

## **Önleyici Kolluk Faaliyeti ve Ceza Muhakemesinde Yapay Zeka Teknolojileri**

**Arş. Gör. Irmak Erdoğan - Galatasaray Üniversitesi**

Yapay zeka yazılımlarının kamu kurumları ve kolluk kuvvetleri tarafından kullanılmaya başlanması, kolluk hukuku ve ceza muhakemesi üzerinde köklü değişikliklere yol açmaktadır. Başta Amerika, Avrupa, Çin ve Hindistan'da "akıllı şehir"ler yaratılmakta, bu şehirlerdeki sokak kameraları ve polis araçları, kişilerin hareketleri, yüz ifadeleri gibi verilerden yola çıkarak tehlike yaratma ihtimallerini otomatik olarak belirleyen yeni yapay zeka yazılımları ile donatılmaktadır. Öte yandan kolluk görevlileri, sosyal medya denetimi yapan algoritmalarla kişilerin yaşam tarzları, paylaşım ve beğenileri üzerinden profillerini oluşturmakta ve "potansiyel suçlu" listeleri yaratmaktadır. Yine Cloud Walk, Predpol, Compas gibi pek çok yazılım, suç dosyaları ve diğer veri havuzlarını kullanarak önleyici kolluk kavramına yeni bir boyut kazandırmakta, hatta bu teknolojiler aracılığıyla kişilerin tekrar suç işleyip işlemeyeceği, herhangi bir tanığa zarar verip vermeyeceği gibi ihtimallere ilişkin yapılan hesaplamalar, Amerika'da hakimlerin tahliye ya da tutukluluk gibi kararlarına dayanak olarak kullanılmaktadır.

İşte kişilerin profillerini oluşturan, takibe alınmasına yol açan ve hayatlarının her alanında bu profilleri karşılarına çıkartan algoritmalar bugün birer distopya ürünü olmaktan çıkmış, pek çok teknoloji şirketinin yatırım odağı haline gelmiştir. Ancak olağan şüphelilerin teknoloji eliyle belirlenmesi, bu kişilerin henüz suç işlemeyen ve herhangi bir hazırlık hareketine dahi başlamadan devlet müdahalesi ile karşılaşma ihtimalini doğurmaktadır.

Ülkemizde henüz detaylı hukuki tartışmalara konu olmayan tüm bu gelişmeler, tebliğde örnekleriyle açıklanacak, ardından yapay zeka yazılımları ve bu yazılımlara konu olan verilerin ayrımcılık yasağı, kişisel verilerin korunması ve ceza muhakemesinin temel ilkeleri çerçevesinde doğuracağı sorunlar ele alınacaktır. Sonuç kısmında ise bu alanda yapılması gereken hukuki düzenleme önerileri sunulacak, bu bağlamda özellikle Avrupa Birliği Genel Veri Koruma Tüzüğü (General Data Protection Regulation–GDPR) m. 22'de düzenlenen otomatik veri işleme sonucu alınan kararlara konu olmama hakkı ve ilgili diğer haklar üzerinde durulacaktır.

## **Anonim Őirket Yönetiminde Yapay Zeka**

**Arş. Gör. Salih Tayfun İnce - Fatih Sultan Mehmet Üniversitesi**

Türk Ticaret Kanunu'na göre anonim Őirketlerde yönetim ve temsil yetkisi, Kanun ve esas sözleşme uyarınca genel kurulun yetkisine bırakılmış bulunan iş ve işlemler dışında, yönetim kuruluna aittir. Yönetim kurulunun seçimi, üyelerin nitelikleri, sorumlulukları ve yetki devri de Türk Ticaret Kanunu'nda düzenlenmiştir. Bilişim alanında yaşanan gelişmeler ile birlikte yapay zeka sahibi robotların Őirket yönetim kurullarında görev alması ya da bu robotlara yetki devri yapılması söz konusu olabileceđi gibi yapay zekanın getireceđi hız ve kararlarında yüksek isabet oranı ile birlikte, bu robotlara yönetimde yer verilmesi özen ve bađlılık yükümlülüđünün bir geređi hâline dahi gelebilecektir. Bu bildiride Türk Ticaret Kanunu, diđer ilgili mevzuat ve öğretilerdeki görüşler ışığında, anonim Őirket yönetim kurullarında yapay zeka robotlarına yetki devri olanađı, bu robotların yönetim kurulunda yer alıp alamayacađı ve yer almaları durumunda asistan ve otonom yapay zeka türlerine göre yönetim kurulundaki sorumluluk ilişkileri incelenecektir.

**ANAHTAR SÖZCÜKLER:** Anonim Őirket, yönetim kurulu, yapay zeka, robot yönetim kurulu üyeleri, yönetim kurulunun sorumluluđu.

## **YOUTUBE SÖZLEŞMESİNDEKİ, İÇERİĞE İLİŞKİN LİSANS DEVRİ HÜKÜMLERİNİN TÜRK HUKUKU BAKIMINDAN DEĞERLENDİRİLMESİ**

**Dr. Öğr. Üyesi Emre Cumalıoğlu - Yaşar Üniversitesi**

Dünyanın dört bir yanında, kadın erkek, çocuk yaşlı yüzbinlerce insan YouTube a video yüklüyor. Bunlardan, “youtuber”ların fikri ürünü olan içeriklerden bazıları eser olarak korunmayı hak ediyorken, büyük çoğunluğu bu korumayı hak edecek nitelikten uzak görünmektedir. Bu videolarla ilgili hukuki sorunlar, genellikle üçüncü kişilerin haklarına tecavüzde bulunulup bulunulmadığıyla ilgilidir.

Diğer yandan YouTube şirketinin genel işlem koşulları niteliğindeki sözleşmesinde (hizmet koşulları) yer alan bazı hükümlerin, kullanıcıların Türk hukukunda emredici hükümlerle korunan bazı haklarını ihlal edici nitelikte olduğu tartışılabilir. Çalışmamızda, kullanıcının yüklediği içerik üzerindeki hakların; karşılıksız, coğrafi olarak sınırsız ve devredilebilir nitelikte lisans hakkının, Youtube şirketine ve sınırlı olarak diğer kullanıcılara devredilmesini konu alan 7.2., 8.1. ve 8.2. maddelerini ele alacağız.

Bu konuda öncelikle yanıtlanması gereken bir soru bulunmaktadır. Acaba, Youtube ile kullanıcı arasında bir hukuki uyumsuzluk çıkarsa, bu uyumsuzluk hangi devlet mahkemesi tarafından, hangi ülke hukuku uygulanarak çözülecektir? Kanımızca, bu tür uyumsuzlukların Türk hukuku uygulanarak çözümü mümkündür. Bu tespitten hareketle, Türk Borçlar Kanunu’nun sözleşmelerin geçerliliğine ilişkin genel hükümleri ve özellikle genel işlem koşullarını düzenleyen maddeleri, Türk Medeni Kanunu’nun ilgili hükümleri, Fikir ve Sanat Eserleri Kanunu’nun eser sahibinin haklarını koruyan ve bu haklar üzerindeki sözleşme ve tasarrufları düzenleyen maddeleri ile Yargıtay kararlarını göz önünde bulundurarak, bahsettiğimiz Sözleşme hükümlerinin geçerliliği hakkında görüşlerimizi açıklayacağız. Sonuç olarak, inceleyeceğimiz Sözleşme hükümlerinin Türk hukuku bakımından geçersiz olduklarını, bu geçersizliğin sözleşmenin tamamını geçersiz kılmayan kısmi geçersizlik olduğunu söyleyebiliriz.

## **BITCOIN ve İcra Hukuku**

**Dr. Nilüfer Boran Güneysu Anadolu Üniversitesi**

**Stj. Av. Burak Memiş İstanbul Barosu**

Bilişim teknolojisindeki gelişme, finans piyasalarını etkilemiş ve kredi kartları, elektronik para, sanal para veya kripto para gibi kavramlar hayatımıza girmiştir. 2008 yılında hayatımıza giren bitcoin, herkesin ilgisini çekmeyi başarmış ve kripto para piyasasının en çok yatırım alan üyesi haline gelmiştir. Bitcoin'in yaygınlaşması ve insanlar tarafından kabulü, sorun ve tartışmaları da beraberinde getirmiştir. 2017 yılında bitcoin bir cinayetin nedenleri arasında gösterilmektedir. Bitcoinin ekonomi ve para piyasaları kadar hukukun da gündeminde olan bir konudur. Bitcoin, ceza veya vergi hukuku ile doğrudan ilişkili olduğu gibi borçlar, yargılama ve icra hukuk ile bağlantılıdır. Takip talebinde alacak miktarının bitcoin olarak gösterilmesi, ödemenin bitcoinle yapılması, bitcoinin haczi veya tasarrufun iptali davasına konu edilebilmesi icra hukuku bakımından değerlendirilmesi gereken konulardır. Bitcoin'in tüm icra ve iflas hukukunun tamamı üzerindeki etkisi, bu çalışmanın sınırlarını aşacak niteliktedir. Takip talebinde bitcoinin gösterilmesi, bitcoin ile ödeme, bitcoinin haczi gibi konular ayrı birer çalışmanın konusu olabilecek niteliktedir. Bu çalışmada, bitcoinin ve icra hukuku ilişkisi işaret edilecek; bitcoinin takip talebi, ödeme aracı, haciz, satış ve tasarrufun iptali davası bakımında etkileri genel olarak değerlendirilecektir.

# ELEKTRONİK HABERLEŞME SEKTÖRÜNDE KİŞİSEL VERİLERİN HUKUKA UYGUN ELDE EDİLME YOLLARI

Arş. Gör. Simay Doğmuş - Yaşar Üniversitesi

Elektronik haberleşme sektöründe kişisel verilerin korunmasının sağlanmasının öncelikli yolu, bu verilerin hukuka uygun olarak elde edilmesidir. Kişisel verilerin elde edilmesi, değişik amaçlar için kullanabilme amacıyla tamamen veya kısmen otomatik ya da herhangi bir veri kayıt sisteminin bir parçası olmak üzere otomatik olmayan yollarla, ilgili kişiler hakkında bilgilerin toplanması ve bir araya getirilmesidir. Elektronik haberleşme sektöründe kişisel verilerin elde edilmesi telefonların dinlenmesi, ilgilinin ses kaydı veya trafik veri konumunun gösterimi şeklinde olabilir. Kişisel verilerin hukuka uygun olarak elde edilebilmesi için bazı ilke ve esaslara uyulmasının yanında, kişinin bilgilendirilerek açık rızası alınmak zorundadır.

Bu anlamda elektronik haberleşme sektöründe kişisel verilerin hukuka uygun olarak elde edilmesinde uyulması gereken ilk ve şemsiye ilke hukuka ve dürüstlük kuralına uygunluktur. Hukuka uygun olması ile kastedilen, veri toplayanın başta Avrupa Konseyi Direktifleri ve Avrupa Birliği Direktifleri ile Kişisel Verilerin Korunması Hakkında Kanun ve Elektronik Haberleşme Mevzuatı olmak üzere ilgili mevzuattan doğan ilke ve yükümlülüklerle uyarak kişisel verileri elde etmesi iken; dürüstlük kuralına uygun olması ile kastedilen kişisel verilerin elde edilmesi sırasında kişilerin yanıltılmaması ve söz konusu amaçla bağdaşmayan veya kişilerin anlayamayacağı başka bir amaç için bu verilerin toplanmamasıdır.

Hukuka uygunluk ve dürüstlük kuralıyla yakın ilişki içerisinde olan bir ilke ise amaca bağlılık ilkesi olup, elektronik haberleşme sektöründe kişisel verilerin önceden belirlenmiş veya belirlenebilen hukuka uygun amaçlar için toplanması anlamına gelmektedir. Diğer bir ifadeyle elektronik haberleşme sektöründe kişisel verilerin toplanmasındaki amaç belirli, açık ve meşru olmalıdır. Ayrıca oranlılık ilkesi gereğince elde edilen kişisel veri, kişinin rıza verdiği amacın gerçekleşmesi bakımından faydalı ve gerekli olmalıdır. Kişisel verilerin toplanma amacı dışında kullanılması, amacı aşması veya amaca ulaşmada faydasız veya gereksiz verilerin toplanması yasaktır. Bu ilkelere Avrupa Konseyi'nin 1995 tarih ve 46 sayılı Veri Koruma Direktifinin 6. maddesi, Avrupa Birliği'nin Genel Veri Koruma Direktifinin 5. maddesinde ve Kişisel Verilerin Korunması Hakkında Kanun'un 4. maddesinde, Elektronik Haberleşme Kanunu'nun 50. ve 51. maddelerinde, BTK tarafından çıkarılan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 4. maddesinde etraflıca yer verilmiştir.

Elektronik haberleşme sektöründe kişisel verilerin hukuka uygun olarak toplanmasının en önemli koşulu ilgili kişilerin toplama faaliyetinden önce veya sırasında bilgilendirilmeleri ve açık rızalarının alınmasıdır. Bilgilendirme yazılı, önceden yazılmış bir sözleşme metni veya sözlü olarak verileri toplayacak özel kişi veya kurum tarafından ilgili içerik, süre, amaç, süre ve kişisel verileri toplayacak kişileri kapsayacak şekilde, saydamlık ilkesine uygun ve eksiksiz bir şekilde yapılmalıdır. Bu bağlamda bilgilendirme, Avrupa Konseyi Direktiflerinin yanı sıra Kişisel Verilerin Korunması Hakkında Kanun'un 6. ve 7. maddeleri ile ikincil düzenlemelere; sektör spesifik düzenlemelerinden başta Elektronik Haberleşme Kanunu'nun 51. maddesi, BTK tarafından yayınlanan Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nin 6. maddesi, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in 4. maddesine uygun olarak yapılmalıdır. Söz konusu bilgilendirme yapılmamışsa, kişisel verileri toplanacak kişi tarafından talep edilmelidir.

Bu işlemin ardından kişisel verilerin toplanabilmesi için kişilerin geçerli ve açık rızası alınmalıdır. Rızanın geçerli olarak kabul edilebilmesi için ise, serbestçe verilmiş, konuya özel; diğer bir ifade ile somut durum ve amaca yönelik, kişinin bilgilendirilmiş ve kesin olması gerekmektedir. Eğer kişi, kişisel verilerin toplanmasından önce kendisi hakkında toplanmakta olan veya toplanabilecek veriler için toplu bir rızada bulunmuşsa, bu rıza hukuka aykırı olarak kabul edilmektedir. Kişiler, basit, kolay ve ücretsiz yollarla rıza verebilecekleri gibi; verdikleri rızayı her zaman aynı şekilde geri alabilmelidirler. Ayrıca kişisel verilerin toplanmasından sonra verilen rıza, kişisel verilerin toplanma işlemini hukuka uygun hale getirmemektedir; ne var ki kişinin rızasını geri alması halinde, önceden toplanan veriler hukuka uygun olmaya devam etmektedir. Avrupa Konseyi'nin 2002 tarihli ve 58 sayılı Elektronik Veri Koruma Direktifi ve Elektronik

Haberleşme Kanunu'nun 51. maddesi gereğince, elektronik haberleşme hizmetlerinin pazarlanması veya katma değerli elektronik haberleşme hizmetlerinin sunulması amacıyla, ihtiyaç duyulan trafik verileri ve yer verileri ilgili abonelerin bilgilendirilerek rızalarının alınması şartıyla, alınan rızaya uygun olarak sadece belirtilen amaçlarla ve ölçülülük ilkesine uygun olarak toplanabilmektedir. Benzer şekilde, insan müdahalesi olmaksızın çalışan otomatik haberleşme sistemlerine doğrudan pazarlama amacıyla kullanımına kural olarak abonelerin rızaların alınması kaydıyla izin verilebilmektedir. Bu husus ayrıca, yerel mevzuatımızda her türlü ticari elektronik iletiyi kapsayacak şekilde 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da da düzenlenmiştir. İstisnaen açık rıza, kanunlarda açıkça öngörülmesi, 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, bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, ilgili kişinin kendisi tarafından alenileştirilmiş olması, bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması hallerinde aranmaz.

Kişisel verileri toplanacak kişilerin, Avrupa Konseyi'nin 1995 tarih ve 46 sayılı Veri Koruma Direktifi ve Elektronik Haberleşme Kanunu gereğince haklarında elde edilecek verilerin doğru ve güncel olmasını talep etme ve toplanan verilerde değişiklik olması durumunda bunların silinmesini veya düzeltilmesini talep etme hakkı bulunmaktadır ve bu hak kişilere toplama anında bildirilmelidir. Elektronik haberleşme sektöründe silme veya düzeltilmesini talep hakkı genellikle kişisel verilerin yanlış, geçersiz veya hukuka aykırı olarak toplanması durumlarında gündeme gelmektedir. Kişisel verileri toplayan kişilerin de bu verilerin doğru ve güncel olması hususunda gerekli makul tedbirleri alma ve hatalı verilerin saptanması halinde bunu ilgili kişilere bildirme yükümlülükleri bulunmaktadır.

Öte yandan kişilerin kamu görevinin ifa edilmesi ya da çıkarlarının korunması amacıyla kişisel verileri hukuka olarak toplanmış veya bu kişilerin bir üstün yararı söz konusuysa toplama işlemine karşın itiraz hakkı bulunmaktadır. Genel itiraz hakkı olarak ifade edilen bu hak, Avrupa Konseyi'nin 1995 tarih ve 46 sayılı Veri Koruma Direktifiyle paralel ve genel olarak kişisel verilerin işlenmesini kapsayacak şekilde Kişisel Verilerin Korunması Kanunu'nun 11. maddesinde, "*İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme*" olarak tanımlanmıştır. İlâveten kişilerin Avrupa Konseyi'nin 1995 tarih ve 46 sayılı Veri Koruma Direktifi ve BTK tarafından çıkarılan Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik gereğince doğrudan pazarlama amacına ilişkin itiraz hakkı da bulunmaktadır. Bir ürünün satılması ya da bir hizmetin sağlanması sırasında aboneye ait iletişim bilgilerin elde edilmesi halinde, söz konusu ürün ya da hizmetin pazarlanması amacıyla iletişim bilgilerinin kullanılması hukuka uygun kabul edilmektedir. Ancak elektronik iletişim bilgileri üzerinden abonelere gönderilen iletilerin abone tarafından her zaman basit ve ücretsiz bir işlemle reddedilebilir olması gerekmektedir.

Son olarak yukarıda belirtilen ilk ve usullere uyulmaksızın kişisel verileri hukuka aykırı olarak izinsiz, yanlış veya geçersiz şekilde elde edilen kişiler, bu verileri toplayan gerçek veya tüzel kişilerden zararının tazminini Medeni Hukuk hükümlerine göre talep edebilmektedirler. Aynı zamanda, söz konusu kişisel veri toplama faaliyeti BTK tarafından çıkarılan İdari Yaptırımlar Yönetmeliği'nin 12. ve 13. maddeleri veya Elektronik Haberleşme Sektörüne İlişkin Tüketici Hakları Yönetmeliği'nin 25. maddesi gereğince de bir ihlal meydana getiriyorsa idari para cezasını gerektirebilecektir.

# **BLOCKCHAIN TEKNOLOJİSİNİN KİŞİSEL VERİLERİN KORUNMASI MEVZUATI AÇISINDAN DEĞERLENDİRMESİ**

**Emrullah Kaya - Ankara Üniversitesi**

Anayasal güvence kapsamında herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu bağlamda, 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe giren Kişisel Verilerin Korunması Kanunu’yla gerekli yasal altyapı tamamlanmıştır. İlgili Kanun’la kişilere, kayıt ortamlarından kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve Kanun’da öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme hakkı verilmektedir. Kanun’un hazırlık ve yasalaşma aşamasında olgunlaşan ve birçok sektörde inovatif uygulamalar geliştirilmesini sağlayan blockchain teknolojisiyle beraber verilerin saklanmasında merkezi veritabanı yaklaşımından merkezi olmayan dağıtık kayıt sistemlerine doğru bir geçiş yaşanmaktadır. Blockchain teknolojisiyle şifreli veriler zincir halkaları şeklinde birbirine bağlanarak blockchain ağında yer alan bütün düğümlerin (node) onayı alındıktan sonra değiştirilemez şekilde dağıtık sunucularda kayıt altına alınması sağlanır. Blockchain ağındaki herhangi bir blokta yer alan bilginin değiştirilebilmesi için blokzincir halkasının başlangıç blokuna kadar müdahale edilmesi gerektiğinden matematiksel olarak imkansıza yakındır. Bu nedenle blockchain teknolojisiyle saklanan verilerin güvenilirliği, değiştirilmesinin veya müdahale edilmesinin imkansıza yakın olması sayesinde sağlanmaktadır. Ancak, anayasal bir hak olan kişisel verilerin korunmasının istenmesi hakkı kapsamında kişisel verinin silinmesini veya düzeltilmesini talep etme hakkı da bulunmaktadır. Bu çerçevede, giderek birçok uygulamada karşımıza çıkan blockchain teknolojisi ile kişisel verilerin korunması mevzuatı arasında uyumsuzluk ihtimali ortaya çıkmaktadır. Kanunun ihlali durumunda çeşitli yaptırımlar mevcut olmakla beraber blockchain ekosisteminde yer alan paydaşlardan hangilerinin veri sorumlusu veya veri işleyen olduğu tespiti muhtaçtır. Yakın gelecekte blockchain uygulamalarının yaygınlaşma ihtimali de göz önüne alındığında geliştiriciler ve diğer paydaşlar açısından yükümlülüklerinin belirlenebilmesi ve uygulamaların hukuki çerçeve içerisinde hayata geçirilebilmesi için söz konusu uyumun/uyumsuzluğun açıklığa kavuşturulması gerekmektedir. Teknolojik gelişmelerin hukuk düzeninde yarattığı değişimin yanında temel hak ve özgürlüklerin de teknolojik gelişmelerde sınırlamalara yol açtığı durumlar yaşanmaktadır. Bu kapsamda, henüz olgunlaşma aşamasında olan söz konusu teknolojinin, anayasal güvence altında olan kişisel verilerin korunmasını sağlayacak şekilde evrilmesine katkıda bulunacak önerilerin geliştirilmesinin önemli olduğu değerlendirilmektedir.

## BLOKZİNCİR VE KRİPTO DEĞERLER

Av. Elif Petek Özlü - İstanbul Barosu

Son zamanlarda geliştirilen en yıkıcı teknolojilerden biri olan blokzincir, 2017 yılında Bitcoin değerinde meydana gelen beklenmeyen yükseliş ile birlikte oldukça popüler bir konu haline geldi. Ne var ki, tartışmalar Bitcoin ve diğer kripto değerlerin birer yatırım aracı olarak kullanılması noktasında yoğunlaşırken, bunların altında yatan teknolojinin değeri henüz tam manasıyla anlaşılabilmiş değil. Oysaki blokzincir ile Bitcoin arasındaki ilişki, tıpkı elektrik-ampül ilişkisine benzemektedir. Bu ilişkide blokzincir elektrik iken, Bitcoin ve diğer kripto değerler ise, yalnızca blokzincir teknolojisinden doğan ürünlerdir. Teknoloji ışık hızıyla gelişmeye devam ederken, yasalar takip etmekte zorluk çekiyor. Bu sebeple öncelikle teknolojinin temellerini anlamak ve bunların yasalar nezdindeki konumlanmasını incelemek gerekiyor. Bu makalede öncelikle blokzincir teknolojisinin ne olduğu ve nasıl çalıştığı kısaca özet geçilecek, sonrasında konuya ilişkin gelişmeler, bilhassa kripto değer arzları hususu, Türk hukuku ve karşılaştırmalı hukuk bakımından değerlendirilecektir. Son olarak da blokzincir ile Avrupa Birliği Genel Veri Koruma Tüzüğü arasındaki ilişkiye değinilecektir.

**Anahtar Kelimeler:** Blokzincir, kripto değerler, Bitcoin, Avrupa Birliği Genel Veri Koruma Tüzüğü, kişisel verilerin korunması.



## **Avrupa Birliđi Genel Veri Koruma Tüzüğü'nün Sınırötesi Uygulanması ve Türk Hukukuna Etkisi**

### **Ayşe Nur Akıncı - Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı Sektörler ve Kamu Yatırımları Genel Müdürlüğü Bilgi ve İletişim Teknolojileri Dairesi**

Bu çalışmada, 1995 yılından beri kişisel verilerin korunması alanında tüm dünyada kabul görerek genel çerçeveyi çizen 95/46/AT sayılı Avrupa Birliđi (AB) Veri Koruma Direktifi'nin yerini alan "AB Genel Veri Koruma Tüzüğü'nün (General Data Protection Regulation–GDPR)" uygulama alanının incelenmesi amaçlanmaktadır. GDPR'nin yürürlüğe girmesinden sonra AB ülkeleri bakımından veri koruma hukuku bağlamında bir kanunlar ihtilafının kalmayacağı, zira söz konusu düzenlemenin üye devletlerin ulusal mevzuatının yerini kesin olarak alacağı kabul edilmektedir. Bununla birlikte, söz konusu düzenlemenin AB üyesi olmayan ülkelerde nasıl uygulanacağını ve uygulamaya etkilerinin dikkatle incelenmesi gerekmektedir.

Mayıs 2018 tarihinde yürürlüğe girerek tüm üye devletlerde doğrudan bağlayıcı hale gelen GDPR hükümlerinde öngörülmekte olan oldukça geniş uygulama alanı, düzenlemenin sınırötesi (extraterritorial application) etkileri bağlamında dikkatle incelenmesi ihtiyacını ortaya çıkarmıştır. Bu kapsamda, Avrupalı veri koruma otoriteleri ile üçüncü ülke hukuk kişileri arasında Tüzüğe uyum konusunu gündeme gelecek muhtemel hukuki uyumsuzlıklarda AB veri hukukunun nasıl uygulanacağı ele alınacaktır.

**Anahtar Kelimeler:** Genel Veri Koruma Tüzüğü; sınırötesi uygulama; veri hukuku.

## **Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu Bağlamında Kişisel Verilerin Korunması**

**Dr. Öğr. Üyesi Candide Şentürk - Yaşar Üniversitesi**

Kişisel verilerin korunması, insan haklarından olan özel hayat ve aile hayatına saygı hakkı bakımından önem arz etmektedir. Özel hayata ve aile hayatına saygı hakkı, gerek Avrupa İnsan Hakları Sözleşmesi'nin 8'inci maddesinde (*herkesin özel hayata ve aile hayatına saygı gösterilmesini isteme hakkı*) gerekse Anayasa'nın 20'inci maddesinde kişinin temel haklarından sayılarak güvence altına alınmıştır.

Kişisel veri, ceza hukuku, idare hukuku, ticaret hukuku, medeni hukuk gibi çok çeşitli hukuk dallarının ilgi alanına giren oldukça geniş bir kavramdır. Bu itibarla tartışmalı olmakla beraber sınırları tam olarak çizilemeyen bir kavramdır. Bazı kişisel veriler, ülkelerin milli hukuklarında ve uluslararası düzenlemelerde "hassas veri" olarak ifade edilmektedir. Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair 108 Sayılı Avrupa Konseyi Sözleşmesi'nin kimi maddelerinde *özellikli veri kategorileri* kavramı kullanılmıştır. 6689 sayılı 24.03.2016 tarihinde kabul edilen Kişisel Verilerin korunması Hakkında Kanun'da ise, "hassas veri" yerine "*özel nitelikli kişisel veri*" kavramı tercih edilmiştir. Görüldüğü üzere, kişisel verilerin çok çeşitli olması da çeşitli hukuk dalları ve düzenlemeler bağlamında terminolojik problemlere yol açmaktadır.

Bilişim teknolojilerinin gelişmesi ve internetin yaygınlaşması ile kişisel verilerin varlığı ve önemi ortaya çıkmıştır. Çok büyük sayılardaki kişisel verilerin çok küçük alanlarda ve aygıtlarda depolanabilmesi, bu verilerin kısa bir zamanda, kapsamlı olarak işlenebilmesi, bilgi kırıntılarından yola çıkılarak bireylerin saptanabilmesine ve devamında bireyin her türlü şahsi bilgisine erişilmesine yol açmaktadır. İşte kişisel veriler ile ilgili gerçek tehlikenin ortaya çıkış noktası da bu olmaktadır. Tehlikeli kişiler, kişisel verilere izinsiz erişebilmekte ve gerçek kişilerin kişisel bilgileri ile ilgili ciddi tehdit oluşturmaktadır.

Ceza hukuku disiplini bakımından kişisel verileri, suça konu olmasıyla sınırlı olarak inceleyeceğiz. Bu bağlamda, kişisel verilerin korunmasının ceza kanununda düzenlenmesinin gerekliliği ve Türk Ceza Kanunu'nda yer alan kişisel verilerin korunmasına ilişkin suçlar öncelikli olarak karşımıza çıkmaktadır. Öğretiye baktığımızda, veri koruma hukuku, kişisel verilerin kim tarafından, kimin için elde edildiğinin, kim tarafından hangi amaçla ve ne süreyle işleneceğinin, kim ya da kimlere aktarılacağı ve ne zaman yok edileceğinin öğrenilmesi hakkını içerir. Kişisel verilerin ele geçirilmesi yoluyla kişilik haklarının ihlal edilebileceği bir diğer durum, devletin resmi güvenlik kuruluşları dışında birçok kurum ve kuruluşun da bireyler hakkında özel bilgi toplaması ve kişilik haklarını bu bilgiler aracılığı ile ihlal etme olanağına sahip olmasıdır. Örneğin özel hastane ya da polikliniklerde çok özel

bilgiler sisteme işlenmekte ve sistemlere izinsiz erişimin sağlanması durumunda bireylerin tüm gizli bilgileri ele geçirilme tehlikesi ile karşı karşıya kalmaktadır. Kimlik hırsızlığı yoluyla kişiler mağdur edilmektedir. 2016 yılında kimlik hırsızlığının önemli bir örneği kamuoyuna yansımıştır. Facebook ve benzeri sosyal paylaşım sitelerinde, kullanıcıların sildiği mesaj ve resimlerinin sistemde saklı kaldığı ve kullanıcıların ciddi kişisel veri ihlal tehlikesi altında kaldığı ifade edilmiştir. Eleştiriler Almanya’da temel insan haklarını korumakla yükümlü olan Anayasa Mahkemesi’nde de gündeme gelmiş ve dönemin Anayasa Mahkemesi Başkanı Andreas Voßkuhle, verdiği röportajda, facebook kullanımının riskler taşıdığını, vatandaşların verilerini sildikten sonra da bunların facebook tarafından kayıt altında tutulup tutulmadığını bilmediklerini belirtmiştir. Facebook bunun üzerine, değişikliklere gitmiş ve kullanıcıların kendi bilgilerini paylaşırken daha dikkatli davranması adına çeşitli önlemler almıştır. Bu gelişmeler bilişim hukuku alanında yeni bir hakkın doğmasına yol açmıştır: Unutulma hakkı (right to be forgotten). Avrupa Adalet Divanı, unutulma hakkını tanıdığı ve tanımladığı *Google Spain SL, Google Inc v. Agencia Esponala de Protección de Datos* kararında bu konuda Avrupa Birliği Veri Koruma Direktifinin uygulamasına ışık tutacak nitelikte olduğu kabul edilen tespitlerde bulunmuştur.

Alanda var olan gelişmeler ve eleştiriler dikkate alınarak TCK’da, kişisel verilerin hukuka aykırı olarak kaydedilmesi, kullanılması veya açıklanması ve verilerin yok edilmemesi eylemleri ayrı maddeler halinde suç olarak düzenlenmiştir. Böylelikle ceza hukukumuzda önemli bir boşluk doldurulmuştur. Kişisel verilere ilişkin suç tipleri “*bilişim alanında suçlar*” başlıklı bölümde diğer suç tipleriyle bir arada değil, benzer hukukî değerlerin korunduğu “*özel hayata ve hayatın gizli alanına karşı suçlar*” bölümünde düzenlenmiştir. TCK’nın 135’inci maddesinde “kişisel verilerin kaydedilmesi suçu”, 136’ıncı maddesinde “verileri hukuka aykırı olarak verme veya ele geçirme suçu”, 137’inci maddesinde bu suçların nitelikli halleri, 138’inci maddede “verilerin yok edilmemesi suçu”, 140’ıncı maddede ise bu suçlara ilişkin olarak tüzel kişiler hakkında uygulanacak güvenlik tedbirleri düzenlenmiştir. Kişisel Verilerin Korunması Hakkında Kanun’un *Suçlar ve Kabahatler* başlıklı beşinci bölümünde yer alan *suçlar* başlıklı 17’inci maddesinde, “*Kişisel verilere ilişkin suçlar bakımından 26/09/2004 tarihli ve 5237 sayılı TCK’nın 135 ilâ 140 ıncı madde hükümleri uygulanır*” denilerek, anılan yasa çerçevesinde olsun olmasın kişisel verilere ilişkin haksızlıklar açısından TCK’ya atıf yapılmış ve 6698 sayılı Yasa ile TCK arasında bağlantı kurulmuştur. Bu bağlamda değerlendirilecek suçlar: TCK m.135-138’inci maddelerde düzenlenen kişisel verilerin kaydedilmesi suçu, verileri hukuka aykırı olarak verme veya ele geçirme suçu, verilerin yok edilmemesi suçudur.

**Anahtar Kelimeler:** Kişisel Veri, Özel Hayatın Gizliliği, Veri Koruma, Özel Hayata Karşı Suç, Verilerin Sahibi.