T.C.
MARMARA ÜNİVERSİTESİ
AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ
AVRUPA BİRLİĞİ HUKUKU ANABİLİM DALI

TÜRK VE AVRUPA BİRLİĞİ VERİ KORUMA HUKUKU BAĞLAMINDA BLOK ZİNCİR TEKNOLOJİSİNDE UNUTULMA HAKKI

YÜKSEK LİSANS TEZİ

GİZEM ÖZ DEMETOĞLU

İstanbul - 2019

T.C.
MARMARA ÜNİVERSİTESİ
AVRUPA ARAŞTIRMALARI ENSTİTÜSÜ
AVRUPA BİRLİĞİ HUKUKU ANABİLİM DALI

TÜRK VE AVRUPA BİRLİĞİ VERİ KORUMA HUKUKU BAĞLAMINDA BLOK ZİNCİR TEKNOLOJİSİNDE UNUTULMA HAKKI

YÜKSEK LİSANS TEZİ

GİZEM ÖZ DEMETOĞLU

Danışman: Doç. Dr. Mesut Serdar Çekin

İstanbul - 2019

TEZ ONAY SAYFASI

Marmara Üniversitesi
Avrupa Araştırmaları Enstitüsü Müdürlüğüne

Enstitünüz, Avrupa Birliği Hukuku Anabilim Dalı Türkçe / İngilizce Yüksek Lisans Programı öğrencisi **Gizem Öz Demetoğlu**, tarafından hazırlanan, **"Türk ve Avrupa Birliği Veri Koruma Hukuku Bağlamında Blockchain Teknolojisinde Unutulma Hakkı"** başlıklı bu çalışma, 3.../9.../2019 tarihin de yapılan savunma sınavı sonucunda ~~OY BİRLİĞİ~~ / **OY ÇOKLUĞUYLA BAŞARILI** bulunarak aşağıda isimleri yazılı jüri üyeleri tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri:

Doç. Dr. Mesut Serdar ÇEKİN	Danışman	.....
Doç.Dr. Mustafa T. KARAYİĞİT	Jüri Üyesi	.....
Dr. Öğr. Üy. Mehmet Bedii KAYA	Jüri Üyesi	.....

Onay

Prof. Dr. Muzaffer Dartan
Müdür

05/09/2019...tarih ve 2019/25.sayılı Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

ÖZET

Gelişen teknoloji ile birlikte hem toplumların hem bireylerin yegane endişesi çağı yakalamak üzerinedir. Yakın geçmişe kadar çağa uyum sağlamak olarak adlandırılan bu durum, günümüzde uyum sağlamaktan çıkmış ve bir zorunluluk haline gelmiştir. Aracıları ortadan kaldırarak maliyetsiz ve daha hızlı işlem yapmayı vaat eden blok zincir teknolojisi de bu süreçte adından söz ettirir hale gelmiştir.

Yine içinde bulunduğumuz çağda tüm teknolojik gelişmeler içerisinde verinin de önemli değer taşıdığı anlaşılmıştır. Veri Koruma Hukuku da tam bu noktada birey ve haklarının güçlüye karşı korunmasını temin etmek amacıyla pek çok ülkede güçlendirilerek karşımıza çıkmaktadır. Gerek Türk Hukuku ve gerekse AB Hukukunda konuya verilen önem ve istenilen bilinç düzeyine paralel olarak bireyin koruma kalkanları da -söz gelimi unutulma hakkı gibi- her geçen gün artmaktadır.

Çalışmamızın temeli ise gelecek vaat eden blok zincir teknolojisinde veri koruma hukuku prensiplerinin uygulanabilirliğine dayanmaktadır. Terazinin bir ucunda kaçırılmaması gereken bir tren ve diğer ucunda birey olmakla kazandığımız hakların irademiz çerçevesinde kullanılabilmesi ve sınırların aşılmamasına yönelik veri koruma hukuku bulunmaktadır.

Nihai olarak bireyin mağdur edilmeksizin haklarının korunması, ancak bu süreçte gelişen bir teknolojinin durdurulmaması ve ilerlemesi yönünde çaba sarf edilmesi ve her ikisinden de vazgeçilmeksizin aralarında uyumun yakalanabilmesine yönelik öneriler geliştirilmiştir.

Anahtar kelimeler: Blok zincir, veri koruma hukuku, kişisel veri, kişisel verilerin korunması, unutulma hakkı.

ABSTRACT

With the developing technology, the only concern of both societies and individuals is to catch up with the age. This situation, which was called adaptation to the age until recently, has ceased to adapt and has become a necessity. Block chain technology, which promises to make transactions faster and cost-free by eliminating the intermediaries, has become prominent in this process.

Again, it is understood that the data carries important value in all technological developments in our age. At this point, Data Protection Law is strengthened in many countries in order to ensure the protection of individuals and their rights against the strong. In both Turkish Law and EU Law, the protection shields of the individual, such as the right to be forgotten, are increasing day by day in parallel with the importance given to the subject and the desired level of awareness.

The basis of our study is based on the applicability of data protection law principles in promising block chain technology. There is a train that should not be missed at one end of the scale and data protection law in order to ensure that the rights we have gained by being an individual at the other end can be exercised within the framework of our will and not to exceed the limits.

Finally, suggestions were developed to protect the rights of the individual without being victimized, but to make efforts not to stop and advance a developing technology in this process and to achieve harmony between them without giving up both.

Keywords: Blockchain, data privacy law, personal data, data privacy, the right to be forgotten.

İÇİNDEKİLER

BİRİNCİ BÖLÜM: BLOK ZİNCİR

İKİNCİ BÖLÜM: VERİ KORUMA HUKUKU AÇISINDAN BLOK ZİNCİR

ÜÇÜNCÜ BÖLÜM: ÇÖZÜM ÖNERİLERİ

TABLO LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

TÜRK VE AB HUKUKU BAĞLAMINDA BLOK ZİNCİR TEKNOLOJİSİNDE UNUTULMA HAKKI

Teknolojik ilerleme, patolojik bir suçlunun elindeki balta gibidir.
Albert Einstein

GİRİŞ

İçinde bulunduğumuz çağ için her geçen yıl yeni bir isim önerisi geliştirilmektedir. 'Uzay Çağı', 'Bilişim Çağı', 'Büyük Veri Çağı' adları ise bunlardan sadece birkaç tanesi olarak karşımıza çıkmaktadır. Verilen adların temelinde her geçen gün gelişen bilgi ve iletişim teknolojileri bulunmaktadır. 'Her geçen gün' ifadesini açmak gerekirse; bundan 10 yıl öncesinde günlük aktivitelerimizin takip edilerek gün sonunda yeterli yürüyüş/egzersiz yapmadığımıza dair geri bildirim verileceği söylendiğinde bunu kimin takip edeceği hakkında kafamızda soru işaretleri oluşmakta iken; bulunduğumuz dönemde bu işi yanımızda taşıdığımız telefonlar hatta sadece saatlerimiz bile gerçekleştirmeye başlamıştır. Aynı şekilde basit bir diş fırçası olarak hayatımıza giren aletler, kendilerini geliştirerek mobil uygulamalar aracılığıyla hangi dişimizin hangi noktasını fırçalamadığımıza dair raporlama yapmaya dahi başladılar. Yine birkaç yıl öncesine kadar eve gelmeden 1 saat önce evin sıcaklığını istediğimiz dereceye getirmek üzere çalışmaya başlayan klima/ısıtma sistemlerinin olacağı söylendiğinde çok uzak bir zaman diliminden bahsedildiği düşünülse de; bu sistemler günümüzde uygulanabilir sistemler haline gelmeye başladılar.

Blok zincir teknolojisi ise son yıllarda özellikle 'Bitcoin' aracılığıyla haberdar olduğumuz yeni bir teknolojidir. Teknolojinin temelinde yatan prensiplerin 'kriptografiye dayalı, anti-merkeziyetçi ve eşten eşe doğrudan veri paylaşımı' olduğu

söylenebilecektir. Blok zincir (blockchain), Satoshi Nakamoto'nun 2008 yılında yayınladığı 'Bitcoin' adlı makalesinde -bitcoine dair ilk yazılı bildiri niteliğindedir- kelime olarak geçmemiş olsa da, kripto paranın altında yatan bir teknoloji bileşeni, kriptografik olarak birbirine zincirlenmiş bir dizi veri bloğu olarak tanımlanmaktadır[1]. Bu anlamda bitcoin,[2] blok zincir teknolojisinin ilk uygulaması ve yaygınlaşmasının en büyük adımlarından birisidir.[3]

Bitcoin ile gündeme gelen ve temelini blok zinciri teknolojisinin oluşturduğu 'dijital finans dünyası', 21. yüzyılın kaçınılmaz evrimi olarak adlandırılabilecektir. Öyle ki geçtiğimiz yıl Bitcoin reklamlarını yasaklayan Facebook, bu yıl 27 farklı şirket ile konsorsiyum kurarak kendi kripto parası Libra'yı çıkaracağını açıklamıştır. Libra'nın kuruluş bildirisine göre dünya çapında finansal sisteme dahil olmamış 1.7 milyar insan olduğu ve bu insanların da 1 milyarının cep telefonu kullanıcısı oldukları, yarım milyar insanın ise internet bağlantılı cep telefonu kullandığı belirtilmektedir. Burada belirtilen yarım milyarlık kitlenin Libra'nın potansiyel hedef kitlesi olacağı anlaşılmakla beraber, yine aynı bildiride geleneksel finansal sistemde zorlukla kazanılan paranın havale-ATM masrafları gibi nedenler ile ciddi biçimde azaldığı, kredi kullanımında ise %30'lara ulaşan yüksek faiz bedellerinin ödenmek zorunda kalındığından bahsedilmiştir.[4] Facebook'un kurucularından Chris Hughes'un ise bu konudaki öngörüsü Libra'nın orta seviyede bir başarı yakalaması halinde dahi paranın kontrolünün büyük bir kısmının merkez bankalarından Vodafone, Uber, Visa gibi şirketlere geçeceği yönündedir.[5]

Blok zincir teknolojisi, finans dünyasının dışında da pek çok sektörde projelere konu edilmektedir;

---

[1] Satoshi Nakamoto, **'Bitcoin: A Peer-To-Peer Electronic Cash System'**, 2008, www.bitcoin.org

[2] Blok zincir teknolojisinin en bilinen uygulaması Bitcoine (BTC) ilişkin olarak 2008 yılında ilan edilen bildirinin (whitepaper) ardından, 2009 yılında ilk Bitcoin bloğu oluşturulmuştur. Bu dönemde borsada Bitcoin'e biçilen değer 1$=1.309 BTC iken, 2010 yılında Bitcoin ile ilk alışveriş yapılmış ve market değeri 1 Milyon $'ı geçmiştir. 2011 yılında bir BTC'nin değeri ilk defa 1$'a denk hale gelmiş ve aynı yılın ortasında 31$ olmuştur. Yine aynı sene içinde ani bir değer düşüklüğü ile 10$'a düşmüş ise de bu durum, 2013 yılında market değerinin 1 Milyar $'a ulaşmasını engellememiştir. 2014 yılında başlayan saldırı durumları ise günümüzde de devam etmektedir. 2014 yılında MT. Gox, 744.000 Bitcoin'in çalındığını bildirerek iflastan korunma başvurusunda bulunmuştur. 2015 yılında ise Bitcoin'in regülasyona tabi ilk borsası Coinbase kurulmuştur. 2016 yılında hükümetler nezdinde ilk adım Japonya'dan gelmiş ve Japonya Bankalar Kurulu, Bitcoin gibi dijital paraların gerçek paraya benzer bir fonksiyonu olduğunu kabul etmiştir. Bir sonraki yıl ise Bitcoin Japonya'da resmi ödeme yöntemi olarak kabul edilmiştir, bu haberin ardından Bitcoin piyasa değeri önce 10.000$'ı aşmış, ardından şu ana dek görülen en yüksek değeri olan 20.089$'a ulaşmıştır. 2018 yılında ise Google ve Facebook Bitcoin reklamlarını yasaklamıştır. 2019 yılı itibarıyla ise Bitcoin'in güncel değeri 9.000$ civarında seyretmektedir.

[3] Hüseyin Avunduk ve Hakan Aşan, Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme, **Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi**, 2018, s.371.

[4] https://libra.org/en-US/white-paper/#introduction Erişim tarihi: 20.07.2019

[5] https://www.ft.com/content/aa97ad20-91a0-11e9-8ff4-699df1c62544 Erişim tarihi: 23.07.2019

-Teknoloji devi Apple'ın kurucularından Steve Wozniak'ın Malta'da geliştirdiği bir blok zincir projesi ile enerjinin tüketiminin daha verimli ve şeffaf hale getirilmesi, para tasarrufunun sağlanması ve çevreye yönelik faydalı işlerin yapılmasının amaçlandığı[6],

-McDonalds, Nestle gibi markaların dijital reklam alımlarının verimliliğini ve şeffaflığını artırmaya yönelik blok zincir projesinin pilot programına dahil oldukları, belirtilen projenin bir sonraki hedefinin tedarik zincirinin optimize edilmesi ve tüm katılımcılar için operasyonel verimliliğin kazanılması olduğu,[7]

-Samsung ve diğer 6 büyük Güney Kore'li şirketten oluşan konsorsiyumun blok zincir tabanlı bir mobil kimlik doğrulama projesi üzerinde çalıştığı, bu projenin özerk kimlik odaklı olduğu ve kullanılan blok zincir teknolojisi sayesinde belge talep edilmeksizin kişiye kimlik belgesinin kısa sürede iletilebileceği,[8] Microsoft'un da benzer şekilde kimlik tanımlama blok zinciri üzerinde çalıştığı, ION adlı bu projenin küresel bir kimlik ekosistemi olmasının hedeflendiği[9] takip edilmiştir.

Globaldeki bu gelişmelerin yanı sıra Türkiye'de de blok zincir çalışmaları kamudan özel sektöre uzanan geniş bir yelpazede ilerlemektedir. Öyle ki;

-Ticaret Bakanlığı tarafından ithalat ve ihracat işlemlerinin hızlandırılması adına blok zincir tabanlı yeni bir sistem üzerinde çalışıldığı, bu proje ile test ve kabul işlemleri gibi ürünlerin gümrükte bekletilmesine neden olan süreçte bürokratik engellerin kaldırılmasının hedeflendiği,[10]

[6] https://www.independent.com.mt/articles/2019-07-18/local-news/Delta-summit-launch-Apple-Co-Founder-Woz-launches-blockchain-company-in-Malta-6736211092 Erişim tarihi: 22.07.2019

[7] https://bitnewstoday.com/news/mcdonald-s-nestl-and-virgin-media-join-blockchain-based-project-for-digital-ads/ Erişim tarihi: 19.07.2019

[8] https://www.forbes.com/sites/darrynpollock/2019/07/16/samsung-and-south-korean-enterprises-enter-the-blockchain-id-race/#50957e5322b5 Erişim tarihi: 22.07.2019

[9] https://www.ledgerinsights.com/microsoft-azure-blockchain-based-digital-identity-ion/ Erişim tarihi: 22.07.2019

[10] https://www.ticaret.gov.tr/haberler/ihracat-blokzincir-teknolojisiyle-hizlanacak Erişim tarihi: 01.07.2019

-Tübitak bünyesinde blok zincir ve dijital para araştırmalarının yapılması amacıyla Blokzincir Araştırma Laboratuvarı kurularak finansal hareketlerden tedarik zincirine[11] ve başkaca blok zincir projelerinin hayata geçirilmesinin hedeflendiği,

-Akbank tarafından blok zincir teknolojisi ile uluslararası para transferinde Ripple ile anlaşma sağlanarak, daha hızlı ve şeffaf para transferinin maliyetinin düşürülmesinin amaçlandığı,[12]

-Borsa İstanbul tarafından hayata geçirilen proje ile Borsa İstanbul, Takas İstanbul ve Merkezi Kayıt İstanbul'un müşteri veri tabanındaki bilgilerin senkronize hale getirilmesinin sağlandığı[13] takip edilmiştir.

Ancak hızlı ve maliyetsiz veri paylaşımını sağlayan bu teknoloji, veri tabanında kayıtlı tüm verilerin oluştukları ilk andan itibaren takip edilebilmelerini sağlamakta ve silinebilmelerini de önlemektedir. İşlemlerde şeffaflığın sağlanması bu teknolojinin en değerli özelliklerinden biri gibi görünüyor olsa da; kişisel verilerin korunması hukuku bağlamında sahip olunan haklar düşünüldüğünde burada sağlanan şeffaflığın veri koruma hukuku ile çelişki yaşatıp yaşatmama ihtimali gündeme gelmektedir.

Türkiye'de ve Avrupa Birliği'nde 1981 yılında Avrupa Konseyi 108 no'lu Sözleşme olan 'Kişisel Verilerin Elektronik İşlenmesi Sırasında, Bireylerin Korunması Sözleşmesi" ile gündeme gelen kişisel verilerin korunması, Türkiye'de Kişisel Verilerin Korunması Kanunu (metnin devamında KVKK/Kanun olarak anılacaktır) ve AB'de Genel Veri Koruma Tüzüğü (metnin devamında GDPR/Tüzük olarak anılacaktır) düzenlemeleri ile nihai halini almıştır. Bu yasal düzenlemeler ile kişisel verinin tanımı ve veri sahibinin kim olduğundan, veri sahibinin haklarına uzanan detaylı açıklamalar tezimizin içeriğinde yer almaktadır. Bunun yanı sıra, veri sahibinin haklarından biri olan 'unutulma hakkı' ve bu hakkın blok zincir teknolojisinde kullanımı ise esas sorunsal olarak belirlenmiştir.

---

[11] https://webrazzi.com/2017/11/21/tubitak-bilgem-blok-zinciri/ Erişim tarihi: 22.07.2019

[12] https://www.akbanklab.com/tr/guncel/basinda-biz/blockchain-teknolojisi-Turkiyede-ilk-kez-akbankta Erişim tarihi: 22.07.2019

[13] https://www.borsaistanbul.com/duyurular/2018/09/05/turkiye-nin-ilk-finansal-blockchain-projesi-borsa-istanbul-bilisim-teknolojileri-ekibi-tarafindan-hayata-gecirildi Erişim tarihi: 22.07.2019

Öyle ki; kişisel verilerin korunması hukuku ‘mümkün olan en az verinin, mümkün olan en kısa süre boyunca saklanmasını’ temel prensip edinmiş iken; bahsettiğimiz hızlı ve maliyetsiz transfer teknolojisi, zincire dahil edilen bir işlemi ancak tüm zinciri bozma pahasına silebileceğini iddia etmektedir.

Bir başka deyişle, hiçbir aracıya ihtiyaç duymadan bireyler arasında her türlü alışverişi sağlayan güncel bir teknoloji olan blok zincir teknolojisi hayatımızı kolaylaştırmak üzere gelmekte; ancak niteliği itibarıyla ‘bloklarda yer alan silinemez veriler’ de veri koruma hukukunun veri sahiplerine bahşettiği ‘unutulma hakkı’nın kullanımını engellemektedir.

Bu noktada kendimize şu soruyu sormalıyız; teknolojik gelişime uyum sağlayamayan toplumların varlıklarının dahi tehdit altında olduğu tartışılan bir çağda tercihimiz ne olmalı? Teknolojiden feragat etmeyi reddedip unutulmadığı için sonsuza dek affedilmeyen bir gelecek mi istiyoruz? Bunu yaparken teknoloji için kişisel hak çerçevesinde yer alan unutulma hakkını gözden çıkarabilecek miyiz? Veya çözümsüzlüğü reddederek blok zincirde unutulma hakkının da kullanımını sağlamak mümkün mü?

Aşağıda yer alan tez çalışmasında bu soruların cevapları aranacak ve blok zincir teknolojisinde unutulma hakkının kullanımı sorunsalı detaylı olarak izah edilecektir.

BİRİNCİ BÖLÜM
BLOK ZİNCİR

I-BLOK ZİNCİR NEDİR?

A. Genel Olarak

İnternetten sonraki en büyük dijital ağ teknolojisi olarak tanımlanan blok zincir, şimdiden küresel etkilerini her sektörde göstermeye başlayan bir teknoloji olmakla beraber; henüz tüm dünyanın bu teknoloji konusunda yolun çok başında olduğu söylenebilecektir.

Blok zincir teknolojisinin büyük kitlelere ulaşması 2008 yılında Satoshi Nakamoto tarafından yayınlanan Bitcoin tanıtım rehberi ile gerçekleşmiştir.[14] Kripto paranın temelini oluşturan bu teknolojinin varlığından makalede bahsedilmiş ise de kelime olarak blok zincir ifadesinin kullanılmadığı görülmektedir. Blok zincir teknolojisi, kriptografik olarak birbirine zincirlenmiş bir dizi veri bloğu olarak ilk kez bu makalede anlatım bulmuştur.[15] Aynı makalede Bitcoin'in çalışma prensibinin şifreleme kanıtı üzerine kurulu olduğu ve doğrudan tarafların birbirine bağlı olduğu elektronik bir ödeme sistemi şeklinde çalıştığı da belirtilmektedir. Bunun yanı sıra, bu çalışmada aracılık faaliyeti gösteren bankaların da eleştirildiği ve elektronik ticaretin ivme kazanmasıyla ticaretin gerçekleşmesi için bankalara ihtiyaç olmadığı vurgusunun yapıldığı da görülmektedir.[16] Bahsedilen çalışma ile açık bir protokol olarak sunulan Bitcoin, zaman içerisinde herkese protokolün alınabilmesi, kodlanabilmesi ve kodunun

[14] Satoshi Nakamoto, **'Bitcoin: A Peer-To-Peer Electronic Cash System'**, 2008, www.bitcoin.org
[15] Avunduk ve Aşan, s.371.
[16] Şerif Dilek, Blockchain Teknolojisi ve Bitcoin, **SETA Analiz Dergisi,** Sayı:231, Şubat 2018, s.8.

değiştirilebilmesine olanak sağladığını ve herkesin kendi P2P (peer-to-peer)[17] para birimlerini başlatabilmesine imkan sağladığını da göstermiştir.

Blok zincirin -özellikle finans dünyasında- aktif olmaya başladığı dönem ise 2008 küresel krizi sonrasına denk gelmektedir. Bu dönemde yaşanan küresel kriz yatırımcıların bankacılık sistemine, finansal kurumlara ve aracılara olan güvenlerini yıkmıştır. Küresel sistemde yaşanan krizin sadece yatırımcıların değil tüm toplumun güven duygusunu sarsması sonucunda da yeni arayışlar ve paranın temeline dair sorgulamalar başlamıştır.[18] Bu dönemde 2008 yılının Eylül ayında Lehman Brothers'ın -ABD hükümeti tarafından 'Too big to fail'[19] olarak adlandırılan bankalardan biri olan yatırım bankasının- iflasından iki ay sonra Satoshi Nakamoto tarafından bir makale yayınlanmıştır. 'Bitcoin: Eşten Eşe Elektronik Nakit Ödeme Sistemi' adındaki bu makalede dağıtık bir veri kayıt sistemi ile çalışan, kullanıcılarının ve üçüncü kişilerin manipülasyon teşebbüslerine karşı koruma sistemlerini içinde barındıran ve dijital bir para birimi olarak Bitcoinden bahsedilmiştir. Bu makalede, Bitcoin iki tarafın birbiri ile doğrudan bağlantılı olduğu ve şifreleme kanıtı üzerine kurulu bir elektronik ödeme sistemi olarak anlatılmaktadır[20]. Blok zincir ise Bitcoin adlı dijital para biriminin temelini sağlayan teknoloji sıfatıyla yazımızın devamında detaylı olarak anlatım bulacaktır.

Blok zincir teknolojisi, büyük topluluk ve organizasyonlara merkezi bir otorite olmaksızın anlaşma yapmalarına izin veren ve aralıksız şekilde veri kaydeden bir teknolojidir. 1990'lı yılların başında bilgi devrimi yaratan WWW (World Wide Web) ve devamındaki 10 yıl içinde hızlı bir olgunlaşma gösteren internet daha da programlanabilir hale gelmiştir. Akabinde sosyal medya ve e-ticaret ile tanışmamızı sağlayan Web2 devrimi karşımıza çıkmıştır. Web2; toplumsal etkileşimlerde devrim yaratarak; bilgi, mal ve hizmetlerin arasındaki zaman ve aracıları azaltarak üreticilerin ve tüketicilerin birbirine daha da yakınlaşmasını sağlamıştır. Bu sayede, küresel ölçekte P2P etkileşimleri de artmıştır. Ancak bu işlemler esnasında arada hep güvenilir bir

[17] P2P yani peer-to-peer kavramı peer kelimesinin karşılığı olan 'eş, denk' ile izah edilmiş ve 'eşler arası' olarak kullanılmaktadır. İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür. Protokolde yer alan eşler, eşit derecede ayrıcalıklı ve eş katılımcılardır.

[18] Dilek, s.10.

[19] Literatüre 'Batmasına izin verilmeyecek kadar büyük' olarak çevrilen bu tabir, iflası halinde ekonomiyi çok derin etkileyecek büyüklükte ve etkide olan kurumlar için kullanılmaktadır. Diğer örnekleri için bkz. https://www.thebalance.com/too-big-to-fail-3305617 Erişim tarihi: 29.01.2019

[20] Dilek, s.10.

aracının olması gerekmiştir. Bir başka deyişle, birbirlerini tanımayan ve aralarında güven ilişkisi de bulunmayan A ve B kişilerinin arasında güvenilir bir aracı olarak hareket eden platformlar yer almaktadır. Bu platformlar P2P ekonomisi yaratma konusunda başarılı teşebbüsler sayılsalar da, işlemlerin tüm kurallarının bu platformlar tarafından dikte edildiği ve bu platformların tüm verilerimize sahip oldukları düşünüldüğünde yeni bir alana daha ihtiyaç olduğu anlaşılmaktadır. Bu bağlamda blok zincir, yeni nesil İnternet'in, Merkezi Olmayan Web'in veya Web3'ün itici gücü gibi görünmektedir. Blok zincir bir aracı olmadan bize gerçek P2P işlemlerini sağlayabilmekte ve Bitcoin bu teknolojinin ilk kullanım hali olarak karşımıza çıkmaktadır. Bitcoin bankalar ve banka yöneticileri olmadan P2P parası iken, bize Bitcoin'i getiren aynı teknoloji artık Uber'siz yolculuk paylaşımı, Airbnb'siz ev paylaşımı ve Facebook ve Twitter'sız sosyal medya kullanımına izin vermiştir.[21] Bu anlamda blok zincir/güven ekonomisi trendi, büyük ve merkeziyetçi güven mekanizmalarından bireye doğru önemli bir güç değişimi göstermektedir.[22] Son 10 yılın en önemli buluşlarından biri kabul edilen bu teknoloji; adil, kapsamlı, güvenli ve demokratik bir dijital ekonomi oluşturmak için önemli bir araç olarak görülmeye başlanmıştır.

B. Kavramlar

Çalışmamızın birinci ana bölümünü oluşturan blok zincir teknolojisinin anlaşılabilmesi adına zinciri oluşturan her bir ögenin tanım ve anlatımlarının yapılmasında fayda olacağı düşünülmektedir. Bu kapsamda sırasıyla blok zincirin ne olduğu, içerisinde yer alan verilerin hangi şifreleme yöntemleri ile bu sistemde saklanabildiği, sistemin temel prensibi olan dağıtık veri tabanı kavramı, uçtan uca veri paylaşımı ve sisteme hakim olan ilkeler -şeffaflık, kayıtların silinemezliği gibi- izah edilecektir.

Blok zincir adını, verilerin gruplar halinde saklandığı ‘blok’lardan almaktadır.[23] Kullanıcılar tarafından onaylanan her bir blok, kendisinden bir önce gelen

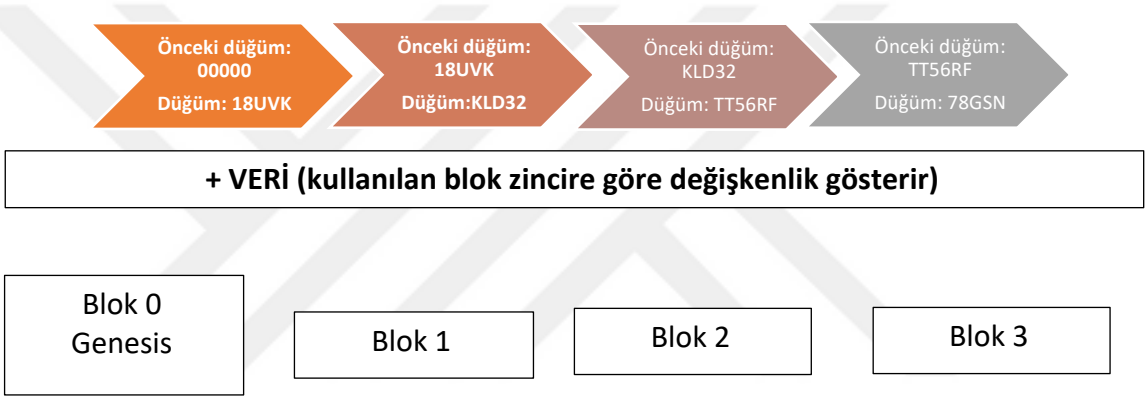
[21] https://blockchainhub.net/web3-decentralized-web/ Erişim tarihi: 08.03.2018

[22] Eric Piscini ve Diğerleri, ‘Blockchain: Trust Economy’**, Tech Trends 2017**, Deloitte University Press, s.94.

[23] Bloklar, blok zincirlerinde işlemleri gruplandırmak için kullanılan veri yapısıdır. İşlemlere ek olarak, bloklar bir önceki bloğun hash ve zaman damgası gibi diğer unsurları da içerir. Esasında blokzincir teknolojisinin temelinin de 1991 yılında geliştirilen dijital zaman damgası tekniğine dayandığını söylemek yanlış olmayacaktır. Dijital zaman damgasının temel işlevi; elektronik ortamda transferi yapılan tüm verilerin şifrelenerek güvenliğinin sağlanması ve

bloğa şifrelenerek kilitlenir[24] ve böylece sürekli büyüyen bir veri zinciri oluşturulur. Ağdaki tüm devreler, merkezi bir yerde tutulmak yerine blok zincirin aynı kopyalarını paylaşır ve doğrulanan yeni bloklar eklendikçe bu durum güncellenmeye devam etmektedir. Bir başka ifadeyle, her blok bir önceki değere içinde bulunduğu değer ile bağlanır. Bir önceki blok onun üst bloğu olarak adlandırılır ve sistem bu şekilde devam ederek sonsuza kadar uzanır. Bu sayede tüm kullanıcılar arasında zincirin kopyaları paylaşılmış halde zincir oluşturulmaya devam eder.

Yukarıda bahsi geçen zincirdeki ilk blok 'Genesis' adını alır ve devamındaki işleyiş Şekil-1'deki gibi ilerler;



Şekil-1

Şekilden de anlaşılacağı üzere; ilk blok (Genesis blok) haricindeki tüm bloklar, bir önceki bloğu işaret etmektedir. Her bir blok, bir önceki bloğa ait hashi, üzerinde taşınması istenen veriyi ve bir sonraki bloğa ait hashi barındırmaktadır. Burada kullanılan 'Hash' adı verilen şifreler ve 'üzerinde taşınması istenen veri' kavramlarını açıklamak gerekirse;

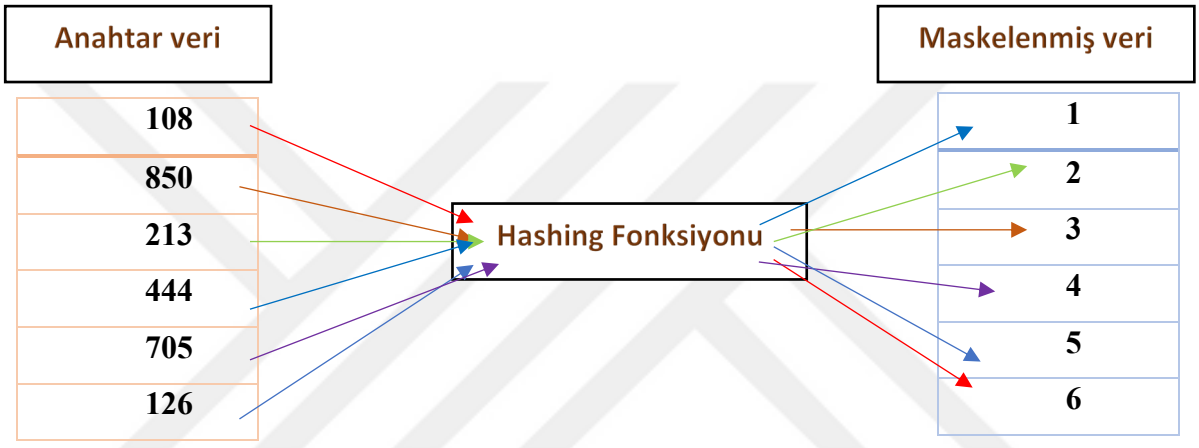
Hash'ler; bir fonksiyon sonucu olarak ortaya çıkan geri döndürülemeyen, benzersiz ve sabit uzunluktaki veri şifreleridir. Bir diğer deyişle, her türlü veriye ait parmak izinin dijital düzlemdeki karşılığıdır. Bir değerin diğerine dönüştürülmesini

değiştirilememesidir. Bu sayede transfer edilmek istenen veri, hem içeriği değişmeden hem de üçüncü kişiler tarafından erişilemeden iletilmesi gereken yere iletilebilmektedir.

[24] Bir mesajın veya işlemin imzalanması, bir çift asimetrik anahtar kullanılarak verilerin şifrelenmesinden oluşur. Asimetrik kriptografi, bir kullanıcının şifrelemek için bir anahtarın, diğerini deşifre etmek için başka bir anahtarın yerine kullanmasını sağlar.

sağlayan bu fonksiyon, yaygın olarak bilgisayarların veri ile ilgili faaliyetlerinde kullanılmaktadır. Bilgisayarların veri ile ilgili faaliyetleri arasında kriptografi, sıkıştırma, sağlama toplamı oluşturma veya veri indeksi hazırlama da sayılabilecektir.[25]

Hashing fonksiyonu orijinal verileri başka değerler ile maskelemektedir. Bu nedenle çalışma prensibi itibarıyla bir veri tablosu -genellikle bir veri tabanı veya veri dizisi olabilmektedir- ve dönüştürme algoritması ile çalışır ve sonuç olarak kendi hazırladığı şifrelenmiş veri tablosunu ortaya çıkarmaktadır. Basit bir anlatımla şematize edildiğinde; (Şekil 2)



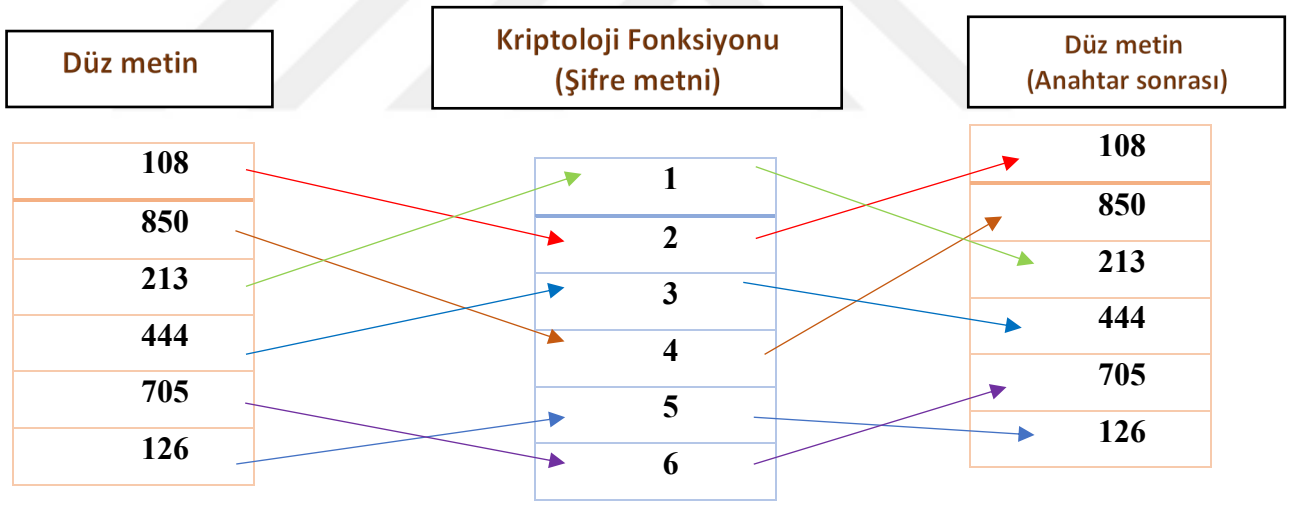
Şekil-2[26]

İlk sütunda yer alan anahtar veri, şifrelenmek istenen orijinal veridir. Tanımlanacak bir algoritma ile anahtar verinin dönüştürülmek istendiği veri kodlanacaktır. Şifreleme fonksiyonunun çalışmasıyla sağda yer verilen maskelenmiş veri dizini oluşacaktır. Bir şifreleme fonksiyonu, yalnızca bir anahtar veri tablosundan değer aranarak kodu çözülebilen bir değer üretmek için kullanılabilecektir. Bunun yanı sıra iyi bir şifreleme neticesinde oluşan maskelenmiş veri, tersine dönüştürülemeyecektir. Buradaki fonksiyon, iletimin güvenliğini saldırılara karşı korumaya yardımcı olan şifrelemeyi oluşturacaktır.[27]

Kriptoloji ise; en basit tanımıyla 'şifreleme bilimi'dir. Üçüncü kişilerin mevcut olduğu bir ortamda güvenli iletişimin sağlanması amacıyla çeşitli iletilerin, yazıların belli bir kural dahilinde şifrelenerek rastgele görünen bir veri kümesine dönüşmesini

[25] https://techterms.com/definition/hash Erişim tarihi: 01.07.2019
[26] https://www.geeksforgeeks.org/file-organization-in-dbms-set-4/ Erişim tarihi:01.07.2019
[27] https://blockgeeks.com/guides/what-is-hashing/ Erişim tarihi: 01.07.2019

amaçlamaktadır.[28] Ancak belirtilmelidir ki, rastgele gibi görünen bu veri kümesinin arka planında verinin esas hali ile kriptolanan veri arasında bir anahtar/algoritma mevcuttur. Bu anahtara/algoritmaya ulaşılamadığı sürece kriptolanan verinin orijinal haline ulaşılması mümkün olmamaktadır. Şu haliyle şifrelenen veri, depolandığı yerden bağımsız olarak sadece anahtar/algoritma sahibi için önem taşımaktadır.[29] Kriptografi ile şifrelenen metin veya şifreler, sadece anahtara sahip olan kişi tarafından çözülebileceğinden, bu yöntem özellikle hassas verilerin siber suçlara karşı korunmasında kullanılan bir yöntemdir. Bunun yanı sıra alıcının da şifreli bir mesajı okuyabilmesi için şifre çözme işleminde kullanılan bir şifresinin veya güvenlik anahtarının olması gerekmektedir. Bu sayede modern iletişim sistemlerinde de veri güvenliğini sağlamanın en etkili yolu olarak kabul edilen bu teknik, blok zincir teknolojisinin de temelini oluşturmaktadır. Kriptolojide şifrelenmemiş veriler düz metin olarak bilinirken, verileri şifrelemek şifre metni olarak ifade edilmektedir. Nihayetinde blok zincir, kriptografi kullanılarak birbirine bağlanan ve büyüyen kayıt listesidir.[30] Kriptolojinin yukarıda tarif edilen çift yönlü fonksiyonu şematize edilirse; (Şekil 3)



Şekil-3

Şifrelenmek üzere alınan veriler düz metin sütununda yer alırken, tanımlanan algoritma ile bu veriler şifrelenmiş veri haline getirilmektedir. Akabinde, şifrelenmiş haldeki verilerin tekrar orijinal hallerine getirilmesi için tekrar bir algoritmaya ihtiyaç duyulacaktır. İşte bu noktada verilerin 2. kez dönüştürülmesini sağlayan anahtar veya

[28] Raghu M E ve Ravishankar K C, 'Application of Classical Encryption Techniques for Securing Data-A Threaded Approach', **International Journal on Cybernetics & Informatics (IJCI),** Cilt 4, Sayı 2 (Nisan 2015), s.125.
[29] Ahmet Usta ve Serkan Doğantekin, Blockchain 101, **MediaCat,** 2017, s.42.
[30] https://www.blockchaintechnologies.com/blockchain-technology/ Erişim tarihi:01.07.2019

algoritmanın varlığı ile mevcut şifreleme işlemi hashingden kriptolojiye dönüşmüş olacaktır.

Hashing ile kriptoloji tanımları anlam ve işlev olarak aynı gibi görünseler de aralarında nüans farklılıkları bulunmaktadır. Her ikisi de bilgi işlem sistemlerinde veri, mesaj ve bilgilerin işlenmesi için idealdir. İkisinde de veriler farklı bir formata dönüştürülebilmekte veya değiştirilebilmektedir. Ancak, hashing işlemiyle dönüştürülen bir veri orijinaline döndürülemez iken, kriptoloji ile dönüştürülen bir metin nihayetinde esas anlamlı haline geri getirilebilmektedir. Bu anlamda hashing fonksiyonu tek yönlü iken kriptoloji çift yönlü bir fonksiyon olarak değerlendirilmektedir.[31]

'Üzerinde taşınması istenen veri' ise blok zincirdeki veri kavramına eşdeğerdir. Blok zincir teknolojisinde veri tanımına ise çalışmanın devamında detaylı olarak değinilecektir. Ancak öncesinde veri tanımının kapsamının, blok zincirin kullanım amacına göre değişkenlik gösterdiği söylenebilecektir. Söz gelimi bitcoin transferinde kullanılan bir blok zincirin taşıdığı veriler 'kimden, kime, gönderilecek bitcoin miktarı' iken; blok zincirin faaliyet alanı nüfus kayıtları olduğunda burada taşınan veri bireylerin adı, soyadı, kimlik numaraları gibi oldukça yoğun kişisel veri içerebilecektir.

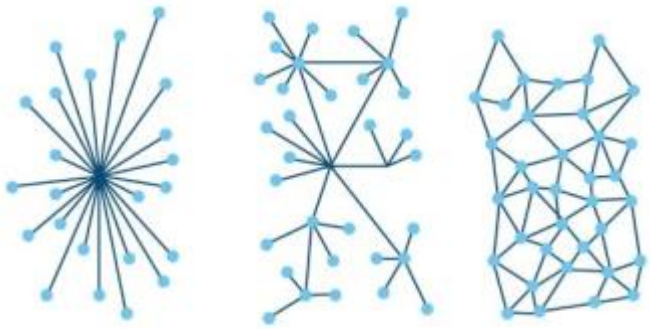
Blok zincir teknolojisinin en temel fonksiyonu olan dağıtık veri tabanı kavramına değinmeden önce veri tabanı tanımı ve akabinde genel olarak veri tabanı çeşitleri irdelenecektir. Veri tabanı, bilgi ya da verilerin -çoğunlukla bir bilgisayar sisteminde- elektronik olarak depolanmış, organize edilmiş, düzenlenmiş yapıdaki halleridir.[32] Veri tabanları, verilerin depolanma sistemlerine göre merkezi, merkezi olmayan ve dağıtık türde olmak üzere 3 farklı şekilde görülebilir.

Merkezi bir veri tabanı, tek bir konumda bulunan, depolanan ve tutulan bir veri tabanıdır (Şekil 4'te yer alan ilk görsel merkezi bir veri tabanını örneklemektedir). Bu konum genellikle merkezi bir bilgisayar veya veri tabanı sistemidir (örneğin bir masaüstü veya sunucu CPU veya bir ana bilgisayar) ve çoğu durumda, merkezi bir kuruluş veya kurum tarafından kullanılmaktadır.[33]

[31] https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption Erişim tarihi: 01.07.2019
[32] https://www.oracle.com/database/what-is-database.html Erişim tarihi: 01.07.2019
[33] https://www.tutorialspoint.com/Centralized-Database-Management-System Erişim tarihi: 07.06.2019

Merkezi olmayan bir veri tabanı, coğrafi olarak farklı konumlarda bulunan ancak bir veri iletişim ağı üzerinden 'bağlantısı olmayan' sistemlere kurulu bir veri tabanıdır (Şekil 4'te yer alan ikinci görsel merkezi olmayan bir veri tabanını örneklemektedir). Bu, aralarında mantıksal bağlantı olmayan bir grup bağımsız veri tabanı olduğu anlamına gelmektedir.[34]

Dağıtık veri tabanı ise; coğrafi olarak farklı konumlara yerleştirilmiş ve bir veri iletişim ağı üzerinden bağlanmış bir dizi bilgisayara yüklenen tek bir mantıksal veri tabanıdır (Şekil 4'te yer alan üçüncü görsel dağıtık veri tabanını örneklemektedir). Bu sistemde hedef; verilerin, iletişim ağları ile birbirine bağlı olan farklı sunucular üzerinde dağıtılmasıdır. Bu sayede, tüm sistemin tek bir kişi, bilgisayar vs. yerine sisteme dahil olan tüm kullanıcılar tarafından yönetilmesi sağlanmaktadır.



Şekil-4[35]

Blok zincir teknolojisinde veri tabanı, devreler (=blok zincir protokolünün yüklü olduğu her bilgisayar=blok zincir ağı katılımcıları=node) arasında dağınık bir halde bulunmaktadır. Bir blok zincir üzerindeki her kullanıcı tüm veri tabanına ve tüm işlem geçmişine erişebilmektedir. Fakat işlemdeki hiçbir taraf veriyi veya bilgiyi kontrol edememekte/değiştirememektedir. İşlemlerdeki her bir taraf, işlemi gerçekleştiren diğer kullanıcıların kayıtlarını aracıya gereksinim duymaksızın doğrulayabilmektedir.[36] Çok sayıda katılımcının yer aldığı bu sistemde, sistem içerisine eklenmek istenen bir işlemin geçerliliği için sistemin geneli tarafından 'sistem içi belirlenen genel kurallara uygunluk' onayının verilmesi gerekmektedir. Burada yer alan genel kurallara uygunluk ve nihayetinde oluşan fikir birliğine 'mutabakat'

[34]https://subscription.packtpub.com/book/application_development/9781787126992/6/ch06lvl1sec26/distributed-and-decentralized-databases Erişim tarihi: 07.06.2019
[35] https://itelligencegroup.com/tr/local-blog/blockchain/ Erişim tarihi:01.07.2019
[36] M. Iansiti ve K. Lakhani, **The Truth About Blockchain,** Harvard Business Review, Vol. 95, No:1, 2017, s.118-127.

denilmektedir. Bu sistemde, ağdaki devrelerin veri tabanına bilgi eklenmesini önerebildiği ve aynı zamanda ağın üzerinde anlaşmaya varılmış versiyonun hangisi olduğunu onaylayabildiği bir konsensus mekanizması mevcuttur. Sistemin dijital ortamda olması ise mutabakat yapısının yine yazılım tarafından garantilenmesini gerektirmekte ve bu noktada da blok zincir teknolojisi devreye girmektedir.[37]

Blok zincir teknolojisi, çok sayıdaki işlemi[38] merkezileştirmek ve otomatik hale getirmek için kullanılabilecek bir teknolojidir. Bilgi konusunda konsensusun sağlanması ve bunların saklanması için -ortak kullanıcı / rakip ayrımı yapılmaksızın niteliği itibarıyla çok sayıda kişi veya kuruluşa izin verebilmektedir. Bu sebeple, blok zincir bir 'güven makinası' olarak addedilmektedir.[39] Bir başka tanıma göre ise, merkezi olmayan ve güvenilir bir sistemle toplu olarak tutulan bir veri tabanının teknik bir planı olarak ifade edilmektedir.[40]

Netice itibarıyla; veri tabanının tüm ağ katılımcılarının arasında merkezilikten uzak şekilde dağıldığı ve blok zincir teknolojisindeki aracısız iletişimin de bahsi geçen dağıtık veri tabanı yapısıyla sağlandığı görülmektedir. Diğer yandan, zincirin veri depolama işleminde kullanılan şifreleme yöntemlerinin hashing ve kriptoloji fonksiyonları ile sağlandığı, sistemin ilerlemesinde -kullanıcılar arası mutabakatı sağlayan- konsensus mekanizmasının rol oynadığı izah edilmektedir. Çalışmanın devamında blok zincir teknolojisine hakim ilkelere değinilecektir.

C. Temel İlkeler

Çalışmanın bu bölümünde, blok zincir teknolojisini diğer veri tabanı/veri transferi teknolojilerinden ayıran ve öne çıkaran temel ilkelere değinilecektir. Genel itibarıyla, dijital teknolojilerin ortaya çıkma süreçleri zaman alıyor olsa da, teknoloji bulunduktan sonra gelişimi yüksek hızda seyreder ve bir süre sonrasında teknolojinin

[37] Usta ve Doğantekin, s.45.

[38] Blok zincirde işlem, bir blok zincir ağı arasında paylaşılabilecek en ayrıntılı bilgi parçasıdır. Kullanıcılar tarafından üretilir ve transferin değeri, alıcının adresi ve veri yükü gibi bilgiler içerir. Ağa bir işlem göndermeden önce, kullanıcı içeriğini bir şifreleme anahtarı kullanarak imzalar. İmzaların geçerliliğini kontrol ederek, devreler işlemdeki gönderenin kim olduğunu belirleyebilir ve ağ üzerinden iletilirken işlem içeriğinin manipüle edilmediğinden emin olabilir.

[39] Blockchain and the GDPR (Thematic Report), **The EU Blockchain Observatory and Forum,** 2018, s.32.

[40] Feng Xia Tian, An agri-food supply chain traceabiliy system for China based on RFID and blockchain technology, Service Systems and Service Management, **13th International Conference on IEEE**. 2016, s.3.

kullanımı arttıkça teknolojiye ulaşım maliyetleri ters orantılı olarak gelişme gösterirler. Bir başka deyişle gelişen her teknoloji, kendinden öncekinin fiyatında düşüşe sebep olmaktadır.

Bir önceki bölümde detaylı olarak izah edilen ve blok zincir teknolojisinin en önemli prensibi olan dağıtık veri tabanı da; gelişen teknoloji ile birlikte ucuzlayan iletişim ağları sayesinde tüm verilerin kullanıcı bilgisayarları arasında kopyalanmış halde bulunmasını sağlamaktadır.[41] Bu sayede merkezi yapıdan uzakta bir sistem geliştirilebilmekte ve sistem kullanıcıları kendi aralarında sağladıkları mutabakat ile işleyişi devam ettirebilmektedir. Böylece blok zincir, içerisinde kayıtların birbirine hash fonksiyonları ile bağlandığı bir dağıtık veri tabanı olarak birbirine eklenmekte ve kullanıcılar sayesinde bir merkeze bağlı olmaksızın sürekli büyümektedir.[42]

Blok zincir teknolojisinin 'aracısız' iletişim ve transferi sağlamasındaki bir diğer ilke ise uçtan uca veri paylaşımıdır. Uçtan uca -veya eşten eşe- veri paylaşımı (Peer to peer / P2P); 2000'li yıllarda eDonkey ve BitTorrent gibi projeler aracılığıyla online ortamda bilgisayarlar üzerinden veri paylaşımı yapılabilmekteydi. Bu tür makine üzerinde veri depolama sistemleri 'Peer To Peer – P2P' olarak adlandırılmaktadır.

Bu sistemlerin temel mantığı verinin tek bir merkezde bulunmaması ve zaman zaman milyonlara ulaşabilen katılımcı bilgisayarlar üzerinde (verinin tamamını depolayan bilgisayarların yanı sıra verinin bir kısmını depolayan bilgisayarlar da mevcuttur) bulunmasıdır. Ulaşılmak istenen veri girildiğinde sistem bu veriyi taşıyan diğer kullanıcıları işaret etmekte ve yönlendirmektedir. Bu kullanıcılardan istenen veri alınarak depolandığında ise sistem nezdinde artık o veri için yeni bir veri kaynağı -talepte bulunan ve yükleyen kullanıcı- daha tanımlanmaktadır. Ancak bahsedilen sistemlerde verilerin şifrelenememesi ve verinin depolanacağı alanların belirlenememesi -veya belirleme yetkisinin kullanıcıya verilmemesi- gibi dezavantajlar nedeniyle kişisel veri veya kurumsal bilgiler açısından yeterli güvenlik sağlanamamaktadır. [43]

Esasında kullanıcıların iletişim kurması için merkezi bir yapı kullanılması gerekirken blok zincir teknolojisi sayesinde bilgi/veri, her kullanıcının özel düğümleri

[41] Usta ve Doğantekin, s.44.
[42] Dilek Şerif, s.10.
[43] Usta ve Doğantekin, s.37.

tarafından eşler arası bir ağda birbirlerine doğrudan iletilmekte ve depolanmaktadır.[44] Bu sistemde düğümler arasında sağlanan mutabakat nedeniyle merkezi otoriteye ihtiyaç duyulmamaktadır.

Yukarıda anlatım bulan blok zincir sisteminde yer alan dağıtık veri tabanı ile uçtan uca iletişim esasları bir arada değerlendirildiğinde; işlemlerin yapılması esnasında tüm bloklara erişimin gerekip gerekmediği gündeme gelebilmektedir. Bu sistemde, yeni işlemlerin gerçekleşmesi için tüm bloklara erişim gerekmemekle beraber, işlemin bir bloğa dahil edilebilmesi için 'yeterli sayıda' düğüme erişmesinin işlemin gerçekleşmesini sağlayacağı söylenebilecektir. Aksi takdirde, tüm düğümlere erişimin işlemin geçerlilik koşulu olması varsayımında, 'kolaylaştıran' bir teknolojiden bahsedilemeyeceği aşikardır.

Blok zincir sistemine hakim ilkelerden bir diğeri olan şeffaflık ilkesi; blok zincir teknolojisinde her işlem ve ilgili değerin, sisteme erişimi olan herkes tarafından görülebilmesi olarak izah edilebilecektir. Bir blok zincirindeki her düğüm veya kullanıcı, onu tanımlayan benzersiz bir 30 karakter ve üzerinde kodlanan alfanümerik adrese (hash olarak adlandırılır) sahiptir. Bu sayede, kullanıcılar isimsiz kalmayı tercih edebilecekleri gibi dilediklerinde kimliklerini üçüncü kişilere kanıtlayabilmektedir. Yapılan tüm bu işlemler blok zincir adresleri arasında gerçekleşmektedir.[45]

Bu noktada blok zincir teknolojisinde işlem sahiplerinin kimliklerine ilişkin farklı görüşlerden bahsedilebilecektir. Blok zincir sistemini duyuran Nakamoto'ya göre 'blok zincir teknolojisi sahipsizdir'. Bir diğer görüşe göre ise blok zincirin takma isimli işlemler ile gerçekleştirildiği savunulmaktadır. Blok zincir teknolojisinde kullanıcılar bu takma adlar sayesinde anonim kalabilmekte ve gerçek kimliklerini açıklamak zorunda kalmamaktadır.[46] Ancak belirtilmelidir ki, tamamen kimliği belirsiz kişiler tarafından yapılan nakit işlemler yerine, blok zincir teknolojisinde her işlem bir hesapla ilişkilendirilmektedir. Her kullanıcı taraf olduğu işlemlerde benzersiz bir adrese sahiptir ve işlemler bu adresler üzerinden gerçekleşmektedir. Bu sayede kullanıcıların hesaplarının (işlemdeki kimlikleri olarak da ifade edilebilecektir) tespit edilmesi de mümkün kılınmaktadır.

[44] Avunduk ve Aşan, s.374.
[45] Iansiti ve Lakhani, s.118-127.
[46] Avunduk ve Aşan, s.375.

Kayıtların silinemezliği ise blok zincir teknolojisinin temel özelliklerinden - çalışmamız kapsamında- en sonuncu ve esasında unutulma hakkı ile bağlantılı olarak bir diğer ilkedir. Bu ilke gereğince veri tabanına bir işlem girildikten ve hesaplar güncellendikten sonra, kayıtlar değiştirilememektedir. Blok zincirde veri tabanına girilen her işlem kendilerinden önce gelen işlem kaydına bağlıdır. Nitekim 'zincir' benzetmesini de bu özelliği sebebiyle almıştır. Veri tabanındaki kaydın kalıcı, kronolojik olarak sıralı ve ağdaki diğer herkes tarafından erişilebilir olmasını sağlamak için çeşitli hesaplama algoritmaları ve yaklaşımları uygulanmaktadır.

Bölüm itibarıyla blok zincir teknolojisinin ilkelerine ve bu ilkeler çerçevesinde blok zincirin işleyişine yönelik bilgilere yer verilmiştir. Merkezilikten uzak ve aracısız olan sistem işleyişinde ise dağıtık veri tabanı ve uçtan uca iletişim prensiplerinin önemli rol oynadıkları, diğer yandan kayıtların silinemezliği ve şeffaflık prensiplerinin de blok zincir teknolojisinin karakteristik ilkeleri olarak korunduğu hususlarına değinilmiştir. Şu halde blok zincirin temelinde; paylaşılan ve eşler arası bir veri tabanı olduğu ve şu ana kadar blok zincir içinde gerçekleştirilen tüm işlemleri depoladığı ifade edilebilecektir.[47]

D. Blok Zincir Türleri

Yukarıda bahsi geçen blok zincir özelliklerinin yanı sıra, blok zincirin kendi içinde de tür itibarıyla çeşitlendiği söylenebilecektir. Bu türlerin genel olarak ortak noktaları bulunmakla beraber, bazı noktalarda ayrıştığı görülebilecektir.

En temel ayrımlardan biri olan özel-kamusal blok zincir ayrımında, özel (private) blok zincirde sisteme dahil olabilmek için mevcut kullanıcıların izin vermesi gerekirken, kamusal (public) blok zincirde konsensüs algoritmalarına dayalı protokoller kullanıma açıktır ve izin sistemi bulunmamaktadır.

Özel blok zincirde; kullanıcıların sisteme dahil olmaları (kod) yazma ve izleme (okuma) faaliyetleri olarak ikiye ayrılmakta ve izinleri de buna göre belirlenmektedir. Şu halde yazma izinleri merkezi bir kuruluşta münhasır olarak tutulurken, izleme

[47] Avunduk ve Aşan, s.376.

izinleri listelenerek ancak belli kullanıcılara tanımlanmaktadır. Örneğin bir şirket tarafından oluşturulan özel blok zincirinde; zincire ekleme yapma yetkisi merkezde tutulurken şirket çalışanlarına izleme izinleri verilebilecek ve tüm bu uygulama belli kullanıcılara tanımlanacağı için yalnızca şirket içi bir uygulama olarak da gizlilik temin edilebilecektir.

Bahsedilen teknolojinin biraz daha somutlaştırılması adına sözgelimi bir eğitim derneğinin yardım projesi amacıyla kendi özel blok zincirini oluşturduğunu varsayalım; burada blok zincirin oluşumu esnasında yazma yetkileri isteğe göre tek bir kişiye ya da derneğin bir birimine verilecektir. Akabinde derneğin üyeleri ise projenin gidişatını bu zincirde kendilerine tanımlanan izleme yetkisi ile takip edebileceklerdir. Yine burada bahsi geçen izleme yetkisi de çeşitlendirilebilecektir. Öyle ki, dernek üyelerinin hem projeye katılımı veya bağış yapabilmesi, hem projenin gider ve maliyetlerini denetlemeleri de tanımlanacak izinler ile sağlanabilecektir. Şu haliyle özel blok zincir, işlemleri dahili olarak doğrulayabilecek gruplar veya katılımcılar oluşturarak blok zinciri teknolojisinden faydalanmanın bir yolu olarak da ifade edilebilecektir. Her ne kadar günümüz koşullarında bahsedilen örneğin online uygulamalar (akıllı telefonlarda kullandığımız applicationlar) aracılığıyla da gerçekleştirilebileceği düşünülse de, yine blok zincirin nihai ilkelerinden biri olan ‘aracıların ortadan kaldırılması’ prensibi gereği blok zincir sayesinde üçüncü bir kişiye ait olan uygulama olmadan da tüm bu organizasyon gerçekleştirilebilecektir.

Kamusal blok zincirde ise üçüncü kişi, sisteme katılım için diğer kullanıcıların rızalarına ve kendi aralarında konsensüs sağlamalarına ihtiyaç duymaksızın sistemden faydalanabilmektedir. Blok zincirin bu türünde, herkes işaret edilen kodu indirebilmekte ve kendi cihazlarında ortak bir düğüm oluşturmak üzere sistem üzerinde çalışmaya (ağdaki işlemlere onay vermeye ve konsensus sürecine katılmaya) başlayabilmektedir. Bunun yanı sıra, herhangi bir kullanıcı dünyanın neresinde olursa olsun sisteme bir işlem iletebilmekte ve geçerli olması halinde işlemin blok zincire eklenmesini bekleyebilmektedir. Kamusal blok zincirde işlemler şeffaf olarak ilerletilmektedir. Ancak belirtilmelidir ki burada ifade edilen şeffaflık, işlemlerin okunabilmesi anlamına gelmekte olup, işlemi gerçekleştiren kullanıcıların kimlik bilgileri kast edilmemektedir. Kamusal blok zincirinde dahi kullanıcılar kimliksiz ya da anonimleştirilmiş halde bulunmaktadır.

Yukarıda açıklanan temel farklılıkların yanı sıra kamusal ve özel blok zincir arasındaki diğer ayrımlar şu şekilde izah edilebilecektir;

	Kamusal Blok Zincir	Özel Blok Zincir
Erişim	Tüm kullanıcıların işlem yazma ve izleme yetkileri vardır	Sadece izin verilen kişilerin işlem yazma ve/veya izleme yetkileri vardır
Hız	Yavaş çalıştığı görülebilir	Kamusala göre daha hızlıdır
Güvenlik	Güvenliğin sağlanması için *İş Kanıtı (Proof of Work), *Pay/hisse Kanıtı (Proof of Stake) *Diğer konsensus mekanizmaları	Tüm kullanıcılar önceden onaylanmış olarak katılım sağlarlar
Kimlik	Kullanıcılar anonim ya da takma adlar ile katılım sağlarlar	Kullanıcılar açık kimlikleriyle katılım sağlarlar
Veri Sorumlusunun Tespiti	Mümkün değildir, tespit edilemez.	Blok zincirin özelliklerine bağlı olarak tespit edilebilir.
İşleyişteki onay prosedürü	Çalışma kanıtı (Proof of Work)	Risk kanıtı (Proof of Stake)
Erişim kontrol şeması	Herhangi bir devre ağa katılabilir, daha geniş kitlelere hitap eden PoW veya PoS benimsenebilir.	Sadece onaylanmış bir grup devrenin mutabakatı gerekir, daha küçük çaplı protokoller uygulanabilir.

Tablo-1

Kamusal ve özel blok zincir arasındaki en temel farklardan bir diğeri ise kamusal / genel bir blok zincir senaryosunda, ağa erişim ve verileri okuma işleminin kısıtlanamıyor olmasıdır. Buna karşılık, özel bir blok zincirine katılım için önceden izin alınması gerekmektedir. İzinsiz ve izinli blok zincirleri arasında da; her düğüm madencilik süreci önemli hesaplama kaynakları gerektirse de, işlemleri izinsiz bir blok zinciri bağlamında doğrulayabilmektedir. İzin verilen bir blok zinciri ortamında yalnızca yetkili düğümler madencilik işlemini gerçekleştirebilmektedir[48].

Çalışmamızın devamında daha detaylı anlatım bulacak olan veri sorumlusunun tespiti konusu da yine kamusal ve özel blok zincir arasındaki farklılık olarak karşımıza çıkmaktadır. Kısaca değinmek gerekirse, veri sorumlusunun tanımı;

Kişisel Verilerin Korunması Kanunu m.3/1-ı bendinde 'kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi'[49] olarak anlatım bulmuş iken,

Genel Veri Koruma Tüzüğü m.4/7 hükmünde; '(kontrolör) yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır' şeklinde yapılmıştır. Ancak blok zincir teknolojisinin dağıtık yapısı gereği veri sorumlusunun tespiti sorunsal teşkil etmekte olup çalışmamızın ilerleyen bölümlerinde detaylı olarak anlatılacaktır.

Bu bölümde, blok zincir türleri arasındaki en temel ayrım olan kamusal ve özel blok zincir üzerinden türler arasındaki işleyiş, izin, yetki farklılıklarına değinilmiştir. Kamusal blok zincirde tüm kullanıcılara sağlanan işlem yapma ve izleme yetkisinin varlığına karşılık; özel blok zincirde kullanıcıların sadece izleme yetkisinin bulunduğu ve katılımın da onaya bağlı olduğu düşünüldüğünde kamusal blok zincirin kullanım ve

[48] Dr. Jörg Kaufmann, Blockchain meets Data Privacy (Part 1), **The Legal Revolutionary**, 2018, s.120-127.

[49] Kişisel Verilerin Korunması Kanunu'nun 2008 yılında TBMM'ye sunulan ilk tasarısında veri sorumlusu yerine 'veri kütüğü sahibi' ibaresi kullanılmıştır. Bu metne göre veri kütüğü sahibi; 'kişisel verilerin işlenmesinin amaç ve metodlarını tek başına veya başkaları ile belirleyen gerçek ve tüzel kişiler' olarak tanımlanmıştır. Burada yapılan tanım ile mevcut Kanun'da yer alan veri sorumlusu tanımı karşılaştırıldığında ise mevcut Kanun ile fiilin yalnızca veri işleme faaliyeti ile sınırlı kalmadığı, veri kayıt sisteminin de tanıma dahil edildiği, bu anlamda veri sorumlusunun kapsamının genişletildiği anlaşılmaktadır. Bunun yanı sıra, her ne kadar eski Tasarı'da veri kütüğü 'sahibi' ibaresi kullanılmış ise de; mevcut Kanun ile veriye sahiplik temel ölçüt olmaktan çıkarılarak esas kriterin işlemler üzerindeki denetim ve etkinlik olduğu kabul edilmektedir.

katılımda daha serbest bir yapısının olduğu, özel blok zincirlerin ise daha küçük/sınırlı sayıdaki topluluklara hitaben kullanım alanı bulabileceği ortaya çıkmaktadır. Çalışmanın devamında ise zincirin işleyişini sağlayan doğrulama/onay mekanizmaları izah edilecektir.

E. Doğrulama/Onay Mekanizması Ayrımı

Bir önceki bölümde izah edilen kamusal-özel blok zincirdeki temel ayrımlardan sonra bu sistemdeki ikinci temel ayrım ise çalışma kanıtı (proof of work) ve risk kanıtı (proof of state) ayrımıdır. Bu ayrımda sistemin işleyişindeki onay yeterliliğinin hangi kritere göre (işlem çokluğu veya işlemin değeri şeklinde) belirleneceği gündeme gelmektedir.

Çalışma kanıtında; en fazla problem/şifre çözme yetisine sahip kullanıcı/kullanıcı grubu işleme onay vermekte ve sistemi devam ettirmektedir. Burada işe yönelik işlem hacmi ve hesaplama gücü 'onay kuralını' belirleyen kriterdir. Söz gelimi Bitcoin blok zincirinden yola çıkarsak; bu ağda özdeş veri kayıt defterine sahip her bir makine ağdaki şifrelemeyi çözmek için birlikte çalışırlar. Şifrelemeyi çözen ilk takım şifrenin çözülmesindeki en iyi hesaplama gücüne sahip olan -en çok çalışan- olarak sisteme onay verir. Sistemin dayandığı temel prensip, yeni bloğun eklenmesi için gereken çalışmanın kullanıcılar tarafından yoğun olarak gösterilmesidir. Çalışma kanıtı sisteminin kamusal blok zincirlerde kullanımı yaygın olmakla beraber, önemli miktarda hesaplama gücü ve elektrik maliyetine sebebiyet vermektedir. Yarattığı bu maliyet ise tüm katılımcıların tanındığı özel bir blok zincir ağında tercih edilmemektedir.

Risk kanıtı ise; işlemlerin doğrulanması için o ağdaki toplam değerin belirli bir yüzdesine sahip kullanıcının onayı gerekmektedir. Onay kuralının bu türünde, işlemde fraud ve saldırıların gerçekleşmesi yüksek maliyetler oluşturacağı için sistemin bu tür saldırılara karşı korunması amaçlanmaktadır. Bir başka deyişle, sistemin ele geçirilmesi pahalıya mal olacağı için risk kanıtı kuralının geçerli olduğu sistemlerin saldırılara karşı daha güvenli olduğu söylenebilecektir.[50]

[50] Manav Gupta, **'Blokchain for Dummies' IBM Limited Edition,** John Wiley & Sons, 2017, s.16-17.

Her ne kadar blok zincir uygulamalarında çok yaygın rastlanılmasa da bir diğer doğrulama mekanizmasına da veri korumaya sağladığı imkan nedeniyle bu çalışmada yer verilecektir. Sıfır Bilgi Kanıtı (Zero-Knowledge-Proof) adındaki bu yöntem, 1980'lerde MIT araştırmacıları tarafından önerilen bir şifreleme şemasıdır.[51] Bu anlaşma, bir tarafın (kanıtlayıcı=prover) diğer tarafa (doğrulayıcı=verifier) bilgi vermeksizin işi yaptığını ispatlayabildiği bir yöntemdir. Sıfır bilgi kanıtının günümüzde taşıdığı önem, içinde bulunduğumuz teknoloji çağı gereği hiç olmadığı kadar veri üretimi yapılması ile ilişkilidir. Doğrulama mekanizmaları arasında veri koruma hukukuna en elverişli olan yöntem olarak gündeme gelen bu mekanizmada, kanıtlayıcı, doğrulayıcıya verinin içeriğine dair bir bilgi vermeden doğrulayıcıya işlemi ispatlamaya çalışmaktadır. Kanıtlayıcı, nihai sonuca göre -kullanılan veri ve süreç bilgisi kullanılmadan- işlem sonucunu iletmektedir. Bu arada doğrulayıcı da sadece sonuçtan haberdar olacaktır ve onay verecektir. Bir diğer deyişle, sahip olunan bir bilgiyi başkasına, bilgiyi o kişiyle paylaşmaksızın ispatlama yöntemi olarak tanımlanmaktadır. Bu algoritma, blok zinciri sistemindeki mahremiyetin arttırılmasında etkili bir yöntem olarak görülmektedir.[52]

Çalışmamızın bu bölümünde blok zincir teknolojisindeki onay kuralını belirleyen esaslara dikkat çekilmiştir. Bir önceki bölümde yer verilen kamusal/özel blok zincir ayrımında da değişkenlik gösteren bu ayrımda, daha geniş bir kitle tarafından kullanılması halinde -kamusal blok zincir örneğindeki gibi- daha fazla problem çözen grubun işleme onay vermesi ile sürecin devam ettirildiği, daha az kullanıcı ile çalışan sistemlerde ise -özel blok zincir örneğindeki gibi- kişi sayısından çok ağdaki toplam değere sahip olan gruba onay yetkisi tanınmaktadır. Bu anlamda çok katılımcının bulunduğu ortamlarda ‘çok çalışan grubun’, daha az katılımcı ile sürdürülen bir sistemde ise ‘riski yüksek olan’ grubun söz sahibi olduğu söylenebilecektir. Çalışmamızın bir sonraki bölümünde ise, onay kuralı türünden bağımsız olarak, sistemin genel itibarıyla konsensusun sağlanması için gerekli teşvik mekanizmasına değinilecektir.

[51] Zero Knowledge Proof yöntemi, ilk olarak 1985 yılında Shafi Goldwasser, Silvio Micali ve Charles Rackoff tarafından hazırlanan ‘The Knowledge Complexity of Interactive Proof-Systems’ adlı makalede kullanılmıştır.

[52] Ersin Ünsal ve Ömer Kocaoğlu, Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri, **Avrupa Bilim ve Teknoloji Dergisi,** Sayı: 13, s.61.

F. Oyun Teorisi

Çalışmamızın bu bölümünde blok zincir sisteminin işleyişindeki teşvik unsuru olan oyun teorisine değinilecektir. Ardından sistemin işleyişinde rol oynayan temel prensipler bir arada değerlendirilecek ve blok zincir sisteminde karşılaşılan güncel sorunlar bölümüne geçiş yapılacaktır.

Oyun teorisi, bir sistemdeki karar mekanizmaları arasındaki karşılıklı bağımlılık ile beslenen, karar vericilerin bu aşamadaki stratejilerini inceleyen uygulamalı matematiğin bir dalı olarak literatürde yer almaktadır.[53]

Blok zincir, -önceki bölümlerde detaylı olarak izah edildiği üzere- eşler arası bir ağda bir dizi devre arasında uzlaşının sağlanarak işleyişin devam ettiği bir veri kayıt defteridir. Buradaki her bir işlem, blok zincirinin temel veri yapısına doğrulanarak eklenmekte ve bu şekilde zincir büyütülmektedir. Devreler arasında kurulan her bir konsensusun neticesi ise gerçekleşmiş bir işlemdir. Bu nedenle ağa katılımın sağlanması için bir grup uzlaşı devresi gerekmektedir. Oyun teorisi bu noktada işleyişe dahil olarak devrelere yönelik teşvik mekanizmalarını oluşturmaktadır. Blok zincir, dağıtık bir sistemde çok sayıda kullanıcının fikir birliğinin sağlanması ile işleyişini sürdürebildiği için ağdaki katılımcıların mutabakatları büyük önem taşımaktadır. Fakat birbirini tanımayan bu katılımcıların da birbirlerine güvenmeleri ancak ortak bir strateji ve dürüst davrandıklarında kazanabileceklerini bilmeleri sayesinde gerçekleşecektir. Nitekim bu devrelerin de rasyonel ve kötü niyetli olarak ikiye ayrıldıkları söylenebilecektir. Rasyonel devreler sistemden sağladıkları faydayı maksimize etmek amacıyla eylem ve stratejiler belirlemekte iken, kötü niyetli devreler blok zincir ağlarına zarar veren saldırılara odaklanmaktadır.

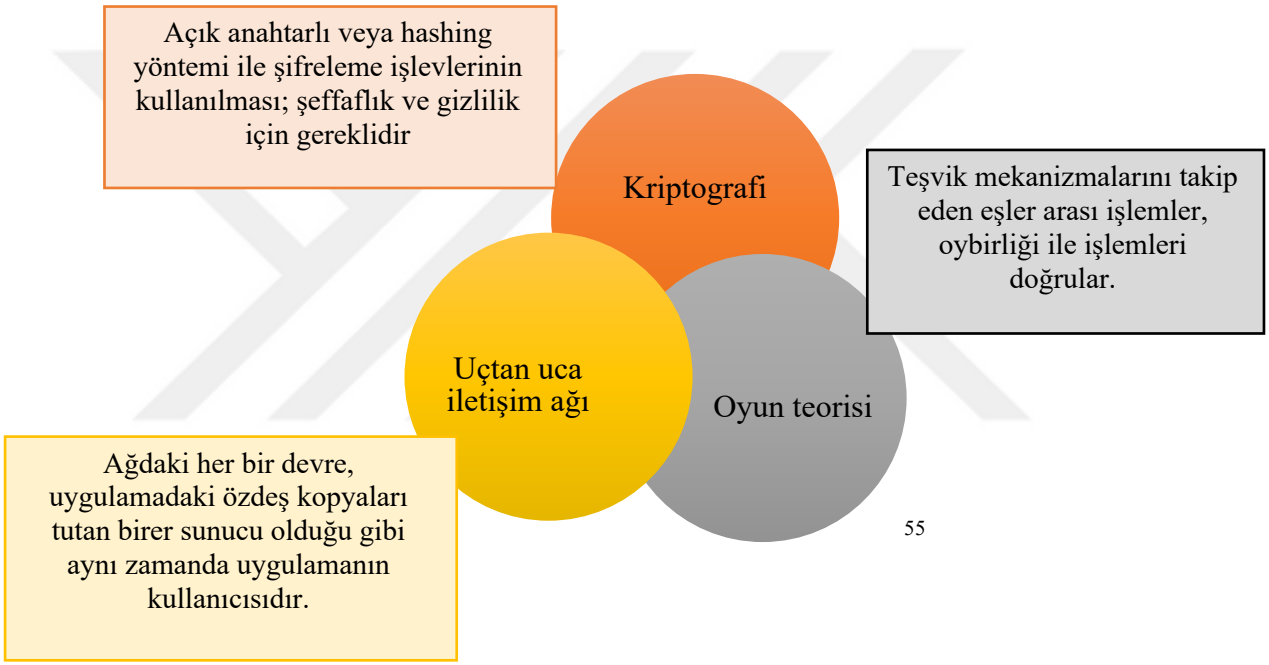
Bu noktada hem sistemin iyi niyetli kullanıcılarının teşviki hem de kötü niyetli kullanıcılara karşı saldırı önlemi alınması gerekmektedir. Bir tarafın kazanırken diğer tarafın kaybettiği oyun teorisi ise tam olarak bu noktada çözüm getirmektedir. Oyun teorisi sayesinde, mutabakat devrelerinin stratejilerini ve aralarındaki etkileşimleri analiz etmek amacıyla da kullanılabilmektedir. Bu sayede, yapılan analiz ile devreler

[53] Sema Yıldız Genç ve Hamza Kadah, Oyun Teorisi ve Nash'in Denge Stratejisi, **Iğdır Üniversitesi Sosyal Bilimler Dergisi,** Sayı:14, Nisan 2018, s.421.

birbirlerinin davranışlarını öğrenebilmekte de tahmin edebilmekte, daha sonra denge analizine dayanarak strateji geliştirebilmektedirler.

Netice itibarıyla oyun teorisi, devrelerin hem saldırılara karşı korunmasını hem de sistemin işleyişi için gerekli devrelere yönelik teşvik mekanizmaları geliştirmek için kullanılmaktadır.[54]

Önceki bölümlerde blok zincir teknolojisini oluşturan tüm unsurlar detaylı olarak açıklanmıştır. Bu sisteme ait temel prensipler üçlü sac ayağı olarak özetlenmek istenirse, Şekil-5'te ifade edildiği üzere;



Şekil-5

Sistemin güvenilirliğini sağlayan gizlilik ilkesi gereği sistemdeki veriler *şifreli* olarak ağda yer almaktadır. Bunun yanı sıra ağdaki her bir devre, birbiriyle eş bilgilere sahip *dağıtık bir veri yapısındadır* ve sistemin çalışması için *ortak bir stratejiyle* hareket etmektedir. Devrelerin arasındaki bu stratejinin belirlenmesi ve her bir kullanıcının dürüst şekilde sistemde onay prosedürünü işletmesi için teşviğin sağlanmasında *oyun teorisi* rol oynamaktadır. Belirtilen esasların somutlaştırılması adına çalışmamızın bir sonraki bölümünde Bitcoin blok zinciri örneğine yer verilecektir.

[54] Liu ve Diğerleri, **A Survey on Applications of Game Theory on Blockchain,** IEEE, 2019, s.1.
[55] https://blockchainhub.net/blockchain-intro/ Erişim tarihi: 01.07.2019

G. Bitcoin Örneği

Bitcoin uygulaması olarak kullanılan blok zincir, Bitcoin aracılığıyla yapılan işlemlerden oluşan bir fiziki defter olarak somutlaştırılabilecektir. Tüm sayfa işlemler ile tamamen dolduğunda yeni bir sayfaya geçilmekte ve işlemler buradan devam etmektedir. Tamamen dolan sayfa, zaman damgası ile benzersiz bir seri numarası alarak damgalanmaktadır ve fiziki defterden ayrılmamak üzere yerini alan bir sayfa haline gelmektedir. Bu somutlaştırmada her bir işlem sayfasını blok zinciri oluşturan 'blok', her sayfaya ait seri numara da bloklar arasındaki bağlantıyı gösterir ve art arda gelen seri numaralar bir 'blok zinciri' oluşturmaktadır. Burada önem taşıyan nokta ise sayfaları birbirine bağlayan seri numaraların birbirine kilitlenerek zinciri oluşturuyor olmalarıdır. Öyle ki bu sayede seri numaralar bir kez oluştuktan sonra sayfalarda yer alan işlemler değiştirilememektedir. Başka bir anlatımla, defterdeki bir işlemin sonradan değiştirilebilmesi için o işlemden sonra gerçekleşen tüm işlem sayfalarının çıkarılması ve bu sayfaların da yeni işlemler ile doldurulması, sonrasında bağlantı için yeni seri numaralarının oluşturulması ve tüm bu yeni sayfaların tekrar deftere eklenmesi gerekir ki; mümkün değildir. Netice itibarıyla, sistemin çalışma prensibi gereği kullanıcılar tarafından art arda eklenen işlemlerde tek bir kullanıcının işlemi değiştirmesi mümkün olmamaktadır ve blok zincirin 'otoriteyi' dağıtmış olmasıyla bu yapının üçüncü kişilerin güvenlik tehditlerine karşı güvenli olduğu söylenebilmektedir.[56]

Bitcoin, son yıllarda deep web'de[57] yaratılan ve bugüne gelen olumsuz algıdan henüz kurtulabilmiş ise de; temelini oluşturan blok zincir teknolojisi toplumlara ve işletmelere kontrol mekanizması olmaksızın ve kimlik denetiminden bağımsız bir uluslararası, hızlı ve güvenilebilir platform olarak kendisini ispatlamıştır.[58] Bitcoin'in yanı sıra dijital finans dünyasına girmiş veya girmeye hazırlanan çok sayıda türev ödeme sisteminin bulunduğu da günümüz gerçekleri arasındadır.[59]

---

[56] Avunduk ve Aşan, s.371-372.

[57] 'Deep web' kavramı, arama motorları tarafından adreslenmemiş, bu aracılar üzerinden ulaşılamayan web siteleridir. Bitcoin yapısı itibariyle kullanıcı kimliklerinin gizliliğini sağlar bu sebeple ilk çıkış noktası deep web'deki yasa dışı gelirler için kullanılan bir uluslararası veri transferi sistemidir. Bu nedenle Bitcoin uygulamasının ilk imajının olumsuz olduğu söylenebilecektir.

[58] Usta ve Doğantekin, s.26-27.

[59] Yakın zamanda dijital bir varlık olarak lanse edilen Libra, Facebook tarafından hazırlanan bir blok zincir altyapısı olarak tanımlanmaktadır. Bu para birimi İsveç merkezli Libra Association tarafından yönetilmeye hazırlanmaktadır.

İnternetin kitlesel kullanımına baktığımızda ise, veri mimarilerinin çoğunlukla kullanıcı-sunucu tabanlı şekillendirildiği görülmektedir. Bir anlamda bu durum, verilerin bir bilgisayarda merkezi olarak depolandığı ve internet üzerinden başka bir bilgisayar tarafından alındığı anlamına gelmektedir. Her cihazın (ekmek kızartma makinesi veya buzdolabının dahi) internete bağlı olduğu bir dünyada yaşanmasına rağmen[60], veriler hala merkezi olarak cihazlarda, USB'lerde veya bulut depolama sistemlerinde depolanmaktadır. Bu noktada güven sorunlarının gündeme gelmesi ise kaçınılmaz olmaktadır. Kullandığımız cihazlar gereği depolanan tüm bu verilerin herhangi bir ihtilaf halinde veri sahiplerine karşı nasıl kullanılacağı, bir hizmetin veya ürünün kullanılabilmesi için işlenmesine rıza gösterilen verilerin merkezi veri tabanlarında hangi güvenlik tedbirleri ile -veya tedbirsiz- saklandıkları, bu merkezi veri depolarının kimlerin yönetiminde olduğu sorunsalları bir bütün halinde merkezi veri kayıt sistemlerinde karşımıza çıkmaktadır.[61]

Çalışmamızın bu bölümünde merkezi veri kayıt sistemlerinin beraberinde getirdiği 'merkezi yöneticiye güven' sorununa değinilmiştir. Blok zincir teknolojisi, her ne kadar dağıtık veri tabanı ile merkezilikten uzaklaşılarak ve aracısız olarak -dolayısıyla güvenmek zorunda olmadan- işlem yapılmasını vaat ediyor olsa da; blok zincir teknolojisinin de henüz çözülememiş sorunları bulunmaktadır. Bir sonraki bölümde bu sorunlara yer verilecektir.

H. Blok Zincir İşleyişinde Güncel Sorunlar

Blok zincir teknolojisinin potansiyel kullanım alanları çok çeşitlilik göstermektedir. Otomotiv, bankacılık, eğitim, enerji ve e-devlet üzerinden sağlık,

---

27 ortaklı şirketin ortakları arasında Uber, Spotify, PayPal, Ebay, Visa, Mastercard gibi farklı sektörlerden yatırımcılar yer almaktadır. 2020 yılında piyasaya sürülmesi beklenen bu dijital paranın ilk aşamada amacı Facebook üzerinden gerçekleşen online alışverişlerde ödeme sistemi olarak kullanılmasıdır. Diğer dijital para birimleri gibi Libra'da da günümüz finans dünyasından farklı olarak 'bir para biriminin bir şirket tarafından yönetilmesi' ve 'bir ülkeye bağlı olmadığı için uluslararası politik gelişmelerden etkilenmeyen bir değerinin olması' gibi gelecekteki dijital finans dünyasının ilkelerinin görünebileceği söylenebilecektir.

[60] Bu noktada 'Nesnelerin İnterneti' kavramı gündeme gelmektedir. Şöyle ki, yakın gelecekte her yönüyle uygulamalarını göreceğimiz bu kavram, çevremizdeki fiziksel olayları kontrol etmemizi ve takip ederek analiz etmemizi sağlayan cihaz, yazılım ve erişim hizmetlerini kapsayan bir iletişim ağıdır. Bir başka anlatımla, sürekli tükettiğiniz içeceğin buzdolabında eksilmesi halinde internet üzerinden ürünün siparişini veren otomatik evlerde oturup, meteoroloji sistemi ile bağlantısı bulunan akıllı yollarda sürücüsüz araçlarda yolculuk yapabilmemizi sağlayacak olan makine-makine (M2M) temelli teknolojidir.

[61] https://blockchainhub.net/web3-decentralized-web/ Erişim tarihi: 08.03.2018

sigorta, hukuk, müzik, sanat, emlak ve seyahat gibi sektörlerin çoğunda değişim amacıyla blok zincire odaklanılmaktadır. Dijital veri kayıt defteri olarak kullanılan blok zincir; gayrimenkul, araç ve diğer kıymetli taşınırların kayıtlarından doğum, evlilik, ölüm gibi nüfus kayıtlarının tutulmasına kadar pek çok kamusal alanda uygulanabilecektir. Bunların yanı sıra, akıllı sözleşmelerin yönetiminden seçimlerin güvenli bir şekilde gerçekleştirilebilmesine ve hatta maliye alanında finansal dokümanların saklanması, işlenmesi ve yönetilmesi alanlarında da fayda sağlayabilecektir. Blok zincir teknolojisi ile bireylere dijital kimlikleri üzerinde geniş kontrol imkanları sağlanmakta ve bu sayede güven ekonomisinin anahtarı olarak da addedilebilmektedir.[62]

Gelecekte uygulama alanlarının daha da çeşitleneceği gözüyle bakılan bu teknoloji, günümüzde dahi çok sayıda sektörde keşfedilmeye başlamıştır. Yaygın kullanımının dijital paralar olduğu görülen blok zincir teknolojisinin; e-ticarette, uluslararası ödeme, havale ve kredilendirme işlemlerinde kullanıldığı görülmektedir. Banka işlemleri konusunda çok sayıda Avrupa bankasının dijital e-ticaret işlemleri için blok zincir teknolojisini test ettikleri, ülkeler arası ticaretin finansal işlemler kısmında blok zincir teknolojisinin kullanımının başladığı eklenebilecektir.

Blok zincirin yaygın olarak gözlemlenen uygulama alanları 4 ana başlıkta toplandığında; sırasıyla akıllı sözleşmeler, dijital paralar ve dolandırıcılık faaliyetlerinin azaltılması, mülkiyet ve güvenlik olarak belirmektedir.

Akıllı kontratlar; blok zinciri üzerinde depolandıktan sonra kendiliğinden uygulayacak kod parçalarıdır, böylece blok zinciri ağının güven ve güvenliğinden yararlanılmaktadır. Akıllı sözleşmeler daha çok bir emtinanın belirli koşullar oluştuğunda el değiştirmesi, devredilmesi amacıyla kurulmaktadır. Bu anlamda herkes tarafından bilinen en yaygın akıllı kontratın içecek/gıda otomatları olduğu söylenebilecektir. Bu en basit akıllı kontratta belirli tutarda atılan madeni paranın karşılığında otomatta yer alan ürün doğrudan ve aracısız olarak alınabilmektedir. Temel mantığı birinci koşulun gerçekleşmesi halinde ikinci aşamaya geçilmesi olan bu kontratlarda; işlem çeşitliliği sağlanabileceği gibi taraf sayısı da arttırılabilecek ve komplike hale de getirebilecektir.

[62] Dilek Şerif, s.11.

Akıllı kontratlar, kullanıcıların işletme mantığını otomatikleştirmelerine izin vermekte ve bu nedenle iş süreçlerini ve hizmetlerini geliştirmekte veya tamamen yeniden tasarlamaktadır.[63]

Dijital paralar ve dolandırıcılık faaliyetlerinin azaltılması kapsamında görülen blok zincir uygulamalarında başta Bitcoin gelmektedir. Öyle ki, aracıların ortadan kaldırılarak uluslararası havale işlemlerinin dahi yapılmasına olanak sağlayan bu teknoloji, kendisini ilk olarak Bitcoin aracılığıyla teyit ettirebilmiştir. 2008 yılında Satoshi Nakamoto tarafından kaleme alınan makale ile Bitcoin ortaya çıkmış ve akabinde Bitcoinin temelinde yatan blok zincir teknolojisi -yıllar önce icat edilmiş olmasına rağmen- bu makale sonrasında tekrar gündeme gelmiştir.

Blok zincirin temel özelliklerinden biri olan eşten eşe transfer sayesinde her türlü aktarım işlemi, aracıya ihtiyaç olmadan taraflar arasında gerçekleştirilebilmektedir. Dolayısıyla banka işlemlerinde zaman zaman aracı sayısının 3'e çıkabildiği durumlardan olan uluslararası havalelerde, aracıları ortadan kaldıran blok zincir teknolojisinin gelişime açık alanlarından biri olduğu aşikardır.

Bu anlamda uluslararası ticaret faaliyetlerinde dijital teknoloji imkanlarının genişletilmesi amacıyla IBM önderliğinde Avrupa'nın en büyük bankaları olan Deutsche Bank, Societe Generale, UniCredit, Natixis, HSBC ve Rabobank ile blok zincir teknolojisi aracılığıyla dijital ticaret zinciri için işbirliği kurma girişiminde bulunmuştur.[64]

Fikri mülkiyet haklarında ise blok zincir ve dağıtık muhasebe teknolojisi, fikri mülkiyet haklarında koruma, tescil ve sicil aşamasının yanı sıra mahkemede kanıt sunulabilmesi açısından büyük olanaklar sağlamaktadır. Bu alanda potansiyel kullanım alanları ise fikri mülkiyet haklarının tescili ve silinmesi, kayıtlı/kayıtsız IP'lerin dağıtımının kontrolü ve izlenmesi, ticari mallarda orijinal (veya ürünün birinci el) olduğuna dair kanıtların sağlanması, online müzik sitelerinde dijital hakların yönetimi, akıllı sözleşmeler yoluyla IP anlaşmalarının yapılması, lisans anlaşmalarının yönetimi

[63] Blockchain and the GDPR (Thematic Report), s.34.
[64] https://www.cnbc.com/2017/06/26/ibm-building-blockchain-for-seven-major-banks-trade-finance.html, Erişim tarihi: 18.06.2019

ve ödemelerin eş zamanlı olarak hak sahiplerine iletimi gibi konulardır. Bunun yanı sıra, blok zincir teknolojisi sahte, çalıntı veya izinsiz olarak üretilen/çoğaltılan malların tespitinde ve orijinallik kanıtında da kullanılabilecektir.

Blok zincir her problem için kesinlikle çözüm olmasa da, akıllı sözleşme otomasyonu ve aracıların kaldırılarak düşük maliyetlerin sağlanması, daha az hata ve dolandırıcılık riskleri ve birçok süreçte önemli ölçüde geliştirilmiş hız ve deneyim sağlayabilmektedir.[65]

Blok zincir, verinin iletişim ağları üzerinden, dağıtılmış şekilde saklanmasını ve bu süreç içinde verinin tüm noktalarda aynı kaldığına dair mutabakat yapılmasını sağlar. Bunun yanı sıra her kullanıcı kendi verisini şifreleyeceği için bu veriyi sadece kendisi kullanabilmekte ve izin verirse diğer tarafların bu veriye erişimi mümkün olabilmektedir.[66] Bir diğer deyişle, merkeziliğinin olmaması, yüksek düzeyde şeffaflık içermesi, şifreleme ve takma adlandırma tekniklerine imkan tanıması özellikleri sayesinde blok zincir bireylerin kişisel verileri üzerindeki kontrolünü arttırma konusunda olumlu bir etkiye sahiptir.[67]

Güvenilir bir üçüncü tarafa gerek kalmaksızın bireyler arasında işlem yapılmasını mümkün kılan bu sistem, aracısız olarak her türlü alışverişin gerçekleştirilmesini sağlar. Bunun yanı sıra, tüm kullanıcıların işlem geçmişlerini görmelerini ve bu sayede eksiksiz bir işlem geçmişi ile sanal paraların geçerliliğini temin eder, sanal paraların oluştuğu andan itibaren izlenmesine imkan sağlar. Ayrıca teknolojiyle çözünürlük sağlanarak geçmişe yönelik şeffaflık da beraberinde getirilmektedir. Bu sayede geçerli kayıtların değiştirilmesi de engellenir. Bu teknoloji sayesinde yönetime ihtiyaç duyulmamakta ve aracısız olarak gerçekleştirilen işlemlerde maliyetleri de düşürülebilmektedir.[68]

Ne var ki, yukarıda sayılan tüm bu olumlu niteliklerinin yanı sıra blok zincir teknolojisinden beklenen tam faydanın sağlanması adına kat edilmesi gereken uzun bir

[65] Blockchain and the GDPR (Thematic Report), s.33.
[66] Usta ve Doğantekin, s.45.
[67] Roberta Filippone, **Blockchain and Individuals Control Over Personal Data in European Data Protection Law**, Master Thesis, Tilburg University Press, 2017, s.28.
[68] Beck ve Diğerleri, Blockchain-the Gateway to Trust-Free Cryptographic Transactions, **European Conference on Information Systems**, 2016, s.4.

yol olduğu da aşikardır. Nitekim mevcut durumda karşılaşılan bazı teknik ve hukuki zorluklardan bahsedecek olursak;

Teknik anlamda blok zincirin iş hacmi, işlem gerçekleşme süreleri, boyut ve bant genişlikleri, güvenlik, kaynak tüketimi, kullanılabilirlik, sürüm, zor çatallar ve çoklu zincirler problem yaratmakta iken hukuki boyutta ise mahremiyet konusu ve nihayetinde çalışmamızın temel başlıklarından biri olan 'unutulma hakkı'nın kullanımı sorunu gündeme gelmektedir.

Blok zincir teknolojisinin başlangıç dönemlerinde yapılan testlerde saniyede yedi işlem yapılabilirken; geliştirmeler sonucunda Amazon İnternet Servisleri'nde gerçekleştirilen büyük ölçekli testin neticesinde Avustralya Ulusal Bilim Ajansı ve Sydney Üniversitesi'nin raporuna göre saniyedeki işlem sayısı 30.000 olarak test edilmiştir.[69] Bu işlem hacmi, ana blok zincirlerde daha düşük seviyelerde iken VISA'nın 2017 Ağustos testlerine göre saniyedeki işlem hacmi ise 65.000 seviyelerindedir.[70]

İşlem gerçekleşme sürelerine bakıldığında ise bir bloğun oluşma süresinin yaklaşık 10 dakika sürdüğü, bu sürenin ise özellikle blok zincir teknolojisinin finans sektöründeki işlemler açısından yetersiz kalabileceği düşünülmektedir.

Blok zincir teknolojisinde daha fazla işlem yapılmasının önündeki engeller fiziksel kaynak veya yazılım kısıtlamalarıdır. Veri aktarım hızı ışık hızı ile sınırlıdır ve birim zamanda gönderilebilecek veri miktarını bant genişliği belirlemektedir. Verinin iletim hızı, işlemin büyüklüğüne bağlı olmakla beraber çoğu küresel ağda bu süre yaklaşık 2-3 saniye sürmektedir. Mevcut durumda, işlem söz gelimi Bitcoin blok zinciri için yaklaşık 500 bayt olduğundan, blok zincirin VISA ile rekabeti söz konusu olduğunda ağın saniyede 8 Megabit ile iletişim kurabilmesi gerekmektedir.

Güvenlik sorunsalı ise -her ne kadar blok zincir teknolojisi güven makinası olarak literatürde yerini almışsa da- blok zincir oluşumunda %51 saldırısı şeklinde ifade

[69] https://www.csiro.au/en/News/News-releases/2018/Next-generation-blockchain-boosts-speed-and-energy-efficiency-on-global-scale Erişim tarihi: 07.06.2019

[70] https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf Erişim tarihi: 07.06.2019

edilen bir risktir. Bu durumun tüm bir blok zincir ağındaki kullanıcıların yarısından fazlasının aynı olumsuz amaca yönelik harekete geçmesi halinde ortaya çıkabileceği göz önüne alınmalıdır. Bir diğer güvenlik sorunu da spesifik olarak dijital para transferi işlemlerinin gerçekleştirildiği takas merkezlerinde ön plana çıkmaktadır. Ancak takas merkezlerinde gözlemlenen güvenlik zafiyetlerinin çoklu imza güvenlik tedbirlerinin önemsenmemesi ve soğuk cüzdan kullanımı gibi önlemlerin ihmalinin sebep olduğu da görülebilmektedir.[71]

Blok zincirde kişisel verilerin korunması konusunda ise blok zincirin sahipsiz yapısı gereği katılımcılar sistemde doğrudan kişisel verilerini kullanmamaktadırlar. Bu anlamda sadece transferlerin gerçekleştirilmesi neticesinde oluşan şifreler ile kişilerin teşhisi mümkün kılınmamaktadır. Ancak Büyük veri uygulamaları aracılığıyla şifrelerin çözümlenerek işlemi gerçekleştiren gerçek kişilere ulaşılabilmektedir.[72]

Blok zincir teknolojisindeki güncel sorunlardan bir diğeri olan enerji tüketimi ise blok zincir teknolojisinin önem arz eden handikaplarından biridir. Öyle ki; bir yandan maliyetlerin düşük olduğu transferler hedeflenmekte iken diğer yandan da blok kullanıcı sayısının artmasıyla zincirlerin oluşma süresi uzamakta ve bu durum da işlemlerin onaylanma sürecinde tüketilen enerji miktarını artırmaktadır.

2019 yılında yapılan bir araştırmaya göre, blok zincir teknolojisinin en bilinen örneği Bitcoin ağının yıllık harcadığı elektrik miktarı ortalamada 50 terawatt/saat olarak hesaplanmıştır. Belirtilen miktardaki elektrik ise Avrupa'daki tüm su ısıtıcılarının 1 yıl boyunca tüketimlerine, ABD'nin tamamında etkin olmayan ev cihazlarının tükettiği 3 aylık enerjiye veya Cambridge Üniversitesi'nin 365 yıllık enerji ihtiyacına denk gelmektedir.[73]

Netice itibarıyla, her ne kadar aracıları ortadan kaldırmayı ve işlem yapabilmek için güvenmek zorunda kalınmayacağını vaad eden bir teknoloji olsa da, blok zincir henüz bir teknolojinin erken çocukluk dönemini yaşamaktadır. Bu anlamda iş hacmi,

---

[71] Ünsal ve Kocaoğlu, Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri, **Avrupa Bilim ve Teknoloji Dergisi**, Sayı:13, 2018, s.61.

[72] Mesut Serdar Çekin, **6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 1. Baskı, 2018, s.37-38.

[73] http://www.epe.admin.cam.ac.uk/cambridge-bitcoin-electricity-consumption-index-cbeci Erişim tarihi:20.07.2019

işlem süreleri, enerji tüketimi gibi teknolojinin diğerlerine tercih edilmesini sağlayan pek çok alanda geliştirilmesi ve öne çıkması gerekmektedir.

İKİNCİ BÖLÜM
VERİ KORUMA HUKUKU AÇISINDAN BLOK ZİNCİR

II-BLOK ZİNCİR TEKNOLOJİSİNİN VERİ KORUMA HUKUKU AÇISINDAN İRDELENMESİ

Çalışmamızın ikinci ana bölümünde, detaylı olarak izah edilen blok zincir teknolojisi içerisinde veri koruma hukukunun durumu irdelenecektir. Ancak öncesinde veri koruma hukukunun Türk ve AB hukuku bağlamında temellendirilmesi yapılarak blok zincir uygulamalarının incelenmesinde fayda olacağı düşünülmektedir.

A. Veri Koruma Hukukunun Kısa Tarihçesi

Çalışmamızın bu bölümünde, Türk ve Avrupa Birliği'nde veri koruma hukukuna yönelik yapılan düzenlemelerin geçmişleri ve gelişimleri incelenecektir. Her ne kadar Kişisel Verilerin Korunması Kanunu ve Genel Veri Koruma Tüzüğü zamanlama olarak birbirine çok yakın olsa da; tarihçelerinde ve temellendirmelerinde farklılıklar taşıdığı gözetilerek iki ayrı başlıkta irdeleneceklerdir.

1.Türk Hukuku'nda:

Türkiye'de kişisel verilerin korunmasına ilişkin süreç, AB ile eş zamanlı olarak 28 Ocak 1981 tarihinde Strazburg'da imzalanan ve 1 Ekim 1985 tarihinde yürürlüğe giren 108 Sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme" ile birlikte başlamaktadır. Ancak bu sözleşmenin iç hukuka uyarlanması ve TBMM onayından geçmesi 35 yıl sonra gerçekleşmiştir. Bu süreç, KVKK Gerekçesi'nde; '*Kişisel verilerin korunmasına dair kanunun hazırlanması, ülkemizin Katılım Ortaklığı Belgesine cevap olarak hazırladığı 2003 Ulusal Programında taahhüt ettiği yükümlülüklerdendir'* ifadesiyle anlatım bulmuştur. Yine aynı gerekçede kişisel verilerin korunmasına yönelik bir mevzuatın bulunmamasının emniyet birimleri arasında etkin bir işbirliğinin sağlanmasını hedefleyen EUROPOL ile ülkemiz arasında operasyonel bir işbirliği anlaşmasının

yapılamadığı, benzer şekilde sınır ötesi suçlarda yargının ortak operasyonlar geliştirebildiği bir oluşum olan EUROJUST ile işbirliği yapamadığı hususları yer almaktadır.[74]

23 Mayıs 2007 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ise internet ortamındaki en önemli aktörler olan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının hak ve sorumlulukları belirlenmeye başlanmıştır. Bu düzenleme ile getirilen 'bilgilendirme yükümlülüğü' kullanıcıların sağlayıcılara erişimini mümkün kılan önemli bir zorunluluk iken yine aynı düzenleme ile gelen 'yer sağlayıcı trafik bilgisi' ise zaman içerisinde gelişim göstererek KVKK'da veri sorumlusunun alması gereken idari ve teknik tedbirler arasında yer edinmiştir.

5651 sayılı Kanun'un ardından, 5 Kasım 2014 tarihli Resmi Gazete'de yayımlanan ve 1 Mayıs 2015 itibarıyla yürürlüğe giren 'Elektronik Ticaretin Düzenlenmesi Hakkında Kanun' ise özellikle KVKK'da yer alan verilerin işlenmesi için açık rıza alınması kavramının temelini oluşturmaktadır.[75]

2016 yılına kadar gelinen süreçte Türk Hukuk Mevzuatında farklı alanlarda ve ortaya çıkan ihtiyaca yönelik olarak kişisel verilerin korunması hakkında farklı düzenlemeler yapılmıştır. Bu süreçte özellikle Anayasa'nın 20. maddesi ve TCK'nın 'Özel hayata ve hayatın gizli alanına karşı suçlar' bölümündeki hükümleri, kişisel verilerin korunmasına yönelik yargılama süreçlerinde önemli rol oynayan düzenlemelerdir. Ancak bu düzenlemelerin hiçbiri önleyici nitelikte değildir. Bu nedenle, konunun özel bir kanun çerçevesinde değerlendirilmesi ihtiyacı artmış ve KVKK'nın yürürlüğe giriş süreci hızlandırılmıştır.[76] Nihayetinde 07.04.2016 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu ile süreç son bulmuştur.

---

[74] https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim tarihi: 22.07.2019

[75] Sanayi ve Ticaret Bakanlığı nezdinde oluşturulan çalışma grubunun, Avrupa Birliği 2000/31/EC sayılı E-Ticaret Direktifi'nin Türk yasalarına uyumuna yönelik çalışması sonucunda adı geçen Kanun oluşturulmuştur. https://ticaret.gov.tr/data/5b87dcea13b8761160fa1832/5ba2e8d35824ddbab72d6e6c477d8c80.pdf, Erişim tarihi:01.07.2019

[76] Türkay Henkoğlu, **Veri Koruma Kanununun Getirdikleri**, Journal of Current Researches on Social Sciences, 2017, s.242.

2.Avrupa Birliği Hukuku'nda:

Avrupa Birliği Hukuku'nda veri koruma süreci, 1995 yılında AB içindeki kişisel verilerin işlenmesini düzenleyen 95/46/EC sayılı Veri Koruma Direktifi'nin kabul edilmesiyle başlamıştır. Ardından 8 Haziran 2000 tarihli 2000/31/EC sayılı Elektronik Ticarete İlişkin AB Yönergesi ile bilgilendirme yükümlülüğü, istenmeyen ticari iletişime karşılık opt-out seçeneğinin düzenli olarak sunulmasının yanı sıra içerik ve yer sağlayıcılarına başvuru hakları gibi hakların düzenlendiği görülmektedir.

2012 yılında ise Avrupa Komisyonu'nun General Data Protection Regulation (GDPR)'ı geliştireceklerini açıklamasıyla veri koruma hukukunda yeni bir sürece girilmiştir. 2015 yılının Aralık ayında, Avrupa Parlamentosu, AB Konseyi ve AB Komisyonu GDPR hakkında anlaşmaya varmışlardır. Aynı yılın Mayıs ayında ise 2016/679 sayılı Regülasyon (GDPR) yürürlüğe girmiştir.

B. Temel Kavramlar

Bir önceki bölümde bahsi geçen yasal düzenlemeler ile birlikte veri koruma hukuku hayatımıza girmiştir. Bu çerçevede veri sahiplerine sunulan haklara değinmeden önce temel kavramlar irdelenecektir;

Veri; olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi olarak tanımlanmıştır.[77] Daha kısa bir ifadeyle ise işlenmemiş, ham bilgi parçacığının adıdır.[78] İngilizce ve Latince dillerinde aynı kelime olarak karşımıza çıkan ve artık günlük yaşamda da dilimize karışmaya başlayan Data kelimesinin Türkçe karşılığıdır.

Veri koruma hukuku nezdinde yer alan kişisel veri ise, genel veri tanımının daha dar bir yorumudur. Şayet elimizdeki veri 'bir gerçek kişiyi adresliyor veya adreslenebilir kılıyor ise' o verinin kişisel veri olduğu kabul edilmektedir. Türk ve AB Veri Koruma Hukukundaki yasal düzenlemelerde yer alan kişisel veri tanımları da aynı paralelde; 'Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi' olarak

[77] http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5c631746ccdb86.53347818 Erişim tarihi: 12.02.2019

[78] Usta ve Doğantekin, s.29.

yer almaktadır.[79] Bu anlamda şirketlere veya makinalara ait veriler kişisel veri sayılmamakta ve GDPR koruma alanına girmemektedir. Fakat gerçek kişilere gelindiğinde, veri kapsamı oldukça genişlemektedir[80]. Bunun nedeni, potansiyel olarak tanımlanabilir gerçek kişi kavramının, hem KVKK hem de GDPR kapsamında sadece açıkça görünen veriler için kullanılmıyor olmasıdır. Bir başka deyişle, bir veri ilk bakışta anlamsız olsa ve kişisel veri olarak görülmese dahi, eğer diğer veriler ile birleştiğinde bir gerçek kişiyi tanınabilir veya adreslenebilir kılıyor ise o veri de kişisel veri olarak KVKK veya GDPR kapsamında değerlendirilmektedir.

KVKK gerekçesinde ise klasik tanıma ek olarak; '*sadece bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgiler de kişisel veridir. Bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade eder. Yani verilerin; kişinin fiziksel, ekonomik, kültürel, sosyal veya psikolojik kimliğini ifade eden somut bir içerik taşıması veya kimlik, vergi, sigorta numarası gibi herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm halleri kapsar. İsim, telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler gibi veriler dolaylı da olsa kişiyi belirlenebilir kılabilme özellikleri nedeniyle kişisel verilerdir.'* ifadesiyle herhangi bir kayıt aracılığıyla kişinin adreslenebilirliğini sağlayan her türlü veriyi kişisel veri olarak değerlendirmiştir.[81]

Örnek vermek gerekirse, bir e-ticaret satıcısının satış işlemlerini gerçekleştirmek için talep ettiği ad, soyad, adres, e-posta adresi ve kredi kartı numarası açıkça kişisel veri kapsamına girmektedir. Ancak aynı satıcıdan mağazanın web sayfası üzerinden nakit para ile satın alınan ve bilgisayara yüklenen indirim kuponunun fiziki mağazada kullanılması durumunda o kupon numarası da kişisel veri olarak

[79] Kişisel Verilerin Korunması Kanunu m.3 hükmü uyarınca yapılan kişisel veri tanımıdır. Avrupa Birliği Veri Koruma Regülasyonu (GDPR) tarafından kişisel veri tanımında işaret edilen gerçek kişinin de ayrıca tanımı yapılmıştır. 'Tanımlanabilir bir gerçek kişi, doğrudan veya dolaylı olarak, özellikle bir ad, bir kimlik numarası, konum verisi, bu gerçek kişinin genetik, zihinsel, ekonomik, kültürel veya sosyal kimliği; bir çevrimiçi tanımlayıcı gibi bir tanımlayıcıya veya fiziksel, fizyolojik özelliklere özgü bir veya daha fazla faktöre atıfta bulunularak tanımlanabilen bir kişidir' şeklinde ifade edilmiştir.

[80] Blockchain and the GDPR (Thematic Report), s.10.

[81] https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim tarihi: 01.07.2019

sayılabilmektedir. Çünkü belirtilen kupon numarasının e-posta adresi veya kredi kartı numarasıyla olan bağlantısı sayesinde satıcı alıcıya ulaşabilir kılınmaktadır.[82]

Veri sahibi (ilgili kişi); tanım olarak KVKK'da 'ilgili kişi' olarak addedilmektedir. KVKK m.3/1-ç bendinde ilgili kişi, 'kişisel verisi işlenen gerçek kişi' olarak tanımlanmaktadır. GDPR içerisinde ise 'veri' tanımı esnasında kimliği belirli veya belirlenebilir 'gerçek kişi' aynı zamanda veri sahibi olarak tanımlanmaktadır. Bu anlamda hakkın öznesi olan ilgili kişinin sadece gerçek kişiden olabildiği, tüzel kişilerin hem Kanun hem Tüzük kapsamında da değerlendirilmediği görülmektedir. He ne kadar bir önceki KVKK Tasarısı'nda tüzel kişiler de bu kapsama alınmışsa da yürürlüğe giren KVKK'da kapsam daraltılarak sadece gerçek kişilerin verilerine yönelik bir düzenleme yapılmıştır. Bunun yanı sıra, Anayasa'nın m.20/3 hükmünde yer alan 'herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir'[83] ibaresindeki 'herkes' ibaresinin kapsamına gerçek ve tüzel kişilerin alındığına dair Anayasa Mahkemesi kararı mevcuttur. İlgili kararda '*Her ne kadar Anayasa'nın 20. maddesinde daha ziyade gerçek kişilerin özel hayatı ve bu bağlamda gerçek kişilere ilişkin kişisel verilerin korunma altında bulundurulduğu ileri sürülebilir ise de madde metninde kişisel verilerle ilgili olarak "herkes" tabirinin kullanılması dikkate alındığında, tüzel kişilere ilişkin verilerin de 20. madde kapsamında değerlendirilmesi gerekeceği açıktır.'* yorumu yapılmıştır.[84]

Veri sahibi sıfatının tüzel kişileri de kapsaması hususu irdelendiğinde, esasında özel hayatın gizliliği başta olmak üzere temel hak ve özgürlük olarak değerlendirilen "*kişisel verilerin korunması hakk"*nın sadece gerçek kişilere ilişkin olması gerekmektedir. Tüzel kişilerin de bu kapsamda değerlendirilmesi, kişisel verilerin korunmasının esasına aykırı olacağı gibi korumanın zayıflamasına da neden olabilecektir. Öyle ki, her tüzel kişinin kuruluşunda bir gayesinin bulunması ve etkinliklerinin de bu hedef doğrultusunda gerçekleştiği, haliyle temel kaygılarının da sadece bu amaç ile ilgili olduğu aşikardır. Ancak kişisel verilerin korunması hakkı insan olmakla kazanılan bir temel haktır ve bu kapsamdaki düzenlemelerinin tek öznesinin

[82] Blockchain and the GDPR (Thematic Report), s.11.

[83] Fıkranın tam hali; 'm.20/3: Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.' şeklindedir.

[84] https://www.anayasa.gov.tr/media/4912/kararlar_dergisi_52_5.pdf Erişim tarihi:01.07.2019

gerçek kişi olması gerekmektedir. Bunun yanı sıra, tüzel kişilerin sahip olduğu gizli veriler, hukuk düzenimize göre 'ticari sır' kapsamında değerlendirilmektedir.[85] Kaldı ki ticari sır olgusu, Türk Ceza Kanunu, Bilgi Edinme Kanunu gibi genel ve özel nitelikteki kanunlar tarafından koruma altına alınmıştır.[86]

KVKK ve GDPR bağlamında yükümlülükleri açısından en büyük önem atfedilenler ise veri sorumlusu ile veri işleyendir. Veri sorumlusu;[87] kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen tek başına veya başkalarıyla birlikte 'gerçek veya tüzel kişi, kamu otoritesi, ajansı veya başka bir kurum' olarak tanımlanır. KVKK ve GDPR'a nezdinde veri sorumlusuna 'merkezi' bir sorumluluk yüklenmiştir. Bu anlamda veri üzerinde hakimiyetini kurabilen gerçek (çalışan, müşteri, tedarikçi) ya da tüzel (kamu kurum veya kuruluşları, ticari şirketler) kişiler veri sorumlusu olacaktır.

Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirilen faaliyetler kapsamında kendileri "veri sorumlusu" olup ilgili düzenlemelerde belirtilen hukuki sorumluluk tüzel kişinin şahsında doğmaktadır. Söz gelimi veri işleme faaliyeti gerçekleştiren şirketteki çalışanın belgeleri tek başına teslim alması ve kayıtları yapıyor olması halinde dahi veri sorumlusu çalışan değil tüzel kişilik olacaktır. Bu konuda kamu hukuku ile özel hukuk tüzel kişileri bakımından herhangi bir farklılık gözetilmemektedir. Bunun yanı sıra bir tüzel kişiliğin bünyesindeki birimlerin ayrı ayrı tüzel kişiliği olmadığında, sadece tek bir birim veri işleme faaliyeti gerçekleştiriyor olsa dahi birim olarak veri sorumlusu olmayacaktır. Ancak bir şirketler topluluğundan

---

[85] Elif Küzeci, **Kişisel Verilerin Korunması,** Ankara 2019, 3. Baskı, s.317.

[86] 'Ticari sırrın korunmasına yönelik' ilgili kanun maddeleri şu şekildedir;

Türk Ceza Kanunu; Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması **Madde 239-** (1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi halinde de bu fıkraya göre cezaya hükmolunur.

(2) Birinci fıkra hükümleri, fenni keşif ve buluşları veya sınai uygulamaya ilişkin bilgiler hakkında da uygulanır.

(3) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu halde şikayet koşulu aranmaz.

(4) Cebir veya tehdit kullanarak bir kimseyi bu madde kapsamına giren bilgi veya belgeleri açıklamaya mecbur kılan kişi, üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır.

Bilgi Edinme Kanunu; Ticari sır (Ceza hükümleri)

Madde 23- Kanunlarda ticari sır olarak nitelenen bilgi veya belgeler ile, kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticari ve mali bilgiler, bu Kanun kapsamı dışındadır.

[87] KVKK'ya göre veri sorumlusu olarak anılan hukuk kişiliği, GDPR tanımlarında 'data controller' yani veri denetleyicisi olarak yer almaktadır. Yükümlülük ve haklar anlamında bir farklılık olmadığı için KVKK literatüründeki hali ile kullanılmıştır.

bahsedildiğinde her bir şirketin kendi tüzel kişiliği mevcut olacağından bu şirketlerin her biri veri sorumlusu ve/veya veri işleyen olarak tanımlanabilecektir.[88]

Veri sorumlusunun sorumluluk alanının kapsamına bakıldığında, gerek KVKK'da ve gerekse GDPR'da verinin yasal düzenlemeler çerçevesinde güvenli bir şekilde işlenmesi/aktarılması için gerekli tüm organizasyonu yapması, teknik ve idari tedbirleri kendi iç organizasyonunda alması ve aktarım yapılacak ise verilerin aktarılacağı veri işleyenin de aynı teknik ve idari tedbirleri sağladığından emin olması beklenmektedir.

Bunun yanı sıra veri sahibinden kişisel verilerini temin ederken yeterli bilgilendirmeyi sunması ve süreç içerisinde de veri sahibinin kişisel verilerine yönelik taleplerine en geç 30 gün içinde cevap verebilmesi gerekmektedir. Ayrıca veri sorumluları siciline kayıt yükümlülüğü ve KVKK ve GDPR'da öngörülen suç ve kabahatler de yine öncelikli olarak veri sorumluları için geçerli olacaktır.

Veri işleyen ise KVKK m.3/1-ğ hükmüne göre; 'Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi' olarak tanımlanmış iken;

GDPR'da 'İşleyici: kontrolör adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır; kişisel verileri veri sorumlusu yerine de işleyebilen kişiliklerdir' şeklinde anlatım bulmuştur. İki tanım arasındaki tek farklılığın GDPR'da veri işleyenin kamu kuruluşu/kurumu da olabileceğinin ayrıca vurgulanmış olmasıdır. Ancak KVKK nezdinde tüzel kişi kapsamına hem özel hem tüzel kişilik alınmış olduğu için uygulamada bir farklılık yaratmamaktadır.

Veri sorumlusunun sistemi nasıl tasarladığına bağlı olarak, bir veri sorumlusunun aynı zamanda veri işleyen olduğu, veya birçok veri işleyen olabileceği gibi sistemde veri sorumlusu haricinde veri işleyenin bulunmadığı durumlar da

[88]Kişisel Verilerin Korunması Kurumu, 'Veri Sorumlusu ve Veri İşleyen' Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf Erişim tarihi: 19.07.2019

görülebilecektir.[89] Bunun yanı sıra, veri işleyenler her ne kadar verileri kendileri işliyor olsalar da bu işlemi veri sorumlusu adına yaptıkları gerekçesiyle, veri sorumlusunun da bu noktada sorumluluğu doğmaktadır.

Kanunda/Tüzükte yer alan sorumluluk hükümleri açısından veri sorumlusu ile veri işleyenin birbirinden ayırt edilmesi önem arz etmektedir. Bir veri işleme faaliyetinde veri sorumlusu ile veri işleyicisinin tespit edilmesi, Kanunun/Tüzüğün uygulanmasında önemli bir rol oynamaktadır. Çünkü veri koruma kurallarına uyulmasından kimin sorumlu olacağı, veri sahiplerinin haklarını nasıl kullanabileceği bu tespite göre belirlenecektir.[90]

Öyle ki, veri sorumlusu Kanundaki/Tüzükteki pek çok yükümlülüğün doğrudan muhatabı iken, veri işleyen daha dar bir alandan sorumlu tutulmuştur. Ayrıca, kişisel verilerin veri sorumlusu adına veri işleyen tarafından işlenmesi, veri sorumlusunun sorumluluğunu kaldırmamakta, aksine müteselsil sorumluluk yüklemektedir.[91]

Veri sorumlusu ile veri işleyenin tespitinde ayırt edici nokta ise tanımlardan da anlaşılacağı üzere 'verilen yetkiye dayanarak' ve 'başkası adına' veri işleme faaliyetinin gerçekleştirilmesidir. Veri koruma hukukunun genel kabulü ise, veri işleyenin veri sorumlusu tarafından verilen talimatlar doğrultusunda veri işlediği yönündedir. Bu noktada önem arz eden husus toplanacak verilerin türleri, bu verilerin işleme amacının ne olduğu, verilerin saklanma süreleri, verilerin toplanma ve işleme araçları, verileri toplanacak olan veri sahiplerinin belirlenmesi, toplanan verilerin aktarılma durumu ve kime aktarılacağı hususlarının veri sorumlusu tarafından belirlenmiş olmasıdır. Veri işleyenin bu faaliyete ilişkin karar verebileceği konular ise verilerin toplanması aşamasında hangi araçların kullanılacağı, toplanan verilerin hangi metodla saklanacağı ve bu verilere ilişkin alınacak güvenlik önlemleri, saklama sürelerine ilişkin doğru uygulamanın yapılması, aktarım yapılacak ise aktarım araçları, verilerin

[89] Kişisel Verilerin Korunması Kurumu tarafından yayınlanan 'Veri Sorumlusu ve Veri İşleyen' rehberinde, her iki kavramın hem gerçek hem tüzel kişiler için geçerli olduğu, söz gelimi bir mali müşavirlik firmasında serbest çalışanın da firmanın da hem veri sorumlusu hem de veri işleyen olabileceği, veya bulut bilişim hizmeti sunan bir şirketin, çalışanlarına ait verilerde 'veri sorumlusu', müşterilerine ait verilerde ise 'veri işleyen' olabileceği belirtilmiştir.

[90] European Data Protection Board, **Opinion 1/2010 on the concepts of 'Controller' and 'Processor',** WP 169, 2010, s.31.

[91] Çekin, s.41.

silinmesi/anonimleştirilmesi veya yok edilmesi eylemleri için kullanılacak yöntemlerin belirlenmesi hususlarıdır.[92]

GDPR nezdinde de; kişisel verilerin işlenmesine dair araç ve yöntemler ile işlenme amacının tespiti konusundaki yetkinlik ve yukarıda yer verilen diğer unsurların belirlenmesi; veri sorumlusu sıfatını etkileyebilecek bir koşul olarak ifade edilmektedir. Amaç ve araçların tespitinde yetkinlik ise hem hukuken hem fiilen değerlendirilmeli ve şekli bir yaklaşımdan kaçınılarak somut olaya göre konular üzerinde en çok söz hakkına sahip gerçek/tüzel kişinin tespiti yapılmalıdır. Bu noktada taraflar arasındaki sözleşme hükümleri hukuken sorumluluğun tespiti açısından kullanılabilecek iken, taraflar arasındaki bağımlılık ilişkisi de fiili durumun tespit edilmesi açısından yardımcı olabilecektir. Başka bir deyişle, kişinin veri işleme faaliyetlerinden sağladığı fayda ne kadar yüksek ise kişinin sorumluluk oranının da o kadar yüksek olması gerekecektir.

Ancak bu ana kriterlerin yanında, veri sorumlusu tarafından verilen önceki talimatların seviyesi, hizmet seviyesinin veri sorumlusu tarafından takip edilip edilmediği, taraflar arasındaki anlaşmalar uyarınca özerk karar verme yetkilerinin sınırları gibi unsurlar da veri sorumlusu – veri işleyen tespitinin yapılmasında kıstas olarak alınabilecektir.[93]

Kanunda/Tüzükte ve rehberlerde ‘veri işleme amacı’ olarak yer alan bu unsurun somutlaştırılması için ‘veri işleme faaliyetinin sonunda nasıl bir sonuç istendiğinin tespiti’ şeklinde ifade edilebilecektir. Aynı şekilde ‘veri işleme aracı’ ise işleme faaliyetinde kullanılacak teknik hususların, organizasyonel yapının, işleme faaliyetinin kapsamının ve kategorilerin, bunun yanı sıra üçüncü kişilerin erişim imkanlarının belirlenmesini işaret etmektedir.[94]

Veri tabanı; bilgisayarlar tarafından verilerin hızlı aranabilmesi ve veriye erişim için özel olarak düzenlenmiş herhangi bir veri veya bilgi tabanı olarak tanımlanmıştır. Veri tabanları, farklı veri işleme teknikleriyle birlikte verilerin

[92] Kişisel Verilerin Korunması Kurumu, Veri Sorumlusu ve Veri İşleyen, s.3-4.
[93] Article 29 EDPB, s.32.
[94] Çekin, s.42.

alınmasını, saklanmasını, değiştirilmesini ve silinmesini kolaylaştırmak amacıyla hazırlanmaktadır.[95]

Belirtilmelidir ki; KVKK ve GDPR öncelikli olarak tüketicilere kişisel verilerini ve şirketlerin bunları nasıl toplayıp kullandıklarını kontrol etme hakkı vermek üzere tasarlanmıştır. Bir başka deyişle Kanun'da ve Tüzük'te tüketicilere kişisel verilerini kontrol etme hakkı verilirken, aynı zamanda tüketicilerin çıkarlarının veri sorumlusu veya kamunun çıkarları karşısında korunmasının farkındalığı da açıkça dikkat çekmektedir.[96]

C. Blok Zincir Teknolojisinde Kişisel Veri

Kişisel veri tanımının *'B.Temel Kavramlar'* bölümünde yapılmış olması sebebiyle bu bölümde doğrudan blok zincir teknolojisinde yer alan bilgilerin kişisel veri niteliğinde olup olmadığı tartışılacaktır.

Blok zincir sisteminde bloklarda yer alan veriler hashing yöntemiyle şifrelenmekte ve dönüştürülmektedir. Bu sayede hiçbir blokta doğrudan gerçek kişiye ait bir kişisel verinin yer alma imkanı bulunmamaktadır. Şayet hashing yoluyla şifrelendikten sonra verinin son hali sadece rakam ve harflerden ibaret anlamsız bir dizi haline gelmektedir.

KVKK ve GDPR'de yer verilen kişisel veri tanımlarına göre ise; kimliği belirli veya belirlenebilir gerçek kişiye ait her türlü veri kişisel veri sayılmaktadır. Hashing yöntemi ile şifrelenen verilerin doğrudan kişisel veri içermemesi nedeniyle bu noktada adreslenebilirlik olgusunun araştırılması gerekmektedir. Elde edilen verilerin bir gerçek kişiyi adreslemesinin tespitinde ise mutlak ve nispi belirlenebilirlik görüşlerinin incelenmesinde fayda olacaktır.

---

[95] https://www.britannica.com/technology/database Erişim tarihi: 01.02.2019

[96] Lee Jim, **GDPR & Blockchain: At the intersection of data privacy and technology,** BDP International https://www.bdpinternational.com/blog/gdpr-blockchain-at-the-intersection-of-data-privacy-and-technology Erişim tarihi: 20.07.2019

1.Mutlak ve Nispi Belirlenebilirlik Olgusu

Mutlak ve nisbi belirlenebilirlik olguları Avrupa Adalet Divanı'nın Scarlet ve Breyer kararları ile ortaya çıkmıştır. Mutlak belirlenebilirlik; veri sorumlusunun kimliği ve veriyi işleme amacından bağımsız olarak, veri sahibinin belirlenmesi için gerekli bilgilerin -bu bilgiler üçüncü kişinin hakimiyetinde olsa dahi- veri sorumlusunun da erişiminde olduğunu kabul eden görüştür. Nisbi görüşe göre ise sadece veri işleyenin kimlik ve bilgisi esas alınmaktadır.

Divan'ın *Scarlet* kararında[97] SABAM adlı bir sanat derneği, Scarlet adındaki internet servis sağlayıcısını, eşler arası bir yazılım kullanılarak telifsiz olan eserlerin indirilmesine aracılık ettiği gerekçesiyle dava etmiştir. Yargılama esnasında kullanıcıların verilerinin düzenli bir şekilde takip edilebilmesi ve denetlenmesi amacıyla bir filtre sisteminin kurulması gündeme gelmiş ise de; belirtilen filtre sisteminin kurulmasının fikri mülkiyet ile kişisel verilerin korunması arasında optimal bir dengenin sağlanmasını engelleyeceği ve orantısız olacağına karar verilerek reddedilmiştir. Scarlet kararında filtre sisteminin kurulmasında gündeme gelen ISP'lerin (internet service provider) kişisel veri niteliğinde olduğuna karar verilmiştir.

Divan'ın *Breyer* kararında ise dinamik IP adreslerinin kişisel veri sayılıp sayılmaması hususu gündeme gelmiş olup bu kararda Divan tarafından 'dinamik IP adresine sahip kişinin, makul imkanlar ölçüsünde internet erişim sağlayıcıları aracılığıyla gerçek kişiye erişimin mümkün olduğu gerekçesiyle dinamik IP'nin kişisel veri olduğuna hükmetmiştir.[98]

Belirtilen kararlar ışığında belirlenebilirlik/adreslenebilirlik olgusunun netleştirilmesi adına blok zincir ağında da kamusal/özel blok zincir ayrımının tartışılması gerekmektedir. Eğer blok zincir ağında katılım için öncelikle bir kayıt gerekiyor ya da kamuya açık olmasına karşılık kişiye özel anahtarlar belirli kişi/kuruluşlar tarafından veriliyorsa bu tahsis eden kişi/kuruluşların da gerçek kişiyi belirleyebileceği aşikardır. Diğer taraftan, blok zincirin kamusal olması da kullanıcıların

[97] Judgment of 24.11.2011, Scarlet Extended SA, C-70/10, EU:C:2011:771, p:15,16,17 http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4413010 Erişim tarihi:20.07.2019

[98] Judgment of 19.10.2016, Breyer, C-582/14, EU:C:2016:779, p:65 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582&from=EN Erişim tarihi:20.07.2019

belirlenebilirliği olgusunu tam anlamıyla ortadan kaldırmamaktadır. Söz gelimi kamuya açık anahtarın kullanımı halinde de big data analiz desteği alınarak ve kişi farklı analizler ile odak yapıldığında belirlenebilmektedir.[99]

Belirlenebilirlik olgusu açısından önem taşıyan big data (büyük veri) uygulamalarından kısaca bahsedilmesinde fayda olacaktır. '*Büyük veri'* terimi, insanlardan, makinelerden, sensörlerden elde edilmiş çok çeşitli ve büyük miktardaki farklı veri türlerini içermektedir. Bu veriler iklim bilgileri, uydu görüntüleri, dijital resimler ve videolar, geçiş kayıtları veya GPS sinyalleri olabileceği gibi; kişisel verileri de içerebilmektedir. Bu anlamda bir gerçek kişiye ait her türlü bilgi de büyük veri teriminin kapsamına girmektedir.[100] Büyük veri uygulamaları ise, farklı kanallardan temin edilen her türlü verinin analiz edilerek anlamlı hale getirilmesini hedefleyen uygulamalardır. Bu uygulamalar sayesinde, yüksek hacimdeki verinin hızlı ve etkili şekilde ayrıştırılması ve her sektörde kişiye yönelik pazarlama, iş geliştirme alanlarında faydalanılması amaçlanmaktadır.

Netice itibarıyla özel blok zincirde kullanıcıların sisteme kabulleri aşamasında merkezi bir gerçek/tüzel kişi mevcut ise bu kabulü veren kişi tarafından kullanıcının belirlenebilirliği olgusu tartışmasızdır. Diğer yandan kamusal blok zincir ağlarında bu tür bir kabul süreci yer almadığı için kullanıcının belirlenebilirliği büyük veri uygulamaları ile imkan dahilinde olmakla beraber, her blok zincir ağında kişisel verinin varlığına dair kesin bir sonuca varılamamaktadır. Netice itibarıyla blok zincirdeki kişisel veri kavramının her somut olaya göre yorumlanmasının en doğru olacağı düşünülmektedir.

D. Blok Zincir Teknolojisinde Veri Sorumlusu

Çalışmamızın bu bölümünde *'B. Temel Kavramlar'* kısmında yer verilen veri sorumlusu ve veri işleyen tanımlarına ek olarak, Veri Koruma Hukuku bağlamında kamusal ve özel blok zincirde sorunsal olarak karşımıza çıkan veri sorumlusunun tespiti

[99] 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(1) İstanbul Hukuk Mecmuası 315 h ps://doi.org/10.26650/mecmua.2019.77.1.0012 , s.16

[100] European Commission, The EU Data Protection and Big Data Factsheet, 2016 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi3x-f8lezkAhXMpYsKHQyZD38QFjAAegQIBBAC&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D41523&usg=AOvVaw0ST2KcGgcpQzrQ8t4JTG3F Erişim tarihi: 20.07.2019

incelenecektir. 6698 sayılı Kişisel Verilerin Korunması Kanunu m.3/I-ı bendi uyarınca *'Veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi '*, 4.5.201 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'ne göre ise '*kontrolör, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organı'* ifade etmektedir. Bölümün devamında detaylı olarak değinileceği üzere, gerek Kanun'da ve gerekse Tüzük'te yer verilen veri sorumlusu tanımlarında verilerin işlenmesindeki yetkinliği ve kontrol gücünün ön plana çıktığı anlaşılmaktadır. Bu çerçevede, özel blok zincirde ve kamusal blok zincirde verilerin işlenme süreçlerinde belirtilen yetkinliğe sahip bir merkezin bulunup bulunmadığının tespiti önem taşıyacaktır. Akabinde Kanun'da yer almayan ancak Tüzük'te tanınan bir veri sorumlusu türü olarak müşterek veri sorumlusu kavramı irdelenecek ve bahsedilen unsurlar eşliğinde blok zincirlerde veri sorumlusu tespit edilmeye çalışılacaktır.

1. Veri Sorumlusu

Veri sorumlusu, veri sahiplerinin haklarını kullanmaya yöneldiği ve kurallara uyulmadığı takdirde uyum ve sorumluluktan sorumlu olan kişiliktir. Bunun yanı sıra, veri işleme sürecinin mimarı ve hesap verilebilirliği noktasında kilit roldedir. KVKK ve GDPR için de veri sorumlusunun tespit edilebilir olması beklenmektedir. Aşağıda detaylı olarak anlatılacağı üzere, Blockchain teknolojisinde ise bu tespitin yapılması her zaman kolay olmamaktadır.[101]

KVKK ve GDPR'de yer alan veri sorumlusu[102] ve veri koruma hukuku çerçevesindeki diğer rollerin tanımları kesin hatlarıyla ve merkezi veri işleme modeli baz alınarak yapılmaktadır. Söz gelimi bir tüketicinin internet üzerinden alışveriş yapması halinde satıcıya ad-soyad, adres ve banka bilgileri gibi verileri iletilmektedir. Tüketici bu esnada bir defaya mahsus veya daha fazla işlemde verilerinin işlenmesine bir onay kutucuğu aracılığıyla izin verebilmektedir.

[101] Blockchain and the GDPR (Thematic Report), s.11.

[102] KVKK'ya göre veri sorumlusu olarak anılan hukuk kişiliği, GDPR tanımlarında 'data controller' yani veri denetleyicisi olarak yer almaktadır. Yükümlülük ve haklar anlamında bir farklılık olmadığı için KVKK literatüründeki hali ile kullanılmıştır.

Bu durumda tüketicinin, kişisel verilerinin satıcı tarafından hangi yollarla ve hangi amaçlarla işleneceğini daha ayrıntılı olarak bilmemesine neden olunabilmektedir. Yukarıdaki e-ticaret örneğine göre satıcı veri sorumlusu ve müşteri veri sahibi (veri öznesi)'dir. Bununla birlikte, tüketicinin kişisel verilerini satıcı adına işleyen veri işleyiciler (veri işlemciler) de olabilecektir.

Ancak veri sorumlusunun tanımı hem KVKK hem GDPR açısından irdelendiğinde, blok zincir teknolojisinde veri sorumlusunun tespitinin somut olaya göre irdelenmesi gerektiği düşünülmektedir. Öyle ki, tüm tanımların *merkezi* bir veri sorumlusuna göre yapıldığı bir hukuk düzeninde; tüm verilerin merkezi olmayan bir sistemde dağıtık halde bulunduğu gerçeğine göre veri sorumlusunun tespiti gerekmekte ve özellikle kamusal blok zincirde mümkün olmamaktadır. Bir başka deyişle, bu ortamda kişisel verilerin işlenmesinin amaç ve araçlarını tek elden belirleyen tek bir kişi veya kuruluş bulunmamaktadır. Çalışmamızın devamında detaylı olarak anlatılacak olan kamusal blok zincirdeki ögelerin hiç biri için, tam olarak veri işlenmesindeki amaç veya araç üzerinde tam bir kontrolünün/yetkinliğinin bulunduğu söylenemeyecektir. Özel blok zincirlerde ise bu tür bir blok zincirin yöneticisi ağa erişim izni vermektedir ve bu sayede KVKK ve GDPR tarafından aranan 'kişisel verilerin işlenmesine yönelik amaçların ve araçların belirlenmesi' koşulu da sağlanmaktadır.[103]

2.Müşterek Veri Sorumlusu

Bu bölümde, veri sorumlusunun tespitine dair *'B.Temel Kavramlar'* bölümünde ve aynı zamanda KVKK'da yer almayan 'müşterek veri sorumlusu' kavramına değinilecektir. Müşterek veri sorumlusu müessesesinin şart ve sonuçları sadece GDPR m.26'da anlatım bulmuştur.

Müşterek veri sorumlusu, birden çok kişinin bir araya gelerek veri işleme eylemine yönelik araç ve amaçların belirlenmesinde söz sahibi olması durumunda gündeme gelmektedir. Bu durumda belirleyici taraflar arasındaki sözleşme kapsamında, GDPR tarafından yüklenen sorumlulukların hangi kısımlarının kime ait olacağına dair belirlemelerin yapılması önem taşımaktadır. Ancak belirtilmelidir ki, müşterek veri sorumluları arasında akdedilecek bu tür bir sözleşme, sadece kendi aralarındaki

[103] Kaufmann, s.124.

sorumluluğa ilişkin olabilecektir. Her ne kadar GDPR m.26/2 uyarınca belirlenen sorumluluk alanları, veri sahiplerine bildirilecek olsa da; yapılan bu sözleşmenin veri sahibinin başvuru haklarında yöneleceği taraf konusunda bir değişiklik yapmadığı da yine aynı maddenin 3. fıkrasında ifade edilmiştir. Bir başka deyişle, müşterek veri sorumlularının aralarında yaptıkları sözleşme, dış dünyaya yönelik sorumluluklarında bir değişiklik yaratmamakta, GDPR nezdinde hepsi tam sorumlu olarak değerlendirilmektedir.[104]

Müşterek veri sorumlusu tespit edilirken, uygulamada tüm veri sorumlularının tek bir işleme eşit düzeyde yetkin oldukları ve işlemden eşit düzeyde sorumlu oldukları durumlara çok ender rastlanılacağı öngörülebilmektedir. Yetkinliğin orantısız şekilde paylaşıldığı durumlarda farklı ihtimaller gündeme geleceği gibi, yetkinliğin veri sorumluları arasında aynı anda veya farklı aşamalarda paylaşılması durumu dahi uygulamada karşılaşılabilecek durumlar arasındadır. Çalışmamızın devamında örnekler üzerinden veri sorumlusunun tespitinde kullanılan kriterlere yer verilecektir.

3. Veri Sorumlusunun Tespiti

Çalışmamızın bu bölümünde, daha önceki kısımlarda izah edilen müşterek veri sorumlusu ve veri sorumlusunun tespiti konularının somutlaştırılması adına örnekler üzerinden kriter değerlendirmesi yapılacaktır. Söz gelimi; bir bina sahibinin, bir güvenlik şirketi ile akdettiği sözleşme uyarınca, güvenlik şirketi, veri sorumlusu olan bina sahibi adına binanın çeşitli yerlerine bazı kameralar kurduğunda, video gözetiminin amaçları ve görüntülerin toplanma ve saklanma şekli sadece binanın sahibi tarafından belirleniyorsa bu işlem için tek veri sorumlusu bina sahibi olarak değerlendirilmektedir.

Şayet bir insan kaynakları firmasının başka bir şirkete personel alımı konusunda yardımcı olması durumunda ise, eğer adayların verileri üzerinde sadece şirket adına hareket edeceğini belirtmiş ise personel alımı yapacak olan şirketin buradaki tek veri sorumlusu olacağı değerlendirilmektedir.

[104] Çekin, s.43.

Ancak aynı örnekte insan kaynakları firması, kendi veri tabanında bulunan özgeçmişler ile alım yapmak isteyen şirkete gelen özgeçmişler arasından bir değerlendirme yaparak uygun adaylar aramakta ise; aralarındaki sözleşme uyarınca imzalanan her iş sözleşmesine göre ücret alıyorsa menfaat olgusu da devreye girmekte ve insan kaynakları firması ile alım yapacak olan şirket ortak veri sorumlusu olarak değerlendirilecektir.[105]

Avrupa Adalet Divanı tarafından benzer konularda verilen kararlara bakıldığında ise; Facebook adlı sosyal paylaşım sitesinde bir Fanpage işleticisinin veri analizindeki parametreleri belirleme imkanını baz alarak Fanpage işleticisinin müşterek veri sorumlusu olduğuna hükmetmiştir.[106] Davaya konu olayda Wirtschaftsakademie Schleswig-Holstein GmbH tarafından yönetilen bir *Facebook Fanpage* sayfasında, Facebook tarafından düzenli olarak veri analizi yapılmaktadır. Bu veri analizi, ilgili siteyi ziyaret edenlerin yaş, ülke, cinsiyet gibi verilerinden oluşmakta ve anonimleştirilerek sayfa yöneticisine iletilmektedir. Bahse konu veriler sayesinde sayfa yöneticisi pazarlama ve reklam stratejilerini belirlemekte/değiştirmektedir. Divan'ın bu karardaki değerlendirmeleri; sayfayı yöneten kişinin, bu verileri analiz eden ve ileten platform işleticisiyle ortak veri sorumlusu olduğu yönündedir. Buradaki sorumluluğun sınırı ise Facebook'un sadece bu sayfa için işlediği verilerdir. Belirtilen sorumluluğun sebebi ise, yapılan veri analizlerindeki parametrelerin -yaş, ülke, cinsiyet vb.- sayfa yöneticisi tarafından belirlenmiş olması olarak gösterilmiştir. Sayfa yöneticisinin belirlediği kriterler doğrultusunda analizin yapılıyor olması, veri sorumluluğunda koşul olarak öngörülen 'kişisel verilerin işlenme amaç ve araçlarının belirlenmesi' olarak kabul edilmiş ve Facebook ile Fanpage yöneticisinin müşterek veri sorumlusu olduklarına hükmedilmiştir.

Divan tarafından yapılan bir diğer veri sorumlusu tespiti ise *Fashion ID/ Verbraucherzentrale NRW e.V* dosyasında görülmektedir. Bahse konu karar, Fashion ID tarafından kendi web sitelerine Facebook ile entegre bir beğen linkinin eklenmesi ve bu

[105] Article 29 DPWP, s.21.

[106]Judgment of 05.06.2018, ULD Schleswig Holstein/Wirtschaftsakademie Schleswig Holstein GmbH C-210/16, EU:C:2018:388,p:37, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4399480 Erişim tarihi: 19.07.2019

linke tıklayan her kullanıcının IP adresi, browser ve çerez bilgilerinin otomatik olarak Facebook'a iletilmesi hakkındadır. [107]

Adı geçen kararda web sayfası sahibi ile Facebook'un müşterek veri sorumlusu olduğuna, Fashion ID her ne kadar veri analizine ilişkin parametreleri belirlemiyor olsa da, sayfasına koyduğu beğen tuşu aracılığıyla kişisel verilerin işlenmesine izin vermekte ve bu sayede reklamını da yaparak ekonomik menfaat elde ettiği gerekçesiyle Fashion ID'nin müşterek veri sorumlusu olduğuna kanaat getirilmektedir.

Bahsedilen her iki kararda da ekonomik menfaat elde edilmesinin veri sorumlusunun tespitinde rol oynadığı görülmektedir. Her ne kadar KVKK ve GDPR'da veri sorumlusunun tespitine yönelik hükümlerde bu unsura değinilmemiş ise de içtihatlar ile ekonomik menfaat unsurunun da belirlemelerde yön vereceği açıklık kazanmaktadır.

Divan tarafından veri sorumlusuna ilişkin olarak verilen bir diğer karar ise dini bir yapılanmadaki faaliyetleri konu edinmektedir.[108] *Yehova Şahitleri* adındaki bu dini yapının gönüllüleri, kapı kapı dolaşarak misyonerlik faaliyetlerini yürütmektedir. Bu faaliyet esnasında tanıştıkları her kişinin ad, soyad, adres vb. kişisel verileri bu gönüllüler tarafından kayıt altına alınmakta ancak paylaşılmamakta, sadece bir daha rahatsız edilmek istemeyenlerin listesi merkezi idareleri ile paylaşılmaktadır. Divan kararında ise merkezi idarenin bu kadar geri planda kaldığı reddedilerek, dini yapının mevcut faaliyetinin merkezi idare tarafından koordine edildiği ve gönüllülerin faaliyetleri konusunda teşvik edildiği, böylece elde edilen kişisel verilerin işlenme amaç ve araçlarının merkezi idare tarafından belirlendiğine ve merkezi idarenin müşterek veri sorumlusu olduğuna hükmedilmiştir.

Netice itibarıyla veri sorumlusunun tespit edilmesi noktasında, verinin işlenme amacının kim tarafından belirlendiği, işlenecek olan verilerin işlenme yöntemleri, işlenen verilerin saklanma yöntemleri gibi unsurlarda yetkin kişinin kim olduğu önem

[107]Judgment of 19.12.2018, Fashion ID/ Verbraucherzentrale NRW e.V., C-40/17, EU:C:2019:629, p:26. http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4401670 Erişim tarihi: 19.07.2019

[108]Judgment of 10.07.2018, Jehovan todistajat, C-25/17, EU:C:2018:551, p:15. http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4403193 Erişim tarihi: 20.07.2019

taşımaktadır. Ancak bunun yanı sıra, belirlemelere eşlik eden bir ekonomik menfaatin de bulunması da veri sorumlusunun tespitinde dengeleri değiştirebilmektedir. Çalışmamızın devamında ise blok zinciri sisteminde en yetkin ögenin bulunabilmesi adına sisteme dahil olan farklı kategorilerdeki oyuncu grupları irdelenecektir.

4.Blok Zinciri ve Sistem Oyuncuları

Veri koruma hukuku, temelinde kişisel verilerin işlenmesinin arkasında her zaman bir veri sorumlusu olduğu varsayımına dayanmaktadır. Ancak blok zincir teknolojisi gibi dağıtık veri tabanı prensibinde ve herkese eşit uzaklıkta olduğu söylenebilen bir sistemde veri sorumlusunun belirlenmesi için, belirli bir blok zinciri uygulamasındaki farklı oyuncuların yanı sıra kendine özgü karakteristikleri dikkate almak gerekmektedir.[109] Blok zincir uygulamasında rol alan sistem oyuncularını 'veri sorumlusu' penceresinden irdelediğimizde;

Kamusal blok zincirdeki yazılım geliştiricisi, yazılım kodlarının yayınlandığı andan itibaren kişisel verilerin işlenmesindeki amaç ve araçları kontrol etme yetkilerinden vazgeçmektedir. Diğer yazılımcılarda da görülebileceği üzere, blok zincir geliştiricisi yalnızca sistemin kişisel verileri işleyebilmesi için bir araç sağlamaktadır. Bununla beraber, yazılımın yayınlanmasının ardından meydana gelen teknik sorunların çözülmesine yönelik işlemler de yine kişisel verilerin blok zincir sistemi tarafından işlenmesinin amaç ve araçlarının belirlenmesi olarak tanımlamamaktadır.

Madenci ise işlemleri onaylayarak sistemin işleyişini sağlamaktadır. Ancak madenci de kişisel bloklardaki verilere etki edememektedir. Öyle ki, bir madencinin işlemleri değiştirmeye çalışması halinde değişen/yanlış veriler diğer madenciler tarafından reddedilmektedir.[110] Madencilerin görevi, kişisel verilerin bir blok zincir sisteminde işlenmesinin amaçlarını ve araçlarını belirleyememekte ve ancak blok zincir protokolü uyarınca kendilerine verilen rol ile sınırlı kalmaktadır.

---

[109] Kaufmann, s.124.

[110] Ağın hesaplama gücünün %50'sinden daha fazlasını birleştiren bir grup madenci, teknik olarak, blok zinciri üzerindeki işlemleri kontrol edebilecek konumda olsa da, madencilik havuzları böyle bir hesaplama gücüne erişememeye çalışacaktır.

Devre (node), blok zincir protokolünü çalıştıran, yazılımın yüklü olduğu her bir bilgisayarın teknik adıdır. Bu anlamda her bir node, blok zincir ağına katılan fakat ticari amaç gütmeyen katılımcılardır. Genel itibarıyla ağdaki devrelerin birbiriyle doğrudan ve aracısız olarak iletişim kurmalarına imkan sağlamaktadır. Her bir devrenin, uymakla yükümlü olduğu bir protokol vardır ve uymaması halinde o devre ağın geri kalanı tarafından sistem dışı bırakılmaktadır. Şu halde, bir devrenin tek başına kişisel verilerin işlenme amaç ve araçlarını belirleyemediği aşikardır. Tüm bir devre grubu ise ortak bir anlaşma aracılığıyla blok zincir ağı ve kişisel verilerin işlenmesi üzerinde tam kontrol sahibi olabilecektir ancak burada da kamusal blok zincirde bu tür anlaşmaların mevcut olmadığı gerçeği ön plana çıkmaktadır. Netice itibarıyla ister tek bir devre ister bir devre grubu halinde olsa da kamusal blok zincirde veri sorumlusu olarak tanımlanamamaktadır.

Node'lara ilişkin bir görüş de Fransız Veri Koruma Otoritesi (CNIL) tarafından yayınlanmıştır.[111] Bu görüşe göre bir blok zincir ağı katılımcısının veri sorumlusu olarak nitelendirilmesinde gerçek yada tüzel kişi olmasına göre şu iki değerlendirmenin yapılması gerektiği; öncelikle kişinin gerçek kişi olması ve veri işleme faaliyetinin bu kişinin ticari ya da mesleki faaliyetinden kaynaklı olup olmamasına bakılması gerektiği, ya da tüzel kişi ise kişisel verilerin blok zincir ağında kaydedilip kaydedilmediği hususuna bakılması belirtilmektedir. Fransız Veri Koruma Otoritesi tarafından her ne kadar bu görüşün temellendirmesi GDPR m.2'de yer verilen 'aile içi' kavramı gösterilmiş ise de,[112] veri koruma hukukunun temel bakış açısına göre; veri işleme faaliyetinin kişinin kendisi veya ailesiyle ilgili olmamasındaki her durumun ticari ya da mesleki bir dayanağının olması mümkün değildir. Kaldı ki, hukuk düzeninde kişisel verilerin korunması hükümlerinin uygulanması için veri işleme eyleminin ticari ya da mesleki faaliyet kapsamında gerçekleştirilip gerçekleştirilmediği ile ilgilenilmemektedir.

Katılımcılar, yukarıda bahsi geçen her bir devreyi çalıştıranlardır ve doğrudan kamusal blok zincir ile etkileşime girmektedirler. Her bir katılımcı tek başına alıcının

[111] https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf Erişim tarihi: 27.07.2019

[112] Benzer bir kavram Kişisel Verilerin Korunması Kanunu m.28/1 hükmünde de yer almaktadır;
'*1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler* kapsamında işlenmesi'

kamusal anahtarına göndereceği kripto para birimine karar vermektedir. Bu işlemdeki veriler ise bloklarda saklanmakta ve geriye dönük olarak değiştirilememekte/silinememektedir. Bahsi geçen kontrol yetkisi sebebiyle KVKK ve GDPR kapsamındaki veri sorumlusu 'katılımcı' olabilir mi sorusu akıllara gelse de; bu tür bir görüş doğası gereği tüm kullanıcılarına yetki veren kamusal blok zincirin dağıtık yapıdaki doğasına aykırı düşmektedir. Öyle ki, blok zincir sistem itibarıyla tek bir noktadan kontrol edilememektedir. Hal böyleyken tek bir kontrol noktası bulunmayan bir sistemde kullanıcılardan birinin seçilerek veri sorumlusu ilan edilmesi de hakkaniyete aykırı ve pratiklikten uzak olacaktır.

Borsa ve e-cüzdanlar ise kullanıcıların kripto paralarını saklamalarını sağlayan bir hizmettir. Kullanıcının blok zincir ağındaki etkileşimi sağlayan servis sağlayıcısı, aynı zamanda işlemlerin yürütülmesi/kullanıcının para birimlerinin depolanmasını da sağlamaktadır. Buradan hareketle borsa ve e-cüzdanlar KVKK ve GDPR uyarınca kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyen veri sorumlularıdır. Ancak her blok zincir ağında borsa veya e-cüzdan kullanımı olmayacağı için çalışmamızın geneline -çalışmamızın kripto paralar ile sınırlı olmaması ve genel itibarıyla blok zincir ağını konu edinmesi sebebiyle- sirayet eden bir veri sorumlusu tespiti olarak kabul edilememektedir.

Bu anlamda, kamusal blok zincir uygulamaları ve protokollerinin geliştiricileri, madencileri, devreleri, katılımcıları, KVKK ve GDPR nezdinde veri sorumlusu olamaz iken, kullanıcılarının sistemdeki etkinliklerini sağlayan ve aynı zamanda veri depolama faaliyeti gösteren borsa ve e-cüzdanlar veri sorumlusu sıfatına haiz olabilmektedir.

Özel blok zincirde ise veri sorumlusunun belirlenmesi, sisteme girişin izinli olması ve bu iznin merkezi olarak verilmesi sebebiyle kolaylık kazanmaktadır. Bu sayede KVKK ve GDPR uyarınca veri sorumlusunda aranan kişisel verilerin işlenmesi amaçlarının ve araçlarının belirlenmesi kriteri de sağlanmış olmaktadır. Söz gelimi çalışmamızın '*D. Blok Zinciri Türleri'* bölümünde verilen bir derneğin bağış toplaması etkinliği için kurulan özel blok zincirde sisteme katılması uygun görülen kişilerin alınması için merkezi bir kişi/otorite tarafından izin verilmesi gerekecektir. Bu durumda izni veren kişi/otorite veri sorumlusu olarak nitelendirilebilmektedir. Özel blok zincirde

devreler ve madenciler genellikle veri işleyicisi olarak kabul edilmektedir. Ancak yine de tüm bu rol tespitlerinin özel blok zincirin özelliklerine bağlı olduğu unutulmamalıdır.

Netice itibarıyla, blok zincir teknolojisinde merkezi bir idare/yöneticinin bulunmaması ve dağıtık bir işlem ağının varlığı nedeniyle hem KVKK hem GDPR'da merkezilik ve hakimiyet ile özdeşleştirilen veri sorumlusu kavramının tespit edilmesi kamusal blok zincirde imkansız olarak addedilebilecektir. Bir an için yukarıda tanımlanan müşterek veri sorumlusu kurumu ile tespitin yapılabileceği düşünülse dahi, kamusal blok zincirlerde her kullanıcının bilgilere erişim yetkisinin bulunduğu ve aynı faydayı sağladığı düşünüldüğünde tüm blok zincir kullanıcılarının ortak veri sorumlusu olması gündeme gelecektir. Bu tespitin ise pratikte uygulanabilirliği mümkün olmayacağı gibi, müşterek veri sorumlusu kuramı KVKK'da da yer almamaktadır. Özel blok zincirde ise sisteme katılıma izin veren ve diğer kriterlerde söz sahibi olan merkezi bir otoritenin/kişinin genellikle var olması sebebiyle veri sorumlusunun tespitinin daha mümkün olduğu söylenebilecektir.[113]

E. Genel Olarak Veri Koruma Hukuku Tarafından Veri Sahiplerine Sağlanan Haklar

Kişisel Verilerin Korunması Kanunu ve Genel Veri Koruma Tüzüğü, kişisel verilerin işlenmesiyle ilgili gerçek kişilerin korunmasına ilişkin kuralların yanı sıra kişisel verilerin serbest dolaşımına ilişkin kuralları da ortaya koymaktadır.

Bu durum, veri koruma yasasının uygulanabilirliğinin kişisel verilerin katılımına dayandığı anlamına gelmektedir. Ancak "kişisel veri" nedir? KVKK ve GDPR, tanımlanmış veya tanımlanabilir gerçek bir kişiyle ilgili herhangi bir bilgiyi kişisel veri olarak tanımlamaktadır. Bununla birlikte, belirli bir verinin arkasındaki gerçek bir kimsenin olası "tanımlanabilirliği" hakkında doktrinde farklı görüşler mevcut olmakla beraber bu "tanımlanabilirlik" kesin olarak dışlanamadığı sürece varsayılmalıdır.[114]

[113] Çekin, s.44.
[114] Kaufmann, Dr. Jörg, s.120-127.

1. Temel Prensipler

Hem Kanunda hem de Tüzükte kişisel verilerin nasıl korunacağına dair temel prensipler ve koruma araçları öngörülmektedir. Bu anlamda veri işlemeye ilişkin altı temel prensipten bahsedilebilecektir. İlk prensip verilerin işlenmesinin, yasal, adil ve şeffaf olmasıdır. Veri sorumlularının veri sahipleri hakkındaki bilgileri toplamak için Kanunda ve Tüzükte yer verilen yasal dayanaklarının olması gerektiği, toplanan bu verilerin kullanım amacı konusunda şeffaf olunması ve tüm veri işleme sürecinin hukuka uygun gerçekleştirilmesi beklenmektedir. Bunun yanı sıra verilerin işlenme amaçları da sınırlı olmalıdır; kişisel verilerin spesifik olarak belirlenmiş, açık ve meşru amaçlar için toplanması ve yalnızca belirtilen amaçlar için kullanılması gerekir. Bir diğer deyişle, veri sorumlusu belirttiği amaçlar dışında verileri toplayamaz ve işleyemez olmalıdır. Bu anlamda GDPR tarafından tanınan -kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçlı- istisnalar hariç tutulmaktadır.

Bir diğer temel prensip ise işlenmek üzere toplanan verilerin sınırlı olmasıdır. Toplanan kişisel veriler, belirtilen amaçlar için "yeterli, ilgili ve gerekli olanlarla sınırlı" olmalıdır. Bu prensip, söz gelimi internet üzerinden pizza dağıtan bir şirkete siparişi tamamlamak için birinin medeni durumunu sorması gibi gerekli olmayan verileri sormayı yasadışı kılar. Aynı şekilde, belirlenen amaçlar çerçevesinde işlenmek elde edilen ve saklanan veriler, gerçek ve güncel olmalıdır. Bu ilkeye göre veri sahipleri, diğer haklarının yanı sıra bir veri sorumlusu tarafından tutulan yanlış verilerin değiştirilmesini isteme veya güncelleme talep etme hakkına sahiptir.

Verilerin saklanma süreleri de işlenme amaçlarına uygun olmalıdır. Toplanan kişisel veriler, kullanım amacı için gerekenden daha uzun süre saklanmamalıdır. Bir diğer deyişle bu ilke ile verilerin süresiz tutulması engellenmesi amaçlanmaktadır. Bu itibarla veri sorumluları, toplanan verilerin artık gerekli olmaması durumunda verileri silebilecek şekilde hazır bulunmalıdır.

Verilerin saklanması esnasında da güvenli ve gizlilik esasına uygun yolların kullanılması gerekmektedir. Veri sorumluları topladıkları kişisel verilerin, kayıp, imha veya hasarlara karşı korunmaları konusunda veri sahibine karşı sorumlulardır.[115]

Yukarıda sayılan tüm bu ilkelerin yanısıra KVKK ve GDPR tarafından öngörülen bir başka kural da; eğer veri sahibi 'özgür iradesiyle, işleme konusuna yönelik olarak, aydınlatılmış ve kesin olarak' rıza beyanında bulunursa verilerin işlenmesi yasal olarak gerçekleşebilecektir.[116]

2. KVKK Tarafından Tanınan Haklar

Yukarıda bahsedilen ilkeler çerçevesinde aynı yasal düzenlemelerle veri sahiplerine de birtakım haklar tanınmıştır. KVKK nezdinde tanınan bu haklar m.11 hükmünde; herkesin veri sorumlusuna başvurarak kendisiyle ilgili kişisel verilerinin işlenip işlenmediğini öğrenmesine, kişisel verileri işlenmiş ise buna ilişkin bilgi talep etmesine, kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenmesine, yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilmesine olanak tanımaktadır. Bunların yanı sıra, veri işleme sürecinden sonrasına dair olarak ise kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini istemek, kişisel verilerin silinmesi, yok edilmesi veya anonimleştirilmesine dair öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini istemek, verilerin düzeltilmesi, silinmesi veya yok edilmesi halinde bu durumun aktarım yapılan üçüncü kişilere bildirilmesini talep etmek, işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etmek ve kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etmek de KVKK tarafından veri sahiplerine tanınan haklar arasında sayılmaktadır.

3. GDPR Tarafından Tanınan Haklar

Genel itibarıyla KVKK ile GDPR'da veri sahiplerine tanınan haklar büyük oranda benzerlik göstermektedir. Bu anlamda GDPR tarafından da bilgilendirilme hakkı

[115] Blockchain and the GDPR (Thematic Report), s.12.
[116] Belirtilen rıza beyanı kavramı, KVKK m.3/I. hükmünde yer alan 'açık rıza' ibaresiyle tanımlanmış olup, belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza olarak ifade edilmiştir.

ile veri sahibinin haklarının kullanımına yönelik şeffaf bilgilendirme, bildirim ve yöntemlerin veri sahibine bildirilmesi olarak yer almaktadır. Erişim hakkı ile bireyler, kişisel verilerinin işlenip işlenmediği hakkında bilgi ve kişisel verilerinin bir kopyasını talep edebilecekler ve düzeltme hakkı ile bireyler, haklarındaki eksik bilgilerin tamamlanmasını veya yanlış bilginin düzeltilmesini isteyebileceklerdir.

Veri sahiplerine tanınan silme hakkı (unutulma hakkı) sayesinde ise bireyler, verilerindeki düzeltmenin yanı sıra kişisel verilerinin silinmesini de talep edebileceklerdir. Bu minvalde veri sahipleri verilerinin tamamen silinmesi yerine veri işleme faaliyetinin kısıtlanmasını talep edebilecektir.

Bunun yanı sıra veri sahipleri, kendilerine ait kişisel verileri veri sorumlusuna sağladıktan sonra da "yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı" ve "kişisel verilerin sağlandığı kontrolörün herhangi bir engellemesi olmaksızın bu verileri başka bir veri sorumlusuna iletme hakkı"na sahiptir.

Diğer yandan bireyler tarafından, belli koşulların varlığı halinde kişisel verilerinin işlenmesine itiraz edilebilecektir.

Sadece GDPR'da yer alan bir hüküm ile de veri sahipleri, profilleme işlemi de dahil olmak üzere otomatik işlemelere karşı haklar; her birey, ekonomik amaçlar sebebiyle algoritmalar veya yapay zeka tarafından otomatik kararlar alınarak verilerinin işlenme faaliyetlerine karşı bu kararların nasıl alındığına dair bilgi talep edebilecektir. Esasında profilleme işlemi, KVKK gerekçesinde bilişim sistemleri üzerinden otomatik yollarla kişisel verilerin sıklıkla kullanıldığı belirtilerek ifade edilmiş ise de; KVKK içerisinde profillemeye ilişkin herhangi bir hükmün yer almadığı dikkat çekmektedir.[117]

---

[117] İfadenin tam hali; '*Günümüzde bu veriler, gerek özel sektör ve gerekse kamu sektörü tarafından bilişim sistemleri üzerinden otomatik yollarla sıkça kullanılmaktadır. Bu bilgilerin kullanılması bireyler ile mal ve hizmet sunanlar bakımından bazı kolaylıklar veya avantajlar sağlasa da, bu durum söz konusu bilgilerin istismar edilme riskini de beraberinde getirmektedir.*' şeklinde yer almaktadır.

https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim tarihi:22.07.2019

F. Özel Olarak Unutulma Hakkı

Çalışmamızın temel konusunun blok zincir teknolojisinde unutulma hakkının kullanımı olması nedeniyle geri kalan bölümde unutulma hakkı detaylandırılacaktır. Ancak unutulma hakkının ne olduğuna dair tanımlamalara yer verilmeden önce bireyde yaşattığı olumsuz psikolojinin daha iyi anlatılabilmesi adına öncelikle somut örnekler üzerinden ilerlenecektir.

Bir öğretmen adayı olan Stacy Snyder, 2006 yılının ilkbaharında, henüz 25 yaşında ve bekar bir anne iken eğitimini tamamlamış ve kariyer hedefine doğru emin adımlarla yürürken Üniversitenin yetkilileri tarafından kendisine 'öğretmen olamayacağı' beyan edilmiştir. Tüm sınavlarını başarıyla geçmiş olması ve tüm stajlarını yüksek puanlar ile tamamlamış olmasına rağmen, davranışları nedeniyle sertifikasını almaya hak kazanamamıştır. Üniversite yetkililerinden 'ne tür bir davranış' nedeniyle hak kazanamadığı öğrenmek isteyen Snyder'e, kendisine ait online bir platform olan MySpace hesabında üzerinde bir korsan şapkası ile elindeki plastik bardağından içerken paylaştığı ve altında 'İçkili Korsan' açıklamasını yaptığı bir fotoğrafı gösterilmiştir. Üniversite yönetimi, Snyder'in paylaştığı bu fotoğrafın Snyder'den eğitim alacak olan öğrenci adayları tarafından da ulaşılabilir olduğu ve bu anlamda alkol alan bir öğretmenin fotoğrafının bu şekilde ifşa edilmesinin meslek etiğine aykırı olacağını beyan etmiştir.[118]

Andrew Feldmar ise Vancouver'de yaşayan Kanadalı bir fizyoterapisttir. 2006 yılında, Seattle-Tacoma Havaalanından arkadaşını karşılamak üzere yola çıkmıştır ve -daha önce defalarca kez yaptığı gibi- ABD/Kanada sınırını geçerken bir sınır görevlisi tarafından Feldmar hakkında internet araması yapılmıştır. Bu arama esnasında Feldmar'ın 2001 yılında bir dergide kaleme aldığı makalesi güvenlik görevlisinin dikkatini çekmiştir. Feldmar'ın bu yazısında 1960'larda LSD kullandığına değinilmektedir. Bu makale üzerine Feldmar, sınırda dört saat bekletilmiş, parmak izi alınmış ve yaklaşık 40 yıl önce aldığı madde yüzünden ABD'ye giriş yapması yasaklanmıştır.

[118] Viktor Mayer-Schönberger, **Delete-The Virtue of Forgetting In The Digital Age**, Princeton University Press, 2011, ABD, s.1.

Andrew Feldmar, hiçbir sabıka kaydı olmayan ve işinde başarılı bir profesyonel iken 1960'lı yıllarda LSD kullanarak kanunları ihlal ettiğinin farkında olduğunu, fakat 1974'ten beri uyuşturucu kullanmadığı iddia etmektedir. Bu olay Feldmar için çok geçmişte yaşanmış ve toplum tarafından unutulmuş olduğunu düşündüğü bir suç iken dijital teknoloji yüzünden, toplumdaki unutabilme yeteneği, yerine mükemmel bir bellek bırakmıştır.[119]

Geçmiş yıllarda Almanya'da dört bin kişilik kapasiteye sahip mega bir gece klubü olan MAD ise, içeride başlattığı 'özel kart' uygulamasıyla gündeme gelmiştir. Müşteriler gece klubüne giriş yaparken kimlik kartlarını veya pasaportlarını göstermekte ve belgede yer alan fotoğraf ile diğer tüm bilgiler bir veri tabanına girilmektedir. Akabinde müşterilere özel bir kart verilmekte ve MAD içerisinde yapılacak tüm yeme-içme harcamalarının bu karttan yapılması sağlanmaktadır. Müşterilerin içeride yaptıkları her bir alışveriş ise o müşteriye ait dijital kayıtlarda saklanmaktadır. 2007'nin sonlarına doğru, basında çıkan bir habere göre, MAD'in veri tabanı 13 binden fazla kişi bilgisi ve milyonlarca işlem detayını içermektedir. Bunların yanı sıra içeride aralıksız kayıt yapan 60 dijital kamera bulunmaktadır ve 8 bin GB depolama hafızasına sahip bu kameralarla gece kulübünün hemen hemen her köşesinden görüntü alınabilmektedir. Müşteriler hakkında edinilen eş zamanlı bir diğer bilgiye göre ise; müşterilerin içeride yaptıkları tüm işlem davranışları ve tüketim tercihleri James Bond filmlerini andıran özel bir kontrol odasında büyük ekranlarda sergilenmektedir. Yönetim ise MAD'e ait hard disklere yerel polisin 7/24 çevrimiçi bir şekilde nasıl ulaşabildiğini gururla açıklamıştır.[120]

Dijital belleğin kendisini göstermeye başladığı bu dönemde Catherine Davis adlı bir PTA (Parent-Teacher Association) yöneticisi durumun ciddiyetini şu sözleriyle ifade etmektedir; 'Artık aptal bir ergenlik hatasının etkileri çok daha büyük olabilir ve hayatlarının geri kalanında kayıtlarda olmaya devam edebilir'.

Yukarıda yer verilen örneklerden anlaşıldığı üzere unutulma hakkı, hukukun gücü kullanılarak geleceğe hangi değerlerin getirilmesi gerektiği ile ilgili bir sorunun cevabıdır. Unutulma hakkı bazen zor nedenler veya gerçekler için kişinin kendisinden,

[119] Mayer-Schönberger, s.4.
[120] Mayer-Schönberger, s.6.

doğru kişilerden veya yanlış kişilerden uzak tutmaya çalıştığı bilgiler için bir tür ricada bulunmaktır.[121] Bir başka tanıma göre unutulma hakkı; bireyin dijital hafızada yer alan kimliği, fotoğrafı, adresi vb. tüm kişisel içeriklerinin kendi talebi ile bir daha geri getirilemeyecek şekilde yok edilmesi/ortadan kaldırılmasıdır.[122]

Şahsi tanımlamamıza göre ise unutulma hakkı; bireyin geçmişin prangalarına takılmaksızın kendini gerçekleştirilebilme hakkıdır. Bireyin kendini gerçekleştirilebilmesi; başkalarının özgürlüklerini ihlal etmemek şartıyla, kendilerini ve iç seslerini dinleme ile fikirlerine sadık kalmaya teşvik edilmesidir.[123] Bu temel özgürlük insan haklarıyla teminat altına alınmaktadır.

Aksi düşünüldüğünde kendi bilgilerine dair denetim hakkının elinden alındığını düşünen birey, geçmişte yaşadığı bir olayı geçmişte bırakamadığı için bugün geleceğinin de yüküyle birlikte daha ağır bir şekilde sırtlanmak zorunda kalmaktadır. Unutulma hakkı, burada kişinin bu yüklerden kurtulmasının bir teminatı olacaktır. Bir başka deyişle bu hak, kişiye hayatında yeni bir sayfa açabilmesini sağlayacaktır.[124]

Şayet kişi, sözlerinin ve eylemlerinin yıllar sonra algılanmasından ve ortaya çıkarılmasından korkar ise, unutulmayacağının bilinmesi kişiyi daha az özgür kılacak ve açık bir şekilde kendisini ifade etmesini engelleyecektir.

Öyle ki, her birey hayatının kaydedildiği ve kendisine dair kayıtların tutulduğu, toplumsal unutmanın yerini tam zamanlı hatırlamanın aldığı bir dünyada yaşadığını düşündüğünde, dünyayı nasıl gördüğü ve nasıl davrandığı derinden etkilenecektir. Böylece birey her anında izlendiğini düşündüğü bir ortamda kendisini gerçekleştirme fikrinden uzaklaşacaktır. [125]

Gelecekte 'unutmayan' bir dünyanın bugün içinde yaşanılan toplumu nasıl bir hale getireceği ise endişe vericidir. Günlük hayatın bir parçası haline gelen sosyal medya aracılığıyla, henüz 18 yaşından küçük bireylerin dahi özel hayatlarına dair her

[121] Jones-Meg Leta, **Ctrl+Z The Right to be Forgotten,** 2016, New York University Press, s.190.
[122] Aydın Akgül, **Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve AB Adalet Divanı'nın 'Google Kararı'**, Türkiye Barolar Birliği Dergisi, 2016, s.16.
[123] Yuval Noah Harari, **21. Yüzyıl için 21 Ders**, 2018, s.58.
[124] Küzeci, s.224.
[125] Viktor Mayer Schönberger, **Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing,** Harvard University John F. Kennedy School of Government, Faculty Research Working Papers Series, 2007, s. 5-6.

türlü paylaşıma ulaşılabilmekte, kimi zaman kendileri gelecekte bu paylaşımlardan etkilenebilecekleri gibi, kimi zaman da haklarının bilincinde olmayan çocuklar büyüme aşamasındayken -çoğu zaman kendi ebeveynleri tarafından- suistimale uğramaktadırlar.[126]

Unutulma hakkının birey yaşantısındaki etkilerini daha detaylı açıklarsak; şayet bireyler haklarındaki herhangi bir bilginin yaşadığı süreden daha uzun bir süre hatırlanacağı konusunda endişelendiğinde, önemsiz meselelerin, kişisel deneyimlerin paylaşılması, çeşitli siyasi yorumlar yapılması konularındaki görüşlerini ifade edecek midir? Veya bunun sonucu bir otosansür mü olacaktır? Mükemmel hafızanın ürpertici etkisi bireylerin davranışlarını değiştirecektir.[127]

Nitekim durumun davranışlara yansıması Synder'in 'Çevrimiçiyken ne yayınladığınıza dikkat edin' ve Feldmar'ın 'İnsanları, internet üzerinde bıraktıkları izlerin bir gün kendilerine karşı kullanılabileceği konusunda uyarıyorum. Onlar silinmiyor' yorumlarıyla da açıkça anlaşılmaktadır.

Gelişen teknoloji ile birlikte yakında çevremizdeki nesneler dahi küçük ve uygun fiyatlı sensörlere sahip olabilecek, nerede olduklarını kaydedebileceklerdir. Bu nedenle potansiyel olarak üçüncü taraflara yalnızca bulunulan yerin kapsamlı bir dijital hafızasını değil, çevredeki şeylerle ne zaman ve nasıl etkileşime girildiğini de sunabileceklerdir. Büyük olasılıkla, eylemlerin daha kapsamlı bir izi daha önce hiç olmadığı kadar toplanacak ve dijital bellekte saklanacaktır.[128]

Dijital bellek, hatırladıklarımızdan daha fazla bilgimizi saklar ve ifşa eder. Oysa geçmişte olumsuz olarak addedilen bir vakanın bireyin her yeni iş ilişkisinde, arkadaşlık ilişkisinde veya herhangi bir zaman/yerde karşısına çıkacağını bilmesi bireyi

[126] 18 yaşından küçüklerin internet paylaşımlarından dolayı gelecekte mağdur olmamaları amacıyla iRights adında bir sivil toplum hareketi başlatılarak bu çocukların yetişkinliğe ulaşmadan doğrudan sosyal medya paylaşımlarını silmelerine izin verilmesi hedeflenmektedir. İçerik itibarıyla 18 yaş altı çocuklar için başlayan bu oluşum, 'içeriklerin kolaylıkla düzenlenebilmesi, silinebilmesi, bilgilerin kimde bulunduğunun bilinmesi ve kimin menfaat elde ettiğinin öğrenilmesi' gibi hakları çocuklara sunacaktır. Bunun yanı sıra, çocukların yasa dışı sayfalardan korunması, dijital okur yazar olabilmeleri ve bilinçli seçimler yapmalarını sağlamak da yine bu oluşumun hedefleri arasında yer almaktadır. 18 yaş altı kullanıcılara özel 'sil' butonlarının getirilmesi ve bu yaş grubundan elde edilen veriler için son kullanma tarihleri sunulacağı da konuya ilişkin gelişmeler arasındadır.
https://www.independent.co.uk/life-style/gadgets-and-tech/irights-under-18s-could-soon-be-able-to-delete-their-sketchy-social-media-past-say-campaigners-10420559.html Erişim tarihi: 27.07.2019

[127] Mayer-Schönberger, s.5.

[128] Viktor Mayer-Schönberger, s.10.

özgürlüğünden, serbestliğinden ve kendini dilediği gibi ifade edebilme hakkından mahrum edecektir. Üstelik bunun çok sessiz ve pasif bir şekilde gerçekleşeceği de aşikardır. Unutulma hakkı ise dijital dünyanın kusursuz hafızasına karşılık birey olarak elimizdeki tek panzehirdir.

1.Türk Yargısında Unutulma Hakkı;

Türk hukukuna göre 'unutulma hakkı' olarak tanımlanmış bir hak bulunmamakla birlikte, Anayasa, Türk Medeni Kanunu, KVKK ve Adli Sicil Kanunu dayanak alınmış ve Anayasa Mahkemesi ile Yargıtay tarafından aşağıda detaylı olarak anlatım bulacak kararlarda açıkça kullanılmıştır.

a.Mevzuat

Kanunlarda yer almayan fakat içtihatlarda tanınan bu hakkın hukuki çerçevede hangi hakların içeriğinde yer aldığı konusu da doktrinde tartışmalara konu olmaktadır. Belirtilmelidir ki, unutulma hakkının birden fazla kanunda dokunduğu noktalar mevcuttur. Anayasa, Türk Medeni Kanunu, Kişisel Verilerin Korunması Kanunu ve Adli Sicil Kanunu unutulma hakkı ile bağdaştırılmaktadır.[129]

Unutulma hakkının Anayasa'da iki farklı maddede temellendirmesi yapılabilmektedir. Anayasa'nın 17. maddesinde düzenlenen maddi ve manevi varlığın

[129] Eren Sözüer, **Unutulma Hakkı,** 2017, On İki Levha Yayıncılık, s.159.

korunması ve geliştirilmesi hakkı[130] ile, 20. maddesinde düzenlenen özel hayatın gizliliği ve korunması hakkı 'unutulma hakkı'nın yasal çatısını oluşturmaktadır.[131]

Türk Medeni Kanunu'nda ise 'kişilik hakkı' olarak unutulma hakkı ve kişilik hakkına saldırı halinde unutulma hakkı olarak ikiye ayırmak mümkündür. Çıkış noktası itibarıyla bir kişilik hakkı olan unutulma hakkı, bireyin sadece insan olması nedeniyle sahip olduğu bir haklar bütününe mensuptur.

Buna karşılık unutulma hakkının kişilik hakkı olarak korunmasında iki ihtimal söz konusu olacaktır. Birincisi kamunun erişiminin mümkün olduğu bir alanda geçen olayın özel alanı ilgilendirmesi halidir. Yargıtay HGK tarafından unutulma hakkının tanındığı kararın bu kapsamda olduğu belirtilebilecektir. Diğer ihtimalde ise herkes tarafından bilinebilir olan bir olgunun bireyin kişilik haklarına zarar verecek ölçüde

---

[130] Maddenin tam hali;

'*I. Kişinin dokunulmazlığı, maddî ve manevî varlığı*
MADDE 17- Herkes, yaşama, maddî ve manevî varlığını koruma ve geliştirme hakkına sahiptir.

Tıbbî zorunluluklar ve kanunda yazılı haller dışında, kişinin vücut bütünlüğüne dokunulamaz; rızası olmadan bilimsel ve tıbbî deneylere tâbi tutulamaz.

Kimseye işkence ve eziyet yapılamaz; kimse insan haysiyetiyle bağdaşmayan bir cezaya veya muameleye tâbi tutulamaz.

Meşru müdafaa hali, yakalama ve tutuklama kararlarının yerine getirilmesi, bir tutuklu veya hükümlünün kaçmasının önlenmesi, bir ayaklanma veya isyanın bastırılması veya olağanüstü hallerde yetkili merciin verdiği emirlerin uygulanması sırasında silah kullanılmasına kanunun cevaz verdiği zorunlu durumlarda meydana gelen öldürme fiilleri, birinci fıkra hükmü dışındadır.'

[131] Maddenin tam hali;

'*MADDE 20- Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.*

Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.'

hatırlatılması halidir. Bu durumda kişilik haklarına saldırı da söz konusu olabilmektedir.[132]

Kişisel Verilerin Korunması Kanunu içeriğinde ise unutulma hakkı terim olarak yer almamakta ise de 11.maddesinde 'ilgili kişinin hakları' olarak belli koşullar halinde verilerin silinmesi/yok edilmesi/anonimleştirilmesini talep etme hakkı kapsamında değerlendirilmektedir.

Adli Sicil Kanunu'na göre tutulan sicil kayıtları ise sicil ve arşiv olarak ikiye ayrılmaktadır. Bu kayıtların gizliliği ve belli bir süre sonunda silinmesi ise bireyin geçmişteki olumsuz durumunun tekrar önüne çıkmasını engeller ve bireyin hayatının geri kalanına prangaları olmadan, temiz bir sayfa açarak devam etmesini sağlamaktadır. Bu yönüyle Kanun, hükümlülerin unutulma hakkını kullanmalarını zımni olarak sağlamaktadır.

Türk hukukunda edindiği yasal dayanaklarını izah ettiğimiz unutulma hakkı, Türk yargı kararlarında da zaman zaman uygulama alanı bulabilmektedir. Belirtilen kararlara çalışmamızın bir sıradaki bölümünde değinilecektir.

b. Yargı Kararları

Yargıtay Hukuk Genel Kurulu 2014/4-56 E. ve 2015/1679 K.[133] sayılı kararında Türk yargısında ilk kez unutulma hakkından bahsedilmiştir. Davanın konusu,

---

[132] Sözüer, s.168.

[133] Yargıtay tarafından verilen bu karar, hala yasalarda yer almayan 'unutulma hakkı'nın Türk Veri Koruma Hukuku nezdinde anılan ilk kararı niteliğindedir. Kararın içerisinde unutulma hakkı şu şekilde tarif edilmiştir;

'*...bireyin kişiliğini serbestçe geliştirmesi, kişiliğinin korunması ve özgür bireylerden oluşan bir toplum düzeninin oluşturulması, ancak bireyin kişisel verilerine ilişkin hakkının korunmasıyla mümkündür.* Bu *hak yukarıda ifade edildiği üzere TC Anayasası'nın 20/2 maddesinde açık bir şekilde düzenlenmiştir.*

Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

başvuranın İzmir C. Başsavcılığı vekilliği yapan şahıs ile çalışmak üzere atandığı, 8 ay boyunca bu şahsın sözlü ve fiziksel tacizine maruz kalması ve durumun çekilmez bir hal alması neticesinde şikayet ettiği ve şahsın soruşturma sonrasında yargılanarak ceza aldığı, o dönemde bu olayın basına da konu olduğu,

Olaydan 4 yıl sonra yorumlu-uygulamalı Türk Ceza Kanunu adıyla yayınlanan eserde ise örnek Yargıtay kararı olarak bu olayın ve tüm aktörlerin isimleri de açıkça yazılmak suretiyle tüm detayıyla anlatıldığı, yeniden gündeme gelen bu olay nedeniyle başvuranın psikolojik bunalıma girdiği, tüm kötü olayları tekrar yaşamak zorunda kaldığı, hala adliyede çalışıyor olması nedeniyle davacı çevresinde ve kitabın potansiyel okuyucuları olan savcı ve avukatlar tarafından da öğrenildiği, başvuranın tüm bu süreçte olayın bilinmemesi için çaba sarf etmesine rağmen dava konusu eser sonrasında artık gizleme gibi bir imkanının kalmadığı, eserin yıllar boyunca yargı çevresi tarafından okunacak bir eser olması nedeniyle başvuranın adının geçtiği ciltlerin toplatılması talep edilmiştir.

Yargıtay *Hukuk Genel Kurulu* konuya ilişkin irdelemeleri yaparken unutulma hakkının bireye sağladığı korumayı, kişisel verilerin korunması ile bilim ve sanat hürriyetinin birbirlerine karşı sınırlarının değerlendirilmesi gerektiğini, 4 yıl önce gerçekleşen bir olayın mağdurunun adı ve soyadının eserde belirtilmesinin -Google kararına atıf yapılarak- üstün bir kamu yararını işaret etmediğini belirtmiştir.[134]

Bu hak bir yandan kişiye "geçmişini kontrol etme", "belirli hususların geçmişinden silinmesini ve hatırlanmamayı isteme hakkı" sağladığı gibi, diğer yandan muhataplarına kişi hakkındaki bir kısım bilgilerin üçüncü kişilerin kullanmamasını veya üçüncü kişilerin hatırlamamasına yönelik önlenmeleri alma yükümlülüğü yükler".

[134] Belirtilen konular karar içeriğinde şu şekilde yer almaktadır;
'…Unutulma hakkına gelince; unutulma hakkı ve bununla ilişkili olan gerektiği ölçüde ve en kısa süreliğine kişisel verilerin depolanması veya tutulması konuları, aslında kişisel verilerin korunması hakkının çatısını oluşturmaktadır. Her iki hakkın temelinde bireyin kişisel verileri üzerinde serbestçe tasarruf edebilmesini, geçmişin engeline takılmaksızın geleceğe yönelik plan yapabilmesini, kişisel verilerin kişi aleyhine kullanılmasının engellenmesini sağlamak yatmaktadır. Unutulma hakkı ile geçmişinde kendi iradesi ile veya üçüncü kişinin neden olduğu bir olay nedeni ile kişinin geleceğinin olumsuz bir şekilde etkilenmesinin engellenmesi sağlanmaktadır. Bireyin geçmişinde yaşadığı olumsuz etkilerden kurtularak geleceğini şekillendirebilmesi bireyin yararına olduğu gibi toplumun kalitesinin gelişmişlik seviyesinin yükselmesine etkisi de tartışılmazdır.

Unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir…

Bu bağlamda değerlendirildiğinde; 4 yıl önce gerçekleşen bir olayın mağduru olan kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiği kabul edilmelidir. Avrupa Birliği Adalet Divanı'nın "Google Kararı"nda açıkladığı gibi ilgili verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde, üstün bir kamu yararını

Bunun yanı sıra, unutulma hakkı tanımlarının genel itibarıyla dijital veriler için düzenlendiği, ancak kamunun erişiminin bulunduğu yerlerdeki kişisel verilere karşı da uygulanması gerektiğine hükmetmiştir.[135]

Nitekim *Yargıtay 19. Ceza Dairesi tarafından 11.03.2019* tarihinde verilen bir diğer kararda; ilgili kişi; 2018 yılında intihar eden eski banka müdürü olan eşi hakkındaki haberlerin çeşitli web sitelerinde yer aldığını, bu haberlerde değişik içeriklerin de bulunduğu ve ilgilinin eşiyle ve arkadaşlarıyla çektirdikleri fotoğraflara da bu haberlerde yer verildiğini, banka müdürünün sır ölümü türevinde başlıklar ile sunulan bu içeriklerin ilgili ile vefat eden eşin müşterek çocuklarının psikolojisini olumsuz yönde etkilediğini, vefat sonrası psikolojik destek almaya başladıklarını ve hala da devam ettiklerini, internette yer alan tüm haberlerin artık güncelliğini yitirdiğini, aile ve özel hayata ilişkin olumsuz bir anı olarak hatırlanan bu olayın internette yayınlanmasında da artık bir kamu yararının bulunmadığını ve ilgilinin fotoğraflarının da bu haberlerde yer almasının kişilik haklarına zarar verdiğini belirterek bu haberlere erişimin engellenmesini talep etmiştir.

Yargıtay'ın karar içeriğinde sırasıyla ifade ve basın özgürlüğü, kişilik hakları, kişisel verilerin korunması kanunu ve unutulma hakkı çerçevesindeki mevzuatın irdelendiğini ve neticesinde;

'*Yargının görevinin, internet haber arşivinin herhangi bir gerekçe olmaksızın ve tamamen ortadan kaldırılması değil, internet arşivinde kişilerin şeref ve saygınlığına yönelen, kişilerin özel hayatı ve kişisel verilerinin kamu yararına katkı sağlamayacak şekilde işlenen, ayrıca güncelliğini yitiren ve tarihsel bir veri olarak da kabul edilemeyeceği anlaşılan kısımların, kişilerin talebi halinde "unutulma hakkı" kapsamında artık herkesin erişimine açık halde tutulmasının engellenmesi olduğu'* yönünde nihai kararını açıklamıştır.

---

ortaya koyan özel sebepler bulunmadığına göre bilimsel esere alınan kararda kişisel veriler açık bir şekilde yer almamalıdır.'

[135] Yargıtay HGK'nın konuya ilişkin ifadesi; '*Ayrıca şunun da ifade edilmesi gereklidir ki; unutulma hakkı tanımlarına bakıldığında her ne kadar dijital veriler için düzenlenmiş ise de, bu hakkın özellikleri ve bu hakkın insan haklarıyla arasındaki ilişkisi dikkate alındığında; yalnızca dijital ortamdaki kişisel veriler için değil, kamunun kolayca ulaşabileceği yerde tutulan kişisel verilere yönelik olarak da kabul edilmesi gerektiği açıktır.'* Şeklindedir.

Yine aynı kararda, üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan ve geçmişte yaşanılan olumsuzlukların belli bir süre sonra unutulmasını, başkaları tarafından bilinmesi istenmeyen kişisel verilerin silinmesinin talep edilmesi ve yayılmasının önlenmesini isteme hakkı olarak tanımlanmıştır.

Türk yargısında unutulma hakkına ilişkin verilen bir diğer karar Anayasa Mahkemesi'nin 24.08.2016 tarihli kararıdır.[136] Kararın içeriği başvuranın, ulusal bir gazetenin internet sayfalarında uyuşturucu kullandığı iddiasıyla geçmişte hükmedilen adli para cezasına ilişkin haberlerin yer alması nedeniyle ilgili haberlere ilişkin internet yayınının kaldırılması talebi hakkındadır.

Anayasa Mahkemesi, kararı değerlendirirken başvuranın şeref ve itibar hakkı ile basın organının basın ve ifade özgürlüğü arasında adil bir dengenin kurulmasını hedeflemiştir. Yapılan değerlendirme neticesinde haberler gerçeğe aykırı olmasa dahi, geçmiş yıllara ait bilgiler içerdiği ve bu haberin arşivden erişiminin önem taşıyor olması için gereken haber değerinin devamlılığının artık olmadığı, bu itibarla haberin geleceğe ışık tutacak nitelikte de olmadığına, buna karşılık başvurucunun itibar ve saygınlığını zedelemesi sebebiyle haberlere erişimin kaldırılması gerektiğine karar verilmiştir.

Özellikle yargı kararlarından da anlaşılacağı üzere unutulma hakkı Türk Hukukunda 'özel yaşamın gizliliği hakkı' çerçevesinde değerlendirilmekte iken, AB Hukukunda 'temel bir insan hakkı' kapsamında ele alınmaktadır.

2. AB Yargısında Unutulma Hakkı;

Bir önceki bölümde unutulma hakkının AB Hukukunda 'temel hak' çerçevesinde incelendiği belirtilmişti. AB Hukukunda benimsenen 'temel hak' kavramının içeriğine bakıldığında bu hakkın insan onuru, bireysel özerklik ve bilgilerin geleceğini belirleme hakkı, özel yaşamın gizliliği hakkı, düşünceyi açıklama özgürlüğü, bilgi edinme hakkı, özel haberleşmenin gizliliği ve bilim özgürlüğü gibi son derece

[136] Anayasa Mahkemesi'nin 24.08.2016 tarihli BB:37/16, N.B.B. kararı https://www.anayasa.gov.tr/tr/haberler/bireysel-basvuru-basin-duyurulari/unutulma-hakkina-iliskin-nbb-karari-basin-duyurusu/ Erişim tarihi: 01.03.2019

geniş kapsamlı bir çerçevede değerlendirildiği anlaşılmaktadır.[137] Çalışmamızın devamında unutulma hakkının GDPR'daki yeri ve konumu, akabinde bu hakkın oluşumunda en büyük katkıyı sağlayan ABAD Kararlarına yer verilecektir.

a.GDPR Nezdinde

Unutulma hakkı, KVKK'dan farklı olarak, GDPR nezdinde tanım olarak yer almış bir haktır. Bunun yanı sıra Avrupa Temel Haklar Şartı ve Veri Koruma Direktifi de bu hakkın temelini oluşturan mevzuatlardır.

Hukuk dünyasında ve basında büyük yankı uyandıran *Google Spain* kararının sonrasında Avrupa Veri Koruma Kurulu tarafından kararın uygulanmasına yönelik bir rehber yayınlama ihtiyacı doğmuştur. Bu rehberde ağırlıklı olarak unutulma hakkı talepleri değerlendirilirken hangi kıstasların sonucu belirlemesi gerektiğine yönelik kriter tespitleri yapılmıştır. Buna göre unutulma hakkı talebine ilişkin otoriteler tarafından bir karar verilmeden önce; arama sonuçlarının doğrudan bir gerçek kişiye ait olup olmadığı, ilgili kişinin çocuk olup olmadığı, ilgili kişinin kamuya mal olmuş bir kişi olup olmadığı, sonuçlarda hassas verilerin bulunup bulunmadığı, sonuçlarda yer alan veriler ilgili kişiye yönelik bir önyargıya sebebiyet verip veremeyeceği, içeriğin orijinalinin basın hakları çerçevesinde yayınlanıp yayınlanmadığı, ilgili kişinin kişisel verilerinin kamuya açık hale getirilmesinde, yayınlayanın yasal bir yükümlülüğü bulunup bulunmadığı, sonuçlarda yer alan verilerin bir suça ilişkin olup olmadığı ve son olarak ulaşılan bilgilerin güncellik durumunun araştırılması gibi kriterlerin değerlendirilmesi gerektiği belirtilmiştir.[138]

b.ABAD Kararları

Unutulma hakkının AB nezdinde temellerinin atılmasını sağlayan *Google Spain vs. AEPD and Mario Costeja Gonzalez* davasında; Mario Costeja adlı avukatın ismi 1998 yılına ait iki haberde geçmektedir ve bu haberlerde şahsın 'sosyal güvenlik

[137] Küzeci, s.58-99.

[138] European Data Protection Board, WP 225, **Guidelines on the Implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez'** C-131/12, 2014, s.13-20.
https://www.pdpjournals.com/docs/88502.pdf Erişim tarihi: 27.07.2019

borçları nedeniyle malvarlığının satıldığı' belirtilmektedir.[139] Costeja eviyle ilgili açık artırma ilanının hala Google arama sonuçlarında yer almasının özel yaşamın gizliliğini ihlal ettiğini, haberde yer alan maddi durumuna ait gerekçelerin artık sona erdiğini ve evini de geri aldığını, haliyle bu haberlerin gereksiz olduğunu belirtmiş ve gazetelerdeki ilgili sayfaların kaldırılması/değiştirilmesi ve Google'da yer alan kendisi hakkındaki kişisel verilerin arama sonuçlarından çıkarılması için mahkemeye başvurmuştur. Mahkeme tarafından bu talebe ilişkin olarak ABAD'a başvurularak,

GDPR'ın Google etkinlikleri açısından uygulanıp uygulanamayacağı,

Google İspanya Firmasının sunucularının ABD'de yer almasına rağmen AB Hukuku'nun uygulama alanı bulup bulamayacağı,

GDPR kapsamında bireyler kendileri hakkındaki kişisel verilerin arama sonuçlarından çıkarılmasını talep etme hakkının var olup olmadığı yönünde soruları iletilmiştir.

Avrupa Birliği Adalet Divanı, bu kararında 95/46 sayılı Bireylerin Kişisel Verilerinin İşlenmesi ve Serbestçe Dolaşımı Karşısında Korunmasına İlişkin Direktif'e atıf yaparak arama sayfalarının etkinliklerini veri işleme faaliyeti olarak kabul etmiş, sayfa sahiplerinin de veri sorumlusu olarak tespit edildiklerine ve AB nezdindeki veri koruma prensiplerinden kaçınamayacaklarını belirtmiştir. Kararda ayrıca arama motorunun ekonomik menfaatleri ile bireyin özel hayatının gizliliği hakları tartışılmış ve Firmanın ekonomik çıkarlarının bireyin haklarına üstün gelemeyeceğine yer verilmiştir. Akabinde bireyin unutulma hakkının mutlak bir hak olmadığına vurgu yapılarak, ifade özgürlüğü ve basın özgürlüğü gibi diğer temel haklar ile dengenin kurularak değerlendirme yapılması gerektiğini ifade etmiştir. Netice itibarıyla Mario Gonzalez'in talebi kabul edilmiş ve unutulma hakkını kullanmasına karar verilmiştir.

Unutulma hakkının kullanımına ilişkin bir diğer örnek dava Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni davasıdır[140]. Davanın tarafları İtalya'da bir turizm kompleksi inşaatı için anlaşan firma

[139] Judgment of 13.05.2014, Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzales, C-131/12, EU:C:2014:317, p:14.http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4488999 Erişim tarihi: 01.03.2019

[140] Judgment of 08.09.2016, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, C-398/15,EU:C:2017:197, p.24,25,26,27,28.

sahibi Manni ile Lecce Ticaret Odası'dır. Manni'nin iddiaları arasında; Ticaret Odası kayıtlarında mevcut şirketinin bilgileri arasında kendisinin ticaret geçmişinin de bulunduğu ve kendi ticaret geçmişinde 1992 yılında iflas eden ve 2005 yılında tasfiye edilen bir şirketin yöneticisi olduğuna dair bilgilerin yer aldığı, bu olumsuz bilgiler sebebiyle ticari hayatının etkilendiği ve şirketinin yaptığı kompleksteki mülklerin satılamadığı yer almaktadır.

İtalya Yüksek Mahkemesi, ulusal mevzuata göre şirketlerin kurulmasında talep edilen ve şirketlere ait verilerin sadece belirli bir süre kayıtlarda tutulmasına izin veren bir hükmün bulunmadığını, bu durumun İtalyan yasa koyucunun bireysel ihtiyaçlar ve toplumun ihtiyaçları arasında yapılan dengeleme uygulamasının bir sonucu olduğunu belirtmiştir. Bunun yanı sıra,

bireyin kendi yönetim geçmişiyle ilgili verilerin kullanılabilirliğinin önlenmesi hususunun, ticari hayatta ekonomik ve sosyal ilişkilerin geliştirilmesi için gerekli olan kesinlik ve şeffaflık prensiplerinin uygulanması konusunda kamu yararından üstün olmadığını ifade etmiştir.

ABAD'ın konuya ilişkin görüşünde, şirket kayıtları gibi kamuya yönelik kayıtların, yalnızca herkese açık olması halinde ve yasal olarak güvenilir bilgilerin şeffaf bir şekilde açıklanması halinde ticari hayatta güvenin sağlanması yönündeki temel amaçlarına ulaşabilecekleri,

Gerçek kişilerin, ticari bir şirket vasıtasıyla ekonomik hayata dahil olmalarının, şeffaflık koşulunu gerektirdiği, şirket kayıtlarında yer alan bireye ait kişisel verilerin belirli bir süre dahilinde kayıtlarda tutulması ile korunan yararın, şeffaf ticari bir hayatın sağlanabilmesi için üçüncü kişilerin bu bilgilere erişim hakkı sebebiyle olduğu ve bireyin hakkından üstün olduğu çıkarımını yaparak bireyin talebinin haksız olduğunu savunmuştur.

Unutulma hakkına ilişkin verilen güncel kararlardan bir diğeri ise G.C., A.F., B.H., E.D. v. Commission nationale de l'informatique et des libertés (CNIL), Google

---

http://curia.europa.eu/juris/document/document.jsf?text=right%2Bto%2Bbe%2Bforgotten&docid=183142&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=4822387#ctx1 Erişim tarihi: 19.07.2019

Inc.[141] davasıdır. Davanın konusu, davacıların Google LLC tarafından işletilen arama motoru sayfasında kendileri hakkında çıkan sonuçların erişime kapatılması hakkındadır.

Davacılardan G.C., kendisi hakkındaki eleştiri içeren bir fotomontaj bağlantısı ile YouTube'da yer alan ve siyasi kariyerini olumsuz etkileyen bir bağlantısının arama kayıtlarından kaldırılmasını,

Diğer davacı A.F. kendi arama sonuçlarında yer alan ve Scientology Kilise'sinde halkla ilişkiler görevlisi olarak çalıştığı dönemde erçekleşen bir intihara ilişkin haberin arama kayıtlarından kaldırılmasını,

Diğer davacı B.H. 1995'te kendisine açılan ve pek çok iş adamı ve siyasetçinin de yer aldığı bir siyasi partinin finanse edilmesine dair soruşturmada adının geçtiğini, ancak konuyla ilgili davadan 2010 yılında beraat aldığını beyan ederek bu haberlere erişimin kaldırılmasını,

Son olarak davacı E.D. ise 15 yaşından küçük çocuklara cinsel saldırıda bulunmak suçundan 7 yıl hapis cezasına çarptırıldığı ve 10 yıl süre boyunca da sosyal ve adli kontrolde tutulmasına ilişkin haberlerin Nice Matin ve le Figaro'da yayınlandığını ve bağlantılardan bu haberlerin çıkarılmasını talep etmiştir.

Tarafların öncelikle Google'a yönelttikleri bu talepleri Firma tarafından reddedilmiştir. Ardından Fransız Veri Koruma Otoritesi'ne (CNIL) başvuru yapmışlarsa da buradan da şikayetlerinin kapatıldığı yönünde bir cevap almışlardır.

Konuya ilişkin ABAD görüşü ise içeriğinde hassas veri taşıyan verilere karşı sistematik olarak kaldırma işleminin yapılması gerektiğini, ancak işlenen suçların ve bunların cezai müeyyidelerine ilişkin kararların internet sayfalarında yer almasının 95/46 sayılı Direktif'in 9. maddesi kapsamında ifade özgürlüğü kapsamında yer aldığını ve bu nedenle erişimlerin silinmesi talebinin reddedilebileceğini ifade etmiştir.

[141] Judgment of 10.01.2019, G.C., A.F., B.H., E.D. v. Commission nationale de l'informatique et des libertés (CNIL), Google Inc., C-136/17, EU:C:2019:773, p:25,26,27,28. http://curia.europa.eu/juris/document/document.jsf?text=right%2Bto%2Bbe%2Bforgotten&docid=209686&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=4822387#ctx1 Erişim tarihi: 20.07.2019

Yukarıda anılan kararlarda unutulma hakkına yönelik taleplerin farklı unsurlar çerçevesinde değerlendirilebildikleri görülmektedir. Öyle ki, Google Spain kararında başvuran hakkındaki haberlerin gerçek dahi olsa güncelliğini yitirmiş olması ve kamuya ilişkin bilgilendirme mahiyetini taşımıyor olması nedeniyle haberlerin erişiminin engellenmesi talebi kabul edilmişken, Manni davasında bireyin şu anki ticari hayatını etkileyen geçmişteki ticari başarısızlıklarına dair haberlerin 'ticari hayatta şeffaflık ve bilinebilirlik ilkesinin' kamu yararı gereği olduğu ve bu durumda bireyin kişisel haklarına üstün olduğuna kanaat getirilerek reddedilmiştir. Güncel unutulma hakkı taleplerinden G.C. ve Diğerleri davasında ise başvuranların erişime kapatılmasını talep ettikleri haberlerde yer alan hassas verilere ilişkin verilere erişimin otomatik olarak kapatılabileceğini, işledikleri ağır suç ve cezalarına ilişkin haberlerin ise kamunun bilgiye ulaşma hakkı ve haberin yayın kaynağının da ifade özgürlüğü kapsamında değerlendirdiği anlaşılmaktadır.

G.Veri Sahiplerine Tanınan En Önemli Haklardan Biri Olan Unutulma Hakkı ile Blok Zincir İlişkisinin İrdelenmesi

KVKK ve GDPR ile verilerin gizliliğine dair haklar korunmakta iken, bu yasalar ile dağıtık ve değişmez bir veri kayıt defteri olarak hizmet sunan blok zincir kavramı aralarındaki ilişki; 'Durdurulamaz bir güç, taşınmaz bir nesneyle karşılaştığında ne olur?' paradoksu ile tartışmalara konu olmaktadır.

Öyle ki, KVKK ve GDPR'ın ülkelerindeki veri sorumlusu ve veri işleyenlere veri koruma düzenlemelerine uyum için verdiği sürenin bitmesiyle ihlal tespitleri ve idari ceza uygulamaları başlamıştır.[142] Bahsedilen cezalar KVKK'da 5.000-TL ile 1.000.000-TL arasında, GDPR'da ise üst sınır 20.000.000-EUR veya sorumlunun tüzel kişi olması halinde o mali yıla ait %4 gelir (hangisi daha yüksek ise) şeklinde belirlenmiştir. Dolayısıyla Türkiye'de ve AB'de veri koruma yükümlülüklerine uymamanın bedeli ciddi biçimde ağırlaştırılmıştır. 'Durdurulamaz bir güç' ifadesi buradaki yasaların yaptırımsal/icrai gücüdür. [143]

'Taşınmaz bir nesne' ibaresi ise, blok zincir üzerinde bir kez bloklara -veri kayıt defterine- kaydedilen bir verinin hiçbir şekilde geri

[142] https://kvkk.gov.tr/Icerik/5419/Kurul-Kararlari Erişim tarihi:19.07.2019
[143] https://medium.com/@immuniweb/top-ten-2018-gdpr-violations-incidents-99e45efa01d9 Erişim tarihi: 19.07.2019

alınamaz/silinemez/değiştirilemez olmasından kaynaklanmaktadır. Bir başka deyişle blok zincirin değiştirilemezliği, KVKK ve GDPR'ın talep ettiği 'yasaya aykırı ise düzelt/değiştir' prensibi ile çatışma yaşamaktadır. Bahse konu teknolojinin temelinde işlemlerin birbirine zincirler halinde bağlanması ve böylece işlemin ilk noktasına dek takip edilebilmesi amacı mevcuttur. Şu halde, zincir üzerindeki bir halkada değişiklik yapılması, bütün zinciri geçersiz hale getirebilecektir. Bunun yanı sıra, bir halkada yapılacak değişiklik ile o işlemin geçmişi ile mevcut bağlantısını koparacaktır.[144]

Veri kayıt defterlerinde silinmeksizin kayıtlar yapılmasının KVKK'da kişisel verilerin silinmesini talep etme hakkı / GDPR'da ise unutulma hakkının ihlaline sebep olması nedeniyle; KVKK ve GDPR'ın blok zincir teknolojisinin gelişiminde engel teşkil edebileceği varsayımlarına yol açmaktadır.

Blok zincir teknolojisinde unutulma hakkının kullanımında ilk sorunsal veri sorumlusunun, bir başka deyişle muhatabın, kim olacağı konusudur. Bölüm B.4'te detaylı olarak anlatım bulduğu üzere kamusal blok zincirde veri sorumlusunun tespiti teoride -eğer tüm kullanıcıların eşit işleme yetkisine sahip olduğu ve eşit menfaat sağladığı düşüncesiyle müşterek veri sorumlusu benimsenirse- mümkün ancak pratikte imkansızdır. Özel blok zincirde somut olayda ağa katılım ve ağ üzerindeki kontrolün bir merkezde toplanması halinde mümkün olabilecektir.

Dağıtık veri ağındaki her katılımcı bilgisayar (node), kendisindeki yazılımı diğer node'lardan bağımsız olarak devam ettirmektedir. Bu sayede bir node tarafından yapılan değişiklik, diğer node'ları etkilemeyecektir, bir diğer deyişle, verinin tek bir bilgisayarda silinmesi, diğer bilgisayarlarda -her bilgisayarda silme işlemi gerçekleşmediği sürece- herhangi bir veri değişikliği yaratmayacaktır.[145]

Diğer yandan, verilerin silinmesi ihtimalinde, blok zincirin yapısı gereği -eklenen bloğu geri dönüşü olmaksızın ilerleyerek devam etmesi prensibi- verinin silinmesi sonrasında zincirin nasıl işlemeye devam edeceği de yine sorun teşkil

[144] Çekin, s.96.

[145] Ağdaki her bilgisayarda silme işleminin gerçekleşmesi ihtimali ise oldukça düşüktür. Şöyle ki; bu node'lar arasında bir iletişim ve hiyerarşi bulunmadığı gibi yönlendirme de yapılamamaktadır. Bu nedenle belirli verilerin erişimlerinin durdurulması, bilgisayarlardaki mevcut verilerin silinmesi yönünde talimat verilmesi ve hatta bu bilgisayarların talimata uyma yükümlülüğü de söz konusu değildir.

etmektedir. Belirlenen sorunlara ilişkin çözüm olabilecek önerilere çalışmamızın ‘Çözüm Önerileri’ bölümünde yer verilmiştir.

ÜÇÜNCÜ BÖLÜM
ÇÖZÜM ÖNERİLERİ

Çalışmada yer verilen blok zincir teknolojisinin değişmez/değiştirilemezliği ile KVKK ve GDPR tarafından tanınan 'belirli şartlar mevcutsa ilgililerin verilerinin silinmesi' hakkının (unutulma hakkı) kişisel veri içeren blok zincir ağlarında büyük sorunlara yol açabileceği aşikardır.

Belirtilmelidir ki, hukuk düzeninin ihlal gerçekleştikten sonra müdahale etmesi yerine henüz teknoloji gelişmekte iken proaktif davranılarak tüm sistemin veri koruma hukuku prensiplerine göre tasarlanması da mümkün olabilecektir. 'Tasarımla veri koruma' veya 'Varsayılan ayarlarla veri koruma'[146] olarak da kullanılabilen bu yöntemde; mahremiyet unsuru hukuki açının yanı sıra organizasyonel ve teknik yapılanma açısından da henüz gelişim aşamasındayken temel alınmaktadır. Böylece veri işleyecek olan sistemin veri koruma prensiplerine göre 'veri işlemeyi en az düzeyde' ve 'mahremiyet esasına uygun' şekilde gerçekleştirmesi sağlanabilecektir. Bu sayede ihlalin oluşumunun önlenmesi amaçlanmaktadır.[147] Blok zincir teknolojisinin de henüz gelişmekte olduğu göz önüne alındığında, belirtilen prensipler uyarınca gerek en az verinin depolanması ve gerekse mahrumiyet ilkelerine göre şekillendirilerek en az veri işleme faaliyetinin sağlanarak ihlallerin önüne geçilebileceği düşünülmektedir.

Blok zincir ağlarında kişisel verilerin işlenmesinden kaçınmak, daha teknik çözümler bulunana kadar ilk ve en basit öneri olacaktır. Kişisel verinin işlenmediği bir ağda KVKK ve GDPR'a aykırılıktan söz edilemeyecektir. Ancak bu durumda, kişisel verilerden tamamen kaçınılması, sadece –veya çoğu zamanda- kişisel veriler ile ilgili olan projelerde blok zincir teknolojisinin kullanımının sınırlanacağı aşikardır.

Veya ilk aşamada ağdaki tüm kişisel verilerin anonimleştirilmesi de çözüm olarak sunulabilecektir. İlk önerinin kullanım alanı itibarıyla kişisel veri içeren tüm projeleri olumsuz etkileyeceği düşünüldüğünde ve neredeyse tüm dünyadaki blok zincir

[146] AB Veri Koruma Hukuku bağlamında sıklıkla kullanılan bu tabirler 'Privacy by design' ve 'Privacy by default' olarak literatüre geçmiştir. Söz gelimi, herhangi bir bankanın müşterisi olunmadığı halde pazarlama faaliyeti kapsamında bireyden veri işleme izni istendiğinde, birey verilerinin işlenmesine izin vermediği sürece sistem otomatik olarak -ve izin alınana dek- 'izin verilmedi' olarak algılar ve bu durum veri koruma hukukuna göre olması gerekendir. Şayet aksi yönde bir sistemin bireyin verisine ulaştığı andan itibaren izinsiz olarak işleyerek ihlalleri başlatacağı aşikardır.

[147] Çekin, s.12.

projelerine bakıldığında bir şekilde kişisel veri içerdikleri görüldüğünden; kişisel verilerin blok zincirde saklanmasına çözümler üretilmesi gerekmektedir. Anonimleştirme yönteminde veriler saklanmadan önce anonimleştirilebilecektir. Ancak KVKK ve GDPR nezdinde tam anonimleştirme kıstaslarının çok güçlü olduğu düşünüldüğünde bu yöntemin de uyum konusunda başarılı olma ihtimali ilk aşamalarda zor olabilecektir.[148]

Öyle ki, KVKK ve GDPR'ın kabul ettiği düzeyde bir anonimleştirmenin yapılabilmesi için, gerçek kişinin adreslenebilirliğinin 'gerçekleşmesi muhtemel' bir durum olmaktan çıkarılması gerekmektedir. Bu kapsamda ağ sorumlusunun, adlar, e-posta adresleri ve diğer belirleyici verilerin haricinde İnternet Prokotolü (IP) ve Medya Erişim Kontrolü (MAC) gibi –çoğu zaman aracısız olarak belirleme yapmaya yaramayan- verilerin de anonim hale getirilmesi beklenmektedir. Kaldı ki, verilerin anonimleştirilmesine yönelik teknolojik gelişmelerin yaşandığı bir ortamda, eşzamanlı olarak big-data uygulamaları da hızla kendini geliştirmekte ve anonim verilerin orijinal hale getirilmesi yönünde de teknikler hızla ve sürekli olarak gelişmektedir. Bir başka deyişle, blok zincir ağları verilerin anonimleştirilmesi yönünde çaba sarf ederken; diğer yandan anonim verilerin çözünebilmesine (orijinal hale getirilmesi) yönelik teknolojiler de ikinci bir mücadele alanı oluşturmaktadır.

Bunun yanı sıra, sistemin bazı temel özellikleri ise zaten veri koruma hukukuna uygun şekildedir. Öyle ki, blok zincir sisteminde veriler sadece doğru anahtara sahip kullanıcıların açabildiği bir şifre -hashing- ile şifrelenmiştir. Bu kendiliğinden şifreleme ile bir gerçek kişiyi işaret eden tüm kişisel veriler, sadece defterde şifrelenmiş halde saklandığında bu bilgilerin toplum tarafından erişilebilir olmaması sağlanabilecek ve KVKK ile GDPR'a ihlalden söz edilemeyecektir. Bir veri sahibi tarafından 'unutulma hakkı'nın kullanımı halinde ise, şifrenin anahtarı silinebilir ve bu durumda dahi talepte bulunan veri sahibinin kişisel verileri çevrimdışı ortamlara yayılmış olsa da şifre anahtarıyla beraber erişilemez duruma gelecektir.[149]

Konuya ilişkin bir başka çözüm önerisi ise işlemi gerçekleştirenlerin belirlendiği kamuya açık anahtarlardaki verilerin anonimleştirilmesi olacaktır.[150]

---

[148] IBM, **GDPR Considerations for Blockchain Solution Architects,** 2018, s.5.
[149] Lee Jim, Erişim tarihi: 20.07.2019
[150] Çekin, s.339.

Ancak buna karşılık, GDPR danışma organı European Data Protection Board nezdinde şifre anahtarı tekniğinin tek başına gerekli korumayı sağlamak adına yeterli olmayacağı, bu işlemin anonimleştirme tekniği olduğu kabul edilmiştir.[151] Bu görüşe göre, veri sorumluları tarafından her ne kadar veri listesinin anonimleştirilmesi için bir veya daha fazla niteleyicinin kaldırılması veya değiştirilmesinin yeterli olduğu varsayılmakta ise de, pek çok örnekte aksi durumun izlenebildiği belirtilmiştir. Söz gelimi eğer niteleyicilerden yarısı değişmemiş ise veya değiştirilmeyen niteleyiciler hala gerçek kişinin belirlenebilirliğini sağlıyor ise sadece ID'nin değiştirilmesi anonimleştirme olarak kabul edilmemektedir.

Tasarımla veri koruma prensibinin blok zincirdeki bir uygulaması olan 'zero-knowledge-proof-process' yöntemi ise bu noktada bir çözüm olabilecektir. Bu yöntemde, işlemlerin içeriğine ve kullanıcılara dair bilgi yer almamakta ve sadece işlemin yapılıp yapılmadığı kayıt altına alınmaktadır.[152] Bu mekanizmada, kanıtlayıcı, doğrulayıcıya verinin içeriğine dair bir bilgi vermeden doğrulayıcıya işlemi ispatlamaya çalışmaktadır. Kanıtlayıcı, nihai sonuca göre -işlenen veri ve süreç bilgisi kullanılmadan- işlem sonucunu iletmektedir. Bu arada doğrulayıcı da sadece sonuçtan haberdar olacaktır ve onay verecektir.

KVKK ve GDPR ile blok zincir uyumu noktasında bir diğer seçenek 'zincir dışı depolama' kavramıdır. Bu depolama türünde gerçek kişiye ait kişisel verilerin normal bir şekilde veri kayıt sistemine kaydedilmesi yerine veri kayıt sistemine kaydedilecek tüm kişisel verilerin tek bir şifre ile merkezi bir veri tabanında tutulması sağlanabilecektir. Bir başka deyişle, blok zincire kayıttan önce basit bir şekilde şifrelenmesi ve şifreleme anahtarlarının kontrolü ile erişimin ve silme işleminin yönetilmesi mümkün olabilecektir. Buradaki kişisel verilere ait girişler için ortak bir güvenin sağlanması için sadece hash değerinin blok zincir ağına işlenmesi ile kişisel veriler ayrı bir koruma altına alınmış olacaktır. Bu durumda da veri sahibinin talebi üzerine depolanan kişisel veriler kolay bir şekilde silinebilecek, şifre anahtarı kullanılamaz hale getirilebilecektir. Her ne kadar bu yöntem ile blok zincirin şeffaflık

[151]European Data Protection Board, **Opinion 05/2014 on Anonymisation Techniques**, 2014, s.21. https://www.pdpjournals.com/docs/88197.pdf Erişim tarihi: 01.07.2019
[152] Çekin, s.339.

ve merkeziyetçi olmama ilkesi zedelenecek ise de, veri sahibinin unutulma hakkını kullanabilmesi sağlanacaktır.[153]

Bir diğer çözüm noktası ise -çalışmamızın *'H.Blok Zincir İşleyişinde Güncel Sorunlar'* başlığında detaylı anlatım bulan- akıllı sözleşmeler aracılığıyla veri korumanın sağlanmasıdır. Akıllı sözleşmeler, kod aracılığıyla kendisine tanımlanan ve koşul odaklı sözleşmelerdir. Belirtilen koşulun yerine getirilmesi ile otomatik olarak devreye girer/işlemleri gerçekleştirirler. Bu noktada, bir akıllı sözleşmenin belirli bir süre sonra o veriye tüm erişim haklarını iptal etmesi/içerikleri silmesi yönünde bir koşul koyularak hazırlanması halinde kişisel verilerin KVKK ve GDPR ile uyumlu şekilde imha sürecine girmesi mümkün olabilecektir.

Ancak belirtilmelidir ki, yukarıda yer verilen tüm bu öneriler blok zincir ağının ortaya çıkışındaki avantajlarından şeffaflığı, merkezilikten uzak dağıtık olması gibi unsurlardan feragat edilmesini gerektiren çözüm önerileridir. Bu nedenle sisteme güvenin azalması ihtimali de daima gözetilerek çözümlerin uygulanması gerekmektedir.

III.SONUÇ

Çalışmamızın konusu; ana hattı itibarıyla her geçen gün ilerleyen ve sınırları olmayan teknolojilere, temel haklarımızdan feragat etmeden uyum sağlamak üzerinedir. Son yıllarda adını Bitcoin ile duyuran blok zincir teknolojisi, merkezi bir idaresi olmaksızın tüm kullanıcılarının sistemi ortak olarak yürüttüğü ve sisteme eşit miktarda hakimiyeti olan bir veri tabanı sistemidir. Kullanıcıları arasında güvenilir bir üçüncü kişinin bulunmasına gerek olmadan transferlerin gerçekleştirilebildiği bu teknoloji, gerek şeffaf -tüm kullanıcılarında eş kayıt defterin bulunuyor olması- ve gerekse düşük maliyet vaat eden yapısıyla son yıllarda hemen her sektörde projelere konu edilmektedir. Ancak bu sistemin yapısı itibarıyla kaydedilen bir verinin geriye dönük olarak silinememesi özelliği ise blok zincir ortamındaki her transfer/veri ile her an tekrar karşılaşabilme potansiyelini de beraberinde getirmektedir. Bir başka deyişle bu teknolojide geçmişteki hiçbir veriden kurtulma şansı bulunmamaktadır.

[153] IBM, s.6.

Geçmişi silip geleceğe prangasız ve özgürce bakabilme hakkı ise veri koruma hukuku bağlamında ‘unutulma hakkı’ olarak tanımlanmaktadır. Bireylerin geçmişlerinde olumsuz olarak anımsadıkları olayların ‘unutmayan dijital hafıza’ sebebiyle bir gün tekrar karşılaşacaklarını bilmek kendilerini özgürce ifade edebilmelerini, davranabilmelerini ve karar alabilmelerine ket vuran bir unsurdur. Unutulma hakkı ise bu noktada bireyin geçmişi ile istemediği bağları koparmasına, bireyin kendini gerçekleştirebilmesine imkan sağlayan bir temel haktır.

Çalışmada incelenen sorunsal ‘gelecek vaat eden fakat unutmayan bir teknoloji’ ile ‘birey olarak kazandığımız bir temel hakkın’ çatışmasıdır. Her ne kadar ilk okunduğunda sorgulanmaksızın temel hakkın ne pahasına olursa olsun korunması ve gerekirse bu teknolojiden feragat edilebileceği akıllara gelse de; çalışmamızın içeriğinde yer verilen çözüm öneriyle ayak uydurulmadığında geride bırakan teknolojiden feragat etmeksizin bireylerin unutulma hakkının -geliştirmeler yapılarak- halel görmeyeceği bir düzlemin de mevcut olabileceği görülmektedir.

Blok zincir teknolojisi, varoluş itibarıyla dağıtık bir yapıya sahiptir. Dolayısıyla veri koruma hukukuna konu veri sorumlusu, veri işleyen tespitinin yapılması son derece güç, hatta kamusal blok zincirde neredeyse imkansız olacaktır.

Kamusal blok zincirde tüm roller irdelendiğinde veri sorumlusunun sahip olduğu niteliklere en yakın olan rolün ‘katılımcılar’ olduğu düşünülse de, dağıtık yapıdaki bir veri tabanına tüm katılımcıların erişiminin mümkün olduğu, bu itibarla tek bir noktadan kontrol edilemeyen bir sistemde herhangi bir kullanıcının veri sorumlusu ilan edilmesi halinde ise hukuken açıklanamayacak bir hadise olacağı aşikardır.

Buna karşılık, KVKK ve GDPR açısından gerek veri sorumlusunun tespiti ve gerekse veriye erişimin ve dağıtımın daha kontrollü yapılabilmesi nedeniyle özel / izinli blok zincirin daha uyumlu olduğu anlaşılmaktadır. Bu anlamda blok zincir teknolojisinde kendini geliştirmek isteyen işletmeler veya şirketler özel / izinli blok zinciri daha çok tercih edebileceklerdir.

KVKK ve GDPR nezdinde blok zincirde saklı kişisel verilerin veri koruma prensiplerine uyumunun sağlanmasında bir diğer çözüm yolu şifre anahtarlarının

silinmesiyle herhangi bir ortamda -çevrimiçi veya çevrimdışı- bulunan kişisel verilerin de kullanılamaz/erişilemez hale getirilmesi olabilecektir.

Bunun yanı sıra veri koruma hukuku çerçevesinde dizayn edilecek akıllı sözleşmeler de bahsi geçen uyumluluk kriterlerini sağlayabilecektir. Bu sözleşmeler kodlarının yazılma aşamasında belirlenen şartların yerine getirilip getirilmemesine göre devreye girmekte/işlemlere başlamaktadır. Bir diğer çözüm önerisi olarak izah edilen şifre anahtarlarının silinmesi eylemi de yine akıllı sözleşmelere tanımlanarak gerçekleştirilebilecektir.

Blok zincir teknolojisinde veri koruma hukukuna uyumun sağlanması adına bir diğer çözüm ise 'Zero-Knowledge-Proof-Process' olacaktır. Doğrulama mekanizmaları arasında veri koruma hukukuna en elverişli olan bu mekanizmada, kanıtlayıcı, doğrulayıcıya verinin içeriğine dair bir bilgi vermeden doğrulayıcıya işlemi ispatlamaya çalışmaktadır. Bir başka deyişle, sistemin içerisine kişisel veri girişi yapılmaksızın sistemin işleyişi sağlanabilecektir.

Netice itibarıyla, blok zincir teknolojisi henüz hem bir teknoloji hem de bir standart olarak, hala başlangıç aşamasındadır ve bu da topluluğun veri koruma hukukunun gereklerine uyumunu sağlamak için ilk aşamada geçici, zamanla da kabul almış kalıcı çözümler geliştirmesini sağlayabilecektir.

Her ne kadar blok zincir teknolojisinin değişmez ve katı yapısı ile gerek KVKK ve gerekse GDPR'ın veri sahibine tanıdığı haklar arasında çatışma yaşanıyor olsa da, yukarıda anlatım bulan çözüm önerileriyle veri koruma hukuku ile uyumlu bir blok zincir teknolojisi mümkün olabilecektir. Unutulmamalıdır ki; içinde bulunduğumuz teknoloji çağı, kişisel verilerin işlenmesi faaliyetlerinde günden güne daha acımasız örnekler ile karşımıza gelmektedir. Fakat yine içinde bulunduğumuz çağın bir gereği de gelişen teknolojileri takip etmek ve hızlı bir şekilde uyum sağlamaktır. Dolayısıyla sadece veri koruma hukukundaki çatışmalarını baz alarak blok zincir teknolojisinin gelişimini durdurmak mümkün olmayacağı gibi, çağa uyum sağlamak adına bireylerin temel hakları arasında değerlendirilen kişisel verilerin korunması hakkı da göz ardı edilemeyecektir.

Mevcut durumda değiştirilemezlik ve şeffaflık prensipleriyle çalışan blok zincir teknolojisi, veri koruma hukukunun taleplerine bütünüyle cevap verememektedir. Ancak buna rağmen, gelecek vaat eden bu teknoloji ile veri koruma hukuku arasındaki sorunlara çözüm olabileceği düşünülen yukarıdaki yöntemler ile temel hakları ihlale izin vermeksizin gelişen teknolojinin takibi de mümkün olabilecek, optimal bir noktada buluşulabilecektir.

KAYNAKÇA

Kitaplar

Elif Küzeci, **Kişisel Verilerin Korunması,** Ankara 2019, 3. Baskı.

Eren Sözüer, **Unutulma Hakkı,** 2017, On İki Levha Yayıncılık, s.159.

Manav Gupta, **'Blokchain for Dummies' IBM Limited Edition,** John Wiley & Sons, 2017.

Meg Leta Jones, **Ctrl+Z The Right to be Forgotten,** 2016, New York University Press, s.190.

Mesut Serdar Çekin, **6698 Sayılı Kişisel Verilerin Korunması Kanunu**, 1. Baskı, 2018.

Viktor Mayer-Schönberger, **Delete-The Virtue of Forgetting In The Digital Age**, Princeton University Press, 2011, ABD, s.10.

Yuval Noah Harari, **21. Yüzyıl için 21 Ders**, 2018, s.58.

Süreli Yayınlar

Anayasa Mahkemesi Kararlar Dergisi, https://www.anayasa.gov.tr/media/4912/kararlar_dergisi_52_5.pdf Erişim tarihi:01.07.2019

Aydın Akgül, **Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı' ve AB Adalet Divanı'nın 'Google Kararı'**, Türkiye Barolar Birliği Dergisi, 2016, s.16.

Dr. Jörg Kaufmann, Blockchain meets Data Privacy (Part 1), The Legal Revolutionary, 2018, s.120-127.

Eric Piscini ve Diğerleri, **'Blockchain: Trust Economy',** Tech Trends 2017, Deloitte University Press, s.94.

Ersin Ünsal ve Ömer Kocaoğlu, Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri, **Avrupa Bilim ve Teknoloji Dergisi,** Sayı: 13, s.61.

Hüseyin Avunduk ve Hakan Aşan, **Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme,** Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi, 2018, s.371.

Kurul Kararları, https://kvkk.gov.tr/Icerik/5419/Kurul-Kararlari Erişim tarihi:19.07.2019

Liu ve Diğerleri, **A Survey on Applications of Game Theory on Blockchain,** IEEE, 2019, s.1.

M. Iansiti ve K. Lakhani, **The Truth About Blockchain,** Harvard Business Review, Vol. 95, No:1, 2017, s.118-127.

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(1) İstanbul Hukuk Mecmuası 315 h ps://doi.org/10.26650/mecmua.2019.77.1.0012 , s.16

Raghu M E ve Ravishankar K C, 'Application of Classical Encryption Techniques for Securing Data-A Threaded Approach', **International Journal on Cybernetics & Informatics (IJCI),** Cilt 4, Sayı 2 (Nisan 2015), s.125.

Sema Yıldız Genç ve Hamza Kadah, Oyun Teorisi ve Nash'in Denge Stratejisi, **Iğdır Üniversitesi Sosyal Bilimler Dergisi,** Sayı:14, Nisan 2018, s.421.

Şerif Dilek, **Blockchain Teknolojisi ve Bitcoin,** SETA Analiz Dergisi, Sayı:231, Şubat 2018, s.8.

Türkay Henkoğlu, **Veri Koruma Kanununun Getirdikleri**, Journal of Current Researches on Social Sciences, 2017, s.242.

Ünsal ve Kocaoğlu, **Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri,** Avrupa Bilim ve Teknoloji Dergisi, Sayı:13, 2018, s.61.

Viktor Mayer Schönberger, **Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing,** Harvard University John F. Kennedy School of Government, Faculty Research Working Papers Series, 2007, s. 5-6.

Diğer Yayınlar

Ahmet Usta ve Serkan Doğantekin, **Blockchain 101,** MediaCat, 2017, s.42.

Anayasa Mahkemesi'nin 24.08.2016 tarihli BB:37/16, N.B.B. kararı, https://www.anayasa.gov.tr/tr/haberler/bireysel-basvuru-basin-duyurulari/unutulma-hakkina-iliskin-nbb-karari-basin-duyurusu/ Erişim tarihi: 01.03.2019

Apple Co-Founder 'Woz' launches blockchain company in Malta, https://www.independent.com.mt/articles/2019-07-18/local-news/Delta-summit-launch-Apple-Co-Founder-Woz-launches-blockchain-company-in-Malta-6736211092 Erişim tarihi: 22.07.2019

Beck ve Diğerleri, **Blockchain-the Gateway to Trust-Free Cryptographic Transactions,** European Conference on Information Systems, 2016, s.4.

Blockchain, https://blockchainhub.net/blockchain-intro/ Erişim tarihi: 01.07.2019

Blockchain and the GDPR (Thematic Report), **The EU Blockchain Observatory and Forum,** 2018, s.32.

Blockchain solutions for a responsible use of the blockchain context of personal data, https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

Blockchain technology is moving into the financial mainstream with IBM and seven European banks, https://www.cnbc.com/2017/06/26/ibm-building-blockchain-for-seven-major-banks-trade-finance.html, Erişim tarihi: 18.06.2019

Blockchain Teknolojisi Türkiye'de İlk Kez Akbank'ta, https://www.akbanklab.com/tr/guncel/basinda-biz/blockchain-teknolojisi-Turkiyede-ilk-kez-akbankta Erişim tarihi: 22.07.2019

Cambridge Electricity Bitcoin Consumption Index, http://www.epe.admin.cam.ac.uk/cambridge-bitcoin-electricity-consumption-index-cbeci Erişim tarihi:20.07.2019

Database, https://www.britannica.com/technology/database Erişim tarihi: 01.02.2019,

Database, https://www.oracle.com/database/what-is-database.html Erişim tarihi: 01.07.2019

Difference Between Hashing and Encryption, https://www.ssl2buy.com/wiki/difference-between-hashing-and-encryption Erişim tarihi: 01.07.2019

Distributed and decentralized databases, https://subscription.packtpub.com/book/application_development/9781787126992/6/ch06lvl1sec26/distributed-and-decentralized-databases Erişim tarihi: 07.06.2019

Elektronik Ticaret Direktifi Çalışma Grubu Raporu, https://ticaret.gov.tr/data/5b87dcea13b8761160fa1832/5ba2e8d35824ddbab72d6e6c477d8c80.pdf, Erişim tarihi:01.07.2019

European Commission, The EU Data Protection and Big Data Factsheet, 2016 https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi3x-f8lezkAhXMpYsKHQyZD38QFjAAegQIBBAC&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fjust%2Fdocument.cfm%3Fdoc_id%3D41523&usg=AOvVaw0ST2KcGgcpQzrQ8t4JTG3F Erişim tarihi: 20.07.2019

European Data Protection Board, **Opinion 1/2010 on the concepts of 'Controller' and 'Processor',** WP 169, 2010, s.31.

European Data Protection Board, WP 225, **Guidelines on the Implementation of the Court of Justice of the European Union Judgement on 'Google Spain and Inc v. Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez'** C-131/12, 2014, s.13-20., https://www.pdpjournals.com/docs/88502.pdf Erişim tarihi: 27.07.2019

European Data Protection Board, Opinion 05/2014 on Anonymisation Techniques , 2014, s.21.,https://www.pdpjournals.com/docs/88197.pdf Erişim tarihi: 01.07.2019

Facebook co-founder: Libra coin would shift power into the wrong hands, https://www.ft.com/content/aa97ad20-91a0-11e9-8ff4-699df1c62544 Erişim tarihi: 23.07.2019

Feng Xia Tian, An agri-food supply chain traceabiliy system for China based on RFID and blockchain technology, Service Systems and Service Management, 13th International Conference on IEEE. 2016, s.3.

Hash, https://techterms.com/definition/hash Erişim tarihi: 01.07.2019

IBM, **GDPR Considerations for Blockchain Solution Architects,** 2018, s.5.

İhracat "Blokzincir" Teknolojisiyle Hızlanacak, https://www.ticaret.gov.tr/haberler/ihracat-blokzincir-teknolojisiyle-hizlanacak Erişim tarihi: 01.07.2019

Judgment of 19.10.2016, Breyer, C-582/14, EU:C:2016:779, p:65 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0582&from=EN Erişim tarihi:20.07.2019

Judgment of 19.12.2018, Fashion ID/ Verbraucherzentrale NRW e.V., C-40/17,EU:C:2019:629,p:26. http://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4401670 Erişim tarihi: 19.07.2019

Judgment of 10.01.2019, G.C., A.F., B.H., E.D. v. Commission nationale de l'informatique et des libertés (CNIL), Google Inc., C-136/17, EU:C:2019:773, p:25,26,27,28.http://curia.europa.eu/juris/document/document.jsf?text=right%2Bto%2Bbe%2Bforgotten&docid=209686&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=4822387#ctx1 Erişim tarihi: 20.07.2019

Judgment of 13.05.2014, Google Spain SL, Google Inc. V. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzales, C-131/12, EU:C:2014:317, p:14.http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4488999 Erişim tarihi: 01.03.2019

Judgment of 10.07.2018, Jehovan todistajat, C-25/17, EU:C:2018:551, p:15. http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4403193 Erişim tarihi: 20.07.2019

Judgment of 08.09.2016, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, C-398/15,EU:C:2017:197, p.24,25,26,27,28. http://curia.europa.eu/juris/document/document.jsf?text=right%2Bto%2Bbe%2Bforgotten&docid=183142&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=4822387#ctx1 Erişim tarihi: 19.07.2019

Judgment of 24.11.2011, Scarlet Extended SA, C-70/10, EU:C:2011:771, p:15,16,17.http://curia.europa.eu/juris/document/document.jsf?text=&docid=115202&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4413010 Erişim tarihi:20.07.2019

Judgment of 05.06.2018, ULD Schleswig Holstein/Wirtschaftsakademie Schleswig Holstein GmbH C-210/16, EU:C:2018:388,p:37, http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=4399480 Erişim tarihi: 19.07.2019

Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf Erişim tarihi: 22.07.2019

Kişisel Verilerin Korunması Kurumu, 'Veri Sorumlusu ve Veri İşleyen' Rehberi, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf Erişim tarihi: 19.07.2019

Lee Jim, **GDPR & Blockchain: At the intersection of data privacy and technology,** BDP International https://www.bdpinternational.com/blog/gdpr-blockchain-at-the-intersection-of-data-privacy-and-technology Erişim tarihi: 20.07.2019

Libra White Paper, https://libra.org/en-US/white-paper/#introduction Erişim tarihi: 20.07.2019

McDonald's, Nestlé and Virgin Media Join Blockchain-based Project for Digital Ads https://bitnewstoday.com/news/mcdonald-s-nestl-and-virgin-media-join-blockchain-based-project-for-digital-ads/ Erişim tarihi: 19.07.2019

Microsoft Azure announces blockchain based identity system, https://www.ledgerinsights.com/microsoft-azure-blockchain-based-digital-identity-ion/ Erişim tarihi: 22.07.2019

Next Generation Blockchain Boosts Speed and Energy Efficiency on Global Scale, https://www.csiro.au/en/News/News-releases/2018/Next-generation-blockchain-boosts-speed-and-energy-efficiency-on-global-scale Erişim tarihi: 07.06.2019

Roberta Filippone, **Blockchain and Individuals Control Over Personal Data in European Data Protection Law**, Master Thesis, Tilburg University Press, 2017, s.28.

Satoshi Nakamoto, **'Bitcoin: A Peer-To-Peer Electronic Cash System'**, 2008, www.bitcoin.org

Samsung And South Korean Enterprises Enter The Blockchain ID Race, https://www.forbes.com/sites/darrynpollock/2019/07/16/samsung-and-south-korean-enterprises-enter-the-blockchain-id-race/#50957e5322b5 Erişim tarihi: 22.07.2019

Tokenized Networks: Web3, the Stateful Web, https://blockchainhub.net/web3-decentralized-web/ Erişim tarihi: 08.03.2018

Top Ten 2018 GDPR Violations & Incidents, https://medium.com/@immuniweb/top-ten-2018-gdpr-violations-incidents-99e45efa01d9 Erişim tarihi: 19.07.2019

TÜBİTAK'tan blok zincirine özel araştırma laboratuvarı, https://webrazzi.com/2017/11/21/tubitak-bilgem-blok-zinciri/ Erişim tarihi: 22.07.2019

Türkiye'nin İlk Finansal Blockchain Projesi Borsa İstanbul Bilişim Teknolojileri Ekibi Tarafından Hayata Geçirildi, https://www.borsaistanbul.com/duyurular/2018/09/05/turkiye-nin-ilk-finansal-blockchain-projesi-borsa-istanbul-bilisim-teknolojileri-ekibi-tarafindan-hayata-gecirildi Erişim tarihi: 22.07.2019

Visa Fact Sheet, https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf Erişim tarihi: 07.06.2019

Web3 Decentralized Web, https://blockchainhub.net/web3-decentralized-web/ Erişim tarihi: 08.03.2018

What is hashing?, https://blockgeeks.com/guides/what-is-hashing/ Erişim tarihi: 01.07.2019

https://www.tutorialspoint.com/Centralized-Database-Management-System Erişim tarihi: 07.06.2019