MÜHF-HAD Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 28, Sayı 1, Haziran 2022, ISSN: 2529-0142, ss. 602-625 • DOI:10.33433/maruhad.1093624

ARAŞTIRMA MAKALESİ
RESEARCH ARTICLE

Blokzincir, Veri Koruma ve Genel Veri Koruma Tüzüğü*

Blockchain, Data Protection and General Data Protection Regulation

Bilâl Toprak**

ÖZ

Blokzincir her geçen gün kullanımı yaygınlaşan bir teknolojidir. Blokzincir ile kriptografi kullanılarak birbirine bağlanan blokların kayıt listesi tutulmaktadır. Blokzincirde veriler sıralanarak bloklara kaydedilir ve her blok bir zaman damgasına sahiptir. Bir blok dolduktan sonra yeni bir blok üretilir.

Dağıtık kayıt sistemlerinde veriler belirli bir yerde değil birden fazla yerde ve yine birden fazla kontrol mekanizmasıyla muhafaza edilerek güvenlik sağlanmaktadır. Böylelikle sistemde bulunan verinin sadece bir yerde tutulması halinde ortaya çıkabilecek olan bozulma, silinme ve saldırıya uğrama gibi problemler ortadan kalkmış olur. Blokzincir sistemi bir dağıtık kayıt sistemidir.

Herhangi bir veri parçası Blokzincir teknolojisi ile işlendiğinde, hash adı verilen benzersiz, 256 bitlik bir sayıya dönüştürülür. Aynı veri girildiği sürece her zaman aynı sonuç ortaya çıkar. Hash sistemi ters çevrilerek çalıştırılamaz, bu sayede sistemden çıkan sonuçtan sisteme giren verilere ulaşmak imkansızdır.

Genel Veri Koruma Tüzüğü madde 4/1'e göre; kişisel veri belirli veya belirlenebilir bir gerçek kişiye ait her türlü bilgi anlamına gelir. Bir Blokzincirin kullanım durumuna bağlı olarak bloklarda depolanan veriler, belirlenmiş veya belirlenebilir bir gerçek kişiye ait veriler olabilir.

Genel Veri Koruma Tüzüğü'ne göre veri sorumlusu kişisel verilerin işlenme amaç ve vasıtalarını tek başına ya da başkalarıyla birlikte belirleyen gerçek veya tüzel kişi, kamu makamı, kurumu ya da diğer bir kamu kuruluşu anlamına gelir. Blokzincir sisteminde veri sorumlusunun kim olabileceği, Blokzincirdeki bütün aktörlerin veri sorumlusu olarak kabul edilip edilemeyeceği, madencilerin hangi kategoriye sokulabileceği hususları değerlendirilmelidir. Ayrıca hash değerlerinin, açık anahtar ve özel anahtarların kişisel veri niteliği, değerlendirilmesi gereken bir başka konudur.

Genel Veri Koruma Tüzüğü'ne göre veri sahibinin veriye erişim, verinin düzeltilmesi ve verinin silinmesini talep etme hakkı bulunmaktadır. Blokzincir sisteminde veri sahibinin bu haklarını nasıl kullanabileceği belirsizdir. Genel Veri Koruma Tüzüğü madde 3'e göre, bu tüzük veri işlemenin Birlik sınırlarında gerçekleşip gerçekleşmediğine bakılmaksızın belirli şartlar dahilinde geniş bir çerçevede uygulama alanı bulur. Blokzincir sisteminin Genel Veri Koruma Tüzüğü'nün uygulama alanına girip girmediği incelenmelidir.

Anahtar Kelimeler: Blokzincir, Kişisel Veri, Veri Koruma, Genel Veri Koruma Tüzüğü, Dağıtık Kayıt Sistemi.

* 12-14 Kasım 2021 tarihlerinde KVKK, İstanbul Üniversitesi ve Türk Alman Üniversitesi ortaklığıyla yapılan I. Uluslararası Kişisel Verileri Koruma Kongresi'nde sunulan sözlü tebliğin genişletilmiş ve düzeltilmiş tam metin halidir.

** Araştırma Görevlisi, Ankara Yıldırım Beyazıt Üniversitesi Hukuk Fakültesi, ORCID ID: 0000-0002-8539-9959.

Sorumlu Yazar/Correspondence Author: Bilâl Toprak
E-posta/E-mail: bilaltoprak@aybu.edu.tr

Geliş Tarihi/Received: 25.03.2022 **Kabul Tarihi/Accepted:** 10.06.2022

ABSTRACT

Blockchain is a technology that is becoming widespread every day. A record list of blocks connected to each other using blockchain and cryptography is kept. In the blockchain, the data is sorted and saved in blocks, and each block has a time stamp. After a block is full, a new block is generated.

In distributed ledger technology, security is ensured by keeping the data not in a specific place, but in more than one place and again with more than one control mechanism. In this way, the problems such as corruption, deletion and attack that may occur if the data contained in the system is kept only in one place are eliminated. The blockchain system is a distributed ledger technology.

When any piece of data is processed using Blockchain technology, it is converted into a unique, 256-bit number called a hash. As long as the same data is entered, the same result will always occur. The hash system cannot be executed by inverting it, so it is impossible to access the data entering the system from the result coming out of the system.

According to Article 4/1 of the General Data Protection Regulation, 'personal data' means any information relating to an identified or identifiable natural person. Depending on the use of a blockchain, the data stored in the blocks may be data belonging to an identified or identifiable natural person.

According to the General Data Protection Regulation, 'controller' means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Who can be the data controller in the blockchain system, whether all the actors in the blockchain can be considered as data controllers, and which category the miners can be put into should be evaluated? In addition, it is another issue that needs to be evaluated whether the hash values, public key and private keys are personal data.

According to the General Data Protection Regulation, the data subject has the right of access to the data, rectification of the data and erasure of the data. It is unclear how the data owner can use these rights in the blockchain system. According to article 3 of the General Data Protection Regulation, this regulation finds wide scope of application within certain conditions, regardless of whether data processing takes place within the borders of the Union. It should be examined whether the Blockchain system falls within the scope of the application of the General Data Protection Regulation.

Keywords: Blockchain, Personal Data, Data Protection, General Data Protection Regulation, Distributed Ledger Technology

GİRİŞ

Genel Veri Koruma Tüzüğü (Tüzük) ve Blokzincir sisteminin birbiriyle ilişkisi çeşitli güçlükleri bünyesinde barındırmaktadır. Tüzük hazırlık aşamasındayken Blokzincir sistemi henüz günümüzdeki kadar yaygın bir şekilde kullanılmadığından göz önünde bulundurulma gereği duyulmamıştır. Bu sistemin o yıllarda bilinen tek uygulama örneği olarak Satoshi Nakamoto tarafından duyurulan Bitcoin sistemi olduğu söylenebilir.

Blokzincir sisteminin kullanım alanlarının yaygınlaşması neticesinde bir taraftan diğer tarafa bilgi akışı oldukça kolay bir hale gelmiştir. Sistem belirli prensipler ışığında çalışmakta ve dünyanın herhangi bir yerinde bulunan taraflar arasında çeşitli veri aktarımı yapılabilmektedir. Tüzük Avrupa Birliği tarafından hazırlanırken belirlenen temel hedeflerden birisi veri aktarımının güvenli şekilde sağlanmasıdır. Burada verinin ne olduğuna ilişkin kapsam da geniş tutularak bireyler bakımından daha geniş bir koruma sağlanması hedeflenmiştir. Kapsamın geniş tutulması, Blokzincir sisteminin

yaygınlaşması ve Tüzük'ün yürürlüğü girmesi neticesinde kişisel verilerin korunmasına ilişkin çeşitli sorunlar ortaya çıkmaya başlamıştır.

Blokzincir sistemi merkeziyetsiz olarak tasarlanmıştır. Bu sisteme giren her şey dağıtık kayıt sistemi adı verilen ve dünyanın hemen her yerine yayılmış sunuculara yayılır. Böylelikle bir sunucudan kaynaklı olası bir sorundan ötürü bilgiye erişim kesintiye uğramaz. Ayrıca sunucularda yer alan bilgiler birbirinin aynısı olacağından bir sunucuya yapılan saldırı neticesinde kötü niyetli ortaya çıkabilecek hareketlerin önüne geçilir. Çünkü diğer sunucularda bu bilgiler ilk halleriyle olduğu gibi korunmaktadır. Tüzük merkeziyetsiz bir yapıya uygun değildir. Tüzük ile veri sahiplerine çeşitli haklar verilmiş, veri sorumlularına ise çeşitli yükümlülükler yüklenmiştir. Burada veri koruma otoriteleri olası uyuşmazlıklarda bir muhatap bulmak isterler. Bu durum Blokzincir sisteminin çalışma mantığı ile birçok noktada uyumsuzluğa neden olmaktadır.

Genel Veri Koruma Tüzüğü ve Blokzincir sisteminin uyumsuz yapıları göz önüne alındığında Blokzincir sisteminde yer alan verilere ilişkin Tüzük bakımından bir değerlendirme yapılması gereği ortaya çıkmıştır. Buradan hareketle Tüzük ve Blokzincir sistemi incelenip problemler ortaya konulmuş ve olası çözüm önerileri sunulmaya çalışılmıştır.

1. BLOKZİNCİR TEKNOLOJİSİ

A. KAVRAM

Blokzincir sisteminin herkes tarafından uzlaşı sağlanmış ve kabul görmüş evrensel bir tanımı bulunmamaktadır. Blokzincir, bir algoritma tarafından tutulan ve birden fazla düğümde yani dağıtık kayıt sistemini depolayan bilgisayarlarda depolanan, paylaşılan ve senkronize olan dijital bir veri tabanıdır[1]. Böylelikle merkezi bir sunucu sistemi ya da güvenilir bir otorite kaldırılarak oluşturulan güven mekanizması internetin geneline dağıtılmış olmaktadır[2]. Ayrıca Blokzincir, verilerin sıralı bir şekilde bloklara kaydedildiği, her bir kaydın zaman damgasının olduğu, bir blok dolunca sonraki blokun üretildiği, blokların zincir şeklinde birbirine bağlı olduğu bir veri tabanıdır[3]. Kısaca söylemek gerekirse Blokzincir, matematiksel yöntemler içeren ve bunun getirdiği imkanlarla şeffaf, güvenilir ve tutarlı bir altyapı sağlayan bir teknolojidir[4].

1 Michèle Finck,'Blockchain Technology' in Michèle Finck (ed), *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018) 6; Rosanna Mannan, Rahul Sethuram and Lauryn Younge,'GDPR and Blockchain: A Compliance Approach' (2019) 5 European Data Protection Law Review (EDPL) 421-426, 422; Georgios Dimitropoulos,'The Law of Blockchain' (2020) 95 Washington Law Review 1117-1192, 1127.

2 Blokzincir teknolojileri hakkında bilgi için bkz; <https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html> Erişim Tarihi 01.12.2021.

3 Vedat Güven ve Erkin Şahinöz, *Blokzincir – Kripto Paralar – Bitcoin* (Kronik 2018) 44; Unal Tatar, Yasir Gokce and Brian Nussbaum,'Law versus technology: Blockchain, GDPR, and tough tradeoffs' (2020) Computer Law & Security Review 1-11, 2.

4 Gülçin Büyüközkan Feyzioğlu,'Teknolojide Yeni Çağın Başlangıcı: Blokzincir' iç E. Eylem Aksoy Retornaz and Osman Gazi Güçlütürk (edr), *Gelişen Teknolojiler ve Hukuk I – Blokzincir ve Hukuk* (Onikilevha 2021) 19.

Ethereum'un mucidi Vitalik Buterin'in Blokzincir tanımı da dikkate değerdir. Buterin'e göre Blokzincir, herkesin program yükleyebileceği ve programları kendi kendilerine çalışması için bırakabileceği, her programın mevcut önceki bütün durumlarının her zaman ve herkes tarafından erişilebilir olduğu ve programların zincir üzerinde çalıştığına dair çok güçlü bir kripto-ekonomik güvenlik garantisi taşıyan sihirli bir bilgisayardır[5].

B. HERKESE AÇIK VE ÖZEL BLOKZİNCİRLER

Blokzincir sistemlerinin tek bir türü yoktur. Herkese açık veya özel, izinli ya da izinsiz, merkezi yapılı veya merkezi yapılı olmayan Blokzincir sistemleri olabilir. Herkese açık ve izin gerektirmeyen blokzincirlerde, herkes gerekli yazılımı temin edip kurarak bir düğümü edinebilir[6]. İzin gerektirmeyen bu tarz bir sistemde katılım için herhangi bir kısıtlama olmamakla birlikte şeffaflık bu sistemlerin önemli bir özelliğidir[7].

Herkese açık sistemlerde herhangi bir erişim kısıtlaması yer almadığı için gerekli yazılıma sahip her kişi sistemdeki bütün defteri indirebilmekte ve eşler arasındaki işlem verilerini görüntüleyebilmektedir[8]. Burada şeffaflık olabilecek en üst düzeydeyken, gizlilik ise en aza indirilmiş olunmaktadır.

Blokzincirlerin birden fazla türünün olabileceğinden bahsetmiştik. Bu sistemler özel ve ancak bir izin aracılığıyla erişilebilir sistemler de olabilir. Burada sisteme bir sanal özel ağ (VPN) ile erişilebilir. Böylelikle sadece belirli kişilerin verilere erişimi bulunabilir[9]. İzinli ve izinsiz sistemler arasındaki temel fark birine katılmak için erişim serbestisi bulunurken diğerinde buna ihtiyaç duyulmamasıdır[10]. İzinsiz Blokzincir sistemleri herkesin kullanımı için genele hitap eder tarzda tasarlanmışken, izinli Blokzincir sistemleri ise genellikle belirli bir amaç için tasarlanırlar. İzinli sistemler herkesin

5 Vitalik Buterin, *Visions, Part 1: The Value of Blockchain Technology* <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/> Erişim Tarihi 01.12.2021.

6 Primavera De Filippi and Aaron Wright,*Blockchain and the Law: the Rule of Code* (Harvard University Press 2018) 31; Rainer Kulms,'Blockchains: Private Law Matters' (2020) Singapore Journal of Legal Studies 63-89, 67; Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone,'Blockchain Technology Overview' (2018) National Institute of Standards and Technology Internal Report 8202 5; Eliza Mik,'Blockchains: A Technology for Decentralized Marketplaces' in Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (2019) 163.

7 Finck, Technologhy, (n1) 14; Büyüközkan Feyzioğlu, (n4) 4; Gyr Eleonor,'Dezentrale Autonome Organisation DAO' (4 Dezember 2017) 4; Robert Herian,'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 1-19, 7; Michael Isler,'Datenschutz auf der Blockchain' (4 Dezember 2017) Jusletter 6; Dimitropoulos, (n1) 1130.

8 Anisha Mirchandani,'The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR' (2019) 29 Fordham Intellectual Property, Media & Entertainment Law Journal 1201-1242, 1210.

9 Mirchandani, (n8) 1211; Eleonor, (n7), 4; Yaga, Mell, Roby and Scarfone, (n6) 5.

10 Büyüközkan Feyzioğlu, (n4) 4; Mesut Serdar Çekin, 'Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı?' (2019) 77 İstanbul Hukuk Mecmuası 315-341, 321.

katılımına ve görüntülemesine açık olan sistemler değildir[11]. Bu sistemlerde tarafların kimlikleri belirli olup sadece bazı niteliklere sahip taraflar sisteme dahil olabilmektedir[12].

C. KULLANICI VE BLOKZİNCİR ARASINDAKİ ETKİLEŞİM

Blokzincir sistemi diğer bütün bilgi teknolojilerinde olduğu gibi veri parçalarından oluşmaktadır. Blokzincir sistemini diğerlerinden ayıran en temel özelliklerden birisi bu veri parçalarının tek bir yerde toplanmaması, düğüm adı verilerin ve birden fazla yere yayılmış şekilde bulunması ve teorik olarak her düğümün birbirinin aynısı olmasıdır[13].

Blokzincir sistemini kullanan bir internet sitesiyle etkileşime giren kullanıcı, açık anahtar adı verilen (bu anahtar uzun bir harf ve sayı dizisinden oluşmaktadır) bir anahtar aracılığıyla tanımlanır[14]. Bu açık anahtar yalnızca kullanıcının kendisi tarafından bilinen bir özel anahtarın kullanımı neticesinde aktive edilmiş olur (özel anahtarın fonksiyonu bir çeşit dijital imza gibidir)[15].

D. DAĞITIK KAYIT SİSTEMİ VE DÜĞÜMLER

Blokzincir sisteminin merkezinde başka bilgi teknoloji sistemlerinde de olduğu gibi dijital veriler bulunmaktadır. Bu parçalar tek bir yerde değil düğüm adı verilen birden çok yerde işlenip depolanmaktadır[16]. Blokzincir sistemini oluşturan her bir bilgi parçası bir sistem aracılığıyla senkronize olmaktadır ve böylelikle merkeziyetsiz bir yapı kurulmaktadır[17]. Buna dağıtık kayıt sistemi denir. Dağıtık kayıt sistemi ile veri bir yerde değil birden çok yerde tutulur. Bunun doğal bir sonucu olarak veri birden çok kontrol mekanizması ile korunarak, tüm verilerin tek bir yerde tutulması neticesinde ortaya çıkabilecek olan silinme, bozulma, kaybolma ve saldırıya uğrama gibi problemlere karşı bir çözüm bulunmuş olur[18]. Veriler aynı anda birden çok yerde depolandığından, bazı düğümlerde bir sıkıntı meydana gelse bile sistemde herhangi bir kayıp meydana gelmemektedir[19].

Düğümler bir Blokzincir sistemindeki her bir katılımcıya verilen genel bir isimdir. Blokzincir ağına bağlı her bilgisayar çeşitli işlemler hakkında bilgi içeren Blokzincirin bir kopyasını alır. Matematiksel algoritmayı açan ve böylece ağın çalışmasını sağlayan Blokzincir ağına bağlı her bir bilgisayar birer

11 Herian, (n7) 7.

12 Finck, Technologhy, (n1) 15; Mik, (n6) 164.

13 Adrien Alberini and Vincent Pfammatter,'Blockchain and Data Protection' in Daniel Kraus, Obrist Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019) 275; De Filippi and Wright, (n6) 34.

14 Grigol Abashidze,'Das Blockchain-System und die Gesetzgebung zu personenbezogenen Daten' (2020) Deutsch-Georgische Zeitschrift Für Rechtsvergleichung 43.

15 Alberini and Pfammatter, (n13) 275-276.

16 Alberini and Pfammatter, (n13) 275; Büyüközkan Feyzioğlu, (n4) 4.

17 Eleonor, (n7), 3; Mik, (n6) 162.

18 Eleonor, (n7), 4; Finck, Technologhy, (n1) 18; Güven ve Şahinöz, (n3) 74; Alberini and Pfammatter, (n13) 275; De Filippi and Wright, (n6)36; Mannan, Sethuram and Younge, (n1) 422.

19 Finck, Technologhy, (n1) 7.

düğümdür[20]. Düğümlerin ortak özelliği Blokzincir ekosistemine dahil olabilmek için her birinin belirli bir donanım ve yazılıma ihtiyaç duymalıdır. Blokzincir sistemi merkezi olmadığı ve eşler arası (P2P) çalışma prensibini benimsediği için düğümler bir yazılım aracılığıyla birbirleriyle etkileşime girerek Blokzincir sisteminin çalışmasını sağlarlar. Düğümler, Blokzincirin bir kopyasını saklar ve bu şekilde blokların güvenliği ve doğruluğu garanti altına alınmış olur[21].

Her düğüm kendi iradesiyle ağa katılmakta ve nihayetinde merkeziyetsiz bir ağ sistemi oluşmaktadır. Özel Blokzincir sistemlerinde düğüm sayısı sınırlıdır ve her düğüm benzersiz bir şekilde tanımlanır. Herkese açık Blokzincir sistemlerinde ise düğüm sayısı sınırsızdır ve herhangi bir kişi bu ağa katılabilir[22].

E. HASH FONKSİYONU

Blokzincir sisteminde bir veri işlenirken bu veri 256 bitlik eşsiz bir diziye dönüştürülür[23]. Buna da hash adı verilir. Hash fonksiyonu, herhangi bir uzunluktaki herhangi bir veriyi standart uzunluktaki bir veriye dönüştüren benzersiz bir parmak izidir[24]. Fonksiyona giren veri tek bir harf veya rakam olabileceği gibi, bir cümle ya da bir paragraf bile olabilir[25]. Kullanıcı sisteme bir giriş değeri verir, sistem bunu hesapladıktan sonra bir çıkış değeri verir. Sisteme girilen veri aynı oldukça çıkış değeri de her zaman aynı olur[26]. Bu husus hash fonksiyonunun değişmez bir kuralıdır. Ancak sisteme giren verinin içindeki harflerden biri küçük harften büyük harfe dönüştürülse bile çıktı verisi tamamen değişir ve yeni bir veri meydana gelmiş olur[27].

Hash fonksiyonunu önemli kılan hususlardan birisi bunun tersine çevrilmesinin mümkün olmamasıdır. Böylelikle çıktı verisi kullanılarak en başta hash fonksiyonuna sokulan veriye ulaşılamayacağı söylenebilir[28]. Ancak gerçekten de hash fonksiyonunun her zaman için tam bir anonimlik sağlayabileceği garanti edilemez. Bazı durumlarda kolaylıkla ve kısa bir sürede hash fonksiyonundan çıkan veri kullanılarak ilk başta sisteme sokulan giriş verisine ulaşmak mümkün olabilir. Bu sebeple hash fonksiyonlarının her zaman için tam anlamıyla anonimlik sonucu doğuracağı söylenemez[29].

20 Geniş bilgi için bkz; <https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f > Erişim Tarihi 01.12.2021.

21 Geniş bilgi için bkz; <https://nodes.com> <https://101blockchains.com/blockchain-nodes/> Erişim Tarihi 01.12.2021.

22 Abashidze, (n14) 44.

23 Yaga, Mell, Roby and Scarfone, (n6) 7.

24 Finck, Technologhy, (n1) 7; Alberini and Pfammatter, (n13) 276; Jorn Erbguth,'Five Ways to GDPR-Compliant Use of Blockchains' (2019) 5 European Data Protection Law Review (EDPL) 427-433, 429.

25 Güven ve Şahinöz, (n3) 50.

26 Alberini and Pfammatter, (n13) 276.

27 Christopher Millard,'Blockchain and Law: Incompatible Codes?' (2018) 34 Computer Law & Security Review 843-846, 844; Yaga, Mell, Roby and Scarfone, (n6) 7; Mannan, Sethuram and Younge, (n1) 423.

28 Alberini and Pfammatter, (n13) 276.

29 Ed Felten, *Does Hashing Make Data "Anonymous"?* <https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous>, Erişim Tarihi 01.12.2021.

Hash fonksiyonlarının anonimliği sorununu kurgusal bir olay ile örneklendirelim; elimizde hash fonksiyonuna sokulmuş bir Türkiye Cumhuriyeti kimlik numarası olduğunu ve çıktı verisini bildiğimizi varsayalım. Bu aşamada henüz kimlik numarasının kendisi bilinmemekte ve hash fonksiyonu geri döndürülemediği için bu veriye ulaşmak mümkün görünmemektedir. Türkiye Cumhuriyeti vatandaşlarının kimlik numaraları 11 haneli rakamlardan oluşmaktadır. 0 rakamı ile başlaması mümkün olmayan bu sayı dizisinin olası bütün ihtimalleri bir Microsoft Excel tablosunda oluşturulup daha sonra hash fonksiyonuna sokulursa ortaya çıkan sonuçlar ile ilk başta elimizde olan hash fonksiyonu çıktısı kıyaslanarak doğru kimlik numarası bulunabilir. Bu işlem günümüzde kullanılan bilgisayarlar aracılığıyla teorik olarak kısa bir sürede yapılabilir. Tüm bunlardan hareketle hash fonksiyonunun Genel Veri Koruma Tüzüğü anlamında bir anonimleştirme ihtiyacını her zaman karşılayamayabileceğini belirtmek faydalı olur[30].

F. AÇIK ANAHTAR – ÖZEL ANAHTAR

Dijital sistemlerin güvenliğinin sağlanmasında çeşitli kriptografik yöntemler kullanılmaktadır. Çoğu zaman kullanıcı adı ve şifre istenen sistemlerde güvenliğin biraz daha artırılmasının istendiği durumlarda daha karmaşık ve çözülmesi zor sistemler kullanılabilmektedir. Blokzincir sisteminde de güvenliğin sağlanması noktasında kriptografik sistemler kullanılarak elde edilen anahtarlar tercih edilmiştir.

Kriptolojide güvenliğin sağlanabilmesi için simetrik ve asimetrik şifreleme kullanılmaktadır. Simetrik şifreleme yönteminde hem şifrenin koyulması hem de çözülmesine yarayan tek bir şifre bulunurken; asimetrik şifrelemede birbiriyle matematiksel olarak bağlantısı bulunan ve farklı olan iki anahtar kullanılmaktadır. Bu iki anahtar birbirinin yerine geçememekte ve birbirini tamamlama görevi görmektedir[31]. Bu anahtarlardan birine açık diğerine ise özel anahtar denir[32]. Açık anahtarlar, gerçek veya tüzel kişilerin ya da bir makinenin işlemlerini takma isimlendirme ile yapabilmesine izin veren bir harf ve sayı dizisinden ibarettir[33]. Açık anahtar şifreleme amacıyla, özel anahtar ise şifrenin çözülmesi amacıyla kullanılmaktadır. Bu anahtarlar arasındaki matematiksel ilişki tek yönlü kabul edilmekte yani açık anahtarın kullanımı ile özel anahtara ulaşılması neredeyse imkânsız kabul edilmektedir[34].

Blokzincir sistemi kullanıldığında özel anahtar kullanıcı ile hesap arasındaki bağlantıyı, genel anahtar ise hesap ile Blokzinciri ağları arasındaki bağlantıyı sağlamaktadır. Her iki anahtar türü de işlemi yapan tarafın izlenebilmesine ancak takma isimlendirme sayesinde bu kişilerin direkt olarak tanımlanamamasına hizmet eder[35]. Açık anahtarlar, isim veya adres gibi ek veriler ile

30 Alberini and Pfammatter, (n13) 283.

31 Yaga, Mell, Roby and Scarfone, (n6) 11.

32 De Filippi and Wright, (n6)15.

33 Finck, 'Blockchains and the General Data Protection Regulation' in Finck Michèle (ed), *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018) 96; Abashidze, (n14) 44.

34 Güven ve Şahinöz, (n3) 45-46.

35 Alberini and Pfammatter, (n13) 281.

ilişkilendirilmedikçe belirli bir veri sahibini nitelemeyen verilerdir[36]. Bu şifreleme sisteminde açık anahtarla şifrelenen veriler yalnızca özel anahtar kullanılarak çözülebilmektedir[37].

G. MADENCİLER

Blokzincir sistemlerinde dijital para birimlerinin iletimi, verilerin depolanması ve akıllı sözleşmelerin işlerlik kazanabilmesi noktasında madencilerin rolü büyüktür. Madenciler bu işlemleri yaptıktan sonra bu çabalarının bir karşılığı olarak blok ödüller ve ücretler almaktadırlar[38].

Madenciler, sisteme bir işlem kaydedildiğinde bunun gerçekliğinin ağ tarafından doğrulanması noktasında yer alan kişilerdir[39]. Dünyanın hemen her yerinden birçok insan bu işlemleri doğrulamak için bir tür rekabet içerisine girer. İşlemlerin doğrulanmasına madencilik denir ve bunun neticesinde çeşitli ödüller alınabilir[40]. Madenciler doğrulama işlemi neticesinde yapılan işlemleri daha önce yapılmış işlemlerin kayıtlarının tutulduğu verilere ekleyerek yaparlar ve Blokzincir defterindeki blokları sabitleyerek bir zincir oluşturup bu blokları birbirilerine bağlarlar[41].

Yeni blokların kabulü bu blokların madenciler tarafından üretilmesine bağlıdır. Bir kullanıcı tarafından yapılan bir işlem imzalandığında bu işlem kaydı bütün sisteme yayılır. Madenciler işlemleri yeni bloklar halinde birleştirirler ve ardından bunu Blokzincir ağında yayınlarlar[42].

2. GENEL VERİ KORUMA TÜZÜĞÜ

A. GENEL OLARAK

Blokzincir ve Genel Veri Koruma Tüzüğü ilişkisini incelemeden önce Tüzük'ün temel kavramlarının incelenmesi isabetli olacaktır. Böylelikle Blokzincir sistemi ile Genel Veri Koruma Tüzüğü ilişkisi incelenirken kavramların daha anlaşılır olması hedeflenmiştir. Bu bölümde Genel Veri Koruma Tüzüğü'nde yer alan bütün hususlar incelenmemiş, sadece Blokzincir sistemiyle alakalı olduğu düşünülen bölümler seçilerek ele alınmıştır.

B. KİŞİSEL VERİ

Kişisel veri gerçek kişiye ilişkin her türlü veri olarak tanımlanabilir[43]. Tüzük m4/1'e göre kişisel veri, belirli ya da belirlenebilir bir gerçek kişiye ait her türlü bilgi anlamına gelir, belirlenebilir gerçek

36 Finck, B. Regulation, (n33) 282.
37 Finck, Technologhy, (n1) 28; Yaga, Mell, Roby and Scarfone, (n6) 11.
38 De Filippi and Wright, (n6)180; Güven ve Şahinöz, (n3) 65.
39 Dimitropoulos, (n1) 1128.
40 Güven ve Şahinöz, (n3) 65; Dimitropoulos, (n1) 1129.
41 Geniş bilgi için bkz; <https://psp.academy/define-blockchain-what-is-the-role-of-miners/> Erişim Tarihi 01.12.2021.
42 Finck, Technologhy, (n1) 20.
43 Geniş bilgi için bkz; Bilal Toprak,İşçinin Kişisel Verilerinin Korunması (Yetkin 2021) 24 vd.

kişi; bir isim, kimlik numarası, konum bilgisi, çevrimiçi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine ilişkin bir veya daha fazla etkene atıfta bulunarak doğrudan ya da dolaylı olarak tanımlanabilen kişidir[44]. Tüzük gerekçesi 30'a göre gerçek kişiler, internet protokol adresleri (IP adresi), çerez tanımlayıcıları veya radyo frekansı tanımlama etiketleri ile ilişkilendirilebilirler[45]. Böylelikle sunucular tarafından alınan benzersiz tanımlayıcılar ve diğer bilgiler birleştirildiğinde gerçek kişilerin profilleri oluşturulabilir.

Kişisel veri, eldeki verilerden ya da veri sorumlusunun elinde bulunan ya da bulunması muhtemel diğer bilgilerle bağlantılı verilerden tanımlanabilen gerçek kişiye ait veriler olarak tanımlanabilir[46]. Kişisel veri tanımının yanında bir de daha çok koruma gerektiren verileri nitelemek için hassas kişisel veriler tanımına da yer verilmiştir. Hassas kişisel veriler, daha yüksek uyumluluk yükümlülükleri ve koşulları içeren, ırk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğine ilişkin veriler ile bir gerçek kişinin kimlik teşhisinin sağlanması amacıyla genetik veriler ve biyometrik veriler, sağlık ile ilgili veriler ya da bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin veriler olarak nitelendirilebilir[47].

C. VERİ İŞLEME

Kişisel verilerin işlenmesi hususu Genel Veri Koruma Tüzüğü'nde tanımlanmıştır. Tüzük m4/2'ye göre işleme, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleşen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla ifşa etme, sıralama ya da birleştirme, sınırlama, silme veya imha etme gibi herhangi bir işlem ya da işlem dizisi anlamına gelmektedir.

Temelde veriler üzerinde yapılacak herhangi bir müdahale veri işleme olarak kabul edilmelidir[48]. İşleme faaliyetinin otomatik yollarla yapılıp yapılmaması yapılan faaliyetin veri işleme niteliğini etkilemez.

D. VERİ SAHİBİ

Kişisel verisi işlenen gerçek kişiye veri sahibi denilebilir. Tüzük'ün tanımlar başlıklı 4'üncü maddesinde doğrudan bir tanım bulunmamakla birlikte 1'inci fıkrada kişisel veri tanımıyla birlikte bir tanıma yer verilmiştir. Buradan hareketle veri işleme faaliyetine konu olan gerçek kişinin, veri sahibi ya da bir diğer kullanımıyla ilgili kişi olduğu kabul edilmek suretiyle tüzel kişiler kapsam dışı bırakılmıştır.

44 Article 29 Data Protection WP,'Opinion 4/2007 on the Concept of Personal Data' (2007) 6.

45 Gerçek kişiyle ilişkilendirilebilen verilerin kişisel veri olduğuna dair bkz; Article 29 Data Protection WP, concept of personal data, (n44) 9.

46 Paul Lambert,*Understanding the New European Data Protection Rules* (CRC Press 2018) 112.

47 Lambert, (n46) 112; Toprak, (n43) 30 vd.

48 Paul Voigt and Axel Von dem Bussche,*The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017) 9; Lambert, (n46) 125; Toprak, (n43) 40.

E. VERİ SORUMLUSU

Veri sorumlusunun tanımına Genel Veri Koruma Tüzüğü'nde yer verilmiştir. Tüzük m4/7'ye göre veri sorumlusu, kişisel verilerin işlenme amaçlarını ve hangi vasıtalar ile işleneceğini tek başına ya da başkalarıyla belirleyen gerçek veya tüzel kişi, kamu kurumu ya da kuruluşu veya diğer herhangi bir organdır. Buradan hareketle hemen her varlığın veri sorumlusu olarak kabul edilebileceği söylenebilir[49].

Veri sorumlusu tek başına hareket edebileceği gibi birden fazla kişiden de oluşabilir. Tüzük hazırlanırken sorumlulukların açık bir şekilde düzenlenmesi hedeflendiğinden 26'ncı maddede ortak veri sorumlularına özel bir düzenlemeye de yer verilmiştir[50].

Veri sorumlusunun tespitinde önemli olan bir diğer husus veri işleme amacının belirlenmesidir. Buna göre veri işlemenin yürütülmesine değil verilerin işlenmesine karar verme gücünü elinde barındıran kişinin veri sorumlusu olduğundan söz edilebilir. Veri sorumlusu işlemenin amacına ve temel unsurlarına karar veren kişidir. Buradan hareketle veri sorumlusu hangi verilerin ne kadar süre işleneceğini, bu verilere kimin erişeceğini, hangi güvenlik önlemlerinin alınması gerektiğini belirleyecek kişidir[51].

F. VERİ İŞLEYEN

Veri işleyenin tanımına Genel Veri Koruma Tüzüğü'nde yer verilmiştir. Tüzük m4/8'e göre veri işleyen, veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu kurumu ya da makamı veya diğer herhangi bir organdır.

Veri sorumlusu veri işleme faaliyetinin bir kısmını veya tamamını, kendi çalışanlarından birine veya dışarıdan seçeceği üçüncü bir veri işleyene devredebilir. Veri işleyenden söz edilebilmesi için veri sorumlusundan ayrı bir gerçek ya da tüzel kişinin bulunması ve veri sorumlusu adına verilerin işlenmesi gerekmektedir[52].

Veri işlemenin hukuka uygun oluşu veri sorumlusunun verdiği iş ile belirlenmektedir. Veri işleyenin görev sınırlarının dışında çıkması durumunda artık o da bir veri sorumlusu olur ve duruma göre ortak veri sorumluluğundan söz edilebilir[53].

49 Voigt and Von dem Bussche, (n48) 18; Lambert, (n46) 125; Toprak, (n43) 34 vd.

50 Voigt and Von dem Bussche, (n48) 18.

51 Voigt and Von dem Bussche, (n48) 19; Toprak, (n43) 34.

52 Article 29 Data Protection WP,'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010) 25; Voigt and Von dem Bussche, (n48) 20; Lambert, (n46) 126; Toprak, (n43) 39.

53 Article 29 Data Protection WP, controller & processor, (n52) 25.

G. ANONİMLEŞTİRME VE TAKMA İSİMLENDİRME

1. ANONİMLEŞTİRME

Anonimleştirme bir gerçek kişiyle verinin herhangi bir bağlantısı kalmayacak şekilde değiştirilmesini sağlayan bir metottur. Tüzük gerekçesi 26'ya göre veri koruma prensipleri veri sahibinin artık tanımlanmadığı ya da tanımlanmayacak şekilde isimsizleştirildiği anonim bilgiler için geçerli olmaz.

Anonimleştirme, rastgeleleştirme ve genelleştirme diyebileceğimiz iki teknikle sağlanabilir. Rastgeleleştirme, veriler ile gerçek kişi arasındaki güçlü bağlantıyı giderirken verilerin doğruluğunu değiştirmeden oluşturulur ve veriler yeterince belirsiz hale geldikten sonra artık gerçek kişiye başvurmak mümkün olmaz[54]. Genelleştirme ise verilerin ilgi ölçeğini veya sırasını değiştirerek (örneğin bir şehir yerine bir bölge ya da bir hafta yerine bir ay) veri sahiplerinin niteliklerini genellemek, seyreltmektir[55].

Genel Veri Koruma Tüzüğü gerekçesi 26'ya göre iyi bir anonimleştirme yapılması halinde artık Tüzük'ün uygulama alanı kalmaz. Anonimleştirme genellikle istatistiki amaçlı veya araştırma odaklı kullanılıyor olsa da veri sorumlusu ya da veri işleyen tarafından anonimleştirilmiş bilgilerin eski haline getirilme ihtimali varsa Tüzük'ün uygulanacağından söz etmek gerekir[56]. Anonimleştirme ile veri sorumluları Tüzük'ün getirdiği birçok yükümlülükten kurtulmakta; zaman, para ve personelden tasarruf edebilmektedir.

Bir işlemin gerçekten anonimleştirme olarak nitelendirilmesi eşiği oldukça yüksektir. Her bir anonimleştirme tekniğinin fonksiyonelliğini test edebilmek için temelde şu üç soruya cevap verilmesi gerekir; (i) bir gerçek kişiyi ayırt etmek hâlâ mümkün müdür? (ii) bir gerçek kişiyle ilgili kayıtları ilişkilendirebilmek hala mümkün müdür? (iii) bir gerçek kişi hakkında bilgiye ulaşılabilir mi?[57] Bu sorulara olumsuz cevap verilebiliyorsa bir anonimleştirmeden söz edilebilir.

2. TAKMA İSİMLENDİRME

Takma isim verme metodu bir gerçek kişinin kimliğinin saklanması için kullanılabilecek pratik bir yöntemdir. Takma isimlendirme kişisel verilerin korunması alanında da kendine yer bulabilmiştir. Tüzük m4/5'e göre takma isimleştirme, ek bilgilerin ayrı bir yerde muhafaza edilmesi ve belirli ya da belirlenebilir gerçek kişiye yöneltilmemesinin sağlanması amacıyla ve teknik ve organizasyonel tedbirlere tabi olması şartıyla, kişisel verilerin ek bilgiler kullanılmadan spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesi anlamına gelir[58].

54 Article 29 Data Protection WP,'Opinion 05/2014 on Anonymisation Techniques' (2014) 12; Article 29 Data Protection WP, concept of personal data, (n44) 21.

55 Article 29 Data Protection WP, Anonymisation, (n54) 16.

56 Voigt and Von dem Bussche, (n48) 13-14.

57 Article 29 Data Protection WP, Anonymisation, (n54) 3.

58 Lambert, (n46) 116.

Takma isimlendirme, ismin veya diğer özelliklerin belirli şekillerde değiştirilmesiyle elde edilir. Kişilerin tanımlanmasına olanak verebilecek ek bilgiler ayrı bir yerde kodlanmalı ve bu bilgilere erişebilecek kişi sayısı sınırlandırılmalıdır[59]. Takma isimlendirilmiş veri anonimleştirilmiş veri değildir ve anonimleştirmenin sağlanabilmesi için ek adımların atılması gerekmektedir[60].

Anonimleştirme neticesinde veri sorumlusunun artık Genel Veri Koruma Tüzüğü bakımından bazı yükümlülükleri yerine getirmek durumunda kalmayacağını söylemiştik. Takma isimlendirmede durum farklıdır. Tüzük gerekçesi 26'ya göre bu yöntem ile ek bilgiler kullanılarak hala veri sahibine erişim mümkündür[61]. Buradan hareketle takma isimlendirme yapan veri sorumluları hâlâ Genel Veri Koruma Tüzüğü kapsamında olup, bundan ötürü ortaya çıkan yükümlülükleri yerine getirmeye devam etmelidirler.

H. VERİ SAHİBİNİN HAKLARI

1. VERİYE ERİŞİM HAKKI

Veri sahibinin en temel haklarından birisi kendisi hakkında işlenmiş olan verilere erişim hakkıdır. Konuyu düzenleyen Tüzük m15'e göre veri sahibi veri sorumlusundan kişisel verilerinin işlenip işlenmediği hakkında doğrulama yapma ve eğer kişisel verileri işleniyorsa bu verilere erişmeyi talep etme hakkına sahiptir. Böylelikle verilerine erişim hakkı olan veri sahibi açısından Tüzük daha etkin bir şekilde uygulanabileceğinden veri işlemenin adilliği ve şeffaflığı da artmış olur[62].

Genel Veri Koruma Tüzüğü gerekçesi 66'ya göre çevrimiçi ortamda unutulma hakkını güçlendirebilmek adına silme hakkı, kişisel verileri herkese açık hale getiren bir veri sorumlusunun bu kişisel verilerin bağlantılarını ve kopyalarını da silmek için bunları işleyen diğer veri sorumlularını da kapsayacak şekilde genişletilmelidir. Bu yapılırken veri sorumlusu veri sahibinin talebini kişisel verilerini işleyen diğer veri sorumlularına da ulaştırılabileceği şekilde gerekli teknolojik altyapıyı hazırlamalıdır.

Veri sahibinin veriye erişim hakkını kullanabilmesi için mutlaka bir veri ihlali olması gerekmemektedir. Veri sahibi istediği her an bu hakkını kullanabilir[63]. Veri sahibinin kişisel verilerine erişim talebinin karşılanmaması durumunda veri sorumlusuna Tüzük m83/5 uyarınca 20.000.000 Euro'ya veya bir önceki mali yıl cirosunun %4'üne kadar idari para cezası uygulanabilir.

59 Voigt and Von dem Bussche, (n48) 15.

60 Article 29 Data Protection WP, Anonymisation, (n54) 21; Alberini and Pfammatter, (n13) 280; Article 29 Data Protection WP, concept of personal data, (n44) 18.

61 Ayrıca bkz; Article 29 Data Protection WP, Anonymisation, (n54) 21; Alberini and Pfammatter, (n13) 281; Article 29 Data Protection WP, concept of personal data, (n44) 12.

62 Voigt and Von dem Bussche, (n48) 150; Lambert, (n46) 182.

63 Lambert, (n46) 183.

2. VERİLERİN DÜZELTİLMESİ VE SİLİNMESİ

a. Genel Olarak

Veri sahibinin kendisiyle ilgili verilerden yanlış işlenenlerinin düzeltilmesini veya silinmesini istemesi Genel Veri Koruma Tüzüğü'nde düzenleme alanı bulabilmiş haklardandır. Tüzük gerekçesi 65'e göre veri işleme özellikle yasa dışı olursa ya da eksik veya yanlış bilgiler içerirse veri sahiplerinin hak ve özgürlüklerini olumsuz yönde etkileneceğinden, Tüzük veri sahibine veri sorumlusunun faaliyetlerini sınırlama ve etkilemeye yönelik farklı imkanlar sunar. Bu haklar düzeltme hakkı ve silme hakkı olarak sayılabilir. Veri sahibi bu haklarını yanlış veya eksik verilerin Tüzük'e göre hukuka aykırı olduğu durumlarda kullanabilir.

Veri sahibi bu haklardan hangisini kullanmak istediğine kendisi karar vermelidir. Hangi hakkın kullanımı en faydalı şekilde olacaksa onun tercih edilmesi veri sahibinin yararına olur. Örneğin veri işleme faaliyetinin yasal olduğu ancak verilerin eksik işlendiği bir durumda düzeltme hakkının kullanımı amaca hizmet eden bir tercih olur[64].

b. Düzeltme Hakkı

Düzeltme hakkı veri sahibinin hakları ve özgürlükleri üzerindeki olası olumsuz veya negatif etkilerin ortadan kaldırılması noktasında yardımcı olabilir[65]. Tüzük m16'ya göre veri sahibi, veri sorumlusundan yanlış olan kişisel verilerinin derhal düzeltilmesini isteme hakkına sahiptir. Veri sahibi, veri işlemenin amaçları göz önünde bulundurulduğunda, gerektiğinde ek beyanda bulunarak eksik kişisel verilerinin tamamlanması hakkına da sahiptir.

Veri sahibinin eksik verilerinin işlenmesi gereken durumlarda veri sorumlusu açısından tekrar hukuka uygunluk kriteri aranmasına gerek yoktur. Burada hem daha önceden hukuka uygun bir veri işleme faaliyetine devam edilir hem de veri sahibinin düzeltme talebinin yerine getirilebilmesi mevzuata uymanın gereğidir. Veri sorumlusu burada bilgi ekleyerek işlenen veri miktarını artırdığından, bu şekilde yapılan bir tamamlama faaliyetinin sadece işleme amacına ulaşmak için gerekli olduğu kadar yapılması önemlidir[66].

c. Silme Hakkı

Genel Veri Koruma Tüzüğü'nün 17'nci maddesinde veri sahibinin verilerinin silinmesini isteyebilmesine yönelik bir düzenleme yapılmıştır. Buna göre veri sahibi, veri sorumlusunun kendisi hakkında işlediği kişisel verilerini gecikme olmaksızın silmesini talep etme hakkına sahiptir ve veri sorumlusu Tüzük m17'de düzenlenen hallerden birinin varlığı durumunda gecikmeden veri sahibinin kişisel verilerinin silmekle yükümlüdür. Tüzük m17/1-a'ya göre hukuka uygun bir şekilde toplanıp yine hukuka uygun bir şekilde işlenen kişisel veriler bakımından en başta var olan veri işleme amacının artık geçerli olmaması durumunda, veri sorumlusunun mevzubahis kişisel verileri silme

64 Voigt and Von dem Bussche, (n48) 154.

65 Voigt and Von dem Bussche, (n48) 154; Lambert, (n46) 191 vd.

66 Voigt and Von dem Bussche, (n48) 156.

yükümlülüğü doğar. Bu durumu bir örnekle açıklayalım. İşçi ihtiyacı duyan bir işverenin vermiş olduğu iş ilanına başvuran işçilerin özgeçmiş dosyalarının işlenmesi ilk etapta hukuka uygundur. Ancak işveren, diğer bir deyişle veri sorumlusu aradığı işçiyi bulup artık o pozisyonu doldurduktan sonra o ana kadar elinde bulunan özgeçmiş dosyaları bakımından veri işleme amacı geçerliliğini yitirmiş olur. Böyle bir durumunda özgeçmiş dosyası sahipleri işverenden talepte bulunabileceği gibi, Tüzük m5/1 uyarınca veri minimizasyonu ilkesi gereği işverenin kendisi de bu dosyaları silme yükümlülüğü altındadır[67].

3. BLOKZİNCİR VE GENEL VERİ KORUMA TÜZÜĞÜ İLİŞKİSİ

A. BLOKZİNCİR SİSTEMİNDEKİ KİŞİSEL VERİLER

1. AÇIK ANAHTAR – ÖZEL ANAHTAR

Blokzincir sisteminde veriler taraflar arasında bir hesaptan diğerine aktarılabilir. Bunun için açık ve özel anahtarlar kullanılmaktadır. Blokzincir sisteminde amaçlanan verilerin taraflar arasında takma isimlendirme yöntemiyle aktarılmasının sağlanmasıdır. Takma isimlendirme, kayıtların birbiriyle ilişkilendirilebilmesini engellemez ve şifrelenmiş kişisel veriler uzmanlar tarafından yeterince zaman ayrıldığında şifre çözme anahtarını bilen birisi gerçek kişiye ulaşabilir[68]. Buradan hareketle şifrelenmiş verilerin anonim veri değil kişisel veri niteliğini haiz veriler olduğu söylenebilir. Böylelikle yoğun bir çaba neticesinde de olsa teorik olarak hâlâ gerçek kişiyle irtibatın sağlanabilmesi açık ve özel anahtarları kişisel veri kategorisine sokmaktadır[69].

Blokzincir sistemine ilişkin yapılan araştırmalar neticesinde açık anahtarların IP adreslerine kadar izlenebildiği, kullanıcıların bir işlemi ağa iletirken doğrudan ağa bağlandıkları ve bu sebeple de IP adreslerinin açığa çıktığı tespit edilmiş ve bu durum kişilerin kimliğine ulaşılabilmesine imkân vermiştir[70]. Kullanıcıların IP adreslerinin tespiti ve yine kendilerine ulaşılması neticesinde açık anahtarların kişisel veri niteliğini haiz olduğu söylenebilir[71]. Avrupa Birliği Adalet Divanı'nın *Patrick Breyer v Bundesrepublik Deutschland* kararında IP adresi kişisel veri olarak sınıflandırılmıştır[72]. Bu karardan hareketle açık anahtarların kişisel veri niteliğini haiz olduğu tekraren söylenebilir. Ancak aynı IP adresini kullanan birden fazla kullanıcı olabileceği için her olayda direkt olarak IP adresinin

67 Voigt and Von dem Bussche, (n48) 157; Lambert, (n46) 198 vd; Toprak, (n43) 126.

68 Finck, B. Regulation, (n33) 96.

69 Alberini and Pfammatter, (n13) 282; CNIL,'Blockchain Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018) 6; Marco Tullio Giordano,'Blockchain and the GDPR: New Challenges for Privacy and Security' in Benedetta Cappiello and Gherardo Carullo (eds), *Blockchain, Law and Governance* (Springer 2021) 282.

70 Finck, B. Regulation, (n33) 97; Abashidze, (n14) 46.

71 Article 29 Data Protection WP,'Processing of Personal Data on the Internet' (1999) 2. Aksi görüş için bkz; Luis-Daniel Ibáñez, Kieron O'Hara and Elena Simperl,'On Blockchains and the General Data Protection Regulation' (2018) 13 University of Southampton 6.

72 Karara ulaşmak için bkz; Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] EU:C:2016:779 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582> Erişim Tarihi 01.12.2021.

bir gerçek kişiye ait kişisel veri olarak nitelendirilemeyeceği kanaatindeyiz. Her somut olayın kendi içinde değerlendirilip sonuca ulaşılması daha hakkaniyetli olur.

Açık anahtar ve özel anahtarların kişisel veri niteliğini haiz olmadan kullanımları için çeşitli önlemler alınabilir. Buna göre karma ve tek seferlik anahtarlara dayalı bir işlem kullanan gizli bir adres ile bu sorun aşılabilir. Monero kripto para biriminde yeni bir özel adres ile gizli bir anahtar oluşturulmak suretiyle işlemin alıcısı gizlenmektedir[73]. Bitcoin'in izahnamesinde ise yapılan işlemin sahibi ile bağlantısını engellemek için yeni anahtar çiftlerinin kullanılması önerilmektedir[74]. Zcash kripto para biriminde yapılan işlemler herkesin erişimine açık şekilde tutulmasına rağmen, ikili doğru yanlış cevap sağlayan sıfır bilgi kanıtları ile gizlilik sağlanabilmiştir[75]. Bir başka çözüm önerisi ise kişisel verilere *gürültü* eklemektir. Bu yapılırken çeşitli işlemler birlikte gruplandırılır ve dışarıdan bakıldığında mevzu bahis işlemin gönderici ve alıcısının tespiti mümkün olmaz[76]. Bu yöntemin umut vadeden yönü 29'uncu Madde Çalışma Grubu'nun aradığı güvencelerin sağlandığı durumlarda, gürültü ekleme tekniğinin kabul edilebilir bir anonimleştirme tekniği olmasıdır[77].

2. DAĞITIK KAYIT SİSTEMİNDEKİ VERİLER

Dağıtık kayıt sistemlerinin standart bir türü bulunmamaktadır. Buradan hareketle her dağıtık kayıt sistemi kendi içinde değerlendirilmeli ve barındırdığı verilerin niteliğine göre değerlendirme yapılmalıdır. Blokzincir sistemine eklenen her veri kişisel veri niteliğini haiz değildir[78]. Herkese açık dağıtık kayıt sistemlerinde her zaman için bir gerçek kişi ile ilgili veya ilişkilendirilebilir veriler bulunabilir. Böyle durumlarda bu veriler Genel Veri Koruma Tüzüğü bakımından korunmaya değer kişisel veriler olur.

Dağıtık kayıt sistemindeki bloklarda veriler düz metin halinde, şifreli olarak ya da zincire hash fonksiyonu ile eklenmiş olarak bulunabilirler. Bloklarda düz metin halinde bulunan ve herhangi bir şifrelemeye tabi olmayan verilerin kişisel veri niteliğini haiz olduğu söylenebilir[79]. Hash fonksiyonuna tabi tutulan işlemler de her zaman için anonimlik sonucuna ulaştırmamaktadır[80]. Bu durum, 29'uncu madde çalışma grubunun değerlendirmesine göre, veriler ile veri sahibinin hala ilişkilendirilebilmesine imkân verdiğinden, bunların kişisel veri niteliğini haiz oldukları söylenebilir[81].

73 Monero kripto para biriminin gizliliği sağlamaya ilişkin politikası hakkında detaylı bilgi için bkz; <https://www.getmonero.org/resources/moneropedia/stealthaddress.html> Erişim Tarihi 01.12.2021.

74 Bitcoin izahnamesine ulaşmak için bkz; <https://bitcoin.org/en/bitcoin-paper> Erişim Tarihi 01.12.2021. Ayrıca bkz; Ibáñez, O'Hara and Simperl, (n71) 7.

75 Geniş bilgi için bkz; <https://z.cash/technology/zksnarks/> Erişim Tarihi 01.12.2021.

76 Finck, B. Regulation, (n33) 98.

77 Article 29 Data Protection WP, Anonymisation, (n54) 12-13.

78 Alberini and Pfammatter, (n13) 282.

79 Finck, B. Regulation, (n33) 93.

80 Mirchandani, (n8) 1225; Isler, (n7) 4.

81 Alberini and Pfammatter, (n13) 283.

Blokzincir sisteminde dağıtık kayıt sistemlerinde yer alan verilerin Genel Veri Koruma Tüzüğü'nün kapsamından çıkarılması için bazı ihtimaller mevcuttur. Sistemde yapılan işlemlere ilişkin verilerin doğrudan Blokzincirinde depolanmasını önleyebilecek birtakım teknik çözümler geliştirilmektedir. Kişisel veriler zincirin dışında muhafaza edilebilir ve sadece bir hash fonksiyonu ile zincire bağlanabilir. Bu durumda zincir içindeki veriler ile zincirin dışında kalan verilerin hash fonksiyonları hâlâ Tüzük anlamında kişisel veri olarak nitelendirilebilecekken, zincir dışı veriler Tüzük kapsamına girmeyecek şekilde ayarlanabilir[82]. Burada zincir dışındaki veriler Tüzük'ün aradığı şekilde başvurunun mümkün olduğu, verilerin şifrelenmiş ve değiştirilme imkanının da bulunduğu bir veri tabanına kaydedilebilirler[83].

B. BLOKZİNCİR SİSTEMİNDE VERİ SORUMLUSU – VERİ İŞLEYEN

Blokzincir sisteminde Genel Veri Koruma Tüzüğü'nden kaynaklanan hakların kullanımı için veri sorumlusunun tespit edilmesi hayati öneme sahiptir. Burada veri sorumlusunun belirlenmesinde zorlayıcı olan kısım dağıtık kayıt sisteminin merkeziyetsiz bir yapısının bulunmasıdır. Genel Veri Koruma Tüzüğü ve diğer birçok veri koruma düzenlemesi, verilerin yönetildiği merkezi yapıların bulunduğu bir düzen için hazırlanmıştır. Ancak Blokzincir sisteminin esası merkeziyetsiz oluşuna dayandığı için burada rolleri tespit etmek her zaman kolay değildir. Genel Veri Koruma Tüzüğü'ne göre veri sorumlusu veri işleme amaçlarını ve araçlarını tek başına belirler[84]. Blokzincir sisteminde bu şekilde tek başına karar alma mekanizması bulunmamaktadır. Bu durum ise veri sorumlusunun tespitini oldukça güçleştirmektedir. Blokzincir sistemindeki aktörleri tek tek ele alarak kimlerin veri sorumlusu olabileceğini tespit etmek faydalı olur.

Blokzincir sistemini ilk defa tasarlayanların veri sorumlusu olup olmadığı sorusu ilk olarak akla gelebilir. Bu tasarımcılar sistemin başlatılması ve işletilmesinden sorumlu olmayıp, veri işleme amacını ve araçlarını belirleme yetkisine de sahip olmadıkları için Genel Veri Koruma Tüzüğü kapsamında veri sorumlusu olduklarından söz etmek mümkün değildir[85].

Blokzincirlerin çeşitli biçimleri bulunmaktadır[86]. Özel Blokzincir sistemlerinde veri sahibinin taleplerine yanıt verebilecek bir sistem yöneticisi gibi merkezi bir aracının tanımlanabilmesi hala mümkündür. Ancak herkese açık dağıtık kayıt sistemlerinde ağ bütün düğümler tarafından merkezi olmayan bir şekilde yönetildiği için tek bir sorumlu ya da merkezi bir kontrol noktası bulunmamaktadır[87].

Düğümlerin veri sorumlusu olup olamayacağı sorusu akla gelebilir ancak düğümler işleme amaç ve araçlarını tek başlarına belirlemedikleri için veri sorumlusu olduklarından söz edilemez. Düğümler

82 CNIL, (N69) 7.

83 Finck, B. Regulation, (n33) 94-95; Mirchandani, (n8) 1229.

84 Veri sorumlusunun nasıl tespit edildiğine dair bkz yukarıda II, E.

85 Alberini and Pfammatter, (n13) 286; Isler, (n7) 13.

86 Bkz yukarıda I, B.

87 Finck, B. Regulation, (n33) 99; Erbguth, (n24) 431.

Blokzincir sistemine katılıp katılmama kararını kendileri verdikleri için özerktirler. Bir görüşe göre düğümler veri işleyendir ve veri sahipleri bu kişilerden talepte bulunabilir[88].

Düğümlerin Genel Veri Koruma Tüzüğü'nün 26'ncı maddesine göre ortak veri sorumlusu olup olmadıklarının da değerlendirilmesi gerekmektedir. Tüzük gerekçesi 79'a göre veri sahiplerinin hak ve özgürlüklerinin yanında denetleyici makamların izleme ve önlemleriyle ilgili olarak veri sorumlularının ve veri işleyenlerin sorumluluk ve yükümlülüklerinin korunması, bir veri sorumlusunun nerede olduğu da dahil olmak üzere Tüzük kapsamına giren sorumluluklar net bir şekilde tahsis edilmelidir. Veri işlemenin amaçları ve araçları diğer veri sorumluları ile belirlendiğinde veya bir veri sorumlusu adına veri işleme faaliyetinin yürütüldüğü durumlarda ortak veri sorumlusu olunmasından söz edilebilir. Düğümlerin hangisinin hangi sorumlulukları veya yükümlülükleri yerine getireceği belli olmadığı gibi veri işleme amaç ve araçlarını da ortaklaşa belirlemeleri söz konusu olmadığından ortak veri sorumlusu oldukları söylenemez[89]. Düğümler Blokzincir sisteminde bireysel bir şekilde hareket ederler. Düğümlerin dışındaki aktörlerden bir grubun ortak amaçlarını gerçekleştirmek amacıyla bir araya gelmeleri halinde ortak veri sorumlusu olup olmayacaklarının da ayrıca değerlendirilmesi gerekmektedir. Fransız Veri Koruma Otoritesi CNIL'e göre bir grup katılımcı Blokzincir sisteminde bir amaç doğrultusunda veri işleme faaliyetine girişecekse veri sorumlusu önceden belirlenmelidir. Bu kişiler grup adına karar veren bir katılımcıyı belirlemeyi ve söz konusu katılımcıyı veri sorumlusu olarak atamayı da tercih edebilirler[90].

Düğümler Blokzincir sisteminde verilerin yalnızca şifrelenmiş halini veya hash fonksiyonunu görür ve üzerinde bir değişiklik yapamazlar. Buradan hareketle düğümlerin Genel Veri Koruma Tüzüğü'nün aradığı şekilde ihtiyaçlara cevap verebilen kişiler olduğu söylenemez[91].

CNIL'e göre, Blokzincire veri yazma hakkına sahip olan ve madencilerin doğrulama yapabilmesi için veri göndermeye karar verebilen katılımcılar veri sorumlusudur. CNIL'e göre bu kişiler veri işleme amaçlarını ve araçlarını belirleyen kişilerdir[92].

Blokzincir sistemi her ne kadar merkeziyetsiz bir yapıda da olsa ve bazı sistemlerde işlemleri kimin gerçekleştirdiğini ve ne zaman gerçekleştirdiğini kimse denetlemese bile, sistemin geliştirilmesi, kurulması, piyasaya sürülmesi ve devam eden faaliyetlerden sorumlu bir veya birden fazla çekirdek geliştirici veya operatör hala bulunmaktadır. Bu kişilerin kişisel verilerin işlenme amaç ve araçlarına muhtemel etkileri göz önünde bulundurulduğunda Genel Veri Koruma Tüzüğü anlamında veri sorumlusu olabileceklerinden söz etmek mümkündür[93].

88 Finck, B. Regulation, (n33) 100; Alberini and Pfammatter, (n13) 288.
89 Alberini and Pfammatter, (n13) 289.
90 CNIL, (N69) 2.
91 Finck, B. Regulation, (n33) 100.; aksi görüş için bkz; Giordano, (n69) 279.
92 CNIL, (N69) 1.
93 Alberini and Pfammatter, (n13) 287. Karşıt görüş için bkz; Isler, (n7) 13.

Birden çok Blokzincir türünün olduğundan söz etmiştik. Özel Blokzincir sistemlerinde kimlerin hangi role bürüneceğinin tespiti nispeten daha kolaydır[94]. Özel sistemlerde işlemleri onaylayan madencilerin veri sorumlusu olduğu söylenebilir[95]. Herkese açık Blokzincir sistemlerinde bütün madencileri veri sorumlusu olarak nitelendirmek ise hayatın gerçeklerinden uzaktır. Burada sorulması gereken soru madencilerin veri işleme amaç ve araçlarını belirleyip belirleyemediğidir. Eğer belirleyebiliyorlarsa madencilere de veri sorumlusu denilebilir[96]. CNIL'e göre madenciler kural olarak sadece katılımcılar tarafından gönderilen işlemleri onaylamakta ve bu işlemlerin amacına dahil olmamaktadırlar. Bu sebeple işleme amaç ve araçlarını tanımlamazlar. Örneğin kendi adına Bitcoin alım satımı yapan kişiler, bu işlemler diğer gerçek kişiler adına mesleki veya ticari bir kaygı güdülmeden yapıldığı sürece veri sorumlusu olarak nitelendirilemezler[97]. Bir an için madencilerin ortak veri sorumlusu olma ihtimali düşünülebilir. Ancak daha önce bahsettiğimiz gibi ortak veri sorumlusu olarak nitelendirilebilmek için birtakım şartların bulunması gerekmektedir. Madencilerin hangisinin hangi sorumlulukları veya yükümlülükleri yerine getireceği belli olmadığı gibi veri işleme amaç ve araçlarını da ortaklaşa belirlemeleri söz konusu olmadığından ortak veri sorumlusu oldukları söylenemez.

Blokzincir sisteminde veri işleyenin tek başına tespiti zordur. Veri sorumlusu adına hareket edilmesi gerekliliği ve Blokzincir sistemlerinin çoğunun merkeziyetsiz yapılardan oluştuğu düşünüldüğünde direkt olarak sistemde yer alan bir kişiye veri işleyen demek hakkaniyetli bir yaklaşım olmaz. Ancak sisteme veri yükleyen herkesin kendisi açısından veri işleyen, diğer kişiler açısındansa potansiyel bir veri işleyen olduğundan söz edilebilir[98]. Bir görüşe göre her düğüm sisteme veri yükleyen diğer düğümler açısından veri işleyendir[99]. Özel Blokzincir sistemlerinde ise durum biraz daha farklıdır. Burada Blokzincir sistemini yöneten bir operatör[100] bulunduğu için bu kişiler veri işleyen olarak nitelendirilebilirler[101]. CNIL'e göre madenciler bazı durumlarda veri işleyen olarak nitelendirilebilirler. Böyle bir durumda madenciler yapılan işlemlerin teknik kriterleri karşılayıp karşılamadığı ve Blokzincir kurallarına göre katılımcının işlemini gerçekleştirmesine izin verilip verilmediğini kontrol ederken veri sorumlusunun talimatlarını takip etmektedirler[102].

C. BLOKZİNCİR SİSTEMİNDE VERİ SAHİBİNİN HAKLARINI KULLANIMI

1. VERİYE ERİŞİM HAKKININ KULLANIMI BAKIMINDAN

Genel Veri Koruma Tüzüğü'nün 15'inci maddesi ile veri sahibine kendisi hakkında işlenen kişisel verilere erişim hakkı verilmiştir. Burada dağıtık kayıt sisteminde bulunan bir veriye erişimin nasıl sağlanabileceği hususunun irdelenmesi gerekmektedir.

94 Giordano, (n69) 279.
95 Isler, (n7) 13.
96 Alberini and Pfammatter, (n13) 287.
97 CNIL, (N69) 2.
98 Alberini and Pfammatter, (n13) 289.
99 Giordano, (n69) 279.
100 Yaga, Mell, Roby and Scarfone, (n6) 35.
101 Alberini and Pfammatter, (n13) 289.
102 CNIL, (N69) 3.

Veri sorumluları dağıtık kayıt sistemlerinde yer alan verilerden hangilerinin şifrelenmiş hangilerinin ise hash fonksiyonuna sokulduğunu her zaman tam anlamıyla bilemeyebilirler. Bir veri sahibinin Blokzincir sistemindeki düğümle düzgün bir bağlantı kurduğu varsayımında bile kendisi hakkında bir veri işlenip işlenmediğini teyit edebilmesi her zaman mümkün olmaz. Veri sahibi istediği her zaman herkese açık bir ağa katılabilir ve buradaki verilerin kopyasını elde edebilir. Ancak burada bu erişimin ve elde edilen verilerin Genel Veri Koruma Tüzüğü anlamında veriye erişimi sağlayıp sağlamadığı düşünülmelidir. Ayrıca Genel Veri Koruma Tüzüğü'ne göre veri sahibi verilerine veri sorumlusu aracılığıyla erişim hakkına sahiptir ve bu veriler kriptografik olarak takma isimlendirilme metoduna maruz kalırsa veri sorumlusu açısından veriye erişim neredeyse imkânsız hale gelir. Kendisi veriye erişemeyen bir veri sorumlusunun veri sahibine cevap verebilmesi mümkün olamaz[103]. Veri sorumlusunun, kişisel verileri doğrulama için madencilere göndermeden önce veri sahibine kolayca erişebileceği ve açık terimlerle formüle edilmiş kısa bilgiler sağlaması bu hakkın kullanımı kolaylaştırabilir[104].

Veri sahibinin verilerine erişimi noktasında değinilmesi gereken bir diğer husus açık anahtar – özel anahtar kullanımıdır. Blokzincir sisteminde diğer dijital platformlarda olduğu gibi 'şifremi unuttum' ya da 'hesabımı kurtar' gibi bir seçenek bulunmamaktadır. Buradan hareketle herhangi bir üçüncü kişinin anahtar aracılığıyla hesap sahibi gerçek kişileri tanımlayabilmesinin mümkün olmadığı söylenebilir[105]. Ancak bir kişi özel anahtarına erişimini kaybettikten sonra bir daha hesabına da erişimi mümkün olmayacağından, veriye erişim hakkını etkili bir biçimde kullanamayacağı da belirtilmelidir.

2. VERİLERİN DÜZELTİLMESİNİ, SİLİNMESİNİ İSTEME HAKKI BAKIMINDAN

Blokzincir sistemi, sonradan kurcalanma ihtimaline karşı dayanıklı ve dirençli oluşuyla öne çıkan bir sistemdir[106]. Özellikle sansüre karşı dayanıklı bir tasarım tercih edildiği için Blokzincir sisteminde bir şeyin '*unutulması*' teorik olarak mümkün değildir[107].

Genel Veri Koruma Tüzüğü m5/1-d'ye göre, kişisel veriler her zaman için doğru ve güncel olmalıdır. Bunun sağlanamadığı durumlarda ise hatalı olan kişisel verilerin gecikme olmaksızın silinmesi veya düzeltilmesinin sağlanması noktasında gerekli bütün makul adımların atılması gerekmektedir.

Veri sorumluları Genel Veri Koruma Tüzüğü bağlamındaki taleplerini veri sorumlusuna yöneltebilirler. Bu durum veri sahibinin söz gelimi kişisel verilerinin düzeltilmesini isteme hakkını bütün düğümlere hitap edebileceği anlamına gelir[108]. Blokzincir sisteminde kapatılan bir bloktaki

103 Finck, B. Regulation, (n33) 106.

104 CNIL, (N69) 8.

105 Alberini and Pfammatter, (n13) 282.

106 Finck, B. Regulation, (n33) 106; De Filippi and Wright, (n6)35; Millard, (n27) 844; Erbguth, (n24) 428; Patrick Van Eecke and Anne-Gabrielle Haie,'Blockchain and the GDPR: The EU Blockchain Observatory Report' (2018) 4 European Data Protection Law Review (EDPL) 531-534, 533.

107 Finck, B. Regulation, (n33) 106; Alberini and Pfammatter, (n13) 291.

108 Finck, B. Regulation, (n33) 105.

veriler bütün düğümlere yayıldığı için veri sahibinin bütün düğümlere ulaşması ve bu talebini iletmesi hayatın olağan akışına aykırıdır. Kaldı ki veri sahibinin düğümlerden birine veya tamamına ulaştığı varsayımında bile Blokzincir sistemi değişikliğe müsaade etmeyecek şekilde programlandığı için düğümlerin böyle bir talebi karşılaması da mümkün değildir[109]. Düzeltilmesi istenen veri yeni bir bloka kaydedildiğinde her ne kadar eski, yanlış veri mevcudiyetini devam ettirecek olsa bile Blokzincir sistemine düzeltilmiş veri de kaydedilmiş olur[110].

Veri sahibinden gelecek taleplere ilişkin çözüm bulunabilmesi adına kişisel verilerin zincir dışında tutulması seçeneği bir çözüm yolu olarak düşünülebilir. Bu şekilde bloka dokunulmadan ve Blokzincir sisteminin değişmezliği ilkesinden de etkilenmeden talepler karşılanabilir[111]. Ayrıca bloklar arasında kişisel verilerin kaldırılmasına izin veren ve blokları birbirine bağlayan hash fonksiyonlarının bozulmadan muhafaza edilebilmesine imkân veren bukalemun hash fonksiyonları da kullanılabilir[112].

Veri sahibinin haklarından bir diğeri veri sorumlusundan kendisi ile ilgili kişisel verilerin gecikmeksizin silmesini istemeyebilmesidir. Bu husus Genel Veri Koruma Tüzüğü'nde 17'nci maddede düzenlenmiştir. Blokzincir sisteminin mevcut haliyle olası veri silme taleplerinin karşılanabilmesi mümkün değildir[113]. Blokzincir sisteminin tasarımında bloklar kapatıldıktan sonra hash fonksiyonu ile bir çıktı alınıp bu değer diğer blokun içine yerleştirildiği için en ufak bir değişiklik bütün blokların değişmesine sebep olur[114]. Hal böyleyken değişikliğe karşı dayanıklı şekilde tasarlanan Blokzincir sisteminde veri sahiplerinin silme taleplerinin mevcut sistemde karşılanmasının imkânsıza yakın olduğu söylenebilir[115]. Veri silme taleplerinin karşılanması için blok dışında şifrelenmiş bir veri tabanı kullanılması bir çözüm yolu olarak değerlendirilebilir[116]. Ayrıca verilerin geri dönüşü olmayacak şekilde şifrelenmeleri halinde bunların Genel Veri Koruma Tüzüğü anlamında silinmiş olduğu kabul edilmektedir[117]. Başka bir metoda göre; bir silme talebi geldiğinde Blokzincire silinmesi istenen veriye referans içeren ve bunu anlamsız kılan bir işlem eklenmesidir. Bu durumda bile hâlâ eski veriler mevcudiyetini muhafaza edebilir[118]. Şu hususu da belirtmek gerekir ki herkese açık

109 Alberini and Pfammatter, (n13) 291; Eleonor, (n7), 4; Mik, (n6) 171; Ibáñez, O'Hara and Simperl, (n71) 6; Giordano, (n69) 282; Tatar, Gokce and Nussbaum, (n3) 5; Herian, (n7) 9.

110 CNIL, (N69) 9.

111 Finck, B. Regulation, (n33) 105; Kulms, (n6) 87; Mirchandani, (n8) 1229; Erbguth, (n24) 433; Mannan, Sethuram and Younge, (n1) 423; Tatar, Gokce and Nussbaum, (n3) 8; Van Eecke and Haie, (n106) 533.

112 Geniş bilgi için bkz; Tatar, Gokce and Nussbaum, (n3) 8.

113 De Filippi and Wright, (n6)35; Alberini and Pfammatter, (n13) 291; Mirchandani, (n8) 1224; CNIL, (N69) 6.

114 Eleonor, (n7), 4.

115 Alberini and Pfammatter, (n13) 293; CNIL, (N69) 8; Mannan, Sethuram and Younge, (n1) 424. Blokzincir sisteminin hiç değişmeyeceğine yönelik düşüncenin hatalı olduğu ve her ne kadar son derece külfetli ve pahalı bir uğraş olsa da bunun mümkün olduğuna dair görüş için bkz Finck, Technologhy, (n1) 30; De Filippi and Wright, (n6)36; Alberini and Pfammatter, (n13) 295; Yaga, Mell, Roby and Scarfone, (n6) 34; Mik, (n6) 172.

116 Finck, B. Regulation, (n33) 107; Kulms, (n6) 87; Mirchandani, (n8) 1229; CNIL, (N69) 8; Millard, (n27) 845; Giordano, (n69) 283.

117 Alberini and Pfammatter, (n13) 295; Mirchandani, (n8) 1238; CNIL, (N69) 8; Ibáñez, O'Hara and Simperl, (n71) 8.

118 Ibáñez, O'Hara and Simperl, (n71) 8.

Blokzincir sistemlerinde '*yüzde 51 saldırısı*'[119] ihtimali bulunmaktadır. Bu saldırının gerçekleşmesi teorik olarak çok zor ve uğraştırıcı olsa bile yinede sisteme müdahalede bulunulabilir[120].

Özel Blokzincir sistemlerinde belirli katılımcıların bloğun içeriğini düzenleme, işlemleri tersine çevirme gibi imkanları bulunmaktadır. Bu sebeple özel Blokzincir sistemlerinde veri sahiplerinden gelecek düzeltme ve silme taleplerinin daha rahat bir şekilde karşılanabileceği söylenebilir.

D. TÜZÜK'ÜN BÖLGESEL UYGULAMA ALANI

Herkese açık Blokzincir sistemlerine dünyanın her yerinden katılım mümkündür. Merkezi olmayan bir sistem şeklinde tasarlanan Blokzincir mekanizmasının bu dağılım üzerinde herhangi bir etkisi bulunmamaktadır. Buradan hareketle tek bir ülkede değil birden çok ülkede eşzamanlı çalışan bir sistem olan Blokzincir sistemine uygulanacak hukuk noktasında problemler ortaya çıkmaktadır.

Genel Veri Koruma Tüzüğü'nün 3'üncü maddesine göre bu tüzük veri işlemenin Birlik içerisinde meydana gelip gelmediğine bakılmadan, Birlik bünyesindeki bir veri sorumlusunun veya veri işleyenin işletmesinin faaliyetleri bağlamında kişisel verilerin işlenmesine uygulanır. Burada amaç Tüzük'ün kapsama alanını geniş tutmaktır. Böylelikle Blokzincir sistemindeki düğümler dünyanın neresinde olursa olsun bloklarda kişisel veri barındırıldığı durumlarda Tüzük'ün uygulama alanına girmiş olurlar.

Blokzincir ve Genel Veri Koruma Tüzüğü'nün bölgesel uygulama alanına ilişkin değinilmesi gereken bir diğer konu sınır ötesi veri işlemelere ilişkindir. Tüzük'ün 44'üncü maddesine göre, işlenmekte olan veya üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarıldıktan sonra işlenmesi amaçlanan kişisel verilerin aktarımı, üçüncü ülke veya uluslararası kuruluşa yapılacak sonraki aktarımları da kapsayacak şekilde, ancak bu Tüzük'ün diğer hükümlerine tabi olmak kaydıyla, bu Bölümde belirtilen koşullara uyulması halinde gerçekleşebilir. Bu Tüzük'le güvence altına koruma seviyesinin zedelenmemesi adına bu Bölüm'de yer alan tüm düzenlemeler uygulanır.

Blokzincir sisteminde bloklar halinde depolanan veriler herhangi bir yerde bulunabilen madenciler tarafından zincire dahil edilmektedir. Dağıtık kayıt sistemi her yeni blokun eklenmesinden sonra bunun düğümlere dağıtılması ve eşitlenmesi şeklinde çalışır. Blokların içinde kişisel veri barındırıldığı göz önünde bulundurulduğunda her yeni blok tamamlandığında sınır ötesi veri işleme faaliyeti yapılmış olur. Burada Tüzük'e uygunluğun sağlanabilmesi için m44'te belirtilen önlemlerin alınması pratikte kolay değildir. Hal böyleyken Tüzük m49/1-a'ya göre veri sahibi bilgilendirilip açık rızasının alınması daha uygulanabilir bir çözüm olabilir[121]. Burada da rızanın nasıl alınacağı ve sonradan veri sahibinin rızasını geri alması durumunda ne olacağı sorusu belirsizliğini korumaktadır. Avrupa

119 Yüzde 51 saldırısı hakkında geniş bilgi için bkz; Güven ve Şahinöz, (n3) 64., ayrıca bkz; <https://medium.com/crypto-wisdom/what-is-51-attacks-in-cryptocurrency-how-does-it-work-ca8642283e43> Erişim Tarihi 01.12.2021.

120 Mik, (n6) 172.

121 Finck, B. Regulation, 103.

Birliği Adalet Divanı *Bodil Lindqvist*[122] kararında kişisel verilerin internet sayfasına yüklenmiş olmasını, bu verilere dünyanın her yerinden erişilebilir olmasına rağmen, sınır ötesi veri aktarımı olarak görmemiş ve bu verilerin gizli olmadığına yönelik değerlendirmede bulunmuştur. Ancak kanaatimizce Blokzincire dahil edilen veriler dünyanın her yerindeki sunucularla eşitlendiği için bunun bir sınır ötesi veri işleme faaliyeti olarak nitelendirilmesi ve buna uygun şekilde veri işleme faaliyeti yapılması gerekmektedir.

SONUÇ

Blokzincir teknolojisinin kullanımı son yıllarda artarak devam etmektedir. Nispeten yeni sayılabilecek bu sistemin kullanım alanları arttıkça daha çok kişiye hitap edeceği ve bünyesinde daha çok kişisel veriyi barındıracağı aşikardır.

Genel Veri Koruma Tüzüğü 2018 yılının mayıs ayında yürürlüğe girmiş ve kişisel verilerin korunması alanında birçok yeniliğe hayatımıza sokmuştur. Tüzük'ün uygulama alanı sadece Avrupa Birliği üyesi ülkeler ile sınırlandırılmadığı için bu değişiklikler ve yenilikler dünyanın her yerindeki birçok kişiyi doğrudan veya dolaylı olarak etkilemektedir.

Blokzincir sistemi ile Genel Veri Koruma Tüzüğü birçok noktada uyumsuzluk içerisindedir. Herkese açık Blokzincir sistemlerindeki veriler ilk bakışta şifrelenmiş ve güvenli gibi görünsede bu bilgilerin kullanımı sonucunda bir gerçek kişinin kimliği tespit edilebilir.

Blokzincir sisteminde merkeziyetçi bir yapı bulunmamaktadır. Bu durum Genel Veri Koruma Tüzüğü'nün aradığı muhatapları / sorumluları bulma noktasında ciddi zorluklara sebebiyet vermektedir. Veri sorumlusu ve veri işleyenin tespiti noktasında bir görüş birliğine şu an için varılabilmiş değildir.

Blokzincir sisteminde veriler herkesin erişimine açık ve değiştirilemez şekilde tutulmaktadır. Bu husus Tüzük'ün temel ilkeleriyle çelişmektedir. Veri sahipleri her zaman için verilerine Tüzük'ün aradığı koşullarda erişemeyebilir. Veri sahibinin en temel haklarından birisi olan verilerin düzeltilmesini ya da duruma göre silinmesini isteme hakkı da Blokzincir sisteminin yapısı gereği amaçlandığı şekilde kullanılamayabilir.

Veri koruma gereklerine cevap verebilecek bir Blokzincir yapısının tasarlanması için çalışmalar yapılmaktadır. Geçici bir çözüm olarak kişisel veri niteliğini haiz bilgilerin Blokzincir dışındaki veri tabanlarında şifreli bir şekilde muhafaza edilmesi ve gerektiğinde düzeltilmesi ya da silinmesi bir çözüm yolu olarak düşünülebilir. Ancak günün sonunda mevzuat ile Blokzincir sisteminin uyumunu sağlayacak değişiklikler yapılmadığı sürece tam anlamıyla bir çözümden söz etmek mümkün olmaz. Kanun koyucu tarafından gerekli düzenlemeler yapıldıktan sonra Blokzincir teknolojisinin veri koruma süreçlerini iyileştirebileceğinden söz edilebilir.

122 Tüzük yürürlüğe girmeden önce uygulamada olan Direktif hükümlerine göre verilen karara ulaşmak için bkz; <https://curia.europa.eu/juris/showPdf.jsf;jsessionid=FCA1C7BD485907B3D581DBA1C747B4C2?text=&docid=48382&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1221894> Erişim Tarihi 01.12.2021.

KAYNAKÇA

Abashidze G, 'Das Blockchain-System und die Gesetzgebung zu personenbezogenen Daten' (2020) Deutsch-Georgische Zeitschrift Für Rechtsvergleichung

Alberini A and Pfammatter V, 'Blockchain and Data Protection' in Kraus Daniel, Obrist Obrist ve Hari Olivier (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Edward Elgar Publishing 2019)

Article 29 Data Protection WP, 'Processing of Personal Data on the Internet' (1999)

Article 29 Data Protection WP, 'Opinion 4/2007 on the Concept of Personal Data' (2007)

Article 29 Data Protection WP, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010)

Article 29 Data Protection WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014)

Buterin V, Visions, Part 1: The Value of Blockchain Technology, <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/>, Erişim Tarihi 01.12.2021

Büyüközkan Feyzioğlu G, 'Teknolojide Yeni Çağın Başlangıcı: Blokzincir' iç Aksoy Retornaz E. Eylem ve Güçlütürk Osman Gazi (edr), *Gelişen Teknolojiler ve Hukuk I – Blokzincir ve Hukuk* (Onikilevha 2021)

CNIL, 'Blockchain Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (2018)

Çekin MS, 'Borçlar Hukuku ile Veri Koruma Hukuku Açısından Blockchain Teknolojisi ve Akıllı Sözleşmeler: Hukuk Düzenimizde Bir Paradigma Değişimine Gerek Var Mı?' (2019) 77 İstanbul Hukuk Mecmuası 315-341

De Filippi P and Wright A, *Blockchain and the Law: the Rule of Code* (Harvard University Press 2018)

Dimitropoulos G, 'The Law of Blockchain' (2020) 95 Washington Law Review 1117-1192

Eleonor G, 'Dezentrale Autonome Organisation DAO' (4 Dezember 2017)

Erbguth J, 'Five Ways to GDPR-Compliant Use of Blockchains' (2019) 5 European Data Protection Law Review (EDPL) 427-433

Felten E, Does Hashing Make Data "Anonymous"?, <https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous>, Erişim Tarihi 01.12.2021

Finck M, 'Blockchain Technology' in Finck Michèle (ed), *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018)

Finck M, 'Blockchains and the General Data Protection Regulation' in Finck Michèle (ed), *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018)

Giordano MT, 'Blockchain and the GDPR: New Challenges for Privacy and Security' in Cappiello Benedetta ve Carullo Gherardo (eds), *Blockchain, Law and Governance* (Springer 2021)

Güven V ve Şahinöz E, *Blokzincir – Kripto Paralar – Bitcoin* (Kronik 2018)

Herian R, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 1-19

Ibáñez LD, O'Hara K and Simperl E, 'On Blockchains and the General Data Protection Regulation' (2018) 13 University of Southampton

Isler M, 'Datenschutz auf der Blockchain' (4 Dezember 2017) Jusletter

Kulms R, 'Blockchains: Private Law Matters' (2020) Singapore Journal of Legal Studies 63-89

Lambert P, *Understanding the New European Data Protection Rules* (CRC Press 2018)

Mannan R, Sethuram R and Younge L, 'GDPR and Blockchain: A Compliance Approach' (2019) 5 European Data Protection Law Review (EDPL) 421-426

Mik E, 'Blockchains: A Technology for Decentralized Marketplaces' in DiMatteo Larry A., Cannarsa Michel ve Poncibò Cristina (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (2019)

Millard C, 'Blockchain and Law: Incompatible Codes?' (2018) 34 Computer Law & Security Review 843-846

Mirchandani A, 'The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR' (2019) 29 Fordham Intellectual Property, Media & Entertainment Law Journal 1201-1242

Tatar U, Gokce Y and Nussbaum B, 'Law versus technology: Blockchain, GDPR, and tough tradeoffs' (2020) Computer Law & Security Review 1-11

Toprak B, İşçinin Kişisel Verilerinin Korunması (Yetkin 2021)

Van Eecke P and Haie AG, 'Blockchain and the GDPR: The EU Blockchain Observatory Report' (2018) 4 European Data Protection Law Review (EDPL) 531-534

Voigt P and Von dem Bussche A, *The EU General Data Protection Regulation (GDPR)* (Springer International Publishing 2017)

Yaga D, Mell P, Roby N and Scarfone K, 'Blockchain Technology Overview' (2018) National Institute of Standards and Technology Internal Report 8202