www.kvkk.gov.tr

Kişisel Verileri Koruma Dergisi

Cilt: 1, Sayı: 2

Geliş: 25.10.2019
Kabul: 13.12.2019

Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu

Osman Gazi, Güçlütürk
Kırklareli Üniversitesi Ticaret Hukuku Anabilim Dalı, Kırklareli, Türkiye, ogucluturk@gmail.com
ORCID: orcid.org/0000-0001-5834-6635

ÖZ
Blokzincir teknolojisi yeniliği, yapısı ve geleneksel veri depolama/aktarma yöntemlerinden farklılıkları sebebiyle önemli tartışmalara konu olmaktadır. Geleneksel sistemlerden farklı olarak birden çok bilgisayarda depolanan bir ağ sistemi sunan, blokzincir teknolojisi üzerinde veri depolanması esnasında farklı tekniklerin kullanılması ve özellikle depolanan verilerin daha sonra müdahalesinin teknik altyapı sebebiyle zorlaştırılmış olması, kişisel verilerin korunması açısından bazı önemli sorunları beraberinde getirmektedir. Bu çalışmada blokzincir üzerinde depolanan verilerin Kişisel Verileri Koruma Kanunu kapsamında kişisel veri olup olmadığı ve bu niteliği taşıyan veriler açısından yine ilgili kanun kapsamında silme, yok etme, anonim hale getirme işlemlerinin yerine getirilip getirilemeyeceği sorunu, özellikle Avrupa Birliği mahkeme kararları ve doktrininde ileri sürülen görüşler ışığında incelenecektir.

Anahtar Sözcükler: Blokzincir, kişisel veri, silme, anonimleştirme, Avrupa Veri Koruma Tüzüğü

The Personal Data Status of Data Stored on a Blockchain and the Question of Erasure

ABSTRACT
Blockchain technology is a subject of ongoing important debate due to its novelty, structure and difference compared to traditional data storing mechanisms. Unlike traditional systems, the fact that the data is stored on multiple nodes connected to a blockchain network by virtue of deployment of different technical infrastructures that is making it difficult to tamper with the date afterwards poses important questions with regards to the protection of personal data. In this study, firstly, the question of whether the data stored on a public-permissionless blockchain can be considered as personal data shall be explored. Following that, secondly, how the processes of erasure and anonymization can be conducted with regards to the data stored on a public-permissionless blockchain shall be examined in light of both the EU case-law and relevant literature.

Keywords: Blockchain, personal data, erasure, anonymization, GDPR

Atıf Gösterme	Güçlütürk, O. G., (2019). Blokzincir Üzerinde Depolanan Verilerin Kişisel Veri Niteliği ve Silinemezlik, Yok Edilemezlik Sorunu, *Kişisel Verileri Koruma Dergisi. 1*(2), 30-40.

GİRİŞ

Blokzincir teknolojisi birimler arası etkileşim ve veri depolamaya ilişkin getirdiği yenilikler sebebiyle birçok alanda önemli tartışmalar yaratmıştır. Bu önemli tartışmalardan bir tanesi de hukuk alanında kişisel verilerin korunması mevzuatının blokzincir uygulamaları ile ilişkisidir. Kişisel verilerin korunmasına ilişkin düzenlemeler geleneksel merkezi sistemler dikkate alınarak hazırlanmış olup hak ve yükümlülükleri merkezi bir veri sorumlusunun varlığı varsayımına göre düzenlenmiştir.

Bu çalışmada daha özelde blokzincir üzerinde depolanan verilerin, kişisel veri niteliği ve blokzincirin değiştirilmesinin zorluğu karşısında bu verilerin silinmesi, yok edilmesi, anonim hale getirilmesi sorunlarına değinilecektir. İlk bölümde blokzincir teknolojisinin teknik altyapısına yönelik özet açıklamalar yapılacak, ikinci bölümde kişisel veri kavramı incelenecek daha sonra ise blokzincir üzerinde depolanan bazı veri tiplerinin kişisel veri niteliği değerlendirildikten sonra çalışma silme ve yok etmeye ilişkin değerlendirmelerle sonlandırılacaktır.

Çalışmanın odağında, her ne kadar Türk Hukuku'ndaki ilgili düzenleme olan 6698 sayılı Kişisel Verileri Koruma Kanunu (KVKK) bulunsa da Türkiye'de bu kanunun henüz genç olması, blokzincir uygulamalarının Türkiye'de yaygın şekilde uygulamasının henüz görülmemiş olması, Avrupa Birliği (AB) genelinde ise kişisel verilerin korunmasına ilişkin olarak 1995 yılında KVKK'ya da kaynaklık teşkil eden 95/46/EC sayılı Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi yürürlüğe girmiş olup 2018'de Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) tarafından yürürlükten kaldırılana kadar geçen süreçte bu alanda önemli bir doktrin ve içtihat birikiminin ortaya çıkmasını sağlaması gibi gerekçelerle çalışma süresince sıklıkla AB Hukuku'nda yer alan görüşlere atıf yapılmıştır.

BLOKZİNCİR TEKNOLOJİSİ

Blokzincir (İng. "*Blockchain*") teknolojisi 2008 yılında kimliği hala bilinmeyen ancak Satoshi Nakamoto takma adını kullanan kişi veya kişilerce, güvene ve merkezi aracı kurumlara dayalı finansal sistemin zayıflıklarına karşı, merkezi aracı kurumlara ihtiyaç duymayan, kullanıcıların doğrudan birbirleriyle iletişim kurmalarına imkan veren elektronik bir ödeme sistemi olarak tasarlanmış, bir kripto varlık olan Bitcoin ile birlikte hayatımıza girmiştir (Nakamoto, 2008).

"*Blockchain*" ifadesinin henüz yerleşik bir Türkçe çevirisi yoktur. Birçok yerde terim orijinal haliyle kullanılmakla birlikte TÜBİTAK "Blokzincir" kavramını kullanmaktadır. Biz de bu çalışmada TÜBİTAK tarafından yerleştirilen kavramı kullanmayı, ancak çalışmanın literatürü İngilizce dilinde geliştiğinden dolayı terimleri kullanırken İngilizce karşılıklarına yer vermeyi uygun gördük.

Blokzincir esasında bir dağıtılmış kayıt tutma teknolojisidir (İng. "*Distributed Ledger Technology*") (DLT). Geleneksel veri depolama sistemlerinde veri, merkezi bir bilgisayarda depolanır ve merkezi aktör veya aktörlerce kontrol edilir. DLT'de ise veri, ağda yer alan çok sayıda birim tarafından depolanır. Bu durum dağıtılmış olma (İng. "*distributed*") özelliğini ifade eder (Güçlütürk, 2018a). Ayrıca, yine geleneksel sistemlerin aksine, DLT tabanlı sistemlerde veri trafiği ve depolanacak veriler merkezi aktörler tarafından değil, bazı kurallar dahilinde katılımcılar tarafından da belirlenebilir. Bu durum ise DLT'nin merkezi olmama (İng. "*decentralized*") özelliğini ifade eder (Güçlütürk, 2018a). Bir DLT

sistemine kaydedilecek verilerin belirlenmesi için izlenen kurallar bütününe ise uzlaşma protokolleri (İng. "*consensus protocol*") adı verilir.

Burada ilk dikkat edilmesi gereken nokta, bazı yazarlar tarafından değişken ifadeler olarak kullanılsalar da blokzincirin DLT ile aynı şey olmadığıdır. Blokzincir teknolojisi DLT tabanlı sistemlerin sadece bir örneğidir. Verilerin bloklar halinde depolanmadığı DLT örnekleri de mevcuttur. Buna bir örnek olarak önde gelen kripto varlıklardan olan IOTA'nın altyapısında kullanılan ve "sarmaşık" anlamına gelen "*Tangle*" gösterilebilir.

Adından da anlaşılabileceği üzere bir blokzincirde veriler, veri blokları içerisinde depolanır ve bu bloklar kriptografik yöntemler kullanılarak birbirine bağlanır. Blokzincir teknolojisinin kişisel verilerin korunması mevzuatıyla olan ilişkisinin incelenebilmesi için öncelikle bir blokzincirde hangi verilerin nasıl depolandığının anlaşılması gerekmektedir. Bu sebeple, çalışmanın bu bölümünde kısaca Bitcoin Blokzinciri örnek alınarak bir blokzincirin işleyiş mekanizmasından bahsedilecektir.

Çalışmaya devam etmeden bir hususa daha dikkat çekilmelidir. Bir blokzincir farklı verileri depolayacak ve farklı protokollerle çalışacak şekilde kurgulanabilir. Nitekim blokzincirler, temelde herkes tarafından erişilebilir olup olmamalarına bağlı olarak açık-kapalı (İng. "*public-private*") ve blokzincire veri ekleme yetkisinin özel bir gruba tanınmış olup olmamasına bağlı olarak izinli- izinsiz (İng. "*permissioned-permissionless*") blokzincirler olarak farklı sınıflara ayrılırlar (Bashir, 2017). Bu sınıflandırmada Bitcoin blokzinciri herkes tarafından erişilebilir olduğu ve aynı zamanda isteyen herkes, gerekli donanıma sahip olmak suretiyle, katılımcı olarak da ağda yer alabileceği için izne tabi olmayan açık bir blokzincir olarak değerlendirilir. Hacim sınırlaması itibariyle bu çalışmada tüm blokzincir tiplerinin incelenmesi mümkün olmayacaktır. Verilerin bir kontrol mekanizması olmaksızın herkesçe erişilebilecek şekilde tutulması sebebiyle, kişisel verilerin korunması bakımından özellikle önem taşıdığı düşünülerek bu çalışmada yer alan açıklamalar izne tabi olmayan açık blokzincirler dikkate alınarak yapılacaktır.

Çoğu blokzinciri oluşturan bloklarda temelde iki tip veri bulunmaktadır. Bunlardan ilki her bloğun ağdaki kullanıcılar tarafından tanınmasını ve onaylanmasını mümkün kılan blok başlığı (İng. "*header*") kısmıdır. Blok başlığında zaman damgası, o blokta bulunan toplam işlem sayısı, o bloğu daha önceki bloklara bağlayan zincir niteliği gören "*hash*" değeri gibi farklı veriler yer alabilir (Bashir, 2017; Güçlütürk, 2018a). "*Hash*", uzunluğuna bağlı olmaksızın bir metin girdisini alarak o girdiden her daim aynı uzunlukta, harf ve rakamlardan oluşan bir dizi üreten bir kriptografik fonksiyonu ve aynı zamanda bu fonksiyon tarafından üretilen çıktıya verilen isimdir (Finck, 2019). *Hash* fonksiyonunun özelliği, her bir girdi için eşsiz bir çıktı oluşturmak suretiyle bir dijital parmak izi niteliği taşıması ve geri dönüştürülemez olması, yani bir hash'dan yola çıkılarak orijinal girdiye ulaşmanın mümkün olmamasıdır (Roy ve Meier, 2005). Her bloğun başlığında bir önceki blok içeriğinin *hash*'ı yer alır. Eğer blok içeriğinde ufak bir değişiklik yapılacak olursa, o bloğa ait *hash* bilgisi de değişeceğinden dolayı değiştirilen blok ile diğer bloklar arasındaki bağ koparılmış olur ve bu durum tespit edildiğinde değiştirilmiş olan blok, ağdaki katılımcılar tarafından onaylanamaz (Güçlütürk, 2018a).

İkinci veri tipi ise asıl depolanmak istenen içeriğe ilişkin verinin yer aldığı kısımdır. Bu verinin tipi ilgili blokzincirin oluşturulma amacına göre değişiklik gösterir. Bir elektronik ödeme sistemi olarak tasarlanan Bitcoin blokzincirinde bu kısım Bitcoin kullanılarak yapılan işlemlerin kaydından oluşmaktadır. Çoğunlukla blok başlığında yer alan veriler o bloğun ağ üzerinde tanınmasını mümkün kıldığı için şifrelenmez iken içeriğe ilişkin veriler şifrelenir (Finck, 2017).

Bir blokzincirde şifrelenmiş olan içeriğe ilişkin verilere erişim bakımından ise kullanıcılar tarafından kullanılan iki veriden daha bahsedilmesi gerekir. Bunlar açık-gizli anahtarlar (İng. "*public-private keys*") olarak adlandırılır. Açık anahtar doğrudan veya *hash*'ı üretildikten sonra bir hesap numarası gibi

kullanılarak kullanıcılar arasında paylaşılır ve işlemlerle birlikte blokzincirde kaydedilir. Diğer yandan özel anahtar şifrelenmiş olan içeriğe erişimi sağladığı için blokzincir üzerinde depolanmaz, kullanıcıların özel anahtarlarını gizli tutmaları gerekir. Bu anahtarlar bir çift olarak üretilir ve aralarında kriptografik bir bağlantı bulunur. Bir açık anahtara bağlanmış veriye, Bitcoin blokzincirinde bir açık anahtara bağlanmış Bitcoinlere, ancak o açık anahtardan üretilmiş olan gizli anahtar ile erişilebilir (Finck, 2019; Güçlütürk, 2018a).

Bir blokzincirin kişisel verilerin korunması mevzuatıyla uyumluluğu incelenirken, bu farklı veri tiplerinin kişisel veri olup olmadıkları ve kişisel veri olmaları durumunda ilgili hukuki düzenlemelerce öngörülen mekanizmaların var olup olmadığına bakılmalıdır.

KİŞİSEL VERİ KAVRAMI

KVKK'nın 3(1)(d) maddesinde kişisel veri "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" olarak tanımlanmıştır. Bu tanım GDPR'nin 4(1) maddesinde yer alan kişisel veri tanımıyla da benzerlik taşımaktadır. Buna göre bir verinin kişisel veri olarak nitelendirilebilmesi için üç temel unsurdan söz edilebilir: Kişisel verinin (i) bir gerçek kişiye (ii) ilişkin olması ve (ii) bu kişinin belirli ya da belirlenebilir olması gereklidir.

Burada ilk dikkat edilmesi gereken nokta, Türk Hukuku'nda kişisel veri korumasının gerçek kişilerle sınırlı olmasıdır. Blokzincir üzerinde depolanan veri tüzel kişilere ilişkin olduğu takdirde kişisel verilerin koruma mevzuatında korunmayacaktır. KVKK bu açıdan GDPR ile benzerlik göstermektedir. Nitekim GDPR'nin Başlangıç (İng. "*Recital*") kısmının 14.paragrafında da tüzel kişilerin koruma dışı bırakıldığı açıkça belirtilmiştir. Ancak belirtmek gerekir ki üye devletler seviyesinde ve AB üyesi olmayan bazı diğer devletlerde de tüzel kişilerin koruma kapsamına alındığı örnekler mevcuttur (Develioğlu, 2017).

İkinci unsurla ilgili olarak bir verinin bir gerçek kişiye ilişkin olup olmadığı pratik bir değerlendirme olup çoğu zaman kolayca tespit edilebilecektir (Article 29 Data Protection Working Party, 2007). İsim, yaş, telefon numarası, adres gibi bilgilerin kişiye ilişkin olduğu tartışmasızdır. Kişinin özel ve aile hayatına dair bilgiler o kişiye ilişkin olarak kabul edilir. Yine kişinin çalıştığı yerde tutulan personel dosyasında yer alan bilgiler veya medikal geçmişine ilişkin bilgiler de o kişiye ilişkin kabul edilir (Article 29 Data Protection Working Party, 2007).

Bazı durumlarda ise verinin bir gerçek kişiye ilişkin olup olmadığı bu kadar açık olmayabilir. Örneğin bir taşıtın teknik bilgileri, servis kaydı kural olarak doğrudan bir gerçek kişiye değil o taşıta ilişkindir. Fakat bu bilgiler üzerinden taşıt sahibinin belirlenebilir olması mümkün olduğundan bu veriler aynı zamanda taşıt sahibine ilişkin olarak kabul edilmelidir (Article 29 Data Protection Working Party, 2007). Bu unsura ilişkin olarak AB Hukuku'nda içerik, amaç ve sonuç açısından değerlendirmeler yapılabileceği ifade edilmiştir. Buna göre bir veri içerik açısından bir gerçek kişi hakkındaysa, bir gerçek kişinin durumunu değerlendirmek veya ona karşı olan davranışları etkileyecek amacıyla kullanılacaksa veya o kişinin hak ve menfaatleri üzerinde etki edecek sonuçlar doğuruyorsa söz konusu veri ilgili kişiye ilişkin kabul edilecektir(Article 29 Data Protection Working Party, 2007).

Üçüncü unsur olan kişinin belirli ya da belirlenebilir olması ise daha fazla incelenmesi gereken bir kavramdır. KVKK'da bu unsura ilişkin detaylı bir açıklamaya yer verilmemiştir. GDPR'de ise m. 4(1)'de kişisel veri tanımının hemen sonrasında belirlenebilir gerçek kişi için de bir tanım verilmiştir.

Buna göre belirlenebilir gerçek kişi "özellikle isim, tanımlayıcı bir numara, konum bilgisi veya çevrimiçi bir tanımlayıcı gibi tanımlayıcılara ya da ilgili kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine ilişkin özelliklerden bir ya da birkaçına referans yapmak suretiyle doğrudan veya dolaylı olarak belirlenebilen" kişileri ifade eder. Görüldüğü üzere GDPR'de yer alan bu tanım son derece geniş bir tanımdır. Önemli olan ise bu kişinin belirlenebilmesidir. Belirli ya da belirlenebilir bir kişiden söz etmek için illa ki o kişinin ismine ulaşılması gerekmez (Article 29 Data Protection Working Party, 2007; Develioğlu, 2017).

Kişinin belirlenebilmesinde dikkate alınacak faktörlere ilişkin olarak yine KVKK'da özel bir düzenleme olmamakla birlikte GDPR'nin başlangıç kısmının 26. paragrafında belirlenebilir bir gerçek kişinin olup olmadığının tespitinde, herhangi başka bir kişi tarafından bir gerçek kişinin tespitinde kullanılması makul tüm yöntem ve bilgilerin dikkate alınacağı belirtilmiştir. Gerçekten de kişisel veriden söz edilebilmesi için ilgili gerçek kişinin kimliğini belirlenmesini sağlayacak tüm bilgilerin tek bir kişinin elinde bulunması gerekmez. Bu durum Avrupa Birliği Adalet Divanı tarafından da Breyer davasında açıkça ifade edilmiştir (Avrupa Birliği Adalet Divanı, Breyer Davası C-582/14, par. 43).

Bir sonraki bölümde blokzincir üzerinde depolanan verilerin, kişisel veri unsurlarını taşıyıp taşımadığı incelenecektir.

BLOKZİNCİR ÜZERİNDE DEPOLANAN VERİLERİN KİŞİSEL VERİ NİTELİĞİ

Bu başlıkta blokzincir üzerinde depolanan verilerin hukuki anlamda kişisel veri teşkil edip etmediği incelenecektir. Blokzincir üzerinde depolanan verilerin kişisel veri olup olmadığının tespiti hukuki açıdan önem taşımaktadır çünkü KVKK m. 3(1)(e) uyarınca kişisel verilerin bir veri kayıt sisteminin parçası olarak kaydedilmesi ve depolanması kişisel verilerin işlenmesi anlamına gelecektir. Kişisel verilerin işlenmesi ise veri işleyen ve veri sorumluları açısından KVKK'da düzenlenen yükümlülüklerin gündeme gelmesine sebep olacaktır.

Blok Başlığında Yer Alan Veriler

Bir blokzincirde temelde iki tip veri bulunduğunu belirtmiştik. Bunlar blok başlığı içerisinde yer alan, ilgili bloğun ağdaki diğer katılımcılar tarafından tanınmasını sağlayan veriler ve blok içeriğinde yer alan, ilgili blokzincirin kullanım amacına göre farklılık gösterecek olan verilerdi. Bu aşamada özellikle belirtilmelidir ki blokzincirler farklı amaçlarla, farklı yapılarda oluşturulabileceklerinden bir blokzincir örneğinin kişisel verilerin korunmasın ilişkin mevzuata uygunluk değerlendirmesinin her durumun özellikleri dikkate alınarak ayrıca yapılması gereklidir (Finck, 2019). Ancak bu durum belirli ortak özellikleri bulunan blokzincirler açısından bazı genel değerlendirmelerin yapılmasına engel değildir. Bu başlık altında açık ve izne tabi olmayan blokzincirlerin ortak özellikleri dikkate alınarak bir değerlendirme yapılacaktır. Açık ve izne tabi olmayan blokzincirlerin en önemli örneği de Bitcoin blokzinciri olduğundan örnek olarak Bitcoin blokzinciri alınacaktır.

İlk incelenmesi gereken nokta blok başlığı içerisinde yer alan bilgilerdir. Bitcoin blokzincirinde ve birçok diğer blokzincirde blok başlığında yer alan bilgiler kullanıcılara ilişkin değil o bloğun ağ üzerinde tanınmasına yönelik bilgiler içerdiğinden ve blok başlığına bakılarak blok içeriğindeki verilere ulaşılamayacağından blok başlığında yer alan bilgiler belirli ya da belirlenebilir gerçek kişilere ilişkin değildir ve dolayısıyla bu bilgilerin kişisel veri olduğundan söz edilemez. Blok içeriğinde yer alan verilerde ise durum bu kadar net değildir.

Açık Anahtarlar/Adresler

Burada öncelikle Bitcoin blokzinciri ve diğer birçok blokzincirde karşımıza çıkan, kullanıcıların ilgili blokzincir ağı üzerinde işlem yapmak için kullandığı harf ve sayı dizileri olan açık-özel anahtar çiftlerine değinilmelidir. Bu anahtar çiftleri doğrudan ilgili kişilerin kimliği hakkında bir bilgi vermez. Özel anahtarlar blokzincir üzerinde depolanmaz. Ancak açık anahtarlar blokzincir üzerinde işlemlerle beraber depolanır ve kullanıcılar arasında hesap numarası veya adres benzeri işlev görecek şekilde paylaşılır. Blokzincir sistemine göre açık anahtarlar doğrudan adres olarak kullanılabileceğinden veya *hash* fonksiyonuna sokularak açık adres haline getirilebileceğinden dolayı bu iki tip veriyi bir arada değerlendirmeyi uygun görüyoruz. Açık anahtarlar, aslında ağdaki kullanıcıların gerçek kimliklerini gizleme işlevine sahiptir. Fakat daha önce belirtildiği üzere kişisel verinin belirli ya da belirlenebilir bir kişiye ilişkin olması için kişinin isminin bilinmesi şart olmadığından, gerçek kimliğin gizlenmesi tek başına bir veriyi kişisel veri olmaktan çıkarmaz, bunun için verinin anonim hale getirilmesi gerekir.

KVKK m. 7/3'e dayanılarak çıkarılan ve 28.10.2017 tarihli 30224 sayılı Resmi Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Yönetmelik) 10/1.maddesinde anonim hale getirme "*kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi*" olarak tanımlanmıştır. Açık anahtarların kullanımıyla kimliğin gizlenmesi, açık anahtarların başka verilerle eşleştirilmesi yoluyla bir gerçek kişiyle ilişkilendirilmesinin önüne geçememektedir. Gerçekten de uygulamada açık anahtarlar üzerinden yapılan incelemeler ve işlemlerin geriye doğru takibi yoluyla gerçek kişilere ulaşmak mümkün olmuştur (Finck, 2019). Bu sebeple açık anahtarların KVKK anlamında da kişisel veri olduğunun kabulü gereklidir.

Açık anahtarlar haricinde blok içeriğinde belirli ya da belirlenebilir gerçek kişilere ilişkin başka kişisel verilerin depolanması da mümkündür. Bir veri, bir blokzincir üzerinde üç temel şekilde depolanabilir. Bunlardan ilki bir verinin blok içerisinde herkesin ulaşabileceği düz bir metin şekilde saklanmasıdır. Ancak bu ihtimalde blokzincirlerde blok kapasiteleri depolanacak verinin boyutunu kısıtladığından kullanılacak yönteme göre bazı sınırlamaların dikkate alınması gerekir. Örneğin Bitcoin blokzincirinin başlangıç bloğunda (İng. "*genesis block*") Satoshi Nakamoto tarafından depolanmış bir mesaj mevcuttur. Bitcoin blokzincirinin her bir bloğunda "*Coinbase transaction*" adı verilen, o bloğu ana blokzincire eklemeyi başaran Bitcoin madencisinin (İng. "*miner*") alacağı ödül Bitcoinlerin bağlı bulunduğu bir özel işlem vardır. Bu işlemin içerisinde madencinin istediği gibi kullanacağı bir veri alanı vardır. Bitcoin başlangıç bloğunda bu kısımda yer alan dizi şu şekildedir:

"*04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73*"

Ancak bu ifade harf ve sayıların bir araya gelmesinden oluşan rastgele ya da şifrelenmiş bir metin değil onaltılık (İng. "*hexadecimal*") sayı sisteminde yazılmış bir metindir. Gerekli dönüşümler yapıldığında - onaltılık sayı sistemine yabancıysanız bu işlem için çevrimiçi dönüştürücüleri de kullanabilirsiniz- ortaya çıkan metin 3 Ocak 2009 tarihli The Times gazetesinin başlığında yer alan şu ifadedir: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*". Bu cümlenin bu çalışma açısından önemi ise *coinbase* işlemi içerisine düz metin şeklinde belirli uzunluk kısıtlamalarına tabi olmak şartıyla istenen verinin depolanabileceğini göstermesidir.

Blok ödülüne ilişkin olan *coinbase* işlemi sadece madenciler tarafından erişilebilecek olup çok kısıtlı bir alan sağlamaktadır. Ancak blokzincir üzerinde veri depolamak için başka yöntemler de geliştirilmiştir. Bunların birçoğu belirli bir kripto varlık feda etme karşılığında sahte adreslere yönelik harcanamaz işlemler yaratarak normalde adresin bulunacağı alana veri depolama temeline dayanmaktadır. Örneğin Bitcoin blokzincirinde 273536 numaralı blok içerisinde yer alan bir işlemde

"15gHNr4TCKmhHDEG31L2XFNvpnEcnPSQvd" açık adresine Bitcoin gönderilmektedir. Bu adres Bitcoin blokzincirindeki teknik altyapı sebebiyle ek bir *hash* işlemine tabi tutulup "334e656c736f6e2d4d616e64656c612e6a70673f" şeklinde depolanmaktadır. Bu ifadeyi ise yine daha önce bahsedildiği gibi onaltılık sistemden metine çevirdiğimizde elde edilen sonuç bir resim dosyası ismi olduğu anlaşılan "3Nelson-Mandela.jpg?" ifadesi olmaktadır. *Coinbase* işleminin aksine bu yöntemle Bitcoin blokzinciri üzerinde herkes veri depolayabilmektedir. Bu sayede isim, adres, şifre, özel gün tarihleri gibi sabit bilgilerin yanında bir internet adresi üzerinden değişken verilerin de blokzincir üzerinde depolanmasının mümkün olduğu görülmektedir.

Şifrelenmiş Veriler

Blok içerisinde veri depolamanın başka bir şekli ise verinin düz metin olarak değil, bir şifrelemeye (İng. "*encryption*") tabi tutularak depolanmasıdır. Şifreleme iki yönlü bir faaliyet olup bu şifrenin çözülmesi (İng. "*decryption*") mümkündür. Bu durumda şifrenin çözülmesi yoluyla kişisel veriye ulaşılabileceğinden bu veri kişisel veri niteliğini kaybetmiş olmaz (Finck, 2019). Bu noktada bazı yazarlar belirli bir seviyenin üzerinde koruma sağlanmış olan verinin artık kişisel veri olarak nitelendirilmemesi gerektiğini savunmuş ve özellikle şifrelemeyi çözecek anahtara sahip olunmayan kişi açısından bir verinin kişisel veri olmayacağını ileri sürmüşlerdir (Hon, Millard ve Walden, 2011).

Bu görüş kabul edilirse AB Hukuku'nda ilgili kişinin belirli ya da belirlenebilir olması şartının verinin depolanacağı süreyle bağlantılı olarak aranacağı da dikkate alınmalıdır. Buna göre eğer veri depolandığı süre boyunca belirli ya da belirlenebilen bir gerçek bir kişiyle ilişkilendirilemiyorsa o zaman kişisel veri olarak nitelendirilemeyecektir (Article 29 Data Protection Working Party, 2007). Bu itibarla eğer şifreleme yöntemi, verinin saklama süresi boyunca saldırılara dayanıklılığını sürdürüyorsa o zaman kişisel veri olarak nitelendirilemeyecektir.

Ancak şifreleme tekniklerinin üçüncü kişiler tarafından ilgili kişilerin rızası olmadan çözülebilmesi ihtimali, özellikle teknolojinin gelişme hızı da dikkate alındığında her an mümkün bulunduğundan ve bu da herhangi bir kişi tarafından ilgili verinin belirli ya da belirlenebilen bir gerçek kişi ile ilişkilendirilmesine imkan vereceğinden bu görüşe katılmıyoruz. Ayrıca böyle bir kabulün, güvenli sanılan sistemlerden siber saldırılar sonucu verilerin çalınması durumunda ilgili kişileri gerekli korumadan yoksun bırakacağını düşünüyoruz.

Hash Olarak Depolanan Diğer Veriler

Blok içerisinde verinin depolanabileceği üçüncü yöntem ise *hash* fonksiyonlarının kullanılması suretiyle oluşturulan çıktıların, yani verinin *Hash*'inin depolanmasıdır. *Hash'*in şifrelemeden farklı tek yönlü bir işlem olmasıdır, bir *hash'*ın çözülmesi ya da kırılması suretiyle asıl veriye ulaşılması mümkün değildir. Ancak asıl veriye ulaşılamayacak olması *hash* fonksiyonlarının kullanımını doğrudan şifreleme yöntemlerine göre daha güvenli hale getirmez. Çünkü *hash* tek yönlü olmakla birlikte aynı zamanda her bir girdi için eşsiz bir çıktı üreten yani her bir veri için dijital bir parmak izi niteliği taşıyan bir değerdir. Bu itibarla bir *hash'*i tersine mühendislik yaparak çözmek mümkün olmasa da mevcut değerleri aynı *hash* fonksiyonuna tabi tutarak çıktıları karşılaştırmak suretiyle *hash* değerlerini bir gerçek kişiyle ilişkilendirmek mümkün olabilecektir. Nitekim ABD Federal Ticaret Komisyonu'nun Teknoloji Şefi Ed Felten de çok sayıda verinin *hash* fonksiyonlarına sokulmasının çok kısa sürede yapılabildiğini ve çıktıların karşılaştırılması vatandaşların suretiyle sosyal güvenlik numaralarına ulaşılabileceğini, *hash* fonksiyonlarının verileri anonim hale getirmediğini ifade etmiştir (Felten, 2012). Nitekim AB Hukuku'nda kişisel verilerin korunması açısından da *hash* fonksiyonlarının veriyi anonim hale getirmediği kabul edilmektedir (Article 29 Data Protection Working Party, 2007; Finck, 2019).

*Hash'*in kullanımındaki önemli başka bir nokta da asıl veriyle bağlantısı incelenmeksizin *hash'*in bir dijital parmak izi gibi faaliyet göstermesidir. Zira veri *hash* haline getirildikten sonra da internet üzerinde kullanılmakta ve kullanıcının bizzat kendi davranışlarıyla ilişkilendirmeyi kolaylaştıracak bilgi akışı yaratılmaktadır. Bunun blokzincirdeki en temel örneği blok içerisindeki işlemler ve daha önce anlatıldığı üzere açık adreslerdir. Bunların izlenmesi suretiyle belirli ya da belirlenebilen gerçeklerle veriyi ilişkilendirmek mümkün olacaktır. Görüldüğü üzere blokzincir üzerinden *hash* olarak depolanan verilerin de bir kişisel veri olabileceği kabul edilmelidir.

BLOKZİNCİR ÜZERİNDE DEPOLANAN KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ, ANONİM HALE GETİRİLMESİ MESELESİ

KVKK m. 7/1 uyarınca mevzuata uygun olarak işlenmiş olmasına rağmen işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir. KVKK m. 7/3 uyarınca kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar Kurum tarafından çıkarılan Yönetmelik ile düzenlenmiştir.

Bu çalışmanın konusunu oluşturan açık-izne tabi olmayan blokzincirler üzerinde depolanan kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi geleneksel sistemlere göre özellik gösterir. Bu blokzincirlerde veriler dağıtılmış bir sistem üzerinde birden çok birimde depolandığından dolayı merkezi sistemlerin aksine tek bir birim üzerinden veriyi silmek yoluyla diğer birimlerin erişimini engellemek mümkün değildir zira her birim isteğe bağlı olarak tüm blokzincir üzerindeki verilere ilişkin kendi kopyasını tutabilmektedir. Birimler tarafından tutulacak kopyalar blokzincirin temelinde yer alan yazılım tarafından belirlenmiş kurallara tabi olmakla birlikte yeni eklenecek verilerin seçimi de yine tek bir kişi ya da kurumun tekelinde olmadığından yani merkezi olmayan bir yapı söz konusu olduğundan bir emir ya da talimat yoluyla kişisel verilere erişimin engellenmesi de mümkün olmayacaktır.

Bu açıklanan sebeplerle açık-izne tabi olmayan blokzincirlerin değiştirilemez (İng. "*immutable*") oldukları ifade edilmektedir ancak bu doğru bir tespit değildir. Blokzincir üzerine depolanan veriler ağdaki katılımcıların bir araya gelip karar vermesi durumunda veya uzlaşı protokollerine uymak suretiyle değiştirilebilir. Nitekim Ethereum blokzincirinde bir yazılımsal boşluğun kullanılması sonucunda yaşanan hırsızlığın etkilerini geri almak için Ethereum blokzincirine müdahale edilmiş ve zincir belirli bir zamandaki haline geri döndürülmüştür (Güçlütürk, 2018b). Blokzincir değiştirilemez veya müdahaleye dayanıklı olması, değişikliğin yapılmasının teknik gerekçelerle çok zor olması şeklinde anlaşılmalıdır (Finck, 2019). Tamamen değiştirilemez olmasa da blokzincir üzerinde depolanan verilerin silinmesinin, değiştirilmesinin, yok edilmesinin çok zorlaştırılmış olması KVKK m. 7 ve anılan Yönetmelik bakımından sorun yaratmaktadır. Blokzincir üzerinde depolanan verileri doğrudan silmek, yok etmek veya anonim hale getirmek gibi değişiklikler çok zor olduğundan bu konuda alternatif çözüm önerileri ileri sürülmüştür.

Öncelikle burada blokzincir üzerinde depolanan verilerin kullanılan teknikler aracılığıyla halihazırda anonim hale getirilip getirilmediği tartışmalı olduğu belirtilmelidir. Eğer şifreleme, *hash* üretme gibi yöntemlerin veriyi anonim hale getirdiği kabul edilirse KVKK m. 7 anlamında bir sıkıntı çıkmayacaktır. Ancak daha önce açıkladığımız üzere biz de genel olarak kabul edildiği üzere bu yöntemlerin veriyi anonim hale getirdiğini düşünmüyoruz. Bu sebeple KVKK m. 7 ile blokzincir teknolojisi arasında uyumsuzluğun başka yöntemlerle çözülmesi gerektiği kanaatindeyiz.

Önerilen yöntemlerden bir tanesi şifrelenmiş veriyi çözebilen veya *hash* olarak depolanan verilere erişimi sağlayan kullanılan özel anahtarların yok edilmesinin silinme kapsamında değerlendirilmesidir (Finck, 2019). Bu ihtimalde aslında veri blokzincir üzerinden, dolayısıyla blokzincir ağına bağlı birimler üzerinden gerçek anlamda silinmemektedir ancak şifrelenmiş verinin çözülmesi veya veriye erişim engellenmiş olmaktadır. Bunun işlevsel anlamda bir silme veya yok etme olup olmadığı tartışmalıdır. İlk olarak bunun blokzincir üzerinde doğrudan depolanan kişisel veriler için bir çözüm üretmediği unutulmamalıdır. İkinci olarak özel anahtarın yok edilmesi şifrenin çözülmesini veya verinin erişimini sadece meşru zeminlerde engelleyecektir. Başka bir deyişle daha önce bahsedildiği üzere söz konusu şifrelenmiş verilerin üçüncü kişiler tarafından çözülmesi ya da gelişen teknolojiyle birlikte ilgili veriye erişimin başka imkanlarla sağlanması mümkün olabilecektir. Fransız veri koruma otoritesi yayınladığı rehberde olası çözümlerden biri olarak *hash*'a erişim sağlayan anahtarın silinmesini de zikretmiş ancak genel olarak bu dahil önerilen yöntemlerin GDPR'a tam uyumluluğuna da sorgulayıcı şekilde yaklaştığını belirtmiştir (Commission Nationale de L'Informatique et des Libertés, 2018).

Bir diğer önerilen çözüm ise kişisel veri niteliğindeki verilerin blokzincir üzerinde depolanmaması, blokzincir üzerinde bu verilerle işlem yapılacak olsa bile kişisel verinin blokzincir dışında depolanması ancak blokzincir üzerinde sadece o veriye erişim sağlayacak bir *hash*'in depolanması şeklindedir (Berberich ve Steiner, 2016; Finck, 2019). Böyle bir yöntemin silme, yok etme ve anonim hale getirme işlemini kolaylaştıracağı şüphesizdir. Gerektiğinde blokzincir dışında depolanan kişisel veri silinecek, yok edilecek veya anonim hale getirilecektir ve bu andan sonra blokzincir üzerinden bu veriye de ulaşılamayacak, ilgili bağlantı işlevini yitirmiş olacaktır. Burada iki önemli noktaya dikkat edilmesi gerekecektir. İlk olarak bazı verilerin blokzincir dışında depolanması blokzincirin önemli bir özelliği olan güvenlik unsurunu zedeleyebilecektir zira kişisel verinin blokzincir dışına taşınması merkezi bir kontrole bırakılması demek olacaktır. İkincisi ve daha önemlisi ise blokzincir üzerindeki bağlantının yani *hash*'ın silinmesi yine de mümkün olmayacağından bu bunun bir kişisel veri olup olmayacağının dikkatle değerlendirilmesidir. Eğer bu *hash* açık adresler gibi bir kimlik işlevi görmeye başlarsa bu takdirde çözüm etkisiz kalacaktır zira bu suretle *hash* kişisel veri niteliği kazanacak ve silinemeyecektir. AB Parlamentosu için hazırlanan raporda da bu konuda belirsizliklerin olduğu ve regülasyona ilişkin çalışmaların yapılmasının gerekliliği vurgulanmıştır (Finck, 2019).

Başka bir öneri olarak özel *hash* yöntemleri kullanılarak daha kolay değiştirilebilir blokzincirlerin oluşturulması ileri sürülmüştür. Ancak kolaylıkla değiştirilen bir blokzincir açık-izne tabi olmayan blokzincirlerin topluluklar tarafından kullanılmasının altında yatan tüm faydaları kaldıracağından böyle bir çözüm aslında söz konusu blokzincirin esaslı unsurlarının değişmesi sonucunu doğuracaktır (Finck, 2019). Bu sebeple anılan soruna uygun bir çözüm olduğunu düşünmüyoruz.
Bunlar haricinde özel şifreleme yöntemleri, sadece belirli bir verinin mevcut olup olmadığına ilişkin dönüş sağlamaya yönelik ve veriye erişimi kapatan ikili güvenlik sistemleri gibi başka çözüm önerileri de ileri sunulmuş olmakla bizce bu detaylı çözümler aynı zamanda ilgili blokzincirin teknik altyapısını ve dolayısıyla sorunun niteliğini değiştirmektedir.

Mevcut blokzincir uygulamaları kapsamında baktığımızda ise bizce de halihazırda işlemekte olan açık ve izne tabi olmayan blokzincirlere depolanacak kişisel verilerin daha sonra silinmesi, yok edilmesi ve anonim hale getirilmesi sorunludur. Mevcut çözümler arasından mevzuata en uygun sonuçları doğuracak olan verilerin blokzincir haricinde depolanmasıdır. Bu çözüm aynı zamanda büyük verilerin depolanamaması sorununa da çözüm getirebilecektir. Ancak verilerin bu şekilde bağlantılarla blokzincirde depolanmasına karar verilirse bu takdirde güvenlik unsuru ve blokzincir ile dışarıda depolanan veriler arasındaki bağlantıyı sağlayacak *hash*'in kişisel veri niteliğinde olmaması özellikle göz önünde bulundurulmalıdır.

SONUÇ

Blokzincirler farklı amaçlarla farklı şekillerde üretilen veri kayıtlarıdır. Verilerin depolanma şeklinden başlayarak içeride depolanan verilerin niteliğine kadar her şey ilgili blokzincirin özelliğine göre değişmektedir. Dolayısıyla bir blokzincir uygulamasının kişisel verilerin korunması mevzuatına uygunluğuna ilişkin değerlendirmenin her bir olayın özelliklerine göre ayrı ayrı değerlendirilmesi gerektiği unutulmamalıdır.

Bununla birlikte açık ve izne tabi olmayan blokzincirlerde bazı ortak sonuçlara ulaşmak mümkündür. Bu blokzincirlerde farklı nitelikte veriler olmakla birlikte çoğunda ortak olan veri tiplerinden blok başlığında yer alan veriler çoğunlukla kişisel veri niteliği taşımamaktadır. Blok içerisinde yer alan verilerden özellikle işlemlerin kullanıcılar tarafından yapılması ve birimler tarafından onaylanması için kullanılan açık anahtarların/adreslerin ise her ne kadar katılımcıların gerçek kimliğini gizlemek için yeterli olsalar da başka bilgilerle birleştirildiğinde belirli ya da belirlenebilen bir gerçek kişiyle ilişkilendirilebildiklerinden KVVK kapsamında kişisel veri olarak nitelendirilmeleri gerekir.

Bunun haricinde blokzincir üzerinde şifreleme veya *hash* fonksiyonlarının kullanımı yoluyla verilerin doğrudan anonim hale getirilemediğinin kabulü gerekir çünkü bu işlemlere rağmen izleme ve diğer bilgilerle birleştirme yoluyla belirli veya belirlenebilen bir gerçek kişiyle ilişkilendirme mümkün olmaktadır.

Blokzincir üzerinde depolanan kişisel verilerin gerektiğinde KVKK m. 7 uyarınca silinmesi, yok edilmesi ve anonim hale getirilmesi konusunda ise henüz tatmin edici teknik bir çözüm mevcut değildir. Blokzincir üzerinde depolanan kişisel verilerin mevcut yaygın açık ve izne tabi olmayan blokzincirlerde kural olarak değiştirilmelerinin çok zor olduğu açıktır. Bu alanda mevzuata uygunluğu sağlayacak teknik mekanizmalar geliştirilene kadar mevzuata uygunluğu en kolay sağlayabilecek yöntem kişisel verinin blokzincir dışında depolanması ve blokzincir üzerinde depolanacak bir *hash* ile bağlantı kurulmasıdır. Ancak bu durumda bu *hash* silinemeyeceği için bu bağlantının ilgili *hash*'a kişisel veri niteliği yüklemeyecek şekilde kurulması önemlidir.

KAYNAKLAR

Article 29 Data Protection Working Party. (2007*). Opinion 4/2007 on the Concept of Personal Data (Opinion No: 01248/07/EN)*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf adresinden 28.10.2019 tarihinde alınmıştır.

Bashir, I. (2017). *Mastering Blockchain*. Birmingham/Mumbai.

Berberich, M. ve Steiner, M. (2016). Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers*? European Data Protection Law Review*, 2(3), 422-426.

Commission Nationale de L'Informatique et des Libertés. (2018). *Solutions for a responsible use of the blockchain in the context of personal data*. https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf adresinden 29.10.2019 tarihinde alınmıştır.

Develioğlu, H. M. (2017). *6698 sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü uyarınca Kişisel Verilerin Korunması Hukuku*. İstanbul: On İki Levha Yayıncılık.

Felten, E. (2012, 22 Nisan). "*Does Hashing Make Data "Anonymous"?* Federal Trade Commission. https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous adresinden 29.10.2019 tarihinde alınmıştır.

Finck, M. (2017). Blockchains and Data Protection in the European Union. *SSRN Electronic Journal*. doi:10.2139/ssrn.3080322

Finck, M. (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* (Study No: PE 634.445). Brussels: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf adresinden 28.10.2019 tarihinde alınmıştır.

Güçlütürk, O. G. (2018a). *Blockchain: A Trustless Network or a Technologically Disguised Shift of Trust?* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3440044 adresinden 29.10.2019 tarihinde alınmıştır.

Güçlütürk, O. G. (2018b). *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts. Medium.* https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562 adresinden 28.10.2019 tarihinde alınmıştır.

Hon, W. K., Millard, C. ve Walden, I. (2011). *Who is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2* (No: 77/2011). Legal Studies Research Paper. Queen Mary University of London.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf adresinden 20.10.2019 tarihinde alınmıştır.

Roy, B. ve Meier, W. (2005). *Fast Software Encryption*. Berlin; London: Springer. http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=3088651 adresinden 29.10.2019 tarihinde alınmıştır.