BİLİŞİM HUKUKU

Türkiye'de Kişisel Verilerin Korunması

Bilişim Alanında Suçlar ve Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri

Geçen Hafta

Kişisel Verilerin Korunmasında Hâkim Olan Temel İlkeler
Kişisel Verilerin Niteliğine İlişkin İlkeler

İlgili Kişinin Katılımı ve Denetimine Yönelik İlkeler

Özel Kategorideki Verilerin Nitelikli Korunması

Veri Güvenliğinin Sağlanması

İstisnalar ve Sınırlamalar

Türkiye'de Kişisel Verilerin Korunması

Avrupa İnsan Haklan Sözleşmesi

Türk Ceza Kanunu

- 1 Haziran 2005 tarihinde yürürlüğe giren yeni Türk Ceza Kanunu uyarınca kişisel verilerin hukuka aykırı kayıt edilmesi, verileri hukuka aykırı verme, yayma veya ele geçirme ile gereken sürelerin geçmesine karşın verileri yok etmeme suç olarak düzenlenmiştir.

- Bu açıdan Türk hukuk sisteminde yasal düzeyde konuya ilişkin en kapsamlı korumanın Türk Ceza Kanunu'nda (TCK) yer aldığı söylenebilir.

- TCK'nin 135. maddesi uyarınca
- Madde 135-
- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.
- (2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

- TCK'nin 136. maddesinde ise kişisel verileri hukuka aykırı olarak başkasına vermek, yaymak ve ele geçirmek suçu düzenlenmiştir. Buna göre;
- *"Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır".*

- Belirtilen eylemlerin yaptırıma bağlanmasındaki amaç kişisel verilerin yetkisiz üçüncü kişilere aktarılmasını ve ele geçirilmesini önlemektir. Bu bakımdan verinin kaydedilmesinin hukuka uygun olup olmadığı, suçun oluşması açısından önemli değildir. 136. maddede yer alan düzenleme kişisel verilerin korunmasını sağlayıcı bir niteliktedir.

- Konuya ilişkin bir diğer önemli düzenlemenin TCK'nin 138. maddesinde yer aldığı görülür. Buna göre:
- *"Kanunların belirlediği sürenin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir".*

- Hükme 2014 yılında eklenen fıkra uyarınca İse
- *"Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır."*

- TCK'nin 138.maddesi ile kişisel verilerin korunması alanında temel ilkelerden biri olan verilerin süresiz olarak tutulmaması gerekliliğinin karşılandığı söylenebilir

- Belirtmek gerekir ki bu suçların hiç birinin takibi şikâyete bağlı değildir. Ayrıca Türk Ceza Kanunun 135. ve 136. maddesinde düzenlenen suçların kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenmesi hâli ağırlaştırıcı sebep olarak belirlenmiş ve cezanın yarı oranında arttırılacağı hüküm altına alınmıştır.

- Bunun yanında bu üç maddede yer alan suçların tüzel kişiler tarafından işlenmesi hâlinde bunlara özgü güvenlik tedbirleri uygulanacaktır.

Türk Medeni Kanunu

- Türk hukuk mevzuatında medeni hukukun kişilik haklarına yönelik düzenlemelerinin kişisel verilerin korunmasına açısından bazı olumlu sonuçlar sağlayabileceği söylenebilir. Medeni hukukta, kişisel verilerin korunması ile yakından ilişkili olan, kişinin onur ve saygınlığı, adı ve resmi üzerindeki hakları ile sır alanı kişilik haklarının alanı içerisinde değerlendirilmektedir.

- Bu doğrultuda konuya ilişkin hukuksal korumanın ise Türk Medeni Kanunu'nun (MK) 24. ve 25. maddelerinde getirildiği görülmektedir. MK'nin 24. maddesinde kişiliğe yönelik saldırılara karşı temel ilke, 25. maddede ise başvurulabilecek hukuksal yollar belirlenmiştir.

Türk Borçlar Kanunu

- Türk Borçlar Kanunu'nda işçinin kişisel verilerinin korunmasına yönelik bir hüküm yer almaktadır.

- Yeni Borçlar Kanunu'nun 419. maddesi uyarınca "*İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir*".

- İş ilişkisi, niteliği gereği işçinin dezavantajlı olduğu bir durum yaratmaktadır. Bu nedenle işçinin kişisel verilerinin yasal düzenlemeler uyarınca korunması son derece önemlidir.

Elektronik Haberleşme Kanunu

- 2015 yılında yapılan düzenlemeyle, Elektronik Haberleşme Kanunu'nun "kişisel verilerin işlenmesi ve gizliliğinin korunması" kenar başlıklı 51. maddesi bu sektörde veri işleme süreçlerine ilişkin kuralları belirleyen bir hüküm hâlini almıştır. Bu madde kapsamında verilerin kaliteli olması ilkesine işaret edildiği görülmektedir.
- Buna göre elektronik haberleşme alanında veri işleme süreçlerinde bu ilkenin bileşenlerine uyumlu hareket etmek bir zorunluluktur. Ayrıca elektronik haberleşmenin ve ilgili trafik verisinin gizliliği temel kural olarak benimsenmiştir.
- Bunun istisnası ilgili mevzuatın ve yargı kararlarının öngördüğü durumlardır. Bunun haricinde haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi yasaklanmıştır.

- Elektronik Haberleşme Kanunu'nun 51.maddesi ile bir yandan kişisel verilerin korunmasına yönelik bu kurallar hüküm altına alınırken diğer yandan kişisel verilerin saklanmasına yönelik bazı hükümler getirilmiştir. Nitekim bu kanun kapsamında sunulan hizmetlere ilişkin olarak; soruşturma, inceleme, denetleme veya uzlaşmazlığa konu olan kişisel veriler ilgili süreç tamamlanıncaya kadar kişisel verilere ve ilişkili diğer sistemlere yapılan erişimlere ilişkin işlem kayıtları iki yıl, kişisel verilerin işlenmesine yönelik abonelerin, kullanıcıların rızalarını gösteren kayıtlar asgari olarak abonelik süresince saklanacağı hüküm altına alınmıştır.

Elektronik Ticaret Kanunu

- 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun 6. maddesi uyarınca:

- *“(1) Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu onay, yazılı olarak veya her türlü elektronik iletişim araçlarıyla alınabilir. 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.*

- *(2) Esnaf ve tacirlere önceden onay alınmaksızın ticari elektronik iletiler gönderilebilir".*

- .

- Kanun'un 10. maddesi ise doğrudan kişisel verilerin korunmasına yöneliktir. Buna göre:

- *"(1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı:*
- *a)Bu Kanun çerçevesinde yapmış olduğu işlemler nedeniyle elde ettiği kişisel verilerin saklanmasından ve güvenliğinden sorumludur,*
- *b) Kişisel verileri ilgili kişinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz".*

- Böylelikle elektronik ticaret etkinlikleri yürüten firmaların, bu süreç içerisinde elde ettikleri kişisel verileri korumaları hüküm altına alınmıştır. Ancak Elektronik Ticaret Kanunu'nda bu yükümlülüğe aykırı hareket edenler için bir yaptırım öngörülmemiş olması bir eksiklik olarak değerlendirilebilir.

Kişisel Verilerin Korunması Kanunu

- Veri koruma alanında temel ilkeleri belirlemeye yönelik yasa hazırlıkları 1989 yılında başlamıştır. 2008 yılında TBMM'ye bir tasarı sevk edilmiş, ancak kadük olmuştur.
- 2010 yılı Anayasa değişiklikleri kapsamında kişisel verilerin korunmasını isteme hakkının anayasal bir hak olarak açıkça düzenlenmesi ile veri koruma alanında çerçeve nitelikte bir yasal düzenleme bir beklenti olmaktan öte anayasal bir zorunluluk hâline gelmiştir.
- 2012 yılında Adalet Bakanlığı bünyesinde yeni bir komisyon kurulmuş ve bu komisyonun çalışmaları neticesinde şekillenen yeni taslak üzerinde çeşitli değişiklik ve düzenlemelerin yapılmasının ardından 26 Aralık 2014 tarihinde Kişisel Verilerin Korunması Kanun Tasarısı Meclise sevk edilmiştir.

- Kişisel Verilerin Korunması Kanunu 2016 yılında yasalaşmıştır. Kanunun 1. maddesine göre "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".

- Kişisel Verilerin Korunması Kanunu Yedi bölümden oluşmaktadır. Buna göre birinci bölümde Kanunun amaç ve kapsamı belirlenmiş; ayrıca kişisel veri, verilerin işlenmesi gibi konuya ilişkin son derece önemli tanımlara yer verilmiştir.

- Kanunun "kişisel verilerin işlenmesi" kenar başlıklı ikinci bölümünde ise veri işlemede hâkim olan temel ilkelere, kişisel verilerin işlenme şartlarına, özel nitelikli(hassas) kişisel verilere, verilerin silinmesi yok edilmesi ve anonim hâle getirilmesi ile kişisel verilerin aktarılması düzenlenmiştir. Kanunun ikinci bölümünde ayrıca kişisel verilerin üçüncü kişilere ve yurt dışında aktarımına ilişkin hükümler yer almaktadır.

- Kanunun üçüncü bölümünde veri sorumlusunun aydınlatma yükümlülüğü ve veri güvenliğine ilişkin yükümlülükler ile birlikte ilgili kişinin hakları düzenlenmiştir. Bu düzenlemelerdeki temel hedef kişinin kendisi ile dijital ortamlarda her gün artan oranda işlenen verileri arasındaki bağın korunmasıdır.

- Bu açıdan önemli başka bazı hükümler de dördüncü bölümde yer alır. Nitekim burada özellikle altıncı bölümde oluşum ve işleyiş prensipleri benimsenen Kişisel Verilerin Korunması Kuruluna şikâyet, bu şikâyetlerin inceleme esasları, yine Kurul Genel Sekreterliği tarafından tutulacak "Veri Sorumluları Sicili" hüküm altına alınmıştır.

- Kanunun 18. maddesi ile “görev ve yetkilerini kendi sorumluluğu altında, bağımsız olarak” yerine getireceği belirtilen bir Kişisel Verileri Koruma Kurulu oluşturulması öngörülmektedir.

- Görev alanına giren konularla ilgili olarak hiçbir organ, makam, merci veya kişi, Kurula emir ve talimat veremez, tavsiye veya telkinde bulunamaz. Kurul, dokuz üyeden oluşur. Kurulun beş üyesi Türkiye Büyük Millet Meclisi, dört üyesi Cumhurbaşkanı tarafından seçilir.

- Kurula üye olabilmek için; kurumun görev alanındaki konularda bilgi ve deneyim sahibi olmak, 14/7/1965 tarihli ve 657 sayılı Devlet Memurları Kanununun 48. maddesinin birinci fıkrasının (A) bendinin (1), (4), (5), (6) ve (7) numaralı alt bentlerinde belirtilen nitelikleri taşımak, herhangi bir siyasi parti üyesi olmamak ve en az dört yıllık lisans düzeyinde yükseköğrenim görmüş olmak şartlarını taşımak gerekir.

Kurulun görev ve yetkileri ise şunlardır:

- Kişisel verilerin, temel hak ve özgürlüklere uygun şekilde işlenmesini sağlamak
- Kişisel verilerle ilgili haklarının ihlal edildiğini ileri sürenlerin şikâyetlerini karara bağlamak
- Şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda kişisel verilerin kanunlara uygun olarak işlenip işlenmediğini incelemek ve gerektiğinde bu konuda geçici önlemler almak
- Özel nitelikli kişisel verilerin işlenmesi için aranan yeterli önlemleri belirlemek

- Veri Sorumluları Sicilinin tutulmasını sağlamak.
- Kurulun görev alanı ile Kurumun işleyişine ilişkin konularda gerekli düzenleyici işlemleri yapmak
- Veri güvenliğine ilişkin yükümlülükleri belirlemek amacıyla düzenleyici işlem yapmak
- Veri sorumlusunun ve temsilcisinin görev, yetki ve sorumluluklarına ilişkin düzenleyici işlem yapmak.
- Bu Kanunda öngörülen idari yaptırımlara karar vermek

- Kanunun yedinci bölümünde yer alan istisnalar, yani bütüncül olarak Kanunim kapsamı dışında kalacak alanlar en çok tartışılan hükümleri arasındadır.

- Bu noktada ilk dikkat çeken istisna istihbarat gibi bazı etkinliklerin kapsam dışında tutulmasıdır. İstihbaratın niteliği gereği gizli yürütülen bir etkinlik olduğu kabul edilse bile, hukuka ve dürüstlük kurallarına uygun olmak, belirli açık ve meşru amaçlar için işlenmek ya da işlendikleri amaç için gerekli olan süre kadar muhafaza edilmek gibi ilkeler bu alanda da öncelikle ve mutlaka geçerli olmalıdır.

- Hukuksal güvenceler, bilişim teknolojileri ile temel hak ve özgürlükler arasındaki dengenin kurulabilmesi için en önemli araçtır. Ancak bunun yanında konuya ilişkin farkındalığın arttırılması ve kişisel önlemlerin alınması gerekir.

- Etkin veri koruması sağlanması yönündeki çalışmalar içerisinde teknolojideki gelişmelerden yardım almak ise son yıllarda dikkat çeken bir önem kazanmıştır. "Dizayn aracılılığıyla gizlilik" (privacy by design, PbD) ya da "varsayılanlar aracılılığıyla gizlilik" (privacy by default) bu kapsamda verilebilecek bir kaç örnektir.

- Bilişim alanında yaşanan gelişmelere bağlı olarak daha önceden hiç öngörülemeyen ve dolayısıyla suç tipleri arasında düzenlenmeyen bir takım yeni fiiller ortaya çıkabildiği gibi, mevcut suç tipleriyle öngörülen fiillerin yeni yöntemlerle işlenmesi de söz konusu olabilmektedir.

- Bu bağlamda yasa koyucunun da bu alanda görülen gelişmelere paralel olarak, mevcut düzenlemelerini değiştirmesi ya da yeni düzenlemeler yapması gerekmektedir.

- Suçlara ilişkin inceleme gerçekleştirilirken suçun unsurları tipik maddi unsur, tipik manevi unsur ve hukuka aykırılık unsuru olmak üzere üç alt başlıkta incelenmiştir.

Bilişim Alanındaki Suçlara İlişkin Türkiye'de Yaşanan Süreç

- Bilişim alanında yaşanan gelişmeler karşısında kanun koyucu, 90'lı yılların başında, bir yandan uygulamada kendini hissettiren ihtiyaçları karşılayabilmek diğer yandan da Türkiye'nin üyesi bulunduğu çeşitli uluslararası kuruluşların tavsiye kararlarına uyum sağlayabilmek amacıyla birtakım düzenlemeler yapmıştır.

- Bu bağlamda bilişim suçlarına ilişkin ilk düzenleme TCK'ya 1991 yılında girmiş ve 3756 sayılı kanunla 765 sayılı TCK'nın ikinci kitabına bazı bilişim suçlarını öngören "Bilişim Alanında Suçlar" başlıklı 11. Bap ilave edilmiştir.

- TCK'da 1991 yılında yapılan söz konusu düzenlemeyi takiben 1995 yılında ise, 4110 sayılı kanunla Fikir ve Sanat Eserleri Kanununda bilgisayar programlarının da eser sayılacağına ilişkin bir değişiklik yapılmış; bilgisayar programlarına karşı gerçekleştirilen birtakım eylemler de yaptırım altına alınmıştır.

- İletim ağlarının ticarette kullanılmaya başlaması ve e-ticaret kavramının ortaya çıkmasına bağlı olarak sözleşme onaylamalarında işlemleri çabuklaştırmak için dünyada hızla kullanılmaya başlayan elektronik imzaya ilişkin düzenleme de Elektronik İmza Kanunu adı altında 2004 yılında kanunlaşmıştır.

- 2004 yılında kanunlaşan ve 2005 yılında yürürlüğe giren 5237 sayılı yeni TCK'da ise bilişim alanında işlenen suçlara, önceki 765 sayılı kanundan daha ayrıntılı düzenlemeler yapılarak yer verilmiştir. Kanunda söz konusu suçlara, özel hükümlerin yer aldığı TCK'nın 2. kitabının topluma karşı suçların düzenlendiği 3. kısmının 10. bölümünde "Bilişim Alanında Suçlar" başlığı altında yer verilmiştir.

- 2007 yılında ise internet vasıtasıyla işlenen suçlarla mücadelenin etkinliğini arttırmak için İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun TBMM tarafından kabul edilip yürürlüğe konulmuştur.

- 765 sayılı eski TCK'da yer alan Bilişim Alanında Suçlara ilişkin düzenlemenin gerekçesinde, "bilişim alanlından kastın "bilgilerin otomatik olarak işleme tabi tutuldukları sisteme ilişkin alan" olduğu ortaya konulmuştur.

- 5237 sayılı yeni TCK'da ise **bilişim sisteminden** bahsedilmiş ve 243. maddenin gerekçesinde "Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir." denilerek konuya açıldık getirilmeye çalışılmıştır. Tanımlamadan anlaşılacağı üzere bilişim sistemi teriminin en temel yansıması bilgisayarlardır.

Bilişim Sistemine Girme

- 5237 sayılı TCK'da izinsiz bilişim sistemine girme düzenlemesiyle birlikte, hukuk sistemimizde, Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde öngörülen hukuka aykırı erişim düzenlemesiyle de paralellik sağlanmıştır. Bilişim sistemine girmenin düzenlendiği 5237 sayılı TCK'nın 243. maddesinin metni şu şekildedir:

Madde 243*-

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada 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) 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*

Suçla korunan hukuki değer

- Suçun hukuki konusu olarak da ifade edilen **suçla korunan hukuki** değer; suçla ihlal edilen hukuki varlık veya menfaattir.

- Bilişim alanındaki suçlara ilişkin düzenlemelerde ise, bilgisayar ortak özelliği teşkil etmek üzere, birden fazla hukuki yarar korunmaya çalışılmaktadır.

Tipik Maddi Unsur

- **Tipik maddi unsur,** suçun konusu, faili, mağduru, fiil

- **Suçun Konusu:** Suçun konusu, suçun üzerinde gerçekleştirildiği eşya veya kişi olarak ifade edilebilir. Bu bağlamda izinsiz bilişim sistemine girme suçunun maddi konusu, bir bilişim sistemi veya ona ait parçalardan herhangi birisidir. Nitekim suç tipiyle yasaklanan davranışlar bir bilişim sistemi veya onun parçaları üzerinde gerçekleştirilmelidir ki suç oluşabilsin.

- **Fail:** Suçun faili tipik eylemleri gerçekleştiren kişidir. Herkes suçun faili olabilir.

- **Mağdur:** Suçla korunan hukuki değerin ait olduğu kimse *mağdur* olarak nitelendirilir.Girilen bilişim sistemini kullanan kimse bu suçun mağdurudur.

- **Fiil:** Kanunda tanımlanan maddi fiil, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek ve orada kalmaya devam etmektir.

Suçun manevi unsuru

- Suçun manevi unsuru kasttır. Suçu oluşturan fiillerin hangi amaçla gerçekleştirildiğinin bir önemi yoktur. Zarar verme veya menfaat sağlama gibi bir amacı olmaksızın, sadece bakmak için hukuka aykırı olarak bir bilişim sistemine giren ve orada kalan kimse bu madde gereğince sorumlu olacaktır.

- Suçun taksirli hâli kanunda düzenlenmemiştir. İnternette gezinirken dikkatsiz davranıp, kastı olmaksızın gerçekleştirdiği bazı davranışlarla bir bilişim sistemine giren kimseler bakımından cezai sorumluluk doğmayacaktır.

- Cebir veya tehdit altında, İnternet vasıtasıyla, girilmesi yasak sisteme giriş yapan bilişim sistemi uzmanı kimse bakımından kusurun varlığından ve dolayısıyla cezai sorumluluktan söz edilemeyecektir.

Hukuka Aykırılık

- Ceza normu ile yasaklanmış tipik davranışların gerçekleştirilmesi **hukuka aykırılığın** karinesini oluşturur.

- Herhangi bir fiilin hukuka aykırı olduğu konusundaki kesin hüküm, ancak herhangi bir hukuka uygunluk nedeninin somut olayda bulunmaması halinde verilebilir.

Kusurluluk

- **Kusurluluk** ve kusurluluğu ortadan kaldıran hallere ilişkin söz konusu suçlar bakımından özellik arz eden bir durum söz konusu değildir.

- Bu bağlamda zorunluluk hali veya karşı konulamayacak bir cebir veya ağır bir tehdit altında buradaki fiilleri gerçekleştirenler bakımından kınanabilirlik söz konusu olmayacağından cezai sorumluluk doğmayacaktır.

- Kaynak
- «BİLİŞİM HUKUKU» Murat Yayınları (Anadolu Üniversitesi Açıköğretim Fakültesi Bilişim Hukuku ders kitabı.)