veri girişi yapılmasını sağlayan girdi aracıdır.

Fare (*mouse*), bilgisayar ekranında yer alan imlecin hareketin yönetimini sağlayan ve kullanıcının komutlarını bilgisayara iletmeyi sağlayan cihazdır.

Çıktı Birimleri

Bilgisayarda belirli bir işleme tabi tutulan verilerin sonuçlarını kullanıcıya aktarmaya yarayan donanım birimleri çıktı birimleri olarak adlandırılmaktadır. Çıktı birimlerine örnek olarak; ekran, hoparlör, yazıcı gibi cihazlar verilebilir.

İç Donanım Birimleri

Bilgisayar kasası içerisinde bulunan ve bilgisayarın temel fonksiyonlarını yerine getirmesini sağlayan donanım birimleri iç donanım birimleri olarak adlandırılmaktadır.

“Anakart” (*Mainboard*); işlemci, RAM gibi bütün donanım birimlerinin üzerine monte edildiği devredir. Bazı cihazların bilgisayara bağlanması için gerekli olan kablo girişleri de anakart üzerinde yer almaktadır. Anakartların üzerinde ses ve görüntü kartı gibi kartların monte edilmesi için kullanılan yuvalar da bulunmaktadır. Bilgisayarda kullanılacak RAM, işlemci ve ekran kartı, anakart türüyle uyumlu olmalıdır.

“İşlemci” (*CPU–Central Processing Unit*); Merkezi işlem birimi veya işlemci, bilgisayarda yüklü olan işletim sistemi ve diğer tüm yazılımların çalışmasını sağlayan, bilgisayardaki tüm işlemleri gerçekleştiren cihazdır. İşlemcinin çalışma ilkesinde, veriler 1 veya 0 olarak işlem görerek, insan duyuları ile algılanabilecek şekle dönüştürülmektedir.

“RAM” (*Random Access Memory*); işlemcinin verilere hızlıca erişmesi için, verilerin geçici olarak saklandığı bellektir. Bilgisayarda hard disk temel depolama birimi olarak kullanılırken, RAM’e ihtiyaç duyulma sebebi, hard diskte depolanan verilere ulaşma hızının RAM’e göre daha düşük olmasıdır. RAM düşük kapasitede veri depolamasına rağmen, işlemcinin ihtiyaç duyduğu verileri hızlıca depolar ve verilere hızlı erişim sağlar. RAM, kalıcı bellek işlevi gören hard disk ile işlemci arasındaki ara depolama birimidir. RAM veriyi geçici depoladığı için bilgisayar kapandığında RAM’de yer alan veriler kaybolur.

“Sabit disk sürücüsü” (*HDD–Hard Disk Drive*); verilerin kalıcı olarak depolandığı cihazdır. Bu cihazlara yüksek boyutlarda veri depo edilebilir. Hard diskler manyetik özelliği olan malzemelerden oluşan birden fazla disk içerir. Veriler bu diskler üzerine yazılır. Veriler, hard disk üzerine mıknatıslanma vasıtasıyla kaydedilir ve silinene kadar sabit kalır. Bu sebeple sabit disk sürücüsü olarak adlandırılmaktadır. Hard disklerin içerisinde yer alan diskler belirli hızlarda (devir/dakika) dönerek disklerin üzerindeki okuma/yazma kafası verileri okuma ve yazma işlemini sağlar.

“Katı hâl sürücüsü” (*SSD–Solid State Drive*); tıpkı hard diskler gibi, verilerin kalıcı olarak depolandığı cihazdır. SSD’ler hard disklere göre yeni bir teknolojik cihazdır. HDD, verileri, belirli hızlarda dönen diskler ve mekanik bir kol üzerindeki disk başlarıyla manyetik olarak yazıp okurken SSD hareket eden bir parçası olmayan cihazdır. SSD’ler verileri yarı iletken hücrelere kaydeder. Bu sebeple, SSD’ler HDD ile kıyaslandığında verileri daha hızlı okur ve yazarlar. Ayrıca SSD’ler sarsıntıya ve ısıya karşı daha dayanıklıdır ve daha az enerji tüketirler. Olumlu yönlerine rağmen HDD’ye göre daha maliyetli ve pahalı olduğu için yüksek boyutlarda veri depolamak için hala HDD’ler kullanılmaktadır.

“Güç kaynağı” (*power supply*); bilgisayara bağlanan tüm cihazlar ile şebeke hattına bağlı priz arasındaki elektrik gücünü düzenleyen cihazdır. Bilgisayar parçalarını şebeke hattından kaynaklı ani akım değişikliklerine karşı korur.

“Ekran kartı”; grafiğin işlenerek ekranda görüntülenmesine imkân veren cihaz ekran kartıdır. Ekran kartları kendi bünyelerinde bellek ve işlemci barındırırlar. Grafik tasarımı, üç boyutlu modelleme, oyun çalıştırma gibi işlemler için yüksek performanslı ekran kartlarına ihtiyaç duyulmaktadır.

Bilgisayar Donanımının Hukuki Niteliği

Medeni hukukta hak kavramı; “mutlak haklar” ve “nisbi haklar” olmak üzere ikiye ayrılmaktadır. Mutlak haklar herkese karşı ileri sürülebilen haklardır. Nisbi haklar ise sadece belirli kişilere karşı ileri sürülebilen haklardır.

Mutlak haklar; “eşya üzerindeki mutlak haklar” ve “kişi üzerindeki mutlak haklar” olmak üzere ikiye ayrılmaktadır. “Eşya üzerindeki mutlak haklar”; ayni haklar (maddi varlığı olan eşya üzerindeki mutlak haklar) ve fikri haklar (maddi varlığı olmayan eşya üzerindeki mutlak haklar) olmak üzere ikiye ayrılmaktadır. “Kişi üzerindeki mutlak haklar” ise kişinin kendi üzerindeki mutlak hakkı olan kişilik hakkı ve kişinin başkaları üzerindeki mutlak hakları olan velayet ve vesayet haklarıdır.

“Nisbi haklar”; alacak hakkı, yenilik doğuran haklar ve borç ilişkisi dışındaki hukuki ilişkilerden doğan nispi haklar olmak üzere üçe ayrılmaktadır.

Konumuzu ilgilendiren husus bilgisayar donanımı üzerinde hangi mutlak hakların kurulabileceğidir. Bilgisayar donanımı üzerinde “kişi üzerindeki mutlak haklar”ın kurulamayacağı açıktır. O halde “eşya üzerindeki mutlak haklar” üzerinden değerlendirme yapmak gerekir. Öncelikle eşya kavramının hukuken ne anlama geldiğini inceleyelim.

Hukuki anlamda eşya, “üzerinde bireysel hakimiyet sağlanabilecek, ekonomik bir değer taşıyan, kişi ve hayvanlar dışındaki cismani varlıklardır.” Fikir ve sanat eserleri ve buluşlar ise hukuken eşya olarak nitelendirilmemektedirler. Bunlar doktrinde, gayri maddi eşya olarak değerlendirilmekte ve üzerlerinde fikri hakların kurulabileceği kabul edilmektedir. Ancak fikir ve sanat eserlerinin, bir tablo veya bir heykel gibi maddi varlık bulduğu şeylerin eşya niteliğinde olduğu kabul edilmektedir.

Bilgisayar donanımının maddi varlığı olan her türlü bilgisayar parçasını ifade ettiğinden bilgisayar donanımının bir cismani varlığının bulunduğu ifade edilebilir. Bilgisayar donanımının ekonomik bir değer taşıdığı da açıktır. Son olarak, bilgisayar donanımı üzerinde bireysel hakimiyet sağlamak mümkündür. Bu açıklamalar ışığında, bilgisayar donanımı hukuken eşya olarak nitelendirilebilir.

Tüm bu anlatılanlara dayanarak, bilgisayar donanımı üzerinde eşya üzerindeki mutlak haklardan, ayni hakların kurulabilmesi mümkündür. Örneğin, ayni haklar arasında yer alan, hak sahibine en geniş yetki sağlayan mülkiyet hakkı, bilgisayar donanımı üzerinde de kurulabilecektir.

Bilgisayar Programlarının Hukuki Niteliği

Bilgisayar programlarının cismani varlığı bulunmadığı için hukuken eşya olarak nitelendirilebilmesi mümkün değildir. Bilgisayar programlarının gayri maddi varlıklarına bağlı olarak üzerlerinde aynı hakların değil, yine mutlak haklar arasında yer alan fikri hakların kurulması mümkündür.

“Bilgisayar programı”, 5846 sayılı Fikir ve Sanat Eserleri Kanunu’nda (FSEK) tanımlanmıştır. FSEK m. 1/B.g bendine göre “bilgisayar programı” kavramı; “bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmalarını” ifade eder.

FSEK m. 2/1’in birinci bendinde “Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları” ilim ve edebiyat eserleri arasında sayılmıştır. Böylece, bir önceki paragrafta tanımlanan bilgisayar programları FSEK kapsamında korunacaktır.

FSEK’in 2. maddesinin son fıkrasında “Arayüzüne temel oluşturan düşünce ve ilkeleri de içine almak üzere, bir bilgisayar programının herhangi bir ögesine temel oluşturan düşünce ve ilkeler eser sayılmazlar.” düzenlemesi yer almaktadır. Burada bahsedilen husus, bilgisayar programına temel oluşturan düşünce ve ilkelerin FSEK kapsamında korunmayacağıdır.

FSEK kapsamında koruma ile kast edilen eser sahibinin; Kanunun 14 ile 17. maddeleri arasında yer alan manevi hakları ve kanunun 20 ile 25. maddeleri arasında düzenlenen mali haklarıdır. Eser sahibi eseri meydana getiren kişiyi ifade etmektedir.

Manevi haklar; eseri umuma arz hakkı (FSEK m. 14), adın belirtilmesi hakkı (FSEK m. 15), eserde değişiklik yapılmasını men etme hakkı (FSEK m. 16) olmak üzere üçe ayrılır.

Mali haklar ise; işleme hakkı (FSEK m. 21), çoğaltma hakkı (FSEK m. 22), yayma hakkı (FSEK m. 23), temsil hakkı (FSEK m. 24) ve işaret, ses ve/veya görüntü nakline yarayan araçlarla umuma iletim hakkı (FSEK m. 25) olmak üzere beşe ayrılır.

Bu haklara ilişkin en önemli nokta, mali hakların sınırsız süreli koruma sağlamayıp, belirli bir süre için koruma sağlamasıdır. Zira FSEK m. 26/1’in ilk cümlesi “Eser sahibine tanınan mali haklar zamanla mukayyettir.” şeklinde düzenlenmiştir. Bu düzenlemeden, mali hakların belirli süreler için koruma sağladığı, manevi haklar için ise böyle bir sınırlama olmadığı için bunların herhangi bir süreye bağlı olmadığı anlaşılmaktadır. Mali haklar, eser sahibinin yaşamı boyunca ve ölümünden itibaren 70 yıl süre ile korunur (FSEK m. 27/1).

FSEK kapsamında düzenlenen hakların ihlal edilmesi halinde eser sahibi; hukuk davalarına (tecavüzün ref’i, tecavüzün men’i, maddi ve manevi tazminat davaları) başvurabileceği gibi ceza davalarına da başvurabilir. Hukuk davaları FSEK m. 66 ve m. 70 arasında; ceza davaları FSEK m. 71 ve m. 73 arasında düzenlenmiştir.

HATIRLATMA

Daha önce de belirtildiği üzere fikri haklar mutlak haklardandır. Burada da eser sahibinin manevi ve mali hakları mutlak hak niteliğinde olduğu için bu hakların herkese karşı ileri sürülebileceğinin unutulmaması gerekir.

Ağ

“Ağ”, en yaygın olarak bilgisayarların ve diğer cihazların birbirleriyle veri paylaşımı yapmasını sağlayacak şekilde bağlantı kurması ile oluşur. Bir diğer ifadeyle “ağ”, birden fazla bilgisayarın veya bilişim sisteminin birbiriyle iletişim kurmasını sağlayan alt yapı, yazılımlar ve bağlı bulunan cihazların bütünüdür. Bilgisayarlar ve diğer cihazlar ağa bağlantı kurduğu anda, ağın bir parçası haline gelirler.

Bilgisayarların veya bilişim sistemlerinin, belirli bir bölge ile sınırlı olmak üzere bağlantı kurması halinde yerel alan ağı (*Local Area Network–LAN*), yerel ağlarının birbirleriyle çok daha geniş bir ağ kurmak için bağlantı kurması halinde ise geniş alan ağı (*Wide Area Network–WAN*) oluşmaktadır. LAN ağından daha geniş olup WAN kadar geniş bir ağ olmayan, bir şehir veya birden çok binayı kapsayan geniş bir alandaki ağ ise metropoliten alan ağı (*Metropolitan Area Network–MAN*) olarak adlandırılmaktadır. Bir ağa bağlanan her bilgisayar bu ağın bir parçası haline gelmektedir. İnternet ise dünya çapında çok geniş kullanımı olan bir ağıdır.

İnternet

İnternet; kamusal ve özel haberleşme ağlarının ara bağlantısı ile IP, TCP protokolleri ve ağlar arası iletişimi küresel çapta yürütmek için gerekli DNS ve veri yönlendirme protokolleri gibi diğer protokolleri kullanan küresel veri iletişimi alt yapısıdır.

Yargıtay bir kararında internet ile ilgili; “*internet, birden fazla haberleşme ağının (network) bilgisayarlar aracılığıyla meydana getirdikleri bir iletişim ortamıdır. Bu ağlar arasındaki ilişkiler IP (internet protokolü) kullanılmak suretiyle bilgisayarlar arasında gerçekleşir. ...*” görüşünü belirtmiştir.

Günümüzde, bilişim sistemlerinin iletişim teknolojisinin temelinde internet yer almaktadır. İnternet, sosyal medya platformları, e-devlet uygulamaları, internet bankacılığı uygulamaları gibi bireylerin kişisel kullanımında sıklıkla tercih edilmekle birlikte, internetin bulut bilişim sektöründen elektronik ticaret sektörüne kadar geniş bir yelpazede kullanım alanı bulunmaktadır. Ağların ağı olarak da adlandırılan internet, dünya çapında iletişimi ve veri kaynaklarına erişimi sağlayan küresel ağ sistemidir.

İnternetin Tarihçesi

2021 yılında yapılan bir araştırmada, günümüzde, dünya nüfusunun %65,6'sının internete erişim sağladığı tespit edilmiştir. Bu kadar yüksek bir oranda kullanım ile günümüzün vazgeçilmez teknolojilerinin başında gelen internetin tarihçesine değinmek gerekir.

1969 yılında, ABD'de Savunma Bakanlığına bağlı İleri Savunma Araştırma Projeleri Kurumunun (DARPA) desteklediği, dayanıklı bir haberleşme altyapısı oluşturma amacıyla oluşturulan ARPANET ağı internetin temelini oluşturmaktadır.

ARPANET projesi öncelikli olarak bilgisayarların veri iletişimi kurabilmesi için ortak bir ağ protokolü standardı oluşturmayı hedeflemiştir. TCP (*Transmission Control Protocol*), kimlik doğrulaması yaparak, bilgisayarlar arası iletişimin küçük paketler halinde gönderilip varış adresinde tekrar birleşmesini sağlar. TCP veri bütünlüğünü korur ve iletişimin kayıpsız gerçekleşmesini sağlar. IP (*Internet Protocol*) ise her veri paketinin nasıl gönderileceği ve yönlendirileceğini tanımlar ve veri paketinin doğru adrese erişmesini sağlar. İnternete bağlı her bilgisayara (ve her bir cihaza) eşsiz bir IP numarası tahsis edilir. Bu sayede, IP, TCP veri paketinin izleyeceği yolu belirler. IP veri içeriği ve niteliğini dikkate almadan yalnızca verinin gideceği adresi belirler.

1980'li yılların başlarında, Vinton Cerf ve Robert Kahn tarafından bilgisayarların iletişiminde standartlaşmayı sağlayan TCP/IP protokolünün geliştirilmesiyle, internet küresel bir ağ haline gelmeye başlamış ve ARPANET yerini sivil bir kuruluş olan Ulusal Bilim Vakfının (NSF) desteklediği NSFNET'e bırakmıştır.

1989 yılında Tim Berners Lee tarafından WWW (*World Wide Web–Geniş Dünya Ağı*) geliştirilmiştir. Ardından Lee, HTML dilini ve HTTP protokolünü geliştirmiş, 1990 yılında ise ilk web tarayıcısını geliştirmiştir. 1990'lı yıllarda, internetin özelleştirilmesi ve ticarileştirilmesi ile birlikte, internet hizmet sağlayıcıları ortaya çıkmış, internet yaygın olarak kullanılan küresel bir ağa dönüşmüştür.



EK BİLGİ

Türkiye'de ise ilk internet bağlantısı 1993 yılında ODTÜ Bilgi İşlem Daire Başkanlığına ait yönlendiriciler ve PTT'den temin edilen 64 kbps kapasiteli kiralık hat üzerinden NSFNET ile bağlantı kurularak gerçekleştirilmiştir.

İnternetin Temel Kavramları

IP Adresi

İnternet ağında yer alan cihazların birbirlerini tanımak ve birbirleri ile veri alışverişi yapabilmek için kullandıkları eşsiz numara dizisidir. IP adresine örnek olarak (193.140.216.43) verilebilir. Ağa bağlı bulunan cihazlar *router* adı verilen cihazlar sayesinde birbirlerini bulabilirler.

Genel IP adresleri “dinamik IP adresi” ve “statik IP adresi” olmak üzere ikiye ayrılır. Dinamik IP adresi düzenli ve otomatik olarak değişir. Dinamik IP adresinin kullanılma sebebi internet servis sağlayıcılar için düşük maliyetli olmasıdır. Zira günümüzde kullanılan IPv4 sistemi sınırlı sayıda IP adresi sunmaktadır. Bu sistemde internet servis sağlayıcılar büyük bir IP adresi havuzu oluşturur ve kullanılmayan IP adreslerini yeniden kullanıcılara dağıtırlar. Statik IP adreslerinde IP adresi sabit kalmaktadır. Statik IP adresi genellikle web sitesi veya e-posta sunucuları için tercih edilmektedir.

DNS (Domain Name System)

IP adresleri akılda tutması zor sayısal bir değer içerdiği için IP adresinin yerine geçmek üzere harf dizileri geliştirilmiştir. Bu sistem Alan Adı Sistemi (*Domain Name System*) olarak adlandırılmaktadır. Alan adı, IP numarasını temsil eden addır. Örneğin, web tarayıcısına 193.140.216.43 IP adresini girmek yerine alan adı olan www.hacettepe.edu.tr yazıldığında bu IP adresine erişim sağlanmaktadır.

URL (Uniform Resource Locator)

URL, internet üzerinde yer alan belirli bir kaynağın adresidir. URL bazıları zorunlu, bazıları isteğe bağlı belirli bölümlerden oluşmaktadır.

Bir örnek üzerinden açıklama yapalım.

(<https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf>) bir PDF dosyasının URL'sidir. Burada;

- [https](https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf) (Hyper Text Transfer Protocol Secure) Güvenli Hiper Metin Aktarım Protokolü,
- [www](https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf) alt alan adı (subdomain),
- [mevzuat](https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf) alan adı (domain),
- [gov.tr](https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf) üst seviye alan adı (top level domain),
- [/mevzuatmetin/1.3.5846.pdf](https://www.mevzuat.gov.tr/mevzuatmetin/1.3.5846.pdf) ise dosya veya sayfa adıdır.

Web–World Wide Web (WWW)

Web kavramı sıklıkla internet kavramı ile karıştırılmaktadır. Web, internet üzerinde yer alan, dosya ve diğer kaynaklara ulaşılması imkânını sağlayan bir bilgi ortamıdır.



EK BİLGİ

Dosyalar ve diğer kaynaklar web sunucuları adı verilen HTTP veya HTTPS protokollerini kullanarak taleplere yanıt vermek için sürekli çalışan, gerekli yazılım ve donanımları içeren bilişim sisteminde yer almaktadır. Bunlara erişim sağlamak için bir web tarayıcısı programı kullanılmaktadır. Web tarayıcılarına yukarıda bahsedilen URL sayesinde, adres girilerek ilgili web sitesine, dosyaya veya diğer kaynağa erişmek mümkün hale gelmektedir. Dosyaların web tarayıcılarında görüntülenebilmesi için HTML (Hyper Text Markup Language) dili kullanılmaktadır.

Web teknolojisi yıllar içerisinde değişikliklere uğramıştır. Geçmişten günümüze web teknolojisi dört döneme ayrılarak incelenmektedir.

Web 1.0: Web teknolojisinin ilk dönemi olarak bilinmektedir. Bu dönemde kullanıcılar yalnızca izleyici/okuyucu konumundadır. Bu dönemde kullanıcılar içerik ekleme veya yorum yapma imkânına sahip değildi. Dolayısıyla web ortamında tek yönlü bir bilgi akışı ve sabit içerikler yer almaktaydı. Bu nedenle bu döneme Salt Okunur Web dönemi de denilmektedir.

Web 2.0: Web 2.0 kavramı ilk defa 2004 yılında kullanılmıştır. Bu dönemde kullanıcılar tarafından sosyal medya etkileşiminin sağlanması, blog kullanımı, video paylaşımı, sohbet etme, web uygulamalarının kullanımı, sesli iletişim, e-mail, anlık mesajlaşma, medya paylaşımı gibi her tür çevrimiçi etkileşim mümkün hale gelmiştir. Kullanıcılar izleyici/okuyucu konumundan çıkıp dinamik katılımcı haline gelmiştir. Sosyal medya siteleri bu dönemde geliştirilmiştir.

Web 3.0: Web 3.0, Web 1.0 ve Web 2.0'da olmayan makine okuması özelliğini web dosyalarına eklemiştir. Bu dönem semantik web olarak da adlandırılmaktadır. Semantik, kelime anlamı olarak "anlam bilimi" anlamına gelmektedir. Semantik web ise doktrinde web'e anlam katılması şeklinde açıklanmaktadır. Semantik web'de veriler makineler tarafından anlamlandırılabilir hale gelmektedir. Semantik web, bir ürün veya hizmeti aramak için gerekli insan çabasını azaltacak web uygulamaları için altyapı sağlamaktadır. Örneğin; kullanıcı, bir uçak bileti araması yaptığında gidilecek ülkenin hava durumu, haritaları, otel ve araba rezervasyonları gibi faydalı olabilecek bilgiler kullanıcıya sunulmaktadır. Kişiselleştirilmiş reklamlar da bu dönemde gündeme gelmiştir.

Web 4.0: Web 4.0 henüz geliştirilme sürecinde olan bir düşüncedir. Doktrinde simbiyotik web olarak da isimlendirilmektedir. Simbiyotik web'in temelinde, üst verinin (metadata) Web 3.0 teknolojisi ile organize edildikten sonra, zihin gücü veya düşünceyle kontrol edilen arayüzlerle insan ve makine etkileşimi sağlanmasının mümkün hale gelmesi yatmaktadır.

İnternetin Uluslararası Yönetişi

İnternet, tek bir merkezden yönetilmemektedir. İnternet, farklı ulusal ve uluslararası kurum ve kuruluşlar tarafından iş birliği ile yönetilmekte ve işletilmektedir. Bu kurumlardan önemli bir kısmına kısaca değinmek gerekir.

ICANN (*Internet Corporation for Assigned Names and Numbers*)

İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN) 1998 yılında ABD merkezli, kâr amacı gütmeyen bir kuruluş olarak DNS sisteminin politikalarını belirlemek ve teknik yönetimini üstlenmek üzere kurulmuştur.

Bugün için ICANN; DNS sunucularının (kök sunucuların) yönetimi ile görevli ve yetkilidir. Kök sunucuların iki önemli işlevi bulunmaktadır. Birincisi, insan tarafından okunabilir olan alan adlarını karşılığı olan sayısal IP adreslerine çevirmek; ikincisi ise bilişim sistemlerini ve internette yer alan kaynakları tespit etmek ve yerini saptamaktır. ICANN, IANA'nın internetin adres defteri olan DNS sisteminin işletilmesine ilişkin teknik görevlerini koordine etmekte yardımcı olmaktadır.

IANA (*Internet Assigned Numbers Authority*)

IANA ya da İnternet Tahsisli Sayılar Otoritesinin görev ve yetkileri; DNS kök sunucusunu, .int ve arpa alan adlarını ve uluslararasılaştırılmış alan adı (IDN) uygulamalarının kaynağını yönetmek; IP ve AS numaralarının küresel havuzunu koordine etmek, özellikle bu havuzu Bölgesel İnternet Tescil Kuruluşlarına (Regional Internet Registries–RIR) temin etmek, standart belirleme organlarıyla birlikte IP numaralama sistemlerini yönetmektir.

IANA, ICANN ile koordinasyon içerisinde görev ve yetkilerini yerine getirir. IANA talep edilmesi halinde, küresel politikaları çerçevesinde Bölgesel İnternet Tescil Kuruluşlarına IP ve AS numaraları atamakta ve atanan her numaranın kaydını tutmaktadır.

Bölgesel Tescil Kuruluşları IANA tarafından kendilerine atanan IP ve AS numaralarını belirli bir bölge için tescil eden ve yöneten, kâr amacı gütmeyen organizasyonlardır. Günümüzde farklı bölgelerde faaliyet gösteren beş Bölgesel Tescil Kuruluşu bulunmaktadır.



DİKKAT EDELİM

IP numaraları IANA tarafından önce Bölgesel Tescil Kuruluşlarına (RIR), buradan RIR tarafından Yerel İnternet Tescil Kuruluşlarına (Local Internet Registry – LIR), LIR tarafından internet servis sağlayıcılara ve son olarak internet servis sağlayıcılar tarafından internet kullanıcılarına tahsis edilmektedir.

IETF (*Internet Engineering Task Force*)

IETF, tüzel kişiliği olmayan, ağ tasarımcıları, operatörleri ve araştırmacılarından oluşan internet mühendisliğinin gelişimiyle ve internetin sorunsuz olarak çalışmasıyla ilgilenen uluslararası bir topluluktur. Topluluk çalışmaları herkese açık olarak yayınlanmaktadır. IETF bağlayıcı kurallar oluşturmadan ziyade, teknik standartlar geliştirmektedir.

ISO (International Organization for Standardization)

Uluslararası Standartlar Teşkilatı (ISO) bağımsız, 167 ulusal standartlaşma kurumunun üye olduğu İsviçre merkezli bir sivil toplum kuruluşudur. ISO, üyeleri aracılığıyla dünyanın çeşitli yerlerindeki uzmanları bir araya getirerek uluslararası standartlar geliştirme amacıyla faaliyet göstermektedir. ISO'nun internet alanında yayımladığı standartlara örnek olarak ISO 30131:2018 nesnelerin interneti (Internet of Things–IoT) referans mimarisi standardı gösterilebilir.

W3C (World Wide Web Consortium)

W3C, web standartlarını geliştirmek üzere faaliyet gösteren uluslararası bir topluluktur. WWW ağı, HTML dilinin geliştiricisi olan Tim Berners-Lee tarafından 1994 yılında kurulmuştur. W3C ayrıca, web ile ilgili eğitimler düzenlemekte, yazılımlar geliştirmekte ve web konusunda tartışmalar için açık bir forum olarak faaliyet göstermektedir.

Diğer Kuruluşlar

Yukarıda sayılanlar haricinde, internet ile ilgili çeşitli çalışmaları olan kurumlar bulunmaktadır. Bunlara örnek olarak; IRTF (Internet Research Task Force), IAB (Internet Architecture Board), IGF (Internet Governance Forum), ISOC (Internet Society) gösterilebilir. Tekrar etmek gerekir ki, internetin yönetimi bir uluslararası kuruluşa bağlı değildir. İnternetin gelişimi ve yönetimiyle ilgili yukarıda sayılan kurum ve kuruluşlar iş birliği içerisinde çalışmaktadır. Burada sayılan hiçbir kuruluşun internet üzerinde doğrudan düzenleme yapma yetkisi bulunmamaktadır.

Türkiye’de İnternetin Yönetişi

Türkiye’de internetin yönetimine ilişkin temel düzenleme 5809 sayılı Elektronik Haberleşme Kanunu (EHK)’dur. Bu kanun ile internetin yönetimi ile ilgili görev ve yetkilerin bir kısmı Ulaştırma ve Altyapı Bakanlığına, bir kısmını Bilgi Teknolojileri ve İletişim Kurumuna verilmiştir.

Ulaştırma ve Altyapı Bakanlığı

EHK’nın 5. maddesine göre;

“a) Numaralandırma, internet alan adları, uydu pozisyonu, frekans tahsisi gibi kıt kaynaklara dayalı elektronik haberleşme hizmetlerine ilişkin strateji ve politikaları belirlemek.” ve

“c) Elektronik haberleşme alt yapı, şebeke ve hizmetlerinin; teknik, ekonomik ve sosyal ihtiyaçlara, kamu yararına ve millî güvenlik amaçlarına uygun olarak kurulması, geliştirilmesi ve birbirlerini tamamlayıcı şekilde yürütülmesini sağlamaya yönelik politikaları belirlemek.” Bakanlığın görev ve yetkileri arasında sayılmıştır. Bu maddeye göre Bakanlığın bu sayılanlardan daha fazla görev ve yetkisi olmakla birlikte, konumuz ile ilgili önemli görev ve yetkileri sayılmıştır.

Ayrıca EHK m. 35; “İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir.” hükmünü içermektedir. Bakanlık bu maddedeki yetkisine dayanarak İnternet Alan Adları Yönetmeliği’ni (İAAY) düzenlemiştir. Yönetmeliğin 1. maddesinde düzenlenme amacının, “.tr” uzantılı internet alan adlarının yönetimine ilişkin usul ve esasların düzenlenmesi olduğu belirtilmiştir. “.tr” uzantısı IANA tarafından Bilgi Teknolojileri ve İletişim Kurumuna tahsis edilmiştir.

HATIRLATMA

Yönetmelik ile yalnızca “.tr” uzantısının düzenlenmesinin sebebi, diğer üst seviye alan adlarının (top-level domains) farklı kurum veya kuruluşlarca yönetiliyor olmasıdır.

Bilgi Teknolojileri ve İletişim Kurumu (BTK)

EHK m. 6/1 bendinde;

“g) Elektronik haberleşme ile ilgili olarak Bakanlığın strateji ve politikalarını dikkate alarak, yetkilendirme, tarifeler, erişim, geçiş hakkı, numaralandırma, spektrum yönetimi, telsiz cihaz ve sistemlerine kurma ve kullanma izni verilmesi, spektrumun izlenmesi ve denetimi, piyasa gözetimi ve denetimi de dahil gerekli düzenlemeler ile denetlemeleri yapmak.” ve

“v) Siber güvenlik ve internet alan adları konularında Cumhurbaşkanı, Bakanlık ve/veya Siber Güvenlik Kurulu tarafından verilen görevleri Telekomünikasyon İletişim Başkanlığı veya diğer birimleri marifetiyle yerine getirmek.” BTK’nın görevleri arasında düzenlenmiştir. Telekomünikasyon İletişim Başkanlığı 2016 yılında kapatılmış, görev ve yetkileri BTK’ya aktarılmıştır.

Bu düzenlemelerden anlaşıldığı üzere, elektronik haberleşme ile ilgili yetkilendirme BTK tarafından yapılmaktadır. EHK m. 3/1 ccc bendine yetkilendirme;

“Elektronik haberleşme hizmetlerinin sunulması ve/veya elektronik haberleşme şebekesi sağlanmasını teminen şirketlerin, Kurum nezdinde kayıtlanmasını veya kayıtlanmasıyla birlikte bu şirketlere elektronik haberleşme hizmetlerine özel, belirli hak ve yükümlülükler verilmesini” ifade edecek şekilde tanımlanmıştır. İnternet servis sağlayıcılığı bir elektronik haberleşme hizmetinin sunulması kapsamında yer aldığı için, bu hizmetin sunulabilmesi BTK’nın yetkilendirme işlemine bağlıdır.

Elektronik haberleşme hizmetinin verilmesi ve/veya elektronik haberleşme şebekesi veya alt yapısının kurulup işletilmesi kural olarak BTK tarafından yapılacak yetkilendirme işlemi ile mümkündür (EHK m. 8/1). Ancak EHK m. 8/2’de bu kurala iki istisna getirilmiştir. EHK m. 8/2/a’da “Bir gerçek veya tüzel kişinin, kendi kullanımındaki taşınmazların dâhilinde ve her bir taşınmazın sınırları dışına taşmayan, münhasıran şahsi veya kurumsal ihtiyaçları için kullanılan ve üçüncü şahıslara herhangi bir elektronik haberleşme hizmeti verilmesinde kullanılmayan, sağlanmasında herhangi bir ticari amaç güdülmeyen ve kamu kullanımına açık olarak sunulmayan”, EHK m. 8/2/b’de “Kamu kurum ve kuruluşlarının münhasıran verdikleri hizmetler ile ilgili olarak özel kanunları uyarınca kurdukları” elektronik haberleşme hizmeti ve/veya şebekesi veya altyapısı yetkilendirmeye tabi tutulmamıştır.

İnternet Alan Adları Yönetmeliği (İAAY) m. 14’te BTK’nın görevleri aşağıdaki şekilde sayılmıştır:

“(1) a) TRABİS’i kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde TRABİS’in üçüncü bir tarafça kurulması ve işletilmesini sağlamak,

b) UÇHS’leri ve KK’ları belirlemek ve bunların iletişim bilgilerini İnternet sitesinde yayımlamak,

c) Alan adı tahsis ve yenilemesine ilişkin ücretler ile uyumsuzluk çözüm mekanizmasının işletilmesi ile ilgili işlemlere ilişkin ücretleri belirlemek ve gerektiğinde değişiklik yapmak,

ç) Tahsise açılacak veya kullanımına son verilecek alt alan adlarını belirlemek,

d) Belgeli tahsis edilen alt alanların tahsisinde istenecek belgeleri belirlemek,

e) Bu Yönetmelikte belirtilen veya Kurul tarafından belirlenen hallerle sınırlı olmak kaydıyla KK niteliğinde faaliyet yürütmek,

f) Alan adı ihtilaflarına ilişkin kendisine iletilen mahkeme kararlarını, UÇHS'nin kendisine ilettiği ihtilafla konu olan alan adları ile hakem veya hakem heyeti kararlarını İnternet sitesinde, kişisel verilerin korunması amacıyla gerekli önlemleri de alarak güncel olarak bulundurmak,

g) Kendisine iletilen talep ve şikâyetleri değerlendirmek ve mevzuat çerçevesinde gerekli tedbirleri almak,

ğ) Her yıl Nisan ayı sonuna kadar bir önceki yıla ait faaliyet raporunu hazırlayarak Kurumun internet sitesinden ve gerekli olduğu hallerde diğer uygun araçlarla kamuoyuna duyurmak,

h) ICANN, RIPE NCC, CENTR gibi kuruluşlar nezdinde gerekliliğiyle yürütmek."

Düzenlemede yer alan kısaltmalar aşağıdaki anlamları ifade etmektedir.

TRABİS: .tr Ağ Bilgi Sistemi (TRABİS); “.tr” uzantılı internet alan adı sisteminin ve buna ait merkezi veri tabanının işletilmesine, rehberin oluşturulmasına, güncellenmesine ve rehberlik hizmetinin sunulmasına ve alan adı başvuru işlemlerinin gerçek zamanlı olarak yapılmasına imkân veren, tüm bu faaliyetlerin güvenli ve iş sürekliliğini sağlayacak şekilde gerçekleştirildiği sistemi” ifade etmektedir (İAAY m.3/1/n).

Kayıt Kuruluşu (KK): “Başvuru, yenileme, iptal gibi alan adları ile ilgili işlemlerin yapılmasına aracılık eden taraf” şeklinde tanımlanmaktadır (İAAY m.3/1/ı).

Uyumsuzluk Çözüm Hizmet Sağlayıcı (UÇHS): “Alan adları ile ilgili ihtilafların çözüm sürecini hakemler veya hakem heyetleri vasıtasıyla yürüten tarafları” ifade etmektedir (İAAY m. 3/1/o).

Bu düzenleme kapsamında BTK'nın en önemli ve bilinmesi gereken görevleri TRABİS'i kurmak ve üçüncü bir tarafça işletilmesini sağlamak, UÇHS ve KK'ları belirlemek ve iletişim bilgilerini internet sitesinde yayımlamak, tahsise açılacak veya kullanımına son verilecek alt alan adlarını belirlemek, alan adı ihtilaflarına ilişkin mahkeme kararlarını ve UÇHS'nin ilettiği hakem veya hakem heyeti kararlarını internet sitesinde güncel olarak bulundurmaktır.

TRABİS 14.09.2022 tarihinde faaliyete başlamıştır. TRABİS'in faaliyete başlamasından önce Türkiye'de “.tr” uzantılı alan adlarının yönetimi 1990 yılından bu tarihe kadar Orta Doğu Teknik Üniversitesi (ODTÜ) bünyesinde faaliyet gösteren Nic.tr tarafından yürütülmüştür. 14.09.2022 tarihinden itibaren “.tr” alan adları yönetimi TRABİS'e devredilmiştir.

Son olarak BTK, yukarıda sayılan görev alanıyla ilgili gerekli gördüğü düzenlemeleri yapmaya, ilgili mevzuat uyarınca KK'ları ve UÇHS'leri denetlemeye, KK'lara ve UÇHS'lere faaliyetlerine son vermek dahil gerekli idari yaptırımları uygulamaya yetkilidir (İAAY m. 15).

.tr Uzantılı Alan Adlarının Tahsisi

Alan adları “a.b.tr” veya “a.tr” şeklinde tahsis edilmektedir (İAAY m.5). “a” kısmı alan adını, “b” kısmı ise alt alan adını ifade etmektedir. Burada yer alan “a” kısmının İAAY m. 6 uyarınca;

a) Yalnız harfler (a-z), rakamlar (0-9) ve tire (-) işaretiyle oluşması,

b) En az iki en fazla altmışüç karakter uzunluğunda olması,

c) Tire (-) işareti ile başlamaması ve/veya bitmemesi,

ç) Yalnızca üçüncü ve dördüncü karakterlerin birlikte tire (-) olmaması,

d) Başkasına tahsisli olmaması,

e) Tahsise kapalı adlar listesinde yer almaması” gerekmektedir.

İAAY Ek kısmında alt alan adlarının (“b” kısmının) neler olduğu belirtilmiştir. Buna göre alt alan adları “.com” “.net” “.biz” “.info” “.bbs” “.name” “.org” “.web” “.gen” “.av” “.tv” “.dr” “.k12” “.tel” “.bel” “.gov” “.edu” “.pol” “.tsk” “.kep” olarak belirlenebilir. Alt alan adlarının güncel listesi BTK tarafından kurumun internet sitesinde yayınlanmaktadır. BTK bu alt alan adlarının kullanımına son vermeye, yeni alan adlarını tahsise açmaya yetkilidir (İAAY m.14/1/ç ve İAAY m. 30/1).

Alan adı başvurusu, alan adına sahip olmak isteyen gerçek veya tüzel kişilerce yapılabilir (İAAY m.7/1). Yukarıda İAAY m.6’da sayılan koşulları taşımayan alan adları için yapılan başvurular reddedilir (İAAY m.7/2). Başvuru BTK’nın veya TRABİS’in internet sitesinde yer alan kayıt kuruluşlarından birine yapılır (İAAY m.7/3).

Alan adı tahsis belgeli veya belgesiz olarak yapılır (İAAY m. 8/1).

Belgesiz alan adı tahsisinde “ilk gelen alır” kuralı geçerlidir. Bu kurala göre, “.tr” uzantılı alan adının tahsisi için ilk başvuran kişiye alan adı tahsis edilir. Örneğin; “bilisimhukukuyayinlari.com.tr” alan adı için ilk başvuru yapan kişiye bu alan adı tahsis edilecektir.

İlk gelen kişinin tespitinde esas alınan zaman, alan adı başvurusunun TRABİS’e ulaştığı andır (İAAY m.8/2). Bu düzenleme doktrinde haklı olarak eleştirilmektedir. Başvurular, BTK tarafından yetkilendirilen kayıt kuruluşlarına yapıldığı için ve kayıt kuruluşunun söz konusu başvuruyu kabul etmesi halinde TRABİS’te gerekli işlemleri yapması söz konusu olduğu için kayıt kuruluşunun başvuruyu TRABİS’e geciktirmesi halinde hak kayıplarının yaşanabileceği ileri sürülmektedir. Bu sebeple haklı olarak İAAY m. 8/2 düzenlemesinin 2. cümlesinin “İlk gelenin tespitinde, alan adı başvurusunun başvuru yapılan KK’nın internet sitesi üzerinden tamamlandığı zaman kaydı esas alınır.” şeklinde değiştirilmesi önerilmektedir.

Belgeli alan tahsisinde ise; gerekli bilgi ve/veya belgelerin başvuru sahibi tarafından kayıt kuruluşuna verilmesi ve bu bilgi ve/veya belgelerin TRABİS’e ulaştırılmasını müteakip alan adı tahsisi yapılır (İAAY m.8/3). Belgeli tahsis edilecek alt alan adları İAAY Ek’inde sayılmıştır. Burada sayılan alan adları sadece belirli kişilere tahsis edilmektedir. Örneğin; “.av” alt alan adı, avukatlar, hukuk büroları ve avukatlık ortaklıklarına tahsis edilmektedir. Bu alan adlarının güncel listesi BTK’nın internet sitesinde yayımlanmaktadır. BTK bu alt alan adlarının da kullanımına son vermeye, yeni alan adlarını tahsise açmaya yetkilidir (İAAY m.14/1/ç ve İAAY m. 30/1).

Alan adı tahsisi kayıt kuruluşlarının TRABİS üzerinden başvuru işlemlerini tam ve doğru olarak tamamladıkları ve ücretin ödendiği an yapılır (İAAY m.8/4).

Alan adı tahsisi bir defada en az bir en fazla beş yıl süre için sağlanır (İAAY m. 8/5). İlgili kayıt kuruluşu, alan adının tahsis süresinin bitmesine en az üç kala alan adı sahibini asgari elektronik posta yoluyla bilgilendirir ve alan adı sahibinden yenileme işlemini yapmasını talep eder (İAAY m. 9/1). Yenileme işlemi yapmak isteyen kişi yukarıda anlatılan başvuru usulüne göre yenileme başvurusu yapar ve yenileme ücretini ödeyerek alan adı tahsisi yenilenir (İAAY m.9/2). Yenilenmemesi halinde tahsis süresinin sonuna kadar alan adının kullanımı iki ay süreyle durdurulur. Bu süre içerisinde de yenileme başvurusu yapılmazsa alan adı yeniden tahsis açılır (İAAY m. 9/3). Yenileme sonrası tahsis süresi beş yılı aşamaz (İAAY m.9/4).

Son olarak, İAAY m. 11/1 uyarınca;

a) Alan adı sahibinin verdiği bilgilerin tam ve/veya doğru olmadığı tespit edilmesi,

b) Alan adının tahsise kapalı adlar listesine alınması,

c) Alan adı tahsisinin iptali ile ilgili UÇHS tarafından Kuruma iletilen hakem ya da hakem heyeti kararının bulunması ve kararın uygulanması için Kurum tarafından belirlenen gerekli şartların mevcut olması,

ç) Alan adı tahsisinin iptaline yönelik bir mahkeme kararının bulunması.”

hallerinde alan adı sahibi ve ilgili kayıt kuruluşu bilgilendirilerek alan adı tahsisi iptal edilir. Belgeli tahsis usulünde, başvuru sırasında sunulan bilgi ve/veya belgelerin geçerliliğini yitirdiği tespit edilirse, BTK'nın ilgili alan adı tahsisini iptal etme yetkisi bulunmaktadır (İAAY m. 11/2).

Türk Hukukuna Göre İnternete Ortamında Yer Alan Søjeler

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (İOK) internet ortamında yer alan søjeleri tanımlamıştır. Kanunda ayrıca bahsi geçen søjelerin yükümlölük ve sorumlulukları ile internet ortamında işlenen bazı suçlarla mücadeleye ilişkin esas ve usuller düzenlenmiştir. Kanun kapsamında yer alan søjeler; içerik sağlayıcı, yer sağlayıcı, sosyal ağ sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıdır.

İçerik sağlayıcı, İOK m. 2/1 f bendine göre; *“İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değıştiren ve sağlayan gerçek veya tüzel kişileri”* ifade edecek biçimde tanımlanmıştır. Madde kapsamında yer alan her türlü bilgi veya veri ifadesi metin, fotoğraf, video, ses ve bunların dışındaki her tür veri ve bilgiyi kapsamaktadır. Bir kişinin içerik sağlayıcı olarak değerlendirilebilmesi için bu bilgi veya veriyi internet ortamı üzerinde üretmesi, değıştirmesi ve sağlaması gerekmektedir.

Yer sağlayıcı, İOK m. 2/1 m bendinde *“Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri”* ifade edecek şekilde düzenlenmiştir. Bu tanıma göre, sosyal ağ sağlayıcılar yer sağlayıcı olarak değerlendirilebilecektir. Ancak Kanun'un m. 2/1 s bendinde sosyal ağ sağlayıcının; *“Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşmalarına imkân sağlayan gerçek veya tüzel kişileri”* ifade ettiği belirtilmiştir.

Erişim sağlayıcı, İOK m. 2/1.e bendinde *“Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri”* ifade edecek şekilde tanımlanmıştır. Erişim sağlayıcı kavramı doktrinde ve uygulamada sıklıkla kullanılan internet servis sağlayıcı kavramına tekabül etmektedir. Erişim sağlayıcı, kullanıcılarına internet erişimi sağlamaktadır. Kanunun bu hükmüne göre hem gerçek hem tüzel kişiler erişim sağlayıcı olabilecektir.

Toplu kullanım sağlayıcı İOK m. 2/1 i bendinde *“Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan”* ifade edecek şekilde düzenlenmiştir. Bu tanım çok geniş bir kitleyi toplu kullanım sağlayıcı kavramının içine aldığı için doktrinde eleştirilmektedir.

Son olarak, internet søjeleri ile ilgili basına yansıması ve güncelliğini koruyan bir hususa değinmek gerekir. 2020 yılında İOK'ta yapılan bir değışiklikle belirli sosyal ağ sağlayıcılara Türkiye'de temsilci bulundurma zorunluluğı getirilmiştir. İOK Ek madde 4/1; *“Türkiye'den günlük erişimi bir milyondan fazla olan yurt dışı kaynaklı sosyal ağ sağlayıcı; Kurum, Birlik, adli veya idari makamlarca gönderilecek tebligat, bildirim veya taleplerin gereğinin yerine getirilmesi ve kişiler tarafından bu Kanun kapsamında yapılacak başvuruların cevaplandırılması ve bu Kanun kapsamındaki diğer yükümlölüklerin yerine getirilmesini temin için yetkili en az bir kişiyi Türkiye'de temsilci olarak belirler ve bu kişinin iletişim bilgilerine kolayca görülebilecek ve doğrudan erişilebilecek şekilde internet sitesinde yer verir. Sosyal ağ sağlayıcı bu kişinin kimlik ve iletişim bilgilerini Kuruma bildirmekle yükümlüdür. Temsilcinin gerçek kişi olması hâlinde Türk vatandaşı olması zorunludur.”* düzenlemesini ihtiva etmektedir.



DİKKAT EDELİM

İOK Ek Madde 4/1'de belirtilen yükümlülüğe uymayan sosyal ağ sağlayıcılara aynı maddenin devam eden fıkralarına göre sırasıyla; idari para cezası, reklam yasağı, internet trafiği bant genişliğinin daraltılması yaptırımları uygulanır.

Bulut Bilişim

Bilişim sistemlerinin kullanılmaya başladığı ilk dönemlerde, ticaret şirketleri, dış kaynak kullanarak verileri depolamak, işlemek ve uzaktan kontrol etmek gibi imkânlarla sahip olmadıkları için kendi bilişim sistemlerini kurarak verileri burada muhafaza etmişlerdir. Bilişim sistemi altyapısı ve yazılımlar yüksek miktarlarda peşin yatırım gerektirdiği için bilişim sisteminin satın alınarak kurum içerisine kurulması, işletmelerin maliyetlerini artırmaktadır. Bu sorunun çözümü ise söz konusu bilişim altyapısı ve yazılımları dış kaynak kullanarak farklı bir şirketten temin etmektir.

Günümüzde şirketler bilişim sistemi altyapısını ve yazılımları ya geleneksel dış kaynak kullanımı sözleşmeleriyle ya da bilişim dış kaynak kullanımının daha yeni bir yöntemi olan bulut bilişim sözleşmeleriyle sağlamaktadır. Bulut bilişimin gelişmesiyle, işletmeler geleneksel dış kaynak kullanımı sözleşmeleri yerine ciddi ölçüde bulut bilişim sözleşmelerine yönelmiştir.

Geleneksel dış kaynak kullanımında bilişim sisteminin altyapısının nerede olduğu belirlidir. Buna karşılık, bulut bilişim sistemlerinde bilişim sisteminin altyapısı hizmet sağlayıcıya ait birden fazla dağınık veri merkezinde yer almaktadır. Dolayısıyla, bulut bilişimde genellikle kullanıcının, verilerinin nerede depolandığını öğrenme imkânı bulunmamaktadır.

Bulut bilişim; paylaşılan bir havuzda yer alan yapılandırılabilir bilişim kaynaklarına (ağ bağlantıları, sunucular, depolama, uygulamalar ve hizmetlere) her an her yerde ulaşılabilir, uygun, talep edildiğinde ağ erişimi sağlayan, asgari düzeyde yönetim çabası veya hizmet sağlayıcı etkileşimi gerektirecek biçimde hızlıca tedarik sağlayan bir modeldir.

Bulut Bilişim Hizmet Modelleri

Bulut bilişim hizmeti kapsamında, kullanıcılara verilerin depolanması, verilerin yedeklenmesi, e-posta sunucusu, web sunucusu, felaket kurtarma, yazılım geliştirme ortamı sağlama gibi birçok hizmet sunmaktadır.

Bulut bilişim kapsamında çeşitli hizmetler sunulmaktadır. Bunlardan en yaygın hizmet modelleri olan; “Hizmet Olarak Altyapı” (*Infrastructure as a Service, IaaS*) modelinde işlemci gücü veya depolama gibi bir bilgisayar kaynağı sunulmakta, “Hizmet Olarak Platform” (*Platform as a Service, PaaS*) modelinde yapılması istenen uygulamalar için araçlar sunulmakta, Hizmet Olarak Yazılım (*Software as a Service,*

SaaS) modelinde ise son kullanıcı uygulamasına benzer işlerlikte uygulama hizmeti bilişim hizmeti olarak sunulmaktadır.

Popüler sosyal medya uygulamalarından, *LinkedIn*, *Facebook (Meta)*, *Instagram* gibi uygulamalar SaaS hizmet modeli örneklerindendir. Bir başka SaaS hizmet modeli ise oyun sektöründe sunulan *Nvidia Geforce Now* hizmetidir. *Microsoft Azure*, *Google App Engine* gibi platformlar PaaS hizmet modeline örnek gösterilebilir. *Google Compute Engine*, *Amazon Web Services (AWS) EC2*, *IaaS* hizmet modelinin örneklerindendir.

Bulut Bilişim Dağıtım Modelleri

Bulut bilişim altyapısının, bir gerçek veya tüzel kişinin kullanımına özel olarak sunulması halinde özel bulut (*private cloud*), genel kullanım için erişim sağlanması halinde ise genel bulut (*public cloud*) söz konusu olmaktadır.

Genel bulutta hizmet sağlayıcı, bilişim hizmetini kullanıcıya internet aracılığıyla sunar ve bilişim altyapısının tamamı hizmet sağlayıcının yönetimindedir. Özel bulutta ise bulut altyapısı ya kullanıcının kendi tesisinde ya da hizmet sağlayıcının veri merkezinde yer alır ve tek bir kişi tarafından kullanılır. Özel bulut altyapısında, yalnızca özel bulut ağına bağlı kişiler buluta erişim sağlayabilmektedir.

İki veya daha fazla bulut altyapısına ilişkin özellikleri kapsamında bulunduran dağıtım modeli ise karma bulut (*hybrid cloud*) olarak karşımıza çıkmaktadır.

Bulut Bilişimin Olumlu ve Olumsuz Yönleri

Avrupa Komisyonu'nun 2010 yılında yayına sunduğu rapora göre bulut bilişim sistemlerinin kullanımının benimsenmesi ekonomik açıdan; altyapı bakım ve devir bedellerinin azalmasına, işletme bünyesinde kurulacak bilişim sistemlerinin veya yerel altyapıların kullanılmasının neden olacağı harcamaların azalmasına, hizmetlere ihtiyaç doğrultusunda ulaşılabilmesine, hizmetlerin piyasaya daha hızlı sunulmasına, karbon ayak izinin ve enerji tüketiminin azalmasına imkân sağlayacaktır.

Veri güvenliği konusunda farklı açılardan değerlendirmeler yapılabilir. Bir açıdan bakıldığında, bulut bilişim hizmetlerinde verilerin kaybolma riski düşüktür. Bunun nedeni, bulut bilişim sisteminde çok sayıda işlemcinin yer alması ve yalnızca dönemsel yedekleme yapmak için bile çalışan donanımların yer almasıdır. Ayrıca, bulut bilişim sözleşmesine göre, verilerin kaybolmasından bulut bilişim hizmet sağlayıcı sorumlu tutulabilecektir.

Karşıt bir açıdan bakıldığında ise, bulut bilişimde, yoğunlukla internet erişimine bağlı olması nedeniyle özellikle hassas verilerin üçüncü kişilerin eline geçmesi, kaybolması riski bulunmaktadır.

Bulut bilişimde, verilerin aynı anda birden fazla veri merkezinde kaydedilebilmesi ve hızlı bir şekilde yer değiştirebilmesi de hukuki açıdan sorunlar doğurmaktadır. Zira bulut bilişim veri merkezlerinin farklı ülkelerin sınırları içerisinde yer alması sözleşmeye uygulanacak hukukun (örneğin, Alman Hukuku veya Türk Hukuku) belirlenmesi ve hangi ülke mahkemelerinin yargılamayı yürüteceği (yargı yetkisi) sorununu ortaya çıkarmaktadır. Bulut bilişim hizmeti alan kullanıcı ve bulut bilişim hizmeti sunan hizmet sağlayıcının genellikle farklı ülkelerin tabiiyetinde olması nedeniyle bu sorunlar doğmaktadır. Söz konusu durum ülkelerin veri güvenliğine ilişkin farklı düzenlemelerinin bulunmasında da kendini göstermektedir. Verilerin korunmasına ilişkin farklı ülkelerde farklı yasaların yürürlükte olmasına bağlı olarak hangi veri koruma yasasına uyum sağlanacağını belirsiz olması risk faktörlerindendir.

BÖLÜM ÖZETİ

Bilişim hukuku, genç ve henüz gelişmekte olan bir hukuk dalıdır. Bilişim hukukunun temel kavramlarını daha kolay anlayabilmek için bilişim, veri, enformasyon gibi kavramların ne anlama geldiğinin kavranması gerekmektedir. Çünkü bilişim hukuku bu temel kavramlar ekseninde (ve daha fazlasında) gelişim göstermektedir. Bilişim hukukunun eksiksiz bir tanımını yapmak alanın dinamik yapısı nedeniyle mümkün değildir.

Bilişim sistemi kavramının ne ifade ettiğinin anlaşılması son derece önemlidir. Çünkü bu kavram mahkeme kararlarına konu olmakta ve bilişim hukuku açısından önem arz etmektedir. En yaygın kullanılan bilişim sistemlerinden biri olan bilgisayarlar, donanım ve yazılımlardan oluşmaktadır. Bilgisayar donanım ve yazılımları hukuken farklı niteliktedir. Bunun sonucu olarak ta farklı hukuki sonuçlar doğmaktadır.

Ağlar, bilgisayarların ve diğer cihazların birbirleriyle veri paylaşımı yapmasını sağlayacak şekilde bağlantı kurmasıyla meydana gelir. Dünya çapında iletişimi ve veri kaynaklarına erişimi sağlayan birçok ağın birleşiminden oluşan küresel ağ sistemi ise interneti oluşturmaktadır. İnternetin tarihçesi ve temel kavramları bugün kullandığımız internet teknolojisini değerlendirebilmek için faydalı olacaktır. Çünkü internet hukuku, bilişim hukuku kapsamında önemli bir yere sahiptir. İnternet, farklı ulusal ve uluslararası kurum ve kuruluşlar tarafından iş birliği ile yönetilmekte ve işletilmektedir. Bu kurum ve kuruluşların her biri internetin yönetiminde önemli bir rol üstlenmektedir. Unutulmaması gerekir ki, bu kurumlardan hiçbiri internet yönetiminde tek merkez değildir. Ülkemizde internetin yönetimiyle ilgili temel düzenleme Elektronik Haberleşme Kanunu (EHK)'n yer almaktadır. Bu kanun kapsamında Ulaştırma ve Altyapı Bakanlığı ile Bilgi Teknolojileri ve İletişim Kurumu, internet yönetiminde çeşitli görev ve yetkileri üstlenmektedir. Bu kurumların görev ve yetkileri ilgili kanun maddelerinde yer almakta olup son derece önemli bir yere sahiptir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (İOK) ile internet ortamında yer alan sűjeler tanımlanmış, bu sűjelerin yükümlölük ve sorumlulukları ve internet ortamında işlenen bazı suçlarla mücadeleye ilişkin usul ve esaslar düzenlenmiştir. Konumuz açısından içerik sağlayıcı, yer sağlayıcı, sosyal ağ sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı önemli olanlardır. 2020 yılında İOK'ta yapılan bir değişiklikle Türkiye'de temsilci bulundurma zorunluluđu belirli sosyal ağ sağlayıcılara getirilmiştir.

Bulut bilişim; paylaşılan bir havuzda yer alan yapılandırılabilir bilişim kaynaklarına (ağ bağlantıları, sunucular, depolama, uygulamalar ve hizmetlere) her an ulaşılabilir, talep edildiğinde ağ erişimi sağlayan, asgari düzeyde yönetim çabası veya hizmet sağlayıcı etkileşimi gerektirecek biçimde hızlıca tedarik sağlayan bir modeldir. Bulut bilişim kapsamında farklı hizmet modelleri sunulmaktadır.

GÖZDEN GEÇİRELİM

1., kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
2., verileri bilgisayar veya bilgisayar gibi belirli bir mantık dahilinde çalışan elektronik cihazlarla işleyen, değerlendiren, aktaran, depolayan, araçların bütünüdür.
3. Üzerine yüklenen yazılımlar aracılığıyla, verileri depolayan, işleyen, değerlendiren, sonuçlar üreten ve bu sonuçları kullanıcıya sunan, veri iletişimini sağlayan cihaz'dır.
4. Ağların ağı olarak da adlandırılan, dünya çapında iletişimi ve veri kaynaklarına erişimi sağlayan küresel ağ sistemidir.
5. IP adresinin yerine geçmek üzere geliştirilen harf dizilim sistemine denir.
6., internet üzerinde yer alan belirli bir kaynağın adresini ifade eder.
7. İnternet üzerindeki dosya ve diğer kaynaklara ulaşılması imkanını sağlayan bilgi ortamı şeklinde adlandırılır.
8., paylaşılan bir havuzda yer alan yapılandırılabilir bilişim kaynaklarına her an her yerde ulaşılabilir, uygun, talep edildiğinde ağ erişimi sağlayan, asgari düzeyde yönetim çabası veya hizmet sağlayıcı etkileşimi gerektirecek biçimde hızlıca tedarik sağlayan bir modeldir.
9. Ülkemizde internetin yönetimiyle ilgili temel düzenleme'dur.
10. 5651 sayılı Kanun ile tanımlanan internet ortamında yer alan sùjeler;, yer sağlayıcı, sosyal ağ sağlayıcı, ve toplu kullanım sağlayıcıdır.

CEVAP ANAHTARI

1. Kişisel Veri	6. Uniform Resource Locator – URL
2. Bilişim Sistemi	7. Web – World Wide Web – WWW
3. bilgisayar	8. Bulut Bilişim
4. internet	9. 5809 sayılı Elektronik Haberleşme Kanunu
5. Domain Name System – DNS	10. içerik sağlayıcı – erişim sağlayıcı

SÖZLÜK

AS Numarası: Bir ya da daha çok ağ operatörü tarafından tek bir kuruluş adına işletilen, birbiri ile bağlı IP routing bütünü.

Bulut bilişim: Özgün işlevleri bulunan sunucuların küresel bir ağ oluşturduğunu ve tek bir ekosistem olarak çalıştığını betimlemek üzere kullanılan bir metafor.

Elektronik haberleşme: Elektriksel işaretlere dönüştürülebilen her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasıdır (EHK m. 3/1/h).

İnternet servis sağlayıcı: Gerçek ve tüzel kişilere internet bağlantısı ve/veya internet hizmetleri sunan şirket.

Metadata: Üst veri. Veriyi tanımlayan veri veya bilgi.

Misli eşya: Kural olarak sayma, tartma gibi ölçüm yöntemleriyle belirli hale gelen eşyadır. Bu malların yerini aynı cinsten başka bir mal alabilir.

Misli: Miktar, eş, benzer, örnek.

TCP/IP Protokolü: Ağa bağlı olan bilgisayar ve diğer cihazların iletişimi sağlamak için standart haline gelmiş kurallar dizisi.

Tüzel kişi: Gerçek kişi olmadığı halde hukuk düzeni tarafından kendisine kişilik hakkı tanınan ve belirli bir amaç için oluşturulan hukuki varlıklardır. Örneğin; devlet, dernekler, vakıflar, ticaret şirketleri.

Yönetişim: Bir ülkenin ilişkilerini yönetmek için gerekli politik, ekonomik ve idari yetkilerin icrasıdır. Resmî ve özel kuruluşlarda idari, ekonomik, politik otoritenin ortak kullanımını ifade eder.

KAYNAKÇA

- Ackoff*, Russell L.: “From Data to Wisdom”, Journal of Applied Systems Analysis, C. 16, 1989, s. 3-9.
- Bocij*, Paul/Greasley, Andrew/ Hickie, Simon: Business Information Systems Technology, B. 5, Harlow Pearson, UK 2015.
- Çiftçi*, Serdar: Yazılım ve Donanım, Bilgisayar Okuryazarlığı I-II, (Ed.: Benzer, Ahmet/ Aksaya, Harun), Pegem Akademi, Ankara 2012.
- Dural*, Mustafa/Sarı, Suat: Türk Özel Hukuku B. 9, C. I, Filiz Kitabevi, İstanbul 2014.
- Dülger*, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, 8. Bası, Seçkin Yayıncılık, Ankara 2020.
- Ekici*, Şerafettin: Bilişim ve Teknoloji Hukuku, Seçkin Yayıncılık, Ankara 2022.
- Glowniak*, Jerry: “History, Structure, and Function of the Internet”, Seminars in Nuclear Medicine, C. 28, S. 2, 1998, s. 135-144.
- Kaya*, Mehmet Bedii: İnternet Hukuku, 2. Bası, On İki Levha Yayıncılık, İstanbul 2021.
- Ketizmen*, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara 2008.
- Leiner*, Barry M./Cerf, Vinton G./Clark, David D./Kahn, Robert E./Kleinrock, Leonard/Lynch, Daniel C./Postel, Jon/Roberts, Larry G./Wolff, Stephen: “A Brief History of the Internet”, ACM SIG-COMM Computer Communication Review, C. 39, S. 5, 2009.
- Mueller*, Milton/Mathiason, John/Klein, Hans: “The Internet and Global Governance: Principles and Norms for a New Regime”, Global Governance, C. 13, S. 2, 2007, s. 237-254, s. 244.
- Oğuzman*, M. Kemal/Seliçi, Özer/Oktay-Özdemir, Saibe: Eşya Hukuku, 21. Bası, Filiz Kitabevi, İstanbul 2018.
- Özgür*, Ahmet Selçuk: Yazılım ve Donanım ile İlgili Temel Kavramlar, Bilişim Teknolojileri, (Ed.: TE-CİM, Vahap), Nobel Akademik Yayıncılık, Ankara 2019.
- Schubert*, Lutz/Jeffery, Keith/Neidecker-Lutz, Burkhard: The Future of Cloud Computing, EC Information Society and Media, 2010.
- Sokol*, Annie W./Hogan, Michael D.: “NIST Cloud Computing Standards Roadmap”, NIST, Special Publication 500-291, 2013.
- Solanki*, Manishkumar R./Dongaonkar, Abhijit: “A Journey of Human Comfort: Web 1.0 to Web 4.0”, International Journal of Research and Scientific Innovation, C. 3, S. 9, 2016, s. 75-78.
- Topaloğlu*, Mustafa: Bilişim Hukuku, Karahan Kitabevi, Adana 2005.
- Tunç*, Aybike: Bulut Bilişim Sözleşmeleri, On İki Levha Yayıncılık, İstanbul 2020.
- Turan*, Metin: Bilişim Hukuku, 5. Bası, Seçkin Yayıncılık, Ankara 2021.
- Yılmaz*, Süleyman/Çavuşoğlu, Gökçe Filiz: Kişisel Verileri Koruma Hukuku, Yetkin Yayıncılık, Ankara 2020.

ÜNİTE 2

BİLİŞİM HUKUKUNDAKİ
GÜNCEL GELİŞMELER VE ETKİLERİ

Doç. Dr. Mete TEVETOĞLU
Arş. Gör. Batuhan DEMİRTAŞ

ANAHTAR KAVRAMLAR

İçerik sağlayıcı

Yer sağlayıcı / erişim sağlayıcı

Blokszincir teknolojisi ve kripto varlıklar

Metaverse

BİLİŞİM HUKUKUNDAKİ GÜNCEL GELİŞMELER VE ETKİLERİ

ÖĞRENME HEDEFLERİ

- 

1 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un öngördüğü usul ve esasları öğrenmek.
- 

2 İçerik, yer, erişim ve sosyal ağ sağlayıcıları ve bunların sorumluluklarını öğrenmek.
- 

3 İnternet ortamında yapılan yayınlara erişimin engellenmesini veya içeriğin kaldırılmasını gerektirebilecek halleri öğrenmek.
- 

4 Blokszincir teknolojisi, kripto varlıklar ve metaverse gibi yeni teknolojilerin bilişim hukukunu nasıl etkilediğini öğrenmek.

GİRİŞ



İnternetin ve diğer bilgi teknolojilerinin gelişmesi ile birlikte anlık, hızlı ve çoğu zaman ücretsiz bir biçimde insanlar arasında etkileşim mümkün hale gelmiştir. İnsanlığın hem yerel hem de ulusal düzeyde daha önce hiç olmadığı kadar kolay ve hızlı bir biçimde birbiri ile etkileşime giriyor olması beraberinde kendine has sorunlar getirmiştir. Reklamcılık faaliyetlerinden politika, edebiyattan eğlence sektörüne hemen hemen her alan kaçınılmaz olarak internet ve teknoloji ekseninde değişmiş ve dönüşmüştür. Birçok sosyal medya platformu reklamcılık faaliyetlerinin odak noktası haline gelmiş, siyasi partiler propagandalarını internet ortamında gerçekleştirmeye başlamıştır. İnsanların haber alma yöntemleri değişmiş, basılı medyanın yerini dijital medya almıştır. Sinema, dizi ve sanat gibi sektörler dönüşmüş; sinema salonlarının yerini dijital yayınlar almış, bankaların fiziki şubelerinin yerini ise internet bankacılığı gibi farklı ve yeni uygulamalar almıştır. Blokzincir teknolojisi ile birlikte hayatımıza kripto varlıklar girmiştir. Bunlara ek olarak teknolojiye gelişim *Metaverse* gibi konularda birçok yeni sosyal, ekonomik ve hukuki problemi gündeme getirmiştir.

Bu değişim ve dönüşüme ek olarak internet alt yapısının giderek yaygınlaşması ve insanların internet ortamında artık sadece bir tüketici olmaktan ziyade üretici haline gelmesi hem özel hukuk hem de kamu hukukunu değiştirmiştir. İnsanların anlık paylaşımlar yaparak dünyanın öbür ucundaki insanlara ulaşabilmesi bilgi çağının en çarpıcı etkilerinden olsa da bu paylaşımların bir başkasının haklarını zedelemesi veya söz konusu paylaşımların suç teşkil etmesi de bir o kadar mümkün ve kolay hale gelmiştir.

Blokzincir teknolojisi ve kripto varlıklar ile birlikte ödeme yöntemlerinde ve birçok noktada yeni hukuki sorular gündeme gelmiştir. İnsanların *Metaverse*’lerde yaşantısının hukuki boyutu ise tartışma yaratan bir diğer husustur.

İnternet Ortamında Yapılan Yayınlar Ve İnternetin Søjeleri

İnternet Ortamında Yapılan Yayınlar

Konu internet ortamında yapılan yayınlar olduğunda akla ilk gelen düzenleme 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'dur. Söz konusu Kanun internet ortamında yapılan yayınları, yayınları gerçekleştirenler çerçevesinde sistematik olarak ele almış ve düzenlemiştir.

İnternet ortamında yayın yapan internet sjojelerinden önce kanunun kapsamını belirlemek adına internet ortamında yapılan yayın ile kanun koyucunun ne kastettiğini belirlemek gerekmektedir. Kanuna göre internet ortamında yapılan yayın, internet ortamında yer alan ve içeriğine belirsiz sayıda kişilerin ulaşabileceği verileri ifade etmektedir. Kanundaki tanımdan yola çıkılarak internet ortamında yapılan yayının iki ana unsuru olduğu sonucuna varılabilmektedir. Birinci unsur, yayının internet ortamında yer alması iken, ikinci unsur söz konusu yayınlara belirsiz sayıda kişinin erişim sağlayabilecek olmasıdır. Birinci unsuru detaylıca açıklamaya gereksinim yoktur; eğer bir yayına internet vasıtası ile erişim sağlanabiliyorsa bu unsurun sağlandığı söylenebilecektir. İkinci unsur ise belirsiz sayıda kişinin söz konusu yayına erişim sağlayabilmesidir. Burada önemli olan söz konusu yayının yayıncı dışında üçüncü kişiler tarafından erişilebilir olmasıdır.



DİKKAT EDELİM

Eğer bir içeriğe sadece yayıncısı erişim sağlayabiliyorsa, burada 5651 sayılı Kanun kapsamında bir yayından bahsedilmesi mümkün olmayacaktır. Önemli olan söz konusu yayına üçüncü kişilerin de erişim sağlayabilmesidir. Bu nedenle bir kişinin bulut depolama sistemlerine sadece kendisinin erişebileceği şekilde yüklediği içerikler bu bağlamda bir yayın olarak kabul edilmeyecektir.

İnternetin Sjojeleri ve Sorumluluk Rejimleri

5651 sayılı Kanunun sistematğinde dört farklı internet sjesi ile karşılaşmaktadır. Bunlar “içerik sağlayıcı”, “yer sağlayıcı”, “erişim sağlayıcı” ve “sosyal ağ sağlayıcı”dır. Her birinin kendine has özellikleri olduğu gibi farklı sorumlulukları ve görevleri de vardır.

İnternet kullanıcıları eskiden birer tüketici konumdayken artık tüketiciden ziyade üretici olarak karşımıza çıkmaktadır. Twitter, Facebook ve Instagram gibi platformlarda internet kullanıcıları paylaşımlar yapmakta, kişisel blog sayfaları artırmakta, YouTube ve Twitch gibi platformlarda video, canlı yayın ve içerik paylaşımları artış göstermektedir. Sonuç olarak günümüzde internet bir içerik üretme

yeri olarak işlev göstermekte ve kullanımının azımsanmayacak bir bölümü kullanıcılarının oluşturduğu içeriklerden oluşmaktadır. Durum böyle olunca internetin sükelerinden birinin de içerik sağlayıcı olması kaçınılmazdır.

İçerik Sağlayıcı Kimdir?

İçerik sağlayıcı, internet üzerinden internet kullanıcılarına bir bilgi veya veriyi sunan, bu veri veya bilgiyi üreten, değıştiren veya sağlayan gerçek ve tüzel kişilerdir. Veri, bilgisayar teknolojileri tarafından üzerinde işlem yapılabilen her türlü değeri ifade ederken, bilgi ise bu verilerin anlam kazanmış biçimleri anlamına gelmektedir. Bilgi ve verinin teknik tanımları ve özellikleri bir yana bırakılacak olursa, internet ortamında gerçek veya tüzel kişilerin yayınladıkları ve üçüncü kişiler tarafından erişilebilir olan her şey içerik olarak tanımlanmaya müsait ve elverişlidir. Bu minvalde yapılan yayınlar içerik olarak değerlendirilmekte ve bu yayınları gerçekleştirenler de içerik sağlayıcı olarak kabul edilmektedir.



İçerik Sağlayıcının Sorumluluğu

İçerik sağlayıcılar, internet ortamında kullanıma sundukları, yani paylaştıkları veya yayınladıkları her türlü içerikten **doğrudan** sorumludurlar. Bir Twitter kullanıcısı paylaştığı tweetten, bir YouTube kullanıcısı yayınladığı videodan veya bir paylaşım yaptığı yorumdan, veya bir Twitch yayıncısı gerçekleştirdiği yayından doğrudan sorumludur. İçeriğin bir suç teşkil etmesi veya bir başkasının haklarını zedelemesi durumunda içerik sağlayıcı olarak sorumluluğu gündeme gelebilecektir.

Peki, bir içerik sağlayıcının internet ortamında kullanıma sunduğu içerik kendisine ait değilse sorumluluğu doğacak mıdır? Kural olarak içerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak bu durumun istisnası bulunmakta olup dikkat edilmesi gereken hususlar mevcuttur. Eğer içerik sağlayıcısı sunuş biçimi göz önünde bulundurulduğunda bağlantı sağladığı başkasına ait içeriği açıkça benimsiyorsa ve internet kullanıcılarının söz konusu içeriğe ulaşmasını açıkça amaçlıyorsa ise bu durumda içerik sağlayıcının genel hükümlere göre sorumluluğu da gündeme gelebilecektir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Twitter ve benzeri platformlarda veyahut diğer çeşitli site veya platformlarda internet ortamında yapılan paylaşımlar, o içeriği yayınlayan açısından sorumluluk doğuracaktır. Ancak başkasına ait bir içeriğin kullanıma sunulduğu durumda içerik sağlayıcı konumunda olan kişinin söz konusu yayını benimseyip benimsemediği ve diğer internet kullanıcılarının o yayına erişimini amaçlayıp amaçlamadığı değerlendirilecektir.

Yer Sağlayıcı Kimdir?

Yer sağlayıcılar, içerik sağlayıcıların ve diğer internet sülerlerinin yayın yaptıkları sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir. İçerik sağlayıcı içeriği üreten iken yer sağlayıcı ise söz konusu içeriklerin bir sistemde veya platformda yayınlanması hizmetini sunmaktadır. Yer sağlayıcı doğrudan içerik yaratmaktan ziyade kullanıcılarının içerik yayınlamasına olanak sağlamaktadır. Sonuç olarak internetin paydaşlarının içeriklerinin veya hizmetlerinin yayınlamasına aracılık eden sistemleri ve platformları sağlayan veya işleten gerçek ve tüzel kişiler yer sağlayıcı olarak nitelendirilmektedir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Twitter, Facebook ve benzeri platformlar açıklanan nedenlerden ötürü yer sağlayıcı olarak nitelendirilmeye elverişlidir. Sayılan platformların ve benzerlerinin aşağıda açıklanacak olan sosyal ağ sağlayıcı olması da kuvvetle muhtemeldir.



DİKKAT EDELİM

Yer sağlayıcılar her ne kadar içerik sağlamaktan ziyade söz konusu içeriklerin yayınlanması noktasında işlev gösterse de yer sağlayıcıların da şartları olduğu takdirde içerik sağlayıcısı olması mümkündür. Örneğin, Twitter bir yer sağlayıcı olduğu kadar sosyal ağ sağlayıcıdır; ancak, içerik sağlayıcı olarak nitelendirilmesi de gündeme gelebilmektedir. Yer sağlayıcılar, kendi sistemlerinde veyahut başka bir sistemde içerik yayınlamaları halinde içerik sağlayıcı konumuna geleceklerdir. Örneğin Twitter esasen bir yer ve sosyal ağ sağlayıcı iken eğer kendisi bir içeriği internet ortamı üzerinden kullanıcılarına sunarsa bu durumda yayına sunduğu içerik bakımından içerik sağlayıcı olarak değerlendirilecek ve yukarıda içerik sağlayıcılar için belirtilen sorumluluklara tabi olacaktır.

Yer Sağlayıcının Sorumluluğu ve Yükümlülükleri

Yer sağlayıcılar, yer sağladıkları içerikleri kontrol etmekle yükümlü değildirler. Ayrıca yer sağladıkları söz konusu içeriklerin hukuka uygunluğunu araştırmaları da gerekmemektedir. Yer sağlayıcıya bu yönde bir yükümlülüğün getirilmemesinin ana sebebi mahiyeti gereği yayınlanmasına imkan sağladığı içerik sayısının sayıca fazlalığıdır.



EK BİLGİ

YouTube'a her dakika toplamda beş yüz saat uzunluğunda video yüklenmektedir. Twitter'da ise her gün beş yüz milyon adet tweet atılmakta, bu sayı saniyede altı bin tweete tekabül etmektedir. Yer sağlayıcıların yer sağladığı içeriklerin sayı bakımından ulaştığı seviye yer sağlayıcıların bütün içerikleri tek tek denetlemesini imkânsız kılmaktadır.

Yer sağlayıcıların her ne kadar yer sağladıkları içerikleri denetleme noktasında bir sorumlulukları olmasa da aşağıda etraflıca incelenecek olan belirli şartlarda hukuka aykırı içeriği yayından çıkarma yükümlülüğü vardır. Yer sağlayıcı kendisine yapılan bildirim çerçevesinde söz konusu hukuka aykırı içeriklerin çıkarılması noktasında gerekli işlemleri yapmakla mükelleftir.

Gereken bildirim yapıldığı takdirde içerikleri yayından çıkarmaya ek olarak yer sağlayıcının sağladığı hizmete ilişkin trafik bilgilerini de saklaması kanuni bir yükümlülüğüdür. Trafik bilgisinin kapsamını yer sağladığı içeriklere ve taraflarına ilişkin IP adresi, port bilgisi, hizmetin başlama ve bitiş zamanı, hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri oluşturmaktadır. Yer sağlayıcı bu trafik bilgilerini bir yıldan az ve iki yıldan fazla olmayacak şekilde yönetmelikte belirtilen süre için muhafaza etmekle mükelleftir.

Erişim Sağlayıcı Kimdir?

Erişim sağlayıcı, kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişidir. İnternet ortamına erişim olanağı sağlama ile kastedilen yer sağlayıcının abonelerine internet altyapısını kullanma ve internete bağlanabilme hizmeti ve olanağı sunmasıdır. Bu hizmet ve olanağı sağlayan gerçek ve tüzel kişiler erişim sağlayıcı olarak nitelendirilmeye elverişlidir. İnternete erişim hizmeti sunan TürkTelekom ve KabloNet gibi kuruluşlar erişim sağlayıcı olarak kabul edilmektedir.

Erişim Sağlayıcının Sorumluluğu ve Yükümlülüğü

Yer sağlayıcılara benzer bir biçimde erişim sağlayıcıları da bilgi, veri ve içeriklerin hukuka aykırı olup olmadığını denetlemekle yükümlü değildir. Erişim sağlayıcıların içeriğe ulaşılmasında etkili ve elzem olduğu düşünüldüğünde bu sonuca varılması da kaçınılmazdır. Bu nedenle, tekrar etmek gerekirse, erişim sağlayıcı erişimine imkan ve hizmet sağladığı içeriklerin hukuka uygun olup olmadığını denetlememekte ve bu nedenle de sorumluluğuna gidilememektedir.

Erişim sağlayıcıların her ne kadar içeriklere ilişkin hukuka uygunluk denetimi yapması gerekmesi de eğer erişim sağlayıcılar bir kullanıcısının yayınladığı hukuka aykırı içerikten kanunun öngördüğü usul ve esaslara uygun bir biçimde haberdar edilirse bu durumda söz konusu hukuka aykırı içeriğe erişimi engellemekle mükelleftir.

Yine yer sağlayıcılara benzer bir biçimde erişim sağlayıcılar sağladıkları hizmetlere ilişkin trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak şartıyla yönetmeliklerde belirtilen süre zarfında muhafaza etmekle mükelleftir. Trafik bilgilerinin kapsamı yer sağlayıcılarının trafik bilgileri ile aynıdır.

Sosyal Ağ Sağlayıcı Kimdir?

Sosyal ağ sağlayıcılar aslında yer sağlayıcıların bir alt kırılımı olarak karşımıza çıkmaktadır. Sosyal ağ sağlayıcıları yer sağlayıcılardan ayıran ana unsur ise kullanıcılarına sosyal etkileşim amacıyla internet ortamında; görüntü, ses, video, metin, konum ve benzeri içerikleri oluşturma, yayınlama ve görüntüleme imkânı sağlamaktadırlar.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Twitter, Facebook ve benzeri sosyal medya platformları sosyal ağ sağlayıcı olarak nitelendirilmeye elverişlidir.

Sosyal Ağ Sağlayıcıların Yükümlülükleri ve Sorumlulukları

Sosyal ağ sağlayıcının sorumluluğu yer ve erişim sağlayıcılar ile paraleldir. Bünyelerindeki içeriklerin hukuka aykırılığından sorumlu olmamakla birlikte, kanun hükümlerine göre kendilerine bir hukuka aykırılık bildirimi yapıldığı takdirde gereğini icra etmek zorundadırlar. Ayrıca yurtdışı kaynaklı sosyal ağ sağlayıcılar, Türkiye’den günlük erişimleri bir milyondan fazla ise bu durumda idari işlemlerin ve taleplerin takip edilmesi ve yerine getirilmesi için yetkili en az bir kişiyi Türkiye’de temsilci olarak belirlemekle mükelleftir. Yetkili kişinin iletişim bilgileri kolayca ve doğrudan erişilebilecek bir şekilde sosyal ağ sağlayıcının internet sitesinde yer almalıdır.

Ek olarak sosyal ağ sağlayıcı kendisine bildiren içerik çıkarılması ve/veya erişimin engellenmesi kararlarını tıpkı yer ve erişim sağlayıcıların yükümlü olduğu gibi yerine getirmekle mükelleftir. Bir içeriğin hukuka aykırı olduğunun bir mahkeme tarafından tespit edilmesi üzerine sosyal ağ sağlayıcıya bildirilecektir. Sosyal ağ sağlayıcı kendisine gerçekleştirilen bu bildirim istinaden bildirimin gereğini yirmi dört saat içerisinde yerine getirmek zorundadır. Yapılan bildirimle rağmen içeriği çıkarma ve/veya erişimi engelleme kararını yerine getirmeyen sosyal ağ sağlayıcı, doğan zararlardan sorumlu tutulabilecektir.



DİKKAT EDELİM

Twitter, Facebook ve benzeri sosyal medya platformları sosyal ağ sağlayıcı olarak nitelendirilmeye elverişlidir.

İnternet Yayınlarında İçeriğin Çıkarılması ve Erişimin Engellenmesi

İnternet ortamında yayın yapmak teknolojinin ve bilhassa internet altyapısının gelişmesi ve yaygınlaşması ile oldukça kolaylaşmıştır. Yapılan yayınların kolaylaşması insanlar arasındaki etkileşimi ve iletişimi artırdığı gibi suç teşkil eden veya başkalarının haklarını ihlal eden yayınların daha sık karşılıklı hale gelmesine ön ayak olmuştur. Bu yayınlar ile mücadele noktasında da kanun koyucu sistematik birtakım önlem ve tedbirler getirme yoluna gitmiştir. 5651 sayılı Kanun çerçevesinde erişimin engellenmesi ve içeriğin çıkarılması dört ana başlık altında toplanmaya elverişlidir.

Kategorik Suçlar

Gösterdikleri öneme istinaden kanun koyucu belirli suç tiplerini özel olarak düzenlemiştir. Bir yayının sayılan suçlardan birini oluşturduğu noktasında yeterli şüphe bulunduğu durumlarda söz konusu yayın çıkarılacak veya yayına erişim engellenecektir. Bu suçlar dokuz adet olup şu şekildedir:

- İntihara yönlendirme,
- Çocukların cinsel istismarı,
- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma,
- Sağlık için tehlikeli madde temini,
- Müstehcenlik,
- Fuhuş,
- Kumar oynanması için yer ve imkân sağlama,
- Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar,
- Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar.

Söz konusu suçların oluştuğuna yönelik yeterli şüphe bulunduğu hallerde kural olarak içeriğin çıkarılması veya erişimin engellenmesi kararı *soruşturma evresinde hâkim tarafından kovuşturma evresinde ise mahkemeler tarafından verilecektir.*



EK BİLGİ

Söz konusu suçlar henüz daha soruşturma evresinde iken, karar alınmasında gecikilmesinde ciddi bir sakınca bulunduğu durumlarda Cumhuriyet Savcıları da erişimin engellenmesi ve/veya içeriğin çıkarılması kararı verebilirler. Bu durumda Cumhuriyet Savcısı kararını yirmi dört saat içerisinde hâkim onayına sunmak zorundadır. Hâkim de kararını en geç yirmi dört saat içerisinde bildirecektir. Hâkim, Cumhuriyet Savcısının kararını onaylamazsa veya yirmi dört saat içerisinde onaylamazsa alınan söz konusu içeriğin çıkarılması ve/veya erişimin engellenmesi kararı Cumhuriyet Savcısı tarafından derhal kaldırılır.

Gecikilmesinde Sakınca Bulunan Haller

İnternet ortamının hızlı etkileşimi nedeniyle bazı durumlarda zaman kaybetmeden bir an önce hareket edilmesi bir zorunluluk olarak karşımıza çıkmaktadır. Dezenformasyon içeren veya kışkırtıcı mahiyetteki yayınlar toplum güvenliğini, sağlığını ve kamu düzenini bazen tehlikede bırakabilmektedir. Bu tür durumların önüne geçilmesi adına;

- Yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması,
- Milli güvenlik ve kamu düzeninin korunması,
- Suç işlenmesinin önlenmesi,
- Genel sağlığın korunması

sebeplerine dayanarak hâkim, içeriğin çıkarılması ve/veya erişimin kaldırılması kararı alabileceği gibi, söz konusu hususlarla ilgili **Bakanlıklar** veya **Cumhurbaşkanlığı** da bu yönde talepte bulunabilir. Bu talep de Bilgi Teknolojileri ve İletişim Kurumu Başkanı tarafından kabul edilebilir.

Blokszincir Teknolojisi Ve Kripto Varlıklar

Blokszincir, blokların birbirinin ardına eklenerek uzayıp giden bir zincir haline geldiği teknoloji olarak tanımlanmaya elverişlidir. Söz konusu bloklar içlerinde kriptografik yöntemlerle şifrelenmiş veriler barındırmaktadır. Bu blokların birbirlerine eklenmesi ile uzamaya devam eden zincire de blokszincir denmektedir. Blokszincir bu yönüyle şifrelenmiş bir veri tabanıdır.

Tek bir blokszincir bulunmayıp blokszincirlerin birden fazla türü mevcuttur. Bazı blokszincirler genel, bazıları ise özel niteliktedir. Genel blokszincirler kural olarak herkesin kişisel bilgisayarları aracılığıyla blokszincir ağına erişim sağlayabildikleri ve işlem yapabildikleri blokszincirlerdir. Genel blokszincirlerin başlıca örnekleri *BitCoin* ve *Ethereum*'dur. Bu blokszincirlere erişim için kural olarak bir izin gerekmemektedir.

Özel blokszincirler genel blokszincirlerin aksine herkesin erişim sağlayamadığı blokszincir yapısıdır. Özel blokszincirlere erişim sağlanabilmesi için önceden erişim izni alınması gerekmektedir. Bu tarz blokszincirler izinli blokszincir olarak da adlandırılmakta ve şu an için genellikle şirketler ve özel organizasyonlarca kullanılmaktadır.

Kripto varlıklar ise genellikle blokszincir teknolojisi ve kriptografik yöntemler ile meydana getirilen sanal varlıklardır. Kripto varlıklar arz ettikleri özelliklere göre farklı sınıflandırmalara tabi tutulabilmektedir. Ana ayırım ise coin ve token olarak karşımıza çıkmaktadır. Coinler genellikle ödeme aracı olarak kullanılma gayesiyle ortaya çıkmaktadır ve kendilerine özgü bir blokszincire sahiptir. Tokenlar ise genel olarak başka bir blokszincir üzerinde faaliyet göstermektedir ve kullanım alanları daha çeşitlidir. Menkul kıymet tokeni, ödeme tokeni, fayda tokeni, NFT ve varlığa dayalı token olmak üzere farklı token türleri mevcuttur.

Arz ettikleri özelliklere göre kripto varlıklara uygulanacak hukuk kuralları da değişiklik göstermektedir. Ödeme aracı vasfı taşıyanların bankacılık mevzuatına tabi olması olasıyken, menkul kıymet vasfı gösterenlerin Sermaye Piyasası Kanunu'na tabi olması mümkündür.

Blokszincir Teknolojisinin Bazı Kullanım Alanları

Blokszincir teknolojisinin kullanım alanlarının sınırları henüz tam olarak netleşmiş değildir. Kullanımı giderek artan ve kolaylaşan blokszincir teknolojisinin gelecekte daha da fazla kullanım alanı bulacağı neredeyse şüphesizdir. Blokszincir teknolojisinin hemen hemen her gün yeni bir kullanım alanı ortaya çıksa da şu an sıklıkla kullanıldıkları ve kullanılmaları muhtemel alanlar; ödeme hizmetleri, değer ve belge saklama hizmetleri, kitle fonlaması ve noterlik işlemleridir.

Ödemelerde Kullanılması

Günümüzde artık hemen hemen bütün ödeme işlemleri, aracı kurumlar vasıtası ile gerçekleştirilmektedir. Genellikle bankalar ve sair kuruluşlar vasıtası ile gerçekleştirilen bu ödeme işlemleri ve para transferleri kimi zaman fazlasıyla maliyetli kimi zamansa uzun sürmektedir. Denizaşırı iki ülke arasında para transferi gerçekleştirilmek istendiğinde aralarında para transferi gerçekleştirilecek kişilere ek olarak genellikle en az üç banka daha sürece müdahil olmakta; her birinin aldığı komisyon transferin maliyetini artırmakta, bürokratik süreçler ise transferin gerçekleştirilme süresini uzatmaktadır.

Klasik sistemin beraberinde getirdiği zamansal ve mali külfete ek olarak bir de söz konusu kurumlara güven duyulması gerekmektedir. Blokszincir teknolojisiyle ise dünyanın herhangi bir yerinden bir başka yerine herhangi bir aracıya ihtiyaç duymaksızın anında ve nispeten çok daha ucuz bir şekilde para ve değer transferi gerçekleştirilmesi mümkündür.

Değer ve Belge Saklama

Kamu kurum ve kuruluşuna ek olarak birçok özel şirket ve organizasyon da değerlerini ve belgelerini çeşitli yöntemlerle saklamaktadır. Üniversiteler diplomaları ve öğrencilerine ilişkin bilgileri, özel veya kamu kurum ve kuruluşları sertifikaları, sağlık kuruluşları hastalara ilişkin bilgi ve belgeleri, şirketler imzaladıkları sözleşmeleri ve personellerine ilişkin bilgileri bir şekilde saklamaktadır. Söz konusu bilgi, belge ve değerlerin doğru ve güncel olması gerekmekte; güvenli bir şekilde saklanması da bir zarurettir. Blokzincir teknolojisi ile söz konusu bilgi, belge ve değerlerin kripto varlık haline getirilmesi ve blokzincir üzerinde güvenle saklanması mümkündür.

Blokzincir üzerinde gerçekleştirilen bütün işlemlerin şeffaf ve takip edilebilir olması sahteciliğin önünde önemli bir güvencedir. Blokzincirdeki kayıtların kural olarak değiştirilemez oluşu saklanmak istenen bilgi ve belgelerin orijinalliğini teyit etme noktasında kritik bir işleve sahiptir.

Kitle Fonlamasında Kullanılması

Kitle fonlamasına ihtiyaç duyulmasının nedeni olarak yeterli ve gerekli sermayeye sahip olmayan girişimcilerin sermaye arayışı gösterilebilir. Girişimci ruha sahip kişiler kimi zaman sermayeden yoksundur. Yaratıcı fikirlerini hayata geçirebilmeleri için bir sermayeye veya finans kaynağına ihtiyaç duymaktadır.

Kitle fonlaması çeşitli usul ve yöntemlerle yapılabilmekte olup; yatırımcılarına sağladıkları fon karşılığında vaat ettiklerine göre çeşitli sınıflara ayrılmaktadır. Bağışa, ödüle, borca ve paya dayalı olmak üzere dört sınıf altında incelenebilmektedir.

Bağışa dayalı kitle fonlamasında fon sağlayan kişiler herhangi bir karşılık almamakta, söz konusu projeye bağış yapmaktadırlar. Ödüle dayalı kitle fonlamalarında ise yatırımcılara bir karşılık olarak finansal değeri olan ya da olmayan, maddi ve/veya manevi bir ödül verilmektedir.

Borçlanmaya dayalı kitle fonlamasında, yatırımcılardan toplanan söz konusu fonlar bir borç niteliğindedir. Vadesi geldiğinde fonlanan girişimciler tarafından fon, yatırımcılara öncesinde belirlenmiş faiz ile birlikte geri ödenmektedir. Paya dayalı kitle fonlamasında ise fonlanan şirket ve/veya proje için borç sermaye aranmasından ziyade söz konusu şirkete ortak aranmaktadır. Paya dayalı kitle fonlaması ile fonlayan sermaye sahibi söz konusu şirketin bir ortağı haline gelmektedir.

Blokzincir teknolojisi ve beraberinde getirdiği avantajlar kitle fonlamasının daha da geniş kitlelere yayılarak uygulanmasına ön ayak olabilecek niteliktedir. Blokzincir üzerinden yapılacak bir kitle fonlaması ile dünyanın her yerinden katılımcıların fonlamaya katılmaları mümkün hale gelecektir. Fonlama karşılığında katılımcılara verilmesi vad edilen hususlar ise yine blokzincir üzerinde kayıt altına alınıp hızlı, güvenli, doğrudan ve nispeten daha ucuz bir şekilde katılımcılara aktarılabilir.

Her ne kadar teknolojik olarak blokzincir teknolojisi kitle fonlamalarında kullanılmaya elverişli görünse de, Türk Hukuku açısından birtakım sorunları gündeme getirmektedir. Zira, kitle fonlaması hukukumuzda 6362 sayılı Sermaye Piyasası Kanunu ve bu kanun uyarınca çıkarılan tebliğler ile düzenlenmektedir. Kitle fonlaması ancak kitle fonlama platformları aracılığı ile gerçekleştirilmektedir ve konuya ilişkin birçok sınırlandırma mevcuttur. Şu ana kadar çıkarılan tebliğler ile paya ve borçlanmaya dayalı kitle fonlaması düzenlenmiş, bağışa ve ödüle dayalı kitle fonlaması ise hukukumuzda öngörülmemiştir. Kitle fonlaması faaliyetinin kapsamı, şekli ve alanı sıkı bir biçimde düzenlendiğinden blokzincir teknolojisinin kitle fonlama faaliyetinde kullanılması hukuken tartışmalı ve hatta sakıncalıdır.

Noterlik İşlemleri

Noterlik, kanunla düzenlenen bir kamu hizmetidir. Noterler genel olarak birtakım işlemleri belgelendirmek yoluyla hukuki güvenliği sağlama işlevi göstermekte; belgelendirdikleri işlemler ile uyumazlıkları önlemeyi hedeflemektedir. Noterlerce yapılan işlemler tekildir. Her noter kendisine başvuru ile ilgili gerekli belgelendirmeyi gerçekleştirerek sistemine kaydetmektedir. Noterler, işlem belgelendirmenin yanı sıra hem doğrulama hem de saklama hizmeti sunmaktadır. Asıl işlevleri işlem ve belgelere olan güveni sağlamak olan noterler yapıları gereği kapsamlı ve riskli bir hizmet sunmaktadır.

Blokszincir teknolojisi ise değiştirilemez, güvenli ve dağıtık defter yapısı sayesinde noterlik işlemlerine uygun bir görünüm sergilemektedir. Noterlerin blokszincir teknolojisini kullanarak sunduğu noterlik işlemlerini blokszincir ağı üzerinde kaydederek doğrulaması ve dağıtık defter şeklinde güvenli saklaması olası bir kullanım alanı olarak dikkat çekicidir.



EK BİLGİ

Dağıtık defter teknolojisi tek bir merkezi olmayan dağıtık bir yapıyı ifade etmektedir. Bu yapıda veriler, bilgiler ve belgeler tek bir merkezde muhafaza edilmez. Verilerin, bilgilerin ve belgelerin birden fazla kopyası farklı ağ ve yerlerde dijital olarak saklanmaktadır. Kopyalardan birinin herhangi bir şekilde yok edilmesi halinde veriler, bilgiler ve belgeler zayi olmamakta; diğer kopyalar vasıtası ile veri güvenliği sağlanmaktadır.

Blokszincir Teknolojisi ve Kripto Varlıkların Hukuka Etkileri

Blokszincir teknolojisi ve kripto varlıkların uygulama alanı yaygınlaştıkça hukuken ele alınmaları kaçınılmaz olmuştur. Bunların ödemelerde kullanılması klasik finansal sistemin dikkatini çekmiştir. Ulaştıkları hacim ise devletleri vergilendirme noktasında düzenleme arayışına itmiştir. Transferleri global ölçekte hızlı ve aracısız olduğu için kara paranın aklanmasıyla mücadele ve terörün finansmanını engelleme noktalarında birtakım yeni önlemlerin alınması şart haline gelmiştir.

Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik

Bazı işletmelerin birtakım kripto varlıklar vasıtası ile ödeme alacağını açıklaması ile birlikte kripto varlıkların ödemelerde kullanılmamasına yönelik bir yönetmelik Türkiye Cumhuriyet Merkez Bankası tarafından çıkarılmıştır. Söz konusu bu yönetmelikte kripto varlıklar, *dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıklar* olarak nitelendirilmiştir.

Tanımlama yapıldıktan sonra ise kripto varlıkların ödemelerde doğrudan veya dolaylı bir şekilde kullanılamayacağı ifade edilmiştir. Ayrıca, kripto varlıkların ödemelerde doğrudan veya dolaylı olarak kullanılmasına yönelik hizmetlerin verilmesi de yasaklanmıştır.

Kripto Varlıklara İlişkin Vergilendirme İhtiyacı

Ortaya çıktığı ilk zamanlarda göz ardı edilebilecek bir boyutta olan kripto varlıkların zaman içerisinde ciddi bir değer kazanması vergilendirme ihtiyacını da gündeme getirmiştir. Kripto varlıkların güncel global piyasa değeri 1,12 trilyon Amerikan Doları civarındadır. Kripto varlıkları bir bütün olarak tek bir ülke olarak değerlendirirsek dünyanın en büyük ilk 20 ekonomisi arasında yer alacaklardır. Ulaştıkları market değeri nedeniyle kripto varlıkların vergilendirilmesine ilişkin düzenleme hareketleri hız kazanmıştır.

Bir hususun vergilendirilebilmesi için öncelikle kanunen öngörülmüş olması gerekmektedir. Kanunsuz vergi olmaz ilkesi gereği kripto varlıkların kanunen bir tanımı yapılması ve başta Gelir Vergisi Kanunu olmak üzere vergi mevzuatındaki yerinin kanun koyucu tarafından tespit edilmesi gerekmektedir.

Kripto varlıkların vergilendirilmesinde karşılaşılan başlıca sorun ise tek tip bir kripto varlıktan söz edilememesidir. Bir tür kripto varlık ödeme aracı özelliği arz ederken bir başka kripto varlık menkul kıymet olarak nitelendirilebilmektedir. Bazı kripto varlıklar hiçbir ekonomik değer taşımazken bazıları çok farklı özellikler arz edebilmektedir.

Amerika Birleşik Devletleri, Kanada, Avustralya ve İngiltere başta olmak üzere bazı ülkeler kripto varlıkları vergilendirmektedir. Sayılan ülkelerin genel eğilimi kripto varlıkları arz ettikleri özelliğe göre inceleyerek ederek hukuk sistemlerinde hangi vergilendirilebilir hususa tekabül ediyorlarsa ona göre vergilendirme yönündedir. Türk Hukukunda ise kripto varlıklara ilişkin doğrudan bir tanımlama yapılmadığı ve başta Gelir Vergisi Kanunu olmak üzere ilgili sair mevzuatta gerekli düzenlemeler yapılmadığı için vergilendirme noktasında birtakım zorluklarla karşılaşmaktadır.

Suç Gelirlerinin Aklanması ve Terörün Finansmanının Önlenmesi Açısından Kripto Varlıklar

Blokzincir teknolojisine ve kripto varlıklara getirilen eleştirilerin başında terörün finansmanında ve kara paranın aklanmasında kullanılma ihtimalleri gelmektedir. Söz konusu suçlarla mücadele edilmesine yönelik çeşitli düzenlemeler bulunmaktadır. Başta finansal kuruluşlar olmak üzere mali piyasa işlemleri ile ilgisi olan kişi ve kurumlar önemli yükümlülükler altındadır.

Kripto varlıkların aracısız, doğrudan, hızlı ve merkeziyetsiz bir biçimde taraflar arasında transfer edilebilmesi nedeniyle terörün finansmanı ve suç gelirlerinin aklanması noktasında ciddi endişeler oluşmuştur. 2021 yılının mayıs ayında Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Yönetmelik'te yapılan değişiklik ile birlikte kripto varlık hizmet sağlayıcılar yükümlü haline gelmiştir. Sonuç olarak kripto varlık hizmet sağlayıcılar, müşterinin tanınması, şüpheli işlem bildirimi, bilgi ve belge temin etme, devamlı bilgi verme ile muhafaza ve ibraz yükümlülüklerine tabi tutulmuştur.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

“Kripto varlık hizmet sağlayıcılar”, günlük hayatta “borsa” olarak adlandırılan ulusal ve/veya uluslararası faaliyet gösteren, kripto varlıkların alım, satım, saklama ve transferi gibi işlemlere aracılık hizmeti sağlayan kuruluşlardır.

Metaverse ve Hukuk

Metaverse her ne kadar son dönemlerde popüler hale gelmiş olsa da aslına bakılırsa yeni bir konsept değildir. *Metaverse* kavramıyla ilk olarak 1992 yılında *Neal Stephenson* tarafından kaleme alınan *Snow Crash* adlı eserde karşılaşılmıştır. İnternet altyapısının gelişerek yaygınlaşması, artırılmış gerçeklik ve sanal gerçeklik teknolojilerinde gerçekleşen atılımlar *Metaverse*’i hiç olmadığı kadar mümkün kılarken; büyük şirketlerin bu alanda gerçekleştirmeyi vadettikleri yatırımlar *Metaverse*’ü oldukça popüler hale getirmiştir. Söz konusu *Metaverse*’lerde kullanıcıların artırılmış gerçeklik, sanal gerçeklik ve giyilebilir teknolojiler vasıtasıyla fiziki dünyadakine benzer veya çok daha farklı bir yaşamı deneyimlemeleri hedeflenmektedir.

Fiziksel ve dijital dünyayı bir araya getiren veyahut en azından getirmeyi vadeden *Metaverse* tekil bir yapıda değildir. Birden fazla *Metaverse* mevcuttur ve sayılarının artması da pek ala mümkündür. Henüz gelişimini tam olarak tamamlamamış olsalar da *Metaverse*’lerin insanlar için yeni bir gerçeklik olarak kabul edilmesi; eğitimden sanata, sağlık hizmetlerinden eğlence sektörüne kadar birçok etkinlik ve hizmetin fiziki ve sanal dünyanın harmanlanarak insanlara sunulmasında kullanılması beklenmektedir.

Metaverse’ler hem kuruluş hem geliştiriliş hem de kullanım süreçlerinde ciddi miktarda veriye ihtiyaç duymaktadır. Fiziki dünyaya bir alternatif yaratma potansiyeli olan bir konseptin ihtiyaç duyduğu veri tipi ve miktarı akıl almaz boyutlardadır. Veri ihtiyacına ek olarak söz konusu *Metaverse*’leri kullanan insanların sırf tüketici olmasından ziyade üretici konumunda olmaları öngörülmektedir.

Metaverse kullanıcılarının birbirleriyle etkileşime girmesi mümkün olduğu kadar teşvik de edilmektedir. Kullanıcılar *Metaverse*’lerde hukuki ilişkilere girmekte, çeşitli varlıklara hak sahibi olmakta ve kişisel verilerini *Metaverse* ile veya üçüncü bir kişiyle doğrudan veya dolaylı olarak paylaşmakta ve *Metaverse*’de bulundukları süreçte birçok yeni veri üretmektedir.

Metaverse mahiyeti gereği klasik hukuk anlayışımızı zorlamakta; başta sanal varlıklara ilişkin hak sahipliği, kullanıcılar arasındaki hukuki durum ve kişisel veri konuları olmak üzere birtakım yeni ve özgün sorunlar gündeme getirmektedir.

Metaverse’de Sanal Varlıklara İlişkin Hak Sahipliği

Dijital dünyada ve bilhassa *Metaverse*’de birçok varlık hak sahipliğine konu edilebilmektedir. Bu varlıkların bir kısmı alan adları kimi tanıdık kavramlar olabilirken bir kısmı yeni ve sanal dünyaya özgü olabilmektedir. Bazı tanıdık kavramların ise farklılaşarak *Metaverse*’lerde yeniden hak sahipliğine konu edilmesi karşılaşılan bir durumdur. Bir video oyununda oyuncunun yönettiği karakterin kuşanması için kılıç ve kalkan gibi dijital nesneler hak sahipliğine konu olabilirken; *Metaverse*’lerde evler, arabalar, araziler ve benzeri birtakım varlıklara ilişkin hak sahipliği ileri sürülebilmektedir.

Söz konusu dijital nesnelerin veya dijitalleşmiş nesnelerin eşya hukuku bakımından hukuki karşılıkları tartışmalıdır. Klasik eşya hukuku kavram ve ilkelerinin, gelişen teknoloji ile hayatımıza giren yeni ihtiyaçları karşılama noktasında kimi zaman yetersiz kalması mümkündür. Eşya hukukunun bazı temel kavram ve esaslarının da dijitalleşen dünyada yeniden yorumlanması gerekebilecektir. Zira, Metaverse’lerde şimdiden görülmeye başlanan sanal arazi satışlarının ve diğer benzeri meta alışveriş işlemlerinin değeri milyon dolarla ifade edilmektedir.

Metaverse Kullanıcıları Arasındaki Hukuki Durum

Metaverse’in interaktif doğası gereği, bu sanal dünyalarda kullanıcılar birbirleriyle avaturları aracılığı ile görsel ve işitsel olarak etkileşime geçebilmekte ve iletişim kurabilmektedir. Kullanıcılarının birbirleriyle etkileşime girebildiği bir sanal veya fiziki ortamın hukuki ve ekonomik sıkıntıları bünyesinde barındırması kaçınılmazdır. Zira, tam da bu nedenden ötürü, kullanıcılarla *Metaverse*’in arasındaki ilişki ve hukuki durum kadar, ki belki daha da fazla, kullanıcıların bizatihi kendi aralarındaki sorunların ve çatışmaların düzenlenmesi gerekmektedir.

Metaverse’de kullanıcılar arasında etkileşim mümkün olduğundan kullanıcılarının birbirleri veya kamu aleyhine hukuka aykırı hareketlerde bulunmaları, kişilik haklarının ve fikri mülkiyet haklarının ihlalini gündeme getirebilecek birtakım eylemlerde bulunmaları da mümkündür. *Metaverse*’e özgü bir hukuki düzenleme bulunmamakta; şu an için bu minvalde bir ihtiyaç da görülmemektedir. Kullanıcılar tarafından gerçekleştirilen işlemler neticesinde ortaya çıkan ihtilaflarda incelenmesi gereken husus somut hukuk kurallarının *Metaverse* gibi sanal dünyalarda gerçekleştirilen işlemlere nasıl ve ne ölçüde uygulanacağıdır.

Kural olarak hukuka aykırı bir işlemin veya eylemin sanal ortamda gerçekleştirilmesi söz konusu işlem veya eylemin hukuka aykırılığını etkilememektedir. Bir işlem veya eylem normal şartlarda hukuka aykırı ise *Metaverse*’de gerçekleştirilmesi halinde de kural olarak hukuka aykırılık teşkil edecektir. Örnek vermek gerekirse, kullanıcıların sanal ortamlarda birbirlerine karşı hakaret ve tehdit içerikli mesajlar, iletiler veya görseller göndermesi; konusu suç teşkil eden eylemlerde bulunması halinde hukuki yaptırımlar ve cezai müeyyideler gündeme gelebilecektir.

Metaverse’de Kişisel Veriler

Veri, *Metaverse* ve benzeri platformların hammaddesi olarak kabul edilmektedir. Kuruluş aşamasında dahi ciddi miktarda veriye ihtiyaç duymakta faaliyete geçtikten sonra ise işlediği veri miktarı gideerek artmaktadır. Veriler yalnızca *Metaverse*’ler için değil, gelişen teknolojiler ile birlikte artık her alanda büyük ekonomik değer taşımaktadır.

Kullanıcılar daha *Metaverse*’e giriş yapıp avaturlarını oluşturmadan önce bile kişisel verilerini söz konusu platformlar ile paylaşmaktadır. *Metaverse*’ü kullanabilmek için gerekli olan artırılmış gerçeklik, sanal gerçeklik veya giyilebilir teknolojileri kullanırken birçok veri kullanıcı tarafından ilgililerle paylaşılmaktadır. Kullanıcılar, *Metaverse*’de platform ile veya diğer kullanıcılar ile etkileşime geçerken ve yahut sadece *Metaverse*’de bulunurken dahi çeşitli nedenlerle ses, parmak izi, yüz veya sair biyometrik veriler paylaşılabilmektedir. Paylaşılan bu minvaldeki verilerin ve sair verilerin güvenliğini sağlamak ve öncesinde ve/veya gerektiği zaman bu verilerin işlenmesine ilişkin gerekli izin ve bildirimleri yapmak verileri işleyen *Metaverse*’in sorumluluğundadır. Bu bağlamda, günümüzde aktif olarak veri işleyen ve kişisel verilerin korunmasına ilişkin ulusal ve uluslararası düzenlemelere tabi olan çoğu kurum ve kuruluş gibi *Metaverse*’ler de kullanıcıların kişisel ve sair bilgilerinin güvenliğini ve gizliliğini korumakla mükelleftir.

BÖLÜM ÖZETİ

İnternet altyapısının gelişmesi ve yaygınlaşması ile birlikte insanlar arasındaki etkileşim ve iletişim hiç olmadığı kadar güçlenmiş ve kolay bir hal almıştır. Bu durum birçok yeni avantajı beraberinde getirmiş olsa da bünyesinde birtakım yadsınamaz sorunları barındırdığı da bir gerçektir. Özellikle internet ortamında yapılan yayınlar kimi zaman ciddi suçlar teşkil edebilmekte kimi zaman da kamu düzenini tehdit edebilmektedir.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun amacı internet ortamında yapılan yayınların düzenlenmesi, suçların engellenmesi, bireylerin ve kurumların haklarını koruma amacıyla birtakım yasal düzenlemeler yapılmasıdır. Bu Kanunla ilk olarak kanun koyucu internet ortamının sürelerini belirleyerek sorumluluklarının çerçevesini çizmiştir. Bu internet sùjelerinin başlıcaları; içerik sağlayıcı, yer sağlayıcı, sosyal ağ sağlayıcı ve içerik sağlayıcı olarak karşımıza çıkmaktadır.

İçerik sağlayıcılar, bir Twitter veya YouTube kullanıcısı olarak karşımıza çıkabilmektedir. İçerik sağlayıcılar kural olarak internet ortamında yayına sundukları her tür içerikten sorumludurlar. Yer sağlayıcılar, içerik sağlayıcıların ve diğer internet sùjelerinin yayın yaptıkları sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir. İçerik sağlayıcı, içeriği üreten iken yer sağlayıcı ise söz konusu bu içeriklerin bir sistemde veya platformda yayınlanması hizmetini sunmaktadır. Erişim sağlayıcılar, kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişidir. İnternete erişim hizmeti sunan TürkTelekom ve KabloNet gibi kuruluşlar erişim sağlayıcı olarak kabul edilmektedir. Sosyal ağ sağlayıcılar ise yer sağlayıcıların bir alt kırılımı olarak karşımıza çıkmaktadır. Sosyal ağ sağlayıcıları, yer sağlayıcılardan ayıran ana unsur kullanıcılarına sosyal etkileşim amacıyla internet ortamında görüntü, ses, video, metin, konum ve benzeri içerikleri oluşturma, yayınlama ve görüntüleme imkânı sağlamalarıdır.

Blokszincir, blokların birbirinin ardına eklenerek uzayıp giden bir zincir hâline geldiği teknoloji olarak tanımlanmaktadır. Söz konusu bloklar, içlerinde kriptografik yöntemlerle şifrelenmiş veriler barındırmaktadır. Bu blokların birbirlerine eklenmesi ile uzamaya devam eden zincire de blokszincir denilmektedir. Blokszincir bu yönüyle şifrelenmiş bir veri tabanıdır. Kripto varlıklar ise genellikle blokszincir teknolojisi ve kriptografik yöntemler ile meydana getirilen sanal varlıklardır.

Metaverse her ne kadar son dönemlerde popüler hâle gelmiş olsa da aslına bakılırsa yeni bir konsept değildir. Metaverse’lerde kullanıcıların artırılmış gerçeklik, sanal gerçeklik ve giyilebilir teknolojiler vasıtasıyla fiziki dünyadakine benzer veya çok daha farklı bir yaşamı deneyimlemeleri hedeflenmektedir. Metaverse tekil bir yapıda değildir. Birden fazla Metaverse mevcuttur ve sayılarının artması da mümkündür. Kullanıcılar, Metaverse’de platform ile veya diğer kullanıcılar ile etkileşime geçerken veya sadece Metaverse’de bulunurken dahi çeşitli nedenlerle ses, parmak izi, yüz veya sair biyometrik veriler paylaşabilmektedir. Paylaşılan bu minvaldeki verilerin güvenliğini sağlamak ve öncesinde ve/veya gerektiği zaman bu verilerin işlenmesine ilişkin gerekli izin ve bildirimleri yapmak verileri işleyen Metaverse’in sorumluluğundadır.

GÖZDEN GEÇİRELİM

1. İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, de-
ğiştiren ve sağlayan gerçek veya tüzel kişilere denir.
2. Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişile-
re denir.
3. yayınladığı içerikten sorumlu olup paylaşım biçiminden benimsediği veya
başkalarından da ulaşmasını istediği anlaşılan başkasına ait içeriklerden de sorumlu tutulabile-
cektir.
4. sorumlulukları, yer ve erişim sağlayıcıların sorumluluğuyla paralel olup
yer sağladıkları içerikleri hukuka uygunluk açısından denetlemek zorunda değildir.
5. Özel hayatının ihlal edildiğini iddia eden bir kişi Kurumuna başvurarak
erişimin engellenmesini talep edebilir.
6. Blokzinciri oluşturan bloklar içlerinde kriptografik yöntemlerle şifrelenmiş
barındırmaktadır.
7. Blokzincir teknolojisiyle ise dünyanın herhangi bir yerinden bir başka yerine herhangi
bir ihtiyaç duymaksızın değer transferi gerçekleştirilmesi mümkündür.
8. Kripto varlıkların doğrudan veya dolaylı olarak kullanılmasına yönelik hiz-
metlerin verilmesi yasaklanmıştır.
9. Kullanıcılar tarafından paylaşılan güvenliğini sağlamak ve öncesinde ve/
veya gerektiği zaman gerekli izin ve bildirimleri yapmak verileri işleyen Metaverse'in sorumlu-
lughundadır.
10. Bir işlem veya eylem normal şartlarda hukuka aykırı ise Metaverse'de gerçekleştirilme-
si halinde de kural olarak teşkil edecektir.

CEVAP ANAHTARI

1. içerik sağlayıcı	6. veriler
2. yer sağlayıcı	7. aracıya
3. içerik sağlayıcı	8. ödemelerde
4. Sosyal ağ sağlayıcıların	9. kişisel veriler(in)
5. Bilgi Teknolojileri ve İletişim	10. hukuka aykırılık

SÖZLÜK

Dağıtık Defter Teknolojisi: Dağıtık defter teknolojisi tek bir merkezi olmayan dağıtık bir yapıyı ifade etmektedir. Bu yapıda veriler, bilgiler ve belgeler tek bir merkezde muhafaza edilmez. Verilerin, bilgilerin ve belgelerin birden fazla kopyası farklı ağ ve yerlerde dijital olarak saklanmaktadır.

Erişim Sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişilerdir.

Erişimin Engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesidir.

İçerik Sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişilerdir.

İçeriğin Yayından Çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasıdır.

Metaverse: Artırılmış gerçeklik, sanal gerçeklik ve giyilebilir teknolojiler vasıtasıyla kullanıcılarına özgün bir deneyim vadeden teknolojidir.

Sosyal Ağ Sağlayıcı: Sosyal etkileşim amacıyla kullanıcıların internet ortamında metin, görüntü, ses, konum gibi içerikleri oluşturmalarına, görüntülemelerine veya paylaşımlarına imkân sağlayan gerçek veya tüzel kişilerdir.

Veri: Bilgisayar teknolojileri tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder.

Yayın: İnternet ortamında yapılan yayındır.

Yer Sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.

KAYNAKÇA

- Aksoy Retornaz*, Emine: 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun Kapsamında İçerik Sağlayıcının Yükümlülükleri ve Ceza Sorumluluğu, *Ceza Hukuku Dergisi*, C. 16, S. 45, Nisan 2021, s. 9-32.
- Bilgili*, Fatih ; *Cengil*, Fatih: BlockChain ve Kripto Para Hukuku, Güncellenmiş 2. Baskı, Dora Yayınevi, 2022.
- Ciuriak*, Dan: On the Metaverse, Web3 and Prospering in the Digital Transformation, Saint Pierre Center for International Security, 2022.
- Çağlayan Aksoy*, Pınar: Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları, Güncellenmiş 2. Baskı, On İki Levha Yayınevi, İstanbul 2021.
- Çınar İsmail*: 5651 Sayılı Kanun Çerçevesinde Koruma Tedbiri Olarak İnternet Ortamında Yapılan Yayınlarda İçeriğin Çıkarılması ve/veya Erişimin Engellenmesi, İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, C. 8, S. 1, Bahar 2021, s. 63-96.
- Çırakoğlu*, Melikşah: 5651 Sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği, Birinci Baskı, Adalet Yayınevi, Ankara Ekim 2018.
- Demiz*, İsmail: Kişilik Haklarının İhlali Nedeniyle İnternet Sitelerine Erişimin Engellenmesi ve/veya İçeriğin Yayından Çıkarılmasında Görev ve Yetki Sorunu, *Bilişim Hukuku Dergisi*, 2021, C. 3, S. 2, s. 338-429.
- Doğan*, Aişe Sena: Kişilik Hakkının 5651 Sayılı Kanun'un 9. Maddesi Kapsamında Korunması, *Bilişim Hukuku Dergisi*, 2020, C. 2, S. 2, s. 143-180.
- Doğancı*, Doğa Ekrem: Blokzincire Dayalı Akıllı Sözleşmelerin Hukuki Nitelikleri, Kuruluşu, Yorumu, İfası ve Bazı Örnek Hukuki Uygulamalar, On İki Levha Yayınevi, İstanbul 2021.
- Gezder*, Ümit: İçerik Sağlayıcının ve Yer Sağlayıcının Hukuki Sorumluluğu ve Sorumluluk Muafiyeri, Birinci Baskı, Beta Yayıncılık, İstanbul Şubat 2017.
- Guadamuz*, Andres: Back to the Future: Regulation of Virtual Worlds. *Journal of Law, Technology and Society*, 4(3), 2007.
- Kaya*, Mehmet Bedii: İnternet Hukuku, İkinci Baskı, On İki Levha Yayıncılık, İstanbul Mayıs 2021.
- Kaya*, Mehmet Bedii: Teknik ve Hukuki Boyutlarıyla İnternete Erişim Engellenmesi, Birinci Baskı, On İki Levha Yayıncılık, İstanbul Mayıs 2010.
- Kılınç*, Doğan: 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması, Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 2016, C. 20, S. 2, s. 577-624.
- Memiş*, Tekin: Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri, Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi, 2009, C. 13, S. 3-4, s. 161-176.
- Özkaya*, Yunus: 5651 Sayılı Kanun Kapsamında Suç İşlenmesinin Önlenmesi Amacıyla İnternet Erişiminin Engellenmesi, *Bilişim Hukuku Dergisi*, 2022, C. 4, S. 1, s. 141-190.

Su Li Cheng, T.: Brave New World for Intellectual Property Rights. Journal of Law, Information and Science, 17, 2006.

Sundquist, Matthew: Online Privacy Protection: Protecting Privacy, The Social Contract, And The Rule Of Law In The Virtual World. Regent University Law Review. Vol 25: 153, 2012.

Suzor, Nicolas: The Role of the Rule of Law in Virtual Communities. Berkeley Technology Law Journal, 25(4), 2010.

Tevetoglu, Mete: Meta Dünya’da Hukuk, Maltepe Üniversitesi Yayınları, İstanbul 2022.

Tevetoglu, Mete: Hukuki Yönleriyle Kripto Varlıklar ve Kripto Varlıkların İlk Arzı, Aristo Yayınevi, İstanbul 2021.

ÜNİTE 3

KİŞİSEL VERİLERİN KORUNMASI HUKUKU

Doç. Dr. Pınar ÇAĞLAYAN AKSOY
Doç. Dr. Hüseyin Can AKSOY

ANAHTAR KAVRAMLAR

Kişisel veri
Açık rıza
İlgili kişi
Veri işleme
Veri sorumlusu

KİŞİSEL VERİLERİN KORUNMASI HUKUKU

ÖĞRENME HEDEFLERİ

-  1 Kişisel veri kavramını tanımlar.
-  2 Kişisel veri üzerindeki hakkın niteliğini analiz eder.
-  3 Veri sorumlusunu ve veri işleyeni tespit eder.
-  4 Kişisel verileri koruma hukukunun temel prensiplerini açıklar.
-  5 Verilerin korunması yollarını tartışır.

GİRİŞ



Dijital teknolojilerdeki gelişmelerin etkilediği alanlardan biri de kişisel verilerin korunmasıdır. Dijital teknolojilerdeki gelişmelerle birlikte, veri artan oranda önem kazanmış ve kişisel verilerin korunması daha da güncel bir sorun haline gelmiştir. Endüstri 4.0'ın temel bileşenlerinden olarak kabul edilen yapay zekâ, nesnelerin interneti (*internet of things*), büyük veri (*Big Data*) ve blokzinciri uygulamaları gibi teknolojiler, kişilere veya makinelere ait verilerin toplanmasına ve kaydedilmesine dayanmaktadır. Bu nedenle, içinde bulunduğumuz çağda veri “yeni petrol” olarak nitelendirilmektedir.

Türk Hukuku'nda kişisel verilerin korunması konusu 2000'lerin başından itibaren gündemde yer almaktadır. 2004 yılında Türk Ceza Kanunu'nda kişisel verilerin korunmasına ilişkin hükümler eklenmiş, 2010 yılında ise kişisel verilerin korunması bir temel hak olarak Anayasa'daki yerini almıştır. Avrupa Birliği'ndeki gelişmelere de paralel olarak Türkiye'de 2016 yılında Kişisel Verilerin Korunması Kanunu (KVKK) yürürlüğe girmiş ve Kişisel Verileri Koruma Kurumu kurulmuştur.

Kişisel verilerin korunması meselesinin merkezinde çatışan iki temel menfaat yer almaktadır. Bir taraftan bilginin serbest dolaşımı sağlanmak istenmektedir; zira inovasyonun teşviki, teknolojik gelişim ve ilerleme için bu dolaşım değerlidir. Diğer taraftan ise ilgili kişilerin hem Devlet hem de özel teşebbüsler karşısında korunması gerekmektedir. Nitekim, bilgi toplumunda kişisel veriler korunmazsa, birey devletler ve özel teşebbüsler karşısında zarar görme riski altına girer. Ayrıca kişisel verilerin korunması temel hak ve özgürlükler ile de yakından bağlantılıdır. Özellikle yapay zekâ teknolojilerindeki gelişmelerle birlikte, karar veren algoritmalar yaygınlaşmış ve veri diktatörlüğü gündeme gelmiştir. İşte kişisel verilerin korunması hukuku bu menfaat çatışmasını çözmeye çalışmaktadır.

Kişisel Verileri Koruma Hukuku'nun Tarihçesi

Öncelikle karşılaştırmalı hukukta kişisel verilerin korunmasına ilişkin olarak bugüne kadar atılan adımlar üzerinde kısaca duralım:

Alman Federe Devleti'nde kabul edilen 1970 tarihli yasa ve takip eden ulusal düzenlemeler ile devletler, vatandaşlarının verilerinin ülke dışına çıkarılmasını kontrol altına almaya çalışmıştır.

Uluslararası kuruluşlar, uluslararası ticarete zarar verilmesini önlemek amacıyla devletlerin kişisel verilere ilişkin olarak sağlaması gereken asgari koruma seviyesini belirlemeye çalışmışlardır. Söz konusu uluslararası düzenlemelerden başlıcaları şunlardır:

1. OECD İlkeleri (1980)
2. 108 sayılı Avrupa Konseyi Sözleşmesi (1981)
3. 45/95 sayılı Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (BM Rehber İlkeleri) (1990)
4. 95/46/EC sayılı AB Yönergesi (1995)
5. 97/55/EC – 2000/31/EC – 2002/58/EC sayılı Yönergeler
6. Avrupa Birliği Genel Veri Koruma Tüzüğü (2016) ("General Data Protection Regulation" veya "GDPR")

Türkiye'de önce 2004 yılında Türk Ceza Kanunu ile kişisel verilerin korunmasına ilişkin düzenlemeler getirildi. Daha sonra 2010 yılında yapılan değişiklik ile, kişisel verilerin korunması bir temel hak olarak Anayasa'ya girdi. 2016 yılında Kişisel Verilerin Korunması Kanunu yürürlüğe girdi. Yine 2016 yılında, 1981 tarihli ve 108 sayılı Avrupa Konseyi Sözleşmesi onaylandı.

Kişisel Verilerin Korunması Kanunu'nun Konu ve Yer Bakımından Uygulama Alanı

KVKK m. 2/1'e göre, *"Bu Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."*

Bazı durumlarda kanun koyucu KVKK'nın uygulama alanı bulmayacağını belirtmektedir. Örneğin, KVKK m. 28/1.a hükmüne göre, şahsi telefon veya adres defteri gibi, kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülöklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi KVKK kapsamında değerlendirilmeyecektir.

Yer bakımından uygulama konusunda ise mülklik prensibi kabul edilmiştir. Bu çerçevede, Türkiye Cumhuriyeti sınırları içerisinde gerçekleştirilen veri işleme faaliyetleri bakımından KVKK uygulama alanı bulacaktır. Kişisel verilerin hukuka aykırı olarak işlenmesi haksız fiil teşkil ettiğinden milletlerarası özel hukuk kuralları gereği de KVKK'nın uygulanması söz konusu olabilir.

Kişisel Veri Üzerindeki Hakkın Niteliği

Kişisel verilerin üzerindeki hakkın niteliği tartışmalıdır. Kişisel veriler bir ekonomik değere sahiptir. Peki buradan hareketle, veri sahiplerinin kişisel verileri üzerinde mülkiyet hakkına sahip oldukları düşünülebilir mi? Gerçekten de kişisel veriler, bireyin kişiliğinin bir ürünüdür. Bu ürünü kullanan kişiler, karşılığında adil bir bedel ödemelidirler. Bununla birlikte, Türk Hukuku'nda da benimsenen eşya

anlayışı çerçevesinde, hukuki anlamda eşya, üzerinde bireysel hakimiyet sağlanabilecek, ekonomik bir değer taşıyan, kişi ve hayvan dışında “cismani bir varlıktır”. Oysa veri, cismani bir varlık niteliği taşımamaktadır. Diğer taraftan, kişisel veriler üzerinde mülkiyet hakkı kabul edildiği takdirde, ilgili kişi, veriyi devralan kişinin veri üzerinde gerçekleştirdiği tasarruflar konusunda söz hakkını kaybedecektir. Oysa, ilerideki bölümlerde de görüleceği üzere, veri işleme yalnızca ilgili kişinin rızasıyla yapılabilir.

Peki kişisel veriler üzerindeki hak fikri mülkiyet hakkı sayılabilir mi? Bir taraftan, kişisel veri üzerindeki hak, eser sahibinin manevi haklarına benzer bir nitelik taşımaktadır. Bunlara örnek olarak eseri umuma arz yetkisi ve eserde değişiklik yapılmasını yasaklama yetkisi gösterilebilir. Bununla birlikte, Fikir ve Sanat Eserleri Kanunu’nda (FSEK) eser türleri sınırlı sayım ilkesine tabi olarak sıralanmıştır. Bu çerçevede, ilim ve edebiyat eseri, sinema eseri, müzik eseri gibi kategoriler belirlenmiştir. Ayrıca, fikri mülkiyet hukukunun varlık amacı, bilinçli olarak sarf edilen çaba ile eser ve buluşların yaratılmasını teşvik etmektir.

Diğer bir ihtimal olarak akla kişisel veri üzerindeki hakkın kişilik hakkının bir parçası olup olmaya- cağı gelmektedir. AB Temel Haklar Bildirgesi (2000), Bölüm II / Özgürlükler, Madde 7’ye bakıldığında şu ifadelerin yer aldığı görülmektedir: “Herkes, özel ve aile yaşamına, konutuna ve haberleşmesine saygı gösterilmesini isteme hakkına sahiptir.” Bu madde ayrıca, üst araması ve konut dokunulmazlığını da kapsamaktadır. Madde 8’de ise, kişisel bilgilerin korunması kenar başlığı ile şu hükme yer verilmiştir:

“1. Herkes, kendisine ilişkin kişisel bilgilerinin korunmasını isteme hakkına sahiptir.

2. Bu tür bilgiler, belirtilen amaçlar için ve ilgili kişinin muvafakatine veya yasada öngörülen başka meşru temele dayalı olarak adil şekilde kullanılmalıdır. Herkes, kendisi hakkında toplanmış olan bilgilere erişme ve bunlarda düzeltme yaptırma hakkına sahiptir.

3. Bu kurallara uyulması, bağımsız bir makam tarafından denetlenecektir.”

Türkiye Cumhuriyeti Anayasası’nda özel hayatın gizliliği kenar başlıklı m. 20/3’te şu ifadeler yer almaktadır:

“(3) 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”

Türk Hukuku’nda 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun amacı ortaya koyan 1. maddesinde şu ifadeler yer almaktadır:

“(1) Bu Kanunun amacı, 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 düzenlemektir.”

Tüm bu metinler dikkate alındığında, hukukumuzda kişisel verilerin bireyin kişilik hakkıyla ilgili olduğu kabul edilmektedir. Nitekim, kişilik hakkının çeşitli görünüm türleri bulunmakta olup bunlar sınırlı sayıda değildir. Bu çerçevede, bireyin kişisel verileri üzerindeki hakkı da tıpkı vücut bütünlüğü, özel yaşamı ve şeref ve haysiyeti gibi kişilik hakkının bir parçasıdır.

Kişisel Verilerin Korunmasına İlişkin Temel Kavramlar

Kişisel Veri

6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (m. 3/d) "kişisel veri", kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır. Bu bağlamda, tüzel kişilere ilişkin veriler ile ölmüş kişiler hakkındaki veriler KVKK kapsamında kişisel veri değildir.

Burada dikkat edilmesi gereken bir diğer nokta, bir gerçek kişiye ilişkin her türlü bilginin kişisel veri niteliği taşıdığıdır. Bu çerçevede, kişinin etnik kökeni, cinsel tercihi, eğitim bilgisi, hobileri, fiziksel özellikleri, yazısı, sesi, görüntüsü kişisel veri niteliği taşımaktadır. Bu bağlamda, bilgi, öznel veya nesnel olabilir. Ayrıca bilgi gizli bir nitelik taşımak zorunda da değildir. Önemle belirtmek gerekir ki, bu bilginin doğru olması da gerekmez.

Kimliği Belirli veya Belirlenebilir Kişi

Kimliği belirli veya belirlenebilir olma kavramlarının ne anlama geldiği üzerinde durulmasında fayda vardır. Belirli olma, verinin, kendi başına ve doğrudan ilgili kişiyi tespiti elverişli olmasını ifade eder. Örneğin, kişinin adı ve soyadı gibi bilgiler kimliği belirli bir kişiye ilişkindir. Belirlenebilir olma ise, bir kimsenin kimliğinin, ismi dışında tanımlayıcılar kullanılarak ve başka verilerle birleştirilerek tespit edilebilir olmasını ifade etmektedir. Örneğin, kişinin TC kimlik numarası, parmak izi veya ayırt edici fiziksel özellikleri gibi bilgiler ilgili kişiyi doğrudan doğruya tespit etmeye elverişli olmamakla birlikte, yine de kişisel veri niteliğindedir.

Anonim ve Takma Adlı (Psödonim Veri)

Anonim hale getirme, "Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini" ifade eder (KVKK m. 3/1.b). Bu nedenle, anonim veriler KVKK kapsamında değildir. Oysa psödonim yani takma adlı veriler, kişisel veri niteliği taşımaktadır. Psödonim veriler, ilave bilgiler olmadan, belli bir gerçek kişiyle eşleştiremeyen verilerdir. Mesela kişilerin adlarının şifreli olarak yayınlandığı bir listenin anahtarı kullanılarak ilgili kişilere ulaşılabilir.

Özel Nitelikli Kişisel Veriler

KVKK m. 6/1'e göre, "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 veridir." Kanun koyucu bu tür verilerin işlenmesi bakımından diğer tür verilere kıyasla daha sıkı şartlar getirmiştir.

Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlemleri ifade etmektedir. Kişisel verilerin işlenmesi, KVKK m. 3/1.e'de şu şekilde açıklanmaktadır: "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" veri işlemdir.

Bilgisayar, cep telefonu, drone, tarayıcı, akıllı saat gibi cihazlarla işlenen veriler de KVKK kapsamında yer almaktadır. Örneğin, kişisel verilerin bir web sitesine yüklenmesi de kişisel veri işleme niteliği taşımaktadır.

Veri Kayıt Sistemi

KVKK'ya göre, kağıt üzerinde kayıt altına alınan verilerin *“herhangi bir veri kayıt sisteminin parçası olmak kaydıyla”* Kanun kapsamında yer alır. KVKK m. 3/1.h bendinde, veri kayıt sisteminden ne anlaşılması gerektiği hüküm altına alınmıştır. Buna göre, veri kayıt sistemi, kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade etmektedir. Bu çerçevede iş yerlerindeki personel dosyaları ve muayenehanelerdeki hasta dosyaları bu kapsamda yer almaktadır. Belirtmek gerekir ki, eğer bir veri kayıt sistemi söz konusu değilse, KVKK'nın uygulanması mümkün olmayacaktır. Bununla birlikte, bu durumlarda da Türk Ceza Kanunu'nun ilgili hükümlerinin uygulanması söz konusu olabilir.

Veri Sorumlusu

KVKK m. 3/1.1 hükmüne göre “veri sorumlusu”, *“Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi...”* ifade etmektedir. Burada altı çizilmesi gereken ilk husus, ilgili kişiler yalnızca gerçek kişiler olabilirken, veri sorumlularının gerçek veya tüzel kişiler olmasının mümkün olduğudur.

Veri sorumlusu, esas itibarıyla, işleme faaliyetinin “neden” ve “nasıl” yapılacağı sorularının cevabını verecek kişidir. Amaç ile kastedilen, veri işleme faaliyetinin sonunda ne tür bir netice elde edilmek istendiğidir. Araç ise veri işleme faaliyetinin organizasyonel ve teknik boyutları; işleme faaliyetinin kapsamı; kişi ve veri kategorileri; üçüncü kişilerin erişim imkanları; verilerin saklanma süresi gibi hususları ifade eder. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında bizzat kendileri veri sorumlusudur. Kanunda, kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemiştir.

Veri İşleyen

Veri işleme kavramıyla bağlantılı bir diğer kavram ise, KVKK m. 3/1.ğ bendinde düzenlenmiş olan veri işleyen kavramıdır. Anılan hükümde “veri işleyen”, *“Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi...”* olarak tanımlanmaktadır. Veri işleyen, veri sorumlusunun kişisel veri işleme sözleşmesi yapmak suretiyle yetkilendirdiği ayrı bir gerçek veya tüzel kişidir. Kişisel verileri kendisine verilen talimatlar çerçevesinde işler. Veri işleyenlerin faaliyetleri daha çok veri işlemenin teknik kısımları ile sınırlıdır.

Burada şu hususa dikkat edilmesi gerekir: Herhangi bir gerçek veya tüzel kişi aynı zamanda hem veri sorumlusu, hem de veri işleyen olabilir. Örneğin, bir muhasebe şirketi kendi personeliyle ilgili tuttuğu verilere ilişkin olarak veri sorumlusu sayılırken, müşterisi olan şirketlere ilişkin tuttuğu veriler bakımından ise veri işleyen olarak kabul edilecektir.

Açık Rıza

KVKK m. 3/1.a hükmüne göre “açık rıza”, *“Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı...”* ifade etmektedir.

Kişisel verilerin, ilgili kişinin açık rızasına dayalı olarak işlendiği hallerde, rızanın en geç işleme anında verilmesi gerekmektedir. Rıza, yazılı, sözlü veya elektronik ortamda verilebileceği gibi ilgili kişi,

rızasını her zaman geri alabilir. Bu durumda, açık rızaya dayalı veri işleme faaliyetine ileriye etkili olarak son verilmelidir. Ayrıca belirtmek gerekir ki, rızanın varlığını veri işleyen ispatlaması gerekmektedir.

Açık rızası alınmadan önce ilgili kişinin veri işleme faaliyeti hakkında bilgilendirilmesi gereklidir. Bunun amacı, ilgili kişinin haklarını etkin biçimde kullanabilmesi ve şeffaflığın sağlanmasıdır. Aydınlatma yapılmaması halinde ilgili kişilerin neye rıza verdiklerini bilmeleri mümkün olmayacağından rıza da geçersiz olacaktır.

Hukukumuzda battaniye rızalar geçersiz kabul edilmektedir. Daha açık bir ifadeyle, rıza genel bir onay şeklinde değil, belirli verilerin yalnızca belirli amaçlarla işlenmesine ilişkin olmalıdır. Kişisel Verileri Koruma Kurulu, 2020 yılında verdiği bir kararda, belirli bir konu ile sınırlandırılmayan ve ilgili işleme sınırlı olmayan genel nitelikteki açık rızaların “battaniye rızalar” olarak kabul edildiğini ve hukuken geçersiz sayıldığını belirtmiştir. (Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulu’nun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti)

Burada dikkat edilmesi gereken bir diğer nokta da, rızanın “opt-in” şeklinde verilmesi gerekliliğidir. Bu çerçevede, kişinin sessiz kalması, örneğin bir web sitesinden ayrılmayarak kalmaya devam etmesi açık rıza kapsamında değerlendirilmemektedir. Kişisel Verileri Koruma Kurulu da vermiş olduğu bir kararında “... yalnızca amazon hizmetlerinin kullanılması suretiyle gizlilik bildiriminde yer alan hususların kabul edilmiş olduğu varsayımının Kanuna uygun bir açık rıza olarak nitelendirilemeyeceği...”ni belirtmiştir (Amazon Turkey Perakende Hizmetleri Limited Şirketi hakkındaki başvuru ile ilgili Kişisel Verileri Koruma Kurulu’nun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti).

Geçerli bir açık rızadan söz edilebilmesi için rızanın özgür irade ile verilmesi gerekir. Bu çerçevede, eğer veri sorumlusu ve ilgili kişi arasında ekonomik dengesizlik veya bağımlılık ilişkisi bulunuyor ise, özgür iradede söz edilemeyebilir. İşçi-işveren ilişkisinin söz konusu olduğu durumlarda, veri sorumlusunun tekel konumunda olması halinde ya da ilgili kişinin söz konusu hizmet ya da ürüne muhtaç olması hallerinde durum böyledir.

Kişisel Verilerin Korunması Hukukuna Egemen Olan Başlıca İlkeler

KVKK m. 4/2’ye göre, kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

- Hukuka ve dürüstlük kurallarına uygun olma.
- Doğru ve gerektiğinde güncel olma.
- Belirli, açık ve meşru amaçlar için işlenme.
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

“Hukuka ve dürüstlük kuralına uygunluk ilkesi”ne göre, veri işleyen, kanuna, diğer hukuk kurallarına ve dürüstlük kuralına uygun hareket etmelidir. Dürüstlük kuralına uygun olma; veriler işlenirken, ilgili kişilerin çıkarlarının ve makul beklentilerinin dikkate alınmasını gerektirmektedir.

Kişisel Verileri Koruma Kurulu vermiş olduğu bir kararında, bir varlık yönetim şirketinin, ilgili kişinin telefon numarasına aynı içerikteki mesajları birden fazla kez göndermesinin veri sahibinin sahip olduğu hakkı kötüye kullanması olarak nitelendirmiştir (Bir varlık yönetim şirketinin ilgili kişiye aynı konu ile ilgili birden çok mesaj gönderimine ilişkin Kişisel Verileri Koruma Kurulu’nun 31/05/2019 Tarihli ve 2019/159 Sayılı Karar Özeti)

Dürüstlük kuralından, “şeffaflık ilkesi” doğar. Buna göre, ilgili kişi, verilerinin kim tarafından ve hangi amaçlarla işlendiğini öğrenebilmelidir. Bilgi; anlaşılır, somut şekilde ve basit bir dille paylaşılmalıdır.

“Doğruluk ilkesi” çerçevesinde, doğru olmayan kişisel veriler gecikmeden silinmeli veya düzeltilmelidir. Nitekim, verilerin doğru olmaması, ilgili kişilerin temel hak ve özgürlüklerine, ekonomik çıkarlarına ve manevi bütünlüğüne zarar verebilir. Örneğin, doğru olmayan adres verisi nedeniyle ilgili kişiye yapılan tebligatlar ulaşmayabilir.

Ayrıca, veri sorumlusu, eğer verilere dayalı olarak ilgili kişiyle ilgili bir sonuç ortaya koyuyor ise, veriler güncel olmalıdır. Örneğin, ilgili kişiler tarafından sağlanan verilere dayalı olarak kredi verme işlemleri gerçekleştiriliyor ise veriler güncel olmalıdır. Kimi hallerde ise, özellikle *delillerin muhafazası amacıyla verilerin* güncellenmemesi zorunlu olabilir.

“Amaca bağlılık ilkesi” çerçevesinde belirli bir amaçla toplanan veriler, farklı bir amaçla işlenemez. Aksi halde, işleme öncesinde bilgilendirme ve açık rıza alma zorunluluğu anlamını yitirir.

“Sınırlı süre saklanma ilkesi”ne göre, eğer mevzuatta verilerin ne kadar süreyle saklanacağı belirtilmemiş ise, kişisel veriler, işlenme amaçlarının gerektirdiğinden daha uzun süre saklanmamalıdır.

Kişisel verileri koruma hukukunun en önemli ilkelerinden biri “veri minimizasyonu (ölçülülük) ilkesi”dir. Bu ilkeye göre, veri sorumlusu, amacına ulaşmak için gerekenden fazla veri işlememelidir. Söz konusu amaca ulaşmak için verilerin işlenmesi şart değilse, veri işlememe yoluna başvurulmalıdır.

Bu konuda Kişisel Verileri Koruma Kurulu’nun vermiş olduğu bir kararda şu ifadeler yer almaktadır: *“Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep etmesi, kimlik doğrulama işlemi için daha az verinin işlenmesinin mümkün olduğundan hareketle veri sorumlusunun somut olayda işlediği kimlik görüntüsünün işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesine aykırıdır.”* (Bir havayolu taşımacılık şirketinin (veri sorumlusu) sunduğu sadakat programını kullanan ilgili kişinin kullanıcı adı ve parola bilgilerini değiştirme talebi karşısında ilgili kişiden arkalı önlü kimlik görüntüsü talep eden veri sorumlusu” hakkında Kişisel Verileri Koruma Kurulu’nun 01.10.2019 Tarihli ve 2019/294 sayılı Karar Özeti)

“Veri güvenliği (bütünlük ve gizlilik) ilkesi”, kişisel verilerin korunması sadece hukuki yöntemlerle sınırlı olmayıp, teknolojik tedbirler alınmasını da gerektirir. Burada “gerekli önlemler”in neler olduğu, işlenen verinin niteliği ve temel hak ve özgürlüklere gelebilecek muhtemel müdahale dikkate alınarak belirlenir. Amaç, bu müdahalenin asgari seviyeye indirilmesidir.

Kişisel Verilerin İşlenme Şartları

Kişisel verilerin işlenmesi hukukuna egemen olan en temel ilkelerden bir tanesi, kişisel verilerin işlenmesinin, kural olarak yasak olması ilkesidir. Bununla birlikte, bir işleme sebebi yani hukuka uygunluk sebebi var ise, kişisel veriler işlenebilir. Nitekim, temel hak ve özgürlükler (kişisel verilerin korunmasını talep etme hakkı) başka hukuki menfaatlerle sınırlandırılabilir. KVKK m. 5’te kişisel verilerin ilgili kişilerin açık rızası olmadan işlenemeyeceği açıkça belirlendikten sonra, kanunda sayılan bazı hallerde, ilgili kişinin açık rızası olmadan da kişisel verilerin işlenmesinin mümkün olacağı belirtilmiştir.

Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

(a) Kanunlarda açıkça öngörülmesi.

(b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

(c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

- (ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
- (d) İlgili kişinin kendisi tarafından alenileştirilmiş olması.
- (e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
- (f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.”

Örneğin, çalışana ait özlük bilgilerinin tutulması İş Kanunu gereği zorunlu olduğundan ilgili kişilerin açık rızasının alınması gerekmez. Keza, kaçırılan veya kayıp kişinin telefonu üzerinden konum bilgisinin belirlenmesi için o kişiden rıza alınması da fiili imkansızlık gereği söz konusu olmayacaktır.

Bu noktada dikkat edilmesi gereken husus, açık rıza ve diğer hukuka uygunluk sebepleri arasında hiyerarşik bir ilişki bulunmadığıdır. Ayrıca, kişisel veri işleme faaliyetinin amacında birden fazla sayıda kişisel veri işleme şartı bulunabilir. Örneğin, maaş bordrosu düzenlemek amacıyla çalışanların kişisel verilerinin işlenmesinin hukuki dayanağı, kişisel veri işleme şartlarından sözleşmenin ifası ve veri sorumlusunun hukuki yükümlülüğünün yerine getirilmesidir.

Özel nitelikli kişisel verilerin işlenmesi bakımından kanun koyucu daha katı bir yaklaşım benimsemiştir. KVKK m. 6’ya göre, özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır. Ancak “...sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. 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.”

İlgili Kişinin Hakları

Veri sorumlularına ve veri işleyenlere birtakım yükümlülükler yükleyen Kanun, ilgili kişilere de bir dizi haklar tanımıştır. Bu çerçevede, KVKK m. 11’e göre ilgili kişiler veri sorumlularına başvurarak kendileriyle ilgili olarak aşağıdaki hakları kullanabilirler:

- “(a) Kişisel veri işlenip işlenmediğini öğrenme,
 - (b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
 - (c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
 - (ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,
 - (d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme,
 - (e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,
 - (f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
 - (g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
 - (ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme,
- haklarına sahiptir.”

İlgili Kişilerin Haklarının Korunması

İlgili kişilerin, bu haklarını kullanabilmeleri için öncelikle veri sorumlularına başvurmaları gerekmektedir (KVKK m. 13). Bu başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya süresinde başvuruya cevap verilmemesi hâllerinde; ilgili kişi, veri sorumlusunun cevabını öğrendiği tarihten itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gün içinde Kurula şikâyetle bulunabilir (KVKK m. 14/1). O halde, ilgili kişilerin Kişisel Verileri Koruma Kurulu'na şikâyetle bulunmadan önce veri sorumlularına başvurmaları usulü bir zorunluluktur. Bununla birlikte, Kurul'un bir ihlal iddiasını öğrenmesi üzerine resen inceleme yapması da mümkündür. Yapılan inceleme neticesinde, kişisel verileri hukuka aykırı olarak işlediği tespit edilen kişilere idari yaptırım uygulanır. Ayrıca bu kişiler yönünden Türk Ceza Kanunu m. 135-140 hükümleri uyarınca cezai yaptırım uygulanması da söz konusu olur. Son olarak, kişisel verileri hukuka aykırı olarak işlendiği için maddi ve manevi zarara uğrayan kişilerin Türk Medeni Kanunu hükümleri çerçevesinde tazminat talepleri saklıdır.

BÖLÜM ÖZETİ

Dijital teknolojilerdeki gelişmelerle birlikte veri, artan oranda önem kazanmış ve kişisel verilerin korunması daha da güncel bir sorun hâline gelmiştir. Endüstri 4.0'ın temel bileşenlerinden biri olarak kabul edilen yapay zekâ, nesnelerin interneti (internet of things), büyük veri (Big Data) ve blokzinciri uygulamaları gibi teknolojiler, kişilere veya makinelere ait verilerin toplanmasına ve kaydedilmesine dayanmaktadır. Bu nedenle içinde bulunduğumuz çağda veri “yeni petrol” olarak nitelendirilmektedir.

Kişisel verilerin korunması meselesinin merkezinde çatışan iki temel menfaat yer almaktadır. Bir taraftan, bilginin serbest dolaşımı sağlanmak istenmektedir; çünkü inovasyonun teşviki, teknolojik gelişim ve ilerleme için bu dolaşım değerlidir. Diğer taraftan ise, ilgili kişilerin hem devlet hem de özel teşebbüsler karşısında korunması gerekmektedir. Bilgi toplumunda kişisel veriler korunmazsa birey, devletler ve özel teşebbüsler karşısında zarar görme riski altına girer. Ayrıca, kişisel verilerin korunması temel hak ve özgürlüklerle de yakından bağlantılıdır. Özellikle yapay zekâ teknolojilerindeki gelişmelerle birlikte karar veren algoritmalar yaygınlaşmış ve veri diktatörlüğü gündeme gelmiştir. İşte kişisel verilerin korunması hukuku, bu menfaat çatışmasını çözmeye çalışmaktadır.

Kişisel verilerin, bireyin kişilik hakkıyla ilgili olduğu kabul edilmektedir. Kişilik hakkının çeşitli görünüm türleri bulunmakta olup bunlar sınırlı sayıda değildir. Bu çerçevede, bireyin kişisel verileri üzerindeki hakkı da tıpkı vücut bütünlüğü, özel yaşamı ve şeref ile haysiyeti gibi kişilik hakkının bir parçasıdır. Türk Hukuku'nda kişisel verilerin korunması, temel bir hak olarak Anayasa'da düzenlenmiştir. Ayrıca, Avrupa Birliği'ndeki gelişmelere paralel olarak Türkiye'de 2016 yılında Kişisel Verilerin Korunması Kanunu yürürlüğe girmiş ve Kişisel Verileri Koruma Kurumu kurulmuştur. Hukukumuzda kişisel verilerin işlenmesinin kural olarak yasak olduğu esası geçerlidir. Ancak bu veriler başta açık rıza olmak üzere, Kişisel Verilerin Korunması Kanunu'nda sayılan veri işleme şartlarından birinin bulunması durumunda ve kişisel verilerin korunması hukukuna egemen olan ilkelere uyularak işlenebilir.

Veri sorumlularına ve veri işleyenlere birtakım yükümlülükler yükleyen Kanun, ilgili kişilere de bir dizi hak tanımıştır. Kanuna aykırı veri işleme faaliyeti gerçekleştirilmesi durumunda, kişisel verileri hukuka aykırı olarak işlediği tespit edilen kişilere idari yaptırım uygulanır. Ayrıca, bu kişiler yönünden Türk Ceza Kanunu'nun 135-140. maddeleri uyarınca cezai yaptırım uygulanması da söz konusu olabilir. Son olarak, kişisel verileri hukuka aykırı olarak işlendiği için maddi ve manevi zarara uğrayan kişilerin Türk Medeni Kanunu hükümleri çerçevesinde tazminat talepleri saklıdır.

GÖZDEN GEÇİRELİM

1. Türk Hukukunda gerçek kişilerin kişisel verileri üzerindeki hak _____ hakkıdır.
2. Kişisel verileri işlenen, kimliği belirli veya belirlenebilir gerçek kişiler _____ olarak isimlendirilir.
3. Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesine _____ adı verilir.
4. Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiye _____ adı verilir.
5. Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiye _____ adı verilir.
6. Belirli veri türlerinin belirli amaçlarla işlenmesini konu almayıp genel bir onay şeklinde verilen rızalar _____ olarak isimlendirilmekte olup geçersizdir.
7. _____ 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.
8. _____ ilkesi'ne göre, eğer mevzuatta verilerin ne kadar süreyle saklanacağı belirtilmemiş ise, kişisel veriler, işlenme amaçlarının gerektirdiğinden daha uzun süre saklanmamalıdır.
9. _____ ilkesi'ne göre, veri sorumlusu, amacına ulaşmak için gerekenden fazla veri işlememeli, söz konusu amaca ulaşmak için verilerin işlenmesi şart değilse, veri işlememe yoluna başvurulmalıdır.
10. İlgili kişilerin, kişisel verilerinin hukuka aykırı olarak işlendiği gerekçesiyle Kişisel Verileri Koruma Kurulu'na şikayette bulunmadan önce _____'na başvurmaları usulü bir zorunluluktur.

CEVAP ANAHTARI

1. kişilik	6. battaniye rızalar
2. ilgili kişi	7. Sağlık ve cinsel hayata
3. anonim hale getirme	8. Sınırlı süre saklanma
4. veri sorumlusu	9. Veri minimizasyonu – Ölçülülük
5. veri işleyen	10. veri sorumluları

SÖZLÜK

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

İlgili kişi: Kişisel verisi işlenen gerçek kişidir.

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

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 işlemidir.

Özel nitelikli kişisel veri: 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 verileridir.

Psödonim (takma adlı) veri: İlave bilgiler olmadan, belli bir gerçek kişiyle eşleştirilemeyen veridir.

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişidir.

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir.

KAYNAKÇA

Aksoy, Hüseyin Can: Medeni Hukuk ve Özellikle Kişilik Hakkın Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara 2010.

Çekin, Mesut Serdar: AB Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması, 3. Bası, On İki Levha Yayıncılık, İstanbul 2020.

Develioğlu, Hüseyin Murat: 6698 sayılı KVKK ile Karşılaştırmalı Olarak AB GVKT Uyarınca Kişisel Verilerin Korunması H., On İki Levha Yayıncılık, İstanbul 2017.

Dülger, Murat Volkan: Kişisel Verilerin Korunması Hukuku, 3. Bası, Hukuk Akademisi, İstanbul 2020.

Küzeci, Elif: Kişisel Verilerin Korunması, 4. Bası, On İki Levha Yayıncılık, İstanbul 2020.

ÜNİTE 4

ELEKTRONİK İMZA VE
ELEKTRONİK İMZA KANUNU

Arş. Gör. Mustafa Can DAĞLI

ANAHTAR KAVRAMLAR

Sözleşmelerde şekil

İmza

Dijital imza

Hash değeri

Elektronik sertifika hizmet sağlayıcısı



ELEKTRONİK İMZA VE ELEKTRONİK İMZA KANUNU

ÖĞRENME HEDEFLERİ

-  1 Sözleşmelerde şekil konusunu öğrenmek.
-  2 Elektronik imza ve dijital imzanın ne olduğunu, farklarının ne olduğunu öğrenmek.
-  3 Dijital imzanın teknik yapısını öğrenmek.
-  4 Güvenli elektronik imzaya bağlanan hukuki sonuçların ne olduğunu öğrenmek.
-  5 Elektronik sertifika hizmet sağlayıcısının rolünü, nasıl faaliyete başladığını, temel yükümlülüklerinin ne olduğunu öğrenmek.

GİRİŞ

Sözleşmelerde şekil, genel olarak tarafları düşünmeye sevk etmesi, sözleşmeye açıklık ve kesinlik sağlaması, ispat ve güvenlik sağlaması, sözleşmenin yorumunu kolaylaştırması açısından faydalı görülmektedir. Ancak hukuki işlemlerin büyük çoğunluğunun, özellikle geçerlilik şartı olarak şekle bağlı olması birçok hukuki işlemin geçersizlik yaptırımıyla karşılaşmasına yol açacaktır. Bir diğer yandan, elektronik ortamda yer alan verilere dayanan hukuki işlemlerin, yapıları gereği ağır şekil koşullarına uyması mümkün değildir. Bu hukuki işlemlerin, özellikle internet üzerinden akdedilen sözleşmelerin katı şekil koşullarına tabi tutulması halinde geçersizlik yaptırımıyla karşılaşma riski doğmaktadır. Bu sebeple ülkemizde ve diğer ülkelerde güvenli elektronik imza düzenlemeleri yapılmış ve güvenli elektronik imzaya belirli hukuki sonuçlar bağlanmıştır.

İmza, kişileri birbirinden ayırmayı, kişinin kimliğini tespit etmeyi mümkün kılar. Kişi, metni imzalayarak irade beyanını ortaya koyar. Böylece, kişinin metinde yer alan hukuki sonucu benimsediği kabul edilir. Elektronik belgelerin metin ve el yazısı unsurlarını içermemesi bu belgelerin nasıl imzalanacağı sorununu doğurmuştur. Bu soruna çözüm olarak dijital imza (güvenli elektronik imza) bulunmuştur. Güvenli elektronik imza da kişinin kimliğini tespit etmeyi mümkün kılar ve elektronik belgenin imzalayan tarafından yazıldığını (bağlayıcı olduğunu), belgenin değişikliğe uğramadığını ve belgenin varlığını doğrulamayı sağlar. Güvenli elektronik imzanın, geleneksel imza ile benzer fonksiyonları yerine getirmesi nedeniyle, güvenli elektronik imzaya önemli hukuki sonuçlar bağlanmıştır.

Bu bölümde genel olarak şekil kavramı, el ile atılan imza, el ile atılan imzaya bağlanan hukuki sonuçlar, elektronik imza, dijital imza, dijital imzanın teknik yapısı, güvenli elektronik imzaya bağlanan hukuki sonuçlar ve elektronik imza ile ilgili belirli düzenlemeler incelenecektir.

Sözleşme Nedir

Borç kavramı doktrinde, dar anlamda borç ve geniş anlamda borç olmak üzere ikiye ayrılarak incelenmektedir. Dar anlamda borç “*alacaklının borçludan istemeye yetkili olduğu, borçlunun da yerine getirmek zorunda olduğu tek bir edimi, yani bir tek alacak veya borcu...*” ifade edecek biçimde tanımlanmaktadır. Geniş anlamda borç ise alacaklı ve borçlu arasında farklı borçlar doğurabilen ve bu borçların bütünü oluşturarak hukuki ilişki ya da borç ilişkisi olarak tanımlanmaktadır.

Borç ilişkileri hukuki işlemde veya doğrudan kanundan kaynaklanabilir. İşte sözleşmeler de borç ilişkisi kuran hukuki işlemlerdir. 6098 sayılı Türk Borçlar Kanunu’nun (RG. 04.02.2011, S. 27836, TBK) 1. maddesinin 1. fıkrasında, sözleşmelerin tarafların karşılıklı ve birbirine uygun irade açıklamalarıyla kurulduğu belirtilmiştir. Bir başka ifadeyle sözleşme, karşılıklı ve birbirine uygun irade açıklamalarıyla kurulan hukuki ilişkidir.

Sözleşmelerde Şekil

İradenin dış dünyaya söz, yazı, işaret gibi bir biçimde aktarılması şekil olarak adlandırılır. Her hukuki işlem ve her irade beyanı belirli bir şekilde yapılır. Örneğin, bir sözleşmenin imzalanması sözleşmenin şekli ile ilgili bir husustur.

Hukuk sistemimizde kural olarak şekil özgürlüğü geçerlidir. Bu kural TBK m. 12/1’de “*Sözleşmelerin geçerliliği, kanunda aksi öngörülmedikçe, hiçbir şekle bağlı değildir.*” şeklinde düzenlenmiştir. Şekle bağlı olmamak ile kastedilen sözleşmelerin belirli bir şekilde yapılmasının zorunlu olmadığı, yani şekil özgürlüğüdür.



DİKKAT EDELİM

Bunlara Dikkat Edelim: Sözleşmelerde şekil amaca göre, geçerlilik şekli ve ispat şekli olmak üzere ikiye ayrılmaktadır. Geçerlilik şekli, tarafların şekil şartına uymamaları halinde hukuki işlemin geçersiz olduğu şekildir. Bir hukuki işlemin ispatı için aranan şekil ise ispat şeklidir.

Geçerlilik Şekli

TBK m. 12/2’ye göre “*Kanunda sözleşmeler için öngörülen şekil, kural olarak geçerlilik şeklidir. Öngörülen şekle uyulmaksızın kurulan sözleşmeler hüküm doğurmaz.*” Söz konusu düzenlemeye göre bir sözleşme, kanun ile belirli bir şekle tabi tutulmuş ise bu şekil geçerlilik şekli olacak ve bu şekle uyulmaması halinde sözleşme hüküm doğurmayacak, yani geçersiz olacaktır. Kanunda düzenlenen şekil şartı yasal şekil ya da kanuni şekil olarak da adlandırılmaktadır.

Şekil, geçerlilik koşulu olarak yalnızca kanunda öngörülmemektedir. Taraflar kendi özgür iradeleri doğrultusunda kanunda şekle bağlanmamış bir sözleşmeyi belirli bir şekilde yapmak üzere anlaşabilirler. Bu durumda iradi şekil söz konusu olmaktadır. İradi şekilde, tarafların kanunda şekle bağlanmamış bir sözleşmeyi belirli bir şekilde yapmak üzere anlaşmaları halinde, belirlenen şekilde yapılmayan sözleşme tarafları bağlamaz (TBK m. 17/1). Ancak, taraflar geçerlilik koşulu yerine ispat koşulu olarak da iradi şekil kararlaştırabilirler. Taraflar, herhangi bir belirleme yapmaksızın yalnızca yazılı şekil kararlaştırırlarsa, yasal yazılı şekle, yani adi yazılı şekle ilişkin hükümler uygulanacaktır (TBK m. 17/2).

Tekrar etmek gerekir ki geçerlilik şekline uyulmamasının yaptırımı sözleşmenin geçersiz olmasıdır.

İspat Şekli

Daha önce belirtildiği gibi ispat şekli bir hukuki işlemin varlığının ispatı için gerekli olan şekildir. Mahkemede görülmekte olan bir davada ispat ise taraf taleplerinin dayandığı olay ve olguların doğru olup olmadığını konusunda hâkimi ikna etme faaliyeti olarak tanımlanmaktadır. İspat şekli kanundan veya taraf iradelerinden kaynaklı olabilir. Taraflar kendi özgür iradeleri doğrultusunda belirli bir ispat şekli belirleyebilirler. Bu durumda da iradi şekil söz konusu olur. İspat, medeni usul hukuku ile ilgili bir konu olduğu için ispata ilişkin kurallar 6100 sayılı Hukuk Muhakemeleri Kanunu'nda (RG. 04.02.2011, S. 27836, HMK) düzenlenmiştir.

HMK'da ispat şekli ile ilgili iki ana kural bulunmaktadır. Birinci kurala göre, HMK'da senetle ispat zorunluluğu başlığı ile düzenlenen m. 200/1 uyarınca, yapıldıkları tarihte miktar veya değeri belirli bir tutarı aşan hukuki işlemler kural olarak yalnızca senet ile ispat edilebilir. Burada senetle ispat zorunluluğu ile kastedilen kesin delille ispat zorunluluğudur. Bu hüküm, bahsedilen hukuki işlemlerde yazılı şekli zorunlu tutmaktadır. Ancak bu kuralın istisnaları bulunmaktadır. İkinci kural ise, HMK m. 201 gereğince; senet ile ileri sürülen her çeşit iddiaya karşı ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemlerin tanıkla ispatının yasak olmasıdır. Bir diğer ifadeyle senede karşı ancak senetle veya diğer kesin delillerle ispat mümkündür. Bu kuralın da belirli istisnaları bulunmaktadır.

İspat şekline uyulmamasının sonucu hukuki işlemin varlığının veya doğruluğunun ispat edilmiş olmasıdır. İspat şekline uyulmaması sözleşmenin geçersiz olmasına neden olmaz. Geçerli olarak kurulan ancak ispatlanamayan bir hak veya hukuki işlem gerçekten var olsa bile mahkeme tarafından dikkate alınmayacaktır. Bu nedenle ispat şekli son derece önemlidir.

Şeklin Türleri

Şekil, yapılış biçimine göre; “sözlü şekil”, “adi yazılı şekil”, “nitelikli yazılı şekil” ve “resmi şekil” olarak dörde ayrılarak incelenmektedir.

Sözlü şekil, tarafların iradelerini sözlü olarak dış dünyaya aktarmalarıdır. Şekil özgürlüğü gereği kural olarak, sözleşmeler -kanunda veya taraflarca yapılan sözleşmede aksi kararlaştırılmadıkça- sözlü şekil ile geçerli biçimde kurulabilmektedir.

Adi yazılı şekil, beyan sahibinin, şekle bağlı irade beyanının içeriğini yazıyla belgeleyip imzalanması şeklinde tanımlanmaktadır. Adi yazılı şeklin metin ve imza olmak üzere iki unsuru bulunmaktadır. Adi yazılı şekilde yalnızca imzanın el yazısı ile olması gerekir. Metin, el yazısı, daktilo, yazıcı vb. araçlarla

oluşturulan, beyanda bulunan kişinin iradesinin yer aldığı somut belgedir. İmza ise belirli bir kişinin belgeyi yazdığını veya onayladığını belirlemek için kullanılan işarettir.

Nitelikli yazılı şekil, adi yazılı şekle göre ilave unsurların yer aldığı şekil türüdür. Örneğin, 4721 sayılı Türk Medeni Kanunu'nun (RG. 08.12.2001, S. 24607, TMK) 538. maddesinin birinci fıkrası uyarınca el yazılı vasiyetname nitelikli yazılı şekle tabi tutulmuştur. Hüküm; *"El yazılı vasiyetnamenin yapıldığı yıl, ay ve gün gösterilerek başından sonuna kadar miras bırakanın el yazısıyla yazılmış ve imzalanmış olması zorunludur."* şeklinde düzenlenmiştir. Görüldüğü üzere, adi yazılı şekilde metnin nasıl yazıldığı önem arz etmezken, el yazılı vasiyetnamede (nitelikli yazılı şekil) metnin başından sonuna kadar belirli unsurlarla birlikte el yazısıyla yazılmış olması şartı aranmıştır. Benzer şekilde, kefalet sözleşmesi de TBK m. 583/1'deki *"Kefalet sözleşmesi, yazılı şekilde yapılmadıkça ve kefilin sorumlu olacağı azamî miktar ile kefalet tarihi belirtilmedikçe geçerli olmaz. Kefilin, sorumlu olduğu azamî miktarı, kefalet tarihini ve müteselsil kefil olması durumunda, bu sıfatla veya bu anlama gelen herhangi bir ifadeyle yükümlülük altına girdiğini kefalet sözleşmesinde kendi el yazısıyla belirtmesi şarttır."* hükmüyle nitelikli yazılı şekle tabi tutulmuştur.

Resmi şekil, bazı hukuki işlemlerin resmi makamların huzurunda ve katılımıyla yapılmasıdır. Resmi şekilde, hukuki işlem veya sözleşme kanunda düzenlenen usul ve esaslara uyularak resmi senet düzenleme yetkisi bulunan kişi tarafından yapılır. Resmi senet düzenlemeye yetkili makamlar genel olarak, sulh hakimliği, noter ve tapu sicil müdürlükleridir. Örneğin, TBK m. 237/1 hükmü *"Taşınmaz satışının geçerli olabilmesi için, sözleşmenin resmî şekilde düzenlenmesi şarttır."* şeklinde düzenlenmiştir. Bu hüküm uyarınca, taşınmaz satışının geçerlilik koşulu resmi şekle bağlanmıştır.

İmza Nedir?

Daha önce belirtildiği üzere imza, bir kişinin bir belgeyi yazdığını veya onayladığını belirlemek için kullanılan işarettir. İmza, kişinin kimliğini tespit etmeye, onu diğer kişilerden ayırmaya yarar. İmza, genellikle ad ve soyadı içerecek biçimde atılır. 2525 sayılı Soyadı Kanunu (RG. 02.07.1934, S. 2741) m. 2'ye göre imzada, öz adın önde, soy adının sonda kullanılacağı belirtilmiştir. Ancak, bu hüküm emredici olmayıp, bir işaret veya başka sözcüklerden oluşan yazılar da imza olarak kabul edilebilecektir. Keza imzanın kısaltılmış hali olan paraflar da imza olarak nitelendirilmektedir. İmzanın her zaman aynı şekilde atılması şart değildir.

TBK m. 14/1 hükmü *"Yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunması zorunludur."* şeklinde düzenlenmiştir. Bu hüküm uyarınca, bir sözleşme ile borç altına giren tarafın sözleşmede imzasının bulunması gerekmektedir. İki tarafa borç yükleyen sözleşmelerde, her iki taraf da borç altına girdiği için iki tarafın da imzasının bulunması gerekmektedir.

Genel kural TBK m. 15/1 gereğince, borç altına giren kişinin el yazısı ile imza atması zorunluluğudur. Bu hükümler birlikte değerlendirildiğinde, adi yazılı şekle bağlı bir sözleşmede, borç altına giren kişinin el yazısı ile atılmış imzasının bulunması zorunludur.

TBK m. 14/2; *"Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer."* hükmünü ihtiva etmektedir. Bu maddede sayılan araçlar adi yazılı şekil şartını yerine getirmektedir. Ancak, bunun için TBK dışındaki bir kanunda bu hükmün aksine bir düzenlemenin yer almaması gerekmektedir.

Güvenli elektronik imza ile gönderilip saklanan metinler konumuz açısından önem arz etmek-

tedir. Kanun, güvenli elektronik imza ile gönderilip saklanan metinlerin adi yazılı şekil şartını yerine getirdiğini kabul etmiştir.

İmza ile ilgili genel kuralın el yazısı ile imza atmak olduğunu belirtmiştik. Bu kuralın TBK m. 15 ve 16'da öngörülmüş üç istisnası bulunmaktadır. Bu istisnalar; bir araçla imza atmak, görme engellilerin imzası ve imza atamayanların imza yerine geçen işaretler kullanması olarak sayılabilir.

Bir araçla imza atmak ancak örf ve adetçe kabul edilen hallerde ve özellikle çok sayıda çıkarılan kıymetli evrakın imzalanmasında geçerli kabul edilmiştir (TBK m. 15/2). Ancak 6102 sayılı Türk Ticaret Kanunu'nun (RG. 14.02.2011, S. 27846, TTK) 756. maddesinin ikinci fıkrası ve 780. maddesi uyarınca bono, poliçe ve çeklerde imzaların el ile atılması zorunludur. Bu senetlerde herhangi bir mekanik araç (örneğin, damga) ile atılacak imza kullanılamaz.

Görme engellilerin imzası ile ilgili TTK m. 15/3'te *"Görme engellilerin talepleri halinde imzalarında şahit aranır. Aksi takdirde görme engellilerin imzalarını el yazısı ile atmaları yeterlidir."* düzenlemesi yer almaktadır. Ayrıca, 1512 sayılı Noterlik Kanunu (RG. 18.01.1972, S. 14090, NK) m. 73 uyarınca noterin; ilgilinin işitme, konuşma veya görme engelli olduğunu anlaması halinde ilgilinin isteğine bağlı olarak işlemlerin iki tanık huzurunda gerçekleştirileceği hüküm altına alınmıştır.

Herhangi bir sebeple imza atamayan kişiler (örneğin, okuma yazma bilmeyenler, sağlık durumları nedeniyle imza atamayanlar) ise, TBK m. 16/1 uyarınca, imza yerine usulünce onaylı parmak izi, el ile yapılmış bir işaret veya mühür kullanabileceklerdir. Ancak, bu hüküm kambyo senetleri için uygulanmamaktadır (TBK m. 16/2). Söz konusu parmak izini, el işaretini veya mührü onaylamaya yetkili makam noterdir. Keza NK m. 75'te *"İlgililerle tanık, tercüman ve bilirkşi imza atamadıkları ve imza yerine geçen bir el işareti kullanmadıkları takdirde, varsa mühür, yoksa sol elinin baş parmağı, bu da yoksa diğer parmaklarından biri bastırılır ve hangi parmağın bastırıldığı yazılır."* hükmü yer almaktadır.

İmzaya Bağlanan Hukuki Sonuçlar

Bir kişi, metne imza atarak irade beyanını açıklar. İmza aracılığıyla hukuki işlemi gerçekleştiren kişinin kimliğinin tespit edilmesi sağlanır ve metinde yer alan ifadelerin imzalayan tarafından kabul edildiği varsayılır. Bir diğer ifadeyle, bir kişi metne imza attığında, kişinin metinde yer alan hukuki sonucu kabul ettiği anlaşılır.

HATIRLATMA

Daha önce belirtildiği üzere, TBK m. 14/1 uyarınca, borç altına giren kişinin sözleşmeyi imzalaması ile yazılı şekil şartı yerine getirilmiş olur. Bir diğer ifadeyle imza, geçerlilik koşulu olarak şekle bağlı bir sözleşmede, geçerlilik koşulunu yerine getirmeyi sağlayan bir unsurdur. Yazılı şekilde yapılması öngörülen bir sözleşme imzalanmadan sözleşme geçerli olmaz.

HMK m. 199 hükmü; *“Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir.”* düzenlemesi ile “belge” kavramının kapsamına nelerin gireceğini belirtmiştir.

Medeni usul hukukunda “belge” ile “senet” kavramları birbirlerinden farklıdır. Senet, hâkimi bağlayıcı nitelikte olan kesin deliller arasında yer almakta iken, belge kesin deliller arasında sayılmamıştır. Senet, onu düzenleyen kişinin imzasını taşımaktadır. Belgede ise böyle bir zorunluluk yoktur. Hatta belgenin onu düzenleyen kişinin imzasını içermesi halinde ortada bir senet söz konusu olabilecektir. Kesin delillerin dayanak teşkil ettiği bir iddiayı hâkim doğru kabul etmek zorundadır. Sonuç olarak imza, diğer unsurlarıyla birlikte bir belgenin hukuken senet olarak değerlendirilebilmesini mümkün kılmaktadır. Bu da ispat açısından önemli sonuçlar doğurmaktadır.

HMK m. 205/1; *“Mahkeme huzurunda ikrar olunan veya mahkemeye inkâr edenden sadır olduğu kabul edilen adi senetler, aksi ispat edilmedikçe kesin delil sayılırlar.”* düzenlemesi ile adi senetlerin aksi ispat edilmedikçe kesin delil olarak nitelendirileceğini hükme bağlamıştır. Adi senet, resmi makamların katılımı olmaksızın düzenlenen senettir.

Elektronik İmza Kanunu

5070 sayılı Elektronik İmza Kanunu (RG. 23.01.2004, S. 25355, EİK) Avrupa Birliği’nin 1999/93 sayılı Yönergesine uygun olarak düzenlenerek 15.01.2004 tarihinde kabul edilmiş ve 23.07.2004 tarihinde yürürlüğe girmiştir. Kanun ile elektronik imzanın hukuki, teknik yönleri ve kullanım esasları düzenlenmiştir. EİK’ya dayanarak hazırlanan, elektronik imzanın hukuki ve teknik yönleri ile uygulamasına ilişkin usul ve esasları düzenleyen Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (RG. 06.01.2005, S. 25692) 06.01.2005 tarihinde yürürlüğe girmiştir.

Elektronik İmza Nedir?

“Elektronik imza” denilince akla “dijital imza” gelse de iki kavramı karıştırmamak gerekir. Elektronik imza, dijital imzayı da kapsamına alan, elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavram olarak değerlendirilmektedir. Elektronik imza yöntemlerine örnek olarak; biyometrik imza (parmak izi, retina taraması gibi), PIN (Personal Identification Number), dijital ortama aktarılmış el yazısı ve dijital imza verilebilir.

EİK m. 3/1/b’de elektronik imza; *“Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi”* ifade edecek biçimde düzenlenmiştir.

Dijital İmza Nedir?

Dijital imza, özel bir algoritma (hash fonksiyonu) kullanılarak oluşturulan ve gönderenin özel anahtarı ile şifrelenen bir ileti/mesaj özetidir. Dijital imza mesaja eklenerek alıcıya gönderilir. Alıcı, kendisine iletilen mesajdan yeniden bir mesaj özeti çıkarır ve gönderenin açık anahtarı ile dijital imza şifresini çözerek elde ettiği özet ile kendi hesapladığı özet karşılaştırır. Böylece gönderilen mesaj ile kendisine ulaşan mesajın aynı olduğu, değişikliğe uğramadığı (veri bütünlüğü), ilgili kişi tarafından gönderildiği (kimlik doğrulama) ve mesajın gönderildiği (gönderildiğini inkâr edememe-bağlayıcılık) doğrulanmış olur.

Dijital imzanın oluşturulması için kriptografi (şifreleme) kullanılır. Kriptografi, anlaşılabilir durumda bulunan verilerin anlaşılamayacak hale dönüştürülmesinde kullanılan matematik yöntemlerinin bütünüdür.

Şifreli mesaj anlamsız bir hale geldiği için, bu mesajı anlamlı bir hale dönüştürmek için şifrenin çözülmesi gerekir. Şifrenin çözülmesi için ise anahtar gereklidir. Şifreleme için birçok teknik bulunmakla birlikte, en sık kullanılan şifreleme yöntemleri; simetrik şifreleme yöntemi ve asimetrik şifreleme yöntemidir.

Simetrik şifreleme yönetiminde tek şifre (anahtar) hem mesajın şifrlenmesi hem de mesajın çözülmesinde kullanılır. Dolayısıyla, gönderici ve alıcı aynı anahtarı kullanır. Bunun için gönderici ve alıcının anahtarı bilmesi gerekir. İletinin güvenli bir biçimde gönderilebilmesi anahtarın gizliliğine bağlı olduğu için, simetrik şifreleme yöntemi yalnızca birbirine güvenen taraflarca kullanılması halinde ve internet ortamı dışarısında bir ortamda paylaşılması halinde güvenli bir biçimde kullanılabilir.

Asimetrik şifreleme yönteminde ise biri gizli (özel) ve biri açık(genel) olmak üzere iki anahtar bulunmaktadır. Gizli anahtara yalnızca kullanıcı erişebilir ve güvenlik gereği bu anahtarın kimse ile paylaşılması gerekir. Açık anahtar ise herkese açıktır ve güvenilir üçüncü kişiler tarafından ilan edilir. Dijital imzanın şifrlenmesi için asimetrik şifreleme yöntemi kullanılmaktadır.

Dijital İmzanın Teknik Yapısı

Asimetrik şifreleme yöntemi sayesinde mesajı gönderenin kimliği tespit edilebilecektir. Mesajın, özet fonksiyonu (hash) kullanılarak üretilen özet değeri (hash değeri) sayesinde ise mesajda herhangi bir değişiklik yapılmadığı tespit edilebilecektir.

Yukarıda bahsedildiği üzere, dijital imza asimetrik şifreleme yöntemi kullanılarak oluşturulur. Asimetrik şifreleme yönteminde açık ve gizli olmak üzere iki anahtar bulunur. Bu anahtarlar elektronik sertifika hizmet sağlayıcılar (ESHS) tarafından üretilir ve bir sertifika ile temsil edilirler. Bu sertifikada anahtar sahiplerinin kimlik bilgileri yer alır. Böylece dijital imzanın kimlik doğrulama fonksiyonu yerine getirilir.

Dijital imzanın taklit edilmesi zordur. Zira asimetrik şifreleme yönteminde kullanılan anahtar çifti uzun ve karmaşık bir yapıdadır. Ancak bu uzun şifrelerin kırılarak taklit edilmesi imkânsız değildir. Bu sebeple dijital imzanın tamamen güvenilir olduğu düşünülmemelidir.

Dijital imza ile imzalanmış mesajın alıcısı, imzanın dayandığı sertifikayı sağlayan sertifika hizmet sağlayıcısının sunucusunda sertifika bilgilerine ulaşabilir ve böylelikle göndericinin kimliğini tespit edebilir. Ayrıca göndericinin açık anahtarı da sertifika hizmet sağlayıcısının sunucusunda yayımlanacağı için, alıcı, mesajın göndericiden gelip gelmediğini kontrol edebilir.

Dijital imzada güvenlik sorunu gizli anahtarın saklanmasıyla ilgilidir. Zira gizli anahtara sahip olan kişi herkesin ulaşabildiği açık anahtara erişerek mesajın içeriğine ulaşabilecektir. Gizli anahtar dijital imzanın oluşturulmasına, açık anahtar dijital imzanın doğrulanmasına imkân vermektedir.

Gizli anahtar kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir. Gizli anahtar yalnızca kullanıcıya tahsis edildiği için bu chip kartın yetkisiz kişilerin eline geçmemesi için kullanıcının gerekli özen ve tedbiri göstermesi gerekir.



EK BİLGİ

Kullanıcı, chip kartını okuyucuya yerleştirip bilgisayara bağladıktan sonra, PIN şifresini girip imzala butonuna tıklayarak elektronik belgeyi dijital imza ile imzalamaktadır. Teknik yapısı anlatılan tüm süreç bilgisayar yazılımları vasıtasıyla otomatik olarak gerçekleştirilmektedir.

Uygulamada chip kartın güvenliğini sağlamak adına PIN (Personal Identification Number-Kişisel Kimlik Numarası) kullanılmaktadır. PIN, genellikle dört veya sekiz haneden oluşan, bir cihazı kullanacak kullanıcıyı doğrulamak için şifre olarak kullanılan sayı dizisidir. Chip kartın şifresi olarak PIN'lerin kullanımı, dört veya sekiz hanelik bir şifrenin zayıf güvenlik önlemi sağlaması nedeniyle doktrinde eleştirilmektedir.

Hash Fonksiyonu (Hash Function-Özet Fonksiyonu)

Asimetrik şifreleme yönteminde sertifikaya bağlanan anahtarlar kimlik doğrulama işlevini yerine getirmektedir. Ancak gönderilen mesajda değişiklik yapıp yapılmadığı yalnızca bu yöntem kullanılarak anlaşılamaz. Alıcıya ulaşan mesajın gönderici tarafından gönderilen orijinal mesaj olup olmadığını tespit etmek amacıyla hash fonksiyonu geliştirilmiştir. Hash fonksiyonu, mesajı belirli bir uzunlukta özet değerine (hash value) dönüştürür. Bu özet değeri mesajı gönderen kişi tarafından mesajla eklenir ve mesajı alan alıcı mesaja tekrar aynı hash fonksiyonunu uygulayarak elde ettiği özet değeri ile gönderici tarafından gönderilen özet değerini karşılaştırır. Mesajda herhangi bir değişiklik yapılması halinde hash değeri de değişeceği için karşılaştırma sonucunda mesajda bir değişiklik yapıp yapılmadığı anlaşılır.



DİKKAT EDELİM

Burada dikkat edilmesi gereken nokta şifrelemenin asıl mesaja değil, asıl mesajın hash değeri üzerine yapılması ve mesaja eklenerek alıcıya gönderilmesidir.



EK BİLGİ

Günümüzde en yaygın kullanılan hash fonksiyonları 128 bit boyutta hash değeri üreten MD5 (Message-Digest algorithm 5) ve 224, 256, 384 veya 512 bit boyutlarında hash değeri üreten SHA-3'tür. (Secure Hash Algorithm 3). MD5 hash fonksiyonu çeşitli saldırılara maruz kalarak güvenilirliği sarsılmış olsa da günümüzde yaygın olarak kullanılmaktadır.

Konuyu bir örnekle açıklayalım. A'nın B'ye dijital imzalı bir mesaj göndermek istediğini varsayalım. A'nın göndermek istediği mesaj *"B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim."* olsun. Öncelikle, A bu mesaja hash fonksiyonu uygulayacak ve bir sonuç elde edecektir. Sonucun *"2e779edc849e4a9c9838dd7e02548838"* olduğunu varsayalım. Daha sonra A, bu hash değerini mesaja ekleyecek ve kendi gizli anahtarını hash değerine uygulayacaktır. Bu durumda *"2e779edc849e4a9c9838dd7e02548838"* hash değeri şifreli olarak (genellikle hash değerine göre çok daha uzun bir şifre olacaktır) mesajın altında yer alacaktır. İşte burada yer alan şifreli hash değeri A'nın dijital imzasıdır. Mesaj bu haliyle B'ye gönderilecektir.

Mesaj kendisine iletilen B, öncelikle *"B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim."* mesajına hash fonksiyonunu uygulayacak ve *"2e779edc849e4a9c9838dd7e02548838"* hash değerini bulacaktır. Daha sonra A'nın gizli anahtarı yalnızca A'nın açık anahtarı kullanılarak çözülebileceği için B, A'nın açık anahtarını şifreli hash değerine uygulayacak ve *"2e779edc849e4a9c9838dd7e02548838"* değerini görebilecektir. İki hash değeri de aynı olduğu için gönderilen mesaj ile iletilen mesajda bir değişiklik yapılmadığı doğrulanmış olacaktır. Zira mesajda yapılacak en ufak değişiklik hash değerinin farklı hesaplanmasına yol açacaktır. Ayrıca şifreli hash değeri A'nın açık anahtarı ile çözülebildiği için mesajın A tarafından gönderildiği aksi ispat edilinceye kadar kesin olacaktır.

Örneği görsel olarak açıklayacak olursak, A'nın B'ye dijital imzalı olarak gönderdiği mesaj;

B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim.

A

04.10.2022

MIIBOwIBAAJBAl3pJFuPgjWya2uM1yuh4mKICmpjiVbYCnWoDOS0SNwROHuvmw6K5F6q4hL1Fm2GDLgPVwoE3UIqkaTzJqYxjECAwEAAQJACil4zgmvxFKbeJ8kRV6ZTH77Z/Tqv8pGrXg0PChg00IYb3JnPEuQfgQrcu7Mfwd3XqqubyO8NOA+1Fa8Vh9NQIhAO3AbqqnaIqSQtSh/VBiHAlmjdOnbdWrZQswHR5DVSNPAiEAmM2JV+Y+ul+nTem6ABguQnqwF8Tg7NORxiNdWODfn8CIQCmnmqwTFx2aKRPcisd73PonqecgkT2LoTEv3ZYpCak/wIgY6Xugm85yyskHTBmRzd9u4btHaMcF/XIY/SeJPQ7xZsCIQDqHEU7Csep/2m9d423nVkiJEiSiqAGqQ4wJ48ceHS1GQ== (A'nın gizli anahtarı)

2e779edc849e4a9c9838dd7e02548838 (B'nin, A'nın gönderdiği mesaja hash fonksiyonu uygulayarak hesapladığı hash değeri)

B öncelikle “B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim.” mesajına hash fonksiyonu uygulayarak “2e779edc849e4a9c9838dd7e02548838” hash değerini elde eder.

Daha sonra B, elektronik sertifika hizmet sağlayıcıdan edindiği A'nın açık anahtarını

(MFw wwDQYJKoZiHvcNAQEBBQADSwAwSAJBAl3pJFuPgjWya2uMlyuh4mKICmpjiVbYCnWo-DOS0SNwROHuvmw6K5F6q4hL1Fm2GDLgPVwoE3UIqkaTzjJqYxjECAwEAAQ==) A'nın gizli anahtarına uygular ve aşağıdaki sonucu elde eder. Bu noktada, şifreli hash değeri A'nın açık anahtarı ile çözü-

B tarafından satılan X markalı Y model dizüstü bilgisayarı 12.000 TL bedel karşılığında satın aldığımı beyan ederim.

A

04.10.2022

2e779edc849e4a9c9838dd7e02548838 (imzalı hash değeri)

lebildiği için mesajın A tarafından gönderildiği aksi ispat edilinceye kadar kesinleşmiş olur.

1. 2e779edc849e4a9c9838dd7e02548838 (B'nin hesapladığı hash değeri)
2. 2e779edc849e4a9c9838dd7e02548838 (imzalı hash değeri)

Son olarak B iki hash değerini karşılaştırır ve mesajın orijinal mesaj olup olmadığını (mesajda değişiklik yapılmadığını) doğrular.

İki değer de aynı olduğu için mesajın A tarafından gönderilen orijinal mesaj olduğu doğrulanmış oldu.

HATIRLATMA

Yukarıda belirtilen teknik işlemlerin tümü bilgisayar tarafından belirli yazılımlar vasıtasıyla otomatik olarak gerçekleşmektedir. Dolayısıyla uzun bir sıralama ile anlatılan güvenli elektronik imzanın oluşturulması ve doğrulanması işlemleri saniyeler içerisinde tamamlanmaktadır.

Zaman Damgası

Hukuki işlemlerin ne zaman gerçekleştirildiği önemlidir. Bir sözleşmenin kurulmasıyla tarafların hak ve borçları doğacak, buna bağlı olarak ifa zamanı belirlenebilecek, süre sınırının olduğu hukuki işlemlerde sürenin bitmesi hak kayıplarına yol açacaktır. Bu gibi sebeplerle irade beyanlarının ne zaman gerçekleştirildiğini belirlemek gerekir.

Elektronik ortamdaki verilerle oluşturulan belgelerde, belgenin oluşturulma zamanına çok basit bir biçimde, bilgisayarın tarih ve saat ayarlarının değiştirilmesi ile müdahale edilebildiği için hukuki işlemin yapılma anını bu şekilde belirlemek güvenli değildir. Zaman damgası, elektronik ortamda yapılan irade beyanlarının yapılma anını belirlemek ihtiyacını güvenilir bir biçimde karşılamak üzere geliştirilmiştir.

EİK m. 3/1 h bendinde zaman damgası; *“Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt ... ifade eder.”* şeklinde tanımlanmıştır.

Zaman damgası elektronik sertifika hizmet sağlayıcısı (ESHS) tarafından elektronik imzayla doğrulanan kayıt sistemidir. Gönderici, mesajını önce ESHS'ye ulaştırır ve ESHS, göndericinin dijital imzasına, mesajın kendisine ulaşma zamanını gösteren bir damga ekler ve elektronik imzasıyla imzalar. Böylece, göndericinin mesajına ESHS tarafından eklenen zaman damgası sayesinde, mesajın gönderilme zamanı güvenli bir biçimde tespit edilebilir. Ayrıca mesajın gönderilme zamanına ESHS tarafından tutulan kayıtlardan da ulaşılabilir.

Güvenli Elektronik İmza Nedir

Güvenli elektronik imza;

- “a) Münhasıran imza sahibine bağlı olan,*
 - b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,*
 - c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,*
 - d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan,”*
- elektronik imza olarak tanımlanmıştır.

Bir elektronik imzanın güvenli elektronik imza sayılması için; münhasıran imza sahibine bağlı olması, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulması, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlaması ve imzalanmış elektronik veride sonradan herhangi bir değişikliğin yapılmamış olması gerekir. Aksi takdirde güvenli elektronik imzaya bağlanan hukuki sonuçlar uygulama alanı bulmayacaktır. Güvenli elektronik imzada kullanılan gizli anahtar, kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir.

EİK kapsamında düzenlenen güvenli elektronik imza, Avrupa Birliği'nin 1999/93 sayılı Yönergesi'nde düzenlenen gelişmiş elektronik imza ile paraleldir.

EİK'da güvenli elektronik imza ile kast edilen elektronik imza türü dijital imzadır.

Münhasıran İmza Sahibine Bağlı Olma Unsuru

Kimlik doğrulaması işlevinin yerine getirilmesi, elektronik imzanın münhasıran imza sahibine bağlı olması ile mümkündür. Yukarıda yaptığımız açıklamalarda el yazısı ile atılan imza için kişinin kimliğini tespit etmeyi ve onu diğer kişilerden ayırmayı sağladığını belirtmiştik. Aynı durum güvenli elektronik imza için de geçerlidir. El yazısı ile atılan imza, el yazısının özgün ve karakteristik olması nedeniyle kimlik tespitini sağlarken, güvenli elektronik imzada kimlik tespiti, güvenli elektronik imza oluşturma aracının sadece imza sahibinin tasarrufunda bulunmasıyla, güvenli elektronik imzanın münhasıran imza sahibine bağlı olmasıyla ve güvenli elektronik imzanın nitelikli elektronik sertifikaya bağlı olmasıyla sağlanmaktadır.

Sadece İmza Sahibinin Tasarrufunda Bulunan Güvenli Elektronik İmza Oluşturma Aracı ile Oluşturulma Unsuru

EİK m. 6'da güvenli elektronik imza oluşturma araçları;

- "a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,*
- b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,*
- c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını*
- d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini,"* sağlayan imza oluşturma araçları olarak tanımlanmıştır.

O halde, güvenli elektronik imzadan bahsedebilmek için, güvenli elektronik imzanın, yukarıda sayılan şartları taşıyan bir güvenli elektronik imza oluşturma aracı ile oluşturulması gerekmektedir. Bu şartları taşıyan elektronik imza oluşturma aracı EİK'ya göre güvenli kabul edilmiştir.

Daha önce belirtildiği üzere, güvenli elektronik imzada kullanılan gizli anahtar, kullanıcı tarafından taşınabilecek nitelikte bir chip kartta muhafaza edilmektedir. Bu chip kart güvenli elektronik imza aracında yer almaktadır. Uygulamada güvenli elektronik imza oluşturma aracı genellikle; chip kart ve kart okuyucu USB parçalarından oluşmaktadır. Bu donanımlar bilgisayara bağlandıktan sonra bir yazılım vasıtasıyla imzalama işlemi tamamlanmaktadır.

Nitelikli Elektronik Sertifikaya Dayanarak İmza Sahibinin Kimliğinin Tespitini Sağlama Unsuru

EİK m. 3/1.1 bendinde elektronik sertifika, “İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı” ifade edecek biçimde tanımlanmıştır.

EİK m. 9’da, nitelikli elektronik sertifikada bulunması gereken unsurlar aşağıdaki şekilde sayılmıştır:

“Nitelikli elektronik sertifikada;

- a) Sertifikanın “nitelikli elektronik sertifika” olduğuna dair bir ibarenin,
- b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,
- c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,
- d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,
- e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,
- f) Sertifikanın seri numarasının,
- g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,
- h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgilerinin,
- ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin,
- j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının, bulunması zorunludur.”

Görüldüğü üzere, kimlik doğrulama işlevinin önemli bir parçası olan nitelikli elektronik sertifikada imza sahibinin teşhis edilebileceği kimlik bilgileri yer almaktadır.

EİK m. 9/1, d bendinde yer alan imza doğrulama verisi EİK m. 3/1/f’ye göre “Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri” ifade etmektedir. İmza sahibinin açık anahtarı bu kapsamdadır.

Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihi de ESHS’ler tarafından sertifikaya işlenir.

İmzalanmış Elektronik Veride Sonradan Herhangi Bir Değişiklik Yapılıp Yapılmadığının Tespitini Sağlama Unsuru

İmzalanmış elektronik veride herhangi bir değişiklik yapıp yapılmadığı hash fonksiyonu ile sağlanmaktadır. Bu konu, yukarıda ayrıntılı olarak açıklandığı için tekrarlanmayacaktır.

Güvenli Elektronik İmzaya Bağlanan Hukuki Sonuçlar

Daha önce belirtildiği üzere, kanunda aksine hüküm bulunmadığı takdirde, TBK m. 14/2 uyarınca güvenli elektronik imza ile gönderilip saklanabilen metinler yazılı şekil yerine geçer.

Gerek EİK m. 5/1, gerek TBK m. 15/1. fıkrasında güvenli elektronik imzanın el ile atılan imza ile aynı hukuki sonucu doğurduğunu hüküm altına almıştır. Ancak, bu kural her hukuki işlem için geçerli değildir. EİK m. 5/2’de bu kuralın istisnaları “Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile banka teminat mektupları ve Türkiye’de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez.” şeklinde düzenlenmiştir.

Böylece, güvenli elektronik imza ile resmi şekle veya özel bir merasime tabi olmayan hukuki işlemler ve teminat sözleşmeleri hariç (yalnızca banka teminat mektupları ve Türkiye’de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri güvenli elektronik imza ile yapılabilir), adi yazılı şekilde yapılabilen tüm sözleşmeler yapılabilir. Nitelikli yazılı şekilde sözleşme metninin de el yazısı ile yazılması arandığı için; nitelikli yazılı şekil şartının bulunduğu sözleşmelerde güvenli elektronik imza kullanılamayacaktır.

Örneğin, kanunla resmi şekle tabi tutulan taşınmaz satışı; kanunun özel bir merasime tabi tuttuğu evlilik; kanunun nitelikli yazılı şekle tabi tuttuğu el yazılı vasiyetname ve kefalet sözleşmesi, banka teminat mektupları ve Türkiye’de yerleşik sigorta şirketleri tarafından düzenlenen kefalet senetleri dışındaki diğer teminat sözleşmeleri geçerlilik şekline uygun olmadığı için güvenli elektronik imza ile gerçekleştirilemez.

Hatırlamak gerekir ki, kanun koyucu HMK’nın 199. maddesinde “...fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları...” belge olarak nitelendirmiştir.

Medeni usul hukukunda kesin deliller; ikrar, kesin hüküm, senet ve yemin olarak sayılmış olup, bu deliller hâkimi bağlayıcı niteliktedir. Hâkim, kesin delillerin dayandığı bir iddiayı doğru kabul etmek zorunda olup, bu konuda hâkimin takdir yetkisi bulunmamaktadır. Kanunda düzenlenen takdiri deliller ise; tanık, bilirkişi, keşif ve uzman görüşüdür. Hâkim bu delillere dayanan iddiaların doğru olup olmadığını takdir yetkisine dayanarak değerlendirebilir.

Yukarıda da belirtildiği gibi senetler kesin deliller arasında yer almaktadır. HMK m. 205/2 hükmü; “Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir.” şeklinde düzenlenmiştir. Hükme göre, usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik verilerin aksi ispat edilinceye kadar kesin delil olarak nitelendirileceği kabul edilmiştir.

HMK m. 205/3, güvenli elektronik imzanın teyit edilmesi ile ilgili; “Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler.” düzenlemesini içermektedir. Re’sen inceleme, hâkimin belgenin elektronik imza ile oluşturulup oluşturulmadığını kendiliğinden araştırması anlamına gelmektedir.

Güvenli elektronik imzalı veriye dayanarak mahkemeden bir talepte bulunulması halinde, karşı taraf bu verinin doğruluğunu veya varlığını inkâr edebilir. Bu durumda HMK’nın “Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur.” şeklindeki 210. maddesi uygulanır. Hükme göre hâkim, tarafları ve gerekirse bilirkişiyi dinleyerek verinin doğruluğu hakkında bir karara varacaktır.

HATIRLATMA

Hatırlamak gerekir ki, burada anlatılan hukuki sonuçlar her elektronik imza için geçerli olmayacaktır. Burada bahsedilen hukuki sonuçlar yalnızca güvenli elektronik imza için geçerlidir.

Elektronik Sertifika Hizmet Sağlayıcısı

Dijital imzanın, güvenli elektronik imza olarak değerlendirilebilmesi için nitelikli elektronik sertifikaya dayanarak imza sahibinin kimlik tespitini sağlaması gerektiğini belirtmiştik (EİK m. 4/1/c). Bunun altında yatan sebep, açık anahtar ve gizli anahtar oluşturma algoritmaları ve yöntemlerinin tek başına güvenli olmamasıdır. Bu algoritmalar ve yöntemlerin kötü niyetli bir kişi tarafından bilinmesi ve imzada kullanılmak üzere sahte bir kimliğe bağlı bir çift dijital imza anahtarı üretilmesi mümkündür. Bu nedenle dijital imza açık anahtarının güvenilir bir üçüncü kişi tarafından onaylanarak belirli bir kişiye tahsis edilmesine ihtiyaç duyulmuştur. Güvenilir üçüncü kişi (*Trust Center*), sertifika makamı (*Certification Authority*) veya onay makamı olarak da adlandırılmaktadır. Türk hukukunda bu makam ESHS'dir. ESHS'lerin yayımladığı sertifikalarda yer alan bilgilerin doğru olduğu kabul edilmektedir. Ayrıca, zaman damgası hizmetini de ESHS sunmaktadır.

Dijital imzada kullanılan asimetrik şifreleme yöntemi kapsamında açık ve gizli anahtarları (şifreleri) ESHS hazırlar. Hazırlanan her anahtar, her bir kullanıcı için ayrı olarak oluşturulmaktadır. Dijital imza kullanıcısı ESHS'ye başvurarak, kimlik bilgilerini iletir, bunun üzerine ESHS, açık anahtarı kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Gizli anahtar ise kullanıcı dışında kimseye verilmez. Kullanıcı, alıcıya dijital imzalı bir mesaj gönderdiğinde alıcı, ESHS'nin listesinden kullanıcının açık anahtarına ulaşabilir ve şifreli mesajı çözerek, okunur hale getirebilir.

Elektronik Sertifika Hizmet Sağlayıcısının Faaliyete Başlaması

ESHS olarak faaliyete başlayabilme şartları EİK m. 8'de düzenlenmiştir. Hükme göre ESHS faaliyete başlamak için herhangi bir izin almak zorunda değildir.

EİK m. 8/1; *“Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.”* şeklinde düzenlenmiştir. Görüldüğü üzere, bu hükme göre gerçek veya tüzel kişiler herhangi bir izne tabi olmaksızın ESHS olabilecektir. Burada düzenlenen usul bildirim usulü olarak adlandırılmaktadır. Ancak bahsi geçen maddenin devam eden fıkralarına ve Elektronik İmza Yönetmeliği'ne birlikte bakıldığında, burada aslında bildirim usulünün değil izin usulünün düzenlendiği anlaşılabacaktır. Bu hususa ilerleyen paragraflarda ayrıntılı olarak değinilecektir.

ESHS'nin faaliyete başlayabilmesi için Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) bildirimde bulunması gerekmektedir. Bu bildirimde belirli şartların sağlanması gerekmektedir.

EİK m. 8/2'de bu şartlar;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak” olarak sayılmıştır. BTK, ESHS'nin bu şartları yerine getirip getirmediğini re'sen inceler. Şartlardan birinin eksik olması veya yerine getirilmediği tespit edilirse, bu eksiklerin giderilmesi için hizmet sağlayıcısına bir ayı geçmemek üzere bir süre verilir, bu süre içinde hizmet sağlayıcısının faaliyetleri durdurulur (EİK m. 8/3). Bu süre içerisinde de eksikler giderilmezse, BTK, ESHS'nin faaliyetlerine son verir (EİK m. 8/3).

ESHS faaliyetlerine devam ederken, yukarıdaki paragrafta sayılan şartları (EİK m. 8/2’de yer alan şartlar) kaybederse yine yukarıdaki paragrafta anlatılan, önce süre verilmesiyle başlayan usul (EİK m. 8/3) uygulanır.

EİK m. 20’de yer alan “*Bu Kanunun uygulanmasına ilişkin usul ve esaslar, ilgili kurum ve kuruluşların görüşü alınarak Kurum tarafından çıkarılacak yönetmeliklerle düzenlenir.*” hükmü gereğince, EİK m. 8/2’de yer alan şartlar, Elektronik İmza Yönetmeliği ile somutlaştırılmıştır. Yönetmelik Ek-1’de bildirimde sunulacak bilgi ve belgeler düzenlenmiştir.

Elektronik İmza Yönetmeliği m. 7/1’de; “*Kurum, yapılan bildirimi derhal incelemeye alır ve incelemeyi iki (2) ay içinde sonuçlandırır. Bildirim şartlarını eksiksiz olarak yerine getiren ESHS, bildirim yaptığı tarihten iki (2) ay sonra faaliyete geçer.*” hükmü düzenlenmiştir. BTK’nın bildirimi re’sen incelemesi, iki ay içerisinde kararını açıklaması, bildirim şartlarını yerine getirmeyen hizmet sağlayıcıların faaliyetinin durdurulması birlikte değerlendirildiğinde “bildirim” adı altında geçen usulün aslında izin usulü olduğu anlaşılmaktadır. BTK’nın ESHS’lerin faaliyetine son verme yetkisi de bu görüşü destekler niteliktedir.

Elektronik Sertifika Hizmet Sağlayıcısının Temel Yükümlülükleri

ESHS’lerin temel yükümlülükleri EİK m. 10’da düzenlenmiştir. Ancak, ESHS’lerin yükümlülükleri bu maddede sayılanlar ile sınırlı değildir. ESHS’lerin EİK’da düzenlenen diğer maddelere ve genel hükümlere göre de yükümlülükleri bulunmaktadır. Biz, bu konu kapsamında en önemli ve bilinmesi gereken yükümlülüklerle değinmekle yetineceğiz.

EİK m. 10/1’ de düzenlenen ESHS’nin önemli yükümlülükleri;

“b) Nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre veya Türkiye Cumhuriyeti kimlik kartı vasıtasıyla uzaktan güvenilir bir biçimde tespit etmek

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak veya sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işlemin güvenliğini sağlamak

e) Kanunlarda öngörülen sınırlamalar saklı kalmak üzere sertifikanın kullanımına ilişkin özellikler, uyumsuzlukların çözüm yolları ile ilgili şartlar ve güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında talep eden kişiyi sertifikanın tesliminden önce bilgilendirmek

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırması konusunda, sertifika sahibini bilgilendirmek

g) Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamak

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmek” olarak sayılabilir.

Güvenli elektronik imzanın en önemli fonksiyonlarından biri olan kimlik tespiti, daha önce de belirtildiği üzere, ESHS’lerce çıkarılan nitelikli sertifikalar ile sağlanmaktadır. ESHS, açık anahtar kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Böylece imza sahibinin kimliği tespit edilebilir.

Güvenli elektronik imzaya bağlanan hukuki sonuçlardan en önemlisi olan güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiye sertifika tesliminden önce bilgi vermek de ESHS’nin yükümlülükleri arasındadır.

ESHS, sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini bilgilendirmek ile yükümlüdür. Bu bilgilendirmeyi yaptıktan sonra imza oluşturma verisini başkasına kullandırmak imza sahibinin sorumluluğuna tabi olacaktır. Uyuşmazlık halinde ESHS, bilgilendirme yaptığını ispatlamakla yükümlüdür. Aksi takdirde meydana gelen zararlardan sorumlu olacaktır. Keza ESHS'nin hukuki sorumluluğunun düzenlendiği EİK m. 13'te *"Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlali suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz."* hükmü yer almaktadır.

ESHS, verdiği hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla yükümlüdür. Ayrıca faaliyetine son vereceğini en az üç ay önce BTK'ya ve sertifika sahibine bildirmekle yükümlüdür.

Son olarak, EİK m. 10/2'de *"Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz."* hükmü yer almaktadır. Bu hüküm gereğince, ESHS'nin ürettiği imza oluşturma verisi yalnızca imza sahibine tahsis edilecek, gizliliği korunacaktır. ESHS kendisi dahi bu veriyi kopyalayamayacak veya bu veriyi saklayamayacaktır.

BÖLÜM ÖZETİ

Elektronik belgeler el ile imzalanamamakta olup imzanın taranarak belgeye eklenmesi güvenlik ihlalleri nedeniyle mümkün değildir. Taranmış imzanın, imzalayan tarafından elektronik belgeye eklendiğini ispatlamak çok zordur. Taranmış imza, kolaylıkla kötü niyetli üçüncü kişilerin eline geçebilir ve imza kopyalanarak taklit edilebilir. Bilgisayarda üretilen belgelerin tarih, saat, yazar bilgileri kolaylıkla değiştirilebilmektedir. Bu sebeplerle elektronik ortamda yer alan verilere dayanan hukuki işlemlerin yazılı şekle uygun yapılamaması sorunu doğmuştur. Bu sorun, elektronik imza düzenlemeleri ile dijital imza ya da Elektronik İmza Kanunu'nda yer alan güvenli elektronik imzanın kullanılmasıyla çözülmüştür.

Gerek Elektronik İmza Kanunu gerekse Türk Borçlar Kanunu güvenli elektronik imzanın el ile atılan imza ile aynı hukuki sonucu doğurduğunu hüküm altına almıştır. Burada güvenli elektronik imza ile kastedilen, kanundaki şartları taşıyan dijital imzadır. Ancak, bu hukuki sonuç yalnızca Elektronik İmza Kanunu madde 4'te tanımlanan güvenli elektronik imza için geçerlidir. Burada sayılan şartları taşımayan veriler, Hukuk Muhakemeleri Kanunu madde 199 gereğince belge olarak kabul edilebilmektedir.

Güvenli elektronik imzaya bağlanan hukuki sonuçlardan bir diğeri ispata ilişkin olmak üzere usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik verilerin, aksi ispat edilinceye kadar kesin delil olarak nitelendirileceğidir. Elektronik imza denilince akla dijital imza gelse de elektronik imza dijital imzayı da kapsamına alan elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavramdır. Elektronik imza yöntemlerine örnek olarak; biyometrik imza (parmak izi, retina taraması gibi), PIN, dijital ortama aktarılmış el yazısı ve dijital imza verilebilir.

Dijital imzanın teknik yapısı temel olarak; asimetrik şifreleme yöntemine, hash fonksiyonuna ve zaman damgasına dayanmaktadır. Asimetrik şifreleme yönteminde kullanılan gizli ve açık anahtarlar elektronik sertifika hizmet sağlayıcıları tarafından üretilir ve bir sertifika ile temsil edilirler. Bu sertifikada anahtar sahiplerinin kimlik bilgileri yer alır. Böylece dijital imzanın kimlik doğrulama fonksiyonu yerine getirilir. Hash fonksiyonu ile mesajda herhangi bir değişiklik yapılmadığı doğrulanır.

Zaman damgası ile güvenli elektronik imzalı belgenin ne zaman oluşturulduğu ve gönderildiği tespit edilir. Zaman damgası hizmeti, elektronik sertifika oluşturulması elektronik sertifika hizmeti sağlayıcıların görevleri arasındadır. Elektronik sertifika hizmeti sağlayıcılar, açık anahtarı kullanıcının kimlik bilgileriyle birlikte sertifikaya bağlar ve listede yayımlar. Gizli anahtar ise kullanıcı dışında kimseye verilmez. Böylece imza sahibinin kimliği tespit edilebilir. Güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiye sertifika tesliminden önce bilgi vermek de Elektronik sertifika hizmeti sağlayıcıların yükümlülükleri arasındadır. Elektronik sertifika hizmeti sağlayıcılar, sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda sertifika sahibini bilgilendirmek ile yükümlüdür.

GÖZDEN GEÇİRELİM

1. Sözleşmelerde geçerlilik şekline uyulmamasının yaptırımını iken ispat şekline uyulmamasının yaptırımını
2. Adi yazılı şekle bağlı bir sözleşmede kural olarak, borç altına giren kişinin bulunması zorunludur.
3. Senet, hâkimi bağlayıcı nitelikte olan arasında yer almaktadır.
4. dijital imzayı da kapsamına alan, elektronik belgeleri imzalamak için kullanılan farklı yöntemleri ifade eden bir üst kavram olarak değerlendirilmektedir.
5. özel bir algoritma (hash fonksiyonu) kullanılarak oluşturulan ve göndere- nin özel anahtarı ile şifrelenen bir ileti/mesaj özetidir.
6. Dijital imzanın şifrelenmesi için kullanılmaktadır.
7. Gerek EİK m. 5/1, gerek TBK m. 15/1 güvenli elektronik imzanın hüküm altına almıştır.
8. Güvenli elektronik imza ile ve teminat sözleşmeleri hariç (yalnızca banka teminat mektupları ve Türkiye’de yerleşik sigorta şirketleri tarafından düzenle- nen kefalet senetleri güvenli elektronik imza ile yapılabilir), yapılabilen tüm sözleş- meler yapılabilir.
9. Usulüne uygun olarak güvenli elektronik imza ile oluşturulan elektronik veriler; aksi ispat edilinceye kadar olarak değerlendirilecektir.
10. Dijital imza açık anahtarının güvenilir bir üçüncü kişi tarafından onaylanarak belirli bir kişiye tahsis edilmesine ihtiyaç duyulmuştur. Güvenilir üçüncü kişi (Trust Center), sertifika ma- kamı (Certification Authority) veya onay makamı olarak da adlandırılmaktadır. Türk hukukun- da bu makam’dır.

CEVAP ANAHTARI

1. sözleşmenin geçersiz olması / sözleş- menin varlığının veya doğruluğunun ispat edilmemiş olmasıdır.	6. asimetrik şifreleme yöntemi
2. El yazısı ile atılmış imzasının	7. el ile atılan imza ile aynı hukuki sonucu doğurduğunu
3. kesin deliller	8. resmi şekle veya özel bir merasime tabi olmayan hukuki işlemler/ adi yazılı şekilde
4. Elektronik imza	9. kesin delil
5. Dijital imza	10. Elektronik sertifika hizmet sağlayıcısı (ESHS)

SÖZLÜK

Algoritma: Bir sorunun çözümü veya cevabını bulmak üzere sınırlı sayıda adımlardan oluşan sistematik yöntem.

Anahtar: Bilişimde şifre yazmak ve çözmek için kararlaştırılmış olan yol.

Bit: Bilgisayarda veri depolama ve aktarımında en küçük birimdir. Bir byte 8 bitten oluşur.

Biyometrik imza: İmza sahibinin biyometrik verilerini kullanarak ve genellikle bu verilerin imzalanan belgeye çözülemez biçimde bağlanmasıyla oluşturulan imzalama yöntemi.

Chip kart: Akıllı kart veya tümleşik devre kartı olarak da adlandırılan, entegre devreler içeren, herhangi bir mikroçip boyutunda karttır.

Delil: Bir vakıanın ispatı için başvuru alan araç veya araçlar.

Dijital: Sayısal.

Hukuki işlem: Bir ya da daha çok kişinin hukuk düzeninin öngördüğü sınırlar içerisinde, hukuki sonuç veya sonuçlar doğurmaya yönelik irade açıklaması.

Hukuki sonuç: Hukuk düzeninin hukuki olaylara bağladığı sonuç. Hukuki sonuca bağlı olarak bir hak veya hukuki ilişki kurulur, değiştirilir veya ortadan kaldırılır.

İrade beyanı: Hukuki bir sonuca yönelik işlem iradesini dış dünyaya açıklamak.

Paraf: Yalnız adın veya ad ve soyadın baş harfleriyle atılan kısa imza.

Sunucu: Bilgisayar biliminde sunucu, istemci adı verilen başka programlar veya cihazlar için işlevsellik sağlayan belirli bilgisayara donanım ve yazılımlarının (bilgisayar programlarının) bileşimidir.

USB: Dış donanımların bilgisayar ile bağlantı kurabilmesini sağlayan bağlantı aparatı.

Üçüncü kişi: Bir sözleşmenin, davanın veya icra takibinin taraflarının dışında olan kişi.

Veri: Ölçüm, deney, gözlem gibi araştırma yöntemleri vasıtasıyla elde edilen ham olgu veya gözlemler.

Yürürlüğe girmek: Bir kanun, yönetmelik vb. düzenlemenin, kararın uygulanır duruma gelmesi.

KAYNAKÇA

- Antalya*, Gökhan: Borçlar Hukuku Genel Hükümler, 2. Bası, C. V/1,1, Seçkin Yayıncılık, Ankara 2019.
- Arslan*, Ramazan/Yılmaz, Ejder/Taşpınar Ayvaz, Sema/Hanağası, Emel: Medenî Usul Hukuku, 4. Bası, Yetkin Yayıncılık, Ankara 2018.
- Eren*, Fikret: Borçlar Hukuku Genel Hükümler, 26. Bası, Yetkin Yayıncılık, Ankara 2021.
- Ertugut*, Mine: Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Yetkin Yayıncılık, Ankara 2004.
- Greenleaf*, Grahan/Clarke, Roger: "Privacy Implications of Digital Signatures", 1997, (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2263663), (E.T.: 04.10.2022).
- Keser Berber*, Leyla: İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Yetkin Yayıncılık, Ankara 2002.
- Kılıçoğlu*, Ahmet M.: Borçlar Hukuku, 25. Bası, Turhan Yayınevi, Ankara 2021.
- Menezes*, Alfred J./Oorschot, Paul C. Van/Vanstone, Scott A.: Handbook of Applied Cryptography, CRC Press, 1997.
- Orta*, Mesut: Elektronik İmza ve Uygulaması, Seçkin Yayıncılık, Ankara 2005.
- Sağlam*, İpek: Elektronik Sözleşmeler, Legal Yayıncılık, İstanbul 2007.
- Sarıakçalı*, Turgay: İnternet Üzerinden Akdedilen Sözleşmeler, 2. Bası, Seçkin Yayıncılık, Ankara 2021.
- Şenocak*, Zarife: "Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", AÜHFD 2001, C. 50, S. 2, s. 97-135.
- Topaloğlu*, Mustafa: Bilişim Hukuku, Karahan Kitabevi, Adana 2005.

ÜNİTE 5

ELEKTRONİK TİCARET
VE TÜKETİCİ HUKUKU

Arş. Gör. Zeynep ÖZKAN

ANAHTAR KAVRAMLAR

Elektronik ticaret
Elektronik pazar yeri
Tüketici
Tüketici işlemi
Mesafeli sözleşme

5 ELEKTRONİK TİCARET VE TÜKETİCİ HUKUKU

ÖĞRENME HEDEFLERİ

-  1 Elektronik ticaret ile hukuk ilişkisini kavrayabilmek
-  2 Tüketicinin korunması hukuku hakkında genel bilgi sahibi olmak
-  3 Elektronik ticarete tüketici işlemlerini ayırt edebilmek
-  4 Elektronik ticarete tüketicinin haklarını öğrenmek



Bilginin yayılmasında kitle iletişim araçları ve internetin kullanımının yaygınlaşması, toplumun her kesimini ve neredeyse her sektörü etkilemiştir. Bu anlamda, ilkel toplumlardan bu yana gelişip değişen ticaret olgusunun teknolojik gelişmeler karşısında tepkisiz kalmaması da şaşırtıcı değildir. Ticarete, pazarlama aracı olarak elektronik iletişim araçlarından yararlanılmasının giderek yaygınlaşmasıyla elektronik ticaret kavramı doğmuştur. Elektronik ticaretin işletmeler için başlıca avantajları, işletmelerin yeni pazarlara açılmasını kolaylaştırması, iş hacimlerini artırmaları ve potansiyel müşterilerine daha hızlı ulaşabilmeleridir. Benzer şekilde, müşteriler de birçok ürünü aynı anda inceleyebilmekte, ürünleri karşılaştırabilmekte, aradıkları ürüne daha hızlı ve kolay ulaşabilmektedir. Ancak elektronik ortamda gerçekleşen ticarete tarafların fiziken karşı karşıya gelmemesi, ürünü inceleme şansının olmaması gibi durumlar alıcı konumunda bulunanlar için dezavantaj yaratmaktadır. Öte yandan, günümüzde elektronik ticaret çoğunlukla elektronik ticaret pazar yerleri üzerinden gerçekleştirilmektedir. Bu çerçevede, elektronik ticarete hizmet sağlayıcıların ve aracı hizmet sağlayıcılarının yükümlülüklerinin ve sorumluluklarının sınırlarının belirlenmesi elektronik ticaretin güvenli bir şekilde sürdürülmesi açısından önem arz etmektedir.

Elektronik ticaretin gelişmesine paralel olarak ortaya çıkan hukuki problemlerin çözümü için ulusal ve uluslararası düzeyde çeşitli çalışmalar yapılmaktadır. Türk hukukunda elektronik ticarete ilişkin temel mevzuat “6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (ETDHK) (RG, 05.11.2014, S. 29166)” ve bu Kanun’a dayanılarak çıkarılan ikincil düzenlemelerdir. Elektronik ticarete ortaya çıkan uyuşmazlık konularına göre, fikri mülkiyet hukuku, kişisel verilerin korunması hukuku, tüketici hukuku gibi alanlarda da elektronik ticarete ilişkin düzenleyici hükümler yer almaktadır. Elektronik ticaret iş hacminde, tüketici işlemlerinin yeri yadsınamayacak kadar fazladır. Bu çerçevede, elektronik ticarete konu sözleşmenin tüketici sözleşmesine vücut verdiği hâllerde tüketicinin etkin bir şekilde korunup korunamayacağı da önemli bir problem olarak varlığını sürdürmektedir. Kitabımızın bu bölümde öncelikle elektronik ticarete ilişkin genel bilgiler verilmiş, elektronik ticaret ve hukuk ilişkisi incelenmiş daha sonra elektronik ticarete tüketicinin korunması konusu üzerinde durulmuştur.

Elektronik Ticaret

Elektronik Ticaret Nedir?

Bilgi teknolojilerinde yaşanan gelişmeler, iletişim olanaklarının çeşitlenmesi, özellikle sosyal medyanın geniş kitlelerce yaygın olarak kullanılması bilgiye ulaşma ve bilgiyi paylaşma hızını artırmıştır. Bu gelişmeler, işletmelerin iş yapış modellerini de büyük oranda etkilemiştir. Geleneksel ticaret, zaman içinde “elektronik ticaret”e evrilmiş ve ortaya çıkan bu kavram günümüzün vazgeçilmez bir parçası hâline gelmiştir. Gerçekten de bugün birçok işletme, iş ve işlemlerinin büyük çoğunluğunu elektronik ortamda yürütmektedir.

Elektronik ticaret, en genel ifadeyle, mal veya hizmetlerin elektronik ortamlarda üretilmesine, reklamının yapılmasına, pazarlanmasına veya sunulmasına yönelik işlemlerin bütünü olarak açıklanabilir. Bu çerçevede, mobil bankacılık ve internet bankacılığı hizmetleri, çevrimiçi psikolojik danışmanlık veya diyetisyenlik hizmetleri, çevrimiçi özel ders hizmetleri, Netflix, Spotify, Blutr gibi platformlar üzerinden alınan hizmetler, turizm ve biletleme hizmetleri, elektronik dergi aboneliği, sanal pazar yerleri üzerinden ürün satışı, internet üzerinde yapılan müzayede, lisanslı bir yazılımın satın alınması gibi birçok işlem elektronik ticaretin kapsamına girmektedir.

Elektronik Ticaretin Unsurları

Yukarıda yapılan tanımdan anlaşıldığı üzere, elektronik ticaretin “elektronik ortam” ve “ticari işlem” olmak üzere iki unsuru bulunmaktadır.

- **Elektronik Ortam**

Elektronik ticaret, tüm elektronik ortamlarda, her türlü elektronik iletişim aracı kullanılmak suretiyle gerçekleştirilebilir. Bu kapsamda, elektronik veri değişimi (EDI*), elektronik posta (e-posta), mobil uygulamalar, kısa mesaj, telefon, teleks ve benzeri araçlar kullanılmak suretiyle elektronik ticaret gerçekleştirilebilir.

*EDI (*electronic data interchange*): Elektronik veri değişimi, elektronik ortamda verilerin değiş tokuşunu ifade eder. İşletmeler arası veri transferi için geliştirilmiştir.

Günümüzde, elektronik ticaret için en çok tercih edilen elektronik ortam, internettir. İnternet, “uluslararası ağ” anlamına gelmekte olup en genel ifadeyle, bilgisayarların birbirleri ile iletişimini sağlayan haberleşme ağıdır. İnternet üzerinden çok farklı hizmetler sunulmakla birlikte, elektronik ticarete yaygın olarak internet hizmetleri; “EDI”, “e-posta” ve “web siteleri” kullanılmaktadır.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Telefon ya da kısa mesajla alınan bir hizmetin bedelinin faturaya yansıtılması örneğinde, elektronik iletişim araçlarıyla gerçekleşmiş bir işlem söz konusu olduğundan bu işlem elektronik ticaretin kapsamına girer.

- **Ticari İşlem**

Elektronik ticaretin bir diğer unsuru olan “ticari işlem” unsurunun, 6102 sayılı Türk Ticaret Kanunu (TTK) (RG, 14.02.2011, S. 27846) anlamında “ticari iş” ile karıştırılmaması gerekir. Elektronik ticarete “ticari işlem” unsuru, telekomünikasyon araçlarıyla yapılan her türlü ekonomik faaliyeti kapsamaktadır. Bu anlamda, elektronik ticaret kapsamında yapılan işlem; “ticari iş”, “tüketici işlemi” veya “adi iş” olabilir.

HATIRLATMA

“Ticari iş” kavramı, TTK’nın 3. ve 19. maddelerinde düzenlenmiştir. Buna göre; TTK’da düzenlenen hususlar ile bir ticari işletmeyi ilgilendiren bütün işler ve fiiller ticari işlerdendir (TTK m. 3). Bununla birlikte, taraflardan yalnız biri için ticari iş niteliğinde olan sözleşmeler, Kanunda aksine hüküm bulunmadıkça, diğeri için de ticari iş sayılır (TTK m. 19/2).



DİKKAT EDELİM

Tüketici işlemi veya ticari iş olmayan her türlü işlem adi iş olarak kabul edilir. Kural olarak adi işlere genel hükümler uygulanır.

Elektronik Ticaret Türleri

- **Elektronik Ticaretin Taraflarına Göre Yapılan Ayrım**

Elektronik ortamda yürütülen işlemler;

- işletmeler arasında (*B2B: business to business*),
- işletme ve tüketici arasında (*B2C: business to consumer*),
- tüketiciler arası (*C2C: consumer to consumer*),

- işletme ile idare arasında (B2G: *business to government*) veya
- idare ile tüketici arasında (G2C: *government to consumer*) olabilir.

İşletme ile tüketici arasındaki elektronik ticaret kapsamında, tüketiciyi koruyucu önlemler ilerleyen kısımlarda ayrıntılı olarak ele alınmaktadır.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Bir restoranın internet üzerinden satış yapan bir firmadan tek kullanımlık ıslak mendil sipariş vermesi, işletmeler arası elektronik ticarete örnektir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Bir restoranın internet üzerinden satış yapan bir firmadan tek kullanımlık ıslak mendil sipariş vermesi, işletmeler arası elektronik ticarete örnektir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Kamu ihalelerinin internet üzerinden yapılması, devletin taraf olduğu elektronik işlemlere örnektir. “e-devlet”, “e-nabız” gibi uygulamalar aracılığıyla da resmî birtakım işlemler elektronik ortamda yapılabilir ancak bu işlemler ticari nitelikli değildir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

“Dolap”, “Letgo”, “Sahibinden” gibi ikinci el eşya satışının gerçekleştiği platformlar üzerinden yapılan satışlar, tüketiciden tüketiciye elektronik ticarete örnektir.

• Dolaylı Elektronik Ticaret – Dolaysız Elektronik Ticaret Ayrımı

Daha önce çeşitli vesilelerle ifade edildiği gibi, birçok mal ve hizmet elektronik ticarete konu olabilir. Elektronik ticarete kurulan sözleşmenin, sözleşme öncesi görüşmelerinden sözleşme konusu mal ya da hizmetin ifasına kadar çeşitli aşamaları elektronik ortamda gerçekleştirilebilir. Sözleşmenin ifa aşaması dikkate alınarak yapılan dolaylı elektronik ticaret-dolaysız elektronik ticaret ayrımına göre;

- dolaylı ticaret, sözleşmenin sanal ortamda kurulduğu ancak ifanın fiziksel olarak yapıldığı;
- dolaysız ticaret gerek sözleşmenin kuruluşunun gerekse karşılıklı edimlerin ifasının elektronik ortamda yapıldığı elektronik ticaret türüdür.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Elektronik ticaretin konusunu kitap, elektronik aletler, giyim ve kozmetik ürünleri gibi maddi varlığı olan bir malın oluşturması hâlinde dolaylı elektronik ticaret söz konusu olur.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Elektronik ticaretin konusunun, bilgisayara indirilen bir oyun, elektronik kitap, çevrimiçi danışmanlık hizmetleri vb. olduğu hâllerde dolaysız elektronik ticaret söz konusudur.

Elektronik Ticaret ve Hukuk

Elektronik ticaret kavramı, hukuki bir kavram olmaktan uzaktır. Öte yandan, bir bedel karşılığında mal veya hizmetin değiş tokuşunun kısmen veya tamamen elektronik yollarla gerçekleştirilmesinin hukukten sonuçları olduğuna şüphe yoktur. Gerçekten de elektronik ticaretin geniş kitlelerce tercih edilmesi, elektronik ticaretin düzenlenmesi ihtiyacını doğmuştur. Bu anlamda, elektronik ticaret piyasasının regüle edilmesine ilişkin uluslararası ve ulusal boyutlarda hukuki çalışmalar yapılagelmektedir.

Türk hukukunda elektronik ticaretin düzenlemesine ilişkin temel kanun, “6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun (ETDHK) (RG, 05.11.2014, S. 29166)”dur. ETDHK’ya dayanarak çıkarılan ikincil düzenlemeler de hukukumuz açısından elektronik ticaretin önemli hukuki kaynaklarını oluşturur. Bununla birlikte, “5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (RG, 23.05.2007, S. 26530)”, “5809 sayılı Elektronik Haberleşme Kanunu (RG, 10.11.2008, S. 27050, mükerrer)”, “6698 sayılı Kişisel Verilerin Korunması Kanunu (RG, 07.04.2016, S. 29677)” gibi farklı kanunlarda da elektronik ticarete ilişkin hükümler yer alır. Tüm bu düzenlemeler, elektronik ortamda yürütülen faaliyetlerin daha güvenli bir şekilde yürütülmesini amaçlar.

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

ETDHK, elektronik ticarete ilişkin esas ve usulleri düzenlemeyi amaçlamakta olup ticari iletişimi, hizmet sağlayıcın ve aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçlarıyla yapılan sözleşmeler ile elektronik ticarete ilişkin bilgi verme yükümlülüklerini ve uygulanacak yaptırımları kapsar.

ETDHK’nın 2. maddesinde kanunda geçen kavramlar tanımlanmıştır. Konumuz açısından önem arz eden kavramlardan bazılarının kanun kapsamındaki anlamlarına aşağıda yer verilmiştir:

- **Elektronik ticaret:** Fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyeti,

- **Ticari iletişim:** Alan adları ve elektronik posta adresi dışında, mesleki veya ticari faaliyet kapsamında kazanç sağlamaya yönelik olarak elektronik ticarete ilişkin her türlü iletişimi,
- **Ticari elektronik ileti:** Telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri,
- **Hizmet sağlayıcı:** Elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişileri,
- **Aracı hizmet sağlayıcı:** Başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişileri
- **Elektronik ticaret aracı hizmet sağlayıcı (ETAHS):** Elektronik ticaret pazar yerinde elektronik ticaret hizmet sağlayıcıların mal veya hizmetlerinin teminine yönelik sözleşme yapılmasına ya da sipariş verilmesine imkân sağlayan aracı hizmet sağlayıcıyı,
- **Elektronik ticaret hizmet sağlayıcı (ETHS):** Elektronik ticaret pazar yerinde ya da kendine ait elektronik ticaret ortamında mal veya hizmetlerinin teminine yönelik sözleşme yapan ya da sipariş alan hizmet sağlayıcı,
- **Elektronik ticaret ortamı:** Elektronik ticaret faaliyetinde bulunulan internet sitesi, mobil site veya mobil uygulama gibi platformları,
- **Elektronik ticaret pazar yeri:** Elektronik ticaret aracı hizmet sağlayıcının aracılık hizmetlerini sunduğu elektronik ticaret ortamını,
- **Elektronik Ticaret Bilgi Sistemi (ETBİS):** Elektronik ticaret hizmet sağlayıcı ve elektronik ticaret aracı hizmet sağlayıcıların kayıt altına alınması, elektronik ticaret verilerinin toplanması, bu verilerin işlenerek istatistiki bilgilerin üretilmesi amacıyla Bakanlık tarafından oluşturulan ve bu Kanun kapsamında kayıt ve bildirim yapılabilmesine imkân sağlayan bilgi sistemini,
- **Bakanlık:** Ticaret Bakanlığı'nı ifade eder.

ETDHK'nın önemli düzenlemelerinden biri, Kanunun 3. maddesinde "hizmet sağlayıcı" için öngörülen "bilgi verme yükümlülüğü"dür. Bilgi verme yükümlülüğü, ticaretin tarafları (ister B2B ister B2C ister olsun) arasında güve sağlamayı amaçlar ve elektronik ticaretin gelişmesine hizmet eder.

Bilgi verme yükümlülüğü kapsamında, hizmet sağlayıcı elektronik iletişim araçlarıyla bir **sözleşmenin yapılmasından önce;**

- Alıcıların kolayca ulaşabileceği şekilde ve güncel olarak tanıtıcı bilgilerini,
- Sözleşmenin kurulabilmesi için izlenecek teknik adımlara ilişkin bilgileri,
- Sözleşme metninin sözleşmenin kurulmasından sonra, hizmet sağlayıcı tarafından saklanıp saklanmayacağı ile bu sözleşmeye alıcının daha sonra erişiminin mümkün olup olmayacağı ve bu erişimin ne kadar süreyle sağlanacağına ilişkin bilgileri,
- Veri girişindeki hataların açık ve anlaşılır bir şekilde belirlenmesine ve düzeltilmesine ilişkin teknik araçlara ilişkin bilgileri,
- Uygulanan gizlilik kuralları ve varsa alternatif uyuşmazlık çözüm mekanizmalarına ilişkin bilgileri

sunar (ETDHK m. 3/1).

Karşı tarafın tüketici olduğu sözleşmelerde yukarıda sayılan hususlar mutlak olarak uygulanır; ancak, taraflar tüketici sıfatını haiz değilse, yukarıdaki düzenlemelerin aksini kararlaştırabilirler (ETDHK m. 3/3). Bilgi verme yükümlülüğü kapsamında yukarıda sayılan şartlar münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelere uygulanmaz (ETDHK m. 3/5). Bununla birlikte, sözleşmenin taraflarına ve hangi elektronik iletişim aracıyla kurulduğuna bakılmaksızın, hizmet sağlayıcı, sözleşme hükümlerinin ve genel işlem şartlarının alıcı tarafından saklanması imkân sağlamalıdır (ETDHK m. 3/4).

Elektronik ticarete önemli konulardan bir tanesi de kuşkusuz ticarete konu ürünün siparişidir. Elektronik iletişim araçlarıyla verilen siparişlerde, hangi esasların geçerli olacağı ETDHK'nın 4. maddesinde düzenlenmiştir. Buna göre; hizmet sağlayıcı, siparişin onaylanması aşamasında ve ödeme bilgilerinin girilmesinden önce, ödeyeceği toplam bedel de dâhil olmak üzere, sözleşmenin şartlarının alıcı tarafından açıkça görülmesini sağlar ve alıcının siparişini aldığını gecikmeksizin elektronik iletişim araçlarıyla teyit eder. Sipariş ve siparişin alındığının teyidi, tarafların söz konusu beyanlara erişiminin mümkün olduğu anda gerçekleşmiş sayılır. (ETDHK m. 4/1). Ayrıca hizmet sağlayıcı, sipariş verilmeden önce alıcıya, veri giriş hatalarını belirleyebilmesi ve düzeltebilmesi için uygun, etkili ve erişilebilir teknik araçları sunar (ETDHK m. 4/2). Tarafların tüketici olmadığı hâllerde, bu düzenlemelerin aksi kararlaştırılabilir.

Münhasıran elektronik posta yoluyla veya benzeri bireysel iletişim araçlarıyla yapılan sözleşmelerde, bu şekilde kurulan sözleşmelerin niteliği gereği, hizmet sağlayıcısının sözleşme şartlarını alıcı tarafından açıkça görülmesini sağlama yükümlülüğü bulunmamaktadır (ETDHK m. 4/4).

ETDHK'nın 9. maddesinde hukuka aykırı içeriğe ilişkin sorumluluğun belirlenmesi hususu düzenlenmiştir. Bu madde 01.07.2022 tarihinde yapılan değişiklik ile Kanuna eklenmiştir. Hukuka aykırı içerikten doğan sorumluluk bakımından ayrıntılar ileride değinilecek olan “Elektronik Ticaret Aracı Hizmet Sağlayıcı ve Elektronik Ticaret Hizmet Sağlayıcılar Hakkında Yönetmelik (Hizmet Sağlayıcılar Yönetmeliği)” ile düzenlenmiştir. Buna göre; diğer kanunlarda aksine hüküm bulunmadıkça, (elektronik ticaret) aracı hizmet sağlayıcı, (elektronik ticaret) hizmet sağlayıcı tarafından sunulan içerik ve içeriğe konu mal veya hizmetle ilgili hukuka aykırı hususlardan sorumlu değildir (ETDHK m. 9/1, Hizmet Sağlayıcılar Yönetmeliği m. 10/1). Bununla birlikte, elektronik ticaret aracı hizmet sağlayıcı, elektronik ticaret hizmet sağlayıcı tarafından sunulan içeriğin hukuka aykırı olduğundan haberdar olur ise bu içeriği, **kırk sekiz saati geçmemek üzere**, gecikmeksizin yayımdan kaldırarak hukuka aykırı hususu, elektronik ticaret hizmet sağlayıcısı ve ilgili kamu kurum ve kuruluşlarına bildirir. Hizmet Sağlayıcıları Yönetmeliği m. 10/3 hükmüne göre; yargı mercilerinin hukuka aykırı içeriğe ilişkin kararının ETAHS'ye bildirilmesi gibi durumların yanı sıra Bakanlığın ya da görev alanlarına giren konularda diğer kamu kurum ve kuruluşlarının hukuka aykırı içerik bildiriminde bulunması durumunda ETAHS'nin hukuka aykırı içerikten haberdar olduğu kabul edilir. Ayrıca, hak sahibinin fikri ve sınai mülkiyet hakkı ihlaline dair bilgi ve belgeye dayanan şikâyeti üzerine, elektronik ticaret aracı hizmet sağlayıcı tarafından hukuka aykırı içeriğin kaldırılacağı; elektronik ticaret hizmet sağlayıcının, şikâyetin aksini gösteren bilgi ve belgeye dayanan itirazını elektronik ticaret aracı hizmet sağlayıcıya sunması üzerine şikâyete konu ürünü yeniden yayımlayacağı düzenlenmiştir (ETDHK m. 9/3).

ETDHK'nın 11. maddesinde Bakanlık yetkileri düzenlenmiştir. Bakanlık, kanunun uygulanmasını ve elektronik ticaretin gelişimini sağlamaya, etkin ve adil rekabet ortamını korumaya, hizmet sağlayıcı ve aracı hizmet sağlayıcının faaliyetlerine yönelik düzenleme yapmaya ve aracılık sözleşmesinde yer

verilmesi zorunlu unsurları belirlemeye yetkilidir. Ayrıca Bakanlık, bu Kanunun uygulanmasını sağlamak amacıyla denetim yapmaya ve denetim sonuçlarını açıklamaya, denetim sırasında özel uzmanlık veya teknik bilgi gerektiren durumlarda bilirkişi görevlendirmeye, bilirkişinin hak ve yükümlülükleri ile görevlendirilmesine ilişkin usul ve esasları yönetmelikle belirlemeye yetkilidir. Bakanlığın yetkilediği personel tarafından yapılan denetim sırasında, denetimin sınırları dahilinde, elektronik ortamda tutulanlar da dahil her türlü bilgi, belge ve defterler incelenebilir. Aracı hizmet sağlayıcı ve hizmet sağlayıcı, ETDHK kapsamındaki iş ve işlemlerine ilişkin bilgi, belge, defter ve elektronik kayıtlarını, iş veya işlemin gerçekleştiği tarihten itibaren on yıl süreyle saklamakla yükümlüdür (ETDHK m. 11/3). Kanuna aykırılık hâlinde uygulanacak cezai yaptırımlar, ETDHK'nın 12. maddesinde ayrıntılı olarak düzenlenmiştir.

Elektronik Ticaret Aracı Hizmet Sağlayıcı ("ETAHS") ve Elektronik Ticaret Hizmet Sağlayıcı ("ETHS") Hakkındaki Düzenlemeler

Elektronik ticaret aracı hizmet sağlayıcı ve elektronik ticaret hizmet sağlayıcı kavramları, 1.7.2022 yılında yapılan ek ile ETDHK'da yerini almıştır. Bu Kanuna dayanarak 29.12.2022 tarihli ve 32058 sayılı Resmî Gazete'de "Elektronik Ticaret Aracı Hizmet Sağlayıcı ve Elektronik Ticaret Hizmet Sağlayıcılar Hakkında Yönetmelik (Hizmet Sağlayıcılar Yönetmeliği)" yayımlanmıştır. Hizmet Sağlayıcıları Yönetmeliği'nin amacı, etkin ve adil rekabet ortamının tesis edilmesini ve elektronik ticaretin gelişiminin sağlanmasını teminen elektronik ticaret aracı hizmet sağlayıcı ve elektronik ticaret hizmet sağlayıcıların faaliyet ve denetimleri ile bunlar arasındaki ticari ilişkilerin düzenlenmesine yönelik usul ve esasları belirlemektir. Yönetmelik, elektronik ticaret aracı hizmet sağlayıcı ve elektronik ticaret hizmet sağlayıcıların yükümlülüklerini, elektronik ticarete haksız ticari uygulamaları, hukuka aykırı içeriği, aracılık sözleşmesini, elektronik ticaret lisansını ve elektronik ticaretle ilgili diğer hususları kapsar. Kapsam dışında bırakılan hususlar, Hizmet Sağlayıcıları Yönetmeliği'nin 2. maddesinin 2. fıkrasında sayılmıştır. Buna göre; bireysel emeklilik, bankacılık, sigortacılık, finansman, sermaye piyasası, ödeme hizmetleri, bahis ve şans oyunları, seyahat acenteliği, sivil havacılık, ile elektronik haberleşme alanlarında faaliyet gösteren işletmelerin elektronik ticaret aracı hizmet sağlayıcı veya elektronik ticaret hizmet sağlayıcı olarak kabul edilmez. Hizmet Sağlayıcıları Yönetmeliği'nde ETHAS ve ETHS'ler net işlem hacimlerine göre orta ölçekli, büyük ölçekli ve çok büyük ölçekli olmak üzere üç gruba ayrılmıştır.

Hizmet Sağlayıcıları Yönetmeliği'nin 5. maddesinde, ETHS'nin bilgi verme yükümlülüğü düzenlenmiştir. Bilgi verme yükümlülüğü, kendine ait elektronik ortamı olan ETHS, elektronik ticaret pazar yerinde satış yapan ve tacir veya esnaf ve sanatkâr olan ETHS ve elektronik ticaret pazar yerinde satış yapan ve tacir veya esnaf ve sanatkâr olmayan ETHS'ler için ayrı ayrı düzenlenmiştir. Hizmet Sağlayıcıları Yönetmeliği'nin 6. maddesinde, ETAHS'nin bilgi verme ve doğrulama yükümlülüğü düzenlenmektedir. ETHAS hem kendisiyle ilgili maddede sayılan bilgileri elektronik ticaret pazar yerinde bulundurmak hem de pazar yerinde faaliyet gösteren ETHS'lerin bilgilerini pazar yerinde göstermesi ve güncellemesini mümkün kılan altyapıyı sunmak ve bu bilgileri doğrulamakla yükümlüdür. Hizmet Sağlayıcıları Yönetmeliği'nin 7. maddesiyle, ETHAS ve ETHS'lerin faaliyet gösterdiği elektronik ortamın ana sayfasında belirli hususları içeren işlem rehberinin bulunması zorunluluğu getirilmiştir. Madde 8'de siparişe ilişkin yükümlülükler ve madde 9'da siparişin teyidine ilişkin hem ETHAS hem de ETHS için çeşitli yükümlülükler getirilmiştir.

Elektronik Ticarete Haksız Ticari Uygulamalar

Bir ticari uygulamanın, mesleki özenin gereklerine uymaması, yöneldiği grubun ortalama üyesinin bir mal ya da hizmete yönelik davranış biçimini önemli ölçüde etkilemesi veya etkileme ihtimalinin olması hâlinde haksız olduğu kabul edilir. Aldatıcı veya saldırgan nitelikteki ticari uygulamaların haksız olduğu kabul edilmiş ve haksız ticari uygulamalar yasaklanmıştır. ETDHK'na 2022 yılında eklenen Ek Madde-1 ile elektronik ticarete haksız ticari uygulamada bulunulamayacağı ifade edilmiş ve haksız ticari uygulama örneklerine yer verilmiştir.

Hizmet Sağlayıcılar Yönetmeliği'nin 11. maddesinde de ETAHS'nin, aracılık hizmeti sunduğu ETHS'nin ticari faaliyetlerini önemli ölçüde bozan, makul karar verme yeteneğini azaltan veya belirli bir kararı almaya zorlayarak normal şartlarda taraf olmayacağı bir ticari ilişkinin tarafı olmasına sebep olan uygulamalarının haksız olduğu kabul edileceği belirtilmiştir. Maddenin devamında haksız ticari uygulama örneklerine yer verilmiştir.

Elektronik Ticaret Lisansı

Hizmet Sağlayıcılar Yönetmeliği m. 30 vd. hükümlerine göre; belirli hadleri aşan ETAHS ve ETHS'lerin faaliyetlerine devam edebilmeleri için Ticaret Bakanlığı'ndan lisans almaları ve lisanslarını yenilemeleri zorunludur. Bir takvim yılındaki net işlem hacmi on milyar Türk lirasının ve iptal ve iadeler hariç işlem sayısı yüz bin adedin üzerinde olan ETAHS, büyük ölçekli ve çok büyük ölçekli ETAHS ile orta, büyük ve çok büyük ölçekli olup toplam satış hasılatının yarısından fazlasını elektronik ticaret satışlarından elde eden ETHS, faaliyetine devam edebilmek için Bakanlıktan lisans almak ve lisansını yenilemek zorundadır (Hizmet Sağlayıcılar Yönetmeliği m. 30/1). Lisans alma başvurusu, hadlerin aşıldığı yılı izleyen takvim yılının, lisans yenileme başvurusu ise eşikler aşıldığı sürece her takvim yılının Mart ayı içinde ETBİS üzerinden yapılır (Hizmet Sağlayıcılar Yönetmeliği m. 30/2). Lisans ücreti Bakanlığın internet sitesinde ilan edilen hesap numarasına peşin olarak yatırılır (Hizmet Sağlayıcılar Yönetmeliği m. 30/3). Tahsil edilen tutarlar genel bütçeye gelir kaydedilir. Lisans ücretinin ödendiğine dair belge, lisans alma veya yenileme başvurusu sırasında ETBİS'e yüklenir (Hizmet Sağlayıcılar Yönetmeliği m. 30/4). Elektronik ticaret lisansı başvurusunun sonuçlandırılması ise Yönetmelik'in 31. maddesinde ayrıntılı olarak düzenlenmiştir.

Ticari Elektronik İletilere İlişkin Düzenleme

İşletmelerin iş hacmini genişletmesini, daha fazla müşteriye ulaşabilmesi, kârlılığını artırabilmesi adına, faaliyetlerini tanıtması ve reklamını yapması önem arz etmektedir. Bu kapsamda, işletmelerin çeşitli kanallardan potansiyel müşterilerine ticari amaçlarla elektronik ileti göndermesi giderek yaygınlaşmaktadır. Zamanla elektronik ticari iletilerin kontrolsüz ve aldatıcı olarak gönderilmesi, muhatapların adeta pazarlama bombardımanına tutulmasına yol açmıştır. Dolayısıyla, elektronik ticari ileti gönderilmesinde, işletmelerin faaliyetlerini genişletmek amacıyla bireylerin elektronik ortamda rahatsız edilmeme hakkı arasında bir denge kurulması ihtiyacı doğmuştur. Ticari iletilere ilişkin temel konu, bireylerin elektronik ortamda rahatsız edilmemesini sağlamaktır. Bu anlamda, kişilere yalnızca

tercih ettikleri elektronik iletişim aracıyla ve özel olarak izin vermiş oldukları gerçek ve tüzel kişiler tarafından ticari amaçlarla ileti gönderilmesi kabul edilmektedir. Ticari elektronik ileti, tüketici hukuku, haksız rekabet, ceza hukuku, reklam kuralları gibi birçok konuyla yakından ilgilidir. Ticari elektronik iletileri düzenleyen temel kanun, ETDHK bu kanuna dayanarak çıkarılan “Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik (E-İleti Yönetmeliği)” ve diğer ikincil düzenlemelerdir.



DİKKAT EDELİM

Bireyin isteği olmadan ve çoğunlukla güvenilir olmayan adreslerden gönderilen iletilere “SPAM” denilmektedir. Bu iletiler, elektronik ticari iletiler ile adeta bıçak sırtı konumdadır. “SPAM” gönderilmesi hukuka aykırıdır. Öte yandan, yasal gereklikler çerçevesinde ticari elektronik iletilerin gönderilmesinde herhangi bir hukuka aykırılık bulunmamaktadır.

ETDHK’ya göre, ticari elektronik iletiler, kural olarak, alıcılara ancak önceden onayları alınmak şartıyla gönderilebilir. Bu kuralın istisnaları da vardır. Bunlardan ilki, kendisiyle iletişime geçilmesi amacıyla alıcının iletişim bilgilerini vermesi hâlinde, temin edilen mal veya hizmetlere ilişkin değişiklik, kullanım ve bakıma yönelik ticari elektronik iletiler için ayrıca onay alınmaz. İkinci istina; devam eden abonelik, üyelik veya ortaklık durumu ile tahsilat, borç hatırlatma, bilgi güncelleme, satın alma ve teslimat veya benzeri durumlara ilişkin bildirimleri içeren iletiler ile hizmet sağlayıcıya ilgili mevzuatla getirilen bilgi verme yükümlülüğü durumlarında önceden onay alma zorunluluğu aranmaz. Ancak bu tür bildirimlerde herhangi bir mal veya hizmet özendirilemez veya bunların tanıtımı yapılamaz. Onay gerektirmeyen bir diğer durum ise esnaf ve tacirlere ticari elektronik ileti gönderilmesidir. Burada bir konuya dikkat etmek gerekir ki, sırf bu düzenleme dikkate alındığında esnaf ve tacirlere herhangi bir sınır olmaksızın ticari elektronik ileti gönderilebileceği gibi bir anlam çıkabilir. Ancak bu hükmü “Kişisel Verilerin Korunması Kanunu (KVKK)” ile birlikte yorumlamak gerekir. Zira, KVKK’ya göre, yalnızca kanunda sayılan hukuki sebeplerin varlığı hâlinde kişisel veriler işlenebilir. Aksi hâlde, kanuna aykırı olarak veri işleyen sorumluluğu gündeme gelir. Yani, gerçek kişi esnaf veya tacire, hukuki bir sebep olmadan rızası dışında elektronik ileti gönderilmesi de KVKK uyarınca mümkün değildir. Son olarak, sermaye piyasasına ilişkin mevzuat uyarınca aracılık faaliyetinde bulunan şirketlerce müşterilerine bilgilendirme amaçlı gönderilen ticari elektronik iletiler için onay alınması zorunlu değildir.

Ticari elektronik ileti gönderimine ilişkin onay alınması, muhatabın iletiyi reddetme hakkını kullanması veya ileti gönderen hakkından şikâyet süreçlerinin yönetilmesi için “ticari elektronik ileti yönetim sistemi (İYS)” kurulmuştur. Ticari ileti göndermek isteyen gerçek ve tüzel kişiler İYS’ye kaydolar. İYS üzerinde onayı bulunmayan alıcılara ticari elektronik ileti gönderilemez. Hizmet sağlayıcının, mal ve hizmetlerini tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içerikler-

le tanınırlığını artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderdiği ticari elektronik iletiler için kendisi tarafından ya da İYS üzerinden önceden onay alınır (E-İleti Yönetmeliği m. 10/A).

Elektronik ticari ileti göndermek için gereken onay yazılı olarak veya her türlü elektronik iletişim araçlarıyla ya da İYS üzerinden alınabilir. Ticari elektronik iletinin içeriği, alıcıdan alınan onaya uygun olmalıdır. Yani, izin alınan içerikten farklı bir ileti gönderilmesi hukuka aykırıdır. İletide, hizmet sağlayıcının tanınmasını sağlayan bilgiler ile haberleşmenin türüne bağlı olarak telefon numarası, faks numarası, kısa mesaj numarası ve elektronik posta adresi gibi erişilebilir durumdaki iletişim bilgileri yer alır. İletide, haberleşmenin türüne bağlı olarak, iletinin konusu, amacı ve başkası adına yapılması hâlinde kimin adına yapıldığına ilişkin bilgilere de yer verilir. Acentelik, özel yetkili işletme ya da bayilik sözleşmesindeki taraflardan birine verilen onay; bu sözleşmeye konu mal, hizmet veya marka ile sınırlı olarak sözleşmenin diğer tarafı için de verilmiş kabul edilir. Hizmet sağlayıcı aldığı onayı, kendi mal veya hizmetleri ile birlikte olmak kaydıyla promosyon olarak sunulan mal ve hizmetler için de kullanabilir. Ancak bu promosyon ilişkisinin bir sözleşmeye bağlı olma şartı aranır. Hizmet sağlayıcı, alıcıdan ticari elektronik ileti onayı vermesini, sunduğu mal ve hizmetin temini için ön şart olarak ileri süremez. İYS üzerinden alınmayan onaylarda, onayın alındığına ilişkin ispat yükümlülüğü hizmet sağlayıcıya aittir. İYS üzerinden alınmayan onaylar, hizmet sağlayıcı tarafından üç iş günü içinde İYS'ye kaydedilir. İYS'ye kaydedilmeyen onaylar geçersiz kabul edilir.

ETDHK'da, alıcıların elektronik iletiyi reddetme hakkı tanınmıştır. Bu hakkın alıcıya aktif bir şekilde sağlanması önem arz eder. Alıcılar diledikleri zaman, hiçbir gerekçe belirtmeksizin ticari elektronik iletileri almayı reddedebilir. Hizmet sağlayıcı ret bildiriminin, elektronik iletişim araçlarıyla kolay ve ücretsiz olarak iletilmesini sağlamakla ve gönderdiği iletime buna ilişkin gerekli bilgileri sunmakla yükümlüdür. Ret bildirimi imkânı, gönderilen her ticari elektronik iletime yer alır. Talebin ulaşmasını müteakip hizmet sağlayıcı üç iş günü içinde alıcıya elektronik ileti göndermeyi durdurur.

Elektronik ticari iletilere ilişkin şikâyet konusu işlemlerde ispat yükümlülüğü hizmet sağlayıcıya ve/veya aracı hizmet sağlayıcıya aittir. Hizmet sağlayıcı ve/veya aracı hizmet sağlayıcı onay kayıtlarını, onayın geçerliliğinin sona erdiği tarihten, ticari elektronik iletilere ilişkin diğer kayıtları ise kayıt tarihinden itibaren üç yıl süreyle saklar.

Ticaret Bakanlığı (Bakanlık), hizmet sağlayıcı, aracı hizmet sağlayıcı ve Kuruluşun bu Yönetmelik kapsamında gerçekleştirdiği faaliyet ve işlemlerini denetlemeye yetkilidir. Bakanlıkça görevlendirilen denetim elemanları, bu Yönetmelik kapsamında Bakanlık yetkisine giren hususlarla ilgili olarak her türlü bilgi, belge ve defterleri istemeye, bunları incelemeye ve örneklerini almaya, ilgililerden yazılı ve sözlü bilgi almaya yetkilidir. İlgililer istenilen bilgi, belge ve defterler ile elektronik kayıtlarını, bunların örneklerini noksansız ve gerçeğe uygun olarak vermek, yazılı ve sözlü bilgi taleplerini karşılamak ve gerekli yardım ve kolaylığı göstermekle yükümlüdür. Bakanlıkça görevlendirilen denetim elemanları, ticari elektronik iletileri gönderen hizmet sağlayıcı ve aracı hizmet sağlayıcının abonelik bilgileri ile gerekli bilgi ve belgeleri ilgili diğer kamu kurum ve kuruluşları ile elektronik haberleşme hizmeti sunan işletmecilerden istemeye yetkilidir.

E-İleti Yönetmeliği'ne aykırı hareket edenler hakkında ETDHK'nın 12. maddesi uyarınca uygulanacak idari para cezalarını vermeye, hizmet sağlayıcı ve aracı hizmet sağlayıcının sicile kayıtlı merkezinin bulunduğu yerdeki il müdürü yetkilidir. Verilen idari para cezaları, tebliğ tarihinden itibaren bir ay içinde ödenir.

Elektronik Sözleşme

ETDHK’da elektronik sözleşmeye ilişkin açıkça bir tanımlama yer almamaktadır. Bununla birlikte, elektronik iletişim araçlarıyla yapılan sözleşmelerin kanun kapsamında olduğu belirtilmiştir (ETDHK m. 1/2). Elektronik sözleşme yeni bir sözleşme türü olmayıp iki veya daha fazla tarafın bir elektronik iletişim aracı vasıtasıyla kurdukları sözleşmeleri ifade eden şemsiye bir kavramdır. Başka bir ifadeyle elektronik sözleşme, geleneksel bir sözleşmenin elektronik ortamda yapılmasıdır. Dolayısıyla, elektronik sözleşmenin kuruluşuna, geçerliliğine ve ifasına ilişkin hususlarda niteliğine uygun düştüğü ölçüde “6098 sayılı Türk Borçlar Kanunu (RG, 04.02.2011, S. 27826) (TBK)”nda yer alan hükümler uygulanır.



DİKKAT EDELİM

Elektronik sözleşme, yeni bir sözleşme tipi değildir.

Geleneksel bir sözleşmenin kuruluşundan ifasına kadar tüm aşamalarının internet üzerinden gerçekleştirilmesi hâlinde olduğu gibi taraflar arasındaki sözleşmenin internet üzerinden kurulup karşılıklı edimlerin birinin ya da tamamının fiziki ortamda gerçekleşmesi hâlinde de elektronik sözleşmenin varlığından bahsedilir. Örneğin, elektronik kitap, elektronik dergi, çevrimiçi psikolojik danışmanlık gibi sözleşmeler ile bir yazılımın indirilmesi (*download*) gibi işlemlerde hem sözleşmenin kuruluşu hem de karşılıklı edimlerin ifası internet üzerinden gerçekleşir. Öte yandan internet üzerinden malın kargo ya da kurye ile gönderilmesi, internet sitesi veya mobil uygulamalar aracılığıyla araç kiralınması, Armut gibi uygulamalardan alınan temizlik hizmetlerinin ifası fiziki ortamda gerçekleşir; bu sözleşmelerin yalnızca kuruluşu internet üzerinden yapılır.

Dikkat edilmesi gereken önemli bir husus, elektronik ortamda gerçekleştirilen her türlü işlemin elektronik sözleşme olmadığıdır. Örneğin, internet siteleri üzerinden bedelsiz olarak altın ve döviz kurları, hava durumu, haber gibi bilgilerin paylaşılması hâlinde elektronik sözleşmeden söz edilemez.



DİKKAT EDELİM

Elektronik ortamda yapılan her işlem elektronik sözleşme değildir.

Elektronik Sözleşmelerin Kuruluşunda Kullanılan Yöntemler

Elektronik sözleşmeler de tıpkı geleneksel sözleşmeler gibi tarafların iradelerini karşılıklı ve birbirine uygun açıklamasıyla kurulur (TBK m. 1). Sözleşmenin kurulmuş sayılabilmesi için tarafların sözleşmenin esaslı unsurları üzerinde anlaşmış olması gerekli ve yeterlidir (TBK m. 2). Tarafların irade açıklaması açık ya da örtülü olabilir (TBK m. 1/2). İradelerini elektronik ortamda açıklayan taraflar, telefon, teleks, faks, internet, EDI, e-posta gibi iletişim araçlarından yararlanabilirler. Bu kapsamda aşağıda, elektronik ticarete en yaygın olarak kullanılan iletişim araçlarıyla ilgili açıklamalara yer verilmektedir.

- **EDI Aracılığıyla Kurulan Elektronik Sözleşmeler**

EDI, işletmeler arası hızlı haberleşmenin sağlanabilmesi için, herhangi bir insan müdahalesi olmadan bilgisayarlar arası veri değişim sistemidir. Veri değişimi sırasında insan müdahalesi olmadığından, diğer bir deyişle, EDI “kişi” sıfatını haiz olmayan bir bilgisayar programı olduğundan, EDI aracılığıyla bir irade açıklamasından bahsedilemeyeceği düşünülebilir. Öte yandan EDI, daha önceden tarafların verdiği komutlar dahilinde karşı tarafa ileti gönderir. Başka bir deyişle, taraflar arasında sözleşmenin şartlarında önceden anlaşmıştır. Dolayısıyla, EDI aracılığıyla kurulan sözleşmelerde de tarafların karşılıklı ve birbirine uygun irade açıklamalarından söz edilebilir.

EDI çoğunlukla işletmeler arası kullanıldığından, EDI aracılığıyla kurulan sözleşmelerle B2B elektronik ticarete karşılıklıdır. EDI, işletmeler arası standartlaşmış siparişlerin, faturaların ve sair bilgi ve belgelerin hızlı bir şekilde değiş tokuşunu sağlar.

- **E-Posta Aracılığıyla Kurulan Elektronik Sözleşmeler**

E-posta, geleneksel yollarla gönderilen postanın elektronik ortamdaki karşılığıdır. Her kullanıcının ileti göndermek ve almak için birer e-posta adresi bulunur. Böylelikle tarafların karşılıklı olarak gönderecekleri e-postalarda sözleşmenin esaslı noktaları üzerinde anlaşmaları hâlinde sözleşme kurulmuş olur. E-posta yoluyla kurulan elektronik sözleşmeler, B2B, B2C, C2C şeklinde olabilir.

- **İnternet Sitesi, Mobil Uygulamalar ve Sanal Pazar Yerleri Aracılığıyla Kurulan Elektronik Sözleşmeler**

Günümüzde elektronik sözleşmelerin kuruluşunda en yaygın yöntemler; internet siteleri, mobil uygulamalar ve çevrimiçi platformlardır. Bir kişi ya da işletme, kendisine ait bir internet sitesi üzerinden mal veya hizmetlerini sunup reklam faaliyetlerini yürütebilir. İnternet sitesi üzerinden yalnızca tanıtım yapılmadığı durumlarda, yani mal satışı ya da hizmet sağlandığı durumlarda elektronik sözleşmeden söz edilir.

İnternet sitesi aracılığıyla sözleşme kurulması, yalnızca kişilerin ve işletmelerin kendilerine ait internet siteleri veya mobil uygulama üzerinden mal satışı veya hizmet sağlanması ile sınırlı değildir. Sanal pazar yerleri olarak da adlandırılan çevrimiçi platformlar da esasen bir internet sitesi aracılığıyla birden fazla satıcı veya sağlayıcının mal ve hizmetlerini alıcılarla buluşturmaktadır. Farklı türlerde sanal pazar yerleri mevcuttur. Örneğin, mesleki ve ticari amaçlarla hareket etmeyenler arasında teklifte bulunma ve sipariş verme gibi işlemlerin yapıldığı sanal pazar yerlerine örnek olarak, “*Couchsurfing, Airbnb, BlaBlaCar, Sahibinden, Dolap*” gibi platformlar sayılabilir. “*Trendyol, Morhipo, Amazon*” gibi platformlar, mesleki ve ticari amaçlarla hareket edenler ile bireysel amaçlarla hareket edenlerin karşılıklı sözleşme ilişkisine girdiği platformlara örnek olabilir. Bunlara ek olarak, mesleki ve ticari amaçlarla hareket edenleri bir araya getiren Alibaba.com gibi platformlar da vardır. Yapılan başka bir ayrıma göre, çevrimiçi pazar yerlerinin bir kısmı yalnızca sözleşmenin taraflarını bir araya getirir. Başka bir deyişle, bu hâlde çevrimiçi platform yalnızca aracılık hizmeti görmektedir. Öte yandan, elektronik sözleşmenin çevrimiçi pazar yeri üzerinden kurulması da mümkündür.

- **Elektronik Temsilci Aracılığıyla Kurulan Elektronik Sözleşmeler**

Elektronik temsilci, insan müdahalesi olmaksızın herhangi bir işlemi başlatabilen, elektronik iletileri cevaplayabilen bir yazılımdır. Elektronik temsilci ile kurulan sözleşmelerde de, tıpkı EDI ile kurulan sözleşmelerde olduğu gibi, sözleşmenin taraflarının irade beyanları, sözleşme kurulmadan önce kodlanmaktadır. Dolayısıyla, elektronik temsilci otonom bir şekilde yani kendiliğinden karar almamakta, yalnızca önceden belirlenen taraf iradesini ortaya koymaktadır.

Elektronik Sözleşmenin Kurulması

Sözleşmenin karşılıklı ve birbirine uygun irade açıklamalarıyla kurulacağı, çeşitli vesilelerle ifade edilmiştir. Bu kapsamda, irade açıklamalarından zaman olarak önce olanı öneridir. Öneri, bir sözleşme kurmak isteyen tarafın bu yöndeki iradesini karşı tarafa açıklamasıdır. Bir irade açıklamasının öneri olarak kabul edilebilmesi için, sözleşmenin esaslı unsurlarını içermeli; önerenin bağlanma iradesi olması ve önerisinde ciddi olması gerekir. Bu anlamda, öneren önerisi ile bağlı olma niyetinde değil ise yalnızca sözleşme hükümleri üzerinde müzakere amacı taşıyorsa o hâlde “öneriye davet” söz konusu olur.

Öneren, önerisi ile bağlı olmama hakkının saklı olduğunu açıkça belirtmemişse ya da işin özelliğinden veya durumun gereğinden bağlanma niyetinde olmadığı anlaşılmıyorsa, öneren önerisiyle bağlıdır (TBK m. 8/1). İnternet sitesi üzerinden fiyatını göstererek mal sergilenmesi aksi açıkça ve kolaylıkla anlaşılmadıkça öneri sayılır (TBK m. 8/2). Muhatabın öneriyi kabulüyle sözleşme kurulur. Kabul beyanı açık veya örtülü olabilir. Öneren, kanun veya işin özelliği ya da durumun gereği açık bir kabulü beklemek zorunda değilse, öneri uygun bir sürede reddedilmediği takdirde, sözleşme kurulmuş sayılır (TBK m. 6/1).

Öneri ve kabul beyanlarının açıklanması ve karşı tarafa varması sözleşmenin kurulması ile hüküm ve sonuçlarını doğurduğu anın tespiti bakımından önem taşır. Bu noktada, hazırlar arası yapılan sözleşme ve hazır olmayanlar arası yapılan sözleşme ayrımına dikkat etmek gerekir. Bir sözleşmenin hazırlar arasında veya hazır olmayanlar arasında olduğunun belirlenmesinde temel etken, tarafların aynı ortamda bulunup bulunmadığı değil, taraflar arası iletişimin doğrudan sağlanıp sağlanmadığıdır. Hazırlar arası sözleşmede, sözleşmenin kurulması ile sözleşmenin hüküm ve sonuçlarını doğurması aynı anda gerçekleşir. Hazır olmayanlar arasında sözleşme, kabul beyanının karşı tarafa varmasıyla kurulur ancak kabulün gönderildiği andan başlayarak hüküm doğurur. Açık bir kabulün gerekli olmadığı durumlarda, sözleşme önerinin ulaşma anından başlayarak hüküm doğurur (TBK m. 11).

Elektronik sözleşmede irade açıklamalarının hazırlar arasında olup olmadığının tespiti, tarafların ne şekilde iletişim kurduklarıyla yakından ilgilidir. Nitekim, TBK m. 4/2'e göre telefon, bilgisayar gibi iletişim sağlayabilen araçlarla doğrudan iletişim sırasında yapılan öneri, hazır olanlar arasında yapılmış sayılır. Dolayısıyla, elektronik sözleşmenin kuruluşunda taraflar her ne kadar fiziksel olarak bir arada bulunmasa da taraflar arasındaki iletişim doğrudan ise hazırlar arasında sözleşmeden bahsedilebilir. Öte yandan, taraflar arasında doğrudan ve kesintisiz bir iletişim söz konusu değilse, başka bir deyişle taraflardan birinin iradesini açıkladığı an ile karşı tarafın bu irade açıklamasını öğrendiği an birbirinden farklı ise bu hâlde hazır olmayanlar arasında yapılan sözleşmeden bahsedilir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Chatbot (sohbet robotu) aracılığıyla kurulan sözleşme, hazır olanlar arası kurulan elektronik sözleşmedir.

**DİKKAT EDELİM**

İki işletme arasında mal tedarikine ilişkin sözleşmenin e-posta yoluyla yapılması hâli, hazır olmayanlar arasındaki elektronik ticarete örnektir.

İnternet sitesi üzerinden yapılan elektronik sözleşmelerde, satıcının malı göndermesi veya paranın alıcının hesabından çekilmesiyle sözleşme kurulmuş sayılabilir. Sözleşme konusunun dijital bir ürün olduğu hâllerde de ürünün indirilmesiyle sözleşme kurulmuş olur. Elektronik pazar yeri aracılığıyla verilen bir sipariş örneğinde, ödeme bilgileri alındıktan sonra bir süre kullanıcının ekranında “onay bekleniyor” ifadesi yer alır. Elektronik pazar yeri üzerinden faaliyette bulunan satıcı, bu süre içerisinde stoklarını kontrol eder. Bu sürede satıcı sözleşmeyi onaylayabilir ya da reddedebilir. Bu örnekte ise sözleşme, satıcının kabulüyle kurulur.

Hazır olmayanlar arasındaki elektronik sözleşmelerde, irade beyanının gönderilme anı ile varma anının tespiti önem taşımaktadır. Bir irade beyanının gönderilmesi, o beyanın muhataba erişmek üzere beyanda bulunanın hâkimiyet alanından çıkması anlamına gelir. Elektronik ileti, gönderenin posta kutusundan ya da sunucusundan (*server*) çıktığında hakimiyet alanından çıkmış olur. Varma anı, irade beyanının muhatabın hakimiyet alanına varması anıdır. İnternet üzerinden açıklanan iradelerde genel kanı, muhatabın erişimine imkân sağlayacak şekilde muhatabın sunucusuna kaydedildiği anda, irade açıklamasının varmış olduğu kabul edilir. Bu anlamda, elektronik posta yoluyla açıklanan iradenin varma anıyla öğrenme anı birbirinden farklı olabilir.

**GÜNLÜK HAYATLA İLİŞKİLENDİRELİM**

Kabul beyanının elektronik posta ile açıklanması hâlinde, e-postanın kabul iradesini açıklayanın posta kutusundan çıktığı an gönderilme anı, muhatabın posta kutusuna ulaştığı an varma anı, muhatap tarafından açıldığı an öğrenilme anı olur.

Borçlar hukukuna hâkim olan sözleşme özgürlüğü ilkesi, sözleşmenin şekli konusunda da geçerlidir. Başka bir deyişle, tarafların bir sözleşmeyi belirli bir şekilde yapma zorunluluğu kural olarak öngörülmemiştir. Bununla birlikte bazı sözleşmelerin geçerliliği, sözleşmenin kanunda ya da taraf iradelerince belirlenen şekilde yapılmasına bağlıdır. Bu hâlde şekil, geçerlilik koşuludur. Öngörülen şekle uyulmaksızın kurulan sözleşmeler hüküm doğurmaz (TBK m. 12/2). TBK uyarınca yazılı şeklin metin ve imza olmak üzere iki unsuru vardır. İmzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza da el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur (TBK m. 15). Böylelikle yazılı olarak yapılması öngörülen sözleşmeler, güvenli elektronik imza ile elektronik ortamda yapılabilir.

Elektronik sözleşmeler, sözleşme özgürlüğü çerçevesindedir ancak her özgürlük gibi sözleşme özgürlüğünün de sınırları vardır. Bu anlamda, konusu emredici hukuk kurallarına, kişilik haklarına, kamu düzenine, genel ahlaka aykırı olmamak şartıyla ve sözleşmenin konusunun imkânsız olmaması ile tarafların iradelerinin sakatlanmış olmaması halinde elektronik sözleşme kurulabilir.

Elektronik Ticarete Tüketicinin Korunması

Daha önce çeşitli vesilelerle değinildiği üzere, elektronik ticarete kurulan sözleşmeler, günümüzde çoğunlukla internet aracılığıyla akdedilmektedir. İnternet üzerinden akdedilen sözleşmelerin büyük bir kısmını da tüketici işlemleri oluşturmaktadır. Gerçekten de hızlilik, pratiklik, ucuzluk, aynı anda birden fazla seçeneği görüp kıyaslayabilme olanağı gibi çeşitli etkenler, tüketicileri mağazadan almak yerine internet üzerinden işlem yapmaya teşvik etmektedir. Bununla birlikte elektronik ticarete tüketiciler, internet sitelerinde gerçeğe aykırı açıklamalar, hileli davranışlar, yanıltıcı reklamlar, eksik veya hatalı yapılan bilgilendirmeler, kişisel verilerin toplanma amacına uygun olmayan şekilde kullanılması, sipariş, ödeme ve teslim aşamalarında yaşanan aksaklıklar gibi sorunlarla karşı karşıya kalmaktadır. Özetle, güvenlik sorunları, bilgi eksikliği, bilgi kirliliği, denetimin yetersiz oluşu gibi sebepler, tüketici açısından dezavantaj yaratmaktadır. Bu sebeplerle, elektronik sözleşmelerde zayıf konumunda olan tüketicinin etkin bir şekilde korunması ve elektronik ticaretin düzenlemesine duyulan ihtiyaç da artmıştır.

Türk hukukunda tüketicilerin korunmasına ilişkin temel mevzuat “6502 sayılı Tüketicinin Korunması Hakkındaki Kanun (RG, 28.11.2013, S. 28835) (TKHK)”dur. Bu Kanun ile borçlar hukukumuzun temel prensiplerinden biri olan “sözleşme özgürlüğü” ilkesi tüketiciler lehine devlet eliyle sınırlandırılmıştır. Şöyle ki, hukukumuzda bir sözleşmenin tarafları, sözleşmenin içeriğini belirlemede kanunda öngörülen sınırlar içerisinde kalmak kaydıyla özgürdür (TBK m. 26). Bu ilke, kuşkusuz, tarafların eşit konumda olduğu ve sözleşme şartları üzerinde karşılıklı olarak müzakere edebildiği hâllerde uygulama alanı bulur. Öte yandan, tarafların eşit olmadığı hâllerde sözleşmenin zayıf konumunda bulunan tarafının devlet eliyle korunması ihtiyacı ortaya çıkar.

TKHK, genel olarak tüketici kavramına açıklık getirerek, tüketici haklarının neler olduğuna ve bu hakların nasıl kullanılacağına ilişkin genel esasları ortaya koymaktadır. Ayrıca ayıplı mal ve hizmetler, haksız şart, ticari reklam ve haksız ticari uygulamalar gibi birçok konuda tüketicileri gözetken düzenlemelere yer verilmiştir. Tüketici uyuşmazlıklarına daha hızlı bir şekilde çözüm bulabilmek adına özel görevli mahkemeler olan tüketici mahkemeleri, tüketici hakem heyetleri ve tüketici konseyleri gibi kurumların oluşturulması öngörülmüştür. Tüm bu düzenlemeler, bir tarafı tüketici olan internet üzerinden akdedilen sözleşmelerde de geçerli kabul edilir.

Tüketici Sözleşmeleri

TKHK'nın 2. maddesinde, bu Kanun'un her türlü tüketici işlemi ile tüketiciye yönelik uygulamaları kapsayacağı belirtilmiştir. Hükümde geçen "tüketici" ve "tüketici işlemi" kavramların ne anlama geldiğine, TKHK'nın "Tanımlar" kenar başlıklı 3. maddesinde yer verilmiştir. Buna göre;

- tüketici, *"ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişi"*;
- tüketici işlemi, *"mal veya hizmet piyasalarında kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla hareket eden veya onun adına ya da hesabına hareket eden gerçek veya tüzel kişiler ile tüketiciler arasında kurulan, eser, taşıma, simsarlık, sigorta, vekâlet, bankacılık ve benzeri sözleşmeler de dâhil olmak üzere her türlü sözleşme ve hukuki işlem"* olarak tanımlanmıştır.

Yukarıda verilen tanımlara göre, tüketici işlemlerinin özellikleri şunlardır:

- Taraflardan biri **"tüketici"** dir. Tüketicinin, mal veya hizmeti kendisi ya da ailesinin özel ihtiyacı için alması gerekir. Bir mal veya hizmetin mesleki ya da ticari amaçlarla alınması hâlinde tüketici sıfatından söz edilemeyeceği için tüketici işleminden de bahsedilemez.
- Sözleşmenin karşı tarafının, **"satıcı"** veya **"sağlayıcı"** olması gerekir. TKHK m. 3 hükmünde satıcı, *"kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye mal sunan ya da mal sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişi"*; sağlayıcı ise *"kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye hizmet sunan ya da hizmet sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişi"* olarak tanımlanmıştır. Özetle, sözleşmenin karşı tarafının ticari veya mesleki amaçlarla hareket etmesi gerekir. Dolayısıyla, bir tüketicinin, mesleki ve ticari amaçlarla hareket etmeyen bir kişiden mal veya hizmet satın alması hâlinde tüketici işleminden söz edilemez.



DİKKAT EDELİM

TKHK sistematğinde, gerçek kişilerin yanında tüzel kişiler de "tüketici" olarak kabul edilmiştir.

Bir kişinin kullanmadığı, kullanmadığı bir eşyasını satması hâlinde mesleki amaçtan söz edilemez.

TKHK'da yer alan "tüketici işlemleri" tanımı belirli sözleşme tipleriyle sınırlanmamıştır. Diğer bir deyişle, bir tarafı "satıcı" veya "sağlayıcı", diğer tarafı "tüketici" olmak şartıyla maddede sayılanlar dışında tüketici işlemleri de olabilir.



DİKKAT EDELİM

Bir tarafı tüketici, diğer tarafı satıcı veya sağlayıcı olmak kaydıyla internet üzerinden akdedilen sözleşmeler, “tüketici işlemi” olarak kabul edilmekte ve TKHK kapsamında tüketiciyi koruyan hükümlerden yararlanmaktadır.

Mesafeli Sözleşme

6502 sayılı TKHK’nın yürürlüğe girmesinden önceki dönemde yürürlükte olan “4077 sayılı Tüketicinin Korunması Hakkında Kanun (mülga TKHK)”’un ilk hâlinde internet üzerinden gerçekleştirilen işlemler, tüketicinin korunması hükümlerinden yararlanamamaktaydı. Daha sonra yapılan değişiklikle, mülga TKHK’ya 9/A maddesi eklenmiş ve “mesafeli sözleşmeler” düzenlenmiştir. Böylelikle, internet üzerinden yapılan işlemlerde tüketicilerin çok sınırlı da olsa korunması sağlanmıştır. 6502 sayılı TKHK’nın yürürlüğe girmesiyle mülga TKHK yürürlükten kaldırılmıştır. Günümüzde internet üzerinden yapılan tüketici işlemlerinde, 6502 sayılı TKHK hükümleri uygulama alanı bulmaktadır.

TKHK’nın 48. maddesinin ilk fıkrasına göre mesafeli sözleşme, “*satıcı veya sağlayıcı ile tüketicinin eş zamanlı fiziksel varlığı olmaksızın, mal veya hizmetlerin uzaktan pazarlanmasına yönelik olarak oluşturulmuş bir sistem çerçevesinde, taraflar arasında sözleşmenin kurulduğu ana kadar ve kurulduğu an da dâhil olmak üzere uzaktan iletişim araçlarının kullanılması suretiyle kurulan sözleşmelerdir*”. Aynı maddenin 7. fıkrasında, mesafeli sözleşme kapsamı dışında kalan sözleşmelerden söz edilmiş ve kapsam dışında kalan sözleşmelere ilişkin belirlemelerin yönetmelikle yapılacağına işaret edilmiştir. Bu maddeye dayanılarak çıkarılan “Mesafeli Sözleşmeler Yönetmeliği (RG, 27.11.2014, S. 29188) (MSY)”nin 2. maddesinin 2. fıkrasında, kapsam dışında bırakılan sözleşmeler sayılmıştır.

MSY’nin kapsamı dışında bırakılan sözleşmeler:

- a) Finansal hizmetler,
- b) Otomatik makineler aracılığıyla yapılan satışlar,
- c) Halka açık telefon vasıtasıyla telekomünikasyon operatörleriyle bu telefonun kullanımı,
- ç) Bahis, çekiliş, piyango ve benzeri şans oyunlarına ilişkin hizmetler,
- d) Taşınmaz malların veya bu mallara ilişkin hakların oluşumu, devri veya kazanımı,
- e) Konut kiralama,
- f) Paket turlar,
- g) Devre mülk, devre tatil, uzun süreli tatil hizmeti ve bunların yeniden satımı veya değişimi,
- ğ) Yiyecek ve içecekler gibi günlük tüketim maddelerinin, satıcının düzenli teslimatları çerçevesinde tüketicinin meskenine veya işyerine götürülmesi,

h) 5 inci maddenin birinci fıkrasının (a), (b) ve (d) bentlerindeki bilgi verme yükümlülüğü ile 18 inci ve 19 uncu maddelerde yer alan yükümlülükler saklı kalmak koşuluyla yolcu taşıma hizmetleri,

ı) Malların montaj, bakım ve onarımı,

i) Bakımevi hizmetleri, çocuk, yaşlı ya da hasta bakımı gibi ailelerin ve kişilerin desteklenmesine yönelik sosyal hizmetler,

j) Kısa mesaj aracılığıyla kurulan ve eş zamanlı olarak tamamen ifa edilen abonelik içermeyen katma değerli elektronik haberleşme hizmetleri ile 23/6/1983 tarihli ve 2860 sayılı Yardım Toplama Kanunu kapsamındaki bağışlar ve kamu kurumlarınca sunulan katma değerli elektronik haberleşme hizmetler.

Elektronik sözleşmelerin tarafları aynı anda aynı fiziki ortamda bulunmadığından, elektronik sözleşmelerin mesafeli sözleşme niteliğinde olduğu kabul edilir. Ancak her elektronik sözleşme mesafeli sözleşme değildir. Mesafeli sözleşmeden söz edebilmek için, yukarıdaki tanımdan da anlaşılacağı üzere, aşağıdaki unsurların bulunması zorunludur:

- Taraflardan birinin tüketici, diğerini satıcı ve sağlayıcı olması.
- Uzaktan pazarlamaya yönelik bir sistemin mevcut olması.
- Eş zamanlı fiziksel varlık göstermeksizin elektronik iletişim araçlarının kullanılması.

Mesafeli sözleşme en nihayetinde bir tüketici işlemidir. Bu sebeple tüketici işlemi olarak kabul edilmeyen elektronik sözleşmelerin, mesafeli sözleşme olduğunun söylenmesi doğru olmaz.



DİKKAT EDELİM

Her elektronik sözleşme, mesafeli sözleşme niteliğinde değildir.

Mesafeli Elektronik Sözleşmelerde Ön Bilgilendirme Yükümlülüğü ve Cayma Hakkı Kapsamında Tüketicinin Korunması

Ön Bilgilendirme Yükümlülüğü

En temel tüketici haklarından biri, kuşkusuz, tüketicinin bilgilendirilmesidir. Özellikle internet üzerinden kurulan sözleşmelerde, tüketici ürünü fiziki ortamda göremez ve ürünü test edebilme olanağına sahip değildir. Bu anlamda, tüketicinin bilinçli bir şekilde karar verebilmesi ve aldatici reklamlara karşı korunması gerekir.

Mesafeli sözleşmelerde sözleşme öncesi bilgilendirme yükümlülüğü TKHK'nın 48. maddesinin 2. fıkrasında düzenlenmiş, yükümlülüğün ayrıntılarının MSY ile belirleneceği ifade edilmiştir. MSY'nin 5. maddesine göre; tüketici, mesafeli sözleşme kurulmasından önce ya da buna karşılık gelen herhangi bir teklifi kabul etmeden önce aşağıda sayılan hususların tamamını içerecek şekilde satıcı veya sağlayıcı tarafından bilgilendirilmek zorundadır. Bu bilgiler, mesafeli sözleşmenin ayrılmaz bir parçasıdır ve taraflar aksini açıkça kararlaştırmadıkça bu bilgiler değiştirilemez. Ön bilgilendirme yapıldığının ispatı, satıcı veya sağlayıcı ile aracı hizmet sağlayıcıya aittir. Mesafeli sözleşmenin platform üzerinden kurulması hâlinde aracı hizmet sağlayıcı ön bilgilendirme yapılmasından satıcı ve sağlayıcıyla birlikte (müteselsilen) sorumludur. Veri girişinin aracı hizmet sağlayıcı tarafından yapıldığı durumlarda aşağıda sayılan zorunlu hususlardaki eksikliklerden ve verilerin doğruluğundan aracı hizmet sağlayıcı sorumludur.

MSY m. 5/1'de sayılan zorunlu unsurlar aşağıdaki gibidir:

- a) Sözleşme konusu mal veya hizmetin temel nitelikleri,
- b) Satıcı veya sağlayıcı ile aracı hizmet sağlayıcının adı veya unvanı, MERSİS numarası veya vergi kimlik numarası,
- c) Tüketicinin satıcı veya sağlayıcı ve aracı hizmet sağlayıcı ile hızlı bir şekilde irtibat kurmasına imkan veren açık adres, telefon numarası ve benzeri iletişim bilgileri ile varsa satıcı veya sağlayıcının adına ya da hesabına hareket eden kimliği ve adresi,
- ç) Satıcı veya sağlayıcı ile aracı hizmet sağlayıcının tüketicinin şikayetlerini iletmesi için (c) bendinde belirtilenden farklı iletişim bilgileri var ise, bunlara ilişkin bilgi,
- d) Mal veya hizmetin tüm vergiler dahil toplam fiyatı, niteliği itibarıyla önceden hesaplanamıyorsa fiyatın hesaplanma usulü, varsa tüm nakliye, teslim ve benzeri ek masraflar ile bunların önceden hesaplanamaması hâlinde ek masrafların ödenebileceği bilgisi,
- e) Sözleşmenin kurulması aşamasında uzaktan iletişim aracının kullanım bedelinin olağan ücret tarifesine üzerinden hesaplanmadığı durumlarda, tüketicilere yüklenen ilave maliyet,
- f) Ödeme, ticari reklam ve tanıtımlarında taahhüt edilen süre ile uyumlu teslim veya ifa süresi, teslimat ve ifaya ilişkin diğer bilgiler ile varsa bunlara ilişkin taahhütler ve satıcı veya sağlayıcı ile aracı hizmet sağlayıcının şikayetlere ilişkin çözüm yöntemleri,
- g) Cayma hakkının olduğu durumlarda, bu hakkın kullanılma şartları, süresi, usulü ve satıcının iade için öngördüğü taşıyıcıya ilişkin bilgiler,
- h) Cayma bildiriminin yapılacağı açık adres, faks numarası veya elektronik posta bilgileri,
- ı) 15 inci madde uyarınca cayma hakkının kullanılmadığı durumlarda, tüketicinin cayma hakkından faydalanamayacağına ya da hangi koşullarda cayma hakkını kaybedeceğine ilişkin bilgi,
- i) Satıcı veya sağlayıcının talebi üzerine, varsa tüketici tarafından ödenmesi veya sağlanması gereken depozitolar ya da diğer mali teminatlar ve bunlara ilişkin şartlar,
- j) Varsa dijital içeriklerin işlevselliğini etkileyebilecek teknik koruma önlemleri,
- j) Satıcı veya sağlayıcının bildiği ya da makul olarak bilmesinin beklendiği, dijital içeriğin hangi donanım ya da yazılımla birlikte çalışabileceğine ilişkin bilgi,
- k) Tüketicilerin uyuşmazlık konusundaki başvurularını Tüketici Mahkemesine veya Tüketici Hakem Heyetine yapabileceklerine dair bilgi.

Zorunlu bilgilendirme kapsamındaki tüm hususlar, kullanılan uzaktan iletişim aracına uygun olarak en az on iki punto büyüklüğünde, anlaşılabilir bir dilde, açık, sade ve okunabilir bir şekilde satıcı veya sağlayıcı tarafından yazılı olarak veya kalıcı veri saklayıcısı ile bilgilendirilmek zorundadır (MSY m. 6). Aynı maddede, mesafeli sözleşmenin internet yoluyla kurulması hâlinde satıcı ve sağlayıcı için, yukarıda sayılanlara ek yükümlülükler getirilmiştir. Buna göre; satıcı ve sağlayıcı, yukarıda sayılan (a), (d), (g) ve (h) bentlerinde yer alan bilgileri bir bütün olarak, tüketicinin ödeme yükümlülüğü altına girmesinden hemen önce açık bir şekilde ayrıca göstermek ve herhangi bir gönderim kısıtlamasının uygulanıp uygulanmadığını ve hangi ödeme araçlarının kabul edildiğini, en geç tüketici siparişini vermeden önce, açık ve anlaşılabilir bir şekilde belirtmek zorundadır.

Ayrıca, satıcı veya sağlayıcı ile aracı hizmet sağlayıcı, tüketicinin ön bilgileri edindiğini teyit etmek zorundadır. Aksi hâlde sözleşme kurulmamış sayılır. Satıcı veya sağlayıcı ile aracı hizmet sağlayıcı, tüketici siparişi onaylamadan hemen önce, verilen siparişin ödeme yükümlülüğü anlamına geldiği hususunda tüketiciyi açık ve anlaşılır bir şekilde bilgilendirmek zorundadır. Aksi hâlde tüketici siparişi ile bağlı değildir.

Ön bilgilendirme yükümlülüğü kapsamında, aracı hizmet sağlayıcısı olarak faaliyet gösterenler aracılık ettikleri mesafeli sözleşmelere ilişkin sorumluluklarının sınırı, TKHK m. 48/6'da belirlenmiştir. Buna göre, aracı hizmet sağlayıcısı;

- a) Tüketicie ön bilgilendirmenin yapılmasından, teyidinden ve ispatından satıcı veya sağlayıcı ile birlikte müteselsilen,
- b) Veri girişinin satıcı veya sağlayıcı tarafından yapıldığı durumlar hariç olmak üzere, yönetmelikle belirlenen ön bilgilendirmede bulunması zorunlu hususlardaki eksikliklerden,
- c) Bu maddede yer alan hususlardan dolayı tüketicilerin satıcı veya sağlayıcılar ile yaptıkları işlemlere ilişkin kayıtların tutulmasından ve istenilmesi hâlinde bu bilgilerin ilgili kamu kurum ve kuruluşları ile tüketicilere verilmesinden,
- ç) Satıcı veya sağlayıcı ile yaptıkları aracılık hizmetine ilişkin sözleşmeye aykırı uygulamaları nedeniyle satıcı ve sağlayıcıların bu madde hükümlerine aykırı davranmasına sebep oldukları her bir işleminden,
- d) Satıcı veya sağlayıcı adına bedel tahsil etmesi hâlinde, mal veya hizmetin tüketiciye teslim veya ifası sonrası bedelin satıcıya veya sağlayıcıya aktarıldığı durumlar ile 11 inci ve 15 inci maddelerde yer alan hakların kullanımı hariç olmak üzere teslim veya ifa ile cayma hakkına ilişkin yükümlülüklerden satıcı veya sağlayıcı ile birlikte müteselsilen,
- e) Satıcı veya sağlayıcı onayı olmaksızın düzenledikleri kampanyalı, promosyonlu veya indirimli satışlarda, sözleşmenin hiç ya da gereği gibi ifa edilmemesinden,
- f) Ön bilgilendirmede yer alan hususlar ile reklamlarında yer alan bilgilerin uyumlu olmasından ve ispatından sorumludur.

Cayma Hakkı

Mesafeli sözleşmelerde tüketicilere tanınan önemli bir hak, cayma hakkı olup MSY'nin 9 vd. maddelerinde düzenlenmiştir. Tüketici, mesafeli sözleşmelerde, ondört gün içinde herhangi bir gerekçe göstermeksizin ve cezai şart ödemeksizin sözleşmeden cayma hakkına sahiptir. Cayma hakkının kullanıldığına dair bildirimin, bu süre zarfında satıcı veya sağlayıcıya yöneltilmiş olması yeterlidir. Cayma hakkının süresi, hizmet ifasına ilişkin sözleşmelerde sözleşmenin kurulduğu gün; mal teslimine ilişkin sözleşmelerde ise tüketicinin veya tüketici tarafından belirlenen üçüncü kişinin malı teslim aldığı gün başlar. Ancak tüketici, sözleşmenin kurulmasından malın teslimine kadar olan süre içinde de cayma hakkını kullanabilir.

Satıcı veya sağlayıcı ile aracı hizmet sağlayıcı, cayma hakkı konusunda tüketicinin bilgilendirildiğini ispat etmekle yükümlüdür. Tüketici, cayma hakkı konusunda gerektiği şekilde bilgilendirilmezse, cayma hakkını kullanmak için on dört günlük süreyle bağlı değildir. Her hâlükârda bu süre cayma süresinin bittiği tarihten itibaren bir yıl sonra sona erer. Tüketici, cayma hakkı süresi içinde malın mutat kullanımı sebebiyle meydana gelen değişiklik ve bozulmalardan sorumlu değildir. Oluşturdukları sistem ile satıcı veya sağlayıcı adına mesafeli sözleşme kurulmasına aracılık eden aracı hizmet sağlayıcılar, sistem aracılığıyla kurulan mesafeli sözleşmelerden doğan hak ve yükümlülüklerin kullanım süresi boyunca tüketicilerin talep ve bildirimlerini iletebilmelerine ve takip edebilmelerine elverişli bir sistemi kurmak ve bu sistemi kesintisiz olarak açık tutmakla yükümlüdür.

Tüketicinin cayma hakkını kullandığına dair bildirimini, süresi içinde, yazılı olarak veya kalıcı veri saklayıcı ile satıcı, sağlayıcı veya aracı hizmet sağlayıcıya yöneltmesi yeterlidir. MSY'nin ekinde, cayma formu örneği yer almaktadır. Tüketici, bu formu kullanabileceği gibi cayma kararını bildiren açık bir beyanda da bulunabilir. Satıcı veya sağlayıcı, tüketicinin bu formu doldurabilmesi veya cayma beyanını gönderebilmesi için internet sitesi üzerinden seçenek de sunabilir. İnternet sitesi üzerinden tüketicilere cayma hakkı sunulması durumunda satıcı veya sağlayıcı, tüketicilerin iletmış olduğu cayma taleplerinin kendilerine ulaştığına ilişkin teyit bilgisini tüketiciye derhâl iletmek zorundadır. Cayma hakkının kullanıldığına dair ispat yükü tüketiciye aittir. Platform üzerinden kurulan mesafeli sözleşmelerde ise aracı hizmet sağlayıcı tüketicinin formu doldurabilmesi veya cayma beyanını gönderebilmesi için platform üzerinde gerekli sistemi kurmak ve tüketicilerin iletmış olduğu cayma beyanlarının kendisine ve satıcı veya sağlayıcıya ulaştığına ilişkin teyit bilgisini tüketiciye derhâl iletmek zorundadır.

MSY'nin 15. maddesinde cayma hakkının istisnalarına yer verilmiştir. MSY m. 15/1-ğ'e göre; elektronik ortamda anında ifa edilen hizmetler veya tüketiciye anında teslim edilen gayrimaddi mallara ilişkin sözleşmelerde, taraflarca aksi kararlaştırılmadıkça cayma hakkı kullanılamaz.

Cayma hakkı kapsamında tarafların yükümlülükleri MSY'de ayrı ayrı düzenlenmiştir. Satıcı veya sağlayıcı, tüketicinin cayma hakkını kullandığına ilişkin bildirimin kendisine ulaştığı tarihten itibaren on dört gün içinde, varsa malın tüketiciye teslim masrafları da dahil olmak üzere tahsil edilen tüm ödemeleri iade etmekle yükümlüdür. Bu kapsamda, yapacağı geri ödemeleri tüketicinin satın alırken kullandığı ödeme aracına uygun bir şekilde ve tüketiciye herhangi bir masraf veya yükümlülük getirmeden tek seferde yapmak zorundadır. Tüketici cayma süresi içinde malı, işleyişine, teknik özelliklerine ve kullanım talimatlarına uygun bir şekilde kullandığı takdirde meydana gelen değişiklik ve bozulmalardan sorumlu tutulmamıştır. 2022 yılında yapılan bir değişiklikle, aracı hizmet sağlayıcının yükümlülükleri de MSY'ye eklenmiş ve ayrıntılı olarak düzenlenmiştir.

Haksız Şartlar Bakımından Tüketicinin Korunması

Haksız şart; tüketiciyle müzakere edilmeden sözleşmeye dâhil edilen ve tarafların sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olan sözleşme şartlarıdır. "TKHK ile Tüketici Sözleşmelerindeki Haksız Şartlar Hakkında Yönetmelik (Haksız Şart Yönetmeliği)" hükümlerinde düzenlenmiştir. Tüketici ile kurulan sözleşmelerde yer alan bir şartın haksız şart olarak kabul edilebilmesi için tüketiciyle müzakere edilmeden sözleşmeye dahil edilmesi ve tarafların sözleşmeden doğan hak ve yükümlülüklerinde dürüstlük kuralına aykırı düşecek biçimde tüketici aleyhine dengesizliğe neden olması gerekir. Tüketici sözleşmesinde,

her iki unsurun da varlığı birlikte aranır. Bir sözleşme şartının önceden hazırlanması ve standart sözleşmede yer alması nedeniyle tüketicinin sözleşmenin içeriğine etki edememesi durumunda, o sözleşme şartının tüketiciyle müzakere edilmediği kabul edilir. Sözleşmeyi düzenleyen, bir standart şartın münferiden müzakere edildiğini iddia ediyorsa bunu ispatla yükümlüdür. Haksız Şart Yönetmeliği'nin ekinde, haksız sözleşme şartları örnek olarak sayılmıştır.

Tüketicisiyle kurulan sözleşmede yer alan haksız şart kesin olarak hükümsüzdür. Ancak sözleşmenin haksız şartlar dışındaki hükümleri geçerliliğini korur. Sözleşmede yer alan hüküm açık ve anlaşılır değilse tüketici lehine yorumlanır.

Ayıp Sebebiyle Tüketicinin Korunması

TKHK'da "ayıplı mal" ve "ayıplı hizmet" ayrı ayrı düzenlenmiştir. TKHK m. 8'e göre; tüketiciye teslimi anında, taraflarca kararlaştırılmış olan örnek ya da modele uygun olmayan ya da objektif olarak sahip olması gereken özellikleri taşımayan nedeniyle sözleşmeye aykırı olan mal, ayıplı maldır. Ambalajında, etiketinde, tanıtma ve kullanma kılavuzunda, internet portalında ya da reklam ve ilanlarında yer alan özelliklerinden bir veya birden fazlasını taşımayan; satıcı tarafından bildirilen veya teknik düzenlemesinde tespit edilen niteliğe aykırı olan; muadili olan malların kullanım amacını karşılamayan, tüketicinin makul olarak beklediği faydaları azaltan veya ortadan kaldıran maddi, hukuki veya ekonomik eksiklikler içeren mallar da ayıplı olarak kabul edilir.

Ayıbın, "maddi ayıp", "hukuki ayıp" ve "ekonomik ayıp" olmak üzere üç türü vardır. Malın, emsalleriyle kıyaslandığında, satın alınmasındaki amaca uygun olmaması, beklenen faydanın sağlanamaması hâlinde maddi ayıptan söz edilir. Yeni alınan koltuğun üzerine oturunca çökmesi, dışarıdan söylenen bir yemeğin içinden cam çıkması, çamaşır makinesinin deterjan gözünün kapanmaması gibi durumlar maddi ayıba örnektir. Maddi ayıp ürünün tamamında ya da bir kısmında olabilir. Sözleşmeye konu malın, objektif hukuk kurallarından kaynaklanan sebepler nedeniyle, beklenen faydayı sağlayamaması hukuki ayıptır. Örneğin, satıcının sattığı ürünlere gümrük tarafından el konulması hâlinde hukuki ayıp söz konusu olur. Sözleşmeye konu malın, beklenen ekonomik faydalarında eksiklik bulunması hâlinde ekonomik ayıptan söz edilir. Örneğin, sıfır diye satılan bir ürünün ikinci el olması ekonomik ayıba örnektir. Ancak, satıcı, kendisinden kaynaklanmayan reklam yoluyla yapılan açıklamalardan haberdar olmadığını ve haberdar olmasının da kendisinden beklenemeyeceğini veya yapılan açıklamanın içeriğinin satış sözleşmesinin akdi anında düzeltilmiş olduğunu veya satış sözleşmesi kurulma kararının bu açıklama ile nedensellik bağı içinde olmadığını ispatladığı takdirde açıklamanın içeriği ile bağı olmaz.

**DİKKAT EDELİM**

Satış sözleşmesine konu malın ithalatının yasaklanmış olması hâlinde, hukuki ayıptan söz edilmez. Bu hâlde, hukuka aykırılıktan söz edilir ve TBK m. 27 uyarınca, bu sözleşme kesin hükümsüzdür.

Satıcı, malı satış sözleşmesine uygun olarak tüketiciye teslim etmekle yükümlüdür. Sözleşmeye konu olan malın, sözleşmede kararlaştırılan süre içinde teslim edilmemesi veya montajının satıcı tarafından veya onun sorumluluğu altında gerçekleştirildiği durumlarda gereği gibi monte edilmemesi sözleşmeye aykırı ifa olarak değerlendirilir. Malın montajının tüketici tarafından yapılmasının öngörüldüğü hâllerde, montaj talimatındaki yanlışlık veya eksiklik nedeniyle montaj hatalı yapılmışsa, sözleşmeye aykırı ifa söz konusu olur.

Bir malın ayıplı olarak piyasaya sunulması da mümkündür. Defolu ürünlerin piyasa fiyatının altında bir ücrete satılması hâli bu duruma örnektir. Bu gibi durumlarda, satışa sunulacak ayıplı mal üzerine ya da ambalajına, üretici, ithalatçı veya satıcı tarafından tüketicinin kolaylıkla okuyabileceği şekilde malın ayıbına ilişkin açıklayıcı bilgiyi içeren bir etiket konulur. Bu etiketin tüketiciye verilmesi veya ayıba ilişkin açıklayıcı bilginin tüketiciye verilen fatura, fiş veya satış belgesi üzerinde açıkça gösterilmesi zorunludur.

Tüketici sözleşmelerinde, teslim tarihinden itibaren altı ay içinde ortaya çıkan ayıpların, teslim tarihinde var olduğu kabul edilir. Bu durumda malın ayıplı olmadığına ispatı satıcıya aittir. Tüketicinin, sözleşmenin kurulduğu tarihte ayıptan haberdar olduğu veya haberdar olmasının kendisinden beklenmediği hâllerde, sözleşmeye aykırılık söz konusu olmaz. Yani bu hâllerde satıcının ayıptan dolayı sorumluluğu gündeme gelmez.

Malın ayıplı olduğunun anlaşılması durumunda tüketicinin seçimlik hakları TKHK'nın 11. maddesinde düzenlenmiştir. Tüketici,

- Satılanı geri vermeye hazır olduğunu bildirerek sözleşmeden dönme,
- Satılanı alıkoyup ayıp oranında satış bedelinden indirim isteme,
- Aşırı bir masraf gerektirmediği takdirde, bütün masrafları satıcıya ait olmak üzere satılanın ücretsiz onarılmasını isteme,
- İmkân varsa, satılanın ayıpsız bir misli ile değiştirilmesini isteme

seçimlik haklarından birini kullanabilir. Satıcı, tüketicinin tercih ettiği bu talebi yerine getirmekle yükümlüdür. Ücretsiz onarım veya malın ayıpsız misli ile değiştirilmesi hakları üretici veya ithalatçıya

karşı da kullanılabilir. Bu hâlde satıcı, üretici ve ithalatçı birlikte (müteselsilen) sorumludur. Üretici veya ithalatçı, malın kendisi tarafından piyasaya sürülmesinden sonra ayıbın doğduğunu ispat ettiği takdirde sorumlu tutulmaz. Ücretsiz onarım veya malın ayıpsız misli ile değiştirilmesinin satıcı için orantısız güçlükleri beraberinde getirecek olması hâlinde tüketici, sözleşmeden dönme veya ayıp oranında bedelden indirim haklarından birini kullanabilir. Orantısızlığın tayininde malın ayıpsız değeri, ayıbın önemi ve diğer seçimlik haklara başvurma hakkının tüketici açısından sorun teşkil edip etmeyeceği gibi hususlar dikkate alınır. Ücretsiz onarım veya malın ayıpsız misli ile değiştirilmesi haklarından birinin seçilmesi durumunda bu talebin satıcıya, üreticiye veya ithalatçıya yöneltilmesinden itibaren azami otuz iş günü içinde yerine getirilmesi zorunludur. Tüketicinin sözleşmeden dönme veya ayıp oranında bedelden indirim hakkını seçtiği durumlarda, ödemiş olduğu bedelin tümü veya bedelden yapılan indirim tutarı derhâl tüketiciye iade edilir. Seçimlik hakların kullanılması nedeniyle ortaya çıkan tüm masraflar, tüketicinin seçtiği hakkı yerine getiren tarafça karşılanır. Tüketici bu seçimlik haklarından biriyle birlikte tazminat da talep edebilir.

Ayıp hâlinde zamanaşımı süreleri TKHK'nın 12. maddesinde düzenlenmiştir. Buna göre; kanunlarda veya taraflar arasındaki sözleşmede daha uzun bir süre belirlenmediği takdirde, ayıplı maldan sorumluluk, ayıp daha sonra ortaya çıkmış olsa bile, malın tüketiciye teslim tarihinden itibaren iki yıllık zamanaşımına tabidir. Ayıp, ağır kusur ya da hile ile gizlenmişse zamanaşımı hükümleri uygulanmaz.



DİKKAT EDELİM

TBK'daki ayıba ilişkin düzenlemelerin aksine, TKHK'da tüketicinin ayıplı mal karşısında seçimlik haklarını kullanabilmesi için malı teslim aldıktan sonra belirli bir süre içerisinde malı gözden geçirme külfeti yoktur.

Dijital bir malın, örneğin bir bilgisayar programının cihaza indirilmesi (*download*) suretiyle satın alınması hâlinde, programın çalışmaması gibi bir ayıp söz konusu olabilir. Bu hâlde, tüketicinin sözleşmeden dönme ile malın ayıpsız misliyle değiştirilmesi hakkını kullanabileceği kabul edilmekle birlikte, ücretsiz onarım ve ayıp oranında indirim haklarının kullanılmasının işin niteliğine uygun düşmeyeceği ifade edilmektedir. Konuyla ilgili Yargıtay kararlarında da ayıp sebebiyle sözleşmeden dönme hakkının son çare olarak kullanılması gerektiği, öncelikle ayıbın giderilmesi yollarına başvurulması gerektiğine işaret edilmiştir.

Ayıplı hizmet, TKHK m. 13 vd. hükümlerinde düzenlemiştir. Ayıplı hizmet, sözleşmede belirlenen süre içinde başlamaması veya taraflarca kararlaştırılmış olan ve objektif olarak sahip olması gereken

özellikleri taşımaması nedeniyle sözleşmeye aykırı olan hizmettir. Hizmet sağlayıcısı tarafından bildirilen, internet portalında veya reklam ve ilanlarında yer alan özellikler taşımayan ya da yararlanma amacı bakımından değerini veya tüketicinin ondan makul olarak beklediği faydaları azaltan veya ortadan kaldıran maddi, hukuki veya ekonomik eksiklikler içeren hizmetler ayıplıdır. Sağlayıcı, hizmeti sözleşmeye uygun olarak ifa etmekle yükümlüdür. Sağlayıcı, kendisinden kaynaklanmayan reklam yoluyla yapılan açıklamalardan haberdar olmadığını ve haberdar olmasının da kendisinden beklenemeyeceğini veya yapılan açıklamanın içeriğinin hizmet sözleşmesinin kurulduğu tarihte düzeltilmiş olduğunu veya hizmet sözleşmesinin kurulması kararının bu açıklama ile nedensellik bağı içermediğini ispatladığı takdirde açıklamanın içeriği ile bağlı olmaz.

Hizmetin ayıplı ifa edildiği durumlarda tüketici, hizmetin yeniden görülmesi, hizmet sonucu ortaya çıkan eserin ücretsiz onarımı, ayıp oranında bedelden indirim veya sözleşmeden dönme haklarından birini sağlayıcıya karşı kullanmakta serbesttir. Sağlayıcı, tüketicinin tercih ettiği bu talebi yerine getirmekle yükümlüdür. Seçimlik hakların kullanılması nedeniyle ortaya çıkan tüm masraflar sağlayıcı tarafından karşılanır. Tüketici, bu seçimlik haklarından biriyle birlikte genel hükümler uyarınca tazminat da talep edebilir. Ücretsiz onarım veya hizmetin yeniden görülmesinin sağlayıcı için orantısız güçlükleri beraberinde getirecek olması hâlinde tüketici bu hakları kullanamaz. Orantısızlığın tayininde hizmetin ayıpsız değeri, ayıbın önemi ve diğer seçimlik haklara başvurma hakkının tüketici açısından sorun teşkil edip etmeyeceği gibi hususlar dikkate alınır. Tüketicinin sözleşmeden dönme veya ayıp oranında bedelden indirim hakkını seçtiği durumlarda, ödemiş olduğu bedelin tümü veya bedelden indirim yapılan tutar derhâl tüketiciye iade edilir. Ücretsiz onarım veya hizmetin yeniden görülmesinin seçildiği hâllerde, hizmetin niteliği ve tüketicinin bu hizmetten yararlanma amacı dikkate alındığında, makul sayılabilecek bir süre içinde ve tüketici için ciddi sorunlar doğurmayacak şekilde bu talep sağlayıcı tarafından yerine getirilir. Her hâlükârda bu süre talebin sağlayıcıya yöneltilmesinden itibaren otuz iş gününü geçemez. Aksi takdirde tüketici diğer seçimlik haklarını kullanmakta serbesttir.

Kanunlarda veya taraflar arasındaki sözleşmede daha uzun bir süre belirlenmediği takdirde, ayıplı hizmetten sorumluluk, ayıp daha sonra ortaya çıkmış olsa bile, hizmetin ifası tarihinden itibaren iki yıllık zamanaşımına tabidir. Ayıp, ağır kusur ya da hile ile gizlenmişse zamanaşımı hükümleri uygulanmaz.

BÖLÜM ÖZETİ

Elektronik ticaret, en genel ifadeyle mal veya hizmetlerin elektronik ortamlarda üretilmesine, reklamının yapılmasına, pazarlanmasına veya sunulmasına yönelik işlemlerin bütünüdür. Elektronik ticaretin “elektronik ortam” ve “ticari işlem” olmak üzere iki unsuru bulunmaktadır. Bu kapsamda “ticari işlem” ile Türk Ticaret Kanunu’ndaki “ticari iş” kavramlarının birbirinden ayırt edilmesi gerekir. Ticari işlem, ekonomik menfaat elde etmek için yapılan her türlü işlem olabilir. Elektronik ticaret kapsamındaki yapılan işlem; “ticari iş”, “tüketici işlemi” veya “adi iş” olabilir.

Türk hukukunda elektronik ticaretin düzenlenmesine ilişkin temel mevzuat, “6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ve bu kanuna dayanılarak çıkarılan ikincil düzenlemelerdir. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, elektronik ticarete ilişkin esas ve usulleri düzenlemeyi amaçlamakta olup ticari iletişimi, hizmet sağlayıcı ve aracı hizmet sağlayıcıların sorumluluklarını, elektronik iletişim araçlarıyla yapılan sözleşmeleri ile elektronik ticarete ilişkin bilgi verme yükümlülüklerini ve uygulanacak yaptırımları kapsar. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun’un 3. maddesinde “hizmet sağlayıcı” için “bilgi verme yükümlülüğü” öngörülmüştür. Bilgi verme yükümlülüğü, elektronik ticaretin tarafları arasında güven sağlamayı amaçlar ve elektronik ticaretin gelişmesine hizmet eder. Elektronik ticaret aracı hizmet sağlayıcı, elektronik ticaret pazar yerinde elektronik ticaret hizmet sağlayıcılarının mal veya hizmetlerinin teminine yönelik sözleşme yapılmasına ya da sipariş verilmesine imkân sağlayan aracı hizmet sağlayıcıyı; elektronik ticaret hizmet sağlayıcı ise elektronik ticaret pazar yerinde ya da kendine ait elektronik ticaret ortamında mal veya hizmetlerinin teminine yönelik sözleşme yapan ya da sipariş alan hizmet sağlayıcıyı ifade eder.

Elektronik ticarete en çok karşılaşılan hukuki sorunlardan biri sözleşme konusunun ayıplı olmasıdır. Satıcı ya da sağlayıcı, sözleşme konusu mal ya da hizmeti sözleşmeye uygun olarak tüketiciye teslim etmekle yükümlüdür. Sözleşme konusunun sözleşmede kararlaştırılan nitelikte olmadığı ya da beklenen yararın sağlanamadığı hâllerde “ayıp”tan bahsedilir. Borçlar hukukunda ayıp halinde alıcının malı gözden geçirme ve ihbar külfeti öngörülmüşken, tüketici hukukunda bu koşul aranmamaktadır. Ayrıca, tüketici sözleşmelerinde teslim tarihinden itibaren altı ay içinde ortaya çıkan ayıpların, teslim tarihinde var olduğu kabul edilir. Bu durumda malın ayıplı olmadığına ispatı satıcıya aittir. Tüketici, ayıplı mal ya da hizmet karşısında Tüketicilerin Korunması Hakkındaki Kanun’da sayılan seçimlik haklarını işin niteliğine göre kullanabilir. Örneğin, elektronik ortamda bir hizmet sağlanması durumunda işin niteliği ayıp oranında bedelden indirim uygulanması mümkün olmayabilir. Öte yandan, tüketici işlemi niteliğindeki elektronik sözleşmelerde de dönme hakkının son çare olarak kullanılması gerekir.

GÖZDEN GEÇİRELİM

1. Elektronik ticaret hizmet sağlayıcı ve elektronik ticaret aracı hizmet sağlayıcıların kayıt altına alınması, elektronik ticaret verilerinin toplanması, bu verilerin işlenerek istatistiki bilgilerin üretilmesi amacıyla Bakanlık tarafından oluşturulan ve bu Kanun kapsamında kayıt ve bildirim yapılabilmesine imkân sağlayan bilgi sistemi

2. Mesleki özenin gereklerine uymayan ve ulaştığı ortalama tüketicinin ya da yöneldiği grubun ortalama üyesinin, bir mal veya hizmete ilişkin ekonomik davranış biçimini önemli ölçüde bozan veya bozma ihtimali olan her türlü ticari uygulama

3. Aracı hizmet sağlayıcı ve hizmet sağlayıcı, ETDHK kapsamındaki iş ve işlemlerine ilişkin bilgi, belge, defter ve elektronik kayıtlarını, iş veya işlemin gerçekleştiği tarihten itibaren yıl süreyle saklamakla yükümlüdür.

4. Tacirlere gönderilen ticari elektronik iletilerde önceden onay alınması

5. Her elektronik sözleşme, mesafeli sözleşme (niteliğindedir/niteliğinde değildir).

6. Satıcının sattığı mallara gümrükte el konulması hâlinde ayıptan bahsedilir.

7. Mesafeli sözleşmelerde tüketicinin bilgilendirildiğine ilişkin ispat yükü veya aittir.

8. Mesafeli sözleşmelerde cayma hakkının kullanımına ilişkin ispat yükümlülüğü aittir.

9. Tüketicinin cayma hakkını kullanma süresi, kural olarak

10. Tüketici sözleşmelerinde, teslim tarihinden itibaren içinde ortaya çıkan ayıpların, teslim tarihinde var olduğu kabul edilir.

CEVAP ANAHTARI

1. ETBİS	6. hukuki
2. haksız ticari uygulama	7. satıcı/sağlayıcıya
3. on	8. tüketiciye
4. gerekmez.	9. ondört gündür.
5. niteliğinde değildir.	10. altı ay

SÖZLÜK

EDI (electronic data interchange): Elektronik veri değişimi, elektronik ortamda verilerin değiş tokuşunu ifade eder. İşletmeler arası veri transferi için geliştirilmiştir.

Elektronik ticaret: Fiziki ortamda karşı karşıya gelinmeksizin, elektronik ortamda gerçekleştirilen çevrimiçi iktisadi ve ticari her türlü faaliyettir (Elektronik Ticaretin Düzenlenmesi Hakkında Kanun m. 2/1-a).

Genel işlem koşulları: Genel işlem koşulları, bir sözleşme yapılırken düzenleyenin, ileride çok sayıdaki benzer sözleşmede kullanmak amacıyla, önceden, tek başına hazırlayarak karşı tarafa sunduğu sözleşme hükümleridir (Türk Borçlar Kanunu m. 20).

Güvenli elektronik imza: Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, mızalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan elektronik imzadır (5070 sayılı Elektronik İmza Kanunu m. 4).

Hizmet: Bir ücret veya menfaat karşılığında yapılan ya da yapılması taahhüt edilen mal sağlama dışındaki her türlü tüketici işleminin konusudur (Tüketicinin Korunması Hakkında Kanun m. 3/1-d).

İfa: Yerine getirme; ödeme; borçlanılan şeyin yerine getirilmesidir.

Kalıcı veri sağlayıcısı: Tüketicinin gönderdiği veya kendisine gönderilen bilgiyi, bu bilginin amacına uygun olarak makul bir süre incelemesine elverecek şekilde kaydedilmesini ve değiştirilmeden kopyalanmasını sağlayan ve bu bilgiye aynen ulaştırılmasına imkan veren kısa mesaj, elektronik posta, internet, disk, CD, DVD, hafıza kartı ve benzeri her türlü araç veya ortamdır (Mesafeli Sözleşmeler Yönetmeliği m. 4/1-c).

Mal: Alışverişe konu olan; taşınır eşya, konut veya tatil amaçlı taşınmaz mallar ile elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri her türlü gayri maddi mallardır (Tüketicinin Korunması Hakkında Kanun m. 3/1-h).

Mesafeli satış sözleşmesi: Satıcı veya sağlayıcı ile tüketicinin eş zamanlı fiziksel varlığı olmaksızın, mal veya hizmetlerin uzaktan pazarlanmasına yönelik olarak oluşturulmuş bir sistem çerçevesinde, taraflar arasında sözleşmenin kurulduğu ana kadar ve kurulduğu an da dâhil olmak üzere uzaktan iletişim araçlarının kullanılması suretiyle kurulan sözleşmelerdir (Tüketicinin Korunması Hakkında Kanun m. 48/1).

Sağlayıcı: Kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye hizmet sunan ya da hizmet sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişidir (Tüketicinin Korunması Hakkında Kanun m. 3/1-ı).

Sanal pazar yeri: İşletmelerin mal veya hizmetlerinin tanıtımını ve reklamını yapmasına, aynı zamanda ihtiyaç duydukları mal ve hizmetleri satın almalarına olanak tanıyan elektronik ortamda kurulmuş ticaret yerleri, internet siteleridir.

Satıcı: Kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla tüketiciye mal sunan ya da mal sunanın adına ya da hesabına hareket eden gerçek veya tüzel kişidir (Tüketicinin Korunması Hakkında Kanun m. 3/1-i).

Tüketici: Ticari veya mesleki olmayan amaçlarla hareket eden gerçek veya tüzel kişidir (Tüketicinin Korunması Hakkında Kanun m. 3/1-k).

Tüketici işlemi: mal veya hizmet piyasalarında kamu tüzel kişileri de dâhil olmak üzere ticari veya mesleki amaçlarla hareket eden veya onun adına ya da hesabına hareket eden gerçek veya tüzel kişiler ile tüketiciler arasında kurulan, eser, taşıma, simsarlık, sigorta, vekâlet, bankacılık ve benzeri sözleşmeler de dâhil olmak üzere her türlü sözleşme ve hukuki işlemdir (Tüketicinin Korunması Hakkında Kanun m. 3/1-l).

KAYNAKÇA

Arslan, Merve: Elektronik Ticaret ve Mesafeli Elektronik Sözleşmelerde Tüketicinin Korunması, Seçkin Yayıncılık, Ankara 2021.

Aydoğdu, Murat; Kahveci, Nalan: Tüketici Hukuku Dersleri, Adalet Yayınevi, Ankara 2021.

Kaya, Ferman: E-Ticaret Hukuku ve Tüketici Hukuku Uygulamaları, Seçkin Yayıncılık, 4. Baskı, Ankara 2021.

Kaya, M. Bedii: Elektronik Ticaret Hukuku Ticari Elektronik İletiler, Onikilevha Yayıncılık, 2. Baskı, İstanbul 2020.

Sarıakçalı, Turgay: İnternet Üzerinden Akdedilen Sözleşmeler, Seçkin Yayıncılık, 2. Baskı, Ankara 2021.

Sert Sütçü, Selin: 6502 Sayılı Tüketicinin Korunması Hakkındaki Kanun Hükümlerine Göre Tüketici Hukuku Uygulamalarında Tüketicinin Korunması, Seçkin Yayıncılık, Ankara 2019.

Yılmaz, Ejder: Hukuk Sözlüğü, Yetkin Yayınları, 10. Baskı, Ankara 2011.

* Kanun ve yönetmeliklerin güncel versiyonları için bkz. www.mevzuat.gov.tr

ÜNİTE 6

BİLİŞİM ORTAMINDA FİKRİ
VE SİNAİ HAKLAR

Doç. Dr. Mete TEVETOĞLU
Arş. Gör. Batuhan DEMİRTAŞ

ANAHTAR KAVRAMLAR

Fikri ve Sınai Haklar
İnternette Fikri Haklar
İnternette Sınai Haklar
Yapay Zekâ ve Eser Sahipliği
Multimedya Eser
Blokzincir
Metaverse

BİLİŞİM ORTAMINDA
FİKRİ VE SİNAİ HAKLAR

ÖĞRENME HEDEFLERİ



1

Bu ünitenin sonunda okuyucunun; fikri ve sınai haklar, bilişim teknolojilerinin fikri ve sınai haklara olan etkisi, internette fikri haklar ve sınai haklar, multimedya eser, yapay zekâ ve blokzincir teknolojilerinin ve Metaverse'nin fikri ve sınai haklara etkisi konularında bilgi sahibi olması hedeflenmektedir.

GİRİŞ

Bilişim teknolojilerin hızla gelişmesi ve bilhassa internet altyapısının güçlenmesi ve dünya genelinde yaygınlaşması hayatın her alanını olduğu gibi insanların entelektüel yaratımlarını da değiştirmekte ve dönüştürmektedir.

İnsanların düşünsel emekleri karşılığında meydana getirdiği entelektüel ürünler hukukumuzda fikri ve sınai mülkiyet hukuku çerçevesinde düzenlenmekte ve korunmaktadır. İlim ve edebiyat eserleri, sinema eserleri ve benzeri fikri ürünler eser olarak nitelendirilmekte ve fikri mülkiyete konu edilmekteyken; marka, patent ve tasarım gibi diğer endüstriyel yaratımlar sınai mülkiyet hukukunun konusuna girmektedir.

Bu bölümde öncelikle; eser kavramı, eser sahibinin kim olduğu, eser sahibinin hak ve yetkileri incelenecek; sonrasında sınai mülkiyet hukukunun konularından marka, patent ve tasarımlar incelenecek, bunların hak sahiplerinin hukuki durumu ortaya konacaktır.

Fikri ve sınai mülkiyete ilişkin gerekli açıklamalar yapıldıktan sonra ise teknolojinin bilhassa bilişim ortamında fikri ve sınai hakları nasıl etkilediği, klasik fikri ve sınai mülkiyet hukuku kavramlarını nasıl değişime zorladığı, karşılaşılan hukuki sorunlar ortaya konacaktır.

Bilişim ortamında fikri ve sınai mülkiyeti derinden etkileyen bütün hususlara bu çalışmada yer verilmesi mümkün olmadığından; multimedya eser kavramı, dijital tükenme, yapay zeka ve eser sahipliği, blokzincir ve metaverse başlıkları üzerinde durulmuştur.

Türk Hukukunda Fikri ve Sınai Haklar

Bilişim teknolojilerinin fikri ve sınai haklara olan etkisi incelenmeden önce konunun Türk hukuk sisteminde nasıl ele alındığının belirlenmesinde yarar vardır. Öncelikle belirtmek gerekir ki konu hukukumuzda fikri mülkiyet ve sınai mülkiyet olmak üzere iki ana başlık altında değerlendirilmektedir. Fikri mülkiyete ilişkin ana düzenleme 1951 tarihli Fikir ve Sanat Eserleri Kanunu (FSEK) olup sınai mülkiyete ilişkin temel düzenleme ise 2016 tarihli Sınai Mülkiyet Kanunudur (SMK).

Kanunların içeriğine ve bilişim teknolojilerin söz konusu kavramları ne derece etkilediğine girmeden önce fikri mülkiyet ve sınai mülkiyetin ayrı ayrı incelenmesi gerekmektedir.

Fikri Mülkiyet Hukuku

Fikri mülkiyet hukuku tarihsel olarak matbaa ve benzeri çoğaltma araçlarının yaygınlaşması ile eser sahipleri ile diğer ilgililer arasındaki menfaat çatışmasının bir sonucu olarak ortaya çıkmıştır. Fikri mülkiyetin temel ögesi eser olup başta eser sahibinin hakları, koruma şartları ve eserden üçüncü kişilerin yaralanmasının şartları olmak üzere tarafların hak ve yükümlülüklerini ele alınmaktadır. **Fikri mülkiyetin konusunu eser oluşturduğu** için öncelikle eser ile kanun koyucunun ne kastettiğinin anlaşılması elzemdir.

Eser Nedir?

Fikir ve Sanat Eserleri Kanununda eser “*sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsulleri*” olarak tanımlanmıştır. Kanundaki tanımdan yola çıkarak bir ürünün eser niteliği taşıması için üç ana şartın gerçekleşmesinin gerektiği anlaşılmaktadır. Bu şartlar; şekli şart, sübjektif şart ve objektif şarttır.

Şekli Şart: Bir fikri ürünün FSEK kapsamında eser olarak nitelendirilebilmesi için o ürünün FSEK’te sınırlı sayıda sayılmış eser kategorilerinden birine dahil olması gerekmektedir. Bu eser türleri “ilim ve edebiyat eserleri”, “musiki eserler”, “güzel sanat eserleri”, “sinema eserleri” ve “işleme ve derlemeler”dir.



DİKKAT EDELİM

Eğer bir fikri ürün FSEK kapsamında sayılan eser türlerinden birine girmeye elverişli değilse FSEK kapsamında korunamayacaktır.

Subjektif Şart: Subjektif şart ile kastedilen; eserin, eser sahibinin hususiyetini taşımasıdır. Yani; eser, eser sahibinin özgün düşünsel emeğinin ve çabasının bir ürünü olmalıdır. Sahibinin hususiyetini taşımayan ürünler eser olarak nitelendirilmeye elverişli değildirler.

Objektif Şart: Bir fikri ürünün eser olarak nitelendirilmesi için gereken üçüncü şart ise objektif şart olarak tanımlanmaktadır. Objektif şart; eserin, eser sahibinin fikri dünyasından ve zihninden çıkıp üçüncü kişilerce objektif şekilde algılanabilir hale gelmesidir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Fikri mülkiyet hukuku fikirleri değil eserleri korumaktadır. Üçüncü kişilerce algılanabilir derecede somutlaşmamış ve zihinde kalmış fikirler eser korumasından faydalanamayacaktır.

Eser Sahibi Kimdir?

FSEK'te eser sahibi "*eseri meydana getiren kişi*" olarak tanımlanmıştır. Eseri fikri dünyasından çıkarıp somutlaştıran ve nihayetinde başkalarının da algılanabilir hale getiren, söz konusu esere hususiyetini bahşeden kişi eser sahibi olarak atfedilmektedir. Kısaca; eser sahibi, eseri meydana getiren kişidir.



EK BİLGİ

Eser sahibinin tek bir kişi olması gerekmiyip bir eserin birden fazla eser sahibi olabilir. Buna eser sahiplerinin birden fazla oluşu denmektedir. Bir eserin her zaman tek bir kişi tarafından meydana getirilmesi mümkün olmadığı gibi zorunlu da değildir. Örneğin; video oyunlarında, sinema eserlerinde veya birden fazla uzmanlık alanı gerektiren uzun monografik eserlerde birden fazla kişinin emeği ve fikri çabası gerekebilmektedir. Bu tür durumlarda, bir araya gelerek meydana getirdikleri eserde her biri kendi katkıları ve meydana getirdikleri kısımlar ölçüsünde eser sahibi olacaklardır. Eğer eser birden fazla parçaya bölünebilir nitelikte ise her bir parça üzerinde o parçayı meydana getiren kişi eser sahibi olacaktır. Ancak eğer eser ayrılmaz bir bütün arz ediyorsa bu durumda eserin sahibi o eseri meydana getirenlerin birliğidir.

Eser Sahibinin Hakları Nelerdir?

Eser sahipliğinden doğan haklar, eser sahibi yaşadığı müddetçe devam eder. Eser sahibinin ölümünden sonra ise yetmiş yıl boyunca mirasçuları nezdinde devam eder. Eser sahibinin hakları iki kategori altında incelenmektedir. Birincisi manevi haklar ikincisi ise mali haklardır.

Manevi haklar;

- eseri umuma arz hakkı,
- eser sahibi olarak tanıtılma hakkı,
- eserde değişiklik yapılmasını engelleme hakkı,
- eserin malikine ve zilyedine karşı eserine kavuşma ve bir süreliğine yararlanma hakkıdır.

Mali haklar ise;

- işleme hakkı,
- çoğaltma hakkı,
- yayma hakkı,
- temsil hakkı,
- işaret, ses ve/veya görüntü nakline yarayan araçlarla iletim hakkıdır.

Umuma Arz Hakkı: Bir eserin topluma veya bir kitleye sunulmasına karar verme hakkı eser sahibine aittir.

Eser sahibi olarak tanıtılma hakkı: Her eser sahibi, meydana getirdiği eser üzerinde eserin sahibinin kendisinin olduğunun belirtilmesini isteme hakkına sahiptir.

Eserde Değişiklik Yapılmasını Engelleme Hakkı: Eser, eser sahibinin fikri dünyasından çıkarak somutlaştığından eser ile eser sahibi arasında sıkı bir bağ vardır. Bu nedenle, eser sahibinin rızası olmadığı müddetçe eser üzerinde değişiklik yapılamaz; kısaltma, ekleme veya çıkarmada bulunulamaz.

Eseri Kavuşma ve Bir Süreliğine Yararlanma Hakkı: Eser sahibi bu hakkını kullanmakla elinden çıkardığı eserine bir süreliğine kavuşmakta, eserini sergileme veya katalog ve benzeri ortamlarda bir süreliğine sergileme imkanına sahip olmaktadır. Bu hak genellikle eser sahibinin eserini bir başkasına devrettiği hallerde kullanım alanı bulmaktadır.

İşleme Hakkı: Bir eseri işleme hakkı kural olarak yalnızca eser sahibine aittir.

Çoğaltma Hakkı: Bir eserin aslını veya kopyalarını tamamen veya kısmen herhangi bir şekilde çoğaltma veya kopyalama hakkı kural olarak yalnızca eser sahibine aittir.

Yayma Hakkı: Bir eserin aslını veya çoğaltılmış nüshalarını, kiralamak, ödünç vermek, satışa çıkarmak veya diğer yollarla dağıtmak hakkı kural olarak yalnızca eser sahibine aittir.

Temsil Hakkı: Bir eserden doğrudan doğruya yahut işaret, ses veya resim nakline yarayan aletlerle umumi mahallerde okumak, çalmak, oynamak ve göstermek gibi temsil suretiyle faydalanma hakkı kural olarak yalnızca eser sahibine aittir.

İşaret, Ses ve/veya Görüntü Nakline Yarayan Araçlarla Umuma İletim Hakkı: Bir eserin aslını veya çoğaltılmış nüshalarını, radyo-televizyon, uydu ve kablo gibi telli veya telsiz yayın yapan kuruluşlar vasıtasıyla veya dijital iletim de dahil olmak üzere işaret, ses ve/veya görüntü nakline yarayan araçlarla yayınlanması ve yayınlanan eserlerin bu kuruluşların yayınlarından alınarak başka yayın kuruluşları tarafından yeniden yayınlanması suretiyle umuma iletilmesi hakkı kural olarak yalnızca eser sahibine aittir.

Sınai Mülkiyet Hukuku

Teknolojinin hızla gelişmesi ve bu teknolojik gelişmelerin kişiler, şirketler hatta devletler arasındaki ekonomik ve diğer rekabet konuları noktasında etkili olması sınai mülkiyet hukukunun gelişmesinde öncü olmuştur. Sınai mülkiyetin konusunu ise bu nedenle marka, coğrafi işaret, tasarım, patent, faydalı model, geleneksel ürün adları vb. unsurlar oluşturmaktadır. Bölümün sınırlandırılması adına bu kısımda sadece marka, patent ve tasarım konularına değinilecektir.

Marka Nedir?

Markanın ana unsuru **bir teşebbüsün mallarının ve hizmetlerinin diğer teşebbüslerinin mallarından ve hizmetlerinden ayrılmasını sağlamasıdır. Bu işlevi gören işaretlere ise marka denmektedir.** Marka teşkil eden işaretin sicilde gösterilebilir olması gerekmektedir. Kişi adları da dahil olmak üzere; sözcükler, şekiller, renkler, harfler, sayılar, sesler ve hatta malların ve ambalajlarının şekilleri dahi marka özelliği göstermeye elverişlidir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Coca-Cola, Apple, Kinder vb. günlük hayatta sıklıkla karşılaştığımız ve ilgili mal ve hizmetleri diğer mal ve hizmetlerden ayırmamızı sağlayan işaretler, kelimeler, logolar vb. işaretler markaya örnek olarak gösterilebilir.

Markaların Koruma Süresi ve Kapsamı Nedir?

Markalar başvuru tarihinden itibaren on yıl süre ile koruma altındadır ve bu süre onar yıllık dönemler halinde herhangi bir sınırlandırma olmaksızın yenilenmeye devam edilebilir. Markanın koruma kapsamı ise konu itibarıyla markanın tescil edildiği alan ile kural olarak sınırlıdır. Markalar belirli faaliyet alanlarında tescillenmekte ve bu faaliyet alanları çerçevesinde korunmaktadır. Bir markanın koruma kapsamına girmeyen başkaca bir faaliyet alanında kullanılması **kural olarak** mümkündür.

Marka Sahibinin Hakları Nelerdir?

Marka sahipliğinden doğan haklar, markanın tescil edilmesiyle birlikte başlamaktadır. Marka sahibi, kural olarak markanın kullanılmasında münhasıran yetkilidir. Marka sahibi aşağıdaki hallerde markanın kullanılmasını engelleme hakkına sahiptir:

- Tescilli marka ile aynı olan herhangi bir işaretin, tescil kapsamına giren mal veya hizmetlerde kullanılmasını,
- Tescilli marka ile aynı veya benzer olan ve tescilli markanın kapsadığı mal veya hizmetlerle aynı veya benzer mal veya hizmetleri kapsayan ve bu nedenle halk tarafından tescilli marka ile ilişkilendirilme ihtimali de dâhil karıştırılma ihtimali bulunan herhangi bir işaretin kullanılmasını,
- Aynı, benzer veya farklı mal veya hizmetlerde olmasına bakılmaksızın, tescilli marka ile aynı veya benzer olan ve Türkiye’de ulaştığı tanınmışlık düzeyi nedeniyle markanın itibarından haksız bir yarar elde edecek veya itibarına zarar verecek veya ayırt edici karakterini zedeleyecek nitelikteki herhangi bir işaretin haklı bir sebep olmaksızın kullanılmasını.

Ek olarak eğer aşağıda sayılacak olan eylemler ve durumlar ticaret alanında gerçekleşirse, marka sahibi bu eylem ve durumları da yasaklama hakkına sahiptir. Bu durum ve eylemler ise:

- İşaretin, mal veya ambalajı üzerine konulması,
- İşareti taşıyan malların piyasaya sürülmesi, teslim edilebileceğinin teklif edilmesi, bu amaçlarla stoklanması veya işaret altında hizmetlerin sunulması ya da sunulabileceğinin teklif edilmesi,
- İşareti taşıyan malın ithal ya da ihraç edilmesi,
- İşaretin, teşebbüsün iş evrakı ve reklamlarında kullanılması,
- İşareti kullanan kişinin, işaretin kullanımına ilişkin hakkı veya meşru bağlantısı olmaması şartıyla işaretin aynı veya benzerinin internet ortamında ticari etki yaratacak biçimde alan adı, yönlendirici kod, anahtar sözcük ya da benzeri biçimlerde kullanılması,
- İşaretin ticaret unvanı ya da işletme adı olarak kullanılması,
- İşaretin hukuka uygun olmayan şekilde karşılaştırmalı reklamlarda kullanılması.

Patent Nedir?

Teknoloji alanındaki her yeni buluşa, *buluş basamağı içermesi ve sanayiye uygulanabilir olması* şartıyla patent verilebilmektedir. Yukarıda sayılan yeni olma, buluş basamağı içermesi ve sanayiye uygulanabilir olma şartlarından birini bile sağlamayan buluşa patent verilmesi mümkün değildir. Sayılan her üç şartın da sağlanması şarttır.

Patentte Yenilik Kavramı Nedir?

Teknolojik uygulamanın ve sanayinin bilinen durumuna dahil olmayan buluşlar yeni olarak kabul edilmektedir. Tekniğin bilinen durumu ise kanunda şu şekilde tanımlanmıştır: “...(patent) başvuru tari-

hinden önce dünyanın herhangi bir yerinde, yazılı veya sözlü tanıtım yoluyla ortaya konulmuş veya kullanım ya da başka herhangi bir biçimde açıklanmış olan toplumca erişilebilir her şeyi kapsar.” Bunun zıt anlamından şu sonuca varılmaktadır: bir buluşta yenilik şartının sağlandığının söylenebilmesi için buluşun; dünyanın herhangi bir yerinde herhangi bir şekilde daha önce ortaya konulmamış, açıklanmamış veya toplumun kullanımına sunulmamış yeni bir özellik göstermesi gerekmektedir.

Buluş Basamağı İçerme Kavramı Nedir?

Kanuna göre; *teknğin bilinen durumu dikkate alındığında, ilgili olduğu teknik alandaki uzmana göre aşikâr olmayan buluşun, buluş basamağı içerdiği kabul edilir.* Yani, eğer bir buluş ilgili olduğu alandaki teknik uzman nezdinde aşikârsa ve biliniyorsa, herhangi bir farklılık teşkil etmiyorsa bu durumda bir buluş basamağından bahsedilmesi mümkün değildir.

Sanayiye Uygulanabilirlik Kavramı Nedir?

Buluşların patente konu olabilmesi için sanayinin herhangi bir dalında üretilebilmesi veya kullanılabilir nitelikte olması gerekmektedir. Uygulaması olmayan sadece teoride kalan buluşların sanayiye uygulanabilir olduğu söylenememektedir. Buluşların kural olarak teknik bir soruna ilişkin tekrarlanabilir teknik bir çözüm oluşturması beklenmektedir. Tek seferlik çözümler ya da tekrarlanması mümkün olmayan buluşlar patente konu edilmeye elverişli değildir.



DİKKAT EDELİM

Sanayiye uygulanabilir olma kavramı başta tarım olmak üzere sanayinin bütün alanlarını kapsamaktadır. Ziraî buluşlar da şartları karşılımları kaydıyla patente konu edilmeye elverişlidir

Patentin Koruma Süresi ve Kapsamı Nedir?

Patentler başvuru tarihinden başlamak üzere yirmi yıllık bir koruma süresine tabidir. Patent sahibi bu süre boyunca patentini aldığı buluşa ilişkin tekel hakkına sahiptir. Bu nedenle patent sahibinin aşağıda sayılan eylemlerin ve durumların önlenmesini talep etme hakkı vardır. Bu eylem ve durumlar ise şu şekildedir:

- Patent konusu ürünün üretilmesi, satılması, kullanılması veya ithal edilmesi veya bu amaçlar için kişisel ihtiyaçtan başka herhangi bir nedenle elde bulundurulması,
- Patent konusu olan bir usulün kullanılması,

- Kullanılmasının yasak olduğu bilinen veya bilinmesi gereken usul patentinin kullanılmasının başkalarına teklif edilmesi,
- Patent konusu usul ile doğrudan doğruya elde edilen ürünlerin satılması, kullanılması, ithal edilmesi veya bu amaçlar için kişisel ihtiyaçtan başka herhangi bir nedenle elde bulundurulması.

Tasarım Nedir?

İçinde bulunduğumuz çağda mal ve hizmetlerin işlevsellikleri kadar görünüşleri de ciddi bir önem arz etmektedir. Görünümü rakiplerine kıyasla daha önde olan mal ve hizmetlerin rekabet açısından daha avantajlı olduğu ve bazen sırf bu sebeple tercih sebebi olduğu durumlarla sıklıkla karşılaşmaktadır. Bir ürünün görünümünün tüketici ve üretici nezdindeki önemi aşikâr olduğundan kanun koyucular bu görünümün hukuken korunmasında fayda olduğu kanaatine varmışlardır.

Hukukumuzda tasarımlar; “ürünün tümü veya bir parçasının ya da üzerindeki süslemenin çizgi, şekil, biçim, renk, malzeme veya yüzey dokusu gibi özelliklerinden kaynaklanan görünümü” olarak tanımlanmaktadır. Tasarımlar, tescil edilmiş olup olmamalarına göre tescilli tasarım ve tescilsiz tasarım olmak üzere iki farklı kategori altında değerlendirilmektedir. Tescilli tasarımlar tescil başvurusundan itibaren beş yıl süreyle korunmakta olup bu süre beşer yıllık yenilenme yoluyla toplamda yirmi beş yıla kadar korunabilmektedir. Tescilsiz tasarımlar ise kamuya sunulduğu tarihten başlamak üzere üç yıl boyunca hukuken korunmaktadır.

Bir ürünün tasarım olarak nitelendirilmesi için iki ana şart vardır. Bunlar yenilik ve ayırt edici nitelik olarak adlandırılmaktadır.

Yenilik Nedir?

Tescilli tasarımlarda yenilik unsuru başvuru tarihi veya rüçhan tarihinden itibaren değerlendirilir. Başvuru tarihinden veya rüçhan tarihinden önce dünyanın herhangi bir yerinde söz konusu tasarım topluma arz edilmemişse bu tasarımın yeni olduğu kabul edilir. Tescilsiz tasarımlarda tasarımın kamuya ilk sunulduğu tarihten öncesi esas alınır.

Ayırt Edici Nitelik Nedir?

Tasarımlarda ayırt edici nitelik şartında dikkate alınan esas unsur tasarımın bilgilendirilmiş kullanıcı üzerinde bıraktığı genel izlenimdir. Tescilli tasarımlar için başvuru veya rüçhan tarihinden önce, kamuya sunulmuş herhangi bir tasarımın aynı kullanıcı üzerinde yarattığı genel izlenimden farklı ise bu tasarımın ayırt edici niteliğe sahip olduğu kabul edilir. Tescilsiz tasarımlar için tasarımın kamuya ilk sunulduğu tarihten öncesi esas alınmaktadır (SMK m. 56/5).

Tasarım Hakkının Kapsamı Nedir?

Tasarım sahibinin tasarımdan kaynaklanan birtakım hakları olup bu haklar münhasıran tasarım sahibine aittir. Tasarımın korunmasının sınırları söz konusu tasarımın özgünlüğüne göre artabilmekte veya azalabilmektedir. Bir tasarım özgün olduğu derecede geniş korumadan yararlanacakken özgünlüğü nispeten daha düşük olan tasarımların koruma kapsamı aynı oranda daha dar olacaktır.

Tasarım sahibinin hakları nedeniyle üçüncü kişilerin söz konusu tasarım üzerindeki tasarruf yetkileri tasarım sahibinin lehine kısıtlanmıştır. *Üçüncü kişiler, tasarım sahibinin izni olmadan koruma kapsamındaki tasarım veya tasarımın uygulandığı ürünü üretmez, piyasaya sunamaz, satamaz, ithal edemez, ticari amaçlı kullanamaz veya bu amaçlarla elde bulunduramaz ya da bu tasarım veya tasarımın uygulandığı ürünle ilgili sözleşme yapmak için öneride bulunamazlar.*

Dijital Ortamda Fikri ve Sınai Haklar

Fikri ve sınai mülkiyetin unsurlarının, öğelerinin ve bu öğelerin esaslarının, korunmalarının kapsamının ve sınırlarının incelendiği bir önceki bölümden sonra bu bölümde söz konusu fikri ve sınai ürünlerin bilişim ortamlarında görünüşleri ve bu konuya ilişkin tartışmalara değinilecektir.

Öncelikle belirtmek gerekir ki hukukumuzda fikri ve sınai hakların dijital ortamlarda kullanılmasına ilişkin ayrı ve tekil bir mevzuat bulunmamaktadır. Konu yine FSEK ve SMK kapsamında değerlendirilmektedir.

Karşılaşılan tartışmaların başında; multimedya eserler, dijital tükenme, yapay zekâ tarafından meydana getirilen eserlerin hukuki statüsü, blokzincir ve türev teknolojilerin fikri ve sınai haklara etkisi ve Metaverse gibi ortamlarda fikri ve sınai hak sahipliği gelmektedir.

Yeni Bir Eser Kategorisi Önerisi Olarak Multimedya Eser

Çalışmanın birinci bölümünde de ifade edildiği üzere bir ürünün eser olarak kabul edilebilmesi ve dolayısıyla eser korumasından faydalanabilmesi için FSEK kapsamında sınırlı sayıda belirtilen eser türlerinden birinin içine girmesi gerekmektedir. FSEK'in kaleme alındığı 1951 yılında belirlenen eser kategorilerinin günümüz fikri ürünlerinin ihtiyaçlarını ne ölçüde karşıladığı tartışmalıdır. Zira, günümüzde yeni teknolojilerin de etkisiyle meydana getirilen fikri ürünler birden fazla eser kategorisine girebilmekte veya her hangi tek bir eser kategorisi altında değerlendirilmeye elverişli olmayabilmektedir. Video oyunları bu kapsamda değerlendirilmeye elverişlidir. **Multimedya eser kavramına neden ihtiyaç duyulduğu video oyunları örneği üzerinden anlatılacaktır.**

Video oyunları bünyelerinde; hikâye, kaynak kodu, ses bileşenleri ve sinematografik unsurlar barındırabilmektedir. Bütün video oyunlarının sayılan bütün unsurlara sahip olması gerekmediği gibi, bazı durumlarda sayılanlardan başka unsurları da pek tabi bünyelerinde bulundurabilmektedirler. Bir video oyunun hikayesinin veya kaynak kodunun FSEK kapsamında ilim ve edebiyat kategorisine girmesi mümkün olduğu gibi ses bileşenlerinin bir musiki eser olarak kabul edilmesi veya animasyonlar ve sair sinematografik unsurlarının sinema eseri olarak nitelendirilmesi mümkündür. Bu durum da video oyunlarının eser niteliğine hâle getirmemektedir.

Video oyunların her ne kadar hikâye, ses bileşeni ve sinematografik unsurlar gibi farklı unsurları olsa da vazgeçilmez olan ve her video oyununda mevcut olan unsur bilgisayar programıdır. Bilgisayar programlarının her bir video oyununun vazgeçilmez ve ayrılmaz parçası olması video oyunlarının sadece bir bilgisayar programından ibaret olduğu yanlışlığına sebebiyet vermemelidir.

Belirtildiği üzere, video oyunları, bünyesinde başlı başına fikri mülkiyet hukukuna konu edilebilecek birçok unsuru barındırdığı için video oyunlarının hangi eser kategorisi altında değerlendirilmesi gerektiği tartışmalıdır. Öğretide kimi yazarlarca video oyunlarının, işlevini sağlayan bilgisayar programı nedeniyle ilim ve edebiyat eseri olduğu; kimi yazarlarca sinema eseri olarak değerlendirilmesi gerektiği, kimi yazarlarsa güncel hukuki durumun bilgisayar oyunlarına yeterli hukuki korumayı sağlamadığını; bu nedenle multimedya eser olarak yeni bir eser kategorisinin mevzuatça tanınması gerektiği savunulmaktadır.

İlim ve Edebiyat Eseri Olduğu Görüşü

Video oyunlarının ilim ve edebiyat eseri olarak kabul edilmesi gerektiğini savunanların ana dayanak noktası FSEK madde 2/1 hükmü olup her video oyunun aslında salt bir bilgisayar programından ibaret olduğu yanılıdır. FSEK madde 2/1 hükmünde ilim ve edebiyat eserleri: *“Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucunu doğurması koşuluyla bunların hazırlık aşamaları”* şeklinde tanımlanmıştır. Gerçekten de video oyunları bir bilgisayar programı üzerine kurulmuştur. Buna rağmen, açıklandığı üzere video oyunları salt bir bilgisayar programından ibaret olmaktan hem insanın entelektüel yaratımı hem de emeği olarak çok ötedir.

Sonuç olarak, video oyununu sadece bir bilgisayar programı ile sınırlandırma yoluna gidildiğinde; eserin kendini gösteriş biçimi olan görsel ve işitsel öğelerin korumadan mahrum kalma ihtimali ile karşı karşıya kalınabilecektir.

Son olarak video oyunlarının salt bir bilgisayar programı olarak kabul edilmesi ihtimalinde tek bir eser sahibi sorunu gündeme gelecektir. Zira, bilgisayar programı sahibi tek kişiyken; bir video oyunun tek bir kişinin fikri ürünü olması ihtimali video oyunlarının içerdiği çeşitli unsurlar nedeniyle oldukça düşüktür. Video oyunlarının bilgisayar programı olarak kabul edilmesi bu açıdan da eser sahipliği hususunda birtakım problemleri beraberinde getirmektedir.

Sinema Eseri Olduğu Görüşü

Sinema eserleri FSEK madde 5’te düzenlenmiş olup *“Sinema eserleri, her nevi bedii, ilmi, öğretici veya teknik mahiyette olan veya günlük olayları tespit eden filmler veya sinema filmleri gibi, tespit edildiği materyale bakılmaksızın, elektronik veya mekanik veya benzeri araçlarla gösterilebilen, sesli veya sessiz, birbiriyle ilişkili hareketli görüntüler dizisi”* olarak tanımlanmıştır.

Video oyunlarının sinema eseri olarak savunulması ihtimalinde oyunun unsurlarını bir araya getiren kişiler yönetmen, oyunun senaryo ve hikayesinin oluşturulmasında görev alan kişiler senaryo sahibi, oyun için özel olarak bir müzik parçası veya ses efekti yaratılmışsa şartları olduğu ölçüde bu kişiler müzik bestecisi, oyun içinde karakterler arasında diyaloglara yer verilmesi halinde ise diyalogları yazan kişiler diyalog yazarı olarak eser sahibi olabilmektedir.

Bilgisayar programı olarak değerlendirilmesine kıyasla video oyunlarının sinema eseri olarak kabul edilmesi eser sahipliği ve diğer unsurların korunması açısından birçok sorunu çözüme kavuştursa da bu durumda da video oyunun teknik temelini oluşturan, onsuz işlev göstermesi mümkün olmayan bilgisayar programı göz ardı edilmektedir.

Multimedya Eser Olduğu Görüşü

Multimedya eser kavramının tam olarak bir Türkçe karşılığı bulunamasa da “çoklu ortam” veya “çoklu eser” olarak dilimize kazandırılması mümkündür. Multimedya eser ile kastedilen aslında birden fazla eser türünün bir araya gelerek kendine has yeni bir eser meydana getirmesidir. Zira, belirtildiği üzere video oyunları farklı eser kategorilerine ait birden fazla eseri bünyesinde barındırmakta; en nihayetinde de hepsinden farklı ve özgün bir eser olarak vücut bulmaktadır.

Bu görüşü savunan yazarların ana çıkış noktaları video oyunlarının kendisini oluşturan eserlerden meydana gelmesine rağmen, bu eserlerin bir araya gelmesi ile kendisini yaratan eser türlerinden bağımsız bir yapıya sahip olmalarıdır. Ayrıca, çalışmanın önceki bölümlerinde de incelendiği üzere, video oyunlarının içine dahil edilmesi muhtemel diğer eser kategorileri ile yeterli düzeyde korunamaması multimedya eser kavramının ortaya çıkmasında bilhassa etkili olmuştur.

Video oyunları ekseninde açıklanmaya gayret edilen multimedya eser kavramı ve bu kavrama neden ihtiyaç duyulduğu sorusu video oyunları dışında başka eserler için de geçerli olabilmektedir. Bir eserin birden fazla eserin bir araya gelmesi ve bölünmez bir bütünlük arz ederek kanunda tanımlanan hiçbir eser kategorisine girmediği durumlarda multimedya eser kavramı gündeme gelebilmektedir.

Klasik Anlamda Tükenme İlkesi ve Dijital Tükenme

Tükenme ilkesi hukukumuzda kural olarak sadece yayma hakkına ilişkindir. Bir eserin aslı veya kopyaları üzerinde eser sahibinin yayma hakkı ilk satıştan veya dağıtımdan sonra sona ermektedir. Bundan anlaşılması gereken; bir fikri ürünün eser sahibi tarafından satıldıktan sonra bunu takip eden satışlara eser sahibinin karışamaması ve bunları engelleyememesidir. Örneğin, ilim ve edebiyat eseri olarak kabul edilmeye elverişli bir kitap kitapçıdan alındıktan sonra bu kitabın üçüncü bir kişiye satılmasına kitabın yazarı olan eser sahibi karışamamaktadır. Bu kitap kural olarak tekrar satışa veya farklı hukuki işlemlere kural olarak konu edilebilmektedir. Başka bir örnekte ise belirli bir marka telefonun satın alındıktan sonra ikinci el olarak satılmasına o telefonun markasının sahibi karışamamaktadır.



EK BİLGİ

Üç tür tükenme türü vardır. Bunlar ülkesel tükenme, bölgesel tükenme ve uluslararası tükenmedir. Ülkesel tükenme, bir ülkede markalı veya patentli bir ürünün hak sahibi tarafından veya onun izni ile satışa sunulduktan sonra söz konusu ülke içerisinde serbestçe dolaşımıdır. X markalı bir ayakkabı bir ülkede hak sahibi tarafından veya onun izni ile satışa sunulduktan sonra, dileyen kişi söz konusu ülkenin herhangi bir bölgesinden X markalı ayakkabıyı satın alıp başka bir bölgesinde satabilecektir.

Bölgesel tükenme, ülkesel tükenmeye benzemekle beraber bu durumda belirli bir ülkeden ziyade ilgili bölge bir ülke olarak kabul edilmektedir. En tipik örneği Avrupa Birliği olup Avrupa Birliği'nde bölgesel tükenme geçerlidir. Markalı veya patentli bir ürünün ilgili bölgenin herhangi bir yerinde satışa sunulması durumunda hak bütün bölgede tükenecektir. Y markalı içeceklerin Avrupa Birliği üyelerinden birinde satışa sunulması durumunda, ilgili içeceklerin bölgenin herhangi bir ülkesinde satın alınıp başka bir ülkesinde satılması mümkündür.

Uluslararası tükenme, markalı veya patentli bir ürünün dünyanın herhangi bir yerinde hak sahibinin izni veya onayı ile satışa sunulması ile hakkın tükenmesidir. Bu durumda, hak sahibi söz konusu ürünün başka ülkelerde satılmasını engelleyemeyecektir. Sınai haklar yönünden ülkemizde açıkça uluslararası tükenme ilkesi kabul edildiğinden paralel ithalat ve gri piyasa serbesttir. Telif hukuku açısından ise yayma hakkı bakımından ülkesel tükenme ilkesi geçerlidir. Bu nedenle yayma hakkının tüketildiği ülke için paralel ithalatın yapılması mümkündür.

Dijital Tükenme

Dijital tükenme olarak yeni bir tükenme kavramına ihtiyaç duyulmasının temel sebebi, dijital ortamda gerçekleştirilen çoğaltma ve yayma faaliyetlerinin fiziki ortama kıyasla neredeyse maliyetsiz olmasıdır. Dijital tükenme, dijital ortamda bir eserin veya sınai ürünün ilk kez satılması veya dağıtılması ile dijital tükenmenin gerçekleştiğini ifade etmektedir. Bu konuya ilişkin yargı kararları somut olaya göre farklılık arz edebilmektedir.

UsedSoft'a Karşı Oracle Davası

Söz konusu davada UsedSoft firması, Oracle tarafından piyasaya sürülen ve satışı gerçekleştirilen yazılımların yeniden satışını gerçekleştirmektedir. Oracle firması ise bu satış gerekçesiyle haklarının ihlal edildiğini iddia etmektedir. Daha önceki bölümlerde de açıklandığı üzere bilgisayar programları FSEK kapsamında ilim ve edebiyat eseri olarak kabul edilmektedir. Tükenme ilkesinin kabul edilmesi halinde UsedSoft bu ilkeye dayanarak ikinci el bilgisayar programı satışı gerçekleştirmeye devam edebilecektir. Tükenme ilkesinin kabul edilmemesi halinde ise Used-Soft'un gerçekleştirdiği satış işlemleri Oracle'ın haklarını ihlal edecektir. Söz konusu somut olay Avrupa Birliği Adalet Divanı'nın ("ABAD") önüne geldiğinde mahkeme, ikinci el satışı gerçekleştirilen bilgisayar programlarına ilişkin yayma hakkının tükendiğine karar vermiştir.

Tom Kabinet Kararı

Tom Kabinet kararı elektronik kitapların ikinci el satışına ilişkindir. Bu olayda ABAD, UsedSoft kararının aksine bir karar vermiş ve elektronik kitaplar noktasında tükenme hakkını kabul etmemiştir. ABAD; kararında, elektronik kitapların ikinci el satışının telif haklarını elinde bulunduranın rızası olmaksızın gerçekleştirilemeyeceğine hükmetmiştir. Tom Kabinet kararı dijital ortamda fikri mülkiyet haklarının korunması noktasında emsal kararlardandır. Bu karar ile tükenme ilkesi dijital ortamın özellikleri dikkate alınarak değerlendirilerek açıklığa kavuşturulmuştur. Ayrıca diğer eser türleri noktasında da şartları uyduğu sürece emsal bir karar özelliği taşımaktadır.

Yapay Zekâ ve Eser Sahipliği

Teknolojideki önü alınamaz hızlı gelişim göz önüne alındığında yapay zekânın bir nevi insan gibi özgün içerikler üretmesi dahi mümkün hale gelmiştir. Bu ürünlerin eser olarak değerlendirilip değerlendirilemeyeceği, eser olarak değerlendirilmesi halinde fikri haklarının kime ait olacağı güncel tartışma konularının başında gelmektedir.

Yapay zekânın meydana getirdiği ürünlerin fikri mülkiyete konu olabilmesi için tıpkı alışılmış klasik eserler gibi eser sıfatını haiz olmaları gerekmektedir. Bunun şartları yukarıda belirtildiği üzere şekil şartı, sübjektif şart ve objektif şarttır.

Yapay zekâ tarafından ortaya konan eserler Fikri ve Sınai Eserler Kanunu'nda sınırlı sayıda belirtilen eser gruplarından birine girmek zorundadır. Günümüzde yapay zekâlar Watson Beat örneğinde olduğu gibi musiki eserler, Racter örneğinde olduğu gibi edebi eserler, DeepDream örneğinde olduğu gibi güzel sanat eserleri ve sinema eserleri üretebilmektedirler.

Anlaşıldığı üzere yapay zekânın ürettiği eserler, eser sayılabilmenin ilk şartlarından olan şekil şartını yerine getirmektedir. FSEK tarafından sınırlı sayıda gösterilen eser türlerinin hemen hemen hepsinde yapay zekâlar şu ana kadar eserler üretmiş ve insanoğlunun kullanımına sunmuştur.

Eser olabilmenin ikinci şartı olan sübjektif şart bakımından ise bu ürünlerin eser sahibinin hususiyetini taşımaları gerekmektedir. Yapay zekâlar da kendi hususiyetlerini taşıyan eserler meydana getirebilmektedirler ve bu eserlerin sayısı azalmak bir yana her geçen gün hızla artmaktadır.

FSEK kapsamında eser sayılabilmenin üçüncü ve son şartı olarak karşımıza objektif şart çıkmaktadır. Bu şart da yapay zekâ tarafından meydana getirilen çoğu ürün açısından sağlanmaktadır.

FSEK madde 8'e göre *"Bir eserin sahibi, onu meydana getirendir."* Yine FSEK madde 1/B (b)'ye göre ise eser sahibi eseri meydana getiren kişi olarak tanımlanmıştır. Bu noktada yapay zekanın meydana getirdiği eser vasfındaki ürünlerin eser sahibinin kim olacağı hususu tartışmalıdır. Zira, yapay zekaya hukukumuzda şu an için hukuki bir kişilik tanınmamıştır. Bu nedenle şu an yapay zekaların eser sahibi olarak kabul edilmesi mümkün görünmemektedir. Bu hususta üç temel görüş bulunmaktadır.

Birinci teoriye göre yapay zekanın fikri meydana getirdiği eserler doğrudan kamuya mal edilmedir. Yapay zekâ bir hukuki kişiliğe sahip olmadığından ve eserin meydana getiriliş noktasında insan katkısından ziyade yapay zekâ etkili olduğundan; yapay zekâ tarafından meydana getirilen eserlerin doğrudan kamuya mal edilmesi savunulmaktadır. Bu yöntemle ile sırf yapay zekâyâ sahip olduğu için bir insanın veya zümrenin yapay zekâ tarafından meydana getirilen eserlerin telif haklarına sahip olmasının önüne geçilmek istenmektedir.

İkincisinde ise yapay zekânın sahibinin eser sahibi olarak kabul edilmesi savunulmaktadır. Bu görüşe göre yapay zekânın sahibi olanlar yapay zekâ tarafından meydana getirilen eserlerin telif haklarına sahip olacaklardır. Yapay zekânın var olmasına imkân tanıyan ve gerekli finansal ve teknolojik altyapıyı sağlayan bu kimseler sonuç olarak ortaya çıkan eserlerin telif haklarına da sahip olacaklardır.

Üçüncü ve pek popüler olmayan diğer teoriye göre ise yapay zekanın kendisine bir hukuki kişilik tanınarak eser sahibi olarak kabul edilmelidir. Bu görüşe göre yapay zekâyı bir nevi hukuki kişilik tanımmalıdır. Kendisine hukuki kişilik tanınan yapay zekâlar sonuç olarak çeşitli haklara sahip olabilecek; ortaya koydukları eserlerin telif haklarını da elinde bulunduracaklardır.

Blokzincir ve Benzer Teknolojilerin Fikri ve Sınai Haklara Etkisi

Blokzincir teknolojisi isminden de anlaşılacağı üzere bloklardan oluşan bir zinciri ifade etmektedir. Her bir blok kendisinden önce gelen bloğa eklenerek bir zincir oluşturmaktadır. Bu bloklar ise verilerden oluşmaktadır. Sonuç olarak veriler blokları oluşturmakta bloklar birbirlerine eklenerek blokzinciri oluşturmaktadır. Tek bir blokzincirden söz edilmesi mümkün değildir. Kullanımda ve proje aşamasında birçok blokzincir bulunmaktadır. Blokzincir teknolojileri genel olarak değiştirilemez, merkeziyetsiz, aracısız, ücretsiz ve global olma hedefleriyle ön plana çıkmakta ve çoğunlukla bir coin veya token arz etmektedirler.

Coinler ve tokenlar barındırdıkları özellikleriyle ve vadettikleriyle farklı kategorilere ayrılabilir. Ana ayrım coin ve token ayrımıdır. Coinleri tokenlardan ayıran en temel fark coinlerin farklı olarak kendilerine ait bir blokzincirleri olmasıdır. Tokenların ise kural olarak kendilerine has bir blokzincirleri bulunmamaktadır. Coinler; Bitcoin, Altcoin, Stablecoin vb. şekilde farklı kategorilere ayrılırken konumuz açısından özel önem arz eden tokenlar ise menkul kıymet tokeni, ödeme tokeni, fayda tokeni, varlığa dayalı token ve NFT olmak üzere farklı kategorilere ayrılmaya elverişlidir. Önemle belirtmek gerekir ki söz konusu sınıflandırma herhangi bir kanundan doğmamakta; öğretide tercih edilen sınıflandırma şeklidir. Coinler ve NFT dışındaki tokenlar bu çalışmanın kapsamına girmediğinden bu konuda daha fazla açıklama yapılmasına yer yoktur. NFT'ler ise "non-fungible token" ifadesinin kısaltmasıdır. Bu ifade Türkçeye misli olmayan, mübadelesi mümkün olmayan token olarak çevrilebilir. NFT'ler eşsiz ve tekindir. Bir NFT bir diğer NFT'nin yerini almaya elverişli değildir.

Fikri ürünler doğaları gereği genel olarak özgünlük, teklik ve eşsizlik ister ve barındırırlar. NFT'lerin eşsiz ve tekil olmaları nedeniyle eser sahiplerinin ve sektör paydaşların NFT'ye olan ilgisi artarak devam etmektedir. Dijital sanat eserleri kolayca kopyalanabilmektedir ve fiziksel sanat eserlerin aksine söz konusu kopyalar orijinal sanat eseri ile tıpatıp aynıdır. Bu nedenle, dijital sanat eserlerinde ve genel olarak dijital eserlerde orijinallik karşılaşılan önemli bir sorundur. NFT'ler ise bu noktada bir çözüm olma potansiyeli taşımaktadır. Dijital bir sanat eseri NFT haline getirilirse bu durumda eşsiz de olabilmektedir. Blokzincirde yer alan ve kural olarak değiştirilemez olan veriler ile söz konusu NFT'nin ve barındırdığı eserin orijinal eser olduğu tespit edilebilmektedir.

Fiziki eserlerin dijitalleştirilmesi noktasında ise çeşitli ihtilafların yaşanması muhtemeldir. Bir eserin NFT haline getirilmesi eser sahibinin haklarını ihlal eder nitelikte olabilir. Bir eserin, eser sahibinin onayı ve/veya rızası olmaksızın NFT haline getirilmesi ve alım-satım gibi çeşitli hukuki işlemlere konu edilmesi eser sahibinin *eserde değişiklik yapılmasını engelleme, işleme, çoğaltma, yayma, işaret, ses ve/veya görüntü nakline yarayan araçlarla iletim hakkının* ihlal edilmesine yol açabilmektedir.



GÜNLÜK HAYATLA İLİŞKİLENDİRELİM

Cem Karaca'nın bir fotoğrafının Cem Karaca'nın mirasçılarının onayı ve/veya rızası alınmaksızın NFT haline getirilmesi mirasçıları tarafından dava konusu edilmiştir. Dava sürecinde mahkeme NFT için ihtiyati tedbir kararı vermiştir.

Fikri mülkiyet hukukunun klasik kavramlarını ve sistematüğını zorlayan bir diğer husus ise akıllı sözleşmelerle karşımıza çıkmaktadır. Akıllı sözleşmeler en basit tanımı ile tarafların birbirine güven duymak zorunda kalmaksızın, açıkladıkları iradelerin zamanı geldiğinde ve şartları gerçekleştiğinde kendiliğinden icra edilebildiği sözleşmelerdir. Günümüzde akıllı sözleşmeler ve NFT'ler çoğu zaman birlikte görülmektedir. Akıllı sözleşmeler ile NFT haline getirilen bir eserin mali haklarının devri gündeme gelebilmektedir. Mali hakların devrine ilişkin sözleşmelerin yazılı olarak akdedilmesi kanuni bir zorunluluktur. Bu nedenle akıllı sözleşmeler ile mali hakların devri şu anki haliyle mümkün görünmemektedir.

Metaverse ve Benzeri Ortamlarda Fikri ve Sınai Haklar

Gelişen teknolojiler ile gündemimize giren en yeni ve popüler kavram olan Metaverse, bünyesinde fikri ve sınai haklara ilişkin birçok tartışmalı hususu bulundurmaktadır. Metaverse genel olarak artırılmış gerçeklik, sanal gerçeklik, giyilebilir teknolojiler ve internet altyapısının gelişmesi ve yaygınlaşması ile birlikte fiziksel ve dijital dünyayı bir araya getiren sanal bir dünya olarak tanımlanabilmektedir.

Metaverse'lerde kullanıcılar birbirleriyle genellikle avatarları aracılığıyla etkileşime girmektedir. Avatar ise kullanıcıların Metaverse'de kendilerini sanal olarak temsil ettikleri karakterler ve görünüm-lerdir. Kullanıcılar avatarları aracılığıyla Metaverse'de yer alan etkinliklere katılabilmekte, birbirleriyle etkileşime geçmekte hatta Metaverse'in yaratılışında ve geliştirilmesinde içerik üretici olarak katkıda bulunmaktadır. Metaverse'lerin fikri mülkiyet hukuku açısından değerlendirilmesi gereken asıl noktası da tam olarak budur. Web 1.0'ın aksine kullanıcılar artık Metaverse ve benzeri platformlarda sadece tüketici olarak yer almamaktadır. Çoğu zaman bu platformların meydana getirilmesinde dahi etkin rol almakta, hatta bu durum Metaverse'i işletenler tarafından da özellikle desteklenmektedir.

Metaverse'lerde kullanıcıların sadece tüketici olarak yer almasından ziyade üretici olarak yer almasının mümkün ve teşvik edilir olması kullanıcılarının bu dijital ortamlarda eser üretmelerini, buluşlar ve tasarımlar meydana getirmelerini dahi mümkün kılmaktadır. Kullanıcıların daha bu dijital ortama ayak basmadan önce meydana getirdikleri avatarlar dahi şartlarını sağladıkları takdirde eser olarak tanımlanmaya elverişlidir. Eser olmanın şartlarını yerine getiren bir fikri ürünün sırf Metaverse

gibi dijital bir ortamda meydana getirilmiş oluđu o fikri ürünün eser olarak nitelendirilmesini engellemeyecektir. Aynı durum sinai mülkiyet hukuku için de geçerlidir. Metaverse’de gerçekleştirilen bir buluş şartlarını taşıdığı ölçüde patente konu edilebilmekte; yine aynı şekilde bir tasarım ortaya konabilmektedir. Bu durumlarda da sinai mülkiyetin temel kural ve prensipleri uygulama alanı bulacaktır.

Metaverse’lerde fikri ve sinai hakların ihlal edilmesi, karşılaşılması muhtemel risklerdendir. Fiziki dünyada var olan ve hukuken koruma altına alınan bir tasarımın veya markanın Metaverse’de hak sahiplerinin onayı olmaksızın kullanılması ihtilaflara yol açmaya elverişlidir. Hak sahiplerinin hakları bu durumlarda da geçerliliğini koruyacaktır. Bu ihlallerin dijital ortamda gerçekleştirilmesi bu eylem ve durumların ihlal teşkil ettiği gerçeğini değiştirmeyecektir.

BÖLÜM ÖZETİ

Fikri mülkiyet hukuku, eser sahipleri ile diğer ilgililer arasındaki menfaat çatışmasının sonucu olarak ortaya çıkmıştır. Türkiye’de fikri mülkiyetin düzenlenmesinde temel kanunlar, 1951 tarihli Fikir ve Sanat Eserleri Kanunu ve 2016 tarihli Sınai Mülkiyet Kanunudur. Fikir ve Sanat Eserleri Kanunu’na göre eser sahibi eseri meydana getiren kişidir. Eser sahibinin hakları, yaşam süresi boyunca devam eder ve ölümünden sonraki yetmiş yıl boyunca mirasçılara geçer. Eser sahibinin manevi hakları arasında eseri umuma arz etme, eser sahibi olarak tanıtılma, eserde değişiklik yapılmasını engelleme ve eseri sahiplenme hakkı yer almaktadır. Mâli hakları ise işleme, çoğaltma, yayma ve iletim hakları içerir.

Sınai mülkiyetin konusu marka, patent, tasarım gibi unsurlardan oluşur. Markanın amacı, bir teşebbüsün ürün ve hizmetlerini diğerlerinden ayırmaktır. Markalar, tescil edildikten sonra on yıl süreyle korunur ve bu süre onar yıllık dönemlerle yenilenebilir. Marka sahibi, markasının izinsiz kullanılmasını engelleme hakkına sahiptir. Benzer şekilde patentler de 20 yıl boyunca korunur ve patent sahibi buluşun izinsiz üretilmesini, satılmasını veya kullanılmasını engelleyebilir.

Tasarımlar ürünlerin çizgi, şekil, renk gibi özelliklerinden kaynaklanan görünümüdür. Tescilli tasarımlar, başvurudan itibaren beş yıl süreyle korunur ve bu süre beşer yıllık yenilemelerle 25 yıla kadar uzatılabilir. Tasarımlar, yenilik ve ayırt edici nitelik taşımalıdır. Tasarım sahibi, izinsiz kullanım durumunda üçüncü kişilerin tasarımını üretmesini, satmasını ve ticari amaçla kullanmasını engelleyebilir.

Yapay zekânın ürettiği eserler, Fikir ve Sanat Eserleri Kanunu’na göre eser sayılabilir. Ancak yapay zekâ, hukuki kişiliği olmayan bir varlık olduğundan, eser sahibi olarak kabul edilip edilemeyeceği tartışmalıdır. Bu konuda üç ana görüş vardır: birinci görüş, yapay zekâ tarafından üretilen eserlerin kamu malı olması gerektiğini savunur. İkinci görüş, yapay zekânın sahibinin eser sahibi olarak kabul edilmesini öngörür. Üçüncü görüş ise yapay zekânın hukuki kişilik kazanarak eser sahibi olmasını savunur.

NFT’ler, eşsiz dijital varlıklardır ve dijital sanat eserlerinin özgünlüğünü sağlamada kullanılır. NFT’ler, dijital sanat eserlerinin kopyalanabilir olmasına karşılık, fiziksel eserlerden farklı olarak eşsizliği garanti eder. Ancak bir eserin izinsiz şekilde NFT’ye dönüştürülmesi, eser sahibinin haklarını ihlal edebilir.

Metaverse, dijital dünya ile fiziksel dünyanın birleşimi olan sanal bir ortamdır. Kullanıcılar, yalnızca tüketici olarak değil üretici olarak da yer alır ve eserler üretebilirler. Metaverse’de oluşturulan eserler, fikri mülkiyet haklarına tabi olabilir. Ayrıca, Metaverse ortamında da sınai ve fikri mülkiyet hakları ihlalleri yaşanabilir. Bir markanın veya tasarımın izinsiz kullanımı, dijital ortamda da hukuki sonuç doğurur.

GÖZDEN GEÇİRELİM

- 1) Bir ürünün eser niteliği taşıması için üç ana şartın gerçekleşmesi gerekip bu şartlar; şart, şart ve şarttır.
- 2) şart ile kastedilen; eserin, eser sahibinin hususiyetini taşımasıdır.
- 3) Eser sahipliğinden doğan haklar eser sahibi müddetçe devam eder ve eser sahibinin ölümünden itibaren yıl boyunca mirasçılarını nezdinde devam eder.
- 4) Bir teşebbüsün mallarının ve hizmetlerinin diğer teşebbüslerinin mallarından ve hizmetlerinden ayrılmasını sağlayan işaretlere denir.
- 5) Markalar başvuru tarihinden itibaren yıl süre ile koruma altındadır ve bu süre yıllık dönemler halinde herhangi bir sınırlandırma olmaksızın yenilenmeye devam edilebilir.
- 6) Buluş basamağı içermesi ve sanayiye uygulanabilir olması şartıyla teknoloji alanındaki yeni buluş konu olabilir.
- 7) Patentler başvuru tarihinden başlamak üzere yıllık bir koruma süresine tabidir.
- 8) Ürünün tümü veya bir parçasının ya da üzerindeki süslemenin çizgi, şekil, biçim, renk, malzeme veya yüzey dokusu gibi özel-liklerinden kaynaklanan görünümüne denir.
- 9) Yapay zekanın eser sahipliği hususunda üç ana teori vardır. Birinci teoriye göre yapay zekanın fikri meydana getirdiği eserler doğrudan mal edilmelidir. İkincisinde ise yapay zekanın sahibinin olarak kabul edilmesi savunulmaktadır. Üçüncü ve pek popüler olmayan diğer teoriye göre ise yapay zekanın kendisine bir tanınarak eser sahibi olarak kabul edilmelidir.
- 10) Taraflar arasında güven ilişkisine ihtiyaç duyulmaksızın yeri ve zamanı geldiğinde kendiliğinden ifa olan sözleşmelere denmektedir.

CEVAP ANAHTARI

1. şekli/objektif/subjektif	6. patent
2. Subjektif	7. yirmi
3. yaşadığı/yetmiş	8. tasarım
4. marka	9. kamuya/eser sahibi/hukuki kişilik
5. on, onar	10. akıllı sözleşme

SÖZLÜK

Akıllı Sözleşme: Taraflar arasında güven ilişkisine ihtiyaç duyulmaksızın yeri ve zamanı geldiğinde kendiliğinden ifa olan sözleşme türüdür.

Blokzincir: Veri içeren blokların birbirlerine eklenmesiyle oluşturulan kriptografik zincirdir.

Eser: Sahibinin hususiyetini taşıyan ve ilim ve edebiyat, musiki, güzel sanatlar veya sinema eserleri olarak sayılan her nevi fikir ve sanat mahsulleridir.

Marka: Bir teşebbüsün mallarının ve hizmetlerinin diğer teşebbüslerinin mallarından ve hizmetlerinden ayrılmasını sağlayan işarettir.

Metaverse: Artırılmış gerçeklik, sanal gerçeklik, giyilebilir teknolojiler ve internet altyapısı-nın güçlenmesiyle fiziki ve sanal dünyayı bir araya getirmeyi hedefleyen bir nevi evrendir.

NFT (Non-fungible Token): Misli olmayan, tekil, eşsiz token türüdür.

Patent: Buluş basamağı içermesi ve sanayiye uygulanabilir olması şartıyla teknoloji alanındaki her yeni buluştur.

Tasarım: Ürünün tümü veya bir parçasının ya da üzerindeki süslemenin çizgi, şekil, biçim, renk, malzeme veya yüzey dokusu gibi özelliklerinden kaynaklanan görünümüdür.

KAYNAKÇA

- Bilgili, Fatih/Cengil, Fatih: BlockChain ve Kripto Para Hukuku, Güncellenmiş 2. Baskı, Dora Yayınevi, 2022.*
- Çağlayan Aksoy, Pınar: Akıllı Sözleşmelerin Kuruluşu ve Geçerlilik Şartları, Güncellenmiş 2. Baskı, On İki Levha Yayınevi, İstanbul 2021.*
- Çağlayan Aksoy, Pınar/Özkan Üner, Zehra: NFTs and Copyright: Challenges and Opportunities, Journal of Intellectual Property Law & Practice, Oxford University Press, 2021, C. 16, S. 10.*
- Doğancı, Doğa Ekrem: Blokzincire Dayalı Akıllı Sözleşmelerin Hukuki Nitelikleri, Kuruluşu, Yorumu, İfası ve Bazı Örnek Hukuki Uygulamalar, On İki Levha Yayınevi, İstanbul 2021.*
- Gokmi, K./Jeon, J. H.: A Study on the Copyright Survey for Design Protection in Metaverse Period. International Journal of Advanced Smart Convergence Vol.10 No.3*
- Grosheide F. Willem/Herwini Roerdink/Karianne, Thomas: "Intellectual Property Protection for Video Games: A View from the European Union" (2014) 9 J Int't Com L & Tech 1.*
- Hristov, Kalin: Artificial Intelligence And The Copyright Dilemma, 2017 (57) (3), IDEA: The Journal of the Franklin Pierce Center for Intellectual Property.*
- Karimov, Elnur: "Bilgisayar (Video) Oyunlarının Fikir ve Sanat Eserleri Kapsamında Korunmasında Uygun Eser Kategorisi Sorunu" (2021) J Com & Intell Prop L 93.*
- Kaynak Koç, Selva/Tevetoğlu, Mete: "Bilgisayar Oyunlarının Telif Hakkı Korumasından Yararlanmaması", (2012), Fikri ve Sınai Haklar Dergisi, Sayı 30.*
- Ondrejka, C.: Escaping the Gilded Cage: User Created Content and Building the Metaverse. New York Law School Law Review, 49(1).*
- Öğretmen Kotil, Zeynep: Avatarlar ve Temsil Ettikleri İnsanlar Arasındaki İlişki Bakımından Hukuki Sorumluluk, İstanbul Barosu, Bilişim Hukuku Komisyonu, Yapay Zeka Çalışma Grubu, Yapay Zeka Çağında Hukuk, 2022.*
- Palace, Victor M.: "What If Artificial Intelligence Wrote This? Artificial Intelligence And Copyright Law" (2019) 71, Florida Law Review, 217, 218.*
- Reuveni, E.: "On Virtual Worlds: Copyright and Contract Law at the Dawn of the Virtual Age" Indiana Law Journal. Vol. 82.*
- Stein, Julian: "The Legal Nature of Video Games – Adapting Copyright Law to Multimedia" Press Start (2015), Cilt 2, Sayı 1.*
- Su Li Cheng, T.: Brave New World for Intellectual Property Rights. Journal of Law, Information and Science, 17.*
- Suluk, Cahit/Nal, Temel/Karasu, Rauf: Fikri Mülkiyet Hukuku, Güncellenmiş 6. Baskı, Seçkin Yayıncılık, Ankara 2022.*
- Tekinalp, Ünal: Fikri Mülkiyet Hukuku, Güncelleştirilmiş ve Genişletilmiş Beşinci Bası, Vedat Kitapçılık, İstanbul 2021.*
- Tevetoğlu, Mete: Hukuki Yönleriyle Kripto Varlıklar ve Kripto Varlıkların İlk Arzı, Genişletilmiş 2. Baskı, Aristo Yayınevi, İstanbul 2021.*
- Zorluel, Mustafa, Yapay Zekâ ve Telif Hakkı, 2019 (142) TBB Dergisi.*

ÜNİTE 7

ELEKTRONİK TİCARETİN
VERGİLENDİRİLMESİ

Dr. N. Nilay DAYANÇ KUZEYLİ

ANAHTAR KAVRAMLAR

E-ticaret
Vergi
Dijital ekonomi
Matrah aşındırma ve kar aktarımı,
Çifte vergilendirme
Dijital hizmet vergisi

ELEKTRONİK TİCARETİN VERGİLENDİRİLMESİ

ÖĞRENME HEDEFLERİ

-  1 E-ticaretin neden olduğu vergisel sorunların neler olduğunu öğrenmek
-  2 Geleneksel ticaretin vergilendirilmesi için uygulanagelen sistemin e-ticaretin vergilendirilmesinde neden yetersiz kaldığını öğrenmek
-  3 E-ticaretin yarattığı vergisel sorunlarla mücadelede atılan adımların neler olduğu hakkında bilgi sahibi olmak
-  4 Türk hukukunda e-ticaretin nasıl vergilendirileceği konusunda fikir yürütebilmek
-  5 Verilerin korunması yollarını tartışır.

GİRİŞ

Elektronik ticaret (e-ticaret), en dar anlamı ile fiziksel veya dijital mal ve hizmet alışverişinin elektronik ortamda gerçekleştirilmesi şeklinde tanımlanabilir. E-ticaret günümüzde teknolojik gelişmelerin sunduğu olanaklar sayesinde fiziki sınırlamalardan bağımsız yeni bir ticaret şekline dönüşmüştür. Bu durum günümüzde işletmelerin iş yapış şekillerini büyük ölçüde etkilemiştir. Son yıllarda ekonominin büyük ölçüde dijitalleşmesi ile birlikte birçok yeni iş modeli ortaya çıkmış ve geleneksel iş modelleri büyük ölçüde değişime uğramıştır. Her geçen gün yeni ticaret araçları ve alanları ortaya çıkmaya devam etmektedir. E-ticaret ile birlikte işletmeler, mal ve hizmetlerini müşterilerinin bulunduğu ülkede fiziki varlık göstermeden veya herhangi bir temsilciliği bulunmadan sunabilme imkanına sahip olmaktadır. Bu durum, işletmelerin faaliyetin yapıldığı ülkede vergi ödemeksizin gelir elde edebilmelerine imkan vermektedir. Bunun nedeni ise, ulusal ve uluslararası vergi sistemlerinin fiziki varlığa dayalı olacak şekilde kurgulanmış olmasıdır.

Açıklanan sebeplerle e-ticaretin vergilendirilmesinde ulusal ve uluslararası vergi sistemlerinin teknolojik ilerlemenin gerisinde kaldığı söylenebilir. Bu sebeple de coğrafi sınırlara bağlı kalmayan ve geleneksel ticaretin kâlıplarına uymayan e-ticaretin, işletmelere ve tüketicilere büyük kolaylıklar sağlarken devletler açısından büyük vergi kayıplarına yol açtığı görülmektedir. Dolayısıyla e-ticaretin günümüzde geldiği nokta, devletlerin vergi gelirlerini doğrudan etkilemektedir¹. Oluşan bu durum ulusal ve uluslararası vergilendirmenin temel sorunlarından birini oluşturmaktadır. Uluslararası e-ticaret, birden çok ülkenin vergilendirme yetkisini gündeme getirebileceği gibi, hiçbir ülkenin vergilendirme yetkisi kapsamına girmemesi, dolayısıyla e-ticaret sebebiyle elde edilen gelirlerin vergilendirilememesi de söz konusu olabilir. Bu açıdan uluslararası çifte vergilendirmeyi önleme anlaşmaları (ÇVÖA) bir çözüm olarak gözükmekle birlikte ÇVÖA'larda yer alan işyeri kavramı e-ticaretin gerekliliklerini karşılamaya yetmediğinden başka çözümler gündeme gelmiştir. Bu çözümler dijital hizmet vergileri gibi ulusal çözümler ve uluslararası alanda özellikle OECD tarafından geliştirilen çözümler olarak karşımıza çıkmaktadır. Bu bölüm kapsamında ilk olarak e-ticaretin vergilendirilmesinde kabul edilen esaslar aktarıldıktan sonra Türkiye'de e-ticaretin vergilendirilmesi ve uluslararası alanda e-ticaretin adil bir şekilde vergilendirilebilmesi için atılmış olan adımlar anlatım konusu yapılacaktır.

¹E-ticaret, ülkeler arasındaki vergi rekabetinin de artmasına sebep olmuştur. E-ticaretin sermayenin dolaşımındaki serbestiyi arttırması, kişilerin yatırım ve işle ilgili kararlarında öncelikli olarak ülkelerin vergi oranlarını göz önünde bulundurmasına neden olmuştur. Bu açıdan ülkelerin vergi politikaları ile ticaret arasında yakın bir ilişki bulunmaktadır. Ülkeler vergi oranlarını düşük tutarak dolaşımdaki sermayeyi kendilerine çekmeye başlamışlar, bu ise ülkeler arasında serbest dolaşan yerli ve yabancı sermayeyi çekmek amacıyla uygulanan vergi politikaları açısından ülkeler arasındaki rekabeti artırmıştır.

Vergilendirme Yetkisinin Kullanımı

Elektronik ticaret ulusal ve uluslararası elektronik ticaret olarak ele alınabilir. Ulusal elektronik ticarete devletlerin vergilendirme yetkisi açısından bir sorun bulunmamaktadır. Uluslararası e-ticaret kapsamında yaygın uygulama çoğu ülkenin kendi sınırları içinde elde edilen gelir üzerinden vergi salmasıdır. Bazı ülkeler ise, kendi sınırları içinde yaşayan kişilerin gelirleri üzerine vergi salar. Elektronik ticaret ülkelerin sınırlarını kolaylıkla aştığından bir ticari işlem aynı anda birden çok devletin vergilendirme yetkisini gündeme getirebilir. Burada elde edilen gelirin hangi ülkenin egemenlik alanına girecek vergilendirme yetkisinin olduğu konusu vergilendirme açısından önem taşımaktadır. Uluslararası vergilendirmenin en temel meselelerinden biri işte bu vergilendirme yetkisinin devletlerarası bölüşümüdür.

Kaynak Esaslı Vergilendirme

Pek çok devlet, kaynağı kendisinde olduğu için gelir üzerinden vergi alır. Kaynak esaslı vergilendirme bir devletin kendi sınırları içinde elde edilen gelirden, elde edenin ülkede yerleşik olup olmadığına aldırmaksızın vergi almasına imkan sağlar. Kaynak, “gelir üreten (doğuran) faaliyetin gerçekleştiği yer” olarak tanımlanabilir. Genel olarak ifade etmek gerekirse, ulusal hukuklarda, çoğu zaman, ticari kazançlara vücut veren faaliyetlerin gerçekleştiği yer o kazançların kaynağı olarak kabul edilir. Benzer şekilde, bir gayrimenkulün bulunduğu yer, o gayrimenkulden elde edilen gelirin kaynağı; fikri hakların kullanıldığı yer de o fikri hakkın lisanslanmasının karşılığı olan gayri maddi hak bedellerinin (royalty) kaynağı olarak kabul edilir. Vergi anlaşmalarında da benzer hükümler yer alır. Anlaşmalar, ticari kazançlar bakımından, bir ülkenin kendi sınırları içinde doğan ticari kazançlar ile esaslı bir ekonomik bağının ve dolayısıyla devletin bu kazançlar bakımından vergilendirme yetkisinin bulunup bulunmadığının belirlenmesinde “işyeri” kavramından yararlanırlar. Kaynak, gelirin kendisinden elde edildiği sermayeye, finansal kaynağa değil; geliri üreten mal veya faaliyetlerin coğrafi kökenine işaret eder. Ancak, gelirin üretilmesi ile bunun coğrafi kökeni arasındaki bağı tespit etmek kolay değildir. Çoğu zaman, gelirin birden fazla ülke ile bağlantısı olabilir; bu halde ilgili ülkelerin tümündeki kaynağın tespitine ilişkin kuralların birlikte değerlendirilmesi gerekir.

Yerleşme Esaslı Vergilendirme

Vergilendirme yetkisinin kullanımının ikinci türü bir ülkede yerleşme ile karşımıza çıkar. Yerleşme esaslı vergilendirme, ülke ile vergi yükümlüsü arasındaki bağa vurgu yaparak, devletin, ülkede yerleşik (yerleşmiş) kişilerin dünya çapında elde ettikleri gelirlerin tümü üzerinden vergi almasını mümkün kılar. Bu bakımdan gelirin kaynağının vergilendirme üzerinde etkisi yoktur. Yerleşme, ülke ile yükümlü arasında kişisel bir bağ kurar ve bu bağ devletin o yükümlüye vergi salmasını meşrulaştırır.

Bir kişi, bir ülke ile yakın kişisel veya ekonomik bağlara sahipse o ülkede yerleşik kabul edilir. Bir kişinin birden fazla ülke ile yakın kişisel ve ekonomik ilişkilerinin olması da mümkün olduğuna göre, o kişinin birden fazla ülkede yerleşik olması ve dolayısıyla, birden fazla ülkede yerleşme esaslı vergilendirmeye tâbi tutulması da elbette mümkündür.

Vergilendirme Yetkisi İhtilaflarının Sonuçları

Bir devletin vergilendirme yetkisi, o devletin kaynak olmasından veya o devlette yerleşik olunmasından kaynaklanabilir. Buna ek olarak, ilgili ulusal hukuklar ve vergi anlaşmaları uyarınca vergi konusu gelir birden fazla ülkeden kaynaklanmış olabileceği gibi, yükümlü de birden fazla ülkede yerleşik olabilir. Bu durum, ülkelerin vergilendirme yetkilerinin çatışmasına yol açar. Daha az karşılaşılsa da bunun aksi de mümkündür. Bir diğer ifade ile, hiçbir devletin yetki alanına girmeyen bir gelir de söz konusu olabilir. Özellikle de e-ticaret kapsamında kaynağın tespitindeki güçlük ve yerleşmeye gerek olmaması gibi durumlar daha çok vergilendirme yetkisi ihtilafına yol açabilecek niteliktedir.

Vergiden Kaçınma ve Vergi Kaçırma

Uluslararası e-ticaret faaliyetleri çifte (hatta çoklu) vergilendirmeyi gündeme getirebileceği gibi vergiden kaçınma veya vergi kaçırma ile sonuçlanabilir. En genel hatlarıyla “vergiden kaçınma”, hukuka uygun yollarla vergi yükünün hafifletilmesi veya tümüyle ortadan kaldırılmasını; “vergi kaçırma” ise aynı sonuca hukuka aykırı yollardan ulaşılmasını ifade eder.

Çifte Vergilendirme

“Çifte vergilendirme”, “iki (ya da daha çok) devlette benzer vergilerin aynı yükümlü üzerine aynı vergiyi doğuran olay nedeniyle ve eş zamanlı vergilendirme dönemlerinde salınması” olarak tanımlanabilir. Çifte vergilendirme iç hukuklarında yerleşikliği tespit için farklı normlar benimseyen devletlerin ilgili normlarının çelişmesinden kaynaklanabilir. Devletlerden her biri kişiyi kendi ülkesinde yerleşik ve dolayısıyla vergilendirme bakımından (tam) yükümlü sayabilir. Birden fazla ülkede yerleşik olmak, eğer yerleşik olunan ülkelerden her biri yükümlünün gelirinin tümünü (küresel gelirini) kaynağına bakmaksızın vergilendirmekle, çifte vergilendirmeye yol açar. Bu durum “yerleşme-yerleşme çatışmasından doğan çifte vergilendirme” olarak adlandırılır. Benzer şekilde, ancak daha nadiren, çifte vergilendirme devletlerin birbiriyle çelişen gelirin kaynağı olma iddialarından doğabilir. Bu durum “kaynak-kaynak çatışmasından doğan çifte vergilendirme” olarak nitelendirilebilir ve bir gelir unsurunun birden fazla ülkede, o ülkenin kaynaklarından doğmuş, elde edilmiş sayılması halinde söz konusu olur.

Çoğu devlet geliri hem kaynak esaslı hem de yerleşme esaslı olarak vergilendirmektedir. Ülkede yerleşik bir yükümlü genellikle küresel geliri üzerinden vergilendirilir; oysa, yerleşik olmayanlar sadece ülkeden kaynaklanan gelirleri üzerinden vergilendirilirler. Bir ülkede yerleşik olan bir yükümlünün diğer bir ülkedeki kaynaklardan gelir elde etmesi halinde ülkelerin “yerleşme-kaynak iddialarının çatışmasından doğan çifte vergilendirme” durumu söz konusu olur.

Ülkelerin çatışan vergilendirme yetkisi kullanımlarından doğan çifte vergilendirme sorununu gidermek için ülkeler iç hukuklarında birtakım önlemler aldıkları gibi uluslararası anlaşmalar yapmak suretiyle de çözümler üretme yoluna gitmişlerdir. Bu kapsamda vergi anlaşmaları sözleşen tarafların uluslararası çifte vergilendirmenin ve vergi uygulamalarında ayrımcılığın önlenmesi, vergi idareleri arasında bilgi paylaşımı ile vergi kaçakçılığının önüne geçilmesi ve vergi pastasının adil paylaşımı için karşılıklı olarak verdikleri tavizleri yansıtır.

Türkiye, gelirden alınan vergilerde uluslararası çifte vergilendirmenin önlenmesi için çoğu OECD, bir kısmı da Birleşmiş Milletler modelini temel alan seksen altı adet iki taraflı vergi anlaşmasının tarafıdır. Bununla birlikte, pek çok ülke gibi Türkiye’de iç hukukunda çifte vergilendirmeyi önlemeye yönelik hükümler barındırmaktadır.

İş Yeri Kavramı

Vergi anlaşmaları gelir unsurları arasında aktif-pasif gelir ayrımı yapmak suretiyle vergilendirme yetkisini taraf devletler arasında paylaşırlar. Buna göre, bir ülkede aktif bir ticari faaliyet (ya da esaslı bir ekonomik varlık) olması halinde, ki bu anlaşmalarda karşımıza “işyeri” kavramıyla çıkar, o ticari faaliyetten elde edilen kazançları vergilendirmede birincil yetki kaynak ülkeye ait olur. Bu durumda kaynak ülkede ödenmiş vergilerin yerleşim yeri ülkesinde tekrar ödenmesini önlemek için gerekli önlemleri alma görevi ikinci ülkeye yüklenir. Kaynak ülkede bir işyeri bulunmaması halinde bu ülke vergilendirme yetkisini kaybeder ve ticari kazançlar sadece yükümlünün yerleşik olduğu ülkede vergilendirilir.

Dijital ekonominin getirmiş olduğu vergisel sorunlar çok yönlü olsa da sorunun “işyeri”ne ilişkin temelinde Model Anlaşmalar uyarınca kullanılan işyeri kavramının, vergilendirme yetkisini kaynak ülkeye verirken o ülkede bir “fiziksel varlık” gerektirmesi şartı bulunmaktadır. Ancak çoğu dijital teşebbüste işyeri oluşturacak nitelikte bir fiziksel varlık bulunmamaktadır. Model Anlaşma’nın 5. maddesinin 1. fıkrasında “işyeri” şu şekilde tanımlanmıştır: “Bu Anlaşmanın amaçları bakımından “işyeri” terimi, bir teşebbüsün işinin tamamen veya kısmen yürütüldüğü işe ilişkin sabit bir yer anlamına gelir.” Görüldüğü üzere tanım iş yeri olarak sabit bir yeri esas almaktadır ancak e-ticaret fiziki işyeri ölçütünü anlamsız bıraktığından işyeri kavramına ilişkin bu kurallar yetersiz kalmaktadır.

Ticari kazançların vergilendirilmesi bakımından OECD Modelinin üzerine inşa edildiği temel ilke uyarınca bir devletin bir teşebbüsü bir diğer devlette bir “işyeri” aracılığıyla ticari faaliyet sürdürmediği sürece o diğer devlet tarafından doğrudan vergilendirmeye tabi tutulması mümkün değildir. İşyerinin varlığı halinde ise devlet sadece “işyerine atfedilebilen kazançlar” üzerine vergi salma imkanı kazanır.

OECD, dijital ekonomide matrah aşındırma ve kar aktarımı olanakları çerçevesinde yeni iş modellerinin neden olduğu vergi sorunlarını fiziksel bağ (nexus), veri ve dijital ekonomiden elde edilen kazançların nitelendirilmesi olarak ele almaktadır. Fiziksel bağ sorunu, işletmelerin yerleşik oldukları ülke dışında bilgi ve iletişim teknolojilerindeki gelişmelerle bir daimi işyeri (permanent establishment) ya da yavru şirket olmaksızın da ekonomik faaliyette bulunma imkanına sahip olması ile ilgilidir.

Birçok dijital iş modelinde, kaynak ülkede fiziksel bir mevcudiyeti olmayan bir şirket, internet sitesi veya başka bir dijital yolla (örneğin cep telefonundaki bir uygulama) o ülkedeki müşterilerle etkileşim kurabilmektedir. Bu noktada web sitelerinin iş yeri sayılıp sayılmayacağına irdelenmesi gerekir. Web sitesi ve internet servis sağlayıcı üzerinde depo edilen elektronik bilgi ve verilerden oluşmaktadır. Buna göre, web sitesi ve web sayfası fiziki bir varlığı temsil etmemektedir. Bu özellikleri dikkate alındığında web sitesi veya web sayfasının yalnız başlarına mevcut işyeri tanımının kapsamında mütalaa edilemeyeceği açık bir şekilde ortaya çıkmaktadır. Aslında web sitesi veya web sayfası elektronik ortamda ticari faaliyetin icra edilmesi için gereklidir. Nitekim dijital ekonomide mal ve hizmet alımı ve satımı faaliyetleri internet üzerinden internet siteleri veya uygulamalar üzerinden gerçekleştirilmektedir. Web sitesi ya da sayfası olmadan bugün internet ortamında yürütülen ticari faaliyetlerin önemli bir kısmının yapılması mümkün olamayacaktır. Bu anlamda web sitesi ya da sayfasının “...bir teşebbüsün işinin tamamen veya kısmen yürütüldüğü işe ilişkin...” olduğu söylenebilir. Ancak, işyeri tanımında yer alan diğer iki unsur “yer” (place) ve “sabitlik” (fixed) de dikkate alındığında web sitesinin iş yeri niteliği zayıflamaktadır. Bu nedenle, web sayfası ve web sitesinin işyeri olarak kabul edilmesi mümkün görülmemektedir. Nitekim, internet siteleri internet ortamındaki sunuculara bağlanmaktadır. Bu sunucular istenilen ülkeye yerleştirilebilmektedir. Web sunucular uzaktan kontrol edilebildiğinden örneğin vergi cenneti olarak adlandırılan ve büyük vergisel avantajlara sahip olan herhangi bir yerde de kurulabilir. Hatta sunucular istenilen ülkeye yerleştirilebildiği gibi değişik ülkelerde bulunan ayna (mirror) internet siteleri aracılığıyla elektronik ortamda yapılan işlemler istenilen adreslere yerleştirilebilmektedir. Bu da sunucuların dahi bir işyeri olarak nerede olduklarının tespit edilmesini zorlaştırmaktadır.

Sonuç olarak; kaynak ülke, eğer o ülkede mükellefin bir işyeri varsa ve bu işyerine atfedilebilen bir gelir varsa mukim olmayan bir mükellefin gelirini vergilendirebilir.

OECD, Matrah Aşındırma ve Kar Aktarımı (base erosion and profit shifting-BEPS) kapsamında, 2019 yılında Dijitalleşen Ekonominin Vergisel Problemlerinin Tanımlanması (Addressing the Challenges of the Digitalisation Economy) başlıklı bir rapor yayımlamıştır. Söz konusu raporda dijital ekonomide vergilendirmeye dair zorluklara değinilmiştir. Dijital ekonomide, özellikle dijital imkanlardan ciddi şekilde yararlanan çok uluslu işletmeler (ÇÜİ), BEPS 7 Numaralı Eylem Planı'na (İşyeri Statüsünden Yapay Yollarla Kaçınmanın Önlenmesi) refleks olarak pazarlama stratejilerini değiştirerek, uzaktan satış ya da al-sat şeklindeki modellerle iş yapmaya başlayarak yanıt vermiştir. Bu durum, örneğin; bir ülkede çeşitli kişilerle işlem yapılarak kazanç yaratılmasına rağmen fiziksel bir varlığın bulunmamasından dolayı söz konusu pazar ülkenin vergilendirememesi ile sonuçlanmaktadır. Bu kapsamda, OECD'nin 2019 yılında yayınladığı dokümanda revize edilmiş kazanç atfetme ve bağlantı kuralı başlığı altında bazı önerilerde bulunulmuştur.

Türk Hukukunda Elektronik Ticaretin Vergilendirilmesi

Türkiye'de elektronik ticaretin vergilendirilmesine özgü bir düzenleme bulunmadığından, bu bölümde elektronik ticaretin vergilendirilmesi bakımından genel düzenlemelere değinilecek olup, elektronik ticaretle ilgili özellik arz eden bazı hususlara değinilecektir.

Yükümlülüğün Tespiti

Yükümlülüğün tespiti açısından ülkeler, sadece kaynağı ya da sadece yerleşim yerini esas alarak vergilendirme yoluna gitmemektedir. Ülkeler, bunlardan her ikisini de değişen ölçülerde kullanılmaktadır. Aynı durum Türkiye için de geçerlidir. Gelirden alınan vergiler bakımından Gelir ve Kurumlar Vergisi Kanunu hem kaynak hem de yerleşme esaslı vergilendirmeyi benimsemiştir. Bu kanunlar, kural olarak, Türkiye'de yerleşik kişilerin gelirlerini, dünyanın neresinde elde edildiğine (kaynağına) bakmaksızın vergilendirirken, Türkiye'de yerleşik olmayan kişilerin ise sadece Türkiye sınırları içinde elde ettikleri gelirlerini vergilendirmektedirler.

Gelir Vergisi Bakımından

Türk vergi hukuku terminolojisiyle kişiler ya "tam yükümlü" ya da "dar yükümlü" oldukları için vergi öderler. Bu tasnif vergilendirilecek geliri hem yükümlülükleri hem de kaynağı itibarıyla ayırabilmek için kullanılır. Tam yükümlüler gerek Türkiye içinde gerekse Türkiye dışında elde ettikleri gelirin tümü üzerinden vergilendirilirler. Dar yükümlüler ise sadece Türkiye içinde elde ettikleri gelir üzerinden vergi öderler.

Tam Yükümlülük

Tam yükümlülüğün koşulları:

Gelir Vergisi Kanunu (m.3-5) tam yükümlülükte "vergilendirmede kişisellik ilkesi"ni kabul etmiştir. Kişisellik ilkesinin iki ölçütü de -uyrukluk ve ikamet ölçütleri- tam yükümlülükte uygulama alanı bulmaktadır. Çünkü, bir gerçek kişinin Türkiye'deki kazançlarının vergilendirilebilmesi için Türkiye'de yerleşmiş olması ya da resmi daire ve müesseselere ya da merkezi Türkiye'de bulunan teşekkül ve te-

şebbüslere bağlı olup da adı geçen daire, müessese, teşekkül ve teşebbüslerin işleri dolayısıyla yabancı ülkelerde oturan Türk vatandaşı olması gerekir.

- Türkiye’de yerleşme ölçütü

Gelir Vergisi Kanunu’nun (GVK) 4. maddesi tam yükümlülük ölçütü olarak Türkiye’de yerleşmeyi “ikametgah (yerleşim yeri)” ve “oturma süresi” olmak üzere iki esasa bağlamıştır.

İkametgah (Yerleşim Yeri) Esası

Gelir Vergisi Kanunu’nun 4. maddesine göre, ikametgahı Türkiye’de bulunanlar Türkiye’de yerleşmiş sayılırlar. GVK, Türkiye’de “yerleşmiş sayılma” deyiminin içeriğini belirlediği halde ikametgah kavramına medeni hukuktan ayrı bir belirleme getirememiştir. Dolayısıyla ikametgah kavramının içeriğinin medeni hukuka göre belirlenmesi gerekir. Türk Medeni Kanunu’nun (TMK) 19. maddesine göre, ikametgah, yerleşmek niyeti (sübjektif unsur) ile oturuş (objektif unsur) yerdur. Bir kimsenin birden çok konutu farklı ülkelerde ise yerleşim yerinin bulunduğı ülkenin saptanması önem taşır. Yaşantının ağırlıklı olarak sürdürüldüğü, iş ilişkilerinin yoğunlaştırıldığı, aile çevresinin bulunduğı yer yerleşim yerinin sübjektif unsurunun belirlenmesinde önemli olabilecek göstergelerdir.

Oturma süresi esası

Türkiye’de yerleşme bakımından yasanın kabul ettiğı ikinci esas oturma süresidir. Bir takvim yılı içinde Türkiye’de sürekli olarak altı aydan fazla oturanlar Türkiye’de yerleşmiş sayılır. Geçici ayrılmalar Türkiye’deki oturma süresini kesmez. Altı aylık oturma süresinin bir takvim yılı içinde aşılmış olması gerekir. Türkiye’de yerleşme bakımından altı aylık oturma esası, ikametgah esasını tamamlayıcı bir ölçüdür. Dolayısıyla bir kişi Türkiye’de altı aydan daha kısa bir süre oturmuş olsa da oturduğu süre içinde ikametgahının Türkiye’de olduğu belli ise tam yükümlü olarak vergilendirilecektir.

GVK’nın 5. maddesi bazı kişilerin altı aylık oturma süresinden fazla kalsalar bile bunların Türkiye’ye yerleşmiş sayılmayacağını belirtmiştir. Buna göre; aşağıdaki kişiler Türkiye’de altı aylık oturma süresinden fazla kalsalar bile Türkiye’ye yerleşmiş sayılmayacaklardır:

- Belli ve geçici görev veya iş için Türkiye’ye gelen iş, ilim ve fen adamları, uzmanlar, memurlar, basın ve yayın muhabirleri ve durumları bunlara benzeyen diğer kimselerle tahsil veya tedavi veya istirahat veya seyahat maksadıyla gelenler;
- Tutukluk, hükümlülük veya hastalık gibi elde olmayan sebeplerle Türkiye’de alıkonulmuş[] veya kalmış olanlar.

- Uyrukluk Ölçütü

GVK’nın 3. maddesinin 2. bendi tam yükümlülükte uyrukluk ölçütünü esas almıştır. Bu hüküm kapsamına giren Türk vatandaşları Türkiye içinde ve dışında elde ettikleri gelirlerin tümü üzerinden vergiye tabi tutulurlar. Ancak istisnai olarak bulundukları ülkede elde ettikleri kazanç ve iratlar için o ülkede gelir vergisi ya da benzeri bir vergi ödemişlerse, o kazanç ve iratlar Türkiye’de ayrıca vergilendirilmez. Yasa bu durumda çifte vergilendirmenin önlenmesinde istisna yöntemini kabul etmiştir.

Dar Yükümlülük

Türkiye’de yerleşmiş olmayan gerçek kişilerin Türkiye’de elde ettikleri kazanç ve iratların vergilendirilmesi ile ilgili bir yükümlülük şeklidir. GVK, tam yükümlülükte kişiselilik ilkesini kabul etmiş olmasına karşılık, dar yükümlülükte mülk ilkesini kabul etmiştir. Nitekim vergileme gelirin Türkiye’de elde edilmesi koşullarına bağlanmıştır. Dar yükümlülükte hedef kişiyi değil, kaynağı Türk ekonomisi olan geliri vergilendirmektir. Dolayısıyla dar yükümlüler sadece Türkiye’de elde ettikleri gelirler üzerinden Türkiye’de vergilendirilirler.

Kurumlar Vergisi Bakımından

Kurumlar Vergisi Kanunu’nun (KVK) 1. maddesine göre kurumlar vergisinin yükümlülükleri sermaye şirketleri, kooperatifler, iktisadi kamu kuruluşları, dernek ve vakıflara ait iktisadi işletmeler ve iş ortaklıklarıdır. KVK’nın 3. maddesinin 1. fıkrasına göre, yasal ya da iş merkezleri Türkiye’de bulunan kurumlar gerek Türkiye’de gerekse yabancı ülkelerde elde ettikleri kurum kazançları üzerinden vergilendirilirler. Yasa, yasal merkez veya iş merkezlerinden birinin Türkiye’de bulunmasını tam yükümlülük için yeterli görmüştür. KVK’nın 3. maddesinin 2. fıkrasına göre; yasal ve iş merkezlerinden her ikisi de Türkiye içinde bulunmayan kurumlar, dar yükümlülüğe tabidir. Bu kurumlar yalnızca Türkiye’de elde ettikleri kazançlar üzerinden vergilendirilir.

Tam ve dar yükümlülüğün kanuni merkez – iş merkezi ölçütleri ile belirlenmesi elektronik ticaret bağlamında işlevini kısmen ya da tamamen yitirmektedir. Nitekim teknolojik gelişmeler sonucunda, şirketler faaliyetlerini ülkeleri dışında fiziki bir varlık göstermeden icra edebilmektedirler. Bir diğer ifade ile, kanuni merkez ölçütü kolaylıkla dolanılabilen, şirketler vergi yükünün daha az olduğu veya hiç olmadığı ülkelerde kurulabilmektedir. Bu ölçütün eksikliğini gidermek için kabul edilmiş olan “iş merkezi” ölçütü de şirketin yönetim kurulu toplantılarının dijital olarak yapılması ya da yönetim faaliyetlerinin teknolojinin sunduğu imkanlardan yararlanılarak birden fazla ülkeye dağıtılması halinde işlevsiz kalabilecektir.

Gelirin Kaynağının Tespiti

Gerek gelir gerekse kurumlar vergisinde tam yükümlüler dünyanın neresinden elde edildiğine bakılmaksızın gelirlerinin tümü üzerinden Türkiye’de vergilendirildiklerinden, bunların elektronik ticaret aracılığıyla elde ettikleri kazançlarının vergilendirilmesi bakımından da – ilkesel olarak – bir problem bulunmamaktadır. Ancak dar yükümlüler bakımından hangi gelir unsurlarının Türkiye’de elde edilmiş olduğunun tespiti ve elektronik ticaretin bunlar üzerindeki etkisi önem taşımaktadır.

Gelir Vergisi Kanunu vergiye tâbi gelirin yedi kazanç ve irat türünden oluştuğunu belirtir. Bunlar ticari kazançlar, zirai kazançlar, ücretler, serbest meslek kazançları, gayrimenkul sermaye iratları, menkul sermaye iratları ve diğer kazanç ve iratlardır. Kurumlar vergisinin konusunu ise kurum kazancı oluşturur. Kurum kazancı gelir vergisinin konusuna giren gelir unsurlarından oluşur. Bununla birlikte, KVK dar yükümlülerin vergiye tabi kazançlarını tahdidi olarak sayma gereği görmüştür:

- (...) Türkiye’de iş yeri olan veya daimî temsilci bulunduran yabancı kurumlar tarafından bu yerlerde veya bu temsilciler vasıtasıyla yapılan işlerden elde edilen ticari kazançlar. (...)
- Türkiye’de bulunan zirai işletmeden elde edilen kazançlar.
- Türkiye’de elde edilen serbest meslek kazançları.
- Taşınır ve taşınmazlar ile hakların Türkiye’de kiralanmasından elde edilen iratlar.

- Türkiye’de elde edilen menkul sermaye iratları.
- Türkiye’de elde edilen diğer kazanç ve iratlar.

Kanun, değinilen kazanç veya iratların Türkiye’de elde edilmesi ve Türkiye’de daimî temsilci bulundurulması konularında, Gelir Vergisi Kanunu’nun ilgili hükümlerine atıfta bulunduğundan aşağıda bu konuda yapacağımız açıklamalar kurumlar vergisi bakımından da geçerli olacaktır.

Gelir Vergisi Kanunu dar yükümlülerin Türkiye’de kazanç ve irat elde etmesini belirli şartlara bağlamıştır. Buna göre:

- Ticari kazançlarda, kazanç sahibinin Türkiye’de işyerinin olması veya daimi temsilci bulundurulması ve kazancın bu yerlerde veya bu temsilciler vasıtasıyla sağlanması;
- Zirai kazançlarda, zirai faaliyetlerin Türkiye’de icra edilmesi;
- Ücretlerde,
 - Hizmetin Türkiye’de ifa edilmiş veya edilmekte olması veya Türkiye’de değerlendirilmesi;
 - Türkiye’de kain müesseselerin idare meclisi başkan ve üyelerine, denetçilerine tasfiye memurlarına ait huzur hakkı, aidat, ikramiye ve benzerlerinin Türkiye’de değerlendirilmesi;
- Serbest meslek kazançlarında, serbest meslek faaliyetlerinin Türkiye’de icra edilmesi veya Türkiye’de değerlendirilmesi;
- Gayrimenkul sermaye iratlarında: Gayrimenkulün Türkiye’de bulunması ve bu mahiyetteki mal ve hakların Türkiye’de kullanılması veya Türkiye’de değerlendirilmesi;
- Menkul sermaye iratlarında, sermayenin Türkiye’de yatırılmış olması;
- Diğer kazanç ve iratlarda, bu kazanç veya iratları doğuran işin veya muamelenin Türkiye’de ifa edilmesi veya Türkiye’de değerlendirilmesi

hallerinde kazanç veya irat Türkiye’de elde edilmiştir.

Bu hüküm elektronik ticaret açısından gözden geçirildiğinde, kanun koyucunun vergilendirme yetkisini, ticari kazançlarda “işyeri veya daimî temsilci aracılığıyla” Türkiye’de elde edilmiş olan, serbest meslek kazançlarında “Türkiye’de icra edilmiş serbest meslek faaliyetleri”nden doğan ve gayrimenkul sermaye iratlarında, “gayrimenkul (...) mahiyetindeki hakların Türkiye’de kullanılması veya Türkiye’de değerlendirilmesi” ile meydana gelen kazançlar üzerinde kullandığı görülmektedir. Bu durumda, bir dar yükümlünün öncelikle elde ettiği bir gelir unsurunun niteliğinin tespitinin yapılması; ardından, bu niteliğe bağlı olarak o kazanç veya iradın Türkiye’de elde edilip edilmediğinin; bir diğer ifadeyle, o gelir unsurunun kaynağının Türkiye olup olmadığının belirlenmesi gereklidir.

Gelir Unsurlarının Niteliğinin Tespiti

Elektronik ticarete gelir unsurlarının niteliğinin tespiti de güçtür. En belirgin nitelendirme sorunu gelir unsurunun ticari kazanç mı yoksa gayrimaddi hak bedeli (royalty) mi olduğu noktasında kendisini gösterir. Bu bakımdan bilgisayar programlarının (yazılımların), telif haklarının (copyright) ve know-how’ların devri veya kullanılması karşılığı elde edilen kazanç veya iratların ticari kazanç mı yoksa gayrimaddi hak bedeli mi olduğunun tespiti oldukça önemlidir. Aynı şekilde, elektronik olarak sunulan teknik, idari veya danışmanlık hizmetlerinin Türk vergi hukukundaki niteliklerinin belirlenmesi gerekir.

Ticari kazanç Gelir Vergisi Kanunu'nun 37. maddesinde "her türlü ticari ve sınai faaliyetlerden doğan kazanç" olarak tanımlanmıştır. "Ticari faaliyet"ten ne anlaşılması gerektiği hususunda Gelir Vergisi Kanunu'nda hüküm bulunmamaktadır. Türk Ticaret Kanunu'ndaki "...bir ticari işletmeyi ilgilendiren bütün işlem ve fiiller ticari işlerdendir." tanımından hareketle bir "ticari işletme"nin her türlü faaliyetinin ticari faaliyet olacağı ve dolayısıyla, bundan elde edilen kazançların Gelir Vergisi Kanunu uyarınca ticari kazanç olarak nitelendirileceği sonucuna varabiliriz.

Gayrimaddi hak bedeli esasen (iç) vergi hukukumuzda kullanılan bir kavram ve terim değildir. Gayrimaddi hak bedellerinin bazıları (kullanma karşılığı olanları) hukukumuzda gayrimenkul sermaye iratları kapsamında düzenlenmiştir.

Serbest meslek kazancı ise Gelir Vergisi Kanunu'nun 65. maddesinde "her türlü serbest meslek faaliyetinden doğan kazanç" olarak tanımlanmıştır. Bu tanımın gereği olarak Kanun'da serbest meslek faaliyeti "sermayeden ziyade şahsi mesaiye, ilmi veya mesleki bilgiye veya ihtisasa dayanan ve ticari mahiyette olmayan işlerin işverene tâbi olmaksızın şahsi sorumluluk altında kendi nam ve hesabına yapılmasıdır" ifadesi yer alır.

Gayrimaddi Hak Bedelleri (Gayrimenkul Sermaye İratları)

Model Anlaşma'nın 12. maddesinin gayrimaddi hakların kullanılması (kiralınması) ya da kullanma hakkı (satışı, devri) karşılığı yapılan ödemelere uygulanacak kuralları içermektedir. Gelir Vergisi Kanunu'nda gayrimaddi hak bedellerine özgü bir hüküm bulunmaz. Gayrimaddi hak bedellerinin bir bütün olarak ayrı bir gelir unsuru halinde düzenlenmediği; gayrimaddi hakların "kullanım" bedellerinin ise gayrimenkul sermaye iratları içine yedirilmiş olduğu görülür.

Kanun 70. maddesinde, başkaca şeylerin yanı sıra, şu mal ve hakların sahipleri, mutasarrıfları, zilyetleri, irtifak ve intifa hakkı sahipleri veya kiracıları tarafından "kiraya verilmesinden" elde edilen iratları gayrimenkul sermaye iradı saymıştır:

"(...) 5. Arama, işletme ve imtiyaz hakları ve ruhsatları, ihtira beratı (İhtira beratının mucitleri veya kanunî mirasçıları tarafından kiralınmasından doğan kazançlar, serbest meslek kazancıdır.), alâmeti farika, marka, ticaret unvanı, her türlü teknik resim, desen, model, plan ile sinema ve televizyon filmle-ri, ses ve görüntü bantları, sanayi ve ticaret ve bilim alanlarında elde edilmiş bir tecrübeye ait bilgilerle gizli bir formül veya bir imalat usulü üzerindeki kullanma hakkı veya kullanma imtiyazı gibi haklar (Bu hakların kullanılması için gerekli malzeme ve teçhizat bedelleri de gayrimenkul sermaye iradı sayılır.);

6. (202 sayılı Kanunun 35'inci maddesiyle değişen bent) Telif hakları (bu hakların, müellifleri veya bunların kanuni mirasçıları tarafından kiralınmasından doğan kazançlar, serbest meslek kazancıdır; (...)"

Bu mal ve hakların bir ticari işletmeye dahil bulunduğu hallerde, bunların iratları gayrimenkul sermaye iradı değil, ticari kazanç olarak nitelendirilir.

Gayrimenkul sermaye iratları içinde sayılan bu tanımın, OECD Model Anlaşması'nda ve buna dayalı olarak Türkiye'nin tarafı olduğu ikili anlaşmalarda yer alan "gayri maddi hak bedelleri", "edebi, sanatsal veya bilimsel eserler üzerindeki herhangi bir telif hakkının (copyright) (...) ya da sınai, ticari veya bilimsel tecrübeye ilişkin bilginin kullanılması ya da kullanma hakkı karşılığı olarak elde edilen her çeşit ödemedir" şeklindeki tanımla uyumlu olduğu söylenebilir.

Hizmet Bedelleri

Elektronik ticaret bağlamında gelirin nitelendirilmesinde üzerinde durulmasında yarar olan bir husus ticari kazanç – serbest meslek kazancı ayrımıdır. Hizmet edimleri bireysel olarak icra edildiğinde serbest meslek kazancına; ticari işletme yapısı içinde icra edildiğinde ise ticari kazançta vücut vermektedir. Elektronik ticaret, pek çok hizmetin çevrimiçi sunulabilmesini mümkün kılmaktadır ama daha da önemlisi elektronik ticaret ile birlikte işletim sistemi, yazılım gibi pek çok ürünün hizmet kapsamında değerlendirildiğini söylemek mümkündür.

Gelirin Elde Edildiği Yerin Tespiti

Gerek gelir vergisi ve gerekse kurumlar vergisi bakımından dar yükümlüler sadece “Türkiye’de elde ettikleri” kazanç ve iratlar üzerinden Türkiye’de vergi öderler. Gerçek kişi veya kurum, bir dar yükümlünün Türkiye’den kazanç veya irat elde edip etmediğinin tespiti Gelir Vergisi Kanunu hükümlerine göre yapılır. Gelir Vergisi Kanunu’nun 7. maddesine göre, ticari kazançlarda, kazanç sahibinin Türkiye’de işyerinin olması veya daimi temsilci bulundurması ve kazancın bu yerlerde veya bu temsilciler vasıtasıyla sağlanması halinde kazanç Türkiye’de elde edilmiş sayılır. Gayrimenkul sermaye iratlarında gayrimenkulün Türkiye’de bulunması ve bu mahiyetteki mal ve hakların Türkiye’de kullanılması veya Türkiye’de değerlendirilmesi; serbest meslek kazançlarında, serbest meslek faaliyetlerinin Türkiye’de icra edilmesi veya Türkiye’de değerlendirilmesi Türkiye’de elde etme anlamına gelir.

Elektronik ticaret bağlamında dar mükelleflerce İnternet üzerinden sunulan hizmetler çoğu kez Türkiye’de icra edilmeyeceğinden bunların Türkiye’de elde edilip edilmediğinin tespiti bunların Türkiye’de “değerlendirilip değerlendirilmediğine”, yani hizmet bedeli ödemelerinin Türkiye’de yapılıp yapılmadığına göre belirlenecektir. Gayrimaddi hakların kullanımı Türkiye’de olabileceğinden, bunlarda yer tespiti sorun yaratmayacaktır.

Ticari kazançlar bakımından ise kazancın elde edildiği yerin tespiti dar yükümlünün Türkiye’de işyeri veya daimi temsilcisinin bulunması ve kazancın bu yer veya temsilci aracılığıyla elde edilmesine bağlanmıştır. Şimdi bu koşulları inceleyelim:

İş Yeri

“İş yeri” Vergi Usul Kanunu hükümlerine göre belirlenir. Vergi Usul Kanunu’nun 156. maddesine göre iş yeri “mağaza, yazıhane, idarehane, muayenehane, imalathane şube, depo, otel, kahvehane, eğlence ve spor yerleri, tarla, bağ, bahçe, çiftlik, hayvancılık tesisleri, dalyan ve voli mahalleri, madenler, taş ocakları, inşaat şantiyeleri, vapur büfeleri gibi ticari, sınai, zirai veya mesleki bir faaliyetin icrasına tahsis edilen veya bu faaliyetlerde kullanılan yerdir.” Bu tanıımı esas alarak aşağıdaki değerlendirmeleri yapabiliriz:

Nesnel Koşullar

İş yerinin fiziki bir varlığa işaret etmektedir. Vergi Usul Kanunu’ndaki iş yeri örnekleri de bunu doğrular niteliktedir. Kanun koyucu örnekleri sayma amacıyla değil, tanımlama amacıyla vermiştir. Sayılanlar dışında kalan ve işlevi itibarıyla onlara benzeyen her yer işyeridir.

Öznel Koşullar

Yerin ticari faaliyetler için “tahsis edilmiş olması” veya bu amaçla “kullanılması” gerekir. Öyle ise iş yerinin, burada ticari faaliyetini sürdüren kişinin mülkiyetinde olması şart değildir. Kanun koyucu belli bir yerde fiili tasarrufu, yani zilyetliği yeterli görmüştür.

Bu fiili tasarrufun devamlılığı yine Kanun’un 156. maddesindeki tanımdan açıkça anlaşılamamaktadır. Ancak hükmün “fiil” değil “faaliyet” ten bahsetmesi, tek seferlik ya da geçici eylemler yerine süreklilik arz eden eylemleri işaret eder. Ayrıca, Kanun’un “iş yeri açma”yı düzenleyen 154. maddesinde “İş yeri açmaktan maksat, belli bir yerde bilfiil ticari veya sınai faaliyete geçmek demektir. Bir yerin ne maksatla olursa olsun sadece tutulmuş olması (...) iş yerinin açıldığını göstermez” denmekle devamlılık unsuru daha açık bir şekilde ifade edilmiştir.

İşlevsel Koşul

İşlevsel koşul olan belli bir yerde “ticari faaliyet sürdürülmesi”, Vergi Usul Kanunu’nun 156. maddesindeki tanımda yer almaktadır. Vergi Usul Kanunu’nda yer alan iş yeri tanımı OECD Model Anlaşması’ndaki iş yeri (fixed place of business) tanımı ile gerek lafzı, gerek unsurları ve gerekse örnekleri itibarıyla hemen hemen aynıdır.

Daimi Temsilci

Kurumlar Vergisi Kanunu’nun 3. maddesinin 4. bendi uyarınca “Türkiye’de daimi temsilci bulundurma” konusunda Gelir Vergisi Kanunu hükümleri uygulanır. Gelir Vergisi Kanunu’nun 8. maddesinin 2. fıkrası uyarınca “daimi temsilci, bir hizmet veya vekâlet akdi ile temsil edilene bağlı olup, onun nam ve hesabına muayyen veya gayrimuayyen bir müddetle veya müteaddit ticari muameleler ifasına yetkili bulunan kimsedir.” Kanun şu kişilerin başkaca şartlar aranmaksızın temsil edilenin daimi temsilcisi sayılacağını öngörmüştür:

1. Ticari mümessiller, tüccar vekilleri ve memurları ile Türk Ticaret Kanunu’nun hükümlerine göre acenta durumunda bulunanlar;
2. Temsil edilene ait reklam giderleri hariç olmak üzere giderleri devamlı olarak kısmen veya tamamen temsil edilen tarafından ödenenler;
3. Mağaza veya depolarında temsil edilen hesabına konsinyasyon suretiyle satmak üzere devamlı olarak mal bulunduranlar.

İlgili maddeye göre bir kimsenin birkaç kişiyi aynı zamanda temsil etmesi daimi temsilcilik vasfını değiştirmez.

Kanun koyucu Türkiye’de elde edilen kazançların vergilendirilmesi noktasında, dar mükellefin kendisine bağımlı veya kendisinden bağımsız bir kişi tarafından Türkiye’de gerçekleşen ticari faaliyetlerde temsil edilmesini yeterli görmüştür. Bu durumda bağımsız temsilciler, tam yükümlü olarak, kendi kazançları üzerinden vergilendirilecekleri gibi, aracılık ettikleri faaliyetlerde bir dar yükümlü tarafından elde edilen kazançlar bakımından da şekli – maddi vergi ödevlerine muhatap olacaklardır.

Elektronik Ticaretin Vergilendirilmesindeki Güçlükler ve Atılan Ulusal ve Uluslararası Adımlar

Ürünlerin dijitalleştirilmesi ürünlerin gayri maddi mallara dönüştürülüp İnternet üzerinden iletilmesini mümkün kıldığı için kaynak, üretim ve tüketimin orijin ve yeri gibi kavramlar bulanıklaşmaktadır. Bunlara ek olarak, İnternet temelli işletmelerin işleyişini etkilemeksizin sunucuların dünyanın herhangi bir noktasına yerleştirilebilmesi sonucu, işyeri kavramı da hem daha belirsiz hem de önemsiz hale gelmektedir. Bu temel coğrafi tanımlardaki bozulma, vergi idareleri için üstesinden gelmeleri gereken yeni zorluklar yaratmaktadır. E-ticaretin vergilendirilmesindeki zorluklarla mücadelede hem ülkeler tek yanlı olarak hem de uluslararası arenada önemli adımlar atılmıştır.

Ülkelerin Tek Taraflı Attığı Bir Adım Olarak Dijital Hizmet Vergisi

Özellikle ülkelerin kendi gayri safi hasılların üzerinde gelir elde eden Amazon, Google, Meta gibi çok uluslu şirketler, diğer ülkelerde fiziki varlıkları olmaksızın bu ülkelerden gelir elde etmektedir. Gelirin elde edildiği ülkede vergi ödemeksizin faaliyet gösterilmesi birçok ülkeyi rahatsız etmiş ve bu konuda OECD'nin üzerinde uzlaşa sağlanacak bir çözüm bulması istenmiştir. OECD'nin aşağıda bahsedilecek olan G20 ile birlikte hazırladığı BEPS'e İlişkin Kapsayıcı Çerçeve'ye kadar dijital ekonominin nasıl vergilendirileceğine yönelik uluslararası arenada ortak bir kabulden söz etmek güçtür. OECD bünyesinde yapılan çalışmaların bir türlü sonuçlanamaması nedeniyle Fransa, Hindistan, İspanya, İtalya, İngiltere gibi birçok ülke alternatif çözüm olarak dijital hizmet vergisi (DVH) gibi vergiler ihdas ederek teknoloji devi çok uluslu şirketleri vergilendirme çabasına girmişlerdir. Ülkemizde de internet aracılığıyla dijital ortamda gerçekleştirilen ticari faaliyetlerin vergilendirilmesini amaçlayan "dijital hizmet vergisi" de 7 Aralık 2019 tarihinde yayımlanan 7194 sayılı kanunla mevzuatımızdaki yerini almış ve 1 Mart 2020'den itibaren yürürlüğe girmiştir. Söz konusu Kanun'da oldukça geniş kapsamlı tanımlara yer verilmiş, bu sayede e-ticaret faaliyetlerinin birçoğu vergi kapsamına alınmıştır. E-ticaret faaliyetlerine yönelik reklamlar, çeşitli dijital içerik satışları ve dijital platform hizmetlerinden elde edilen gelirler %7,5 oranında dijital hizmet vergisine tabi olup, bu faaliyetleri gerçekleştiren şirketlerin yurt dışında yerleşik olması ülkemizdeki mükellefiyetini etkilememektedir.

Ülkemizde elde edilen hasılatın dijital hizmet vergisinin kapsamına girebilmesi için şirketin Türkiye'deki kazancının 20 milyon TL'den ve dünya genelinde kazancının ise 750 milyon Euro'dan fazla olması gerekmektedir, bu eşiklerin altındaki şirketler dijital hizmet vergisinden muaf tutulmuşlardır.

Dijital hizmet vergisinin konusu ilgili Kanun'un 1. maddesinde sıralanmıştır. Buna göre:

- Dijital ortamda sunulan her türlü reklam hizmetleri (reklam kontrol ve performans ölçüm hizmetleri, kullanıcılar ile ilgili veri iletimi ve yönetimi gibi hizmetler ile reklamın sunulmasına ilişkin teknik hizmetler dahil),
 - Sesli, görsel veya dijital herhangi bir içeriğin (bilgisayar programları, uygulamalar, müzik, video, oyunlar, oyun içi uygulamalar ve benzerleri dahil) dijital ortamda satışı ile bu içeriklerin dijital ortamda dinlenmesine, izlenmesine, oynanmasına veya elektronik cihazlara kaydedilmesine veya bu cihazlarda kullanılmasına yönelik dijital ortamda sunulan hizmetler,
 - Kullanıcıların birbirleriyle etkileşime geçebilecekleri dijital ortamların sağlanması ve işletilmesi hizmetleri (kullanıcılar arasında bir mal veya hizmetin satılmasına veya satılmasının kolaylaştırılmasına yönelik sunulan hizmetler dahil),
 - Sayılan hizmetlere yönelik dijital ortamda dijital hizmet sağlayıcıları tarafından verilen aracılık hizmetlerinden elde edilen hasılat,
- verginin konusunu oluşturmaktadır.

Görüleceği üzere söz konusu vergi, dijital platformların büyük bir bölümünü kapsamına almaktadır. Arama motorlarına ait reklamları, bant (banner) reklamlar, yazılımlar yoluyla otomatik biçimde çevrimiçi gönderilen reklamlar, açılır pencereye ait olan reklamlar, laptop, tablet ve telefon gibi cihazlarda kullanılmış olan yazılım ve programlar, film, video, resim, fotoğraf, grafik, makale, dergi, gazete gibi görüntü, ses ve metin dosyası içerikleri, dijital oyunlar, oyun ek paketleri ve oyun kodları gibi her türlü dijital unsur vergi kapsamı içinde değerlendirilmiştir.

Bununla beraber, dijital alanda yer alan bazı hizmetler (içeriği nedeniyle) vergiden muaf tutulmuştur. Bu kapsamda “dijital verilerin çevrimiçi alanlarda depolanması, sanal ortamda satışa sunulan sinema, tiyatro, konser, müze, spor müsabakaları, otobüs, tren, uçak yolcu biletleri gibi doğrudan faydalanılan bir hizmeti temsil eden biletler ve yasa çerçevesinde yetkili olan kuruluşlarca yürütülen şans oyunu ile müşterek bahse ait sanal ortamda satışı yapılan ve çekiliş veya bahse katılma hakkı sunan bilet veya kuponlar” dijital içerik olarak ele alınmamaktadır.

Dijital hizmetlere yönelik vergilerin mükellefi dijital hizmet sağlayıcılarıdır. Kanunda bu kişilerin tam mükellef olmaları ya da olmamaları veya dar mükellefiyet biçiminde bu faaliyetleri ülkede bulunan iş yeri veya sürekli temsilcileri vasıtasıyla yürütüp yürütmediklerinin DHV mükellefiyetine etkisi olmayacağı ifade edilmiştir. Verginin alt sınırının; ülke içindeki faaliyetlerden kazanılan hasılat bakımından 20 milyon TL, dünya çapında kazanılan hasılat açısından ise 750 milyon Euro olması öngörülmüştür. Bu değerlerin altında kalan kazançlar vergiye tabi değildir.

Dijital hizmet vergilerinin hedefindeki şirketlerin ABD menşeli olması, ABD’nin bu ve benzeri vergileri ihdas eden ülkelere karşı soruşturma açması ile neticelenmiştir. Bu soruşturmalar sonunda ABD, dijital hizmet vergilerinin kendi şirketlerine ayırmacılık yaptığı gerekçesiyle söz konusu vergiyi uygulayan veya uygulamayı planlayan ülkelere karşı misilleme yapacağını duyurmuştur.

Bu gelişmeler sırasında aşağıda detaylı açıklanacağı üzere OECD bünyesinde yıllar süren çalışmalar neticelenerek önce G7 ülkeleri, sonrasında G20 ülkeleri dijital ekonominin vergilendirilmesi konusunda uzlaşmaya vardıklarını ifade etmişlerdir. . Çok uluslu şirketlerin vergilendirilmesinde iki sütunlu bir yaklaşım öngören söz konusu uzlaşmaya ilişkin olarak OECD tarafından 8 Ekim 2021 tarihinde bir açıklama yapılmış olup bugün itibarıyla 137 ülke bu uzlaşmayı benimsediklerini açıklamışlardır. Uluslararası vergilendirme kurallarını yeniden belirleyen bu iki sütunlu yapının birinci sütununa göre küresel hasılatı 20 milyar Euro’yu, karlılığı %10’u geçen şirketlerin %10 üzerindeki karının %25’i mal ve hizmet sunulan pazar ülkelere elde edilen hasılat esas alınarak bu ülkelere paylaştırılacak, bunun karşılığında da pazar ülkeleri dijital hizmet vergilerini kaldıracaktır. Söz konusu anlaşmanın 2023 yılında uygulamaya geçirilmesi planlanmaktadır.

İki sütunlu yeni yapı üzerinde uzlaşmaya varılması sonrasında, ABD dijital hizmet vergisi uygulayan ve misillemede bulunacağını ilan ettiği ülkelerle tekrar görüşmüştür. ABD Hazine Bakanlığı, 21 Ekim 2021’de Avusturya, Fransa, İtalya, İspanya ve İngiltere ile Sütun 1’in uygulamaya gireceği geçici dönemde dijital hizmet vergilerinde nasıl bir geçiş yapılacağı konusunda anlaştıklarını duyurmuştur. 22 Kasım 2021 tarihinde ise Türkiye’nin de bu anlaşmaya dahil olduğu Türkiye Hazine ve Maliye Bakanlığı ile ABD Hazine Bakanlığı tarafından duyurulmuştur. ABD Hazine Bakanlığı, en son 24 Kasım 2021 tarihli açıklamasıyla Hindistan’ın da söz konusu anlaşmaya dahil olduğunu açıklamıştır. ABD’nin DHV uygulayan ülkelerle yaptığı anlaşmaya göre söz konusu ülkeler, Sütun 1’in uygulamaya gireceği tarihe kadar dijital hizmet vergisi almaya devam edecekler, ama bu vergileri ödeyen şirketler geçiş sürecinde ödedikleri dijital hizmet vergilerini Sütun 1 uygulamaya girdikten sonra ödeyecekleri kurumlar vergisinden düşeceklerdir. Diğer bir ifadeyle, geçiş döneminde tahsil edilen dijital hizmet vergileri gelecekte tahsil edilen kurumlar vergisinden mahsup edilecektir. ABD ise ticaret önlemlerine ilişkin müeyyidelerini uygulamayacaktır.

Elektronik Ticaretin Vergilendirilmesinde Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) Bünyesinde Atılan Adımlar

Turku Konferansı (1997)

OECD'nin elektronik ticaret ile ilgili çalışmalarının başlangıç noktasını, Kasım 1997'de Turku'da yapılan "Küresel Elektronik Ticarete Engellerin Kaldırılması" başlığını taşıyan konferans oluşturur. Turku Konferansı'nda e-ticarete vergilendirme, devletlerin önlem alması gereken bir alan olarak belirlenmiştir ve hukuki belirsizliklerin en aza indirilmesi gereken meseleler kategorisinde ele alınmıştır.

Konferansta vergi tartışmalarının temelini OECD Mali İşler Komitesi'nin hazırladığı rapor oluşturmuştur. Bu raporda internetin vergi idaresi ve vergi politikası açısından getirdiği sorunlar ele alınmış, internetin özelliklerinin gelir ve tüketim vergilerini ve uluslararası vergi düzenlemelerini nasıl etkilediği incelenmiş ve bu sorunların çözümünde devletlerin kullanabileceği seçenekler sıralanmıştır.

Konferansta kararlaştırılan iki önemli husus şu şekildedir:

- E-ticaretin vergilendirilmesi nispeten basit olmalı, vergi yükümlülerinin gönüllü olarak uygulayacağı bir sistem içermeli, geleneksel ticarete karşı e-ticareti yapay olarak avantajlı veya dezavantajlı duruma getirmemeli ve e-ticaretin gelişmesini gereksiz yere engellememelidir.
- Hiçbir devletin tek başına hareket ederek bu sorunlara çözüm üretemeyeceği hususunda mutabakata varılmıştır. Dolayısıyla OECD'nin vergi sorunlarının çözümünde yetkili organizasyon olarak kabul edilmesi yaklaşımı ön plana çıkmıştır. Bu çerçevede, OECD hem uluslararası diyalog ortamını yaratmak hem de Ottawa konferansında onaya sunulmak üzere e-ticarete çerçeve vergilendirme ilkelerini hazırlamak ve e-ticaretin vergi idarelerinin önüne koyduğu sorunların çözümlerini araştırmaya başlamakla görevlendirilmiştir.

Ottawa Konferansı (1998)

Ekim 1998'de Ottawa'da "Sınırsız bir Dünya: Küresel Elektronik Ticaretin Potansiyelini Anlamak" başlığı altında gerçekleştirilen Bakanlar konferansı, Turku Konferansı'nın devamı niteliğindedir. Turku Konferansı'nda atılan adımlar ve varılan sonuçlar Ottawa Konferansı'nda resmi bir ifade bulmuştur. Bu Konferans'ta OECD'nin öncü kuruluş olduğu kabul edilmiş ve OECD'nin faaliyetleri için bir Eylem Planı oluşturulmuştur. Eylem Planı'nda "dijital pazarın tabi olacağı hukuk kurallarının oluşturulması" başlığı altında vergilendirmeden söz edilmektedir. OECD'ye göre mevcut hukuki kurallar dijital olmayan dönemde, geleneksel ticari yaşama uygun bir şekilde geliştirilmiştir. Tüketiciler ve iş çevreleri dijital dünyada etkinliklerini artırdıkça mevcut kurallar yetersiz kalmış ve şeffaf ve öngörülebilir bazı değişiklikler zorunlu hale gelmiştir. OECD, Eylem Planını şu şekilde belirlemiştir:

OECD, diğer uluslararası ve bölgesel kuruluşlar, iş çevreleri ve üye olmayan devletlerle işbirliği içinde;

- Teknik, protokol ve standartlar bakımından ilgili gelişmeleri izlemeyi ve gerektiğinde vergi sistemlerinin anlamlı çalışmasını güvence altına alacak şekilde bilgi sağlamayı,
- İlgili uluslararası vergi kurallarının açıklığa kavuşturulması için bilgi sağlamayı,
- Elektronik ticarete meydana gelecek gelişmeleri yanıtlamak için mevcut kural ve idari uygulamaların uyarlanması konusunda rehberlik etmeyi sürdürecektir.

Ottawa Konferansı sonucu yayınlanan raporda birtakım ilkeler kabul edilmiştir. Kabul edilen ilkeler,

aynı zamanda geleneksel ticaretin vergilendirilmesinde de hakim olan ilkeler olması bakımından önem taşımaktadır. OECD'nin e-ticaret ekseninde belirlediği ilkeleri, ayırım yapmama ilkesinin bir yansıması olarak değerlendirmek mümkündür. Nitekim OECD, geleneksel ticarete belirlenen vergileme ilkelerinin, elektronik ticarete de belirleyici olması yaklaşımını benimsemiştir. OECD'nin belirlediği çerçeve ilkeler aşağıdaki gibidir:

- Tarafsızlık ilkesi, vergilendirme yapılırken geleneksel ve elektronik ticaret arasında ayırım gözetilmeyerek eşit ve tarafsız vergilendirmenin yapılmasına vurgu yapmaktadır. Oluşturulan bu ilkeye bağlı olarak elektronik ticaret için uygulanması gereken vergilemenin geleneksel ticarete uygulanan vergilemeden farklı olması durumunun önüne geçilmesi hedeflenmiştir. İşletme kararlarının vergisel faktörlerden ziyade ekonomik esaslar dikkate alınarak oluşması sağlanmalıdır. Benzer işlemleri yapan benzer vergi yükümlülükleri benzer vergi yüküne katlanmalıdır.
- Verimlilik ilkesi, vergi verenler için sisteme uyum maliyetlerinin, vergi otoriteleri için yönetsel masrafların en aza indirilmesi açısından adımlar atılmalıdır.
- Belirlilik (kesinlik) ve basitlik ilkesi, vergilendirmeye ilişkin kurallar vergi yükümlülerinin anlayacağı ve dolayısıyla bir işlemin sonuçlarını öngörebileceği şekilde açık ve basit olmalıdır. Yükümlü zorlanmadan verginin ne zaman, nerede ve nasıl hesaplanacağını bilmelidir.
- Etkinlik ve adil olma ilkesi, vergilendirmenin doğru zamanda, doğru vergi miktarı üzerinden yapılması gerekliliğini ortaya koymaktadır. Vergiden kaçınma ve vergi kaçakçılığı olasılığı asgariye indirilmeli ve bu olasılığa karşı alınacak önlemler riskle orantılı olmalıdır.
- Esneklik ilkesi, vergilendirme bakımından öngörülecek sistemler, teknolojik ve ticari gelişmeleri yakalayabilecek şekilde esnek ve dinamik olmalıdır.

Belirtilmiş olan “tarafsızlık, verimlilik, belirlilik ve basitlik, etkinlik ve adillik, esneklik” ilkeleri, günümüzde de geçerliliğini koruyan prensipler olarak kabul görmektedir. OECD, hükümetlerin hem e-ticaretin gelişmesi için gereken mali ortamı oluşturma, hem de kamu hizmetlerinin adil ve öngörülebilir bir biçimde düzenleme yükümlülüğü arasında bir denge sağlanması zorunluluğuna dikkat çekmektedir. Bu anlamda söz konusu ilkeler, bu dengenin doğru bir biçimde kurulması için ilk hareket noktasını teşkil etmektedir.

Paris Forumu (1999)

Ekim 1999'da Paris'te gerçekleştirilen Elektronik Ticaret Forumu, Ottawa Konferansı'ndan sonra geçen bir yıllık sürede meydana gelen gelişmelerin değerlendirildiği bir toplantı olmuştur. Paris Forumu'nda dikkatler önceki konferanslarda belirlenen politikaların uygulanması gerekliliğin altı çizilmiştir.

OECD/G20 Matrah Aşındırma ve Kar Aktarımına (BEPS) İlişkin Kapsayıcı Çerçeve (2021)

2009'dan sonra uluslararası vergi sisteminde önemli bazı değişiklikler olmuştur. G20 önderliğinde 2008 küresel finans krizi sonrasında vergide iş birliği ve bilgi değişimi konuları ön plana çıkmıştır. Bu gelişmeler OECD bünyesinde Global Forum (Küresel Forum)'un oluşmasının öncüsü olarak nitelendirilebilir. Küresel Forum'un yaptığı çalışmaların vergi kaçakçılığı ve banka sırlarının önüne geçilmesinde sağladığı olumlu gelişmeleri takiben G20 dikkatini vergi kayıp ve kaçağı ile çok uluslu işletmelerin (ÇÜİ) etkin bir şekilde vergilendirmesine doğru yöneltmiştir.

OECD tarafından 2013 yılında yayımlanan “Matrahın Aşındırma ve Kar Aktarımı (Base Erosion and Profit Shifting-BEPS) Eylem Planı” 15 eylem planından oluşmaktadır. Bunlardan 1 no.lu eylem planı “Dijital Ekonomiye İlişkin Vergisel Sorunları Tespit Etme” başlığını taşımaktadır. 1 no.lu eylem planına göre dijital ekonominin, mevcut uluslararası vergi düzenlemelerinde neden olduğu zorlukların tespiti ile dolaylı ve dolaysız vergilerin bütüncül bir şekilde ele alınarak bu zorluklara özgü ayrıntılı çözüm seçeneklerinin geliştirilmesi amaçlanmaktadır. Ayrıntılı çözüm seçeneklerinin getirilmesi sektörde kullanılan çeşitli iş modellerinin detaylı bir analizini gerektirmektedir. Örneğin Meta, Twitter, Foursquare gibi sosyal ağlar, kullanıcılar tarafından oluşturulan içerikle yeni iş modellerinin örnekleri olmaktadır. Kullanıcıların genellikle ücretsiz kullandıkları sosyal ağların en önemli gelir unsuru, kullanıcının yaşı, cinsiyeti, ilgi alanları ve konumları gibi birtakım kişisel özelliklerini dikkate alarak yapılan reklamlar oluşturmaktadır. Ayrıca kullanıcıların tek başlarına ya da karşılıklı olarak oynayabildikleri sosyal ağ tabanlı online oyunlar ya da kullanıcılara belirli bir bedel karşılığında standart kullanıcılardan farklı olarak sunulan içerik ya da hizmetler sosyal ağların yarattığı yeni iş modelleri olarak değerlendirilmektedir.

OECD ve G20 de mevcut uluslararası vergi kurallarının, ÇUI’lerin, herhangi bir ülkede asgari düzeyde kurumlar vergisi ödemediği önemli gelir elde etmelerini olanaklı kıldığına karar vermiştir. Bu kapsamda, ülkeler ve uluslararası örgütler ÇUI’ler için geçerli olan uluslararası vergi kurallarına ilişkin değişiklikler üzerinde çalışmalara başlamıştır. BEPS 1 no.lu eylem planı çerçevesinde Dijital Ekonomi Görev Gücü (Task Force On Dijital Economy, TFDE) adında bir komisyon, OECD Mali İşler komitesi (CFA) bünyesinde 2013 yılında kurulmuştur. Komisyona, OECD, G20 üyesi olmayan ülkeler de eşit şartlarda taraf olarak katılmıştır. Komisyon, iş dünyası, sivil toplum, akademisyenler ve gelişmekte olan ülkeler tarafından hazırlanan yazılı girdileri paydaşlarla birlikte kapsamlı bir şekilde analiz ederek ÇUI’lerin vergilendirilmesinde şeffaflığı sağlamak amacıyla 2015 yılında bir rapor hazırlamıştır.

Raporda, hızla dijitalleşen ekonomi ve geliştirdiği elektronik ticaret, uygulama programları satışı, çevrimiçi reklam, çevrimiçi ödeme hizmetleri, bulut bilişim (cloud computing) gibi ticaret modellerinin neden olduğu vergi sorunları ortaya konulmuştur. Nitekim bu ticaret modelleri faaliyetleri sonucunda ortaya çıkan reklama dayalı gelirler, dijital satışlar/kiralama gelirleri, üyeliğe dayalı gelirler, danışmanlık ve finans hizmetleri gelirleri gibi kavranamayan gelirler ortaya çıkmış ve bu durum daha yüksek BEPS risklerini doğurmuştur. Rapor, özellikle bu modelleri sıkça vergi planlama amaçlı kullanan ÇUI’ler karşısında çözüm önerileri geliştirme çabası içerisinde olmuştur.

OECD tarafından 2018 yılında “Dijitalleşme Nedeniyle Ortaya Çıkan Vergi Zorlukları-Ara Rapor” (Tax Challenges Arising from Digitalisation –Interim Report 2018) başlığıyla bir rapor yayımlanmıştır. Raporda dijitalleşen ticaretin getirdiği sorunların kısa dönemli çözümü tartışılmakta ve açıklanmakta olup, bu kapsamda iş modelleri ve değer oluşturma üzerinde durulmaktadır. Dijitalleşen ticaretin vergilendirilmesi ve uluslararası vergilemeye uyumu sağlamak üzere farklı iş modellerinde, katma değer veya değer oluşturma üzerine yoğunlaşmıştır. Bir başka deyişle, katma değer hangi aşamada ve nerede oluşuyorsa o aşamada ve yerde vergilemenin yapılması ve vergi sorumlularının buna göre tanımlanmasının gerektiği belirtilmektedir. Dijital ortamda iş sahipleri ürünlerini fiziki olarak ülkelerde bulunmaksızın ülke tüketicilerine sunmakta olduğundan vergileme yetkisi karşılıklı olarak iç içe geçmektedir.

OECD tarafından 2020 yılında “Dijitalleşme Nedeniyle Ortaya Çıkan Vergi Zorlukları-Ekonomik Etki Değerlendirmesi” (Tax Challenges Arising From Digitalisation-Economic Impact Assessment: Inclusive Framework on BEPS,2020) başlığıyla bir rapor yayımlanmıştır. Raporda, dijitalleşmeden kaynaklanan vergi sorunlarının çözümü için taraf ülkelerce çok taraflı enstrüman (multilateral instrument-MLI) aracılığıyla iki sütunlu bir çözüm önerisi üzerinde durulmuştur. Birinci sütun, nexus ve kâr dağılımına odaklanırken ikinci sütun, kalan BEPS sorunlarını ele almak için tasarlanmış küresel minimum vergiye odaklanmaktadır. Bu çerçevede, birinci sütun (pillar one), kâr tahsisi ve nexus kuralları-

nın tutarlı ve eşzamanlı bir şekilde incelenmesi yoluyla uluslararası vergi sistemini yeni iş modellerine uyarlamayı amaçlamakta; ikinci sütun (pillar two) ise, kalan BEPS zorluklarını ele almak ve merkezi veya faaliyet gösterdiği ülke neresi olursa olsun uluslararası alanda faaliyet gösteren işletmelerin minimum vergi seviyesini ödemesini sağlamak için tasarlanmıştır.

Uluslararası vergi kurallarını güncellemek ve reforme etmek için yapılan uzun müzakerelerin sonucu olarak, Ekim 2021’de, OECD/G20 Matrah Aşındırma ve Kar Aktarımı’na İlişkin Kapsayıcı Çerçeve’nin 137 üyesi, ekonominin dijitalleşmesinden kaynaklanan vergi sorunlarına yönelik iki sütunlu yaklaşımı içeren bildiri üzerinde anlaşmaya varmıştır. 20 Aralık 2021’de ise OECD, OECD/G20 Matrah Aşındırması ve Kâr Aktarımı Projesi (BEPS) kapsamında onaylanan iki adımlı yaklaşımın ikinci adımı-na dair “Küresel Asgari Vergiye İlişkin Model Kuralları” yayınlanmıştır (“Model Kurallar”). Söz konusu Model Kurallar, Gelire Dahil Olma Kuralı (Income Inclusion Rule – IIR) ve Yetersiz Vergilendirilmiş Ödemeler Kuralını (Undertaxed Payment Rule - UTPR) kapsamakta olup; tüm bu kurallar bir bütün olarak Küresel Matrah Aşındırmayı Önleme Kuralları (“GloBE Kuralları”) olarak anılmaktadır.

OECD’nin getirdiği çözüm iki sütundan oluşmaktadır; Sütun 1 (Pillar 1) ve Sütun 2 (Pillar 2). Söz konusu iki sütunlu çözüm, kriterleri sağlayan ÇUI’lerin minimum %15 kurumlar vergisine tabi olmasını sağlamayı ve en büyük ve en kârlı çok uluslu şirketlerin kârlarını dünya çapındaki ülkelere yeniden tahsis etmeyi hedeflemektedir. Bir diğer deyişle, her iki Sütun da temel olarak, hem pazar ülkelerine küresel büyük şirketlerin elde ettikleri kazançtan daha fazla pay verilmesini sağlayacak hem de vergi cennetleri gibi zararlı vergi uygulamalarının önüne geçecektir.

İki sütunlu çözümün önemli noktaları:

Birinci Sütun

- Küresel hasılatı 20 milyar Euro ve karlılığı %10’u geçen ÇUI’lerin kârlarının ve vergi haklarının ülkeler arasında daha adil bir şekilde dağıtılmasını sağlamayı amaçlar. Sütun 1 ile karlılığı %10’u aşan şirketlerin bu oranın üzerindeki artık kârının %25’i pazar ülkeleri arasında hasılataya dayalı dağıtım anahtarı uyarınca paylaştırılır ve bu şekilde ilgili ülkelerde vergilendirilir. Dolayısıyla, Sütun 1 ile bu şirketlerin kârı, söz konusu yetki alanlarındaki fiziksel mevcudiyetinden bağımsız olarak, satışların gerçekleştiği yetki alanlarına/ülkelere yeniden tahsis edilir.

- Zorunlu ve bağlayıcı uyumsuzluk çözüm mekanizması ile vergide belirlilik ilkesi sağlanmaktadır.

- Dijital hizmet vergisi ve benzeri yükümlülüklerin kaldırılması hedeflenmektedir.

- Belli durumlarda uygulanacak olan basitleştirilmiş ve geliştirilmiş bir emsallerine uygunluk ilkesi öngörülmektedir.

İkinci Sütun

- Sütun 2’nin amacı, ÇUI’lerin faaliyet gösterdikleri her bir yetki alanında ortaya çıkan gelir üzerinden ilgili ülkede asgari düzeyde vergi ödenmesini sağlamaktır. Dolayısıyla, Sütun 2 ile ülkelerin vergi tabanlarını korumak için kullanabilecekleri %15 oranında küresel bir asgari kurumlar vergisi getirilerek ülkeler arasındaki vergi rekabetinin belli ölçüde sınırlandırılması için çalışılacaktır.

- GloBE kuralları, ÇUI’lerden nihai ana işletmenin konsolide mali tablolarındaki yıllık gelirin ilgili mali yıl ve öncesindeki dört mali yılın en az ikisinde 750 milyon Euro veya daha fazla olması halinde uygulanır.

İki Sütunlu Çözüm 13.10.2021 tarihinde Washington’da G20 Maliye Bakanları ve Merkez Bankası yöneticilerine sunulularak onaylanmıştır. İki Sütunlu Çözüm ayrıca 30.10.2021 tarihinde Roma’da yapılan G20 Liderler Zirvesinde de liderlerce onaylanmıştır. İki Sütunlu Çözümün 2024 yılı itibarıyla yürürlüğe girmesi planlanmakta ve bununla birlikte ülkelerin tek taraflı olarak yürürlüğe koyduğu dijital hizmet vergisi ve benzeri vergilerin de bu düzenlemeyle kaldırılacağı öngörülmektedir.

BÖLÜM ÖZETİ

Elektronik ticaret, işletmelerin iş yapış şekillerini büyük ölçüde etkilemiş ve değiştirmiştir. Teknolojinin sunduğu imkânlar sayesinde işletmeler, dünyanın herhangi bir noktasından diğerine kolaylıkla mal veya hizmet sunabilmektedir. Bununla birlikte gerek ulusal gerekse uluslararası vergi kuralları, bir ülkenin vergilendirme yetkisini kullanabilmesi için o ülkede ilgili işletmenin bir fiziksel varlığının bulunmasını aramaktadır. Örneğin, Gelir ve Kurumlar Vergisi Kanunlarında yükümlülük, bir gerçek kişinin Türkiye’de yerleşmesine veya bir kurumun Türkiye’de iş merkezi bulunmasına bağlanmıştır.

Uluslararası vergi anlaşmalarında ise ticari kazançların vergilendirilmesi, vergilendirmenin yapılacağı ülkede bir iş yeri veya temsilci bulunmasına bağlanmıştır. Fiziki varlığı esas alan vergi sistemi, e-ticareti vergilendirmede yetersiz kalmıştır. Ulusal ve uluslararası vergi sistemleri, fiziksel varlığa dayalı olacak şekilde kurgulanmıştır. E-ticaret ile birlikte işletmeler, mal ve hizmetlerini müşterilerinin bulunduğu ülkede fiziksel varlık göstermeden veya herhangi bir temsilcilik bulundurmada sunabilme imkânına sahip olabilmektedir. Bu durum, işletmelerin, faaliyetin yapıldığı ülkede vergi ödemeksizin gelir elde edebilmelerine imkân vermektedir. E-ticaretin günümüzde geldiği nokta, devletlerin vergi gelirlerini doğrudan etkilemektedir. Oluşan bu durum, ulusal ve uluslararası vergilendirmenin temel sorunlarından birini oluşturmaktadır.

Uluslararası e-ticarette birden fazla ülkenin vergilendirme yetkisi gündeme gelebileceği gibi hiçbir ülkenin vergilendirme yetkisi kapsamına girmemesi, dolayısıyla vergilendirilememesi de söz konusu olabilir. Elektronik ticaret, ülkelerin sınırlarını kolaylıkla aştığından bir ticari işlem aynı anda birden fazla devletin vergilendirme yetkisini gündeme getirebilir. Bu durumda elde edilen gelirin hangi ülkenin egemenlik alanına girerek vergilendirme yetkisi olduğunun tespiti, vergilendirme açısından büyük önem taşımaktadır. Uluslararası vergilendirmenin en temel meselelerinden biri, işte bu vergilendirme yetkisinin devletlerarası bölüşümüdür.

Uluslararası çifte vergilendirmeyi önleme anlaşmalarında yer alan iş yeri kavramı, e-ticaretin gerekliliklerini karşılamaya yetmediğinden başka çözümler gündeme gelmiştir. Bu çözümler, dijital hizmet vergileri gibi ulusal çözümler ve uluslararası alanda özellikle Ekonomik İşbirliği ve Kalkınma Örgütü tarafından geliştirilen çözümler olarak karşımıza çıkmaktadır. Ekim 2021’de, Ekonomik İşbirliği ve Kalkınma Örgütü/G20 Matrah Aşındırma ve Kar Aktarımı’na İlişkin Kapsayıcı Çerçeve’nin 137 üyesi, ekonominin dijitalleşmesinden kaynaklanan vergi sorunlarına yönelik iki sütunlu yaklaşımı içeren bir bildiriye kabul etmiştir. Buna göre birinci sütun kâr tahsisi ve nexus kurallarının tutarlı ve eşzamanlı bir şekilde incelenmesi yoluyla uluslararası vergi sistemini yeni iş modellerine uyarlamayı amaçlamaktadır. İkinci sütun ise Ekonomik İşbirliği ve Kalkınma Örgütü/G20 Matrah Aşındırma ve Kar Aktarımı’na İlişkin Kapsayıcı Çerçeve’nin zorluklarını ele almak ve merkezi veya faaliyet gösterdiği ülke neresi olursa olsun uluslararası alanda faaliyet gösteren işletmelerin minimum vergi seviyesini ödemesini sağlamak için tasarlanmıştır.

GÖZDEN GEÇİRELİM

1. “iki (ya da daha çok) devlette benzer vergilerin aynı yükümlü üzerine aynı vergiyi doğuran olay nedeniyle ve eş zamanlı vergilendirme dönemlerinde salınması” olarak tanımlanabilir.

2. Ticari faaliyetten elde edilen kazançları vergilendirmede birincil yetkiülkeye aittir.

3. Ticari kazançların vergilendirilmesi bakımından OECD Modelinin üzerine inşa edildiği temel ilke uyarınca bir devletin bir teşebbüsü bir diğer devlette bir aracılığıyla ticari faaliyet sürdürmediği sürece o diğer devlet tarafından doğrudan vergilendirmeye tabi tutulması mümkün değildir.

SORU 4 Ülkemizde elde edilen hasılatın dijital hizmet vergisinin kapsamına girebilmesi için şirketin Türkiye’deki kazancının TL’den ve dünya genelinde kazancının ise Euro’dan fazla olması gerekmektedir.

SORU 5 - ilkesi, vergilendirmeye ilişkin kurallar vergi yükümlülerinin anlayacağı ve dolayısıyla bir işlemin sonuçlarını öngörebileceği şekilde açık ve basit olmalıdır. Yükümlü zorlanmadan verginin ne zaman, nerede ve nasıl hesaplanacağını bilmelidir.

SORU 6 - ile ülkelerin vergi tabanlarını korumak için kullanabilecekleri %15 oranında küresel bir asgari kurumlar vergisi getirilerek ülkeler arasındaki vergi rekabetinin belli ölçüde sınırlandırılması için çalışılacaktır.

SORU 7 - İki Sütunlu Çözümün 2024 yılı itibariyle yürürlüğe girmesi planlanmakta ve bununla birlikte ülkelerin tek taraflı olarak yürürlüğe koyduğu dijital hizmet vergisi ve benzeri vergilerin de bu düzenlemeyle öngörülmektedir.

SORU 8 -yükümlüler gerek Türkiye içinde gerekse Türkiye dışında elde ettikleri gelirin tümü üzerinden vergilendirilirler.yükümlüler ise sadece Türkiye içinde elde ettikleri gelir üzerinden vergi öderler.

9. Gelir Vergisi Kanunu’nun (GVK) 4. maddesi tam yükümlülük ölçütü olarak Türkiye’de yerleşmeyi ve olmak üzere iki esasa bağlamıştır.

10. Gerek gelir vergisi ve gerekse kurumlar vergisi bakımından dar yükümlüler sadece kazanç ve iratlar üzerinden Türkiye’de vergi öderler.

CEVAP ANAHTARI

1. Çifte vergilendirme	6. Sütun 2
2. kaynak	7. kaldırılacağı
3. işyeri	8. Tam yükümlüler/dar yükümlüler
4. 20 milyon / 750 milyon	9. ikametgah (yerleşim yeri)/oturma süresi
5. Belirlilik (kesinlik) ve basitlik ilkesi	10. Türkiye’de elde ettikleri

KAYNAKÇA

- Akçaoğlu, Ertuğrul*: Elektronik Ticaretin Vergilendirilmesi, Mali Akademi Yayınları, 2012.
- Akçaoğlu, Ertuğrul*: “BEPS Eylem 7: İşyeri Statüsünden Yapay Yollarla Kaçınmanın Önlenmesi”, Vergilendirmede Martah Aşındırma ve Kar Kaydırma, (Editör: Billur YALTI), Beta Yayınları, 2018.
- Artar, Yusuf*: Dijital Ekonomide Vergilendirme, Finansal Raporlama ve Denetim: Sorunlar ve Çözüm Önerileri, Legal Yayıncılık, 2019.
- Cangir, Niyazi*: “Sanal İşyeri – I”, Vergi Dünyası, Sayı 227, Temmuz/2000.
- Demirhan, Habip*: “Dijital Hizmet Vergisinin Dünyadaki Uygulamaları ve Türkiye İle Karşılaştırmalı Analizi”, The Journal of Social Science, Sayı, 7, 2020.
- Durdu, Muhammet*: “Avrupa Birliği’nde Dijital Hizmet Vergisi ve Türkiye Uygulaması”, İstanbul Hukuk Mecmuası, 2020, Sayı, 78(4).
- Ekmekçi, Esra*: Küreselleşme ve Vergilendirmede Yeni Eğilimler, Kazancı Hukuk Yayınları, 2003.
- Ekmekçi, Esra ve Güneş, Gülsen ve Kaşıkçı, Mahmut*: “Kurucu ve Yönteme İlişkin Vergisel Temel Öğeler Bağlamında Türk Hukukunda Dijital Hizmet Vergisine Eleştirel Bakış”, İstanbul Üniversitesi Hukuk Fakültesi Armağanlar Dizisi, Prof. Dr. Türkan Rado’nun Anısına Armağan, On İki Levha Yayıncılık, Temmuz, 2020.
- Ferhatoğlu, Emrah*: “BEPS Eylem 1: Dijital Ekonomi”, Vergilendirmede Matrah Aşındırma ve Kar Kaydırma, (Editör: Billur YALTI), Beta Yayınları, 2018
- Kara, Mustafa Cemil*: “Dijital Ekonominin Vergilendirilmesinde Yeni Rabıta ve Kâr Tahsisi Kuralları”, Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı 49, 2022.
- Kara, Mustafa Cemil ve Öz, Ersan*: “Dijital Vergilendirmeye Küresel Bir Bakış”, Vergi Dünyası, Sayı, 424, Aralık/2016.
- Karadağ, Mesut*: Türk ve Uluslararası Vergi Hukukunda Daimi İşyerine Kazanç Atfedilmesi, On İki Levha Yayıncılık, 2021.
- Kılıçer, Erkan/Peker, İmren*: Dijital Ekonomide Vergilendirme, SeçkinYay., 2. Baskı, Mart, 2021.
- Oktay, Cemali*: “Dijital Ekonominin Boyutu, Vergilendirilmesine Yönelik OECD Çalışmaları, Öneriler, Örnek Ülke Uygulamaları ve Türkiye’de Yapılan Düzenlemeler ve Dijital Hizmet Vergisi”, Vergi Sorunları, Sayı, 376, Ocak/2020.
- Reimer, Ekkehart/Rust, Alwxander (Ed.)* Klaus Vogel on Double Taxation Conventions, Fourth Edition, Volume 1, Wolters Kluwer.
- Rençber, Altan*: Uluslararası gelişmeler Işığında Vergi Hukukunda İşyeri, Filiz Kitabevi, 2021.
- Rençber, Altan*: “Dijital Hizmet Vergisi İlk İzlenimler, Sorun ve Sorunsallar”, Vergi Sorunları, Sayı 376, Ocak/2020.
- Sağır, Harun*: “Dijital Hizmetletin Vergilendirilmesinin Tarihsel Süreci ve Geleceği”, Vergi Dünyası, Kasım 2022.
- Saraçoğlu, Fatih/Kahraman, Birkan*: “Dijital Hizmet Vergisi Üzerine Değerlendirmeler”, Vergi Sorunları, Sayı, 376, Ocak/2020.
- Şenses, Nevzat*: “Dijital Dünyada İnternet Sitelerinin Vergisel Durumu”, Vergi Dünyası, Sayı, 450, Şubat/2019.
- Taymaz, Erol*: Dijital Teknolojiler ve Ekonomik Büyüme, Tüsiad Yayınları, 2018.
- Yaltı, Billur*: Elektronik Ticarete Vergilendirme, Der Yayınları, 2003.

OECD, Glossary Of Statistical Terms, <https://stats.oecd.org/glossary/detail.asp?ID=4721>, E: 23.03.2022.

OECD, Glossary Of Statistical Terms, <https://stats.oecd.org/glossary/detail.asp?ID=1438>, E: 23.03.2022

International Monetary Fund (IMF), “Measuring The Digital Economy”, IMF Staff Paper, February 2018, s. 7. (<https://www.imf.org/-/media/Files/Publications/PP/2018/022818MeasuringDigitalEconomy.ashx>) E: 23.03.2022.

OECD (2015), Addressing the Tax Challenges of the Digital Economy, Action 1: Final Report, United Nations Conference On Trade And Development (UNCTAD), Digital Economy Report 2019, s. 4. (https://unctad.org/system/files/official-document/der2019_en.pdf) E: 23.03.2022.

Council directive (EC), on laying down rules relating to the corporate taxation of a significant digital presence, COM (2018), 147 final 2018/0072, Madde 3(5), https://ec.europa.eu/taxation_customs/system/files/201803/proposal_significant_digital_presence_21032018_en.pdf, E:25.03.2022.

OECD (2018), Tax Challenges Arising from Digitalisation –Interim Report 2018.

OECD (2020), Tax Challenges Arising from Digitalisation – Economic Impact Assessment: Inclusive Framework on BEPS.

<https://www.oecd.org/tax/beps/oecd-g20-inclusive-framework-members-joining-statement-on-two-pillar-solution-to-address-tax-challenges-arising-from-digitalisation-october-2021.pdf> E:29.03.2022.

OECD (2021), Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy s. 1-2, <https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.pdf> , E: 29.03.2022.

Communication from the Commission to the European Parliament and the Council A Fair and Efficient Tax System in the European Union for the Digital Single Market’ (COM(2017) 547 final of 21.09.2017).

Council Directive (EC), on the common system of a digital services tax on revenues resulting from the provision of certain digital services, COM (2018), 148 final 2018/0073, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0148&from=EN> , E:30.03.2022.

UNCTAD (2019), Digital Economy Report: Value Creation and Capture: Implications for Developing Countries, <https://unctad.org/webflyer/digital-economy-report-2019> , E: 30.03.2022.

OECD (2014), Gelir ve Servet Üzerinden Alınan Vergilere İlişkin Model Anlaşma; Kısaltılmış Basım 2014, s. 85, https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2014_9789264255265-tr#page81 E:30.03.2022.

OECD (2017), Model Tax Convention on Income and on Capital: Condensed Version 2017, s. 116, https://read.oecd-ilibrary.org/taxation/model-tax-convention-on-income-and-on-capital-condensed-version-2017_mtc_cond-2017-en#page118 , E: 30.03.2022.

<https://ms.hmb.gov.tr/uploads/sites/3/2022/01/2021-Aralik-Ayi-Merkezi-Yonetim-Mali-Istatistikleri-Bulteni.pdf>.

<https://www5.tbmm.gov.tr/sirasayi/donem27/yil01/ss128.pdf>.

ÜNİTE 8

BİLİŞİM SUÇLARI VE BİLİŞİM CEZA HUKUKU

ANAHTAR KAVRAMLAR

Ceza Hukuku

Bilişim Hukuku

Bilişim Suçları

Siber Suçlar

BİLİŞİM SUÇLARI VE BİLİŞİM CEZA HUKUKU

ÖĞRENME HEDEFLERİ

1

Bilişim hukuku ile ceza hukuku bağlantısını kurmak.

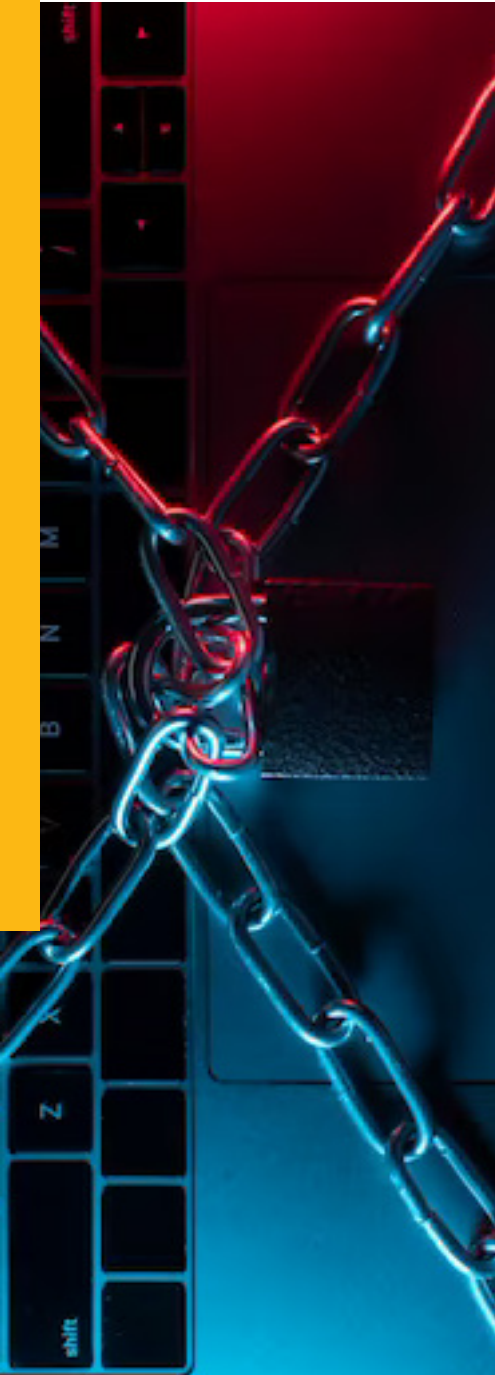


2

Bilişim alanındaki suçların neler olduğunu, unsurlarını ve bu suçlar için öngörülen cezaları öğrenmek



GİRİŞ



Günümüzde bilgi ve enformasyonun etkin olarak işlenmesinde belki de en önemli yere sahip olan bilişim teknolojisinin gelişimi ve özellikle modern bilgisayarın 20 yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşümün içinde şekillenerek kullanımın yaygınlaşmasıyla birlikte, toplumsal kurumları çeşitli yönleriyle etkilemeye başlamıştır. Söz konusu etkinin kapsamı ve boyutları, dönüşümün dinamikleri ve derinliğiyle bağlantılıdır. Toplumsal bir kurum olan hukuk da birçok yönüyle söz konusu gelişimden etkilenmektedir. Bu bağlamda, bilişim suçları, bilgisayar suçları gibi birçok ad altında incelenen suçlar, dönüşümün maddi ceza hukukuna etkisini oluşturmaktadır.

Bu kapsamda bilişim suçları olarak adlandırılan suçlar, tek başına ne bir bilim dalı olarak bilişim ne de bir bilişim sistemi olarak bilgisayar ya da İnternet'in kullanılmaya başlanmasıyla açıklanabilmektedir. Bilişim sistemlerinin kullanılmasının sosyo-ekonomik dönüşüm içinde ceza hukukuna etkisi olarak anlaşılması karşısında, birçok suçun bilişim suçları başlığı altında incelenmesi mümkündür. Nitekim bu gelişimin etkisiyle düzenlenen Avrupa Konseyi Siberaç Sözleşmesi söz konusu etkinin belirli bir dönemdeki etkisi olarak önemli bir örnek oluşturmaktadır.

Farklı nitelikteki birçok suçun bilişim suçları adı altında gündeme gelmesi, bilişim suçlarının incelenmesine ilişkin belirli bir sınırlandırılmaya gidilmesi zorunluluğunu doğurmaktadır. Bu nedenle konu, daha çok 5237 Sayılı TCK'nin 243 ve 244. maddelerinde düzenlenen sınırlı tutulmuş banka ve kredi kartlarının kötüye kullanılması suçuna ve ayrıca Elektronik İmza Kanununda düzenlenen suçlara da ilgisi olduğu ölçüde kısa bir şekilde değinilmiştir. Özellikle TCK'nin 243 ve 244. maddesinde düzenlenen suçlar, ceza mevzuatlarına yeni suçların girmesi anlamında niteliksel bir etki olarak karşımıza çıkmaktadır.

Ayrıca kişisel verilerin korunmasına ilişkin TCK'nin 135 vd. maddelerinde düzenlenen suçlar da inceleme konusu yapılmıştır. Her ne kadar genel olarak bilişim suçları başlığı altında incelenmese ve Siberaç Sözleşmesinde yer verilmemiş olsa da kişisel verilerin korunması da

sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kullanımının önemli bir etkisi olarak ortaya çıkmakta ve kişisel verilerin korunmasına ilişkin suçlar bu etkinin bir sonucu olarak ceza mevzuatlarında yer edinmektedir.

Bu suçların incelenmesi, sosyo-ekonomik dönüşüm içinde anlam kazanan ve bilişim suçları adı altında suç olarak düzenlenen fiiller yönünden, düzenleme yeri ve kapsamına ilişkin soruna ve sorunun çözümüne ilişkin 5237 Sayılı TCK'de hakim olan yaklaşımın ve yöntemin tespiti bakımından önem arz etmektedir.

Bu nedenle, bilişim sistemleri ve özellikle İnternet aracılığıyla işlenen çocuk pornografisi, ırkçılık ve yabancı düşmanlığı, hakaret gibi suçlar ile telif haklarının korunmasına ilişkin suçlar, kapsam dışı bırakılmıştır. Gerçekte, bu tür suçların bilişim suçları arasında incelenmesinin nedeni, bilişim sistemlerinin kullanılması suretiyle işlenme oranlarının artması ve yaygınlaşmasından kaynaklanmaktadır. Niceliksel etki olarak gündeme gelen bu husus farklı açılardan önem az edebilmekle birlikte bu çalışmanın kapsamı dışında bırakılmıştır.

TCK'deki ifadesiyle, "Bilişim Alanında Suçlar" hem 765 Sayılı TCK hem de 5237 Sayılı TCK'nin çeşitli yönleriyle düzenlenmiştir. 765 Sayılı TCK'nin 525a vd. maddelerinde "Bilişim Alanında Suçlar" başlığı altında düzenlenen suçlar, sosyo-ekonomik dönüşümde bilişim sistemleri ve özellikler bilgisayar sistemlerinin kullanımının bir etkisi olarak ilk defa ceza mevzuatımızda yer edinmiştir. Kişisel verilerin korunmasına ilişkin suçlar ise ilk defa 5237 sayılı TCK'de özel olarak düzenlenmiştir.

Bu haliyle ceza hukuku açısından sorunun bir yönü, bilgi ve enformasyonun, korunmasıyla ilgilidir. Sorunun diğer bir yönü, sayısallaşma olarak adlandırılan durum ile ilgilidir. Sosyo-ekonomik faaliyetlerin ağırlıklı olarak bilişim ve bilgisayar sistemleri aracılığıyla gerçekleştiriliyor olması karşısında, bilişim alt yapısının korunması da önemli hale gelmiştir. Bu tür sorunlar, bir bütün olarak, bilişim sistemlerine ve bilgi ya da enformasyonu temsil eden veriye yönelik bir kısım fiillerin suç olarak düzenlenmesine ilişkin tartışmaları beraberinde getirmiştir.

Söz konusu sorunlara ilişkin olarak ceza hukukunda tartışmaların merkezini oluşturan hususlar, hangi değer korunduğu ve bununla bağlantılı olarak bu değerlere yönelik saldırıları ifade eden hangi tür fiillerin suç olarak düzenlenmesi gerektiğidir. Nitekim, bilişim suçları olarak adlandırılan suçlarda, öncelikli olarak ceza müeyyidesiyle koruma altına alınan değer ne olduğunun tespiti önemlidir. Bu husus, bir yandan korumanın amacını ve meşruiyetini göstermektedir. Diğer bir yandan da suçun hukuki konusunun saptanması sonucunu doğurmaktadır. Suç olarak düzenlenen fiiller ise, söz konusu değerlere yönelik ihlal yöntemlerinin ne şekilde olduğunun ya da olabileceğinin belirlenmesi suretiyle tespit edilmiştir.

Sorunun odak noktasının suçun hukuki konusunun ve bununla bağlantılı olarak özellikle suç olarak düzenlenecek fiillerin belirlenmesi olarak ortaya çıkması, söz konusu suçların incelenme yöntemini de belirlemiştir. Bu doğrultuda, tartışmanın merkezinin suçun hukuki konusu ve suç olarak düzenlenen fiiller olması, bu incelemenin ağırlıklı olarak bu iki husus etrafında yapılması tercihinin de belirleyen etkenlerdendir.

Bilişim Suçları - Terim, Tanım ve Kapsam Sorunu

Bilişim ve özellikle bilgisayar sistemlerinin yaygınlaşması ile birlikte ceza hukuku alanında, bunların kötüye kullanımlarına ilişkin fiillerin cezalandırılabilirliği ve kötüye kullanımının ortaya çıkardığı sorunların çözümü ya da çözüme ilişkin yaklaşımlar sonucu, birçok tanım yapılmış ve bu tanımları ifade etmek üzere birçok terim kullanılmıştır. “Bilgisayar suçları”, “bilgisayar suçluluğu”, “bilişim suçları”, “internet suçları” ve Sibersuç sözleşmesinde de ifade edildiği şekliyle “siber suçlar” terimler kullanılabilmektedir.

Tanım ve terim zenginliği yanında, bu alanda ortaya çıkan ihlallerin cezalandırılabilmesine ilişkin suçlar esas alınarak, bilgisayarın ya da bilişim sisteminin suçun maddi konusu ya da suçta kullanılan araç olması gibi hususlar esas alınarak birçok sınıflandırma yapılması kapsam sorunlarını da beraberinde getirmiştir.

Nitekim bu suçlarının ne olduğu üzerinde herkesin ittifakla kabul edebileceği bir tanımın yapılabilmesinin zor olduğunu ve bunun yerine bilgisayar suçlarına ilişkin genel bir kategori suçtan bahsetmenin daha doğru olduğunu ifade edilmiştir. Bu kapsamda söz konusu suçların suçları “ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller” olarak belirlenmesi yerinde olabilecektir. Bilişim ve bilgisayarın farklı anlamlara sahip olduğunu ve “bilgisayar suçu” ile “bilişim suçu”nun birbirinden farklı şeyleri ifade ettiğini; pratikte ise bilgisayarın en yaygın bilişim aracı olması nedeniyle “bilişim suçları” yerine “bilgisayar suçları” teriminin kullanıldığı da bu görüş kapsamında belirtmektedir.

Bilişim ve bilgisayar terimlerinin farklı anlamlara sahip olduğu, bu kavramların birbiri yerine geçecek şekilde kullanılmasının hatalı olduğu Yenidünya ve Değirmenci tarafından da ifade edilmiştir. Yazarlara göre bilişim terimi, bilgisayara göre, daha geniş bir alanı kapsayıp bir üst kavramdır. Bilgisayar verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetlerini, diğer bir anlatımla veri-işlemi tek başına gerçekleştirebilmektedir. Bilişim ise, hem verilerin işlenmesini hem de verilerin aktarımını kapsar. Bilişim sistemlerinin en yaygın kullanılan unsurunun bilgisayarlar olması, “bilgisayar suçu” teriminin yaygınlık kazanmasına neden olmuştur. Bu açıklama doğrultusunda yazarlar bilişim suçu terimini kullanmayı uygun bulduklarını belirtmektedirler.

Ersoy da bilişim suçu ve bilgisayar suçu ayırımını yapmakta, bilişim suçunun bilgisayarı da kapsayan ancak daha geniş olan bilişim araçlarına karşı ya da bilişim araçları ile işlenen suçları da kapsar şekilde anlaşılması gerektiğini ifade etmektedir.

Türk hukukunda, özellikle bilişim suçu ya da bilgisayar suçu terimleri tercih edilmekte ve bu iki terim arasında anlam ve kapsam farklılığı yaratılmaktadır. Söz konusu ayırım “bilişim sistemi” ve “bilgisayar” terimlerinin farklılığından hareketle dile getirilmektedir. Bunlar arasında yapılan ayırım sonucunda, bilişim suçu teriminin bilgisayar suçlarını da içeren geniş bir kapsama sahip olduğu vurgulanmaktadır. Yazarlar tarafından yapılan bu ayırım, özellikle bilişim suçları açısından suçun konusu ya da suçta kullanılan araç olarak “bilgisayar”, 765 Sayılı TCK’de belirtildiği şekliyle, “bilgileri otomatik işleme tabi tutmuş sistem” ve TCK’nin 243 vd. maddelerinde yer alan “bilişim sistemi”nin kapsamının ne olduğuna ilişkin tartışmalardan kaynaklanmıştır.

765 Sayılı TCK’nin 525a vd. ve TCK’nin 243 vd. maddelerinde düzenlendiği şekliyle, suçun konusunun ya da suçta kullanılan aracın tespitinden önce bilişim suçu ile neyin anlaşılması gerektiğinin tespiti gerekmektedir. Yukarıda yapılan tanımlara dikkat edilecek olursa, Türk Hukukunda bilişim ya da bilgisayar suçları, bilişim sistemi, bilgileri otomatik işleme tabi tutan sistem ve bilgisayar terimlerinin anlam ve kapsamı belirlenmek suretiyle tanımlanmaktadır. Bu doğrultuda, bilişim ve bilgisayarın anlamlarından yola çıkılarak ve ayrıca bilişim sistemi olarak değerlendirilen araç ve aygıtlar ve de bilgisayar ara-

sındaki farklar da esas alınarak bilişim ya da bilgisayar suçu tanımları yapılmaktadır. Aynı şekilde söz konusu suçların sınıflandırılmasında da suçta kullanılan araç ya da suçun maddi konusu olan bilgisayar ya da bilişim sistemi esas alınmaktadır.

Bilindiği üzere suçların sınıflandırılmasında suçun maddi konusu ya da suçta kullanılan araç esas alınabilmekte ve suçlar bu şekilde de ayırımı tabi tutulabilmektedir. Bu ayırım ise, Toroslu'nun ifade ettiği üzere, öncelikli olarak maddi konusu olmayan suçların bulunup bulunmadığına ilişkin tartışmalar nedeniyle çeşitli sorunlara yol açabilmekte, bir yandan da farklı nitelikteki suçların bir araya toplanması sonucunu doğurarak, suçların sınıflandırılmasında beklenen yararın sağlanmasına engel olmaktadır. Suçta kullanılan araç ise bazı suçlarda özellikle suça etki eden neden olarak önem taşıyabilmektedir.

Suçların, maddi konu ya da suçta kullanılan aracın esas alınarak sınıflandırılmaya tabi tutulmasında ortaya çıkan sakınca, suçun maddi konusu ya da suçta kullanılan araç esas alınarak suçların tanımlanması durumunda da geçerliliğini korumaktadır. Bu doğrultuda, suçta kullanılan araç ve suçun maddi konusu esas alınarak bilişim ya da bilgisayar suçlarının tanımı yapılması da sosyo-ekonomik dönüşümde bilişim sistemlerinin hukuka etkisinin ve ortaya çıkardığı sorunların doğru biçimde tespitini zorlaştırmaktadır. Bilişim sistemlerinin kullanımının sorunları ne şekilde etkilediğinin saptanması bakımından maddi konu ya da kullanılan araç kapsamında bu suçların topluca incelenmesi kısmen yarar sağlamaktadır. Aynı şekilde, ceza mevzuatlarında yer alan suçların unsurlarının bu tür fiilleri kapsayıp kapsamadığının tespiti bakımından da yarar sağlayabilmektedir. Fakat bu tür fiillerle hangi değere yönelik saldırının söz konusu olduğunun tespitinde yetersiz kalmaktadır. Nitekim bilişim ve özellikle bilgisayar sistemlerinin kullanımının yaygınlaşma oranına bağlı olarak, çok çeşitli fiillerin işlenebilir hale gelmesi, bu tanımların kapsamının çok farklı amaçlara yönelik suçları da kapsayacak şekilde genişletilmesine ya da kendi içinde alt ayırımlar yapılmasına neden olmaktadır.

Bilişim sistemlerinin kullanımının yaygınlaşması, özellikle bilgisayar sistemlerinin ağırlıklı olarak kullanımı, kullanıldığı yere ve amacına göre hukuki sorunlara yol açabilmektedir. Ceza hukuku bakımından ortaya çıkan sorunlar, suçun unsurlarından kaynaklanabildiği gibi cezalandırma siyaseti açısından daha önce suç olarak düzenlenmeyen bir fiilin, suç haline getirilmesinin gerekli olup olmadığı şeklinde ortaya çıkmaktadır. Özetle, suç ve cezada kanunilik ilkesi açısından mevcut suçların unsurlarının bu tür fiilleri kapsayıp kapsamadığı ya da bu tür fiillere ilişkin yeni suçların düzenlenmesi, sorunun odak noktasını oluşturmaktadır.

Suçun hukuki konusu açısından bakıldığında bunun anlamı, ortaya çıkan yeni fiiller karşısında, halihazırda çeşitli suçlar ile korunan hukuki değerlerin, bu tür yeni fiiller karşısında korunmasına ilişkin yöntemin saptanmasıdır.

Sieber, 1998 tarihli çalışmasında, bilgisayar suçları teriminin ilk olarak 1960'lı yıllarda ortaya çıktığını ve ilk başlarda sadece ekonomik çıkar amacıyla işlenen suçlar kapsamında değerlendirilen bilgisayar suçlarının, 1980'li yıllardan itibaren daha da genişleyerek, telif haklarına ilişkin ihlalleri, daha önce kişisel verilerin korunması olarak ayrı başlık altında incelenen hususları ve İnternet'in yaygınlaşması ile birlikte, yasadışı içeriklerin dağıtımı gibi birçok konuyu da kapsamına aldığını ifade etmiştir. Bunun sonucunda "bilgisayar suçları" ve "bilgisayar ile ilgili suçlar" terimlerinin daha geniş bir şekilde her türlü kötüye kullanımları da kapsayacak şekilde genişletildiğini, sonrasında veri veya enformasyon suçu gibi çeşitli terimlerin de kullanıldığını ifade etmiştir. Yazara göre; çeşitli terim ve tanımlar bilgisayarın herhangi bir alanda kullanılması sonucu ortaya çıkan ve o alana ilişkin sorunlara işaret eden tanım ve terimlerdir. Bu nedenle yazar, belirli bir alanda ortaya çıkan sorunlara ya da amaca özgülenen veya teknik açıdan yapılan tanımların ve bunları ifade eden terimlerin, hukuki açıdan sınırlı bir değere sahip olduğunu ifade etmektedir. Bugüne kadar yapılan tanımların yerine, bilgisayar aracılığıyla gerçekleş-

tirilen fiillerin, bu fiiller nedeniyle korunmak istenen hukuki değerlere göre tanımlanması ve incelenmesi gerektiğini savunmuştur. Yazar bu açıdan, “bilgisayarların kötüye kullanımları”, “bilgisayarlarla ilgili ekonomik suçlar”, “bilgisayarla ilgili özel hayatın gizliliğini ihlal” ve “diğer hukuki değerlere yönelik saldırılar” başlıkları altında üç grupta toplamıştır.

Sieber’in aktardığı şekliyle, bilişim, bilgisayar suçları, bilişim suçları gibi birçok adlar altında incelenen suçlar, spesifik bir soruna işaret etmekten çok sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kötüye kullanımlarının yarattığı sorunlara çözüm arayışlarını kapsamaktadır. Sieber’in üç grup altında topladığı etki, bilişim alanındaki gelişime paralel olarak kendi bünyesine yeni konuları da katmaktadır. Bu husus aynı zamanda, bilişim suçu veya bilgisayar suçu gibi çeşitli adlar altında incelenen suçlar arasında niteliksel farklılıklarının olduğunu ve zamanla niteliksel farklılıkların artacağını göstermesi açısından önemlidir.

Bünyesine yeni konuları da ekleyen söz konusu gelişim karşısında, bilişim ya da bilgisayar suçları olarak adlandırılan suçların yukarıda aktarılan, “ceza kuralları uyarınca bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusunu içeren fiiller” örneğinde olduğu gibi suçun maddi konusu ya da suçta kullanılan araç olarak bilişim ya da bilgisayar sistemlerinin esas alınarak tanımlanması, farklı nitelikte ve farklı değerleri korumaya yönelik bir çok suçun bir araya toplanması ve incelenmesi sonucunu doğurur.

Bu durum niteliksel olarak farklı olan birçok suçun bir araya toplanması anlamına gelir. Bu tür tanımlar, ortak özelliği, sadece bilişim ya da bilgisayar sistemlerinin kullanılması olan suçların, bilişim suçları ya da bilgisayar suçları adı altında incelenmesi açısından etkinin yönü, boyutları ve derinliği hakkında bilgi verir. Bunun ötesinde niteliksel bir anlam taşımaz.

Özetle, bilişim suçları ya da bilgisayar suçlarına ilişkin bir tanım yerine, bilişim ya da bilgisayar suçları adı altında incelenen suçların, bilişim ya da bilgisayar sistemlerinin kullanımının belirli bir dönemde ceza hukukuna etkisi olarak nitelendirilmesi mümkündür. Sieber’in ifade ettiği şekliyle, ceza hukuku bakımından etki, farklı hukuki değerlere yönelik ihlalleri içermektedir.

İhlal edilen değere göre de ayırım yapılabilecek olan bu etki yeni suç tiplerinin ceza mevzuatı içerisine girmesi, bunun yanında hâlihazırdaki suçların işlenme kolaylığının ortaya çıkması ya da işlenme oranının artması şeklinde, ayırıma tabi tutulabilir.

Sonuç olarak, “bilişim suçu”, “bilgisayar suçu”, adları altında incelenen suçlar, hukuki konu açısından kategorik bir nitelik taşımamaktadır. Bunlara ilişkin tanımlar da “bir kavramın niteliklerini eksiksiz olarak belirtme veya açıklama” anlamında, tanımdan beklenen faydayı göstermekten uzaktır. Bilişim suçları, bilgisayar suçları gibi adlar altında incelenen suçlar ise, bilişim sistemlerinin ceza mevzuatlarına etkisi bakımından belirli bir dönemde ceza mevzuatlarında yer verilen suç tiplerini ifade etmektedir. Bunun yanında halihazırda ceza mevzuatlarında yer alan bazı suçların bilişim suçu vs. adlar altında incelenmesi, söz konusu suçların işlenme yoğunluğunun bilişim sistemlerinin kullanılması ile artmasında yatmaktadır.

İncelemede “bilişim suçu” teriminin kullanılması, belirli bir tanımın esas alınmasından çok, bu ad altında incelenen suçların sosyo-ekonomik dönüşümle bağlantısının daha rahat kurulabilmesine olanak sağlamasından dolayı tercih edilmiştir.

Bilişim Suçları Açısından Avrupa Konseyi Siberaç Sözleşmesi

Bilişim sistemlerinin kullanımının ceza hukukuna etkisi, sadece ÷lkesel düzeyde düzenlemelerin konusu olmakla kalmamış, aynı zamanda “Avrupa Konseyi Siberaç Sözleşmesi”nin (Resmi Gazete’de yer alan çevirideki adıyla “Sanal Ortamda İşlenen Suçlar Sözleşmesi”) de konusunu oluşturmuştur..

Sözleşmede, bir bilişim sistemi olarak bilgisayar sistemlerinin ceza hukukuna etkisi ve ortaya çıkardığı sorunlar, hem maddi ceza hukuku açısından hem de ceza yargılaması açısından ele alınmış ve bu alanlarda bilgisayar sistemlerinin kullanılması merkezinde ortaya çıkan sorunlara ilişkin çözümler getirilmek istenmiştir. Sözleşmenin ikinci kısmını oluşturan maddi ceza hukukuna ve ceza yargılamasına ilişkin sorunlar iki ana bölüme ayrılmış ve birinci bölümde maddi ceza hukukuna ilişkin düzenlemelere yer verilmiştir. İkinci bölümde ise, ceza yargılamasına ilişkin sorunlar ele alınarak özellikle delillerin elde edilmesi, korunması ve saklanmasına ilişkin olarak ortaya çıkan sorunlara çözüm getirilmek istenmiştir.

Bunun yanında, bilişim suçları olarak adlandırılan suçların özellikle bilişim ağırları ile işlenmesinin yaygın bir hal alması ve İnternet’in hızla yaygınlaşması, bu suçlara ilişkin sorunların ulusal bir sorun olmaktan çok uluslar arası bir sorun haline gelmesi gerçeğinden hareketle ayrıca üçüncü bir kısma yer verilmiştir. Üçüncü kısmın konusu, Sözleşmeye taraf devletlerin birbirleri arasında adli yardımlaşmaları ve suçluların iadesidir.

Sözleşmenin amaçları, “1.Siber suçlar alanında ÷lkelerin maddi ceza hukuku hükümlerini uyumlu hale getirmek, 2. Bu suçların ve bilgisayar sistemi kullanılarak işlenen ya da delilleri elektronik formda olan başka suçların soruşturulması ve koğuşturulması için gerekli olan ulusal ceza muhakemesi hukuku yetkilerini belirlemek, 3. Hızlı ve etkin bir uluslararası işbirliği rejimi oluşturmak” şeklinde sıralanmaktadır.

Sözleşmede yer ver verilen suçlarda ortak amaç, bu tür suçlara ilişkin olarak taraf devletlerin ceza mevzuatlarında uyum sağlamadır. Sözleşmede yer alan suçlar, daha önceki dönemlerde çeşitli ÷lkelere ceza mevzuatında düzenlenmiş olan suçların uluslararası düzeyde ele alınması şeklindedir

Bu doğrultuda, Sözleşmenin ikinci kısmında “Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Karşı Suçlar” başlığı altında yetkisiz erişim (2. madde) yetkisiz müdahale (3. madde), veriye müdahale (4. madde), sisteme müdahale (5. madde) ve aygıtların kötüye kullanılması (6. madde) suçlarına yer verilmiştir.

“Yasadışı erişim”, Sözleşmenin 2. maddesinde, kasten ve hukuka aykırı bir şekilde bir bilgisayar sisteminin tamamına veya bir kısmına girme şeklinde tanımlanmıştır. Aynı maddede, yetkisiz erişim suçunun taraf devletlerin ceza mevzuatlarında düzenlenirken, güvenlik önlemlerinin ihlal edilmesi suretiyle işlenebileceğine, verinin elde edilmesi ya da diğer gayri meşru bir niyetle sisteme girilmesi ya da bilgisayar ağırları vasıtasıyla birbirine bağlı bilgisayar sistemleri aracılığıyla işlenebileceğine ilişkin ek unsurları getirebilecekleri belirtilmiştir.

“Yasadışı araya girme” ise, Sözleşmenin 3. maddesinde düzenlenmiş olup buna göre, bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, bunlara teknik yöntemler kullanılmak suretiyle müdahale edilmesinin suç haline getirilmesi öngörülmüştür. Bu maddeye göre, taraf devletlerin bu suçun oluşmasını kötüniyet ya da bilgisayar ağırları aracılığıyla işlenmesi şartına bağlayabilmeleri mümkündür.

Sözleşmenin 4. maddesinde veriye müdahale, 5. maddesinde sisteme müdahale düzenlenmiştir. Sözleşmenin 4. maddesinde göre, veriye zarar verilmesi, verinin bozulması, değiştirilmesi veya ortadan kaldırılmasının suç olarak düzenlenmesi gerekmektedir. Madde incelendiğinde, verinin bilgisayar içinde bulunması ya da herhangi bir saklama aygıtında olması arasında fark yaratılmadığı gör÷lmekte-

dir. Aynı maddenin ikinci fıkrasında, taraf devletlerin söz konusu suçun gerçekleşmesi için ciddi zararın varlığı şartına yer verebilecekleri ifade edilmiştir.

Sözleşmenin 5. maddesinde, sisteme müdahale düzenlenmiştir. Sözleşmenin beşinci maddesinde sistemin işleyişinin ciddi olarak engellenmesinin suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler, sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınarak düzenlenmiştir. Bu açıdan, fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir.

Sözleşmenin 6. maddesinde ise, birtakım hazırlık hareketlerinin suç olarak düzenlenmesi yoluna gidildiği görülmektedir. Nitekim 6. maddenin 1. fıkrasına göre, Sözleşmenin 2-5. maddelerinde düzenlenen suçların işlenmesi için öncelikli amacının söz konusu suçların işlenmesine yönelik tasarlanmış ya da uyarlanmış olan program da dahil cihazların (m. 1/a. i); söz konusu suçların işlenmesi amacıyla, bir bilgisayarın tamamına ya da bir kısmına erişimi sağlayabilecek bir bilgisayar şifresinin, erişim kodunun ya da benzer verinin (m. 1/a.ii), üretiminin, satışının, kullanılmak için tedarikinin, ithal edilmesinin, dağıtılmasının ya da diğer şekilde erişilebilir kılınmasının taraf devletlerce suç olarak düzenlenmesi hükmüne yer verilmiştir.

Aynı maddenin “b” bendinde, Sözleşmenin 2 ila 5. maddeleri arasında düzenlenen suçların işlenmesi amacıyla, “a” bendinde sayılan hususların elde bulundurulmasının suç olarak düzenlenmesi gerektiği ifade edilmiştir. Elde bulundurma suç sayılabilmesi için taraf devletlerin yukarıda sayılanların belirli bir sayıda olmasına ilişkin ek şart getirebilecekleri hükmüne yer verilmiştir.

Maddenin 2. fıkrasına göre yukarıda sayılan hükümler, bu tür aygıt ya da programların, bir bilgisayarın korunması ya da test amacı gibi Sözleşmenin 2 ila 5. maddelerinde belirtilen suçların işlenmesi amacını gütmeyen meşru amaçlar için üretimi, satışı, kullanılmak için tedariki, ithal edilmesi, dağıtılması ya da diğer şekilde erişilebilir kılınmasını cezalandıracak şekilde yorumlanamaz

Aynı maddenin son fıkrasında ise, bilgisayar şifreleri, erişim kodlarının ya da benzer verilerin satışının, dağıtımının ya da diğer şekillerde erişilebilir kılınmasının cezalandırılabilmesine ilişkin hükümler saklı tutulmak kaydıyla, taraf devletlerin ceza mevzuatında birinci fıkrada düzenlenen hususları kapsam dışı bırakabileceği belirtilmiştir.

Sözleşmenin 7. ve 8. maddelerinde, bilgisayar aracılığıyla sahtekarlık ve bilgisayar aracılığıyla dolandırıcılık fiilleri düzenlenmiştir. Yedinci maddeye göre bilgisayar aracılığıyla sahtekarlık, “*verilerin açıkça okunabilir ya da anlaşılabilir olup olmadığına bakılmaksızın, bilgisayar verilerinin hukuki açıdan orijinal veriler gibi değerlendirilmesi ya da hareket edilmesi amacıyla verilerin orijinalliğinin bozulması sonucunu doğuran, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme, fiillerin hukuka aykırı olarak kasten işlenmesi*” şeklinde tanımlanmıştır. 8. maddede düzenlenen bilgisayar aracılığıyla dolandırıcılık, sistemin işleyişine ekonomik bir yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması, bunların yanında sistemin işleyişine diğer herhangi bir müdahale seçimlik hareketler olarak düzenlenmiştir.

Sözleşmenin 9.maddesinde ise, içerikle ilgili suçlar başlığı altında çocuk pornografisine ilişkin hükümler yer almaktadır. Bu kapsamda yasaklanan fiiller, bilgisayar sistemleri aracılığıyla dağıtmak amacıyla çocuk pornografisinin üretilmesi (m. 9/1.a), sunulması veya temin edilebilir hale getirilmesi (m. 9/1.b) ; dağıtılması ya da iletilmesi (m. 9/1.c); kendisi ya da başkası için bilgisayar sistemi aracılığıyla elde edilmesi (m.9/1.d); son olarak, bilgisayar sistemi içerisinde ya da bilgisayar veri depolama ortamında çocuk pornografisi bulundurulmasıdır (m. 9/1.e). Maddede çocuk pornografisi, bir küçüğün cinsel içe-

rikli bir eylemde kullanılması, küçük gibi görünen bir kişinin cinsel içerikli bir eylemde kullanılması ya da bir küçüğün cinsel içerikli bir eylemde yer aldığını temsil eden gerçekçi imaj olarak tanımlanmıştır. Maddeye göre, küçük 18 yaşından küçükleri ifade etmekte, taraf devletlerin 16 yaşına kadar indirilebilmelerine imkan tanınmaktadır.

10. maddede ise, telif hakları ve bağlantılı hakların korunmasına ilişkin uluslararası düzenlemelerde yer alan hükümlerin etkin bir şekilde uygulanabilmesi ve de ihlallerin cezalandırılabilmesine ilişkin cezai hükümlere yönelik düzenlemelere yer verilmiştir.

Sözleşme incelendiğinde, bilişim suçlarının, Sözleşmedeki ifadesiyle siber suçların kapsamının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilişim sistemlerinin kullanılmasıyla ve özellikle İnternet'in yaygınlaşması ile birlikte niceliksel olarak ortaya çıkan sorunları da kapsadığı görülmektedir. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak Sözleşmeye yapılan ek protokolle kapsama alınan, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler de bu grubu oluşturmaktadır. Sözleşmede bu suçların minimum bir uzlaşmayı temsil ettiği ve taraf devletlerin kendi mevzuatlarında başka suçları da öngörebilecekleri belirtilmiştir.

Bilişim Suçları Açısından Türk Ceza Kanunu

Bilişim Alanında Suçlar

Bilişim Sistemine Yetkisiz Erişim (Bilişim Sistemlerine Hukuka Aykırı Girme)

Yetkisiz erişim suçuna ilişkin olarak TCK'nin 243. maddesinin birinci fıkrasında yer alan düzenleme şu şekildedir: (1) 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. (2) Yukarıdaki fıkra da tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."

Siber Suç Sözleşmesi Madde 2 - Yasadışı Erişim

"Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasa tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir."

Sorun, veri ve veri işleme faaliyetinin yetkisiz kişilerin müdahalesinden uzak bir şekilde gerçekleştirilmesi olduğunda, özellikle, ağ üzerinden bilişim sistemleri ile iletişim kurma imkanlarının artması karşısında, bu tür faaliyetin ana unsurunu oluşturan bilişim sistemlerinin yetkisiz müdahalelerden uzak bir şekilde kullanımının sağlanmasının da önemi artmıştır. Bu açıdan, bilişim sistemlerinde yetkisiz üçüncü kişilerin işlem yapabilme yetkisini elde etme (en azından okuma yetkisi) anlamına gelen bilişim sistemlerine yetkisiz erişimin cezalandırılabilir bir fiil olarak nitelendirilmesi yoluna gidilmiştir.

Bilişim sistemleri aracılığıyla gerçekleştirilebilen diğer ihlaller esas alındığında bilişim sistemine erişim, diğer birçok suçun işlenmesinde bir araç olarak gerçekleşebilmektedir. Bu açıdan, yetkisiz erişimin ayrı bir suç olarak düzenlenmesi, suç olarak düzenlenen diğer fiilleri gerçekleştirme olanağına sahip olan kişinin, somut durumda bunları gerçekleştirip gerçekleştirmediğine bakılmaksızın cezalandırılabilmesine olanak sağlamaktadır. Yetkisiz erişim fiilinin esas alındığı düzenlemelerde ve bu doğrultuda 243. maddede de düzenlendiği şekliyle, sisteme herhangi bir zarar verip verilip verilmediğine bakılmaksızın failin cezalandırılmaktadır ve bu haliyle tehlike suçu niteliğindedir.

Suçun Hukuki Konusu

Genel Olarak

Bilişim sistemlerine yetkisiz erişim suçuyla, söz konusu sistemlerin sahibi ya da kullanıcılarının ilgili sistem üzerinde tasarruf edebilmelerine ilişkin yetkinin korunması amaçlanmıştır. Bu tasarruf yetkisi, genel olarak bir bilgisayar sistemine kimlerin erişim sağlayabileceğinin ya da diğer bir ifade ile girebileceğinin, sistem sahibi ya da sistem üzerinde hak sahibi olan diğer kişiler tarafından belirlenebilmesi anlamındadır. Bu şekliyle, dışa dönük bir nitelik taşıyan tasarruf yetkisinin görünümü, kimi düzenlemelerde kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ve dolayısıyla mameleki bir değer korunması, kimi düzenlemelerde ise, özel hayatın gizliliğinin belirli bir yönünün korunması şeklinde ortaya çıkmıştır.

Mameleki Bir Değerin Korunması Açısından Siberalan

Malvarlığının ve dolayısıyla kişiye ait mameleki değer korunmasına ilişkin yaklaşım, ABD’de özellikle federe devletlerde (eyalet) kendisini göstermektedir. Bu devletlerin ilgili düzenlemelerinde verinin kendisi eşya olarak kabul edilmiş ve dolayısıyla verinin ele geçirilmesi suçu da mameleki değer korunmasına yönelik bir suç olarak düzenlenmiştir. Aynı yaklaşım, yetkisiz erişim suçu bakımından da geçerliliğini korumaktadır. Bu husus, bir yönden yetkisiz erişim suçunun özellikle Federe devletlerde ceza mevzuatları içerisinde düzenlendiği yerde etkisini göstermektedir. Diğer bir yönden, yetkisiz erişim suçunun kıyasen incelendiği ve başkasının mülküne girilmesi olarak çevrilebilecek olan “criminal trespass” suçunun niteliği göz önünde tutulduğunda, ABD ve özellikle federe devletlerde yetkisiz erişim suçu ile mameleki değer korunmak istendiği sonucuna götürmektedir. Burada özellikle vurgulanması gereken nokta, sanal bir alanın varlığı noktasından hareket edilmiş olmasıdır.

Gerçek ve sanal alan ayırımı Avrupa Konseyi Sifersuç Sözleşmesinde de yer almıştır. Sözleşmenin açıklayıcı raporunda da (gerekçesi) siber alan ya da sanal alan “*Enformasyon teknoloji alanındaki hızlı gelişmenin modern toplumun her bölümünde doğrudan etkiler doğurduğu, dünyanın herhangi bir yerinden herhangi bir kişinin erişim sağlayabileceği internet de dahil olmak üzere enformasyon super-otoyollarının ve ağlarının ortaya çıkışının bu gelişmeyi hızlandırdığı. Enformasyon ve iletişim servislerine bağlanılması suretiyle kullanıcıların bir çeşit ortak alan yarattıkları ve bunun siber alan olarak adlandırıldığı...*” şeklinde ifade edilmektedir.

Bu durumda, gerçek alan ve sanal alan ayırımında, Sözleşmenin açıklayıcı raporunda belirtilen ortak alan içinde, kişiye ait ya da kişinin tasarrufu altında olan bir alanın yetkisiz üçüncü kişilerin müdahalesinden korunması söz konusu olmaktadır. Bu yaklaşım ise genel olarak gerçek alan ve sanal alan ya da siber alan şeklinde ikili bir ayırıma dayanmaktadır.

Özel Hayatın Gizliliğinin Korunması Kapsamında Siberalan

Sanal alan gerçek alan ayırımı, İtalyan Ceza Kanununda düzenlenen yetkisiz erişim suçunda da, suçun hukuki konusu bakımından etkisini göstermiştir. Sisteme yetkisiz erişim suçu, Kanunun “*kişilere karşı suçlar*” düzenleyen 12. bölümünde bireysel özgürlüklere karşı suçlar kapsamında, “*konut dokunulmazlığına karşı suçlar*” arasında 615 ter maddesinde düzenlenmiştir. İtalyan Ceza Kanunun 615 ter maddesinde, “*bilişim*” veya “*telematik*” sistemlerine hukuka aykırı girme veya hak sahibinin açık veya zımni rızası hilafına sistemde kalmaya devam etme fiilleri cezalandırılmaktadır.

Konut dokunulmazlığına karşı suçlar arasında düzenlenen yetkisiz erişim suçu ile ilgili olarak maddede gerekçesinde, “*bilişim*” ve “*telematik*” sistemleri ile İtalyan Anayasasının 14. maddesince güvence altına alınan ve daha önemli hallerde İtalyan Ceza Kanunun 614. ve 615. maddeleri ile korunan ilgili kişiye ait saygı alanı kapsamında olan konutun düşünsel olarak genişlediği ifade edilmiştir.

Bu gerekçe incelendiğinde, özel hayatın gizliliği kapsamında fiziksel bir alan olarak korunan konut yanında bilgisayar sistemlerinin kullanılmaya başlanması ile birlikte konutun düşünsel olarak genişlediği ifade edilmekle, düşünsel bir alanın varlığı da vurgulanmaktadır. Bu ikili ayırım doğrultusunda sanal alan içinde kişinin tasarrufunda bulunan alan, ABD’de genel olarak malvarlığına ilişkin bir değer koruması olarak karşımıza çıkmakta iken, İtalya’da, özel hayatın gizliliğinin korunması kapsamında, konutun bir uzantısı olarak algılanmış ve yetkisiz erişim suçu, konut dokunulmazlığının elektronik ihlali olarak ifade edilmiştir.

Sırrın Korunması Açısından Verinin Gizliliğinin Dolaylı Olarak Korunması

Yetkisiz erişim suçunun hukuki konusunun belirli bir alan –siber alan- açısından malvarlığının ve kişinin malvarlığı üzerindeki tasarruf yetkisinin korunması ya da özel hayatın gizliliği kapsamında konut dokunulmazlığının korunması ile aynı yönde olduğu görüşleri yanında, bu suçun hukuki konusu ile ilgili olarak ileri sürülen diğer bir görüş, yetkisiz erişim suçunun sırrın korunmasına yönelik olduğudur.

İtalyan Ceza Kanununda yetkisiz erişim suçunun düzenlendiği yer ve hukuki konusuna ilişkin ileri sürülen eleştirilere göre, bilişim sistemleri yukarıda aktarıldığı üzere konut ve konutun devamı olan bir sanal alan yaratmamaktadır. Bu açıdan, bilişim sistemlerine yetkisiz erişim suçu ile korunmak istenen husus, bilişim sistemleri içerisinde bulunan veri hakkında yetkisiz üçüncü kişilerin bilgi sahibi edine-memesi olup, bu husus konut dokunulmazlığının da dâhil olduğu özel hayatın gizliliğinin korunması bakımından başka bir yönü gündeme getirmektedir. Bu da özel hayatın gizliliğinin korunmasının bir yönü olarak sırrın korunmasıdır. Bilişim sistemleri açısından, sırrın korunması, bilişim sistemleri içerisindeki verilere erişimin korunması olarak ortaya çıkmakta ve söz konusu durum verinin gizliliğinin korunmasını gündeme getirmektedir.

Söz konusu yaklaşım, sırrın korunması esasından hareketle düzenlenen verinin ele geçirilmesine ilişkin suçlarla hukuki konu bakımından paralellik arz etmektedir. Verinin ele geçirilmesine ilişkin suçlarda verinin gizliliğine yönelik doğrudan bir koruma sağlanırken, bilişim sistemlerine yetkisiz erişime ilişkin düzenlemelerde bilişim sistemlerinin gizliliğinin korunması dolayısıyla bilişim sistemleri içerisindeki verinin gizliliği korunmakta; verinin gizliliği bakımından, sırrın korunması anlamında, dolaylı bir koruma sağlanmaktadır.

Türk Ceza Kanunda Düzenlenen Yetkisiz Erişim Suçunun Hukuki Konusu

243. maddede düzenlenen yetkisiz erişim suçunun hukuki konusu ile ilgili olarak çeşitli görüşler ileri sürülmüştür. Bu görüşlerden bir kısmında, 244. maddede düzenlenen suçun hukuki konusunun özel hayatın gizliliğinin korunması olduğu ifade edilmiştir. Kurt, bilişim sistemine yetkisiz erişim suçu ile sistem sahibinin kişisel alanına girildiğini ifade etmiştir. Yazara göre; *“Bilişim sistemine girme ve orada kalmaya devam etme suçunda korunan hukuki yarar, özel hayatın gizliliği ve sırların masuniyeti olarak belirlenebilir. Bilişim sistemi ve içinde bulunan veriler, programlar sistem sahibinin özel alanı da bulunmaktadır. Bu suç ile bu alana girilmesi suretiyle güvenlik ve sükun duygusunun sarsılması önlenmeye çalışılmıştır. Bilişim sistemi sahibinin kişisel alanına girilmektedir. Hak sahibi izin vermedikçe bu alana girilmesi mümkün değildir. Anayasanın 20. maddesindeki ‘özel hayatın gizliliği’ne ilişkin maddesine paralel bir hüküm olarak karşımıza çıkmaktadır.”* Yazarın bu görüşü incelendiğinde, bilişim sistemlerinin kullanılması ile birlikte, ABD’de federe devletlerde başkasının mülküne girme ile aynı yönde gelişen, İtalyan Ceza Kanununda konut dokunulmazlığının elektronik ihlali şeklinde somutlaştırılmak istenen, gerçek alanın yanında bir siber alanın var olduğu görüşü ile paralellik arz etmektedir.

Bıçkın ise, 243. maddede düzenlenen suçun hukuki konusunun karma bir nitelik gösterdiğini ve devamında Kurt ile aynı yönde ilk olarak *“bireyin özel hayatının korunduğunu”* belirtmektedir. Yazar, özellikle 2. fıkra da yer alan düzenlemeyi esas alarak, *“malvarlığının”* da korunan hukuki menfaatler arasında olduğunu, çünkü bu fıkra da bedeli karşılığında yararlanılabilen sistemler hakkında ilgili suçun işlenmesi halinin düzenlendiğini vurgulamaktadır.

TCK’nin 243 maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun karma bir nitelik taşıdığı, başka bir açıdan, Dülger tarafından da ifade edilmiştir. Yazar, yetkisiz erişimin engellenmesiyle sistemin malik ya da kullanıcıları olarak sistemden faydalanan kişilerin birçok sayıdaki farklı türden çıkarları koruma altına alındığını belirtmektedir. Bu kişilerin çıkarlarının, verilerin gizliliğinin korunması, özel hayatın dokunulmazlığı ya da kişilerin ya da kurumların ihtiyaç duyduğu güvenlik duygusu gibi farklı hukuksal değerler olabildiğini ifade etmiştir. Yazar, farklı türden çıkarlar olarak ifade ettiği bu değerlerin üstünde ve bu değerleri kapsayacak şekilde *“bilişim sisteminin güvelliği”* nin korunmasının asıl hukuki konuyu oluşturduğunu belirtmiştir. Aktarılan bu görüş ise, yukarıda belirtildiği üzere, Siber Suç sözleşmesinin 2. maddesinde düzenlenen yetkisiz erişim suçu ile ilgili olarak Sözleşmenin açıklayıcı raporundaki gerekçe ile paralellik arz etmektedir.

Bu kapsamda TCK’nin 243. maddesinde düzenlenen yetkisiz erişim suçunun hukuki konusunun saptanmasında TBMM Genel Kurul görüşmelerinde 244. maddeye ilişkin değişiklik teklifi ve bu teklif hakkındaki görüşlerin bilinmesi önemlidir. Söz konusu değişiklik teklifine ilişkin görüşler maddenin hangi hukuki konuya yönelik olarak düzenlenmek istediğini göstermesi bakımından önemlidir.

Nitekim, 243. maddeye ilişkin TBMM Genel Kurulunda yapılan görüşmelerde suçun unsurlarına ilişkin bir değişiklik teklif edilmiş ve bu teklif kabul edilerek madde son şeklini almıştır. Suçun unsurlarında yapılması istenen değişikliğe ilişkin *“Biliyorsunuz bir de bilgisayar sistemin bozan hackerlar var, onlar size bir şey gönderdi, üzerine tıkladınız ve bir sisteme girdiniz. Hemen bunu suç haline getirirsek, çok geniş bir kapsama almış oluruz, suç kapsamını genişletmiş oluruz. Burada da -hazırladığımız tas-lakta- girme ve orada kalma şerhini koyduk; çünkü, bu bir kasttır. Kazara girersiniz çıkarsınız, bu başka bir şey; ama girdiniz kaldınız, değiştirdiniz, bozdunuz, bu farklı bir şey. İşte biz tasarıda, buraya açıklık getirdik. Bağlantılı olarak 244’te de bir açıklık getiriyoruz.”* gerekçesi ileri sürülmüştür.

Aynı değişiklik teklifinde 243. maddenin son fıkrasında düzenlenen ağırlatıcı nedenin varlığı halinde öngörülen cezanın miktarına ilişkin olarak şu görüş dile getirilmiştir: *“Çocuğunuz 16 yaşında; geldi, bilişim sistemine girdi ve istemeden bir değişikliğe ya da veri kaybına neden oldu. Biz, şu andaki tasarıda diyoruz*

ki, bu kişiyi iki yıldan dört yıla kadar mahkûm edelim; ama, bir sonraki maddede diyoruz ki, bozma niyeti olana, bozma amacıyla, veriyi değiştirme amacıyla, sistemin tamamına zarar verme amacıyla bu eylemi işleyene de bir yıldan üç yıla kadar ceza verelim; hazırlanan metin bu şekilde. Şimdi, bir şey düşünün; suçu işleyen kişi, hâkimin karşısına geçecek, bu işi bilmeyerek yaptıysa, daha az ceza almak için “hâkim bey, benim kastım vardı, bu işi bilerek, isteyerek yaptım” diyecek ve bunun karşılığında daha az bir ceza alıp kurtulacaktı. Fiilde dengesizlik var.”

Her iki görüş incelendiğinde, 243. maddenin hukuki konusu ile ilgili olarak özel hayatın gizliliğinin ya da bu kapsamda sırrın korunmasına ilişkin tercihin esas alınmadığı görülmektedir. Bunun yerine, bilişim sisteminin işleyişinin korunması açısından bilişim alanında işlenen suçların konusunu oluşturan hareketler arasında önem dercesine göre bir ayırım yapılmıştır. Bu açıdan, söz konusu fiiller içinde en hafifi sisteme girilmesi olarak kabul edilmektedir. Her ne kadar hatalı olarak suçun manevi unsuru kapsamında sadece girmenin suç sayılması çeşitli sakıncalara yol açacağı belirtilmişse de gerekçenin devamı incelendiğinde girmenin önem derecesi bakımından en alt sırada olduğu ve en önemli hususun sistemin bozulması olarak ifade edildiği görülmektedir.

Bu kapsamda söz konusu suçla korunan hukuki değere yönelik olarak farklı görüşler ileri sürülmektedir.

Yetkisiz Erişim Suçunun Maddi Unsuru-Sisteme Girme ve ya Orada Kalmaya Devam Etme

Yaygın olarak “illegal access” “yetkisiz veya hukuka aykırı erişim” olarak adlandırılan bu suçun maddi unsurunu oluşturan ilk hareket sisteme erişim (access) olarak düzenlenmektedir. Avrupa Konseyi Siberaç Sözlüğü’nin İngilizce metninde de bu suç “illegal access” (yetkisiz/hukuka aykırı erişim) olarak adlandırılmaktadır. Aynı şekilde ABD ve İngiltere’de bu suç yetkisiz erişim olarak adlandırılmakta ve bu suçla ilişkin düzenlemelerde suçun maddi unsuru, sisteme erişim (access) olarak düzenlenmektedir.

Parker, Türkçeye erişim olarak çevrilen “access” teriminin ceza hukuku alanında karışıklıklara yol açabileceğini, bu terimin fiziksel bir alana erişilmesini ya da girilmesini çağrıştırdığını, fakat bilgisayara girişin bu açıdan imkânsız olduğunu belirtmektedir. Bilgisayar sistemlerinin işleyişinde, bilgisayara sinyal gönderilmesi ve bunun sonucunda, bilgisayarın, bu sinyale belirli bir programın çalışması ve sıklıklı bir programın başlaması şeklinde cevap vermesinin söz konusu olduğunu ifade etmektedir. Bu nedenle, kullanılması gereken doğru terimlerin, “bilgisayara yaklaşılma (approach) ya da enformasyona girilmesi” ve bilgisayarın “kullanılması” olduğunu vurgulamaktadır.

Günümüzde yaygın olarak kullanılan Windows ve Unix tabanlı işletim sistemleri açısından değinilecek olursa, en az bir yönetici hesabı ve bunun yanında sistemin teknik olarak elverdiği sayıda oluşturulabilecek kullanıcı hesabı bulunmaktadır. Kullanıcılar kimi zamanlarda yönetici yetkilerine de sahip olabilmesine rağmen, özellikle çok kullanıcıli sistemler açısından genel olarak sınırlı yetkiye sahip olabilmektedir. Sistem içerisinde kullanıcıların yetkilerinin belirlenmesi genel olarak sistem içerisinde yer alan yönetici tarafından gerçekleştirilmektedir. Bu açıdan yönetici, sistem içerisindeki kullanıcıları belirli izin, klasör ya da dosyalara erişim yani genel olarak verilere erişim bakımından sınırlandırabileceği gibi bununla birlikte belirli işlemlerin yapılması bakımından da sınırlandırabilir. Özellikle, çok kullanıcıli sistemlerde kullanıcıların yetkilerinin belirlenmesi sistem kaynaklarına kimlerin ne şekilde erişebileceğinin önceden tespit edilmesi bakımından önem arz etmektedir.

Yönetici (administrator ya da root), bir bilgisayar sisteminde, sistemin teknik olarak elverdiği ölçüde her türlü yetkileri kullanabilir. Yönetici dışındaki kullanıcılar ise, yönetici ile aynı yetkilere sahip olabileceği gibi bunun yanında daha sınırlı bir yetkilendirme söz konusu olabilir. Bu durum genel olarak yönetici ve diğer kullanıcıların ilgili sistem üzerindeki yetkileri olarak karşımıza çıkmaktadır. Bu yetkiler ise genel olarak iki grupta toplanabilir. Bunlardan birincisi genel olarak sisteme “log on (oturum açma)” yetkisi diğeri ise kullanıcıların sistem içerisinde işlem yapma (okuma-yazma-çalıştırma) yetkisidir.

Bu ayırım içerisinde, oturum açma “log on” yetkisi, kimlerin sistemi kullanma yetkisi olduğunu göstermektedir. Bu açıdan bir sistemde kimlerin oturum açma yetkisinin olduğunu belirlemesi kimlerin sistemde işlem yapabileceğinin tespiti anlamına gelmektedir. Bu yetki aynı zamanda diğer yetkilerin kullanılmasına ilişkin bir ön koşul olarak ortaya çıkar.

Söz konusu yetkiye sahip olan kullanıcının sistemde oturum açmasından sonraki konumu ise, sistem içerisindeki işlem yapma yetkileri gündeme getirir. Bu ise, genel olarak sistem aracılığıyla ya da içerisinde var olan veri ve programlar üzerinde ya da bunlar aracılığıyla işlem yapılabilmesi yetkisi anlamına gelmektedir. Sistemde oturum açma yetkisi olan kullanıcıların sistemde hangi işlemleri yapabileceği, kullanıcı hesabına ya da kullanıcı hesabının bağlı bulunduğu gruba göre sınırlandırılabilir. Bu nedenle, bir bilgisayar sisteminde işletim sisteminin elverdiği ölçüde değişik düzeyde işlem yapabilme yetkisine sahip olan kullanıcı hesaplarının oluşturulması mümkündür.

Bu doğrultuda, yetkisiz erişim fiilinde failin amacı kullanma yetkisi olmadığı bir sistem üzerinde hukuka aykırı olarak kullanma yetkisini sağlaması yani sistemde oturum açması suretiyle en azından okuma yetkisinin elde edilmesi olarak özetlenebilir. Bu durum sistem içindeki yetkilerin elde edilmesi bakımından yönetici düzeyinde ya da kullanıcı düzeyinde erişim olarak adlandırılabilir. Yetkisiz erişim, sistemi kullanmaya yetkili kullanıcılara ait erişim kodlarının (kullanıcı adı, şifre vb.) ele geçirilmesi suretiyle gerçekleştirilebileceği gibi sistem açıklarından faydalanılması ya da sistemde açık yaratılması suretiyle de gerçekleştirilebilir. Ayrıca, sisteme yetkisiz erişim, başka bir bilgisayarın kullanılması suretiyle hedef bilgisayara iletişim araçları aracılığıyla erişilmesi suretiyle gerçekleştirilebileceği gibi, hedef bilgisayarın doğrudan kullanılması yoluyla da gerçekleştirilebilir.

Özetle teknik olarak oturum açma (log on) yetkisi olarak da adlandırılan ve kimlerin sistemde oturum açabileceğini belirleyen yetkinin ihlal edilerek sistemde oturum açma, TCK’nin 243. maddesinde belirtilen hukuka aykırı girmeyi oluşturur. Bu madde kapsamında, sisteme hukuka aykırı olarak elde edilen erişim kodlarından yararlanılması suretiyle girilmesi, sistemdeki açıklardan faydalanılarak ya da sistemde açıklar yaratılarak girilmesi arasında bir fark yoktur. Aynı şekilde sistemin tamamına ya da bir kısmına girilmesi bakımından bir farklılık yoktur.

Yukarıda sistemi kullanma ya da daha teknik bir ifade ile sistemde oturum açma yetkisi olmayan bir kişinin sisteme girmesi olasılığı incelenmiştir. Burada incelenmesi gereken diğer husus, genel olarak bilişim sisteminin bütününe ya da bir kısmına girmeye yetkili olan bir kişinin sisteme kendisine ait oturum açma yetkisinin ilişkilendirildiği kullanıcı hesabından başka bir hesap ile sisteme girmesi olasılığıdır.

Burada özellikle iki olasılık açısından değerlendirme yapılması gerekir Bunlardan birincisi, sistem içerisinde işlem yapma yetkisinin kapsamı diğeri ise, maddede açıkça vurgulandığı üzere, bilişim sistemi içerisinde sistemin belirli kısımlarına girişe ilişkin yetkilendirme olarak karşımıza çıkmaktadır.

Sistem içerisinde işlem yapma yetkisinin kapsamı bakımından incelendiğinde, sistem içerisinde işlem yapma için farklı yetkilendirme söz konusu ise, kural olarak sisteme girme yetkisine sahip bir kişinin başka bir kullanıcı hesabı kullanarak sisteme girmesi durumunda yetkisiz erişim gerçekleşir. Bu durumda, sistem içerisinde sınırlı işlem yapma yetkisine sahip bir kullanıcının daha üst düzeyde işlem yapma yetkisine sahip bir kullanıcı hesabı aracılığıyla sisteme girmesi halinde hukuka aykırı bir girişten bahsedilir. Aynı düzeydeki kullanıcılar bakımından ise, işlem yapma yetkisi bakımından bir farklılaştırma yapıp yapılmadığı sisteme girmenin hukuka aykırılığın tespitinde ölçüt teşkil eder.

Madde metni incelendiğinde sadece sistemin bütününe girişten bahsedilmemekte bunun yanında sistemin bir kısmına girilmesi hali de suç olarak öngörülmektedir. Belirli bir kısma girilmesinin sınırlandırılması, yukarıda belirtildiği üzere, tek bir sistem içerisindeki yetkiler bakımından okuma,

yazma ve çalıştırma yetkileri içerisinde en azından okuma yetkisinin de verilmemiş olması anlamına gelmektedir. Bu ise, yukarı da belirtildiği üzere, oturum açma yetkisi kapsamında düşünülebilir, çünkü olan oturum açma yetkisi sistemde işlem yapma yetkisinin önkoşuludur. Sistem içerisindeki kısım ve bu kapsamda düşünülebilecek veri bakımından işlem yapma yetkilerinin kullanımı konusunda bunlar üzerinde en azından okuma yetkisinin bulunması şarttır.

Bunun dışında, başkasına ait herhangi bir kullanıcı hesabını kullanmadan sistem açıklarında yararlanılması gibi diğer yollarla sistem içerisinde girişin sınırlandırılmış olduğu bir bölüme girilmesi, yetkisiz erişimi oluşturur.

243. maddede düzenlenen suçun gerçekleşmesi için sistemin bütününe ya da bir kısmına hukuka aykırı olarak girilmesi ya da hukuka aykırı olarak, sistemde kalmaya devam edilmesi yani var olan yetkinin sonlandırılmış olmasına rağmen sisteme erişimi gerekmektedir. Sisteme girme veya orada kalmaya devam etme, , 243. maddede düzenlenen yetkisiz erişim suçunun maddi unsurunu oluşturmakta olup bu haliyle son değişiklikle birlikte seçimlik hareketli suç haline getirilmiştir.

Suçta Etki Eden Nedenler

Yetkisiz erişim suçunun düzenlendiği 243. maddenin 2. fıkrasında, fiilin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, cezada indirim sebebi olarak öngörülmüş bunun yanında son fıkra da sistemin içerdiği verilerin değişmesi ve de yok olması hali ise ağırlatıcı neden olarak düzenlenmiştir.

- Yetkisiz Erişim Suçunun Bedeli Karşılığı Yararlanılabilen Sistemler Hakkında İşlenmesi

243. maddenin 2. fıkrasında yetkisiz erişim suçunun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi cezada indirim sebebi olarak düzenlenmiştir. Kanunun madde gerekçelerinde bedeli karşılığı yararlanılabilen sistemlerin ne olduğu ve neden bu şekilde bir cezada indirim sebebinin öngörüldüğü hakkında herhangi bir gerekçeye yer verilmemiştir.

Karagülmez, maddede yer alan bu ifadenin yoruma açık olduğunu, belirli bir ücret karşılığında hizmet veren web sayfalarının bu kapsamda düşünülebileceğini belirtmektedir. Yazar, internet kafe ve benzeri yerlerde bedeli karşılığında sistemin kullanılmasının bu kapsamda düşünülmemeyeceğini ifade ederek maddede sistemin kullanıldığı mekanın değil sistem içerisindeki elektronik yapıda sunulan ücretli hizmetleri vurguladığını savunmaktadır. Yazara göre, belirli bir süre İnternet bağlantı servisinin sağlanması da bu fıkra kapsamında değildir.

Yazıcıoğlu ise, bu fıkra düzenlenirken hafifletici sebebi, ücreti karşılığı hizmet veren sistemlere girilmesi şeklinde yorumlamakta ve devamında ve bu düzenlemenin yetkisiz erişim suçunun uygulanmasının genişliğinden doğacak sakıncaları gidermesi bakımından isabetli olduğunu ifade etmektedir.

- Yetkisiz Erişim Fiili Sonucunda Sistemin İçerdiği Verinin Değişmesi ya da Yok Olması

243. maddenin 3. fıkrasında sisteme yetkisiz erişim sonucunda sistemin içerdiği verinin değişmesi veya yok olması ağırlatıcı neden olarak düzenlenmiştir. Bu fıkra, TCK'nin 23. maddesinde düzenlendiği şekliyle, neticesi sebebiyle ağırlaşan bir suç söz konusu olup ağırlatıcı nedenin uygulanabilmesi için failde verinin değiştirilmesi ya da yok edilmesi yönünde bir kastının olmaması gerekmektedir. Bu fiilin kasıtlı olarak işlenmesi halinde, 244. maddenin 2. fıkrasında yer alan hüküm gündeme gelecektir.

Bilişim sistemlerinde yer alan ve bunların işleyişini sağlayan ana yazılımlar olarak karşımıza çıkan işletim sistemleri açısından değerlendirildiğinde, genellikle bu tür işletim sistemlerinin her açılışında ya da bu sistemlere girilmesinde günlük kayıtları içeren veriler gibi birçok veri sistemin işleyişine bağlı

olarak değişebilmektedir. Bu tür değişiklikler sistemin olağan çalışması için zorunlu ya da işlevsel olup bunlardaki değişiklik bu fıkra kapsamına girmemektedir.

Bu fıkroda öngörülen ağırlatıcı nedenlerin uygulanması açısından birinci ya da ikinci fıkroda düzenlenen sistemler bakımından maddede özellikle cezanın miktarı bakımından bir fark yaratılmamıştır. Fıkroda belirtilen durumun gerçekleşmesi halinde verilecek ceza, yetkisiz erişimin konusunun bedeli karşılığı sistemler olup olmamasına bakılmaksızın altı aydan iki yıla kadar hapis cezasıdır.

Araya Girme

243. maddenin son fıkrasına 6698 sayılı Kanun ile “*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*” hükmü eklenmiştir. Sonradan eklenen bu düzenleme Siber Suç Sözleşmesinde yetkisiz erişim suçundan bağımsız bir suç olarak düzenlenmesi öngörülen “*Yasadışı Araya Girme*” suçuna ilişkin düzenlemenin TCK’deki karşılığı olarak yer almaktadır.

Siber Suç Sözleşmesi Madde 2 - Yasadışı Araya Girme

“Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi içi hukuku kapsamında cezaî suç olarak tanımlanması için gerekli olabilecek yasam tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, sözkonusu suçun sahtekârlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir.”

Diğer nitelikli hallerden farklı olarak bu düzenlemenin yetkisiz erişim suçunu ağırlaştıran bir neden olmaktan çok farklı unsurları içeren bir suça yönelik olduğu görülmektedir. Nitekim düzenlemede fiilin sisteme girmeksizin yapılması gerekliliği getirilmiştir. Aslında bu haliyle bu düzenleme kişiler arasındaki haberleşmenin gizliliğini ihlal suçunun tamamlayıcısı olarak da görülebilir. TCK’nin 132. maddesinde düzenlenen suçun oluşması için kişiler arasında bir haberleşmenin varlığı aranmakla birlikte bilişim sistemleri aracılığıyla yapılan iletişimde taraflar her zaman için hazırda bulunmamakta iletişim kimi zamanlar insan-insan, kimi zamanlar insan-sistem ya da sadece sistem- sistem arasında gerçekleşebilmektedir. Söz konusu düzenleme ile bu hususa ilişkin kişiler arasındaki haberleşmenin gizliliği ihlal suçlarının unsurlarında ortaya çıkan eksiklik tamamlanmaktadır.

Bilişim Sistemine ve Veriye Müdahale

Genel Olarak

Sosyo-ekonomik yapı içerisinde faaliyetlerin ağırlıklı olarak bilgisayar sistemleri aracılığıyla veri işleme şeklinde gerçekleştirilmeye başlanması ve bu kapsamda sayısallaşmanın yoğunluğundaki artış, verinin gizliliğine ve içeriğine ilişkin koruma yanında veri ve bilişim sistemlerinin bütünlüğünün ve erişilebilirliğinin de korunmasını gündeme getirmiştir.

Verinin işlenmesi faaliyeti bilgisayar ortamında genel olarak bir veri grubunu oluşturan ve sistemin nasıl çalışması gerektiğine ve sistem içerisindeki verinin işlenmesine ilişkin komutları içeren programlar aracılığıyla gerçekleştirilebilmektedir. Programın kendisi genel olarak verinin düzenli ve öngörülen şekilde işlenmesini sağlayan bir veri grubunu oluşturmaktadır. Veri işleme süreci içerisinde merkezi bir işleve sahip programlara müdahale edilmesi ise, her zaman için sistemin tamamen zarar görmesine yol açmamakla birlikte, veri işleme faaliyetinde aksamalara neden olabilmektedir. Bu açıdan veri işleme faaliyeti içerisinde, bunların da müdahalelerden korunması önem arz etmektedir.

Verinin işlenmesi faaliyetinin ana unsurunu oluşturan bilgisayar sistemlerinin işleyişinin ve bütünlüğünün korunmasının önemi de bu sistemlerin kullanımının yaygınlaşması ve faaliyetlerin bilişim sistemlerine bağlı olarak yapılmasına paralel bir şekilde artmaktadır¹.

Günümüzde bilgisayar sistemlerinin işleyişine, veri ve programlara müdahale genel olarak bunlara doğrudan erişim yoluyla gerçekleştirilebileceği gibi bu amacı güden kötü amaçlı programların kullanılması da yaygın bir yöntemdir. “Virüs”, “Solucan”, “Mantık Bombaları”, “DOS saldırıları²”, “Truva Atı³” yöntemleri günümüzde yaygın olarak kullanılan yöntemlere örnek gösterilebilir.

Bu gelişim sonucunda, veri ve programlara ve ayrıca bilgisayar sistemlerinin işleyişine müdahalenin engellenmesi zorunluluğu gündeme getirilmiş ve bunlara yönelik müdahaleler ceza mevzuatlarında düzenlenmeye başlanmıştır. Bu düzenlemelerde yeni ve önemli olan nokta, müdahalenin konusunun fiziki varlığı olmayan veri, program ya da genel olarak bilişim sistemlerinin yazılım unsuru olması ve sisteme yönelik müdahalelerin yazılım unsuruna yönelik olarak gerçekleştirilmesidir.

Sibersuç Sözleşmesinde bu husus veri ve programa müdahale esas alınarak, veriye müdahale 4. maddede, sisteme müdahale ise 5. maddede düzenlenmiştir. Sözleşmenin 4. maddesine göre “veriye müdahale”, bilgisayar verilerinin haksız bir şekilde kasten tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilmez kılınmasıdır. “Bilgisayar sistemlerine müdahale” ise Sözleşmenin 5. maddesinde bilgisayar verisi girişi yapmak, bilgisayar verisi göndermek, bilgisayar verilerini tahrip etmek, silmek, bozmak, değiştirmek veya erişilmez kılmak suretiyle bilgisayar sistemlerinin işleyişini ciddi bir şekilde haksız ve kasten engellemek olarak tanımlanmıştır.

Sözleşmenin 4. maddesinde düzenlenmiş olan veriye müdahale fiilinin gerçekleşebilmesi için verinin bilgisayar sistemi içerisinde veya herhangi bir veri taşıyıcısında bulunması arasında fark yaratılmamıştır⁴. Sisteme müdahalede ise, bilgisayar sisteminin fiziki bir zarar görmesi aranmamış işleyişinin

¹HEYMANN, s. 378

²İngilizce “denial of service” teriminin kısaltması olan “DOS” saldırılarında sistemin işleyemez hale gelmesi ya da sisteme erişimin engellenmesini amaçlayan hareketlere verilen genel bir ad olarak tanımlanması mümkündür. YILMAZ, s. 319 vd.

³Truva atı ise adını Truva efsanesinden almış olup genel olarak başka bir programın içine yerleştirilmiş olan kötü amaçlı kod ya da program olarak tanımlanabilmektedir. Bu haliyle bilgisayar program ve verilerine zarar verme gibi birçok amaçla kullanılabilir. PARKER, s. 89,

⁴Bkz. Sözleşme açıklayıcı rapor, parag., 60, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm..>

ciddi bir şekilde engellenmesi esas alınmıştır. Sisteme müdahalede genel olarak sistemdeki verilere müdahale edilmesi ya da sisteme veri iletilmesi suretiyle müdahale esas alınmış ve bu haliyle bilişim sisteminin fiziki varlığını oluşturan donanımına yönelik fiziksel müdahale kapsam dışı bırakılmıştır.

Sözleşmenin 4. maddesinde düzenlenen veriye müdahale ile ilgili olarak Sözleşmenin açıklayıcı raporunda, maddi varlığı olan şeylere yönelik zarar verme girişimlerine korumaya benzer bir şekilde bilgisayar veri ve programlarına yönelik fiillerin korunmak istendiği, bu açıdan verinin bütünlüğü ve düzgün bir şekilde çalışması ve kullanımının korunmasının amaçlandığı belirtilmektedir⁵. Veriye müdahale bakımından ilgili kişinin veri üzerinde, veriye yönelik olarak üçüncü kişiler tarafından gerçekleştirilecek müdahalelerden uzak bir şekilde tasarrufta bulunabilmesi sağlanmak istenmektedir. İlgili kişinin tasarruf yetkisi, verinin elde edilmesinde, üçüncü kişilerin verinin içeriğini öğrenmesinin ya da veriyi kullanmasının önüne geçilmesi şeklinde, dışa dönük olarak korunmakta iken; veriye müdahalede, veriyi elinde bulunduran kişinin veri üzerinde tasarruf yetkisinin, veriye müdahale edilerek ve bu şekilde zarar verilerek hukuka aykırı bir biçimde sınırlandırılması ya da ortadan kaldırılması anlamında içe dönük olarak korunmaktadır.

Türk Ceza Kanununda da söz konusu gelişimin etkisiyle 244. maddenin 1. fıkrasında sisteme müdahale, 2. fıkrasında ise veriye müdahaleye ilişkin düzenlemelere yer verilmiştir. Buna göre “(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) 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. (3) 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. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.”

Suçun Hukuki Konusu Açısından Mala Zarar Verme Suçu Karşısında Sisteme ve Veriye Müdahale

Bilişim sistemine yönelik müdahaleler genel olarak veri ya da programlara müdahale açısından ele alınmakta, bu haliyle ilgili kişinin sistem üzerinde sistemin işleyişi bakımından tasarruf yetkisinin korunması veriye paralel bir şekilde ortaya çıkmaktadır. Nitekim Sözleşmenin açıklayıcı raporunda bu husus, sistemi kullanan kişilerin ya da sistem operatörlerinin sistemin sorunsuz bir şekilde işlemesindeki çıkarlarının korunduğu şeklinde ifade edilmiştir⁶.

Bilişim sistemine ve veriye müdahale suçları yukarıda belirtildiği üzere genel olarak malvarlığına karşı suçlar arasında düzenlenmekte, hukuki konu esas alınarak yapılan düzenlemelerde ise mala zarar verme suçu ile aynı bölümde yer almaktadır. Özellikle hukuki konu bakımından esas alınan bu düzenleme tarzı, bu suçların hukuki konusunun tespitinde önem arz etmekte aynı zamanda bu suçların düzenlenmesinde klasik mala zarar verme suçunun kapsamı bakımından tartışmaları da beraberinde getirmektedir.

Bu kapsamda, klasik mala zarar verme suçunun düzenlenmesinde tarihsel süreç esas alındığında taşınır ya da taşınmaz malın fiziki yapısı ya da diğer bir ifade ile maddi varlığı esas alınarak bunlara yönelik zarar verici fiillerin engellenmesi amaçlandığı görülür. Mala zarar verme suçunun ceza kanunları

⁵Bkz. Sözleşme açıklayıcı rapor, parag. 60 <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

⁶Bkz. Sözleşme açıklayıcı rapor parag. 65 <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

içerisinde düzenlenmesinde ise, genel olarak bu suçun seçimlik hareketli bir suç olarak ele alınması yoluna gidilmiş ve bu yönde mala zarar verme suçunun maddi unsuru belirlenmiştir. Bu açıdan, TCK'de mala zarar verme suçu, Kanunun 152. maddesinde düzenlenmiş olup suçun maddi unsurunu oluşturan hareketler taşınır ya da taşınmaz malın kısmen ya da tamamen yıkılması, tahrip edilmesi, yok edilmesi, bozulması, kullanılmaz hale getirilmesi ve de kirletilmesi olarak karşımıza çıkmaktadır.

Bilişim sistemlerinin yaygınlaşması bu kapsamda veri işleme faaliyetinin artması ile birlikte, veri ya da programları hedef alan müdahalelerin önlenmesi ve bu tür fiillerin cezalandırılabilirliği sorununu ortaya çıkırmıştır. Geleneksel mala zarar verme suçunda genel olarak taşınır ya da taşınmaz malda genel olarak fiziksel bir zarar arandığı ifade edilmekte, bilişim sistemlerine yönelik sistemin yazılım unsuruna müdahale bilişim sistemi bakımından her zaman için fiziksel bir değişikliğe yol açmamaktadır.

Sisteme müdahale bakımından ortaya çıkan sorun, sistemin yazılım ve donanım unsurlarından oluşması karşısında, sistemin fiziki yapısı yani donanımına yönelik olmayan yani yazılım unsuruna yönelik müdahaleler sonucunda sistemin fonksiyonlarını yerine getirememesinin mala zarar verme suçu kapsamında değerlendirilip değerlendirilemeyeceğidir. Bu durumda, suçun unsurlarını oluşturan hareketler ve bu hareketler sonucunda sistemin fiziki yapısında bir değişiklik olmadan sistemin işleyişine müdahale edilmiş olması bakımından soruna yaklaşmak gereklidir.

Bilişim sistemine yönelik müdahalelerde genel olarak sorun, sisteme müdahale teşkil edebilecek fiillerin mala zarar verme suçunu oluşturup oluşturmadığıdır. Bu tür müdahalelerde sistemin maddi varlığı ya da fiziki yapısında bir değişiklik olmamasına karşın sistemin fonksiyonlarını yerine getirememesi söz konusu olmaktadır. Bu haliyle mala zarar verme suçu açısından çözümlenmesi gereken husus, mala zarar verme suçunun unsurlarının bu tür fiilleri kapsayıp kapsamadığı noktasında toplanmaktadır. Sorunun bu noktada toplanması ise, diğer bir husus hakkında, yani bu tür fiillerin cezalandırılması ise korunmak istenen değerini yani bu suçun hukuki konusu bakımından bir çözüme ulaştırabilmektedir. Sorunun suçun maddi unsuru bakımından ortaya çıkması ve bunun çözümü için yeni bir suça yer verilmesi, mala zarar verme suçunun hukuki konusu ile bu suçun hukuki konusunun aynı olduğunu göstermektedir.

Nitekim sisteme müdahale bakımından yukarıda örnek olarak verilen ceza kanunlarında hukuki konu açısından bu yaklaşımın sergilendiği ve sisteme müdahaleye ilişkin ya veriye müdahale ile birlikte ya da veriye müdahaleden bağımsız bir suç şeklinde malvarlığının korunması merkezinde özel düzenlemelerin yapıldığı görülmektedir.

Verinin bütünlüğüne yönelik müdahalelerde ise sorun, yukarıda belirtildiği şekliyle mala zarar verme suçunun unsurları bakımından ortaya çıkmakla birlikte sorunun diğer bir yönü maddi varlığı olmayan verinin, genel olarak maddi varlığı olan taşınır ve taşınmaz malın esas alınarak düzenlendiği mala zarar verme suçunun konusunu oluşturup oluşturmadığıdır⁷.

Verinin mal/eşya olarak kabul edilip edilemeyeceğine ilişkin sorun ise, veriye müdahaleye yönelik fiillerin cezalandırılmasında iki farklı yaklaşımın esas alınmasına yol açmıştır. Birinci yaklaşım, genel olarak ekonomik değer taşıyan verinin mal / eşya olarak kabul edilmesi şeklinde olup bu haliyle genel olarak kıta Avrupasında ve Türk Ceza Hukukunda mala zarar verme suçunun konusunun maddi varlığı olan taşınır veya taşınmaz mal olması şartından uzaklaşmaktadır⁸. Diğer yaklaşım ise, veriye müda-

⁷SIEBER, s. 77.

⁸Enformasyonun bilişim sistemleri içerisinde temsil edici işlevi olan veriye müdahale özellikle verinin müdahalelerden korunması isteği ise öncelikli olarak, yukarıda ifade edildiği üzere günümüzde yaygın olarak enformasyon ya da bilişim toplumu olarak ifade edilen dönüşüm içerisinde verinin içerdiği enformasyonun başlı başına bir ekonomik değer olarak ortaya çıktığı görüşüne işaret etmekte ve ekonomik değere sahip veri saklandığı aygıtın işlevinden bağımsız olarak bir değer ifade etmektedir.

halenin verinin saklandığı diğer bir ifade ile bulunduğu mala yönelik bir zarar verme fiili olduğudur. Burada verinin saklandığı maddi mal esas alınarak, veriye müdahale ile verinin saklandığı malın işlevine müdahale edilmiş olduğu vurgulanmaktadır.

Bu doğrultuda ABD’de özellikle federe devletlerin (eyaletlerin) ceza mevzuatlarında genel olarak ekonomik değeri olan veri, mal olarak kabul edilmiş ve veriye müdahale de verinin mal olarak kabul edilmesi merkezinde düzenlenmiştir. Bu doğrultuda, sisteme ve veriye müdahale mala zarar verme kapsamında ele alınmış bunlara müdahale malvarlığına karşı suçlar olarak düzenlenmiştir.

İkinci yaklaşımda ise, verinin kendisi mala zarar verme suçu kapsamında suçun konusunu oluşturabilecek bir mal olarak kabul edilmemektedir. Burada, veriye yönelik müdahale, doğrudan mala zarar verme olarak kabul edilmemiş, sorun verinin saklandığı mal esas alınarak ele alınmıştır. Söz konusu yaklaşıma göre, veriye müdahale, verinin saklandığı mal, içerdiği veri ile birlikte bir işleve sahip olup veriye müdahale sonucunda bu işleve zarar verilmekte bu haliyle mala zarar verme söz konusu olmaktadır. Bu durumda, veriye müdahaleye ilişkin özel düzenleme yapılması bu duruma ilişkin bir açıklık getirilmesi amacını taşımaktadır⁹. Aynı yaklaşım, sisteme müdahale bakımından geçerli olup, her ne kadar sistemin yazılım unsuruna yönelik müdahale söz konusu olsa da, burada, sistemin işlevini yerine getirememesi söz konusu olduğundan, mala zarar verme suçunun olduğu söylenebilir.

Yukarıda aktarılan hususlar topluca değerlendirildiğinde, sistem ve veriye müdahaleye ilişkin suç ya da suçların, genel olarak mala zarar verme suçuna ilişkin hükümlerin özellikle sistemin yazılım yönüne ve veriye müdahale bakımından uygulanabilir olup olmadığı noktasında ortaya çıkan tartışmalar ve söz konusu soruna açıklık getirme isteği noktasından hareketle ortaya çıktığı görülmektedir. Bu haliyle de sisteme ve veriye müdahale genel olarak mala zarar verme kapsamında değerlendirilmektedir. Söz konusu fiillerin mala zarar verme kapsamında değerlendirilmiş olması, bu yöndeki fiillerin esas alındığı suçların hukuki konusu bakımından da bir işleve sahiptir.

Bu açıdan değerlendirildiğinde, ister ABD de federe devletlerde kabul edildiği şekliyle veri mal olarak kabul edilsin isterse verinin saklandığı malın işlevi ya da sistemin işleyişi esas alınarak soruna yaklaşılsın, mala zarar verme kapsamındaki fiiller söz konusu olmakta bu haliyle de malvarlığının korunması amaçlanmaktadır. Sisteme ve veriye müdahale fiillerine ilişkin suç, mala zarar verme suçu ile aynı hukuki konuya sahiptir.

Türk Ceza Kanununda Düzenlenen Bilişim Sistemine ve Veriye Müdahale Suçunun Hukuki Konusu

Yukarıda sisteme ve veriye müdahalenin hukuki konusu tartışılırken, bu fiillerin ayrıca suç olarak düzenlenmesinin nedenlerinden hareket edilmiş, bu kapsamda mala zarar verme suçunun unsurunda ve kapsamında ortaya çıkan tartışmalar bu suçun hukuki konusunun saptanmasında esas alındığı belirtilmişti.

TCK’nin gerekçesi incelendiğinde de sisteme ve veriye yönelik müdahale fiillerinin mala zarar verme suçuna göre özel bir düzenlemeye tabi tutulduğunun belirtildiği görülmektedir. Sisteme ve veriye müdahale ile ilgili olarak madde gerekçesinde “...sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlevini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkra seçilmiş hareketli bir suç meydana getirilmiştir.” denmektedir.

⁹ Aktaran, SIEBER, s. 91–92

TCK'nin 244. maddesinin 1. ve ikinci fıkralarında düzenlenen “*sistem ve veriye müdahale*” suçunun da mala zarar verme suçu ile bağlantılı olarak incelendiği ve sisteme ve veriye zarar verme fiillerinin ayrıca özel olarak düzenlendiği yazarlarca da kabul edilmektedir. Bu doğrultuda 5237 Sayılı TCK ve 765 Sayılı TCK bakımından da sistem ve veriye müdahalenin genel olarak mala zarar verme suçu kapsamında değerlendirildiği ve 765 Sayılı Kanunun 525/b 1. fıkrasında ve TCK'nin 244 1 ve 2. fıkralarında düzenlenen sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olarak genel kabul gördüğü görülmektedir.

Sisteme ve veriye müdahalenin mala zarar verme suçunun özel şekli olduğu kabulü, aynı zamanda Türk Ceza Hukukunda da sisteme ve veriye müdahalenin hukuki konusu ile mala zarar vermenin hukuki konusunun birbirine paralel olduğu sonucuna götürebilmektedir.

Suçun Maddi Unsuru

Sistemin İşleyişini Engelleme ve Bozma

Genel Olarak

Sistemin işleyişini engelleme ve bozma TCK'nin 244. maddesinin 1. fıkrasında, “*Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*” şeklinde düzenlenmiştir. 244. maddenin birinci fıkrasında suçun unsurunu oluşturan seçimlik hareketler “*bilişim sisteminin işleyişinin engellenmesi*” ve “*sistemin işleyişinin bozulması*”dır. Maddede yer aldığı şekliyle, bilişim sisteminin işleyişi genel olarak veri işleme faaliyeti anlamına gelmekte olup bu haliyle fıkarda veri işleme faaliyetinin engellenmesi ya da bozulması düzenlenmiştir.

Kanunda, engellemenin ve bozmanın tanımına yer verilmemiştir. Türk Dil Kurumu Sözlüğünde “*engellemek*”, “*bir şeyin gerçekleşmesini veya yapılmasını önlemek*”; “*bozmak*” ise, “*bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek*” olarak tanımlanmaktadır. Bu kapsamda bilişim sisteminin işleyişinin engellenmesi sistem aracılığıyla veri işleme faaliyetinin gerçekleştirilmesinin engellenmesi, bilişim sisteminin bozulması ise sistemin veri işleme faaliyetini yapamayacak hale getirilmesi olarak tanımlanabilir.

Nitekim, yazarlar tarafından sistemin işleyişinin engellenmesinin sistemin çeşitli yönleriyle sürekli ya da geçici olarak iş görmesinin engellenmesi anlamına geldiği, sisteme her türlü müdahalenin bu kapsamda değerlendirilmesi gerektiği ifade edilmiştir¹¹. Sistemin tamamen çalışamaz hale gelmesi¹², sistemin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması¹³, haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılmasının¹⁴ sistemin işleyişini bozma anlamına geleceği ifade edilmiştir¹⁵.

¹⁰TCK'nin 244. maddesinde düzenlenen sisteme ve veriye zarar verme suçunun mala zarar verme suçunun özel bir şekli olduğu hakkında ayrıca bkz. İnci BİÇKİN, Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları, Yargıtay Dergisi, C.32, Ocak – Nisan 2006, Sayı 1-2, s. 153. KARAGÜLMEZ, s. 187, KURT, s. 161.

¹¹MERAN, s. 371; Aynı yönde DÜLGER, s. 234, KARAGÜLMEZ, s. 188.

Kurt, bilişim sisteminin engellenmesi halinde sistemin bozulmasının söz konusu olmayıp normalde yerine getirdiği fonksiyonları ifa etmesinin engellendiğini ifade etmektedir. KURT, s. 164.

¹²KURT, s. 164.

¹³MERAN, s. 371.

¹⁴KARAGÜLMEZ, s. 188..

¹⁵Sistemin işleyişinin engellenmesi açısından kimi yazarlarca sistemin elektriğinin kesilmesi durumunda da sistemin işleyişinin engel olma kapsamında değerlendirilebileceği ifade edilmiştir. Bkz. YAZICIOĞLU, Bilgisayar Suçları, s. 263. MERAN, s. 371. Mala zarar verme suçunda belirtildiği şekliyle mala zarar verilmiş olması nedeniyle başkasına zarar verme söz konusu olmakta, bu açıdan elektriğin kesilmesi suretiyle makinelerin işlemesinin engellenmesi örneğinde olduğu gibi doğrudan mala yönelik olmayan fiiller mala zarar verme kapsamında değerlendirilmemektedir. Bkz. TOROSLU, Ceza Hukuku Özel Kısım, s. 156.

Mala Zarar Verme Suçu Açısından Sistemin İşleyişinin Engellenmesi ve Bozulması

244. maddenin 1. fıkrası incelendiğinde, Sibersuç sözleşmesinden farklı olarak, sisteme müdahalenin sistemin yazılımına yönelik olarak sisteme veri gönderilmesi, yerleştirilmesi gibi hareketlerle gerçekleştirileceğine ilişkin bir düzenlemeye yer verilmediği görülmektedir. Burada tespit edilmesi gereken, sistemin yazılımına veri aracılığıyla müdahale halinin mi yoksa her türlü müdahalenin mi bu kapsamda değerlendirilmesi gerektiğidir.

Bu hususun tespiti, 244. maddenin 1. fıkrasının yazılıma yönelik fiiller yanında, maddi varlığı yani donanımına yönelik, mala zarar verme suçunun konusunu oluşturabilecek fiilleri de kapsayan özel bir suç mu olduğu; yoksa bu fıkranın sadece sistemin yazılım unsuruna yönelik fiillerin esas alınarak mala zarar verme suçunu tamamlayan bir suç olarak düzenlendiğinin tespiti bakımından önem arz etmektedir.

Yukarıda belirtildiği üzere, sisteme müdahale, sistemin özellikle yazılım kısmına müdahale teşkil eden fiillerin cezalandırılabilmesine ilişkin mala zarar verme suçunun unsurlarına açıklık getirilmesi amacıyla çeşitli ülke kanunlarında düzenlenmeye başlanmıştır. Sisteme müdahalenin bu kapsamda düzenlenmesi ise, öncelikli olarak yazılıma müdahalenin esas alınması suretiyle sisteme müdahale fiillerinin düzenlenmesi sonucuna götürmüş olup Sibersuç Sözleşmesinin 5. maddesinde de bu husus somutlaştırılmıştır.

244. maddede ise, sadece sistemin işleyişinin engellenmesi veya bozulmasından bahsedilmiş olup bunun sistemin yazılımına veri aracılığıyla müdahale edilerek gerçekleştirileceğine ilişkin açık bir hükme yer verilmemiştir. Madde ile ilgili yaygın kabul, sisteme veri yoluyla müdahale yanında sistemin işleyişini engelleyen ya da bozan her türlü müdahalenin de bu madde kapsamında değerlendirilmesi yönündedir. Bunun yanında, 244. maddenin 1. fıkrasının sadece donanıma yönelik müdahaleleri kapsadığı görüşü de ileri sürülmüştür.

Bu fıkra kapsamında hangi tür fiillerin düzenlendiğinin belirlenmesi, TCK'de sisteme müdahalenin mala zarar verme suçu karşısındaki konumunun saptanması bakımından önemlidir. Eğer bu fıkranın yazılıma yönelik veri aracılığıyla gerçekleştirilen fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçu bakımından 244. maddenin birinci fıkrasında, suçun konusunun sistemin yazılım yönünün esas alındığı sonucuna varılabilecektir. Fakat bu fıkranın donanıma ve yazılıma yönelik fiilleri bir bütün olarak kapsadığı ya da donanıma yönelik fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçuna göre bilişim sistemini bir bütün olarak konu edinen özel hüküm olduğu sonucuna varılabilecektir.

244. maddenin 1. fıkrasında yer alan düzenlemenin mala zarar verme suçunu tamamlayıcı nitelikte bir düzenleme olduğu kabul edilecek olursa, geleneksel olarak taşınır ya da taşınmaz malın maddi varlığına yönelik hareketleri kapsayan mala zarar verme suçu ile sisteme müdahale bir bütün halinde uygulanabilecektir. Bu kapsamda, yazılıma yönelik hareketler sonucunda sistemin işleyişinin engellenmesi ya da bozulması halinde 244. maddenin 1. fıkrası, sistemin tahrip edilmesi, yok edilmesi gibi donanıma yönelik fiilleri kapsayan maddi varlığına yönelik fiillerde ise, TCK. nun 151. maddesi uygulama alanı bulacaktır. Bu durumda, sorun, cezaların miktarında ve 3. fıkroda düzenlenen ağırlatıcı nedenlerin uygulanmasında ortaya çıkmaktadır.

244. maddenin 1. fıkrasının 151. maddeye göre, hem donanıma hem de yazılıma ya da sadece donanıma yönelik fiilleri düzenleyen, özel bir suç olduğu kabul edilecek olursa, bu durumda mala zarar verme suçunun maddi unsurunu oluşturan hareketlerin bilişim sisteminin maddi unsurunu oluşturan donanıma yönelik gerçekleştirilmesi durumunda nasıl bir çözüme varılması gerektiği sorun olarak karşımıza çıkmaktadır. Bu durumda, sorun, mala zarar verme suçunun düzenlendiği 151. maddenin bilişim sistemleri bakımından uygulanıp uygulanamayacağıdır.

Bilişim sistemleri ve özellikle bilgisayar sistemleri esas alındığında bunların karakteristik özelliklerini donanım yani fiziksel yapıdan çok yazılım unsuru belirlemektedir. Bu açıdan, bir aygıt olarak bilgisayar sistemlerini diğer aygıtlardan ayıran unsur yazılım kapsamında belirli komutlar aracılığıyla veri işleme faaliyetini yapabilmesi ya da daha genel bir ifade ile işlem yapabilmesidir. Programlar aracılığıyla verinin işlenmesi ve de saklanması yani yazılım unsuru, sadece donanıma bağlı çalışan aygıtlardan farkını ortaya koymaktadır. Veri işleme faaliyeti olarak adlandırılan bu süreç ise kanunda bilişim sisteminin işleyişi olarak formüle edilmiştir.

Bilişim suçları arasında sisteme müdahalenin ayrı olarak düzenlenmesinin nedeni ise, veriye müdahale edilmesi suretiyle sistemin işleyişine müdahale edilebilmesidir. Bilişim sisteminin işleyişinden, yazılıma bağlı veri işleme faaliyeti olarak anlaşıldığına göre 244. maddenin birinci fıkrasında bilişim sisteminin işleyişine müdahale edilmesi düzenlenmesinin, bilişim sisteminin yazılım yönüne yani veri işleme faaliyetine işaret ettiği sonucuna götürebilmektedir. Bu kapsamda, sisteme yönelik fiziki müdahaleler yoluyla değil, sistemin yazılımına ve veriye müdahale ya da yazılımda değişiklik yapılması nedeniyle işleyişinin engellenmesi ya da bozulması halinin bu fıkra düzenlenmek istendiği söylenebilir.

Bu açıdan incelendiğinde, bilişim sistemi açısından, sistemin işleyişinin engellenmesi, bilişim sistemi olarak bilgisayarın çalışma yöntemi esas alınarak, çalışma yöntemine yani veri işleme faaliyetine müdahale edilmesi yoluyla sistemin çalışmasının engellenmesi olarak karşımıza çıkmaktadır. Nitekim, bir bilgisayar sistemi, işlemleri kapasitesine göre sıraya koyarak gerçekleştirir. Bir bilgisayar sisteminin işlem yapabilme sonuçlandırma hızı onun donanımsal yapısı ile bağlantılıdır. Bir sistemin belirli bir sürede yapabileceği işlem miktarını, yani sistemin işlem kapasitesinin zorlanması ise, bir süre sonra sistemin işlem yapamaz hale gelmesi ile sonuçlanır. Bu durumda, sistemin donanım ya da yazılımında bir bozukluk meydana gelmemesine rağmen kapasitesi üzerinde işlem talep edilmesi nedeniyle çalışamaz hale gelmektedir. Yani sistemin donanım ve yazılımı ile birlikte bütünlüğü ve gördüğü işlev bakımından bir bozukluk meydana gelmemekte fakat sistem belirli bir süre çalışmamaktadır.

Bu kapsamda değerlendirilebilecek müdahale yöntemleri birbirinden farklı olmalarına rağmen, şu örnekle konuyu açıklamak mümkündür. Bir web sayfasına erişim, genel olarak o web sayfasının barındırıldığı sunucu bilgisayara bağlantı kurulması ve sunucuda bulunan web sayfasının içeriğinin yer aldığı verinin kopyalanması anlamına gelmektedir. Web sayfasının yer aldığı sunucunun ise, belirli bir zaman diliminde ancak belirli sayıda bağlantıyı sağlayabilecek ve veri kopyalamasına izin verebilecek bir kapasiteye sahiptir. Birim zamandaki işlem kapasitesinin aşılmasını sağlayacak şekilde sisteme bağlantı kurulması ve veri kopyalanmasına ilişkin bilgisayar aracılığıyla gönderilen talep, yani veri iletilmesi, sistemin gönderilen taleplere cevap verememesi sonucunu doğurabilmektedir. Bu durum ise, belirli bir zaman diliminde sistemin öngörülen hizmeti verememesi, (örn. web sitesine erişilememesi) sonucunu doğurmaktadır.

Yukarıda verilen örnek dışında, sistem içerisindeki veriye müdahale edilmesi, veri yerleştirilmesi yoluyla da bu sistemin işleyişinin engellenmesi mümkün olmakla birlikte bu örnekte olduğu şekliyle sistem içerisindeki verinin ya da genel olarak yazılımın değiştirilmesi, yok edilmesi gibi durumlar gerçekleşmeden ya da sistem bozulmadan da sistemin çalışmaması söz konusu olabilmektedir. Nitekim, bu hususu da kapsamı amacıyla Siberaç Sözleşmesinde diğer hareketler yanında sistemin veri iletilmesi (transmitting) yoluyla işleyişinin engellenmesi de sisteme müdahalenin düzenlendiği 5. maddede yer almıştır.

Bilişim sisteminin işleyişinin bozulması ise, bu kapsamda sistemin yazılımını oluşturan işletim sistemi ya da diğer programlar gibi sistem içerisinde veri işleme faaliyetini ya da genel olarak işlem yapabilmesini sağlayan unsurlarına müdahale edilmesi sonucu, bunların işlem yapabilme kabiliyetinin tamamen ya da kısmen ortadan kaldırılması anlamındadır.

Bilindiği üzere, bir aygıtın fonksiyonunu yerine getirememesi bozulma kapsamında değerlendirilmekte ve bu haliyle bu tür bir fiil mala zarar verme suçunu oluşturabilmektedir. Bir bilişim sistemi ele alındığında sistemin iki farklı şekilde bozulması söz konusu olabilmektedir. Bu açıdan bir bilgisayarın işlemcisine, anakartına, sabit diski gibi donanımına ait unsurlara zarar verilmesi sonucu sistemin kullanılmasının önüne geçilebilmesi mümkündür. Bütün bu fiiller ise mala zarar verme suçu kapsamındadır.

Bunun yanında, bilişim sisteminin ve bu kapsamda ortaya çıkan bilgisayar sistemlerinin donanım ve yazılım unsuru ile birlikte çalışması bunlara yönelik fiiller ile de sistemin bozulması, yani tamamen ya da kısmen kullanılmasının önüne geçilmesi mümkün hale gelmiştir. Bu durumda, sistemin donanımında herhangi bir değişiklik meydana gelmemekle birlikte yazılım unsurunun bozulması nedeniyle sistem çalışmamaktadır.

Aslında burada, sistemin işleyişinin bozulmasına ilişkin bir hükmün yer almamış olması durumunda da sistemin işleyişinin bozulmasının mala zarar verme suçu kapsamında bozma olarak değerlendirilmesi mümkün olabilecektir. Çünkü bozma, sistemin fonksiyonu yerine getirememesi olarak anlaşıldığında bunun fiziksel bir müdahale ya da yazılıma müdahale yoluyla gerçekleştirilmesi arasında bir fark yoktur. Her ikisinde de özgülendiği amaç için kullanılamaması hali ortaya çıkmaktadır.

Bu durumda, sistemin donanımında, diğer bir ifadeyle maddi varlığında ve bütünlüğünde bir değişiklik olmasından ve bozulmasından bağımsız olarak sistemin çalışmaması durumunda, sistemin bozulmuş sayılıp sayılmayacağına ilişkin ortaya çıkabilecek tereddüdün giderilmesi amacıyla bu hükme yer verildiğini söylemek mümkündür. Bunun sonucunda, maddede ayrıca bilişim sisteminin işleyişinin bozulmasına yer verilmesi, bu madde ile fiziksel müdahalelerden çok yazılım ve veriye müdahale yoluyla sistemin bozulmasına ilişkin bir düzenleme yapıldığı sonucuna götürmektedir.

244. maddenin birinci fıkrasında düzenlenen fiillerin, yazılım unsuruna yönelik müdahalelerin veri aracılığıyla gerçekleştirilmesi şeklinde olduğunun kabulü, 2. fıkra da düzenlenen veriye müdahale ile sisteme müdahale arasındaki ilişkinin ise genel olarak geçitli suç şeklinde olması sonucunu doğurmaktadır. Aynı gerekçe söz konusu suçun mala zarar verme suçuna göre, sadece yazılım unsurunu kapsayan, özel bir norm olması sonucuna götürdüğü kanaatindeyiz.

Bilişim Sistemindeki Verileri Bozma, Yok Etme, Değiştirme, Verileri Başka Bir Yere Gönderme

Bu suç, TCK'nin 244. maddesinin ikinci fıkrasında ayrıca düzenlenmiş ve sisteme müdahaleye göre daha az ceza öngörülmüştür. 244. maddenin 2. 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.” hükmüne yer verilmiştir.

Maddede yer alan seçimlik hareketlerden ilki, bilişim sistemi içerisindeki “verinin yok edilmesi”dir. Bilişim sistemi içerisindeki verinin yok edilmesi, verinin varlığına son verilmesi, ortadan kaldırılması, hak sahibinin tekrar elde edemeyeceği ya da büyük güçlükler sonucu elde edebileceği şekilde tasarrufundan çıkarılması verinin yok edilmesi olarak tanımlanabilir.

Maddede yer alan diğer bir seçimlik hareket bilişim sisteminin içindeki “verinin bozulması”dır. Verinin bozulması verinin içeriğine ya da yapısına müdahale suretiyle verinin kısmen ya da tamamen kullanılamayacak hale gelmesi olarak tanımlanabilir. Burada özellikle verinin içeriğine müdahalenin var olan verinin içerdiği bilgi ya da enformasyona olumsuz müdahaleyi kapsadığını belirtmek gerekir.

Sistem içerisindeki veriye ve veri grubunu oluşturan programa virüs vb kötü amaçlı kodların sadece eklenmesi, bu anlamda veriyi bozma değil, verinin değiştirilmesi ya da sisteme veri yerleştirme olarak değerlendirilmelidir. Çünkü bu halde virüs gibi kötü amaçlı kodların öngörülen şekilde çalışmasından önceki bir aşamada var olan bir veriye eklenmesi söz konusu olup bu aşamada veri tamamen ya da kısmen kullanılamaz hale gelmemiştir.

Bu açıklama doğrultusunda, madde metninde yer alan verinin değiştirilmesi ise var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinalliğini ortadan kaldıran her türlü değişiklik olarak tanımlanabilir. Bu açıdan kötü amaçlı kodların veriye yerleştirilmesi bu kapsamda değerlendirilebilmektedir.

“Verinin erişilmez kılınması” ise, genel olarak verinin içerdiği bilgi ya da enformasyona müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup veri, içerik bakımından bütünlüğünü korumaktadır. Veri, ne yok edilmekte ne de bozulmakta, fakat verilere ulaşım için gereken işlem bağı koparılmaktadır. Veriye erişilmesi bakımından erişimin engellenmesinin geçici ya da daimi olması arasında bir fark yoktur.

Yargıtay 8. Ceza Dairesi 2019/3839 E., 2020/5418K.

Sanığın, mağdura ait MSN adresinin internet şifresini, onun bilgisi ve rızası dışında değiştirerek, mağdurun bilişim sistemindeki hesabına erişimini engellemesi biçiminde sübutu kabul edilen eyleminin, TCK’nın 244 /2. madde ve fıkrasında tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede yanlıya düşülerek, yasal ve yeterli olmayan yazılı gerekçelerle sanık hakkında TCK’nın 243 /3. madde ve fıkrasındaki bilişim sistemine girme suçundan mahkumiyet hükmü kurulması,

244. maddenin 2. fıkrasında düzenlenen hareketlerin sonuncusu ise, “sistem içerisindeki verinin başka bir yere gönderilmesi”dir. Verinin başka bir yere gönderilmesinin, verinin transferi, verinin kopyalanması olduğu ve kopyalandığı yerin önemsiz olduğu, ifade edilmiştir.

Yargıtay 8. Ceza Dairesi 2015/1581 E., 2016/9981 K.

Sanıkların, katılana ait bilgisayarlara uzaktan erişim yoluyla bağlanıp katılana ait sunuculara izinsiz olarak girilerek şifrelerinin değiştirildiği, kullanılmaz hale getirildiği ve katılana ait ROP programının tüm datalarının silindiği iddiası üzerine açılan davada; soruşturma aşamasında alınan 23.11.2009 tarihli inceleme raporuna göre katılanın bilgisayarlarında bulunan 4 adet klasörün silindiğinin tespit edildiği ancak uzaktan bağlantı yaptığı tespit edilen IP numarasının kime ait olduğuna, bu IP numarası ile bağlantı yapan bilgisayarın kim tarafından kullanıldığına, sanıkların, bilirkişi raporunda server ve client olarak belirlenen numaralara göre suç tarih ve saatinde katılana ait bilgisayarlardan kendi bilgisayarlarına bağlantı gerçekleştirildiğinin anlaşıldığını beyan etmeleri karşısında, bilirkişi raporunda belirlenen bağlantı IP lerine göre hangi yöne doğru bağlantı yapıldığına, klasörlerin bu bağlantı sırasında silinip silinmediğine, klasörlerin mahiyetine, katılanın sisteme girişinin engellenip engellenmediğine, şifrelerin değiştirilip değiştirilmediğine dair dosya içerisinde bir tespitin bulunmadığı anlaşılmakla; öncelikle katılanın bilgisayarlarına bağlantı yaptığı tespit edilen IP numarasının kime ait olduğunun tespiti ve gerektiğinde bağlantı yapan bilgisayar üzerinde inceleme yaptırılarak belirtilen hususlarda bilirkişi raporu alınması ile tüm deliller birlikte değerlendirilip sonucuna göre sanıkların hukuki durumlarının takdir ve tayini gerektiği gözetilmeden eksik araştırmayla yazılı şekilde hükümler kurulması,

Bu suça ilişkin özel bir düzenleme de Elektronik İmza Kanununda yer almaktadır. Özü itibariyle veriye müdahale teşkil eden fiiller elektronik imza ve sertifikaya ilişkin özel düzenleme yapma gereği olarak ayrıca düzenlenmiştir. Bu kapsamda Elektronik İmza Kanunun 16. maddesinde **“İmza oluşturma verilerinin izinsiz kullanımı”** suçu *“Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar. Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.”* hükmüne yer verilmiştir. Aynı Kanunun **Elektronik sertifikalarda¹⁶ sahtekârlık** başlıklı 17. maddesinde ise *“Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır. Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.”* hükmüne yer verilmiştir.

Her iki düzenleme de incelendiğinde özü itibariyle veriye müdahaleye ilişkin hareketlerin elektronik imza ve sertifika açısından önemli görülen yönlerinin düzenlenmesi şeklinde olduğu görülür. Bu haliyle veriye müdahale açısından özel hüküm niteliğinde olup elektronik imza ya da sertifika verilerine müdahale durumunda maddelerde sayılan hareketlerin (kopyalama, yeniden oluşturma, elde etme vs, taklit tahrif vs.) gerçekleştirilmesi durumunda Elektronik imza Kanununda düzenlenen bu suçlar uygulanma alanı bulur.

Suç Etki Eden Nedenler

244. maddenin 3. ve 4. fıkralarında suça etki eden nedenler açısından iki ağırlatıcı nedene yer verildiği görülmektedir. Bunlardan birincisi, 244. maddenin 1. ve 2 fıkrasında düzenlenen fiillerin bir kamu kurum ya da kuruluşuna ya da banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmesidir.

Son fıkra da yer alan hüküm ise, genel olarak bilişim ya da bilgisayar sistemleri aracılığıyla yarar sağlama fiillerinin cezalandırılmasına yönelik bir düzenlemedir. Bu düzenleme Bilgisayar dolandırıcılığı adı altında halihazırda bir çok ülke mevzuatında yer alan suça paralel bir hüküm içermektedir. Bu açıdan sorun bilgisayar sistemleri aracılığıyla, veriye ya da sisteme müdahale yoluyla yarar sağlanması halinde veri ya da program manipülasyonunun yani hileli bir takım hareketlerin söz konusu olması, lakin dolandırıcılık suçunun unsuru açısından bunun gerçek kişiye yönelik bir hile olmaması ve bu şekilde yarar sağlanması nedeniyle dolandırıcılık suçu kapsamında değerlendirilememesidir. Bu sorunu gidermek amacıyla da Sibersuç Sözleşmesinde de öngörüldüğü şekliyle özel bir düzenleme yapılması yoluna gidilmesi tercih edilmiştir.

Siber Suç Sözleşmesi Madde 8 - Bilgisayar ile Bağlantılı Dolandırıcılık

Taraflardan her bir, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, ir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezaî suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

¹⁶ Söz konusu Kanuna göre elektronik sertifika, imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder.

Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

- a. bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme;*
- b. bir bilgisayar sistemini işleyişine herhangi bir müdahalede bulunma.*

Uygulamada söz konusu hüküm ilk başlarda internet bankacılığını kullanmak suretiyle başkalarının hesaplarından hukuka aykırı olarak para transferi yapılması fiillerinde uygulanmış iken sonrasında Yargıtay Ceza Genel Kurulu'nun 2009/11-193 E., 2009/ 268 K. sayılı kararı ile söz konusu fiiller hırsızlık suçu kapsamında değerlendirilmeye başlanmıştır. Hali hazırda bu son fıkradaki düzenlemeye örnek olarak başkasının Bitcoin hesabından hukuka aykırı olarak Bitcoin transfer etme fiilleri gösterilebilir.

Bu hükmün yürürlükten kalkmış olan 765 sayılı TCK'de karşılığı olarak düzenlendiği ifade edilen 525b/1. maddesi söz konusu hükmün yürürlükte olduğu dönemlerde başkalarına ait banka ya da kredi kartlarının söz konusu kartları kullanılması fiillerine bilgileri otomatik işleme tabi tutan ATM cihazları ya da birer terminal niteliği taşıyan POS cihazlarının kullanılması nedeniyle uygulanmıştır. Bu fiillere yönelik olarak 5237 TCK'de özel düzenleme yapılması yoluna gidilmiş ve söz konusu fiiller 245. maddede özel olarak düzenlenmiştir.

Yasak Cihaz veya Programlar

Siber Suç Sözleşmesine uyum sürecinde TCK bağımsız bir suç olarak 245/A maddesinde düzenlenen bir suç olup söz konusu maddeye göre *“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.”*

Bu hüküm incelendiğinde korunan hukuki konu ya da hukuki değer açısından birçok suçun işlenmesine yönelik hazırlık hareketi olarak nitelendirilebilecek davranışların cezalandırılması yoluna gidilmesi ve bu kapsamda soyut tehlike suçu olarak düzenlenmesi nedeniyle belirsizliğin söz konusu olduğu ifade edilebilir. Nitekim TCK'nın 245/A maddesinde, bilgisayar programı, şifre veya güvenlik kodunun ya münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesi için yapılması ya da farklı bir amaçla yapılmış olmakla birlikte söz konusu suçları işlemeye yönelik sonradan uyarlanmış olması gerekmektedir.

Bu haliyle suçun oluşumu açısından özel kast, yani münhasıran bilişim alanında işlenen suçların veya bilişim sistemleri aracılığıyla işlenebilen diğer suçların işlenmesi için maddede sayılan hareketlerden bir ya da birkaçının gerçekleşmesi gerekmektedir. Haliyle örneğin test ya da bilimsel bir faaliyet kapsamında bu maddede sayılan hareketlerin yapılması manevi unsurunun oluşmamasından dolayı suç olmayacaktır.

Banka veya Kredi Kartlarının Kötüye Kullanılması

Genel Olarak

765 sayılı TCK döneminde başkasına ait banka ya da kredi kartlarının kullanılması ATM ya POS cihazlarının bilgileri işleme tabi tutan sistem olarak kabul edilmesi ve bu tür fiillerde bilgileri işleme tabi tutan sistem aracılığıyla yarar sağlandığı sonucuna varılmasına binaen adı 765 sayılı TCK'nin 525b/2. maddesinin uygulanması yoluna gidilmişti (YARGITAY CGK E. 2000/6-62 K. 2000/72 T. 11.4.2000). Söz konusu uygulama sonrasında 5237 Sayılı Türk Ceza Kanununda banka ve kredi kartlarının kötüye kullanılmasına ilişkin 245. maddede özel düzenleme yapılması yoluna gidilmiştir. Bunun yanında 5464 sayılı Banka ve Kredi Kartları Kanununda da 5237 sayılı TCK'ye ek yeni suçlar düzenlenmiştir.

Özellikle kredi kartlarının bilişim sistemlerinin kullanılmasından çok daha önce kullanılmaya başlanması karşısında kredi kartlarının bilişim alanında suçlar arasında değerlendirilmesine yol açan husus söz konusu kartlar açısından bir niteliksel etki olmaktan çok TCK açısından adı geçen maddenin uygulanmasından kaynaklanan bir sorun olarak gündeme gelmiştir. Bunun yanında, bu tür kartların elektronik ticaret alanında en yaygın ödeme aracı olarak kullanılıyor olması, bunların kötüye kullanılmasının bilişim suçları arasında anılmasının diğer bir sebebidir. Bu nedenle bu suçların bilişim suçları arasında değerlendirilmesi çok da yerinde olmamakla birlikte hem genel olarak elektronik ticarete yaygın olarak kullanılıyor olması hem de eski TCK'de uygulanacak normun tespiti açısından gündeme gelmesi ve nihayetinde 5237 sayılı TCK'de bilişim alanında suçlar arasında özel düzenleme yapılması nedeniyle aşağıda TCK'de düzenlenen suçlara kısaca değinilecektir.

Başkasına Ait Kartın Hukuka Aykırı Olarak Kullanılması

TCK'nin 245. maddesinin birinci fıkrasında *“Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.”* hükmüne yer verilmiştir.

5464 sayılı Kanunun 3. maddesinde banka ve kredi kartı tanımlanmıştır. Buna göre, “banka kartı,” *“Mevduat hesabı veya özel carî hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kartı”* ifade eder. “Kredi kartı” ise *“Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını,”* ifade eder.

TCK 245/2. maddesinin uygulanması açısından failin kartı ne şekilde ele geçirdiğinin önemi olmamaktadır. Bu kapsamda kartın hukuka uygun olarak ele geçirilmesi veya elde bulundurulması neticesinde kartın rıza dışı olarak kasten kullanılması durumunda suç oluşabilecektir. Bu nedenle kartın örneğin hırsızlık sonucu ele geçirilmesi, teslim edilen kuryenin kartı kullanması, kartın bulunması sonrasında rıza dışı kullanımı arasında fark bulunmamaktadır. Burada önemli olan husus kartın hukuka aykırı olarak kullanılması olup ele geçirme ya da elde bulundurma ayrı bir su teşkil ettiği durumda ayrıca söz konusu suçlardan dolayı da cezalandırılır.

Yargıtay CGK, 30.04.2019 tarihli ve 172-361 Sayılı Karar

“Ayrıntılarına Ceza Genel Kurulunun 30.03.2010 tarihli ve 17-65 sayılı kararında da yer verildiği gibi; 5237 sayılı TCK’nın 245/1. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun kanundaki düzenleniş şekli göz önüne alındığında bileşik suç olarak düzenlenmediği görülmektedir. Banka veya kredi kartının kötüye kullanılması suçu ile birlikte oluşabilecek diğer suçlara kanunda öngörülen ceza miktarları da, bu suçun bileşik suç olarak düzenlenmediğini açıkça ortaya koymaktadır. Bu nedenle, banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma, dolandırıcılık gibi suçlar ile banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralı uygulanarak fail her bir suçtan ayrı ayrı cezalandırılmalıdır. Banka veya kredi kartının kanunlarda suç olarak düzenlenen eylemlerle ele geçirilmesi ve şartların varlığı hâlinde, TCK’nın 245. maddesinin birinci fıkrasındaki suçun yanında ayrıca hırsızlık, dolandırıcılık ya da yağma gibi suç oluşabileceği kabul edilmelidir...”

Suçun oluşumu için kart hamilinin rızasının bulunmaması gerekir. Bu kapsamda kart hamilinin kartın çalınması ya kayıp başvurusunda bulunması sonrasında rızaen kullanması ya da başkalarına kullandırması durumunda ise 5464 sayılı Banka ve Kredi Kartları Kanunun 37/1. maddesinde düzenlenen suç kapsamında değerlendirilmesi gerekir. Söz konusu hükme göre, *“Banka kartı veya kredi kartını kaybettiği ya da çaldığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar bir yıldan üç yıla kadar hapis ve ikibin güne kadar adli para cezası ile cezalandırılırlar.”*

TCK’nın 245. maddesinin 1. fıkrasında yer alan düzenleme açısından aynı Kanunda şahsi cezasızlık sebepleri ve etkin pişmanlık hali düzenlenmiştir. TCK’nın 245/1. maddesine göre, *“Birinci fıkra da yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz. (5) (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.”*

Söz konusu hükmün maddeye konularak malvarlığına karşı suçlar ile ilişkinin de kurulması karşısında bu suçun esasen malvarlığına karşı suç olarak kabul edilerek korunan hukuki değer kişinin malvarlığı üzerindeki hakları olduğu sonucuna ulaşılabilir.

Sahte Banka veya Kredi Kartı Üretme, Satma, Devretme, Satın Alma veya Kabul Etme

TCK’nın 245/2. maddesinde *“Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.”* hükmüne yer verilerek sahte kredi kartı ya da banka kartlarına yönelik olarak zararın oluşmasını esas almayan tehlike suçu niteliğinde bir düzenlemeye yer verilmiştir.

Söz konusu suçun oluşabilmesi açısından öncelikli olarak başkalarının banka hesaplarıyla ilişkilendirilmiş bir banka ya da kredi kartının sahte olarak oluşturulması gerekmektedir. Bu kapsamda kart başvurusunda sözleşme ve eki belgelerde sahtecilik yapılmış olması durumunda 5464 sayılı Banka ve Kredi Kartları Kanunun 37/2. maddesi uygulanır. Söz konusu hükme göre *“Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler.”* Yargıtay kararlarında bu iki hükmün uygulanması açısından sahte belge ibraz suretiyle başvurulma aşamasında 37/2’nin uygulama alanı bulacağını kartın üretilmiş olması durumunda TCK’nın 245/2. maddesinin uygulanma alanı bulacağı sonucuna ulaşılmıştır (Örnek karar için bkz. Yargıtay 8. Ceza Dairesi 2019/19765 E., 2020/578 K.).

245/2. maddesinde suç olarak düzenlenen hareketler sahte kartın üretilmesi (oluşturma, yaratma, kopyalayarak oluşturma), devredilmesi (bir malın mülkiyetini, ya da mal üzerindeki hakkı başkasına geçirmek), satın alma, (belirlenen fiyatın ödenerek mal edinme), kabul etme (sunulan bir şeyi alma) olarak tanımlanmıştır. Bu haliyle kartın kullanılması suretiyle yarar sağlanması ya da zarar verilmesi şartı aranmamakla bir tehlike suçu olarak düzenlenmiştir. Bu hükümle korunan değer in sahtecilik suçlarıyla aynı yönde banka ve kredi kartlarına duyulan güven ilişkisi olduğu söylenebilir.

Sahte Banka veya Kredi Kartının Kullanılması Suretiyle Yarar Sağlanması

TCK 245/2 maddesinde tehlike suçu olarak düzenlenen suça ilişkin olarak sahte kartın kullanılması şartını aramamaktaydı. Bu düzenleme ile sahte olarak oluşturulmuş olan kartın ayrıca kullanılarak yarar sağlanması hali düzenlenmiştir. Burada yararın ekonomik bir yarar olacağı söylenebilir.

Yargıtay kararlarına göre, bu husus tartışmalı olmakla, 245/2 madde kapsamında kartta sahtecilik fiilinin gerçekleştirilmesine binaen kartların kullanılmış olması durumunda fail hem 245/2 hem de 245/3'ten cezalandırılması gerektiği sonucuna ulaşılmaktadır (Örnek karar için bkz. Yargıtay 8. Ceza Dairesi 2013/7794 E., 2014 / 13790 K.; Yargıtay 11. Ceza Dairesi 2012/2110 E., 2013/9973 K.).

Kişisel Verilerin Korunmasına İlişkin Suçlar

Genel Olarak

Bilindiği üzere, özel hayatın korunması kimi yönleri açısından cezai düzenlemelerin konusunu da oluşturmuştur. Nitekim, 765 Sayılı TCK'de özel hayatın gizliliği kapsamında değerlendirilen konut dokunulmazlığı ile haberleşmenin gizliliğine ilişkin suçlar yer almaktaydı. 765 Sayılı TCK'nin 193. vd. maddelerinde yer alan *“mesken masuniyeti aleyhine cürümler”*, 195. vd. maddelerinde yer alan genel olarak haberleşmenin gizliliğini korumaya yönelik olarak karşımıza çıkan *“Sırrın Masuniyeti Aleyhine Cürümler”* 765 Sayılı TCK'de özel hayatın gizliliğinin korunmasına ilişkin suçlar olarak düzenlenmekteydi.

5237 Sayılı TCK'de ise, hem özel hayatın gizliliği genel olarak, hem de özel hayatın gizliliğinin çeşitli yönleri ayrıca özel olarak düzenlenmiştir. 5237 Sayılı TCK'de özel hayatın gizliliğine ilişkin suçlar, genel olarak, *“Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar”* başlıklı 9. bölümünde 132. vd. maddelerinde düzenlenmiştir. Kanunun 132. maddesinde *“haberleşmenin gizliliğini ihlal”*, 133. maddesinde *“kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”*, 134. maddesinde *“özel hayatın gizliliğini ihlal”*, suçlarına yer verilmiştir.

765 Sayılı TCK'den farklı olarak, TCK'de, ayrıca kişisel verilerin korunmasına ilişkin kimi suçlara yer verilmiştir. Kanunun 135. maddesinde, *“kişisel verilerin kaydedilmesi”* 136. maddesinde, *“verileri hukuka aykırı olarak verme veya ele geçirme”*, 138. maddesinde ise, *“verileri yok etmeme”* suçları düzenlenmiştir. Kişisel verilerin korunmasına ilişkin suçlara ilişkin olarak 137. maddede, kişisel verilerin korunmasına ilişkin 135 ve 136. maddelerde düzenlenen suçların *“kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle”* ve *“Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle”* işlenmesi halinde verilecek cezanın yarı oranında arttırılacağı öngörülmüştür.

Bu hususlar doğrultusunda, öncelikli olarak TCK'nin 135 vd. maddelerinde düzenlenen suçların hukuki konusu olarak ortaya çıkan özel hayatın gizliliği esas alınırken bu hususu Anayasanın özel hayatın gizliliğine ilişkin 20. maddesinde 2010 yılında yapılan değişiklikle açık bir hükme bağlanmıştır. Bu haliyle bu düzenlemelerde yer alan suçlarla korunan hukuki değer genel olarak özel hayatın gizliliği kapsamında değerlendirilen kişisel verilerin korunması hakkı olup Anayasanın 20 maddesinin son fıkrasına göre, *“(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hak-*

kına 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.” Bu düzenleme ile bağlantılı olarak 2016 yılında 6698 sayılı Kişisel Verilerin Korunması Kanunu kabul edilerek hükümleri Kanunda belirtilen tarihlerde yürürlüğe girmiştir.

Söz konusu Kanun incelendiğinde kişisel verilerin işlenmesine ilişkin genel olarak usul ve esasların belirlendiği görülür. Kanunda “kişisel veri”, “Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak tanımlanmıştır. Kanuna göre “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 işlemi” ifade eder

Kişisel verilerin işlenmesi açısından genel olarak uyulması gereken ilkeler ise Kanunun 4. maddesinde genel olarak düzenlenmiştir. Buna göre kişisel veriler işlenmesinde “a) Hukuka ve dürüstlük kurallarına uygun olma. b) Doğru ve gerektiğinde güncel olma. c) Belirli, açık ve meşru amaçlar için işlenme. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.” ilkelerine uyulması zorunludur.

Kanunda belirtilen sorumluluk ve yükümlülüklerin yerine getirilmemesi açısından ise ikili bir yaptırım yoluna gidilmiş olup bir kısım fiiller açısından Kanunun 18. maddesinde idari yaptırım içeren kabahatler olarak düzenlenmiştir. Söz konusu maddede Kanunda düzenlenmiş bulunan aydınlatma yükümlülüğünün ihlali, veri güvenliğine ilişkin yükümlülükleri yerine getirilmemesi, Kurul tarafından verilen kararları yerine getirilmemesi, ve veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi fiilleri kabahat olarak düzenlenmiştir.

Ceza hukuku anlamında suç oluşturan fiiller açısından ise Kanunun 17. maddesinde “(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140 ıncı madde hükümleri uygulanır. (2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.” hükmüne yer verilerek TCK’nin ilgili maddelerinin uygulanacağı belirtilmiştir.

Türk Ceza Kanunun 135 vd. maddelerindeki suçlar incelendiğinde, genel olarak kişisel verilerin işlenmesine ilişkin ilkeler olarak ifade edilen, hem ulusal hem de uluslararası düzenlemelerde çeşitli şekillerde yer verilen kişisel verilerin işlenmesine ilişkin usul ve esasları esas alındığı görülmektedir. Bu açıdan, TCK’nin 135 vd. maddelerinde, dürüst ve hukuka uygun toplama ve işleme, amaçla bağlılık ilkeleri başlığı altında incelenen kişisel verilerin işlenmesine ilişkin usul ve esasların belirli yönleriyle konu edildiği görülmektedir. Nitekim, 135. maddede suçun maddi unsuru olarak kişisel verinin kaydedilmesi, 136. maddede düzenlenen suçun seçimlik hareketlerini oluşturan, kişisel verinin ele geçirilmesi, verinin başkasına verilmesi ve yayılması, dürüst ve hukuka uygun toplama ve işleme ayrıca amaçla bağlılık ilkesinin bir görünümü olarak karşımıza çıkmaktadır. 138. maddede düzenlenen verinin yok edilmemesi ise özellikle amaçla bağlılık ilkesi ile ilişkisi bulunmaktadır.

Kişisel Verilerin Kaydedilmesi Suçu

TCK'nin kişisel verilerin korunmasına ilişkin ilk suç kişisel verilerin hukuka aykırı olarak kaydedilmesi suçudur. TCK'nin 135. maddesinde, *“(1) Hukuka aykırı olarak kişi-sel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir... Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.”* hükmüne yer verilmiştir.

135. maddede düzenlenen suçun maddi unsuru, kişisel verilerin kaydedilmesidir. Kanunda kaydetmenin ne anlama geldiğine ilişkin bir tanıma yer verilmemiştir. TDK sözlüğüne göre *“kaydetme”* genel olarak yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; sesi veya resmi manyetik bant üzerine geçirmek; bilişim açısından ise, elektronik veya sayısal araçlarda bilgiyi korumaya almak anlamlarını taşımaktadır. Bu kapsamda, genel olarak, her türlü kişisel verinin hukuka aykırı olarak kaydı, 135. maddede düzenlenen suç oluşturur. Bunun yanında 135. maddenin ikinci fıkrasında ikili bir ayırıma gidilmiş *“kişilerin siyasi, felsefi veya dini görüşlerine, ırkı kökenlerine”, “hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına”* ilişkin bilgilerin kişisel veri olarak kaydedilmesi durumunda düzenlemenin son haliyle ceza daha da artırılmaktadır.

Verileri Hukuka Aykırı Olarak Verme, Yayma veya Ele Geçirme Suçu

Kişisel verilerin korunmasına ilişkin olarak TCK'nin 136. maddesinde yer alan diğer bir suç, şu şekilde düzenlenmiştir: *“(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır... (2) 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.”*

Maddede kişinin kendisi hakkındaki verileri kontrol edebilmesi bakımından, ilgili kişi hakkındaki verinin, sadece rıza gösterdiği ya da hukuken kişisel veri işlemeye yetkili kişilerin elinde bulunması ve yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi için kişisel verinin başkasına verilmesi, yayılması ve ele geçirilmesi şeklinde seçimlik hareketli bir suç olarak düzenlenmiştir. TCK'nin 136. maddesinde düzenlenen suç, genel olarak hangi tür verilerin, kimler tarafından ne şekilde kaydedilebileceğine ilişkin bir koruma sağlarken, bu maddede düzenlenen suç, kişisel verinin yetkisiz üçüncü kişilerin eline geçmesinin önlenmesi ya da kişisel verinin içeriğinin genel olarak öğrenilmesinin engellenmesi açısından, kişisel verilerin işlenmesi süreci içerisinde, kişi bakımından bir koruma getirmektedir. Aynı şekilde,

Yargıtay 19. Ceza Dairesi 2019/28161 E., 2020/13552 K.,

“...TCK'nun 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 gerektiğinin belirtilmesi karşısında, her türlü kişisel verinin hukuka aykırı olarak başkasına verilmesi, yayılması ve ele geçirilmesi fiillerinin kanunun 136. maddesindeki suçu oluşturduğu kabul edilmelidir.”

kişisel verilerin korunması genel olarak kişinin kendisi hakkındaki verileri kontrol hakkı olarak tanımlandığında, ilgili kişinin kendisi ile ilgili verileri kimlerin işlediğini bilebilmesi veya öngörebilmesi bakımından 136. maddede düzenlenen suç önem taşımaktadır.

Maddede yer alan seçimlik hareketlerden, kişisel verinin başkasına verilmesi ve yayılması, bir yönüyle kişisel veri işlemeye yetkili olan kişilere yönelik verinin işlenmesine ilişkin bir iç sınırı oluşturmaktadır. Kişisel veri işlemeye yetkisi olan kişilerin hukuka uygun olarak kişisel verileri kaydetmesi halinde de söz konusu veriler üzerindeki tasarrufu, verinin üçüncü kişilere verilmesi ya da verilerin içeriğinin birçok kişi tarafından öğrenebilecek şekilde başkalarının bilgisine sunması yani yayması bakımından sınırlandırılmaktadır. Bu haliyle, kişisel verilerin kullanımının sınırlandırılması ve istenmeyen ya da yetkili olmayan ifşalardan korunması istenmektedir.

Maddede düzenlenen suçun maddi unsurunu oluşturan seçimlik hareketlerden bir diğeri, verinin yetkisiz üçüncü kişiler tarafından ele geçirilmesidir. Bu hüküm bakımından, kişisel verilerin yetkisiz üçüncü kişiler tarafından elde edilmesinin engellenmesine yönelik bir işleve sahiptir. 135. maddede genel olarak kişisel verilerin toplanmasından bahsedilmesi karşısında, bu maddede düzenlenen kişisel verinin ele geçirilmesi, kaydedilmiş olan kişisel verinin hukuka aykırı olarak elde edilmesi anlamına gelmektedir.

Yargıtay 8. Ceza Dairesi 2019 / 23499 E., 2020 / 17559 K.

“...Bölge Müdürlüğü önündeki ... Bankası ATM'sine kart kopyalama düzeneği yerleştirilmesinden sökülmesi anına kadar her hangi bir kart hamiline ait banka kartı veya kredi kartı bilgilerini kopyalama suretiyle elde edip etmediği konusunda Bankalararası Kart Merkezi tarafından rapor aldırılıp sonucuna göre; kart hamillerine ait kart bilgileri kopyalanarak bir kart oluşturulmaması halinde ele geçirilen kopyalama cihazında bilgi bulunması halinde eyleminin mağdur sayısına TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme, bulunmaması halinde ise kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı ve suçun mağdurunun kart bilgilerinin sahibi olan banka müşterileri olacağı cihetle; manyetik şerit bilgilerinin kopyalanarak sahte bir banka veya kredi kartı üretilmesi halinde kartları gerçeğe aykırı olarak üretilen banka sayısına TCK'nın 245/2. maddesi ile aynı bankanın birden fazla kartının değişik zamanlarda kopyalanması durumunda 43. maddesinin, sanığın bankanın ATM cihazlarına yerleştirdiği düzeneğe, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışması halinde ise eyleminin TCK'nın 136, 35. ve 43/2. maddelerinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırmayla yazılı şekilde hüküm kurulması...”

Verileri Yok Etmeme Suçu

Kişisel verilerin korunmasına ilişkin olarak TCK'de yer alan üçüncü suç kişisel verilerin yok edilmesidir. Verileri yok etmeme başlığını taşıyan 138. maddeye göre “(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir... (2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır.” Kişisel Verilen Korunması Kanunun 17/2. maddesi de söz konusu Kanuna tabi kişisel veri işleme faaliyetleri açısından suçun unsurlarını genişletmiştir. Buna göre: “(2) Bu Kanunun 7 nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hâle getirmeyenler 5237 sayılı Kanunun 138 inci maddesine göre cezalandırılır.” Kanunun 7. maddesinde ise “MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. (2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır. (3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.” hükmüne yer verilmiştir.

Kişisel verilerin kaydedilmesinin ve işlenmesinin kişisel verilerin korunmasına ilişkin hükümlerle ayrıntılı olarak düzenlenmesi ve bu açıdan kişisel verilerin işlenmesi, kişisel verilerin korunması hakkı kapsamında istisnai bir durum olması, beraberinde kişisel veriye ihtiyaç duyulmadığı durumlarda verinin yok edilmesi ya da ilgili kişiyle olan doğrudan ya da dolaylı bağlantısının ortadan kaldırılmasını gündeme getirmektedir.

Kişisel verinin yok edilmesi yukarıda belirtildiği üzere, verinin tamamen ortadan kaldırılması anlamına gelebileceği gibi bunun yanında verinin içerdiği bilgi ya da enformasyon ile ilgili kişinin arasındaki bağlantının ortadan kaldırılması şeklinde de gerçekleştirilebilir. Bu ikinci husus, özellikle bilimsel ve istatistikî amaçlarla kişisel verinin işlenmesinde önem arz etmektedir. Saklama zorunluluğunun ortadan kalkması sonrasında, bu tür faaliyetler için verinin gerekli olduğunda kullanılabilmesi açısından verinin yok edilmesi tamamen ortadan kaldırma yanında ilgili kişi ile bağlantısının kurulamayacak hale getirilmesi olarak anlaşılmalıdır. Bu son durumda, verinin ilgili kişi ile doğrudan ya da dolaylı bir biçimde irtibat sağlanamayacak hale getirilmesi sonucunda kişisel verilerin korunmasına ilişkin düzenlemelerin amacını oluşturan veri/enformasyon mahremiyeti kapsamında özel hayatın gizliliğinin korunmasına ilişkin bir beklenti söz konusu olmamaktadır. Bu durumda, verinin içerdiği bilgi ya da veri herhangi bir konu hakkında genel bir bilgi olarak kalmakta ve ancak istatistiki ya da bilimsel bir anlam taşıyabilmektedir.

TCK'nin 138. maddesinde, amacın ortadan kalkması ya da amacın gerçekleştirilmesi sonucunda kişisel verilerin yok edilmesi hususuna yer verilmemiş, bunun yerine kanunların belirlediği sürelerin geçmiş olması sonucunda verinin yok edilmemesi esas alınmış ve ihmali bir suç olarak düzenlenmiştir. Bu son husus Kişisel Verilerin Korunması Hakkında Kanunun 17. maddesinde düzenlenerek adı geçen Kanun kapsamında kalan kişisel veri işleme faaliyeti açısından suç kapsamına alınmıştır.

BÖLÜM ÖZETİ

Günümüzde bilgi ve enformasyonun etkin olarak işlenmesinde teknik açıdan belki de en önemli yere sahip olan bilişim teknolojisinin gelişimidir. Bilişim teknolojisi, özellikle modern bilgisayarın 20. yüzyılın ikinci yarısından itibaren etkisini hissettirmeye başlayan sosyo-ekonomik dönüşümünün içinde şekillenerek toplumsal ilişki ve kurumları çeşitli yönleriyle etkilemeye başlamıştır. Toplumsal bir kurum olan hukuk da birçok yönüyle söz konusu gelişimden etkilenmiştir. Bu bağlamda bilişim suçları, bilgisayar suçları gibi birçok ad altında incelenen suçlar, dönüşümün ceza hukukuna niceliksel ve niteliksel etkisini oluşturmaktadır.

Ceza hukuku açısından sorunun bir yönü bilgi ve enformasyonun, korunmasıyla ilgilidir. Sorunun diğer bir yönü ise sayısallaşma olarak adlandırılan durum ile ilgilidir. Söz konusu sorunlara ilişkin olarak ceza hukukunda tartışmaların merkezini oluşturan hususlar, hangi değer korunduğu ve bununla bağlantılı olarak bu değerlere yönelik saldırıları ifade eden hangi tür fiillerin suç olarak düzenlenmesi gerektiğidir. Bilişim suçları olarak adlandırılan suçlarda, öncelikli olarak ceza müeyyidesiyle koruma altına alınan değer ne olduğunun tespiti önemlidir. Bu husus, bir yandan da korumanın amacını ve meşruiyetini göstermektedir. Hâliyle bu da suçun hukuki konusunun ve bununla bağlantılı olarak özellikle suç olarak düzenlenecek fiillerin belirlenmesine yönelmeyi gerekli kılmaktadır.

Farklı nitelikteki birçok suçun bilişim suçları adı altında gündeme gelmesi, bilişim suçlarının incelenmesine ilişkin belirli bir sınırlandırılmaya gidilmesi zorunluluğunu doğurmaktadır. Bu nedenle bu bölümde 5237 Sayılı Türk Ceza Kanunu'nun 243. ve 244. maddelerinde düzenlenen suçlar ağırlıklı olarak incelenmiştir. Banka ve kredi kartlarının kötüye kullanılması suçu ile Elektronik İmza Kanununda düzenlenen suçlar da ilgisi olduğu ölçüde ele alınmıştır. Sosyo-ekonomik dönüşüm sürecinde bilişim sistemlerinin kullanımının diğer önemli bir etkisi olarak ortaya çıkan kişisel verilerin korunmasına ilişkin Türk Ceza Kanunu'nun 135 ve diğer maddelerinde düzenlenen suçlar da yine niteliksel bir etki olarak inceleme konusu yapılmıştır.

GÖZDEN GEÇİRELİM

Yetkisiz erişim suçundan bahsedilebilmesi için sisteme erişim açısından en azından
..... yetkisinin elde edilmiş olması gerekir.

Veriye müdahale suçunda sistem üzerineyetkisinin kullanılmış olması esastır.

Cihazların kötüye kullanma suçunun gerçekleşebilmesi için maddede belirtilen suçların işlenmesine yönelik olarak kastın bulunması gerekir.

Bilişim sistemleri aracılığıyla dolandırıcılık suçu özü itibariyle dolandırıcılık suçunda
..... unsurunun bulunmaması nedeniyle klasik dolandırıcılık suçunun unsurlarında ortaya çıkan eksikliği gidermek amacıyla düzenlenmiştir.

Yargıtay kararlarına göre sahte kredi kartını devralan ve sonrasında kullanarak yarar sağlayan fail, göre cezalandırılır.

CEVAP ANAHTARI

1. okuma
2. yazma
3. özel
4. hile
5. hem 243/2 hem de 243/3. maddelere

KAYNAKÇA

(Bu bölüm ağırlıklı olarak Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Adalet Yayınevi Ankara 2008, adlı eserden özetlenerek hazırlanmış olup aşağıda doğrudan yararlanılan kaynaklar gösterilmiştir. Kaynakçanın tamamı için söz konusu eser esas alınmalıdır.)

Akıncı, Hatice/Alıç, A. Emre/Er, Cüneyd: Türk Ceza Kanunu ve Bilişim Suçları, İnternet ve Hukuk, Der. Yeşim M. Atamer, Baskı, İstanbul 2004, s. 157-275.

Biçkin, İnci: Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları, Yargıtay Dergisi, C. 32, Ocak-Nisan 2006, s. 145-168.

Carter, David L.: Computer Crime Categories: How Techno-Criminals Operate, <http://www.lectlaw.com/files/cril4.htm>. (E.T. 20.11.2022)

Danışman, Ahmet: Ceza Hukuku Açısından Özel Hayatın Korunması, Konya 1991.

Dönmezer, Sulhi/Erman, Sahir: Nazari ve Tatbiki Ceza Hukuku, Genel Kısım, C. I, 12. B., İstanbul 1997.

Dülger, Murat Volkan: Bilişim Suçları, 1. Baskı, Ankara 2004.

Erem, Faruk/Toroslul, Nevzat: Türk Ceza Hukuku Özel Hükümler, Savaş Yayınevi, 9. Baskı, Ankara 2003.

Ersoy, Yüksel: Genel Hukuki Koruma Çerçevesinde Bilgisayar Suçları, Prof. Dr. Yılmaz Günel'a Armağan, Ank. Ün. SBFD, C. 49, Haziran-Aralık 1994, No. 3-4, Ankara 1995, s. 149-183.

Falzetti, Valerio I.: Computer Crimes, 83 vd. <http://www.unicam.it/ssdici/falzetti.pdf>. (E.T. 13.10.2005)

Gülşen, Recep: İnternet ve Suç, İnternet ve Toplum, Editör: Ahmet Tarcan, Ankara 2005, s. 200-256.

Güney, Niyazi/Özdemir, Kenan/Balo, Yusuf S.: Yeni Türk Ceza Kanunu, 1. Baskı, 2004.

Heymann, Stephen P.: Legislating Computer Crime, 34. Harv. J. on Legis. (1997), pp. 373 - 391. (Heinonline)

Ippolito, Carlo Sarzana di S.: Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalyadaki Durum, İHFM, C: LV, S. 3, 1997, Çev. Vesile Sonay Daragenli. s. 389-405.

İçel, Kayıhan: Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İHFM, C. LIX, S. 1-2, 2001, s. 3- 9.

Karagülmez, Ali: Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 1. Baskı, Ankara 2005.

Karakurt, Eren, A.: "Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre Ya Da Güvenlik Kodlarının Üretilmesi, Yayılması veya Bulundurulması Suçu". Türkiye Adalet Akademisi Dergisi (2020), s. 219-246

Keskin, Serap: Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İHFM, C. LIX, S. 1-2, s. 155 – 180.

Koca, Mahmut: Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, C. III, s. 785-816.

La Greca, Federico Tavassi: Hacking e Criminalità Informatica, http://www.dvara.net/hk/hacking_e_criminalita_informatica.doc (E. T. 20.11.2022)

Meran, Necati: Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında İşlenen Suçlar, Seçkin Yayınevi, 1. Baskı, Ankara 2005.

Nicholson, Laura J./Shebar, Tom F./Weinberg, Meredith R.: Computer Crimes, 27 Am. Crim. L. Rev. (2000), pp. 207-259.

Özbek, Veli/Doğan, Koray/Bacaksız, Pınar: Türk Ceza Hukuku Özel Hükümler. 17. Baskı, Seçkin Yayıncılık, Ankara 2022.

Rasch, Mark D.: 11. Criminal Law and The Internet, <http://cla.org/RuhBook/chp11.htm>. (E.T. 03.04.2006)

Sieber, Ulrich, Legal Aspects of Computer - Related Crime, in the Information Society, - COMCRIME - Study, 1998, <https://www.law.tuwien.ac.at/sieber.pdf> (E.T. 20.11.2022)

Sinrod, Eric J./Reilly, William P.: Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Computer & High. Tech. L. J. (2000), pp. 177-232.

Sokullu-Akıncı, Füsun: Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi, İHFM, C. LIX, S. 1-2, 2001, s. 11-38.

Soyaslan, Doğan: Ceza Hukuku Özel Hükümler, 5. Baskı, Ankara 2005.

Toroslu, Nevzat: Ceza Hukuku Özel Kısım, 1. Baskı, Ankara 2005.

Wallace, Wang: Steal This Computer Book 3: What They Won't Tell You About the Internet, San Francisco, 2003. (Ebrary)

Yazıcıoğlu, Yılmaz: Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi, Yeditepe Hukuk Fakültesi Dergisi, C. 2, S. 2, 2005, s. 393-412.

Yazıcıoğlu, Yılmaz: Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları İle, 1. Baskı 1997.

Yenidünya, A. Caner/Değirmenci, Olgun: Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 1. Baskı, 2003.

Yılmaz, Davut: Hacking, Bilişim Korsanlığı ve Korunma Yöntemleri, İstanbul 2004.