Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr Cilt:6 Sayı:1 Geliş:30.05.2024
Kabul:27.06.2024

Blok Zincir Teknolojisinde Kişisel Verilerin Korunması

Rabia Pelin, OPAN GÜNDAL
Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Öğrencisi
avpelingundal@gmail.com
ORCID ID : 0000-0002-1399-2745

ÖZ

Bilişim teknolojilerinin sürekli gelişmesiyle birlikte yeni bilişim sistemleri ortaya çıkmaktadır. Blok zincirler de bu yeni teknolojik sistemlerden birisidir. Blok zincirler, teknik bakımdan siber saldırılara karşı son derece dayanıklı, güvenilir, yapısal olarak değiştirilemeyen, kullanıcılarının hiçbir aracı kurum veya üçüncü kişiye ihtiyaç duymaksızın üzerinde işlemler gerçekleştirebildiği bir bilişim teknolojisi niteliğindedir.

Blok zincirlerde barınan verilerden bazılarının kişisel veri niteliğinde olması nedeniyle blok zinciri teknolojisi, kişisel verilerin korunması hukuku açısından incelenmelidir. Zira, blok zinciri teknolojisi, kişisel verilerin korunması hususunda bazı boşluklar barındırmaktadır ve bu boşluklar, kişisel verilerin korunması hukuku bakımından birtakım uyuşmazlıklara neden olabilecektir. Bu noktada blok zincirlerde korunması gereken kişisel verilere yönelik olan boşluklar ve bu nedenle yaşanabilecek sorunlar tespit edilerek çözülmesi gerekmektedir. Bu makalede öncelikle Türkiye ve uluslararası hukuk boyutunda düzenlenen kişisel verilerin korunması mevzuatları ışığında blok zinciri teknolojisi incelenecektir ve sonrasında kişisel verilerin korunması bakımından blok zincirlerde yer alan yaşanan sorunlar tespit edilerek çözüm önerileri belirtilecektir.

Anahtar Kelimeler: Blok Zincirler, Kişisel Verilerin Korunması, Kişisel Veriler, Dağıtık Defter Teknolojisi

Protection Of Personal Data In Block Chain Technology

ABSTRACT

With the continuous development of information technologies, new information systems emerge. Blockchains are one of new information technology that technically extremely resistant to cyber-attacks, reliable, unchangeable and on which users can perform transactions without the need for any intermediary institution or someone.

Since some of the data hosted in blockchains are personal data, blockchain technology should be examined in terms of personal data protection law. Because blockchain technology contains some gaps in the protection of personal data, therefore, blockchains cause problems in personal data protection law. Therefore, gaps in personal data that need to be protected in blockchains need to be identified and resolved. In this article, firstly, blockchain technology will be examined in the light of the personal data protection legislation regulated in Turkey and international law, then the problems in blockchains in terms of the protection of personal data will be identified and solution suggestions will be stated.
Keywords: Blockchains, Protection of Personal Data, Personal Datas, Distributed Ledger Technology.

Atıf Gösterme Opan Gündal, R. P., (2024). Blok Zincir Teknolojisinde Kişisel Verilerin Korunması, *Kişisel Verileri Koruma Dergisi. 6*(1), 28-47.

GİRİŞ

"Dijital çağ" olarak adlandırılan içinde bulunduğumuz çağda bilişim teknolojisi, kişilerin gündelik yaşamına birçok fayda ve kolaylık sunduğu için bilişim sistemlerinin türleri ve kullanımı günden güne artmaktadır. Blok zincirler (blockchains) de bu bağlamda ortaya çıkan teknolojilerden biridir.

Blok zincirler, Satoshi Nakamoto lakaplı bir kişi tarafından "Bitcoin" isimli kripto paranın ve yeni nesil bir ödeme şeklinin sunulması amacıyla yayınlanan bildiri metni sonucu hayatımıza giren bir teknolojik sistemdir. Günümüze gelindiğinde ise blok zincirler, Satoshi Nakamoto'nun belirttiği kullanım amacıyla sınırlı kalmayıp başkaca birçok alanda da yaygın olarak kullanılabilir duruma gelmiştir. Öyle ki, devletler dahi yapacakları seçimler ve oylamalarda veya e-devlet gibi uygulamalarda blok zincir teknolojisini kullanmayı tercih etmeye başlamıştır.

Blok zincirlerde herhangi bir sayı sınırına tabi olmaksızın, çok sayıda veri tutulabilmektedir. Bu verilerden bazılarının, ülkemizde yürürlükte olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK 2016) ile Avrupa Birliği tarafından kabul edilmiş olan 2016/679 sayılı General Data Protection Regulation (GDPR, 2016) anlamında kişisel veri olarak nitelendirilmesi mümkündür. Bu bakımdan söz konusu mevzuatlar nezdinde, blok zinciri teknolojisinde veri sorumlusu, veri işleyen gibi kavramların tespit edilmesi ve kişisel verilerin korunması hukuku açısından blok zinciri teknolojisinin irdelenmesi gerekmektedir. Zira, blok zincirlerde veri güvenliğinin sağlanması açısından kişisel verilerin korunabilmesi ve bu anlamda sorumlu olan süjelere getirilen yükümlülüklerin yerine getirilmesi için öncelikle veri sorumlusu ve veri işleyen süjelerinin tespit edilmesi elzemdir. İşte tam bu noktada, blok zincirlerde kişisel verilerin korunması hukukuna ilişkin olarak birtakım boşluklar ve sorunların mevcut olduğundan bahsetmek mümkündür.

Örnek vermek gerekirse, bazı blok zincirlerinin dağıtık ve herkesin erişimine açık yapısı dolayısıyla bu blok zincirlerde veri sorumlusu veya veri işleyen sıfatını haiz hiçbir süje dahi bulunmamaktadır. Buna bağlı olarak da kişisel verilerin korunması mevzuatlarıyla veri sorumlusu ve veri işleyenlere getirilen aydınlatma yükümlülüğü gibi önemli yükümlülükler yerine getirilemeyeceğinden dolayı ilgili kişilerin haklarının korunması bakımından ihlaller meydana gelecektir.

Bir başka örnek ise, blok zincirindeki bloklar ve bloklar üzerindeki verilerin değiştirilemeyen ve silinemeyen yapısı nedeniyle, KVKK ve GDPR'da yer alan düzenlemelerden örneğin kişisel verisi işlenen kişinin, hatalı veya eksik işlenen kişisel verilerinde düzeltme veya silme işleminin yapılmasını talebini veri sorumlusu süjesine iletmesi hakkının blok zincirler bakımından uygulanmasının mümkün olmamasıdır. Bu husus da yine blok zincirlerin kişisel verilerin korunması hukuku bakımından problemli olmasına yol açmaktadır. Ayrıca her ne kadar blok zinciri teknolojisinin güvenilir yapısından bahsetmek mümkünse de siber saldırıların hedefi olması da ihtimal dahilindedir. Ve bu siber saldırılar blok zincirlerde yer alan kişisel verilerin ihlal edilmesine de yol açabilmektedir. Tüm bu sebeplerden dolayı oldukça yaygın kullanılan blok zincir teknolojisinde kişisel verilerin korunmasına yönelik bu sorunların, blok zincirlerin yapısına ve ilgili kişilerin haklarına halel getirmeyecek en uygun şekilde üretilecek çözüm yöntemleriyle çözülmesi zorunlu hale gelmiştir.

Bu çalışmada öncelikle blok zincir teknolojisinin tarihçesinden kısaca bahsedilerek blok zinciri tanımlanmış; sonrasında blok zincirine ilişkin önemli kavramlar, blok zincirinin türleri ve özelliklerine değinilmiştir. Ardından da kişisel verilerin korunması hukuku bakımından blok zinciri teknolojisi ele alınmış olup, KVKK ve GDPR metinlerinde yer alan tanımlar blok zinciri bağlamında analiz edilmiştir. Eş zamanlı olarak da kişisel verilerin korunması noktasında blok zinciri teknolojilerinde mevcut olan boşluklar ve sorunlar tespit edilerek uygun çözüm önerileri sunulmuştur.

Bu çalışma ile ulusal ve uluslararası kişisel verilerin korunması mevzuatları incelenerek blok zinciri teknolojisinin Kişisel Verilerin Korunması Hukuku'na uyumlu olabilmesi hususu amaçlanmıştır.

BLOK ZİNCİR (BLOCKCHAIN) TEKNOLOJİSİ

Blok Zincir Teknolojisinin Ortaya Çıkışı

Blok zincirinin ortaya çıkışı, "Too big to fail" listesinde yer alan bir Amerikan bankasının 2008 yılında iflas etmesi üzerine yaşanan küresel çaplı bir ekonomik krizin ortaya çıkmasına dayanmaktadır. Söz konusu bankanın iflası ve tüm dünyada yaşanan ekonomik kriz nedeniyle, bankalara güvensizlik duyulmaya başlanmıştır. Bu sırada Satoshi Nakamoto takma adlı bir kişi, bankalar gibi aracı kurumları tamamen ortadan kaldırma fikrini ileri sürmüştür. Satoshi Nakamoto, bu iddiasını "Bitcoin: Eşler Arası Elektronik Ödeme Sistemi" başlıklı makalesinde yayımlayarak blok zincir teknolojisi adını verdiği bir sistem üzerinden gerçekleştirmeyi hedeflemiştir. (Nakamoto, 2008)

Satoshi Nakamoto, bahsolunan makalesinde, kriptografik ve özel bir şifreleme yöntemiyle korunan yeni bir ödeme sistemini ve Bitcoin adı verilen sanal bir para birimini tanıtmıştır. (Tekelioğlu, 2022)

Satoshi Nakamoto makalesinde yer verdiği bu yeni sistem sayesinde, hiçbir üçüncü kişiye (bir banka, finans kuruluşu ya da herhangi bir aracı fark etmeksizin) gerek kalmadan, tarafların birbirleriyle doğrudan ve oldukça güvenli bir sistemle ödeme yapabilmenin mümkün olduğu görüşünü öne sürmüştür.

Ayrıca Satoshi Nakamoto, tasarlamış olduğu bu teknoloji sayesinde, gerçekleştirilecek işlem maliyetlerinin düşeceğini ve ödeme sistemlerinde gerçekleşen dolandırıcılık faaliyetlerinin de büyük oranda önüne geçilebileceğini ileri sürmüştür. Satoshi Nakamoto tarafından tasarlanan bu blok zinciri ağının ilk bloğu ise 2009 yılında meydana getirilmiştir ve böylelikle blok zinciri teknolojisi ortaya çıkmıştır. (Öz Demetoğlu, 2019)

Günümüz çağında ise blok zincir teknolojisinin kullanım alanı, yalnızca kripto para akışını sağlamak ile sınırlı kalmamıştır. Zira blok zincir teknolojisi başkaca birçok alan ve sektörde yaygın olarak kullanılmaya başlanmıştır.

Blok Zincirin Tanımı

Blok zincir, içerisinde çok sayıda dijital verilerin barındığı her bir bloğun birbirine bağlanması suretiyle bir zincir meydana getiren teknolojik bir sistemi ifade etmektedir. Bir başka deyişle, blok zincirler, herhangi bir aracı veya üçüncü kişi bulunmaksızın, iki taraf arasında verilerin güvenli bir şekilde iletilmesi, depolanması ve yönetilmesi için oluşturulmuş, saydam ve doğrulanabilir, merkeziyeti bulunmayan bir sistemi ifade etmektedir. (Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu, 2022)

Blok zincirinin Türk Dil Kurumu tarafından yapılan resmi bir tanımı bulunmamaktadır. TÜBİTAK'a göre ise blok zinciri, "Dijital para birimlerini, varlıkları ve emtiaları besleyen ve mutabakatla güncellenen dağıtılmış bir veri tabanı ya da paylaşılmış kayıt (muhasebe) defteri içeren sistem" şeklinde ifade edilmektedir. (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, 2024)

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü'ne göre de blok zincirleri, "Dış müdahaleye dayanıklı, yetkisiz erişimi gösteren, dağınık (merkezi bir veri havuzu olmayan), bir kullanıcı

topluluğunun işlemlerini topluluk içerisinde paylaşımını sağlayan, değiştirilemez yapıda ve merkezi bir otoriteye dayanmayan dijital defterler" olarak tanımlanmaktadır. (Teperdijan, 2020)

Blok Zinciri Teknolojisine İlişkin Önemli Kavramlar

Blok zincir teknolojisini kavrayabilmek ve daha sonrasında kişisel verilerin korunması hukuku bağlamında inceleyebilmek için öncelikle birtakım önemli kavramların ele alınması gerekmektedir.

Bloklar

Blok zinciri sisteminde yapılacak bir işlemin aynı sistemdeki diğer taraflarca kriptografik olarak doğrulanmasıyla birlikte blok zincirini oluşturan kavrama blok denilmektedir. Bir blok zinciri ağını oluşturan ilk blok, başlangıç bloğu olarak adlandırılmaktadır. Zinciri oluşturan her blokta, blok başlığı, işlem kayıtları ve bir zaman damgası yer almaktadır. (Ünal, 2018) Zaman damgası sayesinde bloklar, kronolojik olarak sıralanmaktadır. (Öz Demetoğlu, 2019)

Blokların içerisinde yapılan işlemlerin her türlü içerik verisini barındıran kayıtlar bulunmaktadır. Kayıtlara örnek olarak, para akışı bilgisine veya müşterilere ait veriler gösterilebilir. Ayrıca kayıtların içerisinde kişisel veri niteliğinde bilgiler de yer alabilmektedir.

Hash Değeri

Zincirdeki blokların birbirinden ayırt edilebilmesini ve birbirlerine bağlanabilmelerini sağlayan değeri ifade etmektedir. Bu nedenle de hash değeri, blokların parmak izi gibi değerlendirilmektedir.

Hash değeri sayesinde bloklarda yer alan veriler, taraflar harici başka bir üçüncü kişinin anlayamayacağı derecede karmaşık olarak şifrelenmektedir. Öyle ki, bu şifreleme sisteminin örneğin bilgisayar korsanları tarafından kırılması, teknik olarak neredeyse imkansızdır. Blok zincirlerin bu şekilde korunaklı bir yapıya sahip olmasından dolayı da blok zincirler, güvenilir bir sistem olarak görülmektedir.

Düğümler (Nodes)

Blok zincir ağını çalıştırabilen bilgisayarlar, teknik anlamda "düğüm" olarak tanımlanmaktadır. Düğümler, dünyanın pek çok yerinde dağınık olarak bulunabilmektedir.

Dijital Cüzdanlar (Wallets)

Dijital cüzdanlar, paranın sanal boyutta tutulabilmesini ve takas edilmesini sağlayan bir yazılım sistemidir. (Tuvay, 2020) Bazı blok zincirinde yapılacak işlemler için mutlaka bir dijital cüzdana sahip olunmalıdır. (Aksoy, 2021)

Özel Anahtar ve Genel Anahtar

Blok zincirinde yapılacak işlemler için özel ve genel anahtara ihtiyaç duyulmaktadır. Özel anahtar, üçüncü kişilerle paylaşılmaması ve özenle saklanması gereken anahtardır.

Genel anahtar ise özel anahtarın aksine özenle saklanmasına ihtiyaç duyulmayan anahtarı ifade etmektedir. Özel ve genel anahtarlar kriptografik şifreleme yöntemi için kullanılırlar ve bu anahtarlar sayesinde blok zincir ağında taraflar işlemlerini, üçüncü kişilerden gizli olarak yapabileceklerdir.

Madenciler (Miners)

Madenciler, blok zincirindeki yapılan işlemlere onay verebilenleri ifade etmektedir. (Öz Demetoğlu, 2019) Madenciler, blok zincirinin bir kopyasını, sisteme eriştikleri cihazlarda saklama yetkisine sahiptir. (Forensis, 2020)

Mutabakat Mekanizması

Bir blok zincir sisteminde tarafların blok zincir üzerindeki yapacakları işlemler konusunda aralarında bir mutabakatın bulunması gerekmektedir. Zira, mutabakat mekanizması sayesinde ilgili blok zincir sisteminde yeni bir blok oluşturmak için birtakım kurallara uyulması belirlenmiştir. (Öz Demetoğlu, 2019)

Protokol

Blok zincir sistemini yöneten birtakım kurallar ve yükümlülüklere protokol denilmektedir. Blok zincir sistemlerinde protokoller sayesinde kullanıcıların yaptığı işlemler doğrulanmaktadır.

Akıllı Sözleşmeler

Blok zinciri teknolojisinde akıllı sözleşmeler kullanılmaktadır. Bu nedenle akıllı sözleşmeler blok zinciri teknolojisinde temel kavramlardan birisidir. Akıllı sözleşmeler, düğümler (nodes) aracılığıyla yazılım kodları ile oluşturulan, güvenilir, merkeziyetsiz, otomatik çalışan ve blok zinciri teknolojisinde gerekli olan protokolleri kullanan yeni nesil dijital sözleşmelerdir. (Durdu- Gökçe, 2022)

Blok Zincir Teknolojisinin Özellikleri

Blok zincirleri, çok fazla veri barındıran aracısız, merkezsiz ve dağıtık bir veri kayıt sistemdir. Bu bağlamda taraflar hiçbir aracıya, merkeze veya üçüncü bir kişiye ihtiyaç duymaksızın doğrudan, eşler arası olarak işlem gerçekleştirebilmekte ve doğrulayabilmektedir. (Iansiti- Lakhani, 2017) Bununla birlikte blok zincirin doğası gereği, işlemlerin yürütüldüğü süreç, otomatik olabilmektedir. Bir başka deyişle blok zincirlerine otomatik olarak yeni bloklar eklenebilmektedir. Bu noktada blok zinciri teknolojisinin bir yandan işlem maliyetlerini azalttığı sonucuna ulaşmak mümkün iken bir yandan da blok zincirlerin çalışabilmesi için çok fazla enerji ve oldukça pahalı cihazlara ihtiyaç olduğu sonucuna ulaşmak mümkündür. (Tanrıverdi-Uysal vd., 2019)

Blok zinciri sistemi, şeffaftır. Bir başka deyişle, blok zinciri ağında yapılan işlemler veya tutulan veriler, ağa erişim sağlayabilen herkes tarafından görüntülenebilmektedir. Bu bakımdan blok zincirinin dağıtık bir sistem olduğu ve hatta blok zinciri sisteminin adeta bir "Dağıtık Kayıt Defteri" olduğunu da vurgulamak gerekmektedir. Blok zincirinin dağınık ve merkezsiz oluşu, sistemde gerçekleştirilen tüm işlemlere ait kayıtların tek bir merkezde değil de sisteme erişebilen tüm katılımcıların "düğüm" adı verilen bilgisayarlarında tutulabilmesini ifade etmektedir. Blok zincirin dağıtık olması nedeniyle verilerin kaydedildiği sistemin aynı anda birden çok bilgisayarda bulunması, dağıtık olmayan yani merkezli bir veri tabanı sistemine göre daha güvenlidir. (Usta- Doğantekin, 2018) Zira, blok zincir ağına bağlanabilen düğümlerin ayrı ayrı siber saldırıya uğraması, tek bir merkezi olan bir sisteme nazaran çok daha güçtür; hatta neredeyse imkansızdır. Bununla birlikte blok

zincirindeki blokların birbirine kriptografik, karmaşık ve özel bir şifreleme metoduyla bağlı olması da blok zincirlerde veri bütünlüğü ve güvenliğinin sağlanmasında önemli bir işleve sahiptir. Ancak yine de blok zincir sistemlerinin en bilindik örneklerinden olan kripto para borsaları, saldırıya uğrayabilmektedir. Örneğin bilgisayar korsanları, Japonya'da faaliyet gösteren Mtgox adlı kripto para borsasına 2014 yılının mart ayında siber saldırı düzenlemiştir ve 450 milyon dolarlık Bitcoin çalmıştır. Başka bir örnek vermek daha gerekirse, 2016 yılında bir blok zincir olan "Decentralized Autonomous Organization (DAO)" sistemi siber saldırıya uğramıştır. (Li, 2020) 2022 yılında da kripto paralara yönelik gerçekleştirilen siber saldırılar neticesinde yaklaşık 3,7 milyar dolar değerinde hırsızlık gerçekleştirilmiştir. Dolayısıyla blok zincirlerinde de güvenlik açıkları bulunduğu görülmektedir.

Blok zincirindeki bloklar, değiştirilemez yapıdadır. Blok zincirin bu özelliği, bloklar oluşturulduktan sonra blokların içerisinde yer alan kayıtların hiçbir şekilde değiştirilememesini ifade etmektedir. (Ünal- Uluyol, 2020) Buna ek olarak, blok zincirinin yapısının zincirde herhangi bir kopma durumuna mahal vermediğine ve bunun sonucu olarak zincirdeki bloklara işlenen bir verinin süre sınırlaması bulunmaksızın sistemde tutulabildiğine de değinmek gerekmektedir.

Blok Zincir Türleri

Blok zincir sistemlerinin erişilebilirliklerine göre üç çeşidi bulunmaktadır: Herkesin erişebildiği blok zincirler, açık blok zincir olarak adlandırılmaktayken; erişimi sınırlı olanlar, kapalı blok zincir olarak ifade edilmektedir. (Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu, 2022) Üçüncü olarak ise açık ve kapalı blok zincirlerin karışımı olan hibrit blok zincirler mevcuttur.

Açık Blok Zincir

Herkesin erişim sağlayabileceği ve blok zincirdeki verileri görebileceği algoritmayla işleyen sisteme açık blok zinciri denilmektedir. (Mingxiao- Xiaofeng vd., 2017) Açık blok zincirinin temel özelliği, katılımcıların anonim veya takma adlı olmasına olanak tanımasıdır. Bununla birlikte özellikle açık blok zincirleri, kullanıcılarıyla bağlantı kurulamayan bir yapıdadır. (Narayanan- Arvind vd., 2016) Açık blok zincirinin izne tabi olup olmamasına göre de iki alt türü vardır: (Usta- Doğantekin, 2018)

İzne Tabi Olmayan Açık Blok Zincirler

Bu tür blok zincirlerde sisteme girmek, verilere erişmek ve zincirde yeni blok oluşturabilmek için bir izne ihtiyaç bulunmamaktadır. Bu tür açık blok zincirler hem açık yapıda olmaları hem de ayrıca bir izne de tabi olmamaları nedeniyle sisteme oldukça çok sayıda katılımcının blok zincirde taraf olmasını sağlamaktadır. Bu sayede de bu blok zincirler, siber saldırıya uğrama riski bakımından daha güvenilir bir yapıdadır. Bitcoin ağı, bu grupta yer alan örneklerden birisi olarak gösterilebilir.

İzne Tabi Olan Açık Blok Zincirler

Bu tür blok zincirler, herkesin erişimine açıktır ancak mutabakat mekanizması içerisinde yer almak ve zincire yeni blok ekleyebilmek için otoriteden izin alınmasını gerektirmektedir. Örnek olarak, müzik paylaşılabilen ve dinlenebilen bir blok zincir algoritmasındaki tüm katılımcıların bu sistem üzerinden müzik dinleyebileceği ancak sadece belirli kişilerin buraya parça yükleyebildiği bir blok zincirini gösterebiliriz. (Usta- Doğantekin, 2018)

Kapalı Blok Zincir

Bu tür blok zincirler, açık blok zincirlerin aksine, kontrollü ve kısıtlı bir erişim sistemine sahiptir. Kapalı blok zincirleri, güvenlik veya başka herhangi bir gerekçeden kaynaklı olarak ilgili blok zincirde yer alan verilerin başkalarının erişmemesi için kullanılmaktadır. Kapalı blok zincirindeki katılımcılar, yine açık blok zincirinin aksine anonim değildir ve kimlikleri belirlenebilir.

Hibrit Blok Zincir

Bu tür blok zincirler, herkesin erişimine açık olması yönüyle açık blok zincirlere benzerken aynı zamanda bu sistem içerisinde belirli verilere herkesin erişimine açık olmaması ve izinle girilebilmesi yönünden kapalı blok zincirlere benzemektedir. (Akdemir Altınbaşak, 2018) Açık ve kapalı blok zincirlerin özelliklerini aynı anda taşıdığı için de hibrit blok zincirler olarak anılmaktadır. Hibrit blok zincirlerinin bu özel yapısı sayesinde bu sistemlere "51 saldırısı" olarak bilinen siber saldırı düzenlenmesi mümkün değildir.

Blok Zincir Teknolojisinin Kullanım Alanları

Yukarıda belirtildiği üzere blok zincirinin çıkış noktası, Bitcoin'e yani kripto para birimlerine dayanmaktadır. Ancak blok zincirinin içinde bulunduğumuz dijital çağ bakımından güvenilir ve düşük maliyetli bir bilişim sistemi olması sebebiyle kullanım alanı günden güne yaygınlaşmaktadır. Öyle ki, blok zinciri teknolojisi hemen hemen her alanda kullanılabilmektedir. Bu bakımdan günümüzde blok zinciri teknolojisinin dijital kimlikler, telif kayıt sistemleri, tedarik zinciri yönetimi, tapu sistemi, noterlik uygulamaları ve seçimler gibi birçok alanda kullanılabildiğinden bahsetmek mümkündür. Bu hususla bağlantılı olarak da blok zincirlerde yer alan verilerin güvenliğinin sağlanması gerekmektedir.

BLOK ZİNCİR TEKNOLOJİSİ VE KİŞİSEL VERİLERİN KORUNMASI HUSUSU

Kullanım alanı günden güne yaygınlaşan blok zinciri teknolojisi, olumlu yönlerinin yanında birtakım olumsuz yönleri de bünyesinde barındırmaktadır. Bu noktada adeta bir "elektronik veri bankası" niteliğindeki blok zincir teknolojisinde işlenen veya işlenecek kişisel verilerin korunması hususu, özellikle önemli bir konu teşkil etmektedir.

Kişisel Verilerin Korunmasına İlişkin Mevzuatlar

Blok zincir teknolojisinde kişisel verilerin korunması hususu hem Türk Hukuku hem de uluslararası hukuk kapsamında incelenecektir. Dolayısıyla Türk hukuku ve uluslararası hukuk kapsamında Avrupa Birliği ile Avrupa Konseyi hukukunda yer alan kişisel verilerin korunmasına ilişkin mevzuatlar ve başkaca diğer düzenlemeler çerçevesinde blok zinciri teknolojisi ayrı ayrı ele alınacaktır.

Avrupa Birliği Hukukunda Yer Alan Düzenlemeler

Avrupa Birliği'nde kişisel verilerin korunmasına yönelik atılan ilk adım 1995 yılında kabul edilen "Veri Koruma Direktifi"dir. Ardından 1998 yılında "95/46EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif" metni yayınlanmıştır. Avrupa Birliği tarafından en son yapılan düzenleme ise 2018 yılında yürürlüğe giren 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) metnidir. (Kişisel Verileri Koruma Kurumu, 2024)

GDPR, bir yandan kişisel verilerin Avrupa Birliğine üye olan çeşitli ülkeler arasında serbest dolaşımını kolaylaştırmayı amaçlarken diğer yandan da Avrupa İnsan Hakları Sözleşmesi'nin 8.

maddesini esas alarak kişisel verilerin korunması hakkını güvence altına almayı amaçlamaktadır. Bu bağlamda GDPR, veri sorumlularına birtakım yükümlülükler getirmiş; veri işleme araçlarını ve amaçlarını belirlemiş ve kişisel verilerin korunması için düzenlemeler getirmiştir.

Avrupa Konseyi Tarafından Getirilen Düzenlemeler

Avrupa Konseyi tarafından hazırlanan ve ülkemizin de taraf olduğu 1953 tarihli "İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi"dir. Sonrasında ise 1981 yılında 108 sayılı "108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" yürürlüğe girmiştir. Ayrıca Konsey tarafından bu sözleşmenin esas ve usul bakımından nasıl uygulanacağı bakımından yol gösteren 20 tavsiye kararı da çıkarılmıştır. 2001 yılına gelindiğinde ise Avrupa Konseyi tarafından "181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol" çıkarılmıştır. Bu düzenlemelerin yanı sıra Avrupa İnsan Hakları Sözleşmesi'nin "Özel ve Aile Hayatına Saygı Hakkı" başlığıyla kaleme alınan 8. Madde kapsamında da kişisel veriler korunmaktadır.

Diğer Düzenlemeler

Uluslararası alanda kişisel verilerin korunması hususuna ilişkin olarak Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) tarafından 1980 tarihli "OECD'nin Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri" ile Birleşmiş Milletler tarafından 1990 yılında yayımlanan "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" de önem arz eden diğer metinler olarak karşımıza çıkmaktadır. (Kişisel Verileri Koruma Kurumu, 2019)

Türk Hukukunda Yer Alan Düzenlemeler

Ülkemizde kişisel verilerin korunması bağlamında ilk olarak 1981 yılında "108 sayılı Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" imzalanmıştır ve bu sözleşme 1985 yılında yürürlüğe girmiştir. Fakat bu sözleşmenin hukuk sistemimize entegre edilmesi oldukça uzun bir süreden sonra gerçekleşmiştir. (Öz Demetoğlu, 2019) Bu süre zarfında, kişisel verilerin korunması bağlamında ayrıca bir kanun metni bulunmadığı için bu husus ancak Anayasamızın 20. maddesinde yer alan "özel hayatın gizliliği" başlıklı hüküm kapsamında ele alınmıştır.

Anayasa, bahsi geçen maddesi ile bireylere açık rızaları ve kanuna uygun şekilde işlenecek kişisel verileri hakkında bilgi verilmesi, gerektiğinde işlenen kişisel verilerinin düzeltilmesi, silinmesi ya da korunmasını talep etme hakkı vermektedir. Kişisel verilerin normlar hiyerarşisinin en üstünde yer alan anayasamızda korunmasının yanı sıra 2016 yılında KVKK'nın yürürlüğe girmesiyle kapsamlı bir düzenlemeye konu edilmiştir ve ayrı bir mevzuat ile de güvence altına alınmıştır.

Kişisel verilerin korunmasına ilişkin olarak ayrıca 5237 sayılı Türk Ceza Kanunu'nda (TCK) da birtakım düzenlemeler bulunmaktadır. Bu kanunda kişisel verilere yönelik işlenen suçlar belirtilmiş ve buna ilişkin cezalara yer verilmiştir. Bu bağlamda TCK, kişisel verilere yönelik işlenecek suçların cezalandırılmasını düzenlediği için TCK da kişisel verilerin korunması hususuna işlev sağlayan mevzuatlar arasında yer almaktadır.

KVKK ve GDPR Metninin Uygulanma Alanları

KVKK'nın 2. maddesi uyarınca bu metinde yer alan hükümler, kişisel veri niteliğindeki verileri işlenen gerçek kişiler ile yine kişisel verileri otomatik olarak işlenmekte olan veya otomatik olup

olmaması fark etmeksizin veri kaydı yapılabilen bir sisteme işlenen gerçek ya da kamu veya özel tüzel kişisi ayrımı yapılmaksızın tüm tüzel kişiler bakımından uygulanmaktadır. Ancak değinmek gerekir ki, KVKK yalnızca Türkiye sınırları içerisinde kişisel veri işleyenlere sorumluluklar yüklemiştir.

GDPR da 2. maddesinin 1. fıkrasında KVKK hükmüne çok benzer olarak uygulama sınırlarını belirtmiştir. Ancak GDPR metni KVKK'na göre daha kapsayıcı bir alana sahiptir. Zira, GDPR sadece Avrupa Birliğine üye olan devletler bakımından değil; üye olmayan devletler için de uygulanabilmektedir.

Değinmek gerekir ki, özellikle açık ve izin gerektirmeyen blok zincir ağlarındaki veriler, sistemdeki tüm kullanıcılar tarafından kayıt altına alınabilmekte ve dünyanın birçok yerinde bulunan düğümlerde dağıtık olarak kopyaları tutulabilmektedir. Diğer bir deyişle, blok zincirlerdeki veri sorumlusu ve veri işleyenler dünyanın farklı farklı yerlerinde bulunabilmektedir. Dolayısıyla da blok zincir teknolojisinde işlenen kişisel veriler konusunda bir ihtilaf söz konusu olduğu zaman hangi ülkenin mevzuatının uygulanacağının tespiti konusunda soru işaretleri bulunmaktadır ve bu husus tartışmalı bir konudur.

Kişisel Verilerin Korunması Hukuku Bağlamında Yer Alan Tanımlar ve Blok Zinciri Bağlamında Değerlendirilmesi

Kişisel Veri

KVKK'da yer alan en temel kavram, söz konusu kanunun 3. maddesinin 1. fıkrasının d bendinde tanımlanan "kişisel veri" kavramıdır. Zira KVKK, bir veriyi kişisel veri olduğu takdirde koruma altına alacaktır. KVKK'nun ilgili hükmüne göre kişisel veri, bir kişinin kimliğinin belirlenmesini sağlayabilecek herhangi bilgi anlamına gelmektedir. KVKK'nun gerekçesinde ise kişisel veri daha detaylı olarak tanımlanmıştır. Kanunun gerekçesine göre kişisel veri, somut içeriğe sahip olan ve bir kişinin fiziksel, ailevi, ekonomik, kültürel veya sosyal herhangi bir bilgisi olabilmektedir. Bu kapsamda kişilerin telefon numarası, ismi, özgeçmiş bilgisi, biyolojik bilgileri, araç plakası gibi verilerinin de kişisel veri niteliğinde kabul edileceği gerekçe metninde açıkça belirtilmiştir. KVKK'ya paralel olarak GDPR metninde de kişisel veri kavramı tanımlanmıştır ancak burada daha net ve kapsamlı olarak düzenlenmiştir. GDPR'a göre kişisel veri, doğrudan bir kişinin kimliğinin belirlenmesini sağlayan fiziksel, zihinsel, kültürel gibi herhangi bir verisi olarak tanımlanmıştır. Ayrıca GDPR'a göre şifrelenerek bir ağda depolanan veriler, takma adlı (psödonim) veri olarak nitelendirilmektedir. Bu kapsamda GDPR'a göre ilgili kişilerin psödonim verileri de kişiyi belirlenebilir kıldığı için kişisel veri olarak kabul edilmektedir. Söz konusu mevzuatlarda kişisel verilerin yalnızca gerçek kişilere ait olabileceği düzenlenmiş olduğundan dolayı tüzel kişilerin kişisel verisinin söz konusu olması mümkün değildir.

Blok zincir teknolojilerinde kişisel verilerin korunması hususuna değinmeden önce ilk olarak blok zincirlerde tutulan verilerin kişisel veri niteliğinde olup olmadığının tespiti gerekmektedir. Elbette, blok zincirlerde yer alan her veri, kişisel veri niteliğinde değildir. Ancak değinmek gerekir ki, blok zincir teknolojisi en başta her ne kadar gizlilik ve anonimlik vaadiyle ortaya çıkmış olsa dahi, bloklarda yer alan kayıtlarda kişisel veriler de yer alabilmektedir. Zira, blok zincirlerde tutulan veriler, KVKK ve GDPR'da tanımlandığı şekilde bir kişinin kimliğini belirlemeye yarayan kişisel verisi niteliğinde olabilmektedir. Diğer bir deyişle, bir blok zincirinde yer alan düğümlerde, kişisel veriler işlenebilmektedir.

Örneğin, bir blok zinciri sistemindeki bir kullanıcının takma adı niteliğindeki genel anahtarı veya gerçekleştirdiği işlem bilgileri, o kullanıcının kimliğini belirleyebilecek nitelikteyse söz konusu veriler, kişisel veri olarak kabul edilecektir. Veyahut başka bir örnek olarak, bir blok zincir ağına

katılım için öncelikle bir kayıt yapmak gerekiyorsa ya da söz konusu blok zincir sisteminde belirli kişi veya kuruluşlar tarafından katılımcılara özel anahtarlar veriliyorsa, burada yer alan veriler sayesinde gerçek kişi katılımcıların kimliği belirlenebileceğinden bu kişilere ait verilerin de yine kişisel veri olarak nitelendirilecektir. (Öz Demetoğlu, 2019)

Kişisel veri niteliğinde veriler barındıran blok zincir sistemleri söz konusu olduğu takdirde, bu verilerin korunması gereksinimi ortaya çıkacaktır. Bu gereksinim, KVKK'nun 6. maddesinin 1. fıkrasında düzenlenen özel nitelikli kişisel veri olması halinde daha elzem bir husustur. Ayrıca bu takdirde blok zincire işlenecek kişisel verilerin KVKK'nun 4. maddesinin 2. fıkrasında yer alan genel ilkelere uygun olarak işlenme zorunluluğu da doğacaktır. Fakat burada blok zincirinin yapısından dolayı sorunlu noktalar bulunmaktadır. Zira, blok zinciri teknolojisinin herhangi bir kopukluğa izin vermeyen yapısı olduğundan dolayı, blok zincire işlenen veriler, bir süre kısıtlamasına tabi olmaksızın daima zincirde kalmaktadır. Değinmek gerekir ki, KVKK'nın 4. maddesinin 2. fıkrasının d bendi hükmüne göre kişiler verilerin ancak amaca uygun bir saklama süresi zarfında muhafaza edilmesi söz konusudur. Dolayısıyla bu noktada blok zinciri sisteminin söz konusu KVKK hükmüyle çatıştığı açıkça görülmektedir.

Değinildiği üzere, madenciler blok zinciri sisteminde yer alan verilerin bir kopyasını kendi düğümlerinde de tutmaktadır. Bununla bağlantılı olarak, ilgili blok zinciri sistemindeki kayıtların çok sayıda kopyasının dünyanın çeşitli yerlerinde bulunması mümkündür. Bu husus da blok zinciri kullanıcılarının kişisel verilerinin güvenliğini açısından risk oluşturmaktadır. Zira örneğin, ilgili kişinin blok zincirinde tutulan kişisel verilerine kimlerin eriştiğini öğrenebilmesi olası değildir. Bununla birlikte, özellikle açık blok zincirlerin herkesin erişimine açık yapıda olması nedeniyle, ilgili kişinin açık rızası alınmadan işlenen kişisel verilerinin alenileşme riskiyle karşı karşıya olduğunu da belirtmek gerekmektedir. Bu husus da yine KVKK'nun lafzı ve ruhuyla çelişen bir durumdur.

Kişisel Verilerin İşlenmesi

Kişisel verilerin işlenmesi hususu, KVKK'nın 3. maddesinin 1. fıkrasının e bendinde ayrıntılı olarak düzenlenmiştir. Bahsi geçen hükme göre kişisel verilerin işlenmesi, veri kaydedilen sistemlere bireylerin kişisel verilerini kaydetmek, depolamak, muhafaza etmek, değiştirmek, aktarmak vb. gibi eylemler aracılığıyla mümkündür. Kişisel verilerin işlenmesi hususu, GDPR metninde de 4. maddesinin 2. Fıkrasında benzer eylemler üzerinden tanımlanmıştır. Ek olarak hem KVKK hem de GDPR'da kişisel verilerin işlenmesi hususunda, kişisel verilerin yalnızca amaca uygun olarak işlenebileceğine ilişkin bir yükümlülük de düzenlenmiştir. (Kaya, 2015)

Blok zincirlerde otomatik yollarla veya değil fark etmeksizin KVKK ve GDPR anlamında kişisel veri işlenmesi mümkündür. Zira, blok zincirin yapısı gereği, zincirdeki bloklara veri aktarıldığı zaman bu veri bloklara kaydedilmekte, depolanmakta ve muhafaza edilmektedir. Blok zincirlere kişisel veri işlenebileceğinden dolayı blok zincirlerde yer alan kişisel verilerin korunması gerekmektedir.

İlgili Kişi

İlgili kişi, KVKK'nda tanımlanan süjelerden biridir. KVKK'na göre, ilgili kişi kişisel verisi işlenen gerçek kişi olarak tanımlanmaktadır. Bu bakımdan kanunda yer verilen ilgili kişi tanımına tüzel kişiler dahil edilmemiştir.

Blok zincir özelinde ise ilgili kişi süjesi, açık veya kapalı blok zincirlerine göre ayrıca değerlendirilmelidir. Açık blok zincirlerinde ilgili kişi, anonim veya takma adlı katılımcılar olabilir. Açık blok zincirlerinde her ne kadar anonim veya takma adlı kullanıcılar yer alıyor olsa dahi kimliklerini belirlemeye yarayacak verilerin bulunması mümkündür. Diğer bir deyişle, blok

zincirlerde mutlak bir anonimlik söz konusu değildir. (Çağlayan Aksoy- Aksoy, 2023) Bu durumda KVKK kapsamında kişisel verisi işlenen ilgili kişi veya kişilerin mevcudiyeti söz konusu olacaktır. Aynı şekilde kapalı blok zincirlerde de elbette kişisel verileri işlenen ilgili kişi veya kişilerin bulunması olasıdır.

KVKK'nun 11. maddesinde ilgili kişinin kişisel verilerinin korunmasına yönelik olarak sahip olduğu birtakım haklar bulunmaktadır. Ancak blok zinciri teknolojisinin teknik yapısı nedeniyle ilgili kişinin sahip olduğu bu hakların kullanılması ve kişisel verilerinin korunması noktasında problemler bulunmaktadır. Örneğin blok zinciri teknolojisinin dağıtık yapısı nedeniyle, ilgili kişinin blok zinciri sisteminde kişisel verilerinin işlenip işlenmediğini veya kişisel verilerinin hangi düğümlerde tutulduğunu öğrenmesi; işlenen kişisel verileri hakkında bilgi talep edebilmesi; kişisel verilerinin söz konusu blok zincir sisteminde amacına uygun olarak kullanılıp kullanılmadığını öğrenmesi; kişisel verilerinin yurt içinde veya yurt dışında fark etmeksizin aktarıldığı üçüncü kişileri bilmesi pek mümkün değildir. Bu husus da blok zincirinin KVKK ve GDPR özelinde yine problemli olmasına yol açmaktadır.

Ayrıca ilgili kişinin GDPR ve KVKK hükümlerine dayanarak blok zincirinde yer alan kişisel verilerinin silinmesini, yok edilmesini veya bir eksiklik ya da yanlışlık söz konusuysa bunların düzeltilmesi için talepte bulunması da mümkün değildir. Zira, örneğin kişisel verilerin silinmesi, bu verilere hiçbir şekilde tekrar erişilememesini ve kullanılamaması sonucunu doğuran bir işlemdir. Ancak blok zincirinin teknik yapısı dolayısıyla bloklarda yer alan hiçbir verinin silinmesi veya yok edilmesi mümkün olmadığından dolayı ilgili kişinin bu hakkını kullanamaması da söz konusu olacaktır.

Yine kişisel verilerin yok edilmesi ise, geri getirilemeyecek şekilde bu verilere hiçbir surette erişim sağlanamamasını ifade eden bir işlemdir. Bu bağlamda, blok zinciri sistemlerinin değiştirilemez, silinemez veya yok edilemez yapıda olmasından kaynaklı olarak, bu madde kapsamındaki unutulma hakkı ile söz konusu verilerin doğruluğu ve güncelliğinin sağlanması noktasına problemler bulunmaktadır. (Diri-Yalçınkaya, 2022)

Son olarak blok zincirinin değiştirilemeyen ve zincirde kopukluk yaşanmasına izin vermeyen yapısı nedeniyle, KVKK'nın 7. maddesi bağlamında ilgili kişinin blok zinciri sisteminde yer alan kişisel verilerinin silinmesini, yok edilmesini veya anonim hale getirmesini talep etmesi de mümkün değildir. (Diri-Yalçınkaya, 2022) Dolayısıyla blok zinciri sistemi, KVKK ve GDPR kapsamında güvence altına alınmış olan ilgili kişinin haklarının korunması konusunda problemli hususları barındırmaktadır.

Veri Sorumlusu

Veri sorumlusu, KVKK'nın 3. maddesinin 1. fıkrasının ı bendinde tanımlanmıştır. Buna göre KVKK kapsamında, Türk vatandaşı olma şartı aranmaksızın herhangi bir kişi, bir veri tabanını oluşturma, yönetme ve verilerin işlenmesi hususunu belirleme yetkisine sahip olduğu takdirde veri sorumlusu niteliğini haizdir. GDPR'da veri sorumlusuna karşılık gelen kavram, veri denetleyicisi olarak ifade edilmiş olup; veri sorumlusunun tanımı KVKK'daki hükümle benzer olarak düzenlenmiştir.

KVKK ve GDPR kapsamında veri sorumlusu, önemli yükümlülüklere tabi tutulan bir süjedir. Bu bağlamda blok zinciri sistemlerinde bu yükümlülüklere tabi olanların belirlenebilmesi zaruridir. Buna göre öncelikle blok zinciri sisteminde hangi aktör veya aktörlerin veri sorumlusu olarak kabul edilebileceğinin belirlenmesi gerekmektedir.

Blok zincir teknolojisinde veri sorumlusunun tespiti, esasında blok zincir türüne göre farklılık arz etmektedir. Kapalı blok zincirlerde veri sorumlusunun tespiti daha kolaydır. Zira, kapalı blok zincirler genellikle bir kişi veya kurum tarafından kurulacağı, yönetileceği için ve ayrıca bu kişi veya kurumun sisteme erişim izni verme yetkisine sahip olacağı için bahsi geçen kişi veya kurum, KVKK kapsamında veri sorumlusu niteliğindedir. (Kaufmann, 2018)

Açık blok zincirlerinde ise sistemdeki veriler, merkezi olmayan ve dağıtık bir sistemde tutulduğundan dolayı bu tür blok zincirlerinde veri sorumlusunun tespiti güçtür. (Öz Demetoğlu, 2019) Bir başka deyişle, bu ortamda kişisel verilerin işlenmesinin amaç ve araçlarını belirleyen tek bir kişi veya kuruluş bulunmadığından veri sorumlusunun kim olacağı konusunda problemler mevcuttur.

Açık blok zincirlerinde yer alan aktörlerin (blok zincir protokolü geliştiriciler, düğümler, madenciler, kripto para borsaları ve cüzdanlar) ayrı ayrı ele alınarak veri sorumlusu olarak değerlendirilip değerlendirilemeyeceği hususuna değinilmesi gerekmektedir. Açık blok zincirlerde protokol geliştiricisi, yalnızca kişisel verileri işlenebileceği bir sistem oluşturarak vasıta belirlemektedir. Bu noktada protokol geliştiriciler veri sorumlusu olarak değerlendirilemezler. (Öz Demetoğlu, 2019; Ibáñez- O'hara vd., 2018) Aynı şekilde madenciler de veri sorumlusu niteliğini haiz değildir. Zira, madenciler, ilgili blok zincir ağında yer alan kişisel veri niteliğindeki verilerin işlenmesinin amaçlarını ve araçlarını belirleme yetkisine sahip değillerdir.

Açık blok zincirlerindeki düğümlerin veri sorumlusu olup olamayacağı noktasında, öncelikle düğümlerin birbirlerinden habersiz ve bağımsız olarak çalıştığı gözetildiğinde tek başlarına veri sorumlusu olarak nitelendirilemeyecektir. Genel olarak bakıldığında ise, düğümler yoluyla katılımcılar, sistemdeki verilere doğrudan erişmekte ve doğrulamaktadır. Sonuç olarak ise blok zincirinde yer alan düğümler, blok zincir sisteminde tutulan kişisel verilerin işleme amaç ve vasıtalarını belirleyemediği için veri sorumlusu olarak da nitelendirilemeyecektir. (Karatay- Solak vd., 2020)

Son olarak, açık blok zincirlerinde rol oynayan aktörlerden olan kripto para borsaları ve cüzdanlarının da veri sorumlusu olup olamayacağının incelenmesi gerekmektedir. Kripto para borsaları ve cüzdanlar, kullanıcıların kripto paralarını saklama işlevine sahiptir. Söz konusu kripto para borsaları ve cüzdan sistemlerini oluşturan kişi veya kurumlar, KVKK ve GDPR nezdinde veri sorumlusu olma koşulunu sağlamaktadır. Zira, bahsi geçen borsa ve cüzdanlar, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyebilmekte ve veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu tutulabilmektedir. Dolayısıyla da kripto para borsaları ve cüzdanlar, açık blok zincirlerinde veri sorumluları niteliğini haiz olabilecektir. (Öz Demetoğlu, 2019) Özetle, açık blok zincirlerinde protokol geliştiricileri, madenciler, düğümler, katılımcılar, KVKK ve GDPR nezdinde veri sorumlusu olamaz iken; kullanıcıların sistemdeki etkileşimini sağlayan ve aynı zamanda verileri depolayan kripto para borsaları ve cüzdanlar, veri sorumlusu sıfatını haiz olabilmektedir.

KVKK, veri sorumlusu niteliğindeki süjeye, işledikleri kişisel veriler hakkında ilgili kişilere bilgi vermek ve aydınlatmak; kişisel verilerini işledikleri ilgili kişilerin talebi halinde onların kişisel verilerini silmek, yok etmek veya anonim hâle getirmek, Veri Sorumluları Siciline kaydolmak gibi yükümlülükler yüklemektedir. GDPR metni de KVKK'na benzer olarak, veri sorumlusuna birtakım yükümlülükler getirmiştir. Bu bakımdan KVKK ve GDPR metinleri, veri sorumlusuna getirdikleri bu yükümlülükler ile kişisel verilerin korunmasını hedeflemektedir. (Öz Demetoğlu, 2019)

KVKK'nın 10. maddesi bağlamında veri sorumluları veya temsilcileri, ilgili kişilerin kişisel verilerini elde ederken onları aydınlatmakla yükümlendirilmiştir. Kanunun bu hükmü gereğince kapalı blok zincirler bakımından da veri sorumluları, kişisel verilerini işleyecekleri kişileri bu hususa ilişkin olarak aydınlatmakla yükümlüdür. Açık blok zinciri bakımından ise veri sorumlusu süjesinin tespiti

oldukça güç olduğundan dolayı, kişisel verileri işlenen ilgili kişileri bu hususa ilişkin aydınlatma yükümlülüğünün yerine getirilmemesi riski bulunmaktadır.

Ancak yine de tüm blok zincirlerinde, kişisel verilerin sisteme hangi maksat ve metotla işleneceği konusunda ilgili kişilere bilgi verilmesi mümkündür. Bu bağlamda ilgili kişilerin kişisel verilerin işlenebileceğine yönelik olarak önceden hazırlanmış bir bilgilendirme metnini onaylamaları halinde blok zincirine erişim sağlanmasına olanak tanıyan bir blok zinciri sisteminin tasarlanması doğru bir adım olacaktır.

KVKK'nın 12. maddesinde veri sorumlularına, kişisel verileri hukuka aykırı olarak işlememek, işledikleri kişisel verilere ise hukuka aykırı olarak erişilmemesi için önlem almak ve kişisel verilerin güvenli şekilde saklanmasını sağlamak gibi birtakım yükümlülükler getirilmiştir. Ancak bu yükümlülüklerin blok zincirleri bakımından yerine getirilmesi hususunda da problemler bulunmaktadır.

Öncelikle açık blok zincirlerinde veri sorumlusunun bulunmaması, tespit edilememesi veya tespit edilse dahi veri sorumlusunun dünyanın herhangi bir yerinde bulunma olasılığı nedeniyle KVKK'nın 12. maddesinde yer alan yükümlülüklerin yerine getirilmesi söz konusu olmayacaktır. Zira, bu noktada hangi ülke hukukunun uygulanacağı hususunda problemler bulunmaktadır. Dolayısıyla uluslararası erişim sağlanabilen bir blok zincirinde veri sorumlusunun KVKK hükümlerine göre denetim yaptırması mümkün değildir. Aynı şekilde, açık blok zincirlerindeki veri sorumlusunun, KVKK'nın 12. maddesinin 1. fıkrasının c bendi kapsamında, ilgili kişilerin kişisel verilerinin korunması amacıyla her türlü idari ve teknik tedbiri alabilmesi de mümkün olmayacaktır. Kapalı blok zincirlerinde ise veri sorumlularının KVKK'nın 12. Maddesinde yer alan yükümlülükleri yerine getirebilmesi, açık blok zincirlerine göre daha mümkündür.

Yukarıda da değinildiği üzere, uluslararası nitelikteki blok zincirlerine hangi ülkenin hükümlerini uygulanacağı noktasında tartışmalar olduğundan dolayı, GDPR'nin 15. maddesi ile KVKK'nın 13. maddesi kapsamında ilgili kişinin veri sorumlusuna başvurması veya ilgili kişinin veri sorumlusuna başvurduktan sonra veri sorumlusunun ilgili kişinin talebini sonuçlandırması hususları da problemlidir ve bu problemin çözülmesine yönelik hukuki bir yol henüz düzenlenmemiştir. Bu nedenlerden dolayı, ilgili kişinin kişisel verilerinin korunması bakımından hak ihlali yaşaması ihtimal dahilindedir.

Değinilmesi gereken bir başka husus ise, uluslararası erişim sağlanabilen ve Türk hukukunun uygulanabilirliğinin bulunmadığı bir blok zincirlerinin veri sorumlusunun, KVKK bağlamında Veri Sorumlulukları Siciline kaydolmakla yükümlü tutulmasının pratik açıdan elverişli olmadığı hususudur. Son olarak yine blok zincirinin yapısından kaynaklı olarak veri sorumlusunun işlenen kişisel verileri silmek, yok etmek veya anonim hale getirmek yükümlülüklerini yerine getirmesi mümkün olmadığından dolayı TCK kapsamında cezalandırılması da mümkün olamayacaktır.

Veri İşleyen

Veri sorumlusu, bir gerçek veya tüzel kişiye kişisel verilerin işlenmesi hususunda yetki verebilir. KVKK kapsamında veri sorumlusunun yetkilendireceği bu süje, veri işleyen olarak tanımlanmaktadır. GDPR metninde de veri işleyen kavram benzer bir tanıma sahiptir.

Blok zincirlerde, somut olayın şartlarına göre, veri işleyen ve veri sorumlusu sıfatı aynı kişide toplanabilir; veri işleyen sayısı birden fazla olabilir veya veri işleyen niteliğini haiz hiç kimse bulunmayabilir. Blok zincirlerde veri işleyen niteliğini haiz bir süjenin bulunmaması durumunda,

KVKK'nda veri işleyenlere yönelik getirilen, işledikleri kişisel verileri kimseye açıklamama ve amaç dışı kullanmama yükümlülüklerin yerine getirilmesi hususunda boşluklar bulunmaktadır.

Kapalı blok zincirlerde ise veri sorumlusu sıfatını haiz bir süje bulunması mümkün olduğu için veri işleyen niteliğindeki bir süjenin bulunması da mümkündür. Buna göre kapalı blok zincirlerinde rol oynayan düğümler veya madenciler veri işleyen olabilecektir.

Blok Zincirlerde Yer Alan Kişisel Verilerin Korunmasına Yönelik Çözüm Önerileri

Yukarıda bahsedildiği üzere, blok zinciri sistemleri ile KVKK ve GDPR arasında çatışmalar yaşanmaktadır ve blok zincirlerde yer alan kişisel verilerin korunabilmesi bakımından genel olarak problemler ile bazı boşluklar mevcuttur. Bu nedenle blok zincirlerin, KVKK ve GDPR çerçevesinde kişisel verileri koruma hususuyla uyumlu olabilmesi adına birtakım çözüm önerileri düşünülmektedir.

Bu önerilere örnek olarak veri sorumlularının blok zincirindeki veri akışıyla ilgili olarak katılımcılara yönelik rehberler yayınlanması gerektiği gösterilebilecektir. Bu sayede KVKK ve GDPR nezdinde yer alan ilgili kişileri aydınlatma ve onlara bilgi verme yükümlülüğü yerine getirilebilecektir. Ayrıca kişisel verilerin işlenebileceği bir blok zincir sistemi söz konusuysa, veri sorumlusunun, katılımcıların sisteme erişmesinden ve bu sisteme veri girişinde bulunmasından önce kişisel verilerinin işlenebileceği hususunda bilgilendirme yapması gerekmektedir. Ek olarak veri sorumlusu, katılımcılara bu hususa ilişkin bir sözleşme veya bildiri metni sunarak açık rızalarını aldıktan sonra blok zincir sistemine erişimlerini sağlamalıdır. Burada kişisel verilerin güvenliğinin sağlanması bakımından veri sorumlusu ve veri işleyenler için düzenlenen yükümlülüklerin yerine getirilmesi ve kişisel verilerin korunması bağlamında önemli bir adım atılacağından bahsetmek mümkündür. Bununla birlikte, kişisel veri niteliğindeki verilerin, zincir dışı (off chain) olarak depolanması önerilerden biridir. Bu sayede ilgililerin kişisel verileri, blok zincirinin değiştirilemez yapısına tabi olmayacak ve KVKK ile GDPR metnine uygun olarak, bu kişisel verilerin silinmesi, yok edilmesi veya değiştirilmesi mümkün hale gelecektir. Ancak doktrinde kişisel veri niteliğindeki verilerin blok zincir dışında depolanması hususunun blok zincirinin yapısıyla ters düşeceği ileri sürülmektedir. Zira, zincir dışında depolanacak veriler, blok zinciri korumasından çıkacak ve siber saldırıya uğrama riskiyle karşı karşıya kalacaktır. (Mirchandani, 2019.)

Hileli akıllı sözleşmeler ile oluşturulan blok zincirler, özel yazılımlar aracılığıyla tespit edilmeli ve sonrasında bu blok zincirlerine erişimin kapatılması sağlanmalıdır. Bu sayede kişisel verilerin istenmeyen yollarla sızdırılmasının önüne geçilebilecektir.

Blok zincirlerde yer alan kişisel verilerin korunabilmesi için diğer bir öneri ise blok zincirlerde homomorfik şifre ile koruma sağlanmasıdır. Homomorfik şifreleme, özellikle açık blok zincirlerinde verileri şifreleyerek veri güvenliğini koruyacaktır. (Çağlayan Aksoy- Aksoy, 2023.) Veya öznitelik tabanlı şifreleme adı verilen ve herhangi bir otoritenin gerekli olmadığı, gizli anahtar yoluyla şifreleme yapılan bir şifreleme yöntemi kullanılabilir. (Çağlayan Aksoy- Aksoy, 2023.) Zira, öznitelik tabanlı şifreleme, özel anahtar vasıtasıyla şifrenin çözülebileceği bir sistem olup blok zincirinde yer alan verilerin daha iyi korunmasını sağlayacaktır. (Sahai- Waters, 2005.)

Blok zincirlerinin dağıtık bir sistem olması, blok zincirlerde tutulan kişisel verilerin yurt dışına aktarılması sonucunu doğurabilecektir. (Blockchain TÜRKİYE, 2019.) Ancak bu noktada Avrupa Birliği Adalet Divanı (ABAD) tarafından alınan Lindqvist (C 101/01) kararı kapsamında, verilerin yalnızca internet sayfasına yüklenmesi ile o sayfaya erişebilen tüm ülkelere veri transferi yapıldığı anlamına gelmediğine ilişkin verdiği karar baz alınarak blok zincirlerde yer alan verilere dünyanın herhangi bir yerinde bulunan bir düğümün erişebilmesi hususunun verilerin transfer edilmediği görüşünün ileri sürüldüğüne değinmek gerekmektedir. (Hogan, 2008.) Tabii yine de uluslararası veri

aktarımı mümkün olan blok zincirlerde, katılımcılar ve madenciler bu blok zincirine erişim sağlamadan ve veri girişi sağlamadan önce kişisel verilerinin uluslararası olarak aktarılabileceği yönünde ilgili kişilerin önceden bilgilendirilmesi sağlanmalıdır. Bu sayede kişisel verilerin korunması açısından KVKK'nun 9. maddesine uyumluluk sağlanabilecektir.

Yeni kurulacak bir blok zincirinin, kullanım amacına uygun düştüğü takdirde, öncelikle kontrollü ve sınırlı erişimin sağlandığı kapalı bir türde oluşturulması tercih edilmelidir. Zira bu sayede, veri sorumlusu ve veri işleyen niteliğini haiz kişilerin bulunması ve tespit edilmesi daha kolay olacaktır. Buna bağlı olarak da kişisel verilerin güvenliğinin sağlanması bakımından veri sorumlusu ve veri işleyenler için düzenlenen yükümlülüklerin yerine getirilmesi ve kişisel verilerin korunması bağlamında önemli bir adım atılmış olacaktır. (Çağlayan Aksoy- Aksoy, 2023.)

Blok zincirlerde gerçek kişilere ait veriler yer almamalı; sadece tüzel kişilere ilişkin veriler tutulmalıdır. Zira, KVKK ve GDPR metinlerinde yer alan kişisel veri tanımına tüzel kişilerin verileri girmediğinden dolayı bu yöntemle gerçek kişilerin kişisel verilerinin korunması bakımından hak ihlali söz konusu olmayacaktır.

Blok zincir teknolojisinin teknik yapısı nedeniyle bloklarda yer alan kişisel verilerin silinememesi, yok edilememesi veya anonimleştirilememesi, kişisel verileri koruma hukukunda temel ilkelerden birisi olan verilerin doğru ve güncel olması ilkesi bakımından potansiyel bir sorun niteliğindedir. (Ayözger Öngün, 2019.) Bu sorunun çözümüne yönelik olarak, kişisel veri içeren blokların özel anahtarının yok edilmesi şeklinde bir çözüm yolu uygulanabilir. Böylelikle söz konusu verilere erişilemeyecek ve KVKK ile GDPR metni kapsamında kişisel verilerin korunması bakımından düzenlenen önemli bir yükümlülük yerine getirilmiş olacaktır. (European Parliamentary Research Service (EPRS), 2019.) Bununla birlikte, kişisel verileri silme veya anonim hale getirilmesi kavramlarının tanımlandığı bir rehberin yayımlanması yoluyla da izin gerektiren blok zincirlerde kişisel verilerin korunması hukukuna uygunluk sağlayacağı savunulmaktadır. (Mirchandani, 2019.)

Blok zincirlerde ortaya çıkacak herhangi bir uyuşmazlık konusunda hangi ülke mevzuatının uygulanacağı noktasında da problemler bulunmaktadır. Bu problemin veri sorumlusu tarafından önceden hazırlanan bir bildiri ile kişisel verilerin korunması hakkını en üst düzeyde koruma altına alan ülke mevzuatının uygulanmasının kararlaştırılması ile çözülmesinin uygun olduğu düşünülmektedir.

Son çözüm önerisine değinmeden önce veri minimizasyonu ilkesinden bahsetmek gerekmektedir. Buna göre veri minimizasyonu ilkesi, yalnızca yeterli, ilgili ve gerekli olan verilerle sınırlı olarak belli ve meşru bir amaca uygun olarak verilerin toplanmasını ifade etmektedir. (Yücedağ, 2019) Veri minimizasyonu ilkesi ile kişisel verilerin amaca uygun olarak işlenmesi sağlanabilecektir. Bu bağlamda, blok zincirde yer alan kişisel verilerin veri minimizasyonu ilkesine uygun olarak depolanması gözetilmelidir. (Ibáñez- O'hara vd., 2018)

SONUÇ

Satoshi Nakamoto tarafından yayımlanan bir makalede aracısız ve sanal olarak yeni bir ödeme yöntemi tanıtılmıştır. Aynı makalede bu yeni ödeme sistemi, "Bitcoin" adlı dijital bir yeni para biriminin kullanıldığı ve blok zincir altyapısına bağlı bir sistem olarak tasarlanmıştır. Satoshi Nakamoto, bu makalesi ile blok zincir teknolojisini de tüm dünyaya duyurulmasını sağlamıştır. Blok zincir teknolojisi, görüldüğü üzere ilk olarak kripto para birimleriyle gerçekleştirilen bir ödeme sistemi için tasarlanan bir sistem olsa dahi bu teknoloji, günümüzde yalnızca kripto para akışıyla

sınırlı olmaksızın birçok farklı alanda da kullanılmaktadır. Ancak her bilişim sisteminde olduğu gibi, blok zincirlerinde de katılımcıların kişisel verileri elde edilip bloklar üzerine işlenmektedir.

Bu noktada KVKK ve GDPR metinleri ile korunması hedeflenen kişisel verilerin blok zincir teknolojilerinde amaca uygun olarak nasıl tutulması gerektiği hususu incelenmelidir. Bu bağlamda karşılaşılan en büyük engel, blok zinciri sisteminin teknik yapısının değiştirilemez, bloklarda yer alan verilerin silinemez ve yok edilemez olmasından kaynaklanmaktadır. Zira, KVKK ile GDPR metinlerinde elde edilecek kişisel veri söz konusu olduğu takdirde, bu verilerin makul ve amaca uygun bir süre boyunca tutulması ve ilgili kişinin talebi doğrultusunda söz konusu kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi; hatalı veya eksik bir bilgi durumunda da bu verinin güncellenerek tamamlanması veya doğru hale getirilmesi gerekmektedir. Ancak blok zincirlerin yapısı teknik olarak bu şekilde hareket etmeye elverişli değildir. Bu bağlamda, blok zincirleri şu anki haliyle KVKK ve GDPR'ın özüyle, sözüyle ve ruhuyla bağdaşmamaktadır.

Değinmek gereken bir başka husus ise, blok zincirlerdeki veri sorumlusu ve veri işleyen kavramlarının tespitinin yapılması gerektiğidir. Zira bu tespitin yapılması, KVKK ve GDPR nezdinde kişisel verilerin güvenliğinin sağlanması açısından veri sorumlusu ve veri işleyen süjelerine yüklenen yükümlülüklerin yerine getirilmesi bakımından önemlidir. Bu noktada en büyük sorun, bazı blok zincirlerde veri sorumlusu ve/veya veri işleyen olarak nitelendirilebilecek kimsenin bulunmayışıdır. Veri sorumlusu ve veri işleyenin bulunmaması da onlar için getirilen yükümlülüklerin hiç yerine getirilmemesi nedeniyle kişisel verileri işlenen ilgili kişilerin başta Anayasa ve daha sonra KVKK ile korunmak istenen haklarının ihlal edilmesine yol açacaktır.

Yine, blok zincirinin şeffaf bir yapıda olması nedeniyle, ilgili kişilerin açık rızaları bulunmadan söz konusu kişisel verilerine diğer katılımcılar veya üçüncü kişiler tarafından erişilmesi hususu da KVKK ve GDPR bakımından oldukça problemli bir hususdur ve bu metinlerde korumaya alınan hak ihlallerinin yaşanmasına sebebiyet verecektir.

Son olarak, blok zincirlerin dünyanın birçok yerine kopyaları dağıtılmış bir defter niteliğinde olması ve düğümlerin dünyanın herhangi bir yerinde bulunabiliyor olması, kişisel veriler bakımından bir ihtilaf söz konusu olduğunda hangi ülke veya ülkelerin hukukunun uygulanacağının tespitini de güçleştirmektedir. Bu hususa ilişkin olarak tartışmalar da mevcuttur. Bu noktada, veri sorumlusu tarafından önceden hazırlanan bir bildiri ile kişisel verilerin korunması hakkını en üst düzeyde koruma altına alan ülke mevzuatının uygulanmasının kararlaştırılması çözüm olabilecektir.

Yukarıda yapılan tüm açıklamalar ışığında, her ne kadar blok zincirlerin teknik anlamda oldukça güvenilir olduğu savunuluyor olsa da kişisel verilerin korunması hukuku bağlamında zayıf bir konumda yer aldığı görülmektedir. Ancak sırf bu yüzden blok zincirlerden kaçınmak değil; KVKK ve GDPR metinleri göz önünde bulundurularak kişisel verilerin güvenliğinin sağlanması için birtakım çözüm önerilerinin uygulanması gerekmektedir. Bu sayede blok zincirleri, ulusal veya uluslararası kişisel verilerin korunması mevzuatlarına uyumlu bir şekilde faaliyet gösterebilecektir.

KAYNAKÇA

Akdemir Altınbaşak, T. (2018). "Blok Zincir (Blockchain) Teknolojisi ile Vergilendirme". Maliye Dergisi 174: 360-371. https://ms.hmb.gov.tr/uploads/2019/09/174-17.pdf. (20.01.2024)

Avunduk, H., Aşan, H. (2018). "Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme". Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi 33 (1): 369-384. https://doi.org/10.24988/deuiibf.2018331746.

Ayözger Öngün, Ç. (2019). "Blokzinciri Teknolojisinde Kişisel Verilerin Korunması". https://www.srp-legal. com/tr/2019/10/10/blokzinciri-teknolojisinde-kisisel-verilerin-korunmasi/ (10.01.2024).

Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi. "Blokzincir Nedir?". https://blokzincir.bilgem.tubitak.gov.tr/blokzincir-nedir/. (25.01.2023)

Blockchain Türkiye. (2019). Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu. https://bctr.org/dokumanlar/KVKK_ve_Blokzincir_ Teknolojisi.pdf. (24.06.2024).

Çağlayan Aksoy, P. (2021). "Blokzincir Teknolojisinin Kişisel Verilerin Korunması Kanunu Bakımından Değerlendirilmesi". Kişisel Verileri Koruma Kurumu semineri.

Çağlayan Aksoy, P., Aksoy, H. (2023). "Kişisel Verilerin Korunmasına Akademik Bakış". Kişisel Verileri Koruma Kurumu (Der.) https://kvkk.gov.tr/SharedFolderServer/CMSFiles/0cd33e96-77cf-4989-b29b-d331af6a463f.pdf. (04.03.2024)

Diri, N., Yalçınkaya, B. (2022). "Blokzincir Uygulamalarında Kişisel Veri Problemi: Depolama Riskleri ve Öneriler". Bilgi Yönetimi Dergisi 5 (1): 47-67. https://doi.org/10.33721/by.1000702.

Durdu, A., Gökçe, A. (2022). "Blokzincir teknolojisi akıllı sözleşme uygulamalarının kamu alımlarında kullanımı". Sakarya Üniversitesi İşletme Enstitüsü Dergisi 4 (2): 43-48. https://doi.org/10.47542/sauied.1019897.

European Parliamentary Research Service (EPRS) (2019). "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?". https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf. (17.01.2024)

Hogan, L. (2008). "A guide to blockchain and data protection". https://www.hlengage.com/_uploads/pdfs/DataProtection-BlockchainPaperNov16Low-res.pdf (24.06.2024).

Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu- Blockchain Türkiye Platformu (BCTR) (2022). "Kişisel Verilerin Korunması Hukuku ve Blokzinciri Teknolojisi Raporu". https://bctr.org/dokumanlar/KVKK_ve_Blokzincir_Teknolojisi.pdf. (01.02.2024)

Iansiti, M., Lakhani, K. R. (2017). "The Truth About Blockchain". Harvard Business Review, 95 (1): 118- 127. https://hbr.org/2017/01/the-truth-about-blockchain. (04.02.2024)

Ibáñez, L. D., O'hara, K., Simperl, E., "On Blockchains and the General Data Protection Regulation", University of Southampton, 2018.

Karatay, E., Solak, M. vd. (2020). "Blokzincir Projeleri Özelinde Kişisel Verilerin Korunması Kanunu'na İlişkin Hukuki Değerlendirmeler". Finans Hukuku Gündemi Dergisi 4: 1-16. https://www.kanunum.com/file/cid12679960_vid22134934_fid1060904. (03.02.2024)

Kaya, M. (2015). Elektronik Ortamda Kişilik Hakkının Korunması. Ankara: Seçkin Yayıncılık.

Kişisel Verileri Koruma Kurumu. "Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler". https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler. (20.02.2024)

Kişisel Verileri Koruma Kurumu (2019). "Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi".

Li, X. (2020). "A survey on the security of blockchain systems". Future Generation Computer Systems 107: 841-853. https://doi.org/10.1016/j.future.2017.08.020.

Mingxiao, D., Xıaofeng, M. vd. (2017). "A review on consensus algorithm of blockchain". International Conference on Systems, Man, and Cybernetics: 2567-2572. https://doi.org/10.1109/SMC.2017.8123011.

Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR". Fordham Intellectual Property, Media and Entertainment Law Journal 29 (4): 1201-1241.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf. (06.01.2024)

Narayanan, Arvind vd. (2016). "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction".

Öz Demetoğlu, G. (2019). Türk ve Avrupa Birliği Veri Koruma Hukuku Bağlamında Blok Zincir Teknolojisinde Unutulma Hakkı. Yüksek Lisans Tezi. İstanbul: Marmara Üniversitesi.

Sahai, A., Waters, B. (2005). "Fuzzy Identity-Based Encryption". Advances in Cryptology – Eurocrypt 2005. Lecture Notes in Computer Science 3494: 457-473,

Tanrıverdi, M., Uysal, M. vd. (2019). "Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi". Bilişim Teknolojileri Dergisi 12 (3): 203-217. https://doi.org/10.17671/gazibtd.547122.

Tekelioğlu, N. (2022). "Dijital Tapu Sicili: Blokzinciri Teknolojisinin Tapu Sicilinde Kullanılmasına Dair Karşılaştırmalı Bir İnceleme". İstanbul Hukuk Mecmuası 80 (1): 1-39. https://doi.org/10.26650/mecmua.2022.80.1.0001.

Teperdijan, R. (2020). "The Puzzle of Squaring Blockchain with the General Data Protection Regulation". Forthcoming in Jurimetrics 60 (3): 1-61.

Tuvay, B. (2020). "Dijital Cüzdan Dönemi Başlıyor". e-Dönüşüm dergisi. https://www.qnbefinans.com/uploads/20201201114504437.pdf. (18.01.2024)

Usta, A., Doğantekin, S. (2018). "Blockchain 101". Bankalar Arası Kart Merkezi. https://bctr.org/dokumanlar/Blockchain101v2r2.pdf. (25.01.2024)

Ünal, E. (2018). "Bitcoin ve Blockchain Nedir? Nasıl Çalışır?". https://enginunal.medium.com/bitcoin- ve-blockchain-nedir-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-78d5c9e28095. (06.01.2024)

Ünal, G., Uluyol, Ç. (2020). "Blok Zinciri Teknolojisi". Bilişim Teknolojileri Dergisi 13 (2): 167-175. https://doi.org/10.17671/gazibtd.516990.

Yücedağ, N. (2019). "Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler". Kişisel Verileri Koruma Dergisi, 1 (1): 47-63. https://dergipark.org.tr/tr/download/article-file/737938. (06.02.2024)