BLOCKCHAIN
TÜRKİYE

KİŞİSEL VERİLERİN KORUNMASI HUKUKU VE BLOKZİNCİRİ TEKNOLOJİSİ RAPORU

KASIM 2019

Hukuk, Düzenlemeler ve
Kamu İlişkileri Çalışma Grubu

TBV
TÜRKİYE BİLİŞİM VAKFI

KİŞİSEL VERİLERİN KORUNMASI HUKUKU VE BLOKZİNCİRİ TEKNOLOJİSİ RAPORU

KASIM 2019

***

Tasarım ve Grafik Uygulama
TERMİNAL MEDYA LTD. ŞTİ.
Maslak Mah. Bilim Sokak No:5 SUN Plaza Kat:13 Sarıyer/İSTANBUL
0(212) 367 4988 ve 0(532) 643 6959

Editör
ÖZLEM ÖZKAN

Grafik Uygulama
GÜLİSTAN ŞENOL

Baskı
SET POZİTİF MATBAA
Maslak Mah. Ahi Evran Cad. No: 29/A Rentaş İş Mrkz Kapı No: 62
Sarıyer / İSTANBUL
0(212) 286 4933

Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu

SORUMSUZLUK BEYANI

Türkiye Bilişim Vakfı altında çalışmakta olan Blockchain Türkiye Platformu'nun "Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu" tarafından hazırlanan işbu rapor blokzincir teknolojisinin mevcut kişisel verilerin korunması mevzuatı ve uygulamaları bakımından incelenmesinden ibaret olup; teknik kapsam ilgili teknolojinin hukuki açıdan özümsenebilmesi amacıyla yayımlanmıştır. Kişi ve kurumları bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu rapor kamuya açık kaynaklardan yararlanılmış bilgileri içermekte olup, söz konusu bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır.

İÇİNDEKİLER

TÜRKİYE BİLİŞİM VAKFI

Türkiye Bilişim Vakfı, *Türkiye'nin bilgi toplumuna dönüşebilmesi için altyapının oluşturulabilmesine katkıda bulunmak ve bilişim sektörünün ekonomideki payının arttırılması için, bilimsel araştırma ve geliştirme etkinliklerinde bulunarak ekonomik ve sosyal çalışmalar yapmak, projeler üretmek ve uygulamalarını sağlamak amacıyla kurulmuştur.*

BLOCKCHAIN
TÜRKİYE

Blockchain Türkiye Platformu, *Türkiye Bilişim Vakfı (TBV) liderliğinde Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu oluşturmak amacıyla kurulmuştur.*

SUNUŞ

Faruk Eczacıbaşı
Blockchain Türkiye
Yürütme Kurulu Başkanı
Türkiye Bilişim Vakfı
Yönetim Kurulu Başkanı

Türkiye Bilişim Vakfı'nı Mayıs 1995'te kurduğumuzda, kendine çok basit bir misyon belirlemişti; bilgi ve iletişim teknolojilerinin ülkenin verimliliğine katkıda bulunmasını sağlamak. Bugün ister Dördüncü Endüstri Devrimi diyelim, ister bilgi toplumu, gerçek şu ki dünya gittikçe hızlanan bir aşamaya girdi ve bizi de yeni bir düşünme biçimine zorluyor.

Blokzincir, bu yeni düşünce kalıbının en devrimsel sonuçları olacak ürünlerinden biri ve bu teknolojinin anlaşılabilmesi, uygulanabilmesi için, deneyimin kazanılması beklenmeli. Her yeni teknolojide olduğu gibi, blokzincirde de konseptlerle başlayan deneysel süreçlerin pilot aşamalarına, bunların da nihai ürüne dönüşmesi gerekiyor.

Blokzinciri diğer teknolojilerden ayıran en temel özellik ise beraberinde getirdiği sektörler arası konsorsiyumlar, platformlar gibi ortamlarda "birlikte çalışma" ihtiyacı. Yeni bir düşünce kalıbı olarak blokzincir, ekosistemlerin önemini artırırken, teker teker şirketler ve onların ürünlerinden ziyade, bir arada değer yaratmayı başarabilen ekosistemleri ön plana çıkarıyor.

Bu sebepten, Türkiye Bilişim Vakfı olarak 8 Haziran 2018 tarihinde bir adım attık. Blokzincir teknolojisinin Türkiye'de yaygınlaşması, bilinirliği ve kullanımının artırılması, faydalarının araştırılması ve stratejik önceliklerinin saptanması gibi temel hedeflerle, Blockchain Türkiye Platformu'nu (BCTR'yi) hayata geçirdik. Blockchain Türkiye Platformu (BCTR), Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu.

Umuyorum ki dünya, buhar makinesinin icadından bu yana alıştığımız "önce üret, sonra sat" iş modelinden, "birlikte üret, sat ve tüket" (Co-create & Prosume) kavramlarına doğru yolculuğa çıkarken, bu platformun ve ürettiği çalışmaların ülkemize bir faydası dokunsun.

KATKI SAĞLAYAN KURUMLAR

BKM BANKALARARASI KART MERKEZİ

BOĞAZİÇİ VENTURES

BtcTurk

BTS & PARTNERS

CANPOLAT LEGAL

NAZALI

SRP legal
strateji regülasyon politika

TURKCELL

ÖNSÖZ

Dr. Soner Canko
Blockchain Türkiye
Yürütme Kurulu Üyesi

Hukuk, Düzenlemeler ve
Kamu İlişkileri Çalışma
Grubu Sponsoru

Devrimsel bir teknoloji olan blokzincir teknolojisinin iş hayatına verimli ve hızlı bir şekilde entegre edilmesinin sadece teknik anlamdaki gelişmeler ile değil, blokzincir teknolojisinin karakteristik özelliklerini dikkate alarak inşa edilmiş ve bu teknolojiyle uyumlu şekilde çalışan bir hukuki altyapı ile mümkün olabileceğine inanıyoruz.

Blokzincir teknolojisinin özünde bir veri saklama yöntemi olduğu dikkate alındığında, hiç şüphesiz ki Kişisel Verilerin Korunması mevzuatları, blokzincir ile uyumluluğu en önem arz eden mevzuatlardan birisi haline gelmektedir. Hatta blokzincir teknolojisi ve bu hukuk dalındaki mevzuatların birbiriyle uyumlu olmaması halinde bu uyumsuzluğun blokzincir teknolojisinin yaygınlaşmasına sekte vuracağını söylemek yanlış olmayacaktır.

Bu amaçla "Hukuk, Düzenlemeler ve Kamu İlişkileri Çalışma Grubu" olarak blokzincir teknolojisinin ülkemizde yürürlükte bulunan 6698 sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği'nde yürürlükte bulunan Genel Veri Koruma Tüzüğü mevzuatları başta olmak kişisel verilerin korunmasına yönelik mevcut mevzuatlar ile ilişkisini incelemeyi ve iyileştirme önerileri sunmayı hedefledik.

Siz değerli okuyuculara, bu fikirle yola çıkarak yola çıkarak oluşturduğumuz "Kişisel Verilerin Korunması Hukuku ve Blokzincir Teknolojisi Raporu"nu sunmaktan mutluluk duyarız.

YÖNETİCİ ÖZETİ

Geleneksel olarak yetkili otoriteler, arabulucular ve benzeri üçüncü kişilerin tesis etmekte olduğu "güven" olgusu, gelişen teknolojiler ile günümüzde yerini merkeziyetsiz bir yapı olan blokzincir teknolojisine bırakmaktadır. Kişisel veriler de dahil ağ üzerinde tutulan veriler blokzincir teknolojisinin temel bileşenlerinden birini oluşturmakta olup; söz konusu teknoloji bu bakımdan, son zamanlarda kişisel verilerin korunması mevzuatına dair yapılan çalışmaların önemli konularından birini oluşturmakta ve zaman zaman sert eleştiri oklarının da hedefi olmaktadır.

Zira, kişisel verilerin korunmasına dair mevzuat düzenlemeleri temelde, kişisel veri sahiplerinin yasal mevzuat kapsamında kendilerine tanınan haklarına ilişkin başvurularını yöneltebilecekleri ve kişisel veri işleme faaliyetlerini ilgili mevzuat hükümlerinde düzenlenen yükümlülüklere uyumlu şekilde gerçekleştirmekle yükümlü en az bir gerçek veya tüzel kişi veri sorumlusunun mevcudiyeti varsayımına istinaden oluşturulmuş ve uygulamaya alınmıştır. Dolayısıyla, söz konusu yasal düzenlemeler, merkeziyetçi bir yapı üzerine inşa edilmiştir. Oysa blokzincir teknolojisinin temel unsurları arasında yer alan dağıtık ağ yapısı ile blokzincir üzerinde gerçekleştirilen tüm işlemlere ait kayıtlar, tek bir merkezde tutulmak yerine, bir ağ yapısı üzerindeki her bir katılımcıya eşlenik olarak dağıtılmakta ve böylece veri sorumlusu gibi ara aktörler ortadan kaldırılmaktadır. Diğer bir ifadeyle, söz konusu teknoloji merkeziyetsiz bir yapı üzerine kurulmuştur. Temelde yaşanan bu zıtlık, blokzincir teknolojisi ile kişisel verilerin korunmasına dair düzenlemeler arasındaki tansiyonu yükseltmektedir.

Bu kapsamda, işbu Kişisel Verilerin Korunması Hukuku ve Blokzincir Teknolojisi Raporu ile 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü hükümleri bakımından blokzincir teknolojisinin incelenmesi, uyuşmazlık noktalarının tespiti ve mevcut gelişmeler ışığında sunulan çözüm önerilerinin derlenmesi amaçlanmaktadır.

A. GİRİŞ

Geleneksel olarak yetkili otoriteler, arabulucular ve benzeri üçüncü kişilerin tesis etmekte olduğu "güven" olgusu, gelişen teknolojiler ile günümüzde yerini merkeziyetsiz bir yapı olan blokzincir teknolojisine bırakmaktadır. Kriptografi yöntemleri kullanılarak güvenli hale getirilen ve blok adı verilen yapıların birbirlerine bağlanarak sürekli büyüdüğü bir kayıt listesi olan blokzincir, 2008 yılında Stoshi Nakamoto'nun blokzincir algoritmasını yaratması ve blokzinciri kavramsallaştırmasından günümüze kadar büyük bir hızla gelişmiş ve gelişmeye devam etmektedir.[1] Bilgi ve veri transferlerini hızlı ve güvenli bir şekilde gerçekleştirebilen blokzincir teknolojisi, günlük hayatta karşılaşılan önemli sorunları çözüme kavuşturmayı ve halihazırdaki süreçleri optimize etmeyi hedeflemekte olup; söz konusu teknoloji günümüzde pek çok farklı sektörde kullanılmaktadır. Blokzincir teknolojisi bu bakımdan pek çok mevzuatın da kapsamına girmektedir.

İşbu Kişisel Verilerin Korunması Hukuku ve Blokzincir Teknolojisi Raporu'nda **("Rapor")**, 7 Nisan 2016 tarihli ve 29677 sayılı *Resmi Gazete*'de yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu[2] **("KVK Kanunu")** ve 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü[3] **("GDPR")** başta olmak üzere (i) kişisel verilerin korunmasına ilişkin mevzuat düzenlemelerinin blokzincir teknolojisi ile temas eden noktalarına dair detaylı açıklamalara, (ii) mevcut durumdaki olası soru(n)ların tespitine ve (iii) söz konusu olası soru(n)lar hakkındaki çözüm önerilerine yer verilecektir.*

* Avrupa Parlamentosu'nun yayımlamış olduğu "Blockchain and the General Data Protection Regulation" isimli raporda yer alan görüş ve çalışmalara, İşbu Rapor'a ilişkin final versiyonun ilgili Avrupa Parlamentosu çalışmasının yayım tarihinden önce tamamlanması nedeniyle yer verilmemiştir.

[1] Brito, Jerry ve Castilllo, Andrea, Bitcoin A Primer for Policymakers (2013), 1. Basım, Virginia, Mercatus Center George Mason University, s. 3.

[2] 24 Mart 2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu. <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> s.e.t. 27.06.2019.

[3] 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü, <https://gdpr-info.eu/> s.e.t. 27.06.2019.

B. BLOKZİNCİR TEKNOLOJİSİNİN TEMEL UNSURLARI VE BLOKZİNCİR TÜRLERİ

I. Blokzincir Teknolojisi Nedir?

Blokzincir, değer içeren verilerin güvenli ve emin bir şekilde depolanması, bir aracıya ihtiyaç duyulmadan iki taraf arasında verilerin değiş tokuşu ve yönetilmesi için tasarlanmış şeffaf ve doğrulanabilir bir teknolojidir.

II. Blokzincir Teknolojisinin Temel Unsurları

a. Blok Yapısı

Blokzincir kriptografi kullanılarak bağlanan ve güvenli hale getirilen, "blok" adı verilen, sürekli büyüyen bir kayıt listesidir. İlk blok yapısına "başlangıç bloğu (*genesis block*)" adı verilmiştir. Bloklar belli sayıda işlemi barındırırlar ve her blok kendisinden önceki bloğa bağlanarak blokzincire eklenir.

Bir blok temel olarak, o bloğu tanımlayan ve özetini içeren blok başlığından (block header) ve işlem kayıtlarından (*transactions*) oluşmaktadır.[4] Zincir üzerindeki her bir blok, kısmen kendinden önceki bloktan üretilmektedir. Zira, her bir blok kendisinden önceki bloğun özetlenmiş bilgisini içermektedir.

b. Dağıtık Ağ Yapısı

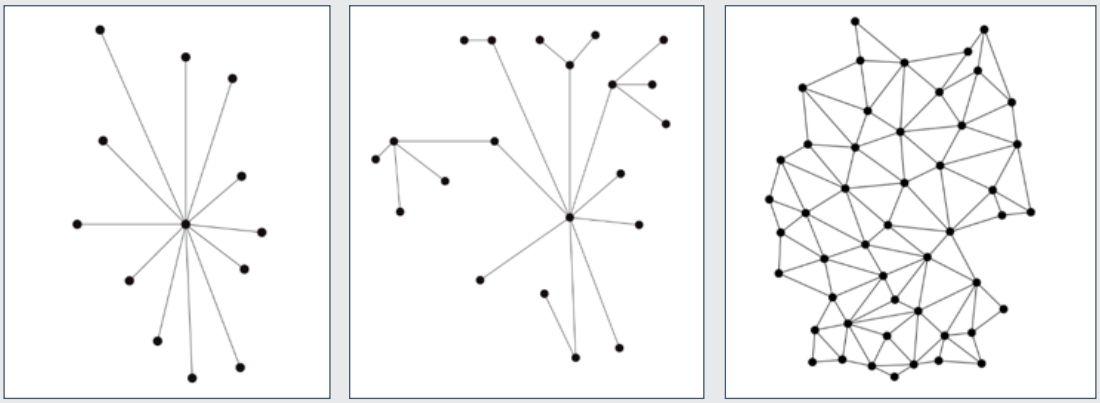
Dağıtık ağ yapısı, blokzincir üzerinde gerçekleştirilen tüm işlemlere ait kayıtların tek bir merkezde tutulması yerine, bir ağ yapısı üzerindeki her bir katılımcıya aynı kayıtların eşlenik olarak dağıtılmasıdır. Tüm kayıtlar katılımcılar tarafından tek bir kayıt sistemine (defter) yazılır ve her bir katılımcıda bu defterin kopyası bulunur. Başka bir ifade ile defter ortaktır ve dağıtıktır. Defter güncellendiğinde ise defterin kopyası tüm katılımcılarda güncellenmiş hali ile bulunur.

Dağıtık ağ yapısının merkeziyetçi bir yapıya oranla daha güvenli olduğu görüşü hakimdir. Bir örnekle[5] açıklayacak olursak, verilerin depolandığı yer bir ev gibi düşünülebilir. Bir kişinin bir eve izinsiz şekilde girebilmesi, gerekli güvenlik önlemlerinin alınmış olması şartıyla çok zordur ancak imkânsız değildir. Blokzincir teknolojisinin dağıtık ağ yapısı sayesinde verilerin tutulduğu veri tabanı milyonlarca parçaya bölünmüş ve bu parçalar binlerce bilgisayara yayılmış hale gelmektedir. Dolayısıyla, verilere izinsiz erişmek isteyen kişinin sadece bir eve girmesi yeterli olmamakta ve bunun yerine veri tabanında bulunan evlerin çoğunluğuna girmesi gerekmektedir.

[4] Ünal, Engin (2018), Bitcoin ve Blockchain Nedir? Nasıl Çalışır?, <https://medium.com/@enginunal/bitcoin-ve-Blokzincir-nedir-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-78d5c9e28095> s.e.t. 27.06.2019.

[5] B. Woolf, Nicky (2017), Everything You Need to Know About Blockchain But Were Too Embarrassed to Ask, <https://medium.com/s/welcome-to-blockchain/everything-you-need-to-know-about-blockchain-but-were-too-embarrassed-to-ask-b3cee3e918f8> s.e.t. 27.06.2019.

Aşağıda tek merkezli ağ, çok merkezli ağ ve dağıtık ağ yapılarının görselleri yer almaktadır.



c. Mutabakat Yapısı

Blokzincir ağındaki verinin eşlenik bir kopyasının, ağ üzerindeki tüm makinelerde olabilmesi için ağ genelinde mutabakat yapılmalıdır. Diğer bir ifadeyle, blokzincir ağında gerçekleşen bir işlemin geçerli olabilmesi için katılımcıların[6] işlemin geçerliliği üzerinde hemfikir olması gerekmektedir.

Blokzincir platformları mutabakat süreci bakımından farklı çözümler sunmaktadır. Örneğin, en popüler blokzincir platformlarından olan Bitcoin[7] ve Ethereum'da[8] emeğin/çalışmanın ispatı (*proof of work*) mutabakat yaklaşımı kullanılmaktadır. Emeğin/çalışmanın ispatı, düğümlerin (nodes) blokzincirine yeni bir blok ekleyebilmek için ortaya koydukları emeği ispat etmeleridir.[9]

d. Değiştirilemezlik

Blokların içindeki verinin fark edilmeksizin değiştirilmesi mümkün değildir. Bunun için "kriptografik özetleme" (*cyrptographic hashing*)[10] ve zaman bilgisi kullanılmaktadır.

[6] Blokzincir türlerine göre mutabakat sürecine dahil olacak katılımcı niteliği ve buna bağlı olarak sayısı değişiklik gösterebilmektedir.

[7] 2008 yılında rumuzu Satoshi Nakamoto olan anonim bir kişi tarafından deneysel olarak ortaya atılmış; herhangi bir merkezi otoriteye bağlı olmaksızın kullanıcılar arasında aracısız olarak değer transferi sağlayan dijital ödeme yöntemidir. Ulusal para birimlerine alternatif olarak ortaya çıkmış ancak henüz Türk hukuku çerçevesinde resmi bir ödeme aracı olarak kabul görmemiştir. Sembolü , kısaltması ise BTC'dir.

[8] Açık kaynak kodlu bir blokzinciri projesi olarak geliştirilen ve herkes tarafından erişilebilir olan Ethereum Sanal Makinası üzerinde faaliyet gösteren blokzinciri platformunu ifade eder.

[9] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 122.

[10] Kriptografik özet (hash): Verileri rastgele bir sayı ve harf dizisine dönüştürmek için algoritmik bir işlem uygulanmasını ifade eder. Böylece, blokzincir ağında işlenecek veri, zincir içerisinde yer edinmesini sağlayan dijital bir parmak izi haline gelir.

Yukarıda bahsedildiği üzere, bloklar yapıları gereği, her biri kendisinden önceki bloğun özetlenmiş bilgisini içermektedir. Dolayısıyla blokzincir ağı üzerindeki bir blok içeriğinin değiştirilebilmesi için hem hedef bloğun hem de ondan sonra gelen tüm blokların değiştirilmesi gerekmektedir. Blokzincir ağındaki bir blokta hata mevcut ise, bu yanlışlığı düzeltmek için yeni bir işlem yapılmasına ihtiyaç bulunmaktadır. Dolayısıyla, örneğin;[11] bir hacker bir bloğu değiştirmeyi başarabilse bile yaptığı her değişiklik anında ve kalıcı olarak görünür olacaktır. Ancak bir blokzincir ağında hesaplama gücünün %50'sinden fazlasını kontrol eden bir madenci grubu tarafından yapılan %51 saldırısında, saldırganlar yeni işlemlerin onaylanmasını engelleyebilmekte ve bazı veya tüm kullanıcılar arasındaki işlemleri durdurabilmektedirler.

III. Blokzincir Türleri

Blokzincir ağları, ağa erişimin herkese açık olup olmamasına göre ikiye ayrılmaktadır:

>> Herkesin erişimine açık olan ağlar; Açık veya Genel (*Public*) Blokzincir Ağları, ve

>> Herkesin erişimine kapalı olan ağlar; Kapalı veya Özel (*Private*) Blokzincir Ağları.

Pratikte genellikle, güvenlik endişesi veya farklı sebeplerle verilerin herkese açık olmasını tercih etmeyen kurumlar, kapalı blokzincir ağlarını tercih etmektedirler.

Açık blokzincir ağlarını ikiye ayırmak mümkündür:

>> **Bütünüyle İzin Gerektirmeyen Blokzincir Ağları**[12]

Bir blokzincir ağına girerek kayıtlı verileri okumak ve bu ağın mutabakat yapısına uyarak, yeni bloklar ekleyebilmek için mutabakat sürecine dahil olmak için izin alınmasını gerektirmeyen ağlara bütünüyle izin gerektirmeyen blokzincir ağları (**"Bütünüyle İzin Gerektirmeyen Blokzincir Ağları")** adı verilmektedir.

Olabildiğince çok kişinin sisteme dahil olması suretiyle ağın daha güvenli olmasının sağlandığı bu ağ türüne Bitcoin platformu örnek verilebilir.

>> **Kısmen İzin Gerektirmeyen Blokzincir Ağları**[13]

Bir blokzincir ağına girerek kayıtlı verileri okumak için izin alınması gerekmemesine rağmen bu ağın mutabakat yapısına uyarak yeni bloklar eklemek ve mutabakat sürecine dahil olmak için izin alınması gereken ağlara kısmen izin gerektirmeyen blokzincir ağları (**"Kısmen İzin Gerektirmeyen Blokzincir Ağları"**) adı verilmektedir.

Bu tür ağlara örnek olarak, sisteme giren herkesin tüm müzik parçalarını dinlediği ancak mutabakat yapısı gereği sadece bağımsız müzisyenlerin parça ekleyebildiği bir blokzincir platformu verilebilecektir.

[11] Song, Jimmy (2018) Why Blockchain is Hard, <https://medium.com/@jimmysong/why-Blockchain-is-hard-60416ea4c5c> s.e.t. 27.06.2019.

[12] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 30. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

[13] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 31-32. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

Kapalı blokzincir ağlarını ikiye ayırmak mümkündür:

>> Kısmen İzin Gerektiren Blokzincir Ağları[14]

Bir blokzincir ağına girerek kayıtlı verileri okumak için izin alınması gereken ancak sonrasında bu ağın mutabakat yapısına uyarak yeni bloklar eklemek ve mutabakat sürecine dahil olmak için izin alınması gerekmeyen ağlara kısmen izin gerektiren blokzincir ağları ("**Kısmen İzin Gerektiren Blokzincir Ağları**") adı verilmektedir.

Amacı, kaydedilen verileri sadece ilgili tarafların erişimine açmak ancak içeriye giren herkesi mutabakat sürecine dahil etmek olan bu tür ağlara, bir bankanın kendi şubeleri arasında havale işlemlerini gerçekleştirmek için kurulmuş bir blokzincir platformu örnek verilebilir.

>> Bütünüyle İzin Gerektiren Blokzincir Ağları[15]

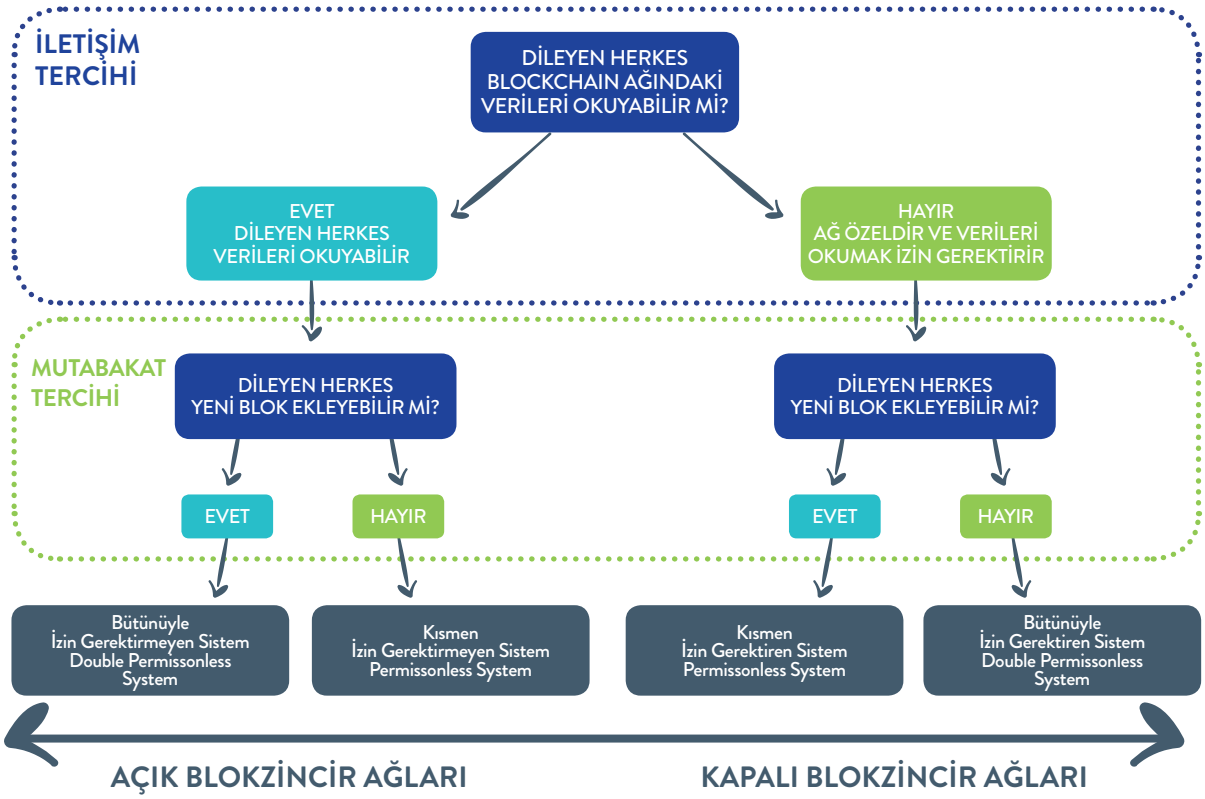
Bir blokzincir ağına girerek kayıtlı verileri okumak için ve sonrasında bu ağın mutabakat yapısına uyarak yeni bloklar eklemek ve mutabakat sürecine dahil olmak için izin alınması gereken ağlara bütünüyle izin gerektiren blokzincir ağları ("**Bütünüyle İzin Gerektiren Blokzincir Ağları**") adı verilir.

Amacı, kaydedilen verileri sadece ilgili tarafların erişimine açmak ve veri erişimine izin verilenler arasından da sadece seçilmiş tarafları mutabakat sürecine dahil etmek olan bu tür ağlara bankalar arasındaki Elektronik Fon Transferi (EFT) işlemlerini gerçekleştirmek için kurulan bir blokzincir platformu örnek olarak verilebilir.

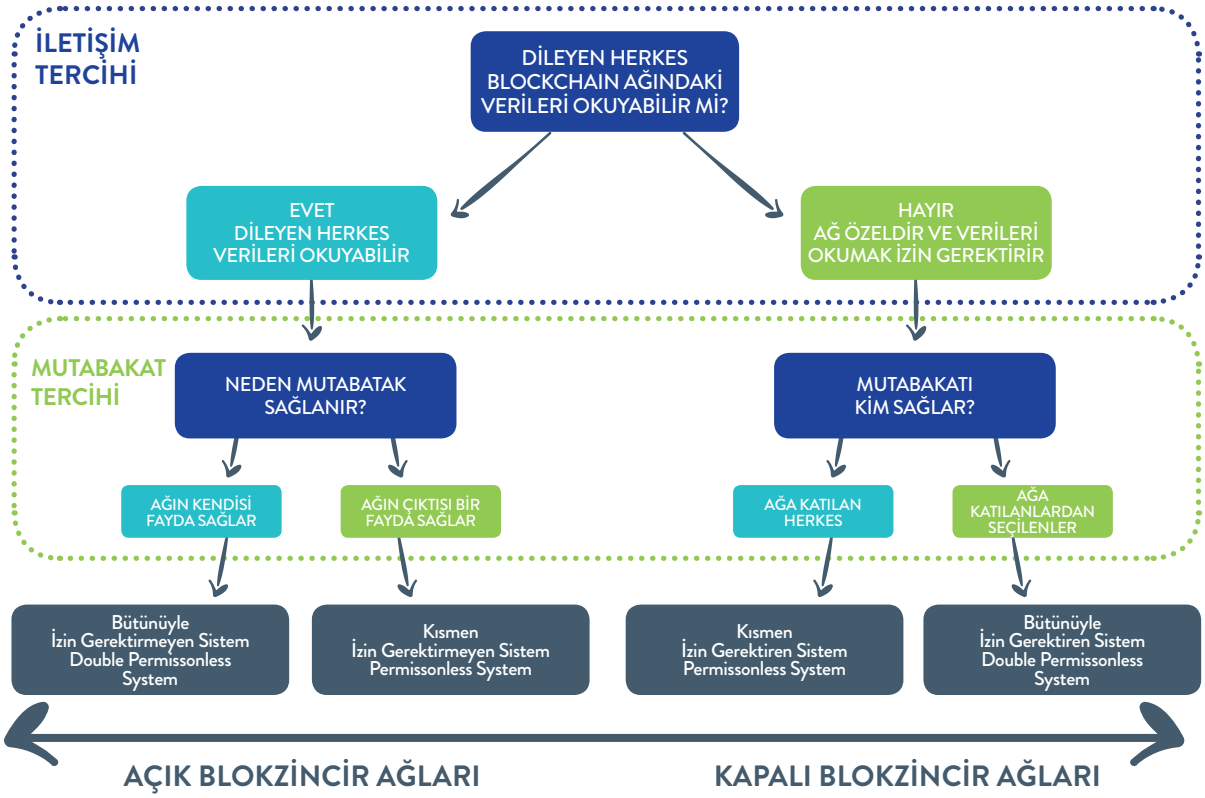
[14] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 33. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

[15] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 33-34. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

Bahsi geçen blokzincir türlerini özetleyen şemayı aşağıda inceleyebilirsiniz.[16]



Mutabakat sistemine katılım sağlanmasına göre blokzincir türlerini özetleyen şema ise ayrıca aşağıdaki görselleştirilmiştir.[17]



[16] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 34. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

[17] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 35. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf

C. KİŞİSEL VERİLERİN KORUNMASI MEVZUATI

I. Kişisel Verilerin Korunması Mevzuatının Tarihçesi

a. Dünya'da Kişisel Verilerin Korunması

Yüzyıllar boyunca Dünya üzerinde yaşanan savaşlar, kıyımlar ve soykırımlar dünya tarihine birer kara leke olarak kazınmıştır. Savunmasız ve suçsuz olan özellikle azınlık gruplar ve ölüme mahkum edilen uluslar, kendi haklarını savunamamış ve adeta bir etnik kıyıma maruz kalmışlardır. Söz konusu anlayış ve muamelere son verilmesi bir zorunluluk haline gelmiş ve öncelikle bazı devletlerin bireysel adımları ile insan haklarına ilişkin bildiriler yayımlanmıştır.

i. İnsan Hakları Evrensel Beyannamesi

Devletlerin, bireylere tanınan hak ve özgürlüklerin güvence altına alınması konusunda ortak paydada buluşmalarının etkisi ile evrensel bir mahkeme ve konu hakkındaki davaların hukuka uygun ve eşitlik ilkesi çerçevesinde sonuca kavuşturulması gerekliliği, İnsan Hakları Evrensel Beyannamesi'nin[18] (**"Beyanname"**) ortaya çıkışına zemin hazırlamıştır. Beyanname, Birleşmiş Milletler (**"BM"**) İnsan Hakları Komisyonu tarafından hazırlanmış olup; BM Genel Kurulu tarafından 10 Aralık 1948 tarihinde kabul edilmiştir. Türkiye ise, 6 Nisan 1949 tarihinde Beyanname'yi kabul eden ülkeler arasında yerini almıştır.[19]

ii. İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi

Beyanname'de yer alan hakların topluca güvence altına alınması için Avrupa Konseyi üyelerinin üzerinde anlaştığı İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (*Avrupa İnsan Hakları Sözleşmesi*) (**"AİHS"**)[20] ise 4 Kasım 1950 tarihinde Roma'da kabul edilmiş ve 3 Eylül 1953 tarihinde yürürlüğe girmiştir. Türkiye, AİHS'ni kabul tarihinde imzalamış ve 10 Mart 1954 tarihli ve 6366 sayılı İnsan Haklarını ve Ana Hürriyetleri Koruma Sözleşmesi ve Buna Ek Protokolün Tasdiki Hakkında Kanun ile onaylayarak iç hukukuna dahil etmiştir.

iii. Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri

Yukarıda bahsedildiği üzere 2. Dünya Savaşı'nın etkileri ve yansımaları hâlâ devam ederken, özellikle azınlık grupların bu dönemde kimliklerinin belirlenmesi ve bu kişilerin fişlenmesinden dolayı zarar görmeleri nedeniyle Dünya'nın her yerinde insan hakları kapsamında kişisel verilerin korunması ile ilgili çalışmalar önem ve hız kazanmıştır. Bu kapsamda, 1980 tarihinde Ekonomik Kalkınma ve İşbirliği Örgütü'nün

[18] Birleşmiş Miletler Genel Kurulu tarafından ilan edilen İnsan Hakları Evrensel Bildirgesi, <http://www.unicankara.org.tr/doc_pdf/h_rigths_turkce.pdf> s.e.t. 27.06.2019.

[19] İnsan Hakları Evrensel Beyannamesi, <https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf> s.e.t. 27.06.2019.

[20] İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme, <https://www.ombudsman.gov.tr/contents/files/891a2--Insan-Haklari-ve-Temel-Ozgurluklerin-Korunmasina-Iliskin-Sozlesme.pdf> s.e.t. 27.06.2019.

(*OECD*) Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri[21], [22] yayımlanmıştır.

iv. 108 Numaralı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Takiben, 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan 108 Numaralı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi ("**108 Numaralı Sözleşme**")[23] 1 Ekim 1985 tarihinde yürürlüğe girmiş ve kişisel verilerin toplanması, işlenmesi, saklanması ve transferi gibi işlemler birtakım kurallara bağlanmıştır.

v. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi

1995 tarihinde ise 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi ("**Direktif**")[24] ile kişisel veri tanımı yapılmış olup; Avrupa Birliği ("**AB**") içinde yeknesak bir veri koruma hukukunun temelini oluşturulmuştur. Tüm AB üyesi ülkeler bu doğrultuda kendi kanunlarını hazırlayarak yürürlüğe koymuştur. Direktif, kişisel verilerin korunması alanında Avrupa coğrafyası ile sınırlı kalmayan ve tüm Dünya'da kabul gören bir çerçeve düzenleme teşkil etmiştir.

vi. GDPR

Çeşitliliği ve kapasitesi artan veri trafiği, toplanan verilerin işlenmesindeki yeni yaklaşımlar ile teknolojideki gelişmeler sonucu yetersiz kalmaya başlayan Direktif hükümlerinin günümüze uyarlanmasına yönelik kapsamlı bir reforma gidilmesi ihtiyacı sonucunda GDPR ortaya çıkmıştır. AB, kişisel verilerin korunması alanında ortaya çıkan ihtiyaçları karşılamak üzere 2012 yılında yeni bir regülasyon çalışması başlatmıştır. Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından hazırlanan GDPR, 14 Nisan 2016 yılında Avrupa Parlamentosu tarafından onaylanmış olup; 25 Mayıs 2018 tarihinde Direktif'i ilga ederek yürürlüğe girmiştir. GDPR, Avrupa'daki gizlilik yasalarında son 20 yıldır yapılan en önemli reform olarak kabul edilmekle beraber, aşağıda detaylı açıklandığı üzere yalnızca AB üye devletleri değil, belli kriterler[25] sağlandığında diğer tüm ülkeleri de kapsamına alan bir düzenlemedir.

[21] Organization for Economic Co-Operation and Development, The OECD Privacy Framework, (2013) <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> s.e.t. 27.06.2019.

[22] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, İlk (Orijinal) Versiyonu, <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> s.e.t. 27.06.2019.

[23] 2016/8576 sayılı onaylanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi, <https://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2016/03/29/KisiselVerilerinOtomatikIslemeTabiTutulmasiKarsisindaBireylerinKorunmasiSozlesmesi.pdf> s.e.t. 27.06.2019.

[24] 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi, <https://kisiselveri.com/9546ec-turkce> s.e.t. 27.06.2019.

[25] GDPR'ın 3'üncü maddesi uyarınca veri sorumlusunun veya veri işleyenin AB'de yerleşik olması veya veri sorumlusunun veya veri işleyenin AB'de yerleşik olmaması ancak AB'deki ilgili kişiyi hedeflemesi veya izlemesi durumunda GDPR uygulanmaktadır.

b. Türkiye'de Kişisel Verilerin Korunması

i. 108 Numaralı Sözleşme

Yukarıda açıklandığı üzere Türkiye, 108 Numaralı Sözleşme'yi 28 Ocak 1981 tarihinde imzalayarak ilgili sözleşmeye taraf ilk ülkelerden biri olarak yerini almıştır.

ii. Türk Ceza Kanunu

Takiben, 12 Ekim 2004 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ("**TCK**") ile kişisel verilerin işlenmesi ile ilgili suçlar belirlenerek, suçun meydana gelmesi halinde hangi yaptırımların uygulanacağı ilk kez kanunlaştırılmıştır.

TCK'daki kişisel verilerin işlenmesi ile ilgili suçlar "Özel Hayat ve Hayatın Gizli Alanına Karşı Suçlar" (md. 132-140) başlıklı dokuzuncu bölümde yer almaktadır. Bu bölümde kişisel verilerle ilgili suçlar; haberleşmenin gizliliğini ihlal (md. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (md. 133), özel hayatın gizliliğini ihlal (md. 134), kişisel verilerin kaydedilmesi (md. 135), verileri hukuka aykırı olarak verme veya ele geçirme (md. 136) ve verileri yok etmeme (md. 138) suçları olarak karşımıza çıkmaktadır. Ayrıca TCK'nın 140'ıncı maddesinde bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik tedbiri uygulanacağı hüküm altına alınmıştır.

iii. 1982 Anayasası

12 Eylül 2010 tarihli 5982 sayılı Kanun'la yapılan Anayasa değişikliği ile Anayasa'da,[26] kişisel verilerin korunmasıyla ilgili detaylı düzenlemelerin kanunla yapılacağı açıkça düzenlenmiş ve ayrıca "kişisel verilerin korunmasını isteme hakkı" anayasal bir hak olarak kabul edilmiştir.[27]

iv. Kişisel Verilerin Korunması Kanunu Tasarısı

Türkiye'de kişisel verilerin korunmasına ilişkin özel bir kanun çıkarmak için ilk kez 1989 yılında bir komisyon oluşturulmuştur. Bu komisyon henüz çalışmalarını tamamlayamadan dağılmıştır.

2000 yılında yeni bir komisyon oluşturulmuş ve bu komisyon üç yıllık çalışmasının neticesinde bir kanun tasarısı hazırlanmıştır. Ancak, hazırlanan tasarı çeşitli nedenlerle kanunlaşamamıştır.

[26] 18 Ekim 1982 tarihinde kabul edilen 9 Kasım 1982 tarihinde yayımlanan 2709 kanun numaralı Türkiye Cumhuriyeti Anayasası, <https://kisiselveri.com/9546ec-turkce> s.e.t. 27.06.2019.

[27] "(Ek fıkra: 12/9/2010-5982/2 md.) 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."

Türkiye'nin AB'ye katılım sürecinde büyük önem taşıyan, yedi ilkeden biri olan, AB müktesebatına uyum koşulu çerçevesinde, kişisel verilerin korunması konusunda yasal bir düzenleme yapılması birçok başlıkta yerine getirilmesi gereken önemli bir koşul olarak ön plana çıkmıştır. 2008 ve 2014 yıllarında, Adalet Bakanlığı öncülüğünde yeni bir tasarı hazırlanarak Türkiye Büyük Millet Meclisi'ne ("**TBMM**") sunulmuşsa da yasama dönemi sona erdiği için ilgili kanun teklifi kadük hale gelmiştir. Yukarıda bahsedildiği üzere Anayasa'da da kişisel verilerin korunmasıyla ilgili detaylı düzenlemelerin kanunla yapılacağı belirtilmektedir. Bu kapsamda, 26 Aralık 2014 tarihinde Kişisel Verilerin Korunması Kanunu Tasarısı[28] TBMM Başkanlığı'na sunulmuştur.

v. 108 Numaralı Sözleşme'nin İç Hukuka Dahil Edilmesi

108 Numaralı Sözleşme, yaklaşık 35 senenin ardından, AB'ye katılım süreci kapsamında 17 Mart 2016 tarihli ve 29656 sayılı *Resmi Gazete*'de yayımlanarak iç hukuka dahil edilmiştir.

vi. KVK Kanunu

26 Aralık 2014 tarihinde TBMM Başkanlığı'na sunulan Kişisel Verilerin Korunması Kanunu Tasarısı, 24 Mart 2016 tarihinde kanunlaşmış ve KVK Kanunu[29] 7 Nisan 2016 tarih ve 29677 sayılı *Resmi Gazete*'de yayımlanarak yürürlüğe girmiştir.

II. KVK Kanunu ve GDPR'ın Uygulama Alanı ve Bölgesel Kapsamı

a. Uygulama Alanı

KVK Kanunu'nun 2'nci maddesi uyarınca, ilgili kanun, kişisel verileri işlenen gerçek kişiler ve bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır.

GDPR ise, kişisel verilerin tamamen ya da kısmen otomatik araçlarla işlenmesi ve kişisel verilerin otomatik araçlar haricinde bir dosyalama sisteminin parçasını oluşturan veya bir dosyalama sisteminin parçasını oluşturması amaçlanan araçlarla işlenmesi faaliyetlerinde uygulanmaktadır.

[28] Kişisel Verilerin Korunması Kanunu Tasarısı, <http://www.adalet.gov.tr/Tasarilar/kisisel_verilerin_korunmasi.pdf> s.e.t. 27.06.2019.

[29] Kişisel Verilerin Korunması Kanunu, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf> s.e.t. 27.06.2019.

b. Bölgesel Kapsam

KVK Kanunu ulusal nitelikte olup, münhasıran Türkiye sınırları içerisinde kişisel veri işleme faaliyetinde bulunan veri sorumluları ve veri işleyenler hakkında uygulanmaktadır.

GDPR ise yalnızca AB üye devletlerinin coğrafi sınırlarını hedef almayıp, bunu aşan bir uygulama alanı öngörmektedir. GDPR'ın bölgesel kapsamı düzenleyen ilgili maddesi, AB içerisinde kurulu olmayan veri sorumluları ve veri işleyenlerin veri işleme faaliyetlerini de ilgilendiren düzenlemeler ihtiva etmektedir.

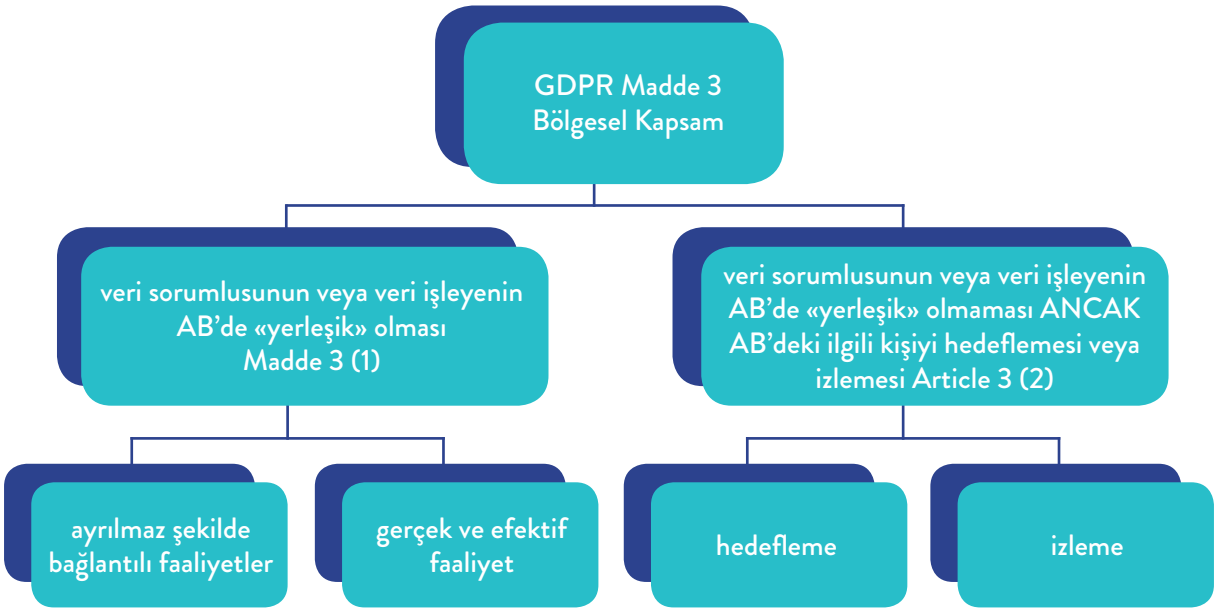
Bölgesel kapsam, GDPR'ın 3'üncü maddesi kapsamında düzenlenmiş olup, buna göre GDPR:

(i) işleme faaliyetinin AB içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, kişisel verilerin bir veri sorumlusu yahut veri işleyenin AB'de yerleşik olan bir kuruluşunun faaliyetleri kapsamında işlenmesi,

(ii) AB sınırları içerisindeki ilgili kişiye ait kişisel verilerin AB'de kurulu olmayan bir veri sorumlusu veya veri işleyen tarafından işlenmesine karşın veri işleme faaliyetlerinin (i) AB içerisindeki ilgili kişiye mal ya da hizmet sunulması veya (ii) ilgili kişinin AB içerisinde gerçekleştirilen davranışlarının gözetlenmesi hususlarıyla alakalı olması, veya

(iii) kişisel verilerin, AB'de kurulmuş olmamasına karşın AB hukukunun uluslararası kamu düzeninden uygulama alanı bulduğu bir ülkede kurulmuş olan veri sorumlusu tarafından işlenmesi

durumlarında uygulanacaktır.[30] Avrupa Veri Koruma Kurulu'nun (European Data Protection Board) ("**EDPB**") yayımlamış olduğu GDPR'ın bölgesel kapsamı ile ilgili 3/2018 sayılı Kılavuzu[31] ("**Kılavuz**") çerçevesinde ilgili madde aşağıdaki alt başlıklar altında değerlendirilebilecektir.



[30] Avrupa Birliği Genel Veri Koruma Tüzüğü Madde 3, <http://www.privacy-regulation.eu/en/article-3-territorial-scope-GDPR.htm> s.e.t. 27.06.2019.

[31] 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bölgesel kapsamı hakkındaki rehber (2018), <https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en> s.e.t. 27.06.2019.

a. Veri Sorumlusunun veya Veri İşleyenin AB'de Yerleşik Olmasına İlişkin Kriterler

i. AB'de yerleşik (establishment) bir kuruluşun varlığı

Yukarıda anıldığı üzere GDPR, kişisel veri işleme faaliyetinin AB içerisinde gerçekleşip gerçekleşmediğine bakılmaksızın, kişisel verilerin bir veri sorumlusu yahut veri işleyenin AB'de yer alan bir kuruluşunun faaliyetleri kapsamında işlenmesi halinde uygulanmaktadır.

Burada "kuruluş" ifadesinden neyin kastedildiği önemlidir. Her ne kadar GDPR kapsamında bir tanım yapılmamış olsa dahi, GDPR'ın başlangıç hükmünde (*Recitals*)[32] yer alan ve Direktif'in giriş 19'uncu maddenin de tekrarı olan 22'nci madde bu noktada yol gösterici bir rol oynamaktadır.[33] Direktif döneminde ilgili madde kapsamında Avrupa Birliği Adalet Divanı'nın ("**ABAD**") vermiş olduğu birçok karar mevcuttur.[34] Bu kapsamda kuruluş ifadesi, etkin ve gerçek bir faaliyetin istikrarlı düzenlemelerle sağlandığı durumu ifade eder ve bunun için bir şubenin veya tüzel kişiliği haiz bir iştirakin varlığı da şart olarak aranmamaktadır. Dolayısıyla, anılan madde kapsamında GDPR, AB sınırları içerisinde kurulmuş olan veri sorumluları ve veri işleyenlerin yanı sıra, AB'de kurulmuş olmamasına karşın, AB dışında kurulmuş olan şirketlerin iştiraklerinin ve şubelerinin ve AB'de bir çalışanı olan veya mümessili olan şirketlerin veri işleme faaliyetlerine uygulanabilecektir.

ii. Kişisel veri işleme faaliyetinin ilgili kuruluşun faaliyetleri ile ilişkili olması

Kuruluş şartının varlığı halinde, ilgili veri işleme faaliyetlerinin söz konusu kuruluşun faaliyetleri kapsamında gerçekleştirilip gerçekleştirilmediği kriteri incelenmelidir. Kılavuz uyarınca EDPB, ilgili veri işleme faaliyetlerinin bir veri sorumlusu yahut veri işleyenin AB'de yerleşik bir kuruluşunun faaliyetleri ile ilişkili olup olmadığının somut olaya göre değerlendirilmesi gerektiğini ancak burada korumanın etkin olarak uygulanabilmesi için dar yorum yapılmaması gerektiğini savunmaktadır.[35] Dolayısıyla, söz konusu bağ incelenirken çok geniş yorum yapılmamalı ve ilgili veri sorumlusunun veya veri işleyenin yalnızca AB sınırları içerisinde bir ticari faaliyetinin olması sebebiyle AB veri koruma düzenlemelerine tabi olmayacağı sonucuna varılabilecektir.[36]

[32] GDPR'ın giriş kısmında yer alan düzenlemeler GDPR hükümlerinin anlamına ve uygulanmasına ilişkin tereddütlere düşülmesi durumunda ABAD tarafından hüküm tesis edilmesi amacıyla düzenlenmiştir.

[33] GDPR Başlangıç Hükmü 22, <https://gdpr-info.eu/recitals/no-22/> s.e.t. 27.06.2019.

[34] Judgment of the Court, 1 Ekim 2015, C-230/24, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, paragraf 31, <http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN> s.e.t. 27.06.2019.

[35] A.g.e paragraf 25 ve ABAD, 25 Haziran 2013, C-131/12, Google Spain SL-Google Inc./Agencia Española de Protección de Datos-Mario Costeja González, <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN> s.e.t. 27.06.2019.

[36] Çalışma Grubu 29, 8/2010 sayılı ABAD'ın Google Spain kararının ışığındaki yürürlükteki yasalarla ilgili görüşünün güncel versiyonu, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640614> s.e.t. 27.06.2019.

Burada AB sınırları dışında kurulmuş olan veri sorumlusu veya veri işleyen ile AB sınırları içindeki kuruluşu arasındaki ilişkinin tespitinde, AB'den gelir elde edip etmediği de değerlendirme kriterleri arasında yer almaktadır. Bu kapsamda EDPB, AB dışında kurulu veri sorumlularını ve veri işleyenleri, kişisel veri işleme faaliyetlerinin yukarıda belirtilen kriterler kapsamında AB içerisindeki yapılanmaları ile ilişkili olup olmadığını tespit etmeye teşvik etmektedir.[37] Ayrıca, AB mevzuatı kapsamında veri sorumlularına veya işleyenlere getirilen yükümlülüklerin veri sorumlusu ve veri işleyen bakımından da ayrı ayrı yorumlanması gerekmektedir. Örneğin; AB'de kurulu bir veri işleyen, veri işleme faaliyetleri bakımından AB mevzuatında veri işleyen için düzenlenen hükümlere uyumlu olarak hareket etmelidir.

>> **Örneğin;** ABAD, 2014 yılında verdiği kararda[38] Amerika'da yerleşik Google Inc. tarafından yürütülen arama motoru faaliyetlerinin, Google Spain'in reklam faaliyetleri ile ayrılmaz bir bağ içerisinde olduğunu (*inextricably linked*) belirterek, Google Inc.'i AB'de "yerleşik" olarak kabul etmiştir.

Yapılan değerlendirme sonucunda, AB içerisinde kurulup kurulmadığına ve AB içerisinde mutlaka bir iştiraki yahut şubesi olup olmadığına bakılmaksızın, etkin ve istikrarlı bir uygulama ile AB'deki faaliyeti bakımından kişisel veri işlediğine karar verilen veri sorumluları ve veri işleyenler bakımından ilgili GDPR hükümleri uygulanacaktır.[39]

iii. Kişisel veri işleme faaliyetlerinin AB sınırları içerisinde gerçekleşip geçekleştirilmediğine bakılmaması

GDPR'ın bölgesel kapsamı bakımından değerlendirmede önemli olan veri işleyenin veya veri sorumlusunun AB'de kurulmuş olması veya yukarıda değinildiği üzere AB'de ticari olarak bir varlığının olmasıdır. Bu kapsamda veri sorumlusunun, veri işleyenin veya bunların kuruluşlarının AB'de olması ve verilerin bunların AB'deki faaliyetleri ile ilişkilendirilebilmesi yeterli olup; veri işleme faaliyetlerinin kendisinin AB içerisinde gerçekleşmesi GDPR'ın uygulanması için aranan bir şart değildir.

GDPR'a tabi olan bir veri sorumlusunun, AB dışında bulunan ve GDPR'a tabi olmayan bir veri işleyeninin AB'deki ilgili kişinin kişisel verilerini faaliyeti bakımından kullanmayı seçmesi durumunda, veri sorumlusunun, söz konusu veri işleyenin GDPR'a uygun olarak işlemesini sözleşme veya başka bir yasal işlemle güvence altına alması gerekecektir ve AB'nin yurt dışına veri aktarımı düzenlemelerine uyması gerekecektir.[40]

[37] 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bölgesel kapsamı hakkındaki rehber.

[38] ABAD, 25 Haziran 2013, C-131/12, Google Spain SL-Google Inc./Agencia Española de Protección de Datos-Mario Costeja González, <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN> s.e.t. 27.06.2019.

[39] 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bölgesel kapsamı hakkındaki rehber.

[40] 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bölgesel kapsamı hakkındaki rehber.

b. AB'de Yerleşik Olmayan Veri Sorumlularının veya Veri İşleyenlerin Kişisel Veri İşleme Faaliyetlerinin İlgili Kişinin AB İçerisinde Gerçekleştirilen Davranışlarının Gözetlenmesi Hususları ile İlgili Olmasına İlişkin Kriterler

i. Verisi işlenen gerçek kişinin AB içerisinde bulunması

"AB içerisindeki kişiler" ifadesinden anlaşılması gereken AB sınırları içerisinde bulunan gerçek kişilerdir. Vatandaşlık, ikametgâh yahut sair hukuki nitelendirmeler burada bir önem arz etmemektedir. Bu yaklaşım, GDPR'ın başlangıç hükmünün 14'üncü maddesinin birinci bendinde düzenlenen "uyruğu yahut ikamet yeri her neresi olursa olsun" ibaresinde de anlaşılabilmektedir.[41]

ii. İşleme faaliyetlerinin AB içerisindeki ilgili kişiye mal ya da hizmet sunulması ile ilgili olarak (hedeflenerek) gerçekleştirilmesi

Kişisel veri işleme faaliyetlerinin, AB'deki ilgili kişiye mal ya da hizmet sunulması ile alakalı olarak (AB'deki kişilerin hedeflenerek) gerçekleştirilmesi durumlarında, GDPR hükümlerinin uygulanması söz konusu olacaktır. Bu noktada "AB içerisindeki ilgili kişiye mal ya da hizmet sunulması" ifadesinin kapsamının da ayrıca açıklığa kavuşturulması gerekmektedir. AB içerisinde yerleşik olmayan bir veri sorumlusu veya veri işleyenin, AB içindeki herhangi bir kişiye mal veya ve hizmet sunup sunmadığının belirlenmesine ilişkin ölçütler GDPR'ın giriş bölümünde yer alan 23'üncü maddesi[42] kapsamında açıklanmıştır.

İlgili giriş maddesi uyarınca, GDPR'ın üçüncü maddesi çerçevesinde bir mal veya hizmet sunumundan bahsedilebilmesi için, veri sorumlusunun veya veri işleyenin, bilinçli olarak özellikle AB içindeki kişilere mal veya hizmet sunmaya yönelik açık bir iradesinin mevcut olması gerekmektedir. Bu kapsamda, AB içerisindeki ilgili kişi tarafından, yalnızca veri sorumlusuna veya veri işleyene ait internet sitesine, e-posta adresine yahut sair iletişim bilgilerine erişilebiliyor olması, yukarıda bahsi geçen açık iradeyi ortaya koyan unsurlardan biri olarak değerlendirilecek olup; AB üyesi devletlerden bir veya daha fazlasında geçerli olan bir dilin veya para biriminin bahse konu dilde mal veya hizmet siparişi verilmesi ihtimali kapsamında kullanılması ve AB içerisindeki müşterilerin veya kullanıcıların hedeflenmesi, veri sorumlusu veya veri işleyenin yukarıda açıklanan nitelikte bir bilinçli iradeye sahip olduğunun göstergesi olarak kabul edilmiştir. Ancak belirtmek gerekir ki, GDPR'ın ilgili giriş maddesinde yer alan unsurlar sınırlı sayıda değil, örnek teşkil etmesi adına sayılmıştır.

GDPR'ın giriş bölümünde yer alan 23'üncü ve 24'üncü maddeleri uyarınca, AB içerisindeki ilgili kişiye mal ya da hizmet sunulduğunun kabulü için yalnızca işletmenin internet sitesine AB'den erişilebiliyor olması yeterli değildir. İlgili işletmenin faaliyetlerinin AB içerisindeki ilgili kişilere yönelik mal ve hizmet sunumu ile ilgili olduğu açıkça tespit edilebilmelidir.

[41] GDPR'ın Başlangıç Hükmü 14 <https://gdpr-info.eu/recitals/no-14/> s.e.t. 27.06.2019.
[42] GDPR'ın Başlangıç Hükmü 23, <https://gdpr-info.eu/recitals/no-23/> s.e.t. 27.06.2019.

Yukarıdaki açıklamalar kapsamında aşağıdaki kriterler bir işletmenin GDPR'a tabi olup olmadığının belirlenmesinde önemli rol oynamaktadır:[43]

- AB üyesi bir devletin dilinin ya da para biriminin kullanılması, bu dilde sipariş verilmesinin mümkün olması,
- AB içerisindeki kullanıcıların ya da müşterilerin hedef olarak gösterilmesi,
- Bir arama motoruna AB içerisindeki ilgili kişinin işletmenin internet sitesine erişimini kolaylaştırmak için reklam verilmesi/ödeme yapılması,
- Faaliyetlerin uluslararası niteliği,
- Uluslararası alan kodlu telefon numaralarının sunulması,
- AB üyesi devletin ülke alan adı uzantısı (.eu, .fr vb.) kullanımı, ve
- Çeşitli AB üyesi devletlerde ikamet eden müşterilerden oluşan müşteri tabanından söz edilmesi.

iii. Kişisel veri işleme faaliyetlerinin AB içerisindeki ilgili kişiye mal ya da hizmet sunulması ile ilgili olarak gerçekleştirilmesi

AB'de yerleşik olmayan bir veri sorumlusu veya veri işleyen tarafından ilgili kişinin AB içindeki davranışlarının gözetlenmesi/izlenmesi ve buna bağlı olarak kişisel verilerin işlenmesi halinde de GDPR hükümleri uygulama alanı bulacaktır. EDPB, bilinçli olarak ve yeniden kullanmak saikiyle AB'deki bir kişinin davranışlarının izlenmesini (*monitoring*) bu kapsamda yorumlamakta olup; yayımlamış olduğu Kılavuz'da ise davranışsal reklam, konum takibi, çerezlerle yahut diğer takip teknolojileri ile çevrimiçi takip, kişisel diyet ve sağlık analitik servisleri, pazar araştırmaları ve şahısların profili üzerinden diğer davranışsal çalışma ile kişilerin sağlık durumunun izlenmesi ve düzenli şekilde raporlanması faaliyetlerini ilgili kişinin izlenmesine örnek olarak göstermiştir.[44]

c. AB Hukukunun Uluslararası Kamu Düzeninden Uygulama Alanı Bulduğu Bir Ülkede Kurulma Kriterleri

Kişisel verilerin, AB'de kurulmuş olmamasına karşın AB hukukunun uluslararası kamu düzeninden uygulama alanı bulduğu bir ülkede kurulmuş olan veri sorumlusu tarafından işlenmesi halinde de GDPR uygulama alanı bulmaktadır.

[43] Belirtilen kriterler sınırlı ya da bağlayıcı olmamakla birlikte AB dışındaki bir işletmenin GDPR'a tabi olup olmadığı her somut olay kapsamında ayrı olarak değerlendirilecektir.

[44] GDPR'ın Başlangıç Hükmü 30, <https://gdpr-info.eu/recitals/no-30/> s.e.t. 27.06.2019.

✣ Blokzincir Teknolojisinin KVK Kanunu ve GDPR'ın Uygulama Alanı ve Bölgesel Kapsamı Bakımından Değerlendirilmesi

Yukarıdaki açıklamalar ışığında, blokzincir teknolojisinde kişisel verilerin yalnızca bir merkez veya bir merkez grubu tarafından değil, sisteme dahil olan herkes tarafından kayıt altına alındığı açıktır.[45] Bu sistemde belirlenen kuralları ve bu kurallar dahilinde üretilen kayıt zincirinin herkese dağıtılması öncelikli olup, ayrıca tarafların birbirini tanımasına gerek bulunmamaktadır. Bu doğrultuda, blokzincir ağındaki tüm verilerin kopyasına sahip olan ana işlevli düğümler (*masternode*), özellikle Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda dünyanın her yerinde olabilirler. Bu nedenle, söz konusu tam işlevli düğümlerin hangi ülkede oldukları ve/veya hangi ülkenin mevzuatının bölgesel alanı/tabiyeti içerisinde olduklarının tespiti oldukça güçtür. Bu noktada, uygulanacak hukuk bakımından ne GDPR'ın ne de KVK Kanunu'nun sözleşme serbestisine tabi olmadığının; diğer bir ifadeyle ilgili mevzuat kapsamına giren her durum için söz konusu mevzuat hükümlerinin doğrudan uygulanacağının ayrıca altını çizmek isteriz.

Ayrıca, yukarıda detaylarına yer verildiği üzere, özellikle GDPR'ın bölgesel kapsamının çok geniş yorumlanması, bilhassa Açık Blokzincir Ağları'nın neredeyse tamamına söz konusu mevzuatın uygulanması sonucuna yol açacaktır. İlgi aktörlerin bu kapsamda GDPR'da düzenlenen yükümlülüklerin tamamını yerine getirmesi bekleneceği değerlendirilmektedir.

Öte yandan, ilgili mevzuatların doğrudan uygulama alanı bulması nedeniyle, özellikle Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda veri sorumluları ve veri işleyenlerin dünyanın her yerinde olabileceğinden bahisle, aynı anda birden çok veri koruma mevzuatına uyumlu hareket etme yükümlülüğü de ortaya çıkabilecektir.

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'ın uygulama alanı ve bölgesel kapsamı bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

Blokzincir ağ yapılarına hangi ülke hukuku uygulanacaktır?

Birden çok ülke hukukunun aynı anda uygulanması mümkün müdür?

[45] Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi, s. 23 ila 25.

III. Kişisel Veri

a. Kişisel Veri

KVK Kanunu'nun 3'üncü maddesinin (d) fıkrası uyarınca kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. KVK Kanunu kapsamında bir kişisel veriden söz edebilmek için, verinin bir gerçek kişiye ilişkin olması ve bu kişinin belirli ya da belirlenebilir nitelikte olması gerekmektedir. Buna tanıma göre kişisel veri, gerçek kişiye ilişkin olup; doğrudan tüzel kişilere ilişkin veriler kişisel veri tanımı ve dolayısıyla KVK Kanunu kapsamında değerlendirilmemektedir.[46]

Kişisel veri, ilgili kişinin doğrudan kimliğini gösterebileceği gibi, o kişinin kimliğini doğrudan göstermemekle birlikte, herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm bilgileri kapsamaktadır. Buna göre, yalnızca bir gerçek kişinin, adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmişi, fotoğrafı, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobileri, tercihleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.[47] KVK Kanunu'nda hangi bilgilerin kişisel veri olarak kabul edileceğine ilişkin sınırlı sayım yoluna gidilmediğinden, kapsamının genişletilmesi mümkündür. Bu noktada önemli olan, söz konusu verinin ilgili kişiyi tekilleştirmesidir ve dolayısıyla tanımlayabilmesidir.

KVK Kanunu'nda ayrıca kişisel verilerden farklı olarak "özel nitelikli kişisel veri" ayrımına gidilmiştir. Özel nitelikli kişisel veriler ise, öğrenilmesi halinde ilgili kişi hakkında ayrımcılık yapılmasına veya mağduriyete neden olabilecek nitelikteki verilerdir. Bu nedenle, diğer kişisel verilere göre çok daha sıkı şekilde korunmaları gerekmektedir. Özel nitelikli kişisel veriler ilgili kişinin açık rızasının varlığı ile ya da KVK Kanunu'nda sayılan sınırlı hallerde işlenebilmektedir. KVK Kanunu'nun 6'ncı maddesi kapsamında düzenlenen özel nitelikli kişisel veriler ise, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri olarak sınırlı sayıda listelenmiştir. KVK Kanunu'nda, özel nitelikli kişisel veriler arasında da bir ayrım yapmıştır. Buna göre, sağlık ve cinsel hayata ilişkin kişisel veriler ile bunlar dışındaki özel nitelikli kişisel verilerin, açık rıza olmaksızın işlenme şartları farklı düzenlenmiştir.[48]

[46] Şirketin ticaret unvanı ya da adresi gibi tüzel kişiliğe ilişkin bilgiler (bir gerçek kişiyle ilişkilendirilebilecekleri durumlar haricinde) kişisel veri sayılmayacaktır.

[47] Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanun'da Yer Alan Terimler, <https://www.kvkk.gov.tr/SharedFolderServerCMSFiles/7452edd6-9ce1-4988-9cfc-95b3758fbd1b.pdf> s.e.t. 27.06.2019.

[48] KVK Kanunu'na göre, özel nitelikli kişisel verilerin işlenmesi, ilgili kişinin açık rızası dışında aşağıdaki hallerde mümkündür; sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, ancak kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel veriler, ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebilmektedir.

GDPR'da ise kişisel veri tanımı, KVK Kanunu'na nazaran daha kapsamlı ve daha açık olarak düzenlenmiştir. Buna göre kişisel veri, belirli veya özellikle isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktördeki belirleyiciler vasıtasıyla doğrudan veya dolaylı şekilde belirlenebilir bir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmıştır.[49]

GDPR'ın başlangıç hükmü 30'da[50] çevrimiçi tanımlayıcı unsurlar kavramına da açıklık getirilerek; gerçek kişilerin cihazları, uygulamaları, aletleri ve protokolleri gibi internet protokol adresleri (*internet protocol address*) (**"IP"**) ve çerez veya diğer radyo frekansı tanımlama etiketleri gibi tanımlayıcılarla ilişkilendirilebilir unsurlardan bahsedilmiştir. Bu doğrultuda, özellikle özgün tanımlayıcı ya da sunucular tarafından verilen bilgilerle birleştirildiğinde gerçek kişilerin profillerini yaratmak ve onları tanımlamak için kullanıldığından, IP adreslerinin ve çerezlerin de GDPR hükümleri uyarınca kişisel veriler kapsamında yer aldığı açıkça düzenlenmiştir.

Nitekim, Alman Federal Yüksek Mahkemesi (*Bundesgerichtshof*), davacı Breyer'in Almanya Adalet ve Tüketicinin Korunması Bakanlığı'nın (*Bundesministerium für Justiz und Verbraucherschutz*) internet sitesini ziyaretine ilişkin olarak IP adresinin kaydının silinmesi talebine binaen önüne gelen davada, internet sitesi sahibinin/işletenin, ziyaretçinin belirlenebilirliği noktasında üçüncü kişinin (somut durumda internet servis sağlayıcısının) elindeki ek veriye ihtiyaç duyması halinde IP adreslerinin kişisel veri olarak nitelendirilip nitelendirilemeyeceği hususunda ABAD'ın görüşüne başvurmuştur.

ABAD ise, 19 Ekim 2016 tarihli Patrick Breyer v. Almanya Kararı'nda,[51] veri sorumlusunun kişisel ilgili kişinin IP adreslerini, IP adreslerinin sahibi kişiler ile ilişkilendirebilecek araçlara doğrudan sahip olmadığı hallerde bile, dinamik IP adreslerinin kişisel veri olarak değerlendirilmesi gerektiği sonucuna ulaşmıştır.

ABAD kararında, internet site sahibinin (somut durumda Almanya Adalet ve Tüketicinin Korunması Bakanlığı) toplamış olduğu dinamik IP adresi verisinin kişisel veri olduğunu ifade etmiştir. ABAD ayrıca bir verinin kişisel veri olarak değerlendirilebilmesi için doğrudan ya da dolaylı olarak bir kişiyle ilişkilendirilebilmesi gerekliliğine işaret etmiş; dolayısıyla internet site operatörünün elindeki IP adresinin mutlak olarak kişisel veri olarak nitelendirilemeyeceğini belirtmiştir. İlgili kararda ayrıca, her bir somut durumun kendi içerisinde değerlendirilmesi gerekliliğine atıf yapılmış ve karara konu uyuşmazlıkta ilgili kişinin belirlenebilmesi açısından dinamik IP adresi ile internet servis sağlayıcısı tarafından tutulan ilave bilgilerin birleştirilebilmesi imkânına da önem atfedilmiştir.[52]

[49] GDPR'ın 4'üncü maddesi, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> s.e.t. 27.06.2019.

[50] GDPR'ın Başlangıç Hükmü 30, <https://gdpr-info.eu/recitals/no-30/> s.e.t. 27.06.2019.

[51] Dr. Munz, Martin, Hickman, Tim ve Goetz Matthias, (2016), Court confirms that IP addresses are personal data in some cases, White and Case, <https://www.whitecase.com/publications/alert/court-confirms-ip-addresses-are-personal-data-some-cases> s.e.t. 27.06.2019.

[52] A.g.e.

Yukarıdaki açıklamalara ek olarak GDPR'da, "takma adlı veri" (*pseudonymous*) adlı bir kavrama da yer verilmiştir. Takma ad kullanımı veya rumuzlaştırma olarak da kullanılan söz konusu süreç GDPR'da, ilave bilgilerin (örneğin; şifre çözme anahtarı) teknik ve idari önlemler alınarak belirli veya belirlenebilir bir ilgili kişi ile ilişkilendirilemeyecek şekilde ayrı olarak muhafaza edilmesi şartlarının varlığı halinde, kişisel verilerin ilave bilgiler kullanılmaksızın belirli bir ilgili kişi ile ilişkilendirilemeyecek şekilde işlenmesi olarak tanımlanmaktadır.[53] GDPR uyarınca bu veriler, kişisel verilerin doğrudan tanımlayıcı unsurları olarak sayılmamaktadır. Dolayısıyla ayrı olarak tutulan ek bilgiler olmadan, veri ile bir gerçek kişi arasında bağlantı kurmak mümkün olamayacaktır. Ayrıca, GDPR'ın başlangıç hükmü 28[54] uyarınca, söz konusu ilgili kişiye karşı riskin minimize edilebilmesi ve veri sorumluları ile veri işleyenlerin veri koruma yükümlülüklerini yerine getirmelerinde yardımcı olması bakımından kişisel verilerin rumuzlaştırılması önerilmektedir.

Özel nitelikli kişisel veriler bakımından ise GDPR kapsamında listelenmiş özel nitelikteki kişisel veriler ile KVK Kanunu'nda listelenmiş söz konusu veriler paralellik göstermektedir. Buna göre, GDPR kapsamında özel nitelikli kişisel veriler, (i) ırk veya etnik köken, (ii) siyasi görüş, (iii) dini veya felsefi inançlar, (iv) sendika üyeliği, (v) genetik veriler, (vi) biyometrik veriler, (vii) sağlık verileri veya (viii) cinsel yaşam veya cinsel eğilime ilişkin veriler olarak sınırlı sayıda listelenmiştir.

✣ Blokzincir Ağındaki Verilerin KVK Kanunu ve GDPR Bakımından Değerlendirilmesi

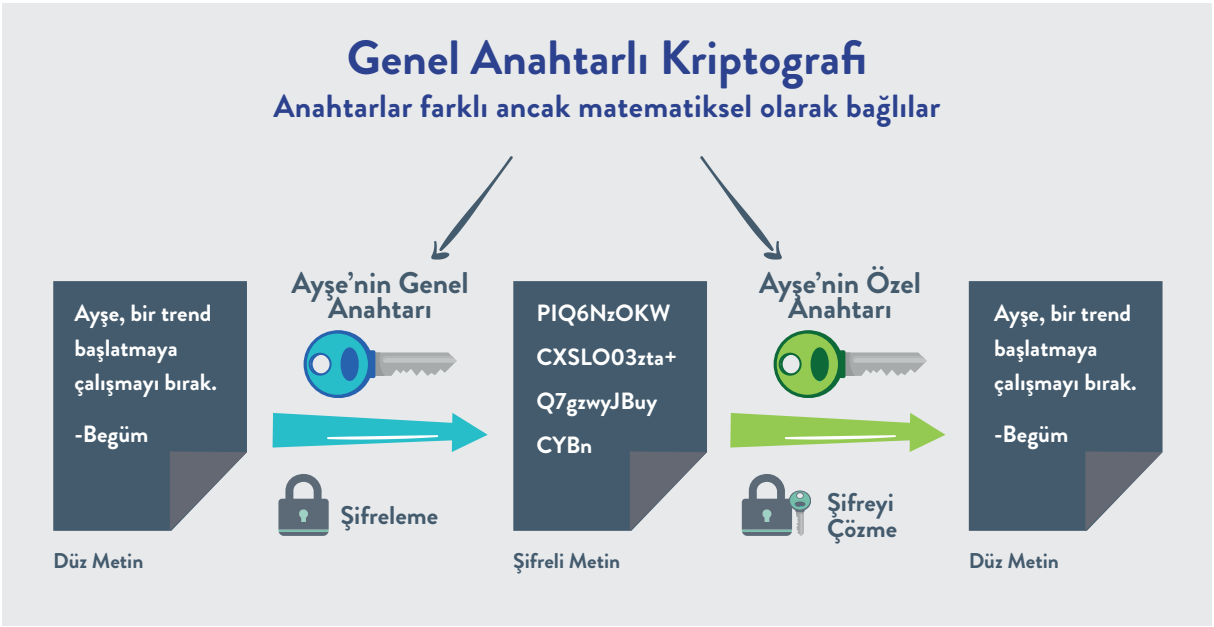
Blokzincir ağları üzerindeki verilerin kişisel veri olarak değerlendirilmesi halinde, GDPR ve KVK Kanunu başta olmak üzere ilgili kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin uygulanacağı şüphesizdir. Bu nedenle, öncelikle blokzincir ağındaki verilerin yukarıdaki açıklamalarımız kapsamında kişisel veri olarak nitelendirilip nitelendirilemeyeceği tespit edilmelidir. Bu doğrultuda, öncelikle blokzincir teknolojisindeki bazı kavramlar açıklanacak olup; takiben ağ üzerindeki veriler, kişisel veri tanımı bakımından değerlendirilecektir.

Dağıtık defter teknolojisi (*distributed ledger technology*) ("**DLT**"), iki basamaklı doğrulama sistemine sahip asimetrik bir şifreleme sistemine dayanmaktadır.[55] Her bir kullanıcı bir özel anahtar (*private key*) ve bir genel anahtar (*public key*) aracılığıyla asimetrik şifreleme sistemini kullanmaktadır. Genel anahtar, işlemleri etkinleştirmek için başkalarıyla paylaşılan hesap numaralarına benzeyen anahtardır. Özel anahtar ise, başkalarıyla paylaşılmaması gereken ve parolaya benzeyen anahtardır.

[53] Maldoff, Gabe (2016), Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization, iapp, <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/> s.e.t. 27.06.2019.

[54] GDPR'ın Başlangıç Hükmü 28, <https://gdpr-info.eu/recitals/no-28/> s.e.t. 27.06.2019.

[55] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, EDPL, <https://edpl.lexxion.eu/article edpl/2018/1/6> s.e.t. 27.06.2019.



Blokzincir teknolojisinde veriler (i) düz metin olarak (in plain text), (ii) şifreleme (encrypted) metoduyla veya (iii) kriptografik özetleme yöntemleriyle depolanmaktadır.

Şifreleme yönteminde anahtarlar yardımıyla bir veri, blokzincirde saklanırken şifreleme (log-out) ve şifreyi açma (log-in) olarak iki yönlü bir işleve sahiptir. Bitcoin gibi SHA-256 algoritmasını[56] kullanan kriptografik özetleme yöntemi ise, tek yönlü bir işlevi yerine getirir.

Blokzincirde depolanan verilerin potansiyel olarak kişisel veri sayılabilmesi hususunda işlem verileri ve genel anahtar kavramlarının tartışması önemi haizdir. GDPR ve KVK Kanunu uyumu sebebiyle işlem verileri ve genel anahtar kavramları sırasıyla aşağıda açıklanmıştır.

i. İşlem Verileri

İşlem verileri, doğrudan işlemlerin bir sonucu olarak elde edilen bilgilerdir. Genellikle söz konusu işlemle ilgili zaman, yer, fiyat, ödeme yöntemleri, iskonto değerleri ve miktarları tanımlayan bir referans verisidir.[57]

Şifreleme yönteminde veri, doğru anahtarlarla tekrardan ulaşılabilir bir seviyede olacağı için anonim veri olarak kabul edilmemektedir. İlgili kişinin dolaylı olarak tanımlanabileceği ve böylece kendi başına bir anonimleştirme tekniği olarak değerlendirilemeyeceği göz önüne alındığında şifreleme, AB veri koruma rejimine göre bir takma ad kullanımı olarak kabul edilmektedir.[58] Dolayısıyla, şifreleme

[56] SHA-2 altındaki 6 kriptografik özetleme algoritma setinden bir tanesidir. SHA-256, Bitcoin madenciliğindeki emeğin ispatının hesaplanmasında ve Bitcoin adresi oluşturma işlemlerinde kullanılır. Bilinen kriptolama fonksiyonları arasında en yüksek güvenliğe sahip olanlardan biridir.

[57] Transactional Data, What does Transactional Data mean?, <https://www.techopedia.com/definition/30367/transactional-data> s.e.t. 11.07.2019.

[58] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, GDPR's Material Scope: Does Data Stored on a Blockchain Qualify as Personal Data, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s. 22.

yöntemi ile ağda depolanan veriler, takma adlı veriler olarak değerlendirilmekte ve ilgili kişilerin söz konusu verileri, belirlenebilir olduğu için kişisel veri olarak kabul edilmektedir.

KVK Kanunu kapsamında takma adlı veri kavramına yer verilmemektedir. Ancak, ilgili otoritenin mevzuatın düzenlenmesi ve yorumlanması bakımında AB mevzuatını esas aldığı göz önünde bulundurulduğunda, takma adlı verilerin de kişisel veri olarak değerlendirilebileceği öngörülmektedir. Ancak, söz konusu kavrama KVK Kanunu'nda açıkça yer verilmemesi, blokzincir teknolojisinin Türk hukukuna uygulanması açısından belirsizlik teşkil edebilecektir. Yukarıda detaylarına yer verildiği üzere, GDPR ve dolayısıyla AB mevzuatı bakımından takma adlı verilerin kişisel veri olarak kabul edileceği hususu netleştirilmiştir.

Paralel şekilde, kriptografik özetleme işlemi yapılan veriler GDPR'a göre kişisel veri olarak nitelendirilmektedir.[59] Tersine işlem yapılamayan tek yönlü bir kriptografik özetleme işlevi, şifreleme yerine daha güçlü gizlilik garantileri sunabilse de verilerin GDPR bakımından kişisel veri olarak nitelendirilmelerinin önüne geçilemeyecektir. Direktif'in 29'uncu maddesi uyarınca, kişisel verilerin korunması ile ilgili bağımsız danışmanlık hizmeti sunan ve AB üye devletlerinin Direktif'in veri koruma kurallarına göre uyumlulaştırılması için yardımcı olan 29. Madde Çalışma Grubu (*Article 29 Working Party*) ("**29. Madde Çalışma Grubu**")[60], kriptografik özetleme yönteminin, veri setini ilgili kişi ile ilişkilendirmenin hâlâ mümkün olması nedeniyle anonimleştirme değil; takma adlandırma tekniği ile oluşturulduğuna dair kesin görüştedir.[61]

Böylece, şifrelenmiş veya kriptografik özetleme işleminden geçmiş işlem verilerinin GDPR kapsamında kişisel veri olarak kabul edileceği sonucuna varılabilmektedir. Tekrar önemle belirtmek gerekir ki, takma adlı veri kavramı GDPR açısından işlem verilerini kişisel veri saysa da KVK Kanunu'nda ilgili tanıma yer verilmediği veya ilgili otorite tarafından henüz konuya ilişkin bir karar veya görüş açıklanmadığı için konu hakkında nihai ve mutabakat sağlanmış bir görüş mevcut değildir.

[59] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, Introduction, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s. 17.

[60] Article 29 Working Party, 'Opinion 04/2014 on Anonymisation Techniques' (2014) 0829/14/EN, 20. 25 Mayıs 2018 tarihinden itibaren, 29. Madde Çalışma Grubu lağvedilmiştir ve yerine Avrupa Veri Koruma Kurulu (European Data Protection Board) kurulmuştur.

[61] 05/2014 sayılı Anonimleştirme Tekniklerine İlişkin Görüş (2014), Çalışma Grubu 29, Executive Summary, <https://www.pdpjournals.com/docs/88197.pdf> s.e.t. 27.06.2019, s. 3.

ii. Genel Anahtar

Genel anahtarlar, işlem veya iletişim amacıyla gerçek veya tüzel bir kişinin takma adlı veri olarak tanımlanmasına izin veren bir harf ve sayı dizisidir.[62] Adres ve isim bilgilerini bünyelerinde barındırdıkları için anonim olarak kabul edilmeyen; takma adlı veri olarak tanımlanan verilerdir. Ayrıca akademik araştırmalar, genel anahtarların IP adreslerine kadar izlenebileceği ve böylece ilgili kişinin belirlenebileceği görüş birliğindedir.[63]

GDPR kapsamında, ilave veri setleri ile birleştirildiğinde bir gerçek kişinin adreslenebildiği takma adlı verilerin, kişisel veri olarak nitelendirildiğinden kuşku duyulmamaktadır.[64] Öte yandan, yukarıda detaylı olarak bahsedildiği üzere kullanıcının internete bağlandığı zamanlarda, internet servis sağlayıcısı tarafından geçici olarak atanan ve değişken olan dinamik IP adresleri de kişisel veri olarak sınıflandırmıştır.[65] Öte yandan, işlem verileri bakımından açıklandığı üzere, KVK Kanunu'nda ilgili tanıma yer verilmediği veya ilgili otorite tarafından henüz konuya ilişkin bir karar veya görüş açıklanmadığı için konu hakkında nihai ve mutabakat sağlanmış bir görüş mevcut değildir.

Sonuç olarak, genel anahtarların da tıpkı işlem verileri gibi kişisel veri niteliği taşıdığı değerlendirilmektedir. Önemle belirtmek gerekir ki, işlem verilerinin aksine genel anahtarlar blokzincirin dışında depolanamamaktadır. Zira, genel anahtarlar, blokzincir teknolojisinin en temel unsurlarındandır ve bir işlemin doğrulanması için gerekli olan "meta verilerin" bir parçasını oluştururlar. Bu nedenle genel anahtarlara ilişkin mevzuat uyumlu çözümlerin sunulması, işlem verilerine nazaran daha güçtür.

iii. Tersine Çevrilebilir Şekilde Şifrelenmiş Veriler (Reversibly Encrypted Data)

Tersine çevrilebilir şifreleme, bir veri parçasının içeriğinin anlaşılamayacak şekilde karıştırılması anlamına gelmektedir. Yalnızca şifreleme anahtarına sahip olan kişi verinin şifresini çözebilir. Simetrik şifreleme (şifreleme ve şifreyi açma için aynı anahtar kullanılır) ve asimetrik şifreleme (yukarıda bahsedilen genel/özel anahtar şifreleme olarak da adlandırılan farklı anahtarlar kullanılır) gibi çeşitli tersine çevrilebilir şifreleme türleri mevcuttur.[66]

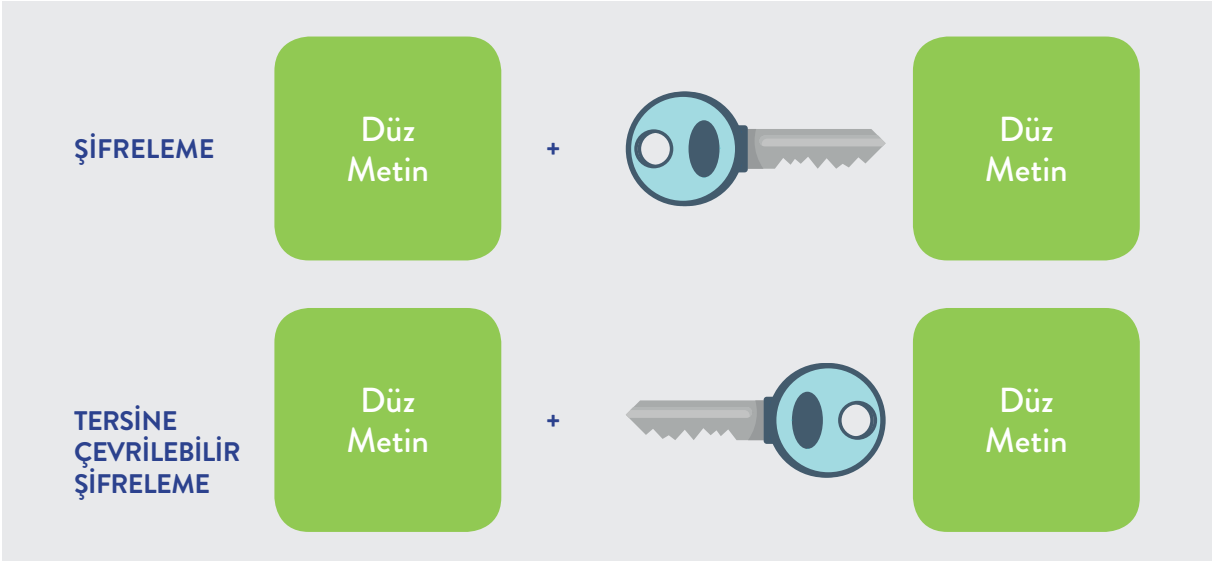
[62] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, Public Key, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019.

[63] Biryukov, Alex, Khovratovich, Dmitry ve Pustogarov, Ivan (2014), Deanonymisation of Clients in Bitcoin P2P Network, University of Luxemburg, <https://orbilu.uni.lu/bitstream/10993/18679/1/Ccsfp614s-biryukovATS.pdf> s.e.t. 27.06.2019.

[64] GDPR'ın Başlangıç Hükmü 26, <https://gdpr-info.eu/recitals/no-26/> s.e.t. 27.06.2019.

[65] ABAD, 12 Mayıs 2016, C 582/14, Patrick Breyer ve Bundesrepublik Deutschland, <http://curia.europa.eu/juris/document document.jsf?docid=178241&doclang=EN> s.e.t. 27.06.2019.

[66] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019.



Kişisel veriler üzerinde güçlü şifreleme teknikleri kullanılsa dahi, bu teknikler ile verilerin tam olarak anonimleştirildiğinden bahsedilemeyecektir. Zira, söz konusu teknikler ile kişisel veriler yalnızca takma adlı verilere dönüştürülmektedir. Kişisel veri, anahtar vasıtasıyla tersine çevrilebilir olduğu için ilgili kişi hakkında bazı bilgileri ortaya çıkarabilmektedir.

Özetlemek gerekir ise, genel anahtarlar, işlem verileri ve tersine çevrilebilir şekilde şifrelenmiş veriler çoğu zaman kişisel veri olarak kabul edilmekte ve blokzincir ağında kullanılmaları halinde KVK Kanunu ve GDPR hükümleri ile uyumlu şekilde işlenmeleri gerekmektedir.

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan kişisel veri kavramı bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

Kriptografik özetleme işlemi yapılan veri, kişisel veri midir?

Şifrelenmiş veri, kişisel veri midir?

Blokzincir ağ yapısında gerçekleştirilen her bir işlem, kişisel veri işleme faaliyeti midir?

IV. Kişisel Verilerin İşlenmesi

a. Kişisel Verilerin İşlenmesi

KVK Kanunu'nun 3'üncü maddesinin (e) bendi uyarınca; kişisel verilerin işlenmesi, kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir. Dolayısıyla, kişisel verilerin ilk defa elde edilmesiyle başlayan bir süreç ve devamındaki her türlü işleme, veri işleme olarak tanımlanmıştır.

Kişisel verilerin işlenmesi bakımından ise KVK Kanunu'nun 4'üncü maddesi kapsamında bazı temel ilkeler ortaya konmuştur. Buna göre, kişisel veriler (i) hukuka ve dürüstlük kurallarına uygun olmalı, (ii) doğru ve gerektiğinde güncel olmalı, (iii) belirli, açık ve meşru amaçlar için işlenmeli, (iv) işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olmalı ve (v) ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

GDPR kapsamında ise, kişisel verilerin işlenmesine ilişkin şartlar 5'inci maddede düzenlenmiştir.

GDPR, kişisel verilerin işlenmesi faaliyeti ancak aşağıdaki şartlardan en az biri geçerli olduğunda hukuka uygun olduğuna hükmetmiştir:

- İlgili kişinin bir veya birden fazla sayıda belirli/spesifik amaca yönelik olarak kişisel verilerin işlenmesine onay vermesi,
- ilgili kişinin taraf olduğu bir sözleşmenin uygulanması veya sözleşme yapılmadan önce ilgili kişinin talebi üzerine adımlar atılması için veri işleme faaliyetinin gerekli olması,
- veri sorumlusunun tabi olduğu bir yasal yükümlülüğe uyum sağlanması amacıyla veri işleme faaliyetinin gerekli olması,
- ilgili kişinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile veri işleme faaliyetinin gerekli olması,
- kamu yararı kapsamındaki bir görevin yerine getirilmesi veya veri sorumlusuna verilen resmi yetkinin uygulanması hususunda veri işleme faaliyetinin gerekli olması ve
- özellikle ilgili kişinin çocuk olması halinde ilgili kişinin kişisel verilerinin korunmasını gerektiren menfaatleri veya temel hak ve özgürlüklerinin bir veri sorumlusu veya üçüncü bir kişi tarafından gözetilen meşru menfaatlerine göre daha ağır olması halinde, söz konusu menfaatler doğrultusunda veri işleme faaliyetinin gerekli olmasıdır. Bu istisnası ise kamu kurumları tarafından görevlerinin yerine getirilmesi hususunda gerçekleştirilen veri işleme faaliyetinde uygulanmamasıdır.

b. Otomatik İşleme (Automated Processing)

Otomatik işleme kavramı, KVK Kanunu'nda tanımlanmamış olmasına rağmen, Kişisel Verileri Koruma Kurumu ("**Kurum**") tarafından yayımlanan Kişisel Verilerin Korunması ve Uygulaması Rehberi'de[67] söz konusu tanıma yer verilmiştir. İlgili rehber kapsamında otomatik olarak veri işlenmesi, bilgisayar, telefon, saat vb. işlemci sahibi cihazlar tarafından yerine getirilen, yazılım veya donanım özellikleri aracılığıyla önceden hazırlanan algoritmalar kapsamında insan müdahalesi olmadan kendiliğinden gerçekleşen işleme faaliyeti anlamına gelmektedir.

Paralel şekilde, GDPR kapsamında da söz konusu tanıma açıkça yer verilmemiştir. Öte yandan, Ekonomik Kalkınma ve İşbirliği Örgütü (*Organisation for Economic Co-operation and Development*) tarafından otomatik işleme, insan müdahalesi ya da yardımı konusundaki ihtiyacı asgari seviyeye indiren, kendi aralarında bağlantılı ve etkileşimli elektrikli veya elektronik bir sistem tarafından gerçekleştirilen veri işleme faaliyeti olarak tanımlanmıştır.[68]

Bazı tıbbi tedavilerde profillemenin belli gruplanmış özelliklerin esas alınarak makine öğrenimi metodu vasıtasıyla hastaların sağlığı hakkında tahminde bulunmak veya belirli bir hasta için bir tedavinin başarılı olma ihtimalini hesaplamak amacıyla kullanılması otomatik işlemeye örnek verilebilecektir.[69]

✣ Blokzincir Ağlarında Veri İşleme Faaliyetlerinin KVK Kanunu ve GDPR Bakımından Değerlendirilmesi

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan kişisel verinin işlenmesi bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

Blokzincir ağlarında gerçekleştirilen her bir işlem kişisel veri işleme faaliyeti midir?

[67] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi> s.e.t. 27.06.2019.

[68] OECD, İstatistik terimler sözlüğü, Otomatik Veri İşleme, <https://stats.oecd.org/glossary/detail.asp?ID=4370> s.e.t. 27.06.2019.

[69] Information Commisioner's Office ("ico"), <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/> s.e.t. 27.06.2019.

V. Kişisel Verilerin Aktarılması

KVK Kanunu'nun 8'inci maddesi uyarınca, ilgili kişinin açık rızası olmaksızın kişisel veriler aktarılamaz. Ancak yukarıda belirtildiği üzere, kişisel verilerin ilgili kişiden açık rızanın temin edilmesine gerek kalmadan işlenmesi için KVK Kanunu'nun 5'inci maddesinin 2'nci fıkrasındaki istisnaların gerçekleşmesi gerekmektedir. KVK Kanunu'nun 8'inci maddesinin 2'nci fıkrasının (b) bendi uyarınca, yeterli önlemler alınmak kaydıyla, yine yukarıda belirtildiği üzere, KVK Kanunu'nun 6'ncı maddesinin 3'üncü fıkrasında yer alan özel nitelikli kişisel veriler için açık rızanın temin edilmesine gerek duyulmamasına ilişkin istisnanın kişisel verilerin aktarılmasında da geçerli olduğu belirtilmiştir.

KVK Kanunu'nun 9'uncu maddesi uyarınca kişisel verilerin yurt dışına aktarılması için açık rızasının temin edilmesi gerekmektedir. Ancak kişisel verilerin işlenmesinde ve özel nitelikli kişisel verilerin işlenmesinde açık rızanın temin edilmesinin gerekli olmadığı hallerden birinin varlığı halinde ve kişisel verinin aktarıldığı yabancı ülkede;

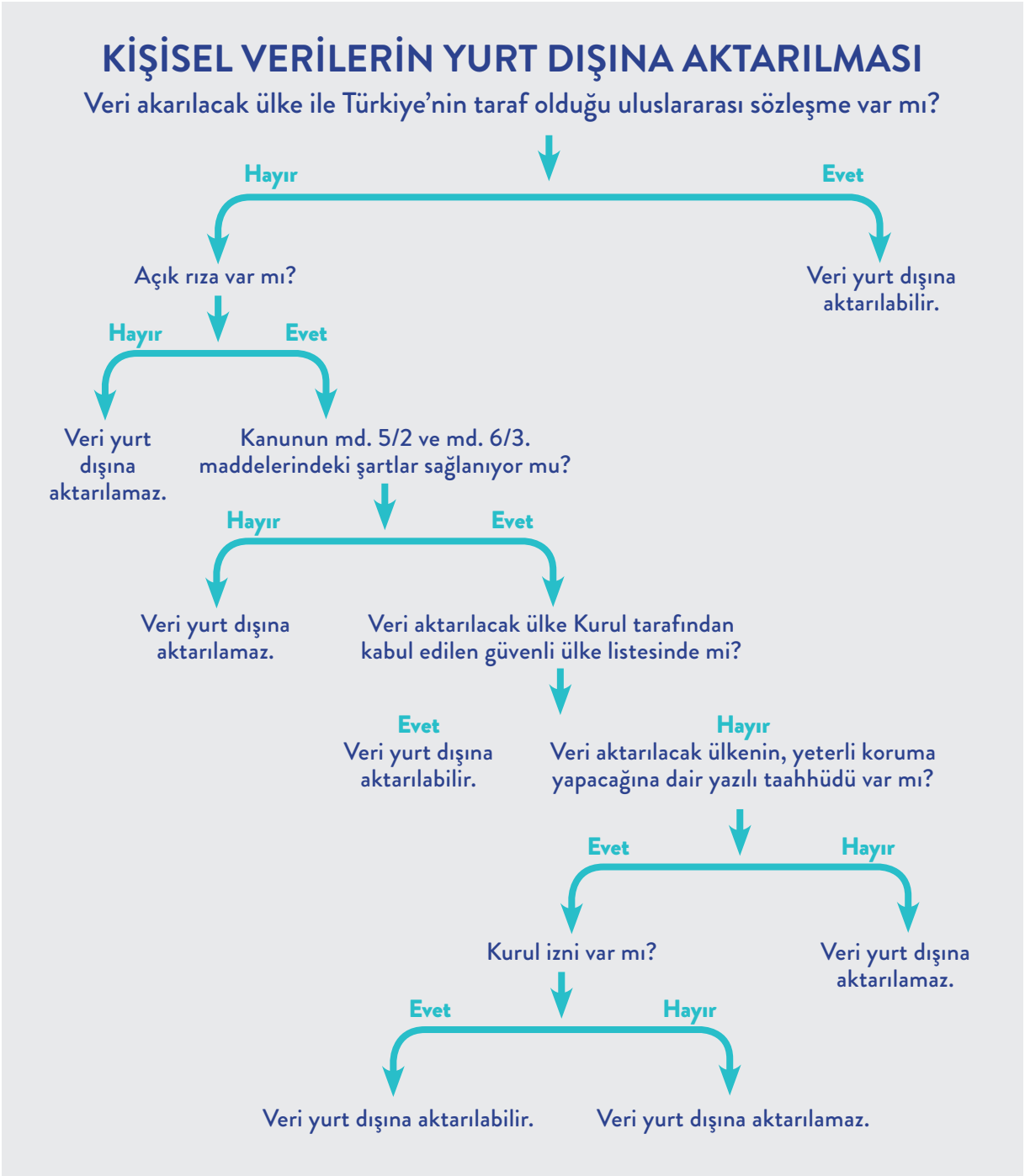
(a) Yeterli korumanın bulunması,[70]

(b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurul'un izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

KVK Kanunu'nun 9'uncu maddesinde Kurul'a, Türkiye'den yurt dışına yapılacak olan veri aktarımlarında Türkiye Cumhuriyeti'nin veya ilgili kişinin menfaatlerinin ciddi bir şekilde zarar görme ihtimali olduğunun tespit edilmesi halinde, bu veri aktarımını onaylama veya yasaklama imkânı verilmiştir.[71] Dolayısıyla Türkiye Cumhuriyeti'nin veya ilgili kişinin menfaatlerinin ciddi bir şekilde zarar görme ihtimali olması halinde, Türkiye'den yurt dışına yapılacak tüm veri aktarımları gerekli görüldüğü takdirde Kurul'un onayına tabi olabilecektir.

[70] Yeterli korumanın bulunduğu ülkeler Kurul tarafından belirlenerek ilan edilmesi gerekmektedir ancak henüz böyle bir liste ilan edilmemiştir.

[71] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılması Rehberi, <https://kvkk.gov.tr/yayinlar K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20YURTDI%C5%9EINA%20AKTARILMASI.pdf> s.e.t. 27.06.2019.



>> Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurumu ve kuruluşunun görüşü alınarak Kurul'un izniyle yurt dışına aktarılabilir.

GDPR'ın 44'üncü ila 49'uncu maddelerinde, üçüncü ülkeye veya uluslararası bir kuruluşa, şirketler topluluğu içerisinde gerçekleştirilen veri aktarımı da dahil olmak üzere, yapılacak olan kişisel veri aktarımı detaylı olarak düzenlenmiştir. Kişisel verilerin yurt dışına aktarılması için verinin aktarılacağı ülkede, bölgede ya da ilgili ülkenin belirli bir sektöründe yeterli

derecede koruma sağlanması şarttır. Yeterli derecede koruma sağlanması kararı Komisyon tarafından verilmektedir. Kararın verildiği hallerde, bu ülke veya uluslararası kuruluşa yönelik bir kişisel veri aktarımı gerçekleşebilir.

GDPR'daki veri aktarıma ilişkin hükümler uyarınca verinin aktarılacağı ülkede yeterli derecede koruma sağlandığına Komisyon tarafından bir değerlendirme yapılmaktadır. Komisyon tarafından üçüncü ülkenin veya bir uluslararası kuruluşun yeterli derecede koruma sağladığına ilişkin değerlendirmesinde ABAD'ın 6 Ekim 2015 tarihinde verdiği "Schrems Kararı"yla[72] da etkilidir. İlgili karar ile, AB yurttaşlarının kişisel verilerinin ABD'ye aktarılmasına izin veren "Safe Harbor" anlaşmasının geçersiz olduğuna hükmetmiştir. İlgili anlaşma kişisel verilerin aynı düzeyde korunduğu ülkelere aktarımının izin verilmesi kapsamında AB ile ABD arasında imzalanmıştır. Bu anlaşmanın geçersizliğine ilişkin kararın önemi haiz olmasının sebebi ise AB yurttaşlarının kişisel verilerinin AB sınırları dışına çıkarılmasının belli şartlar sağlanmadığı takdirde mümkün olmadığına hükmedilmesidir.

GDPR'ın başlangıç hükmü 104'üncü maddede de belirtildiği üzere, Komisyon söz konusu üçüncü ülkede hukukun üstünlüğü, adalete erişimi, uluslararası insan hakları norm ve standartlarına uygunluğu, sektörel iç hukuk düzenlemeleri, kamu düzenine ilişkin kurallar da dahil savunma ve ulusal güvenlik ile ceza hukuku mevzuatı bakımından bir değerlendirme yapmaktadır. Tüm bu değerlendirme neticesinde verilerin aktarılması için üçüncü ülkenin veya uluslararası kuruluşun AB'de sağlanan veri koruma mevzuatı çerçevesine uygun yeterli koruma düzeyini sağlayabiliyor olması gerekmektedir.

GDPR'ın 45'inci maddesinde tanımlanan anlamda bir yeterli koruma düzeyi kararının bulunmaması durumunda ise 46'ncı maddeye göre kişisel verilerin aktarımı, ancak uygun önlemlerin alındığı ve ilgili kişinin haklarının korunarak buna ilişkin etkili yaptırım mekanizmalarının sağlandığının garanti edildiği durumda mümkündür. Bu yöntem ise hem yasal belirsizlikler dolayısıyla kanıtlanması zor hem de maliyeti bakımından dezavantajlı bir mahiyet arz etmektedir.

GDPR uyarınca gibi işlenmiş veya işlenecek olan kişisel verilerin üçüncü ülkelere veya uluslararası kuruluşlara aktarımı için sınırlamalar getirildiğinden bahsedilmiştir. Eklemek gerekir ki, veri aktarılan ülke, eş değer veri korumasını sağlamıyor ise bağlayıcı şirket kuralları, sertifikasyon, veri işlenmesi davranış kuralları ve çerçeve sözleşmeler ile veri aktarılması bu ülkeye yapılabilmektedir.

[72] • ABAD, 6 Ekim 2015, C-362/14, Maximillian Schrems ve Data Protection Commissioner <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362> s.e.t. 27.06.2019.

• 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün bölgesel kapsamı hakkındaki rehber.

GDPR'ın 47'nci maddesi uyarınca, bağlayıcı şirket kuralları; grup şirketleri arasında veri aktarımında kendilerinin belirlediği iç kurallardır. Başka bir ifade ile grup şirketlerin, aynı şirket grubunda olan uluslararası düzeyde "kişisel verileri yeterli düzeyde koruma sağlamayan" ülkelere veri aktarımı yaparken bu aktarıma izin verilmesidir. Bağlayıcı şirket kuralları ile bir şirketler grubundaki tüm veri aktarımlarının güvenli olmasını sağlamaktadır. Bunun için de gizlilik kuralları, şeffaflık ve veri güvenliği önemlidir. Ayrıca bu kuralların bağlayıcılığını gösteren ve kanıtlayan unsurlar da yer almalıdır.

Kısaca, KVK Kanunu'ndan farklı olarak GDPR'da ilgili kişi veri sorumlusuna kendi kişisel verilerinin üçüncü ülkeye veya uluslararası kuruluşa aktarılmasına ilişkin rıza vermiş olsa dahi, veri aktarımı yapılan ülkede yeterli düzeyde koruma sağlandığına ilişkin karar verilmediği sürece, verinin AB dışına aktarılması yasaklanmaktadır.

✣ Blokzincir Ağlarında Verilerin Aktarılmasının KVK Kanunu ve GDPR Bakımından Değerlendirilmesi

Özellikle, Açık ve İzin Gerektirmeyen Blokzincir Ağlarında verilerin AB dışına aktarılması sorun oluşturabilir. Bir blokzincirdeki tüm işlem kayıtları; tüm madencilere gönderilen işlem (kişisel veri içerebilir) onay talebi ve tüm katılımcılar için zincire yeni eklenen blokların güncel halini içermektedir. Önemle belirtmek gerekir ki, madenciler olsun veya olmasın, katılımcılar AB dışındaki ülkelerde bulunabilmektedir. Bu nedenle, AB dışına aktarımlar için KVK Kanunu ve GDPR uyarınca belirtilen yükümlülüklere uyulması sorunu gündeme gelmektedir.

AB dışındaki bir ülkeye veya uluslararası kuruluşa veri aktarımı için uygun güvenlik önlemlerinin alınması (bağlayıcı şirket kuralları ve veri işleme davranış kuralları) Kapalı ve İzin Gerektiren Blokzincir ağında pratik olarak mümkün iken, veri sorumlusunun madencilerin konumları bakımında gerçek bir kontrole sahip olmadığı Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda pratik olarak mümkün değildir.[73]

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da yer alan verilerin aktarılması bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

> Verilerin hangi üçüncü ülkeye aktarıldığı ve bu ülkelerin yeterli derecede koruma sağlandığının tespiti nasıl yapılacaktır?

[73] Torre, Lydia F de la (2019) Blockchain: Challenges and solutions for compliance with the GDPR, <https://medium.com/golden-data/blockchain-challenges-and-solutions-for-compliance-with-the-gdpr-c354987f8fae> s.e.t. 27.06.2019.

VI. Aktörler

a. İlgili Kişi (*Veri Sahibi*)

KVK Kanunu'nun 3'üncü maddesinin (ç) bendi uyarınca ilgili kişi, kişisel verisi işlenen gerçek kişiyi ifade etmektedir.[74]

İlgili kişi, GDPR'ın 4'üncü maddesinin 1'inci fıkrası uyarınca ise özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak belirlenebilen kişi olarak tanımlanmıştır.

Yukarıda detaylarına yer verildiği üzere, blokzincir ağında bir kişisel verinin depolanması üç alternatif şekilde gerçekleşmektedir. Söz konusu depolanma yöntemleri düz metin, şifrelenme veya kriptografik özetlenme yöntemleridir. Bu üç yöntemle kişisel verileri işlenen gerçek kişiler, ilgili kişi olarak kabul edilmektedir. Düz metin yöntemi bakımından blokzincir ağında depolanan verilerin gerçek kişiler ile ilişkilendirilebildiği her durumda söz konusu kişilerin GDPR ve KVK Kanunu kapsamında ilgili kişi olarak nitelendirileceği açıktır. Öte yandan, genel anahtarların ve işlem verilerinin takma adlı veri olarak kabul edilmesi ve bu nedenle kişisel veri olarak değerlendirilmesi sebebiyle blokzincir ağında kişisel verileri işlenen gerçek kişiler hem GDPR hem de KVK Kanunu kapsamında ilgili kişi olarak kabul edilmektedir.

b. Veri Sorumlusu

KVK Kanunu'nun 3'üncü maddesinin (ı) bendi uyarınca veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak tanımlanmıştır.

GDPR'ın 4'üncü maddesinin 7'nci bendinde ise veri sorumlusu, tek başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kurumu, kuruluşu veya diğer herhangi bir organ olarak tanımlanmış ve söz konusu işleme amaçları ve yöntemlerinin AB veya üye devlet hukukuna göre belirlenmesi durumunda, veri sorumlusu veya veri sorumlusunun belirlenmesine özgü kriterlerin AB veya üye devlet hukukuna göre belirlenebileceği belirtilmiştir. GDPR'ın 26'ncı maddesinde ise birden fazla işletmenin, ortaklaşa bir ürün veya servis sunması halinde, ortak veri sorumlusu (*joint controller*) sıfatıyla hareket edecekleri düzenlenmiştir. Buna göre, iki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, söz konusu veri sorumluları ortak veri sorumlusu olarak nitelendirilmektedirler.

[74] KVK Kanunu ve ilgili düzenlemeler çerçevesinde kişisel verileri işlenen kişiler için "ilgili kişi" ifadesi kullanılmıştır.

Veri sorumlusu statüsü, blokzincir teknolojisinde kilit rol oynamaktadır. Zira, ilgili kişiye ilişkin kişisel verilerin ilgili mevzuat hükümlerine uygun işlenmesi ve ilgili kişinin kişisel verileri ile ilgili olan haklarını talep etmesi bakımından sorumluluk veri sorumlusuna ait olacaktır. Ancak, blokzincir teknolojisinde veri sorumlusunun kim olduğunu tespit edebilmek çoğu zaman kolay değildir. Veri sorumlusunun tespiti bakımından farklı blokzincir ağları özelinde değerlendirme yapılması gerekmektedir.

Kapalı Blokzincir Ağları'nda veri sorumlusunun tespiti diğer ağ türlerine göre nispeten daha kolay olabilecektir. Zira, Kapalı Blokzincir Ağları'nda ilgili blokzincir sisteminin işletilmesinden sorumlu olan kişiler, ağa erişime izin veren konumundadır[75] ve bu şekilde, blokzincir üzerindeki kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirleyebilmektedirler.[76] Örneğin, GDPR'ın 26'ncı maddesi uyarınca bir grup bankanın Kapalı ve İzin Gerektiren Blokzincir Ağı oluşturması durumunda, söz konusu grup içerisinde yer alan bankalar ortak veri sorumlusu olacaktır.

Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda ise, blokzincir sisteminin merkeziyetsiz yapısı düşünüldüğünde veri sorumlusu veya ortak veri sorumlularının kimler olduğuna ilişkin tespitin yapılması oldukça zor ve tartışmalıdır.[77] Fransız Veri Koruma Otoritesi konumundaki Fransa Ulusal Bilişim ve Özgürlükler Komisyonu (**"CNIL"**),[78] bu bakımdan blokzincir konsorsiyumlarına, en kısa sürede veri sorumlusu veya ortak veri sorumlularının kim olacağının tespit edilmesine ilişkin çağrıda bulunmuştur.[79] Bu durumda dahi, veri sorumlularının tespit edilmesi, blokzincir yapısının merkeziyetsizlik karakterini zedeleyebileceği gibi kanunilik ilkesi gereği bu tanımlamanın hukuken ne derece bağlayıcı olduğu ayrıca bir tartışma konusunu oluşturmaktadır.

Söz konusu ağ türlerindeki veri sorumlularının tespiti, EDPB, ilgili otoriteler veya mahkemelerce henüz çözüme kavuşturulmamıştır.[80] Blokzincir teknolojisi kapsamında konuya ilişkin görüşler genel itibariyle aşağıdaki temel noktalarda toplanmaktadır.

[75] Kunde, Elke ve Dr. Kaulartz, Markus ve Naceur, Med Ridha Ben ve Liban, Samater ve Kunz, Matthias ve Prof. Dr. Skwarek, Voler ve Prof. Dr. Adam, Kataria ve Weiß, Rebekka ve Liesenjohann, Marco (2018) Blockchain und Datenschutz, Faktenpapier, bitkom, <https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf> s.e.t. 27.06.2019, s. 30.

[76] Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254), <https://www.uni-speyer.de/files/de/Lehrst%c3%bchle/Martini/PDF%20Dokumente/Typoskripte/BlockchainundRechtaufVergessenwerdenTyposkriptversion20-03-19NZ.pdf> s.e.t. 11.07.2019.

[77] Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller, <https://legal-revolution.com/images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf> s.e.t. 27.06.2019.

[78] Commission Nationale de l'Informatique et des Libertés ("CNIL"), <https://www.cnil.fr/professionnel> s.e.t. 27.06.2019.

[79] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019.

[80] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 17.

i. Protokol Geliştiricileri (*Protocol Developers*)

Protokol[81] geliştiricileri, bilgisayar mühendisleri gibi kod yazarak protokoller geliştiren ve ilgili protokolleri sürdüren kişilerdir. Bahsi geçen kişiler genellikle kişisel veri işleme faaliyeti gerçekleştirmemektedirler veya bu kişisel veri işleme faaliyeti kapsamında verilerin nasıl kullanılacağına karar vermemektedirler.[82] Aynı zamanda bu kişiler hazırlanan protokolün hangi amaçlar doğrultusunda kullanılacağını da belirlememektedirler. Birçok durumda, örneğin Bitcoin'de olduğu gibi Açık Blokzincir Ağı'nı oluşturan ve sürdüren protokol geliştiricilerinin veri sorumlusu olarak değerlendirilmesinin uygun olmadığı ifade edilmiştir.[83] Protokol geliştiricileri, Açık Blokzincir Ağı üzerinde çalışmaya gönüllü olmakta ve çoğu durumda çabaları için doğrudan bir kazanımları olmamakla birlikte, özünde bu aracın nasıl kullanılması gerektiğini tayin etmek yerine, faydalı bir araç yaratmaktalardır. Bu şartlar altında protokol geliştiricilerinin veri sorumlusu olarak kabul edilmesi ve veri işleme faaliyetlerinden sorumlu olmaları, Savunma İleri Araştırma Projeleri Ajansı ("**DARPA**")[84] veya World Wide Web'in[85] mucidi Tim Berners-Lee'nin dünya çapındaki sitelerde gerçekleşen her faaliyetten dolayı veya mysQl[86] yaratıcılarının veri tabanı teknolojisinin kullanımından dolayı veri sorumlusu olarak kabul edilmeleri varsayımı ile benzerlik göstermektedir.[87] Yazılım kodunun yayınlanmasıyla, Açık Blokzincir Ağı'nda protokol geliştiricileri, kişisel verilerin işlenmesinin amaçlarından ve araçlarının kontrolünden etkin bir şekilde feragat etmektedir.[88]

Bu nedenle, protokol geliştiricileri aynı zamanda KVK Kanunu ve GDPR kapsamında belirtilen "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen" bir niteliğe sahip olmadığından veri sorumlusu olarak kabul edilmemelidir.

ii. Onaylama Düğümleri (Validating Nodes) ve Katılma Düğümleri (*Participating Nodes*)

Düğümler (*nodes*)[89] genelde, defterlerin depolandığı bilgisayarları ifade etmektedir. Blokzincir ağında yer alan düğümler işlem kayıtlarını alabilen ve gönderebilendir.

Onaylama düğümleri, konsorsiyum mekanizması olarak adlandırılan ve kararlaştırılan bir algoritmaya göre, deftere veri eklemeye izin verilmesi anlamına gelmektedir.

[81] Bir ağdaki etkileşimleri tanımlayan, genellikle fikir birliği, işlem doğrulaması ve ağa katılım şartlarını içeren kuralları ifade eder.

[82] CMS Law and Tax (2019) The tension between GDPR and the rise of blockchain Technologies, <https://cms.law/en/INT Publication/The-tension-between-GDPR-and-the-rise-of-blockchain-technologies> s.e.t. 27.06.2019, s. 6.

[83] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 17.

[84] https://www.darpa.mil/

[85] World Wide Web, belli bir hiper-metin dili kullanan ve internet tarayıcısı adı verilen yazılımlar sayesinde kullanılan bir bilgi sistemdir. World Wide Web üzerinde bulunan her bir doküman veya sayfaya kısaca "Web Sayfası" denir.

[86] Defense Advenced Research Projects Agency, <https://www.mysql.com/> s.e.t. 27.06.2019.

[87] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 17.

[88] Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 125 1 (1254), <https://www.uni-speyer.de/files/de/Lehrst%c3%bchle/Martini/PDF%20Dokumente/Typoskripte/BlockchainundRechtaufVergessenwerdenTyposkriptversion20-03-19NZ.pdf> s.e.t. 11.07.2019.

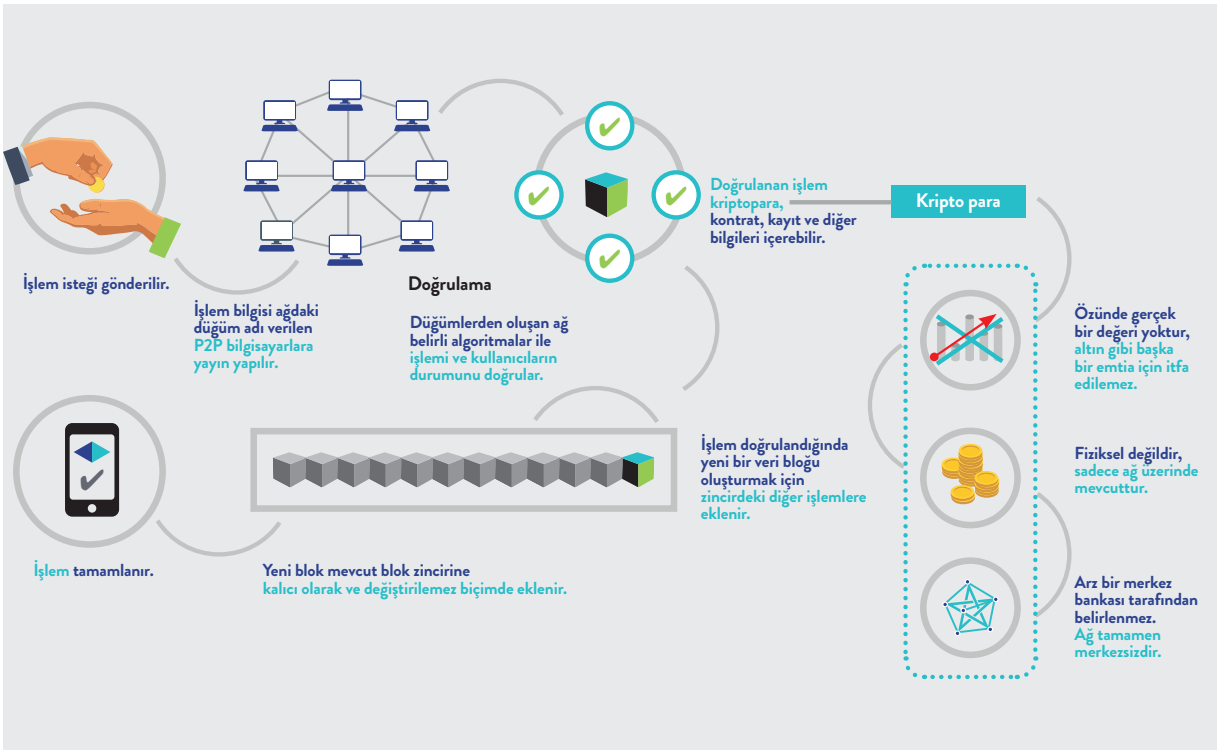
[89] Bir blokzincirdeki katılımcı tarafından işletilen defterin kopyasını ifade etmektedir. Kriptopara blokzinciri ağlarında, düğümlerin işlem onayı yetkisi yokken, bazı ağlarda düşük işlemci gücü tüketimi nedeniyle düğümler işlem onayı yapabilmektedirler.

Katılma düğümleri ise, verilerin senkronize kopyalarının saklanmasını ifade etmektedir. Ağda yer alan tüm düğümlerin, depolanan verilerin tamamını depolamadığı durumlar olabilmektedir. Zira, bir kullanıcı bir katılma düğümüne bağlıysa, deftere yeni veriler ekleyebilir ancak bu verinin önce katılma düğümüne yazılması ve sonra onaylama düğümüne gönderilmesi gerekmektedir.

Tam düğümler (*full nodes*), doğrulama yaparken başka bir düğüme ihtiyaç duymayan, blokzincirinin tamamının kopyasına sahip olan istemciyi ifade etmektedir.

Ana Düğümler, hem düğüm hem de tam düğümün tanımında yer alanları gerçekleştiren ve ayrıca ek işlevlerinin mevcut olduğu bir istemcidir. Bu ana düğümler normal düğümlere göre daha ağır düğümlerdir. İşlemleri onaylama, kaydetme ve yayımlamanın yanı sıra, ana düğümler bazen protokol işlemlerinin yürütülmesini sağlamaktadır. Ana düğümler hep çevrimiçidir ve normal düğümlerden çok daha fazla hafıza alanları mevcuttur. Ana düğümler, bir ana bilgisayarın ağdaki çok büyük bir sunucuyu barındırmasına benzerdir.[90]

Madenci ile düğümler birbirinden farklı iki aktörlerdir. Bir madencinin yeni bir blok oluşturacak onaylanmış işlem kaydını seçmesi için her zaman tam düğümü çalıştırması gerekmektedir. Tam düğüm olmadan, mevcut blokzincirin işlem geçmişine göre hangi önerilen işlemlerin geçerli olduğunu belirleyememektedir, bunun sebebi ise tüm blokzincir ağının geçmişine erişememesidir. Bu nedenle bir madenci her zaman tam bir düğümdür ancak tam düğümün her zaman bir madenci olması zorunlu değildir.



[90] S., Jimi (2018), Blockchain: What are nodes and masternodes?, <https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f> s.e.t. 27.06.2019.

Örneğin, Açık ve İzin Gerektirmeyen Ağ türü olan Bitcoin'de herkesin katılma düğümü veya onaylama düğümü olması mümkündür. Bitcoin'deki işlemler madenci düğümü tarafından doğrulanır ve blokzincire kaydedilen bir işlem bloğuna dahil edilmektedir.

Kapalı ve İzin Gerektiren Blokzincir Ağları'nın bazılarında ise, yalnızca onaylanmış aktörler onaylama düğümü olabilir ve deftere veri ekleyebilmektedir.[91],[92] Söz konusu onaylayıcı düğümlerin ve katılma düğümlerinin genellikle şirketler veya devlet kurumları konsorsiyumu şeklinde, aktörlerin yönetimi tarafından onaylanması gerektiği anlamına gelmektedir. Ayrıca, bazı durumlarda kimin hangi verileri görebileceğini tanımlayan kurallar da mevcuttur.

Onaylama düğümlerinin ve katılma düğümlerinin veri sorumlusu olup olmadığı ile ilgili tartışmalar mevcuttur ve aşağıda bu tartışmalar kapsamındaki bazı görüşlere yer verilmiştir.

>> Bir görüşe göre, yazılımın aktif olarak indirilmesi ve çalıştırılması ile düğümler verileri işlemenin amacını ve araçlarını belirlemektedir. Genellikle bir protokolün yeni bir versiyonunun piyasaya sürüldüğü hallerde, düğümlerin onları çalıştırmakta veya çalıştırmamakta serbest olduğu ve bu nedenle platformun nasıl geliştiğini etkilediklerine işaret edilmektedir.[93]

>> İkinci bir görüşe göre ise, düğümlerin veri işlemenin amacını ve araçlarını belirlemediğini savunmaktadır.[94] Protokolü, bir ödül kazanmak için, ağın istikrarını sağlamak amacıyla veya üçüncü taraf aracılara güvenmeksizin kendileriyle ilgili verilere erişmenin bir yolu olarak yürütmekte olunduğu düşünülmektedir.

>> Farklı bir görüş ise, her bir düğümün veri sorumlusu sayılması durumunda, önemli komplikasyonların ortaya çıkacağını savunmaktadır. Zira, bir zincirdeki düğümlerin tam sayısı, konumları ve kimlikleri net olarak bilinememektedir ve bu belirsizlik veri sorumlularına ait yükümlülüklerden sorumlu tutulmasını oldukça zorlaşmaktadır. Bu sebeple, düğümlerin veri sorumlusu kabul edilmesi hem uygulama hem de hukuki nitelendirmenin yapılmasında problematik bir hal alabilmektedir.

Benimsenen görüşe ve bakış açısına bağlı olarak, düğümler geliştiriciler tarafından tasarlanan yazılım talimatlarına tabi veya blokzincir yönetiminde aktif katılımcılar tarafından kullanılan pasif araçlar olduğu kabul edilmektedir. Dahası, düğümler yalnızca verilerin şifreli veya kriptografik özet sürümünü görmektelerdir ve ilgili verilerde herhangi bir değişiklik yapamamaktadırlar.

[91] Alastria Construye Futururo, <https://alastria.io/> s.e.t. 27.06.2019.

[92] Sovrin, <https://sovrin.org/> s.e.t. 27.06.2019.

[93] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 18.

[94] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 18.

Onaylama düğümlerinin ve katılma düğümlerinin Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda veri sorumlusu olarak tanımlanması zor olacaktır. Düğümlerin Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda veri sorumlusu olmaktan ziyade veri işleyen olarak nitelendirilebileceği görüşünde ise,[95] veri sorumlusu ile veri işleyen (dolayısıyla her bir düğüm) arasında gerçekleştirilecek olan sözleşmenin yapılmasının mümkün olmadığı savunulmaktadır.

Ayrıca, GDPR'ın 26'ncı maddesinin 1'inci fıkrası uyarınca düğümler, işleme amaçlarını ve araçlarını birlikte belirlemediklerinden ortak veri sorumlular olarak nitelendirilemez.[96] Ortak veri sorumlusu olunması açık ve şeffaf bir sorumluluk dağılımını gerektirmektedir. Düğümler, Açık ve İzin Gerektirmeyen Ağlara katılıp katılmayacaklarını ve hangi işlevde katılacaklarını (tam node vb.) belirlemekte serbesttirler. Düğümler, GDPR'ın 26'ncı maddesi uyarınca belirlenen kriterlere genel olarak uymamaktadır; aksine sistem, düğümlerin ortak değil bireysel davranışları tarafından şekillendirilmiştir. Bir blokzincir, çeşitli düğümlerin etkileşimi ile gelişirken, bu düğümler diğer düğümlerin veri işleme yöntemlerini belirleyememektedir.[97]

iii. Ağ Kulanıcıları (*Network Users*)

Ağ kullanıcıları, bir düğüm aracılığıyla blokzincir ağına katılan ve işlem kaydı oluşturan kişiler olarak tanımlanmaktadır. Ağ kullanıcıları konusunda da yukarıdaki aktörlerde olduğu gibi farklı görüşler mevcut olmakla birlikte, iki ana görüş ön plana çıkmaktadır.

İlk görüş; ağ kullanıcıları, iş faaliyetleri dahilinde kişisel verileri blokzincir ağına kaydederlerse büyük olasılıkla veri sorumlusu olarak kabul edileceğini savunmaktadır. Burada önemli olan husus ise iş faaliyetlerinin tanımıdır. İş faaliyetleri; yazılımı çalıştıran varlıkları ve kişisel verileri bir blokzincir ağına kaydeden ürünleri veya hizmetleri içermektedir. Örneğin, kişisel olarak kripto varlık satın almak veya satmak için verlerin kişisel kullanım amacıyla blokzincir ağına kaydedilmesi durumunda veya diğer gerçek kişiler adına bir mesleki veya ticari faaliyetin parçası olarak gerçekleştirmiyor ise ağ kullanıcıları GDPR kapsamında veri sorumlusu sayılmayacaklardır.[98]

[95] CMS Law and Tax (2019) The tension between GDPR and the rise of blockchain Technologies, <https://cms.law/en/INT Publication/The-tension-between-GDPR-and-the-rise-of-blockchain-technologies> s.e.t. 27.06.2019, s. 6.

[96] GDPR 26(1) "İki ya da daha fazla sayıda veri sorumlusunun işleme amaçları ve yöntemlerini ortak bir şekilde belirlediği hallerde, bu veri sorumluları ortak veri sorumlularıdır."

[97] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, GDPR's Material Scope: Does Data Stored on a Blockchain Qualify as Personal Data, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s. 26.

[98] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 18.

KVK Kanunu'nun 28'inci maddesi uyarınca 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 KVK Kanunu'nun uygulanmayacağı hallerden biri olarak belirtilmiştir. Ağ kullanıcısının ancak 28'inci madde kapsamında bahsi geçen şartlar dahilinde veri sorumlusu olarak değerlendirilemeyeceği aşikardır.

iv. Madenciler (Miners)

Madenciler işlemleri onaylayarak blokzincir ağının işleyişine büyük katkı sağlamaktadır.[99] Madenciler, bireysel bloklardaki işlem verilerini etkileyememektedirler. Bir madenci blokzincir ağındaki işlemleri manipüle etmeye çalıştığında, sahte veriler diğer madenciler tarafından reddedilmektedir.[100] Ağın hesaplama gücünün çoğunluğunu ve/veya protokolde belirlenen oranı birleştiren bir grup madenci, teknik olarak blokzincir üzerindeki işlemleri kontrol eden konumunda olacaktır.[101]

Madenciler, kişisel verilerin bir blokzincir sisteminde işlenmesinin amaçlarını ve araçlarını belirleyememektelerdir. Aksine, madencilerin veri işleme faaliyetleri blokzincir protokolünde kendilerine verilen rolle sınırlıdırlar. Bu nedenle, KVK Kanunu ve GDPR kapsamında madencilerin veri sorumlusu olarak kabul edilmediği görüşü yaygındır.[102]

v. Borsa ve Cüzdanlar (*Exchange and Wallets*)

Kripto para birimleri kullanıcıları, borsadan veya cüzdandan yararlanmaktadırlar. Borsa, kripto para biriminin fiyat para veya diğer kripto para birimleri ile alım satımını yapan bir internet sitesi anlamına gelmektedir.[103] Cüzdan ise, kullanıcıların kripto paralarını saklamalarına izin veren bir hizmettir. Her iki durumda da kullanıcı ile blokzincir ağı arasındaki etkileşim bir servis sağlayıcı tarafından gerçekleştirilmektedir.[104]

[99] Kunde, Elke ve Dr. Kaulartz, Markus ve Naceur, Med Ridha Ben ve Liban, Samater ve Kunz, Matthias ve Prof. Dr. Skwarek, Voler ve Prof. Dr. Adam, Kataria ve Weiß, Rebekka ve Liesenjohann, Marco (2018) Blockchain und Datenschutz, Faktenpapier, bitkom, <https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf> s.e.t. 27.06.2019, s. 28.

[100] Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller, <https://legal-revolution.com images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf> s.e.t. 27.06.2019.

[101] Hajdarbegovic, Nermin (2014) Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack, coindesk, <https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack> s.e.t. 27.06.2019.

[102] Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller, <https://legal-revolution.com images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf> s.e.t. 27.06.2019.

[103] Bkz. De la Torre, Quora, May 25, 2016, What are the differences between a Bitcoin exchange vs a Bitcoin wallet, https://www.quora.com/What-are-the-differences-between-a-Bitcoin-exchange-vs-a-Bitcoin-walletwebsite.

[104] Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller, <https://legal-revolution.com/ images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf> s.e.t. 27.06.2019.

Servis sağlayıcısı, işlemlerin yürütülmesi veya kullanıcıya ait kripto para birimlerinin depolanması üzerinde kontrol sahibidir. Dolayısıyla borsalar ve cüzdanlar, kişisel verilerin işlenmesinin amaçlarını ve araçlarını belirlemeleri nedeniyle işlemlerin yürütülmesi veya kullanıcıya ait kripto para birimlerinin depolanması bakımından GDPR ve KVK Kanunu kapsamında hizmet kullanıcısı karşısında veri sorumlusu olarak kabul edilebileceklerdir.

vi. Katılımcılar (*Participants*)

Katılımcı; blokzincir ağında başlangıçtan itibaren tüm işlem kayıtlarının kopyasını tutan bir aktördür. Bir katılımcı varlık/lar yaratabilmekte ve ayrıca diğer katılımcılar ile bu varlık/ları paylaşabilmektedir.

CNIL, blokzincir ağında yazma hakkına sahip olan katılımcıların, veri sorumlusu olarak kabul edilebileceği kanaatindedir.[105] Bahsi geçen görüşe göre, blokzincir katılımcıları, işlemenin amaçlarını ve işlemenin anlamını tanımlamaktadır.

Daha spesifik olarak, CNIL aşağıda belirtilen şartlar dahilindeki katılımcı/ların veri sorumlusu olarak değerlendirilebileceği görüşündedir:

- Katılımcının gerçek bir kişi olması ve kişisel veri işlemenin mesleki veya ticari bir faaliyetle ilgili olması veya
- Katılımcının tüzel kişi olması ve kişisel verileri bir blokzincire kaydetmesi durumunda.

Örneğin, bir noterin ilgili kişilerin tapu belgelerini kayıt altına alması veya bir bankanın müşterilerinin verilerini müşteri yönetimi sürecinin bir parçası olarak bir blokzincir ağına kaydetmesi halinde söz konusu kişiler veri koruma mevzuatları bakımından veri sorumlusu olarak kabul edilebileceklerdir.

Bir grup işletme, ortak bir amaç doğrultusunda bir blokzincir üzerinde işleme faaliyeti yürütmeye karar verdiğinde, CNIL, katılımcıların veri sorumlusunun sorumlulukları hakkında ortak bir karar almalarını ve bu aktörlerin önceden tanımlanmasını önermektedir. Bu takdirde, katılımcıların, veri sorumlusu olarak bir tüzel kişilik oluşturarak veya tek bir tüzel kişiyi veri sorumlusu olarak belirleyerek grup için karar verici olarak ataması ile veri sorumlusu belirlenebilecek olup; aksi halde tüm katılımcıların ortak veri sorumlusu olarak kabul edilmesi muhtemel olacağını belirtmiştir.[106] İlgili kişiler (kişisel verileri blokzincir ağına kaydedilmiş olan ve/veya kaydedilenler) haklarını etki bir şekilde kullanabilmek için kime veya nereye başvurabileceklerini önceden bilmeli ve veri sorumlusunun önceden belirlenmesi ile veri koruma otoritelerinin kimi sorumlu tutacağı önceden belirlenmesi gereken bir husustur.

[105] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019.

[106] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019.

Düğümü çalıştıran bir katılımcı Açık ve İzin Gerektirmeyen Blokzincir Ağı'nda doğrudan etkileşime girmektedir. Açık anahtardan alıcının açık anahtarına gönderilecek olan tam kripto para birimi miktarına tek bir elden karar vermektedir. Yukarıda detaylı olarak anlatıldığı üzere işlem kayıtları blokzincir ağında saklanmakta ve sonradan silinememektedir. Bu nedenle bir görüş[107] katılımcıların veri sorumlu olarak kabul edilmesi gerektiğini savunmaktayken bu görüşün karşıt görüşü ise Açık ve İzin Gerektirmeyen Blokzincir Ağı'nda bunun mümkün olmadığını düşünmektedirler. Bahsi geçen blokzincir ağlarında tek bir kontrol noktası yoktur. Bu nedenle, tek bir Blokzincir Ağı katılımcısına veri sorumlusunun tüm sorumluluklarının yüklenmesinin imkânsız ve pratik olduğu savunulmaktadır. Yine bu görüş her bir veri işleme faaliyetinden dolayı veri sorumlusunun sorumlu olmasının temelsiz olduğunu çünkü Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda bu kontrol mekanizmasının imkânsız olduğu belirtilmiştir. Blokzincir katılımcılarının, GDPR uyarınca veri sorumlusu olarak kabul edilmediği görüşünü savunmaktadırlar.

c. Veri İşleyen

KVK Kanunu'nun 3'üncü maddesinin (ğ) bendi uyarınca veri işleyen, veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmıştır. GDPR'ın 4'üncü maddesinin 8'inci fıkrası uyarınca ise veri işleyen, veri sorumlusu adına kişisel verileri işleyen bir gerçek ya da tüzel kişi, kamu kurumu, kuruluşu veya diğer herhangi bir organ olarak tanımlanmıştır.

Bir blokzincir ağında, GDPR ve KVK Kanunu uyarınca aşağıdaki kişiler veri işleyen olarak kabul edilebileceği düşünülmektedir:

>> Veri sorumlusu olan katılımcı adına kişisel verileri işleyen akıllı sözleşme geliştiricileri

CNIL, akıllı sözleşmelerle ilgili olarak herhangi bir yazılım da olduğu gibi, algoritma geliştiricisi yalnızca çözüm sağlayıcı olabilir veya söz konusu algoritma geliştiricisi veri işleme faaliyetine katıldığında, verilerin kullanım amacının belirlenmesindeki rolüne bağlı olarak veri işleyen olarak nitelendirilebileceği belirtilmiştir.

Örneğin, bir akıllı sözleşme geliştiricisi bir sigorta şirketine, yolcuların uçuşları ertelendiğinde yolcuların paralarının otomatik olarak geri ödenmesini sağlayan akıllı sözleşme ile çözüm sunmaktadır. Bahsi geçen akıllı sözleşme geliştiricisinin, sigorta şirketinin (veri sorumlusu) adına ertelenen uçuşlar için para iadesi yapılması gibi bir çözüm sağlaması amacıyla kişisel verileri işlemesi sebebiyle veri işleyen olarak nitelendirilebilecektir.

[107] Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller, <https://legal-revolution.com/images//pdf/Blockchain-meets-Data-Privacy_Blockchain-and-the-Data-Controller.pdf> s.e.t. 27.06.2019, s. 126.

>> Bir blokzincir üzerindeki kişisel verileri içeren işlemi onaylayan madenciler

Bazı durumlarda, madenciler de GDPR kapsamında veri işleyen olarak değerlendirilebilmektedir.[108] Esasen, işlemin teknik kriterlere (format ve belirli bir maksimum boyut gibi ve katılımcının blokzincir ağının kurallarına göre işlem yapmasına izin verilip verilmediği haller gibi) uyup uymadığını kontrol ederken veri sorumlularının verdiği talimatlara uymaktadırlar.

>> Örneğin, birden fazla sigorta şirketinin işlemlerinde Müşterini Tanı (*Know Your Customer*) (**"KYC"**) yükümlülüklerine uymak için Kapalı Blokzincir Ağı oluşturmaya karar vermeleri durumunda, sigorta şirketlerinden birinin veri sorumlusu olduğunu kararlaştırabilirler.[109] KYC prosedürü, yatırım danışmanlarının müşterilerinin risk toleransı, yatırım bilgisi ve finansal durumu hakkında ayrıntılı bilgi sahibi olmasını sağlayan yatırım endüstrisinde yer alan standart bir formdur.[110] Bu durumda, madenciler olarak işlemleri doğrulayan diğer sigorta şirketleri, veri işleyen olarak kabul edilmesi muhtemeldir.

✣ Blokzincir Ağlarında Veri Sorumlusunun ve Veri İşleyenin KVK Kanunu ve GDPR Bakımından Değerlendirilmesi

Özetle, yukarıda belirtilen birçok farklı görüş ve değerlendirme ışığında, her durum özelinde ayrı ayrı değerlendirilme yapılması, veri işleyenin ve veri sorumlusunun hukuki statüsü KVK Kanunu ve GDPR kapsamında belirlenirken Blokzincir ağının niteliği ve içeriği incelenerek tespit edilmelidir.

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan veri sorumlusu/veri işleyen kavramı bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

Blokzincir ağında veri sorumusu ve veri işleyen kimdir?

Çeşitli blokzincir ağı türlerinde veri sorumlusunun ve veri işleyenin tespit edilmesi bakımından değerlendirme farklılık göstermekte midir?

[108] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019, s. 3.

[109] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019.

[110] Koinbülteni, KYC (Know Your Client) Nedir?, Know Your Client – Müşterini Tanı, <https://koinbulteni.com/kyc-know-your-client-nedir> s.e.t. 27.06.2019.

VII. İlgili Kişinin Hakları

İlgili kişi, KVK Kanunu ve GDPR düzenlemeleri kapsamında birtakım haklara sahiptir. İlgili kişilere kişisel verilerin korunması kapsamında tanınan haklar bakımından, ülkemizde yürürlükte olan mevzuat ile GDPR arasında paralel olan hususlar bulunmakla birlikte, GDPR ilgili kişiye ek ve daha geniş kapsamlı haklar tanımaktadır.

a. İlgili Kişinin KVK Kanunu'ndan Doğan Hakları:

KVK Kanunu'nun 11'inci maddesi uyarınca herkes, veri sorumlusuna başvurarak kendisiyle ilgili aşağıdaki hususlara ilişkin olarak bilgi almak hakkına sahiptir:

>>Kişisel verilerinin işlenip işlenmediğini öğrenme.

>>Kişisel verileri işlenmişse buna ilişkin bilgi talep etme.

>>Kişisel verilerinin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme.

>>Yurt içinde veya yurt dışında kişisel verilerinin aktarıldığı üçüncü kişileri bilme.

>>Kişisel verilerinin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme.

>>KVK Kanunu'na ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerinin aktarıldığı üçüncü kişilere bildirilmesini isteme.

>>İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle aleyhine bir sonucun ortaya çıkması durumunda buna itiraz etme.

>>Kişisel verilerinin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme.

b. İlgili Kişinin GDPR'dan Doğan Hakları:

GDPR, kişisel verileri korumaya yönelik olarak ortaya çıkarılmış yasal düzenlemeler içerisinde, AB'nin, kişisel verilerin korunmasına ilişkin Direktif'i ile getirilen ilgili kişinin haklarını bir adım öteye taşımıştır. GDPR, veri işleme faaliyetleri bakımından hesap verebilirlik (accountability) ve şeffaflık (*transparency*) kavramlarını ön plana çıkararak, veri sorumlularının bu kavramlara uygun hareket etmesini, ilgili kişinin haklarının sağlanması bakımından gerekli görmektedir.

Bu doğrultuda GDPR, KVK Kanunu'nun da temelini oluşturan Direktif ile tanınan hakları bir adım öteye taşıyarak ilgili kişinin kendi kişisel verileri üzerinde daha kapsamlı hakimiyet sahibi olmalarını sağlayan ilave haklar öngörmüştür. GDPR'ın ilgili kişilere sağladığı haklar ve bunlara ilişkin özet bilgileri aşağıda inceleyebilirsiniz.

i. Erişim hakkı

İlgili kişinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini veri sorumlusundan teyit etme ve işleme faaliyeti olması halinde, kişisel verilere erişim ile aşağıdaki bilgileri veya aksiyonları talep etme hakkı bulunmaktadır:

- İşleme amaçları,
- İlgili kişisel veri kategorileri,
- Üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin aktarıldığı veya aktarılacağı alıcılar veya alıcı kategorileri,
- Mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler,
- Veri sorumlusundan ilgili kişiye ilişkin kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkı,
- Bir denetim makamına şikâyette bulunma hakkı,
- Kişisel verilerin ilgili kişiden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler, ve
- Profil çıkarma da dahil olmak üzere, otomatik karar mekanizmalarının varlığı ve en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin ilgili kişi açısından önemi ve öngörülen sonuçları

Blokzincir ağında yukarıda bahsi geçen ilgili kişinin erişim hakkını nasıl kullanacağı konusunda sorunlar/çelişkiler mevcuttur. Bu tartışmaların başında yine yukarıda bahsedildiği üzere veri sorumlusunun tespit edilmesi ile erişim hakkının kime sunulacağının belirlenmesi yer almaktadır. Ayrıca, veri sorumlularından aktarımı yapılan verilere ve aktarılan taraflara ilişkin bilgi de talep edilebildiği için Açık ve İzin Gerektirmeyen Blokzincir ağında bu verilerin temin edilmesi yönünde sorunlar yaşanabilir.

CNIL, blokzincir teknolojisinin ilgili kişinin bilgi edinme hakkına ilişkin olarak problemler ortaya çıkarmayacağını, veri sorumlularının ilgili kişiye, kişisel verilerin blokzincir madencileri tarafından zincire kaydedilmesinden önce, kişisel verilerin işleneceğine ilişkin olarak kolayca erişilebilir ve açık şekilde bilgilendirme yapılmasının gerektiğini belirtmiştir. CNIL, raporunda erişim hakkı ve veri taşınabilirliği[111] hakkının blokzincir teknolojisinin teknik özellikleri ile uyumlu olduğunu vurgulamaktadır.[112] Bu noktada önemli olan, veri sorumlularının tespitinin yapılabilmesi olacaktır.

[111] İşbu raporun "Veri Taşınabilirliği" bölümünde detaylı olarak açıklanmıştır.

[112] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019, s. 1.

ii. Düzeltme hakkı

İlgili kişilerin kendileri ile ilgili doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin düzeltilmesini veri sorumlusundan talep etme hakkı bulunmaktadır. İşleme amaçları dikkate alınarak, ilgili kişinin, bir ek beyan yoluyla da dahil olmak üzere, eksik kişisel verileri tamamlatma hakkı bulunur.

Blokzincir teknolojisinin değiştirilemez yapısından dolayı KVK Kanunu ve GDPR'ın blokzincir teknolojisi ile arasındaki en temel sorunlardan biri ise düzeltme hakkının blokzincir teknolojisinde nasıl uygulanacağıdır. İlgili kişi hatalı veya eksik olan verisinin düzeltilmesine ilişkin talebini veri sorumlusuna sunduğunda veri sorumlusunun verileri düzeltmesi gerekmektedir ancak; blokzincirin güvenilirliği ilkesinin temelindeki husus değiştirilemez olmasıdır.

iii. Silme hakkı (Unutulma hakkı)

Unutulma hakkı GPDR'da tanımlanmış ve KVK Kanunu'nda tanımlanmamış olmasına karşın, dijital ortamda yer alan ilgili kişiye ait rahatsız edici her türlü kişisel içeriğin ve meşru amacını kaybeden kişisel verilere ilişkin içeriğin ilgili kişinin talebi üzerine kaldırılması anlamına geldiği anlamına gelmektedir.

İlgili kişinin kişisel verilerinin silinmesini talep etme ve unutulma hakkı GDPR'ın 17'nci maddesinde hükme bağlanmış olup üç fıkrada incelenmiştir.

Birinci fıkraya göre; ilgili kişinin kişisel verilerinin silinmesini veri sorumlusundan talep etme hakkı bulunur. İlgili kişinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini veri sorumlusundan talep etme hakkı bulunmaktadır.

İlgili kişinin verilerinin silineceği durumlara kişisel verilerin işleme amaçlarıyla ilişkili olarak saklanmasının artık gerekli olmaması, ilgili kişinin işleme faaliyeti için verdiği rızasını geri çekmesi ve işleme faaliyeti ile ilgili başka bir yasal gerekçe bulunmaması, kişisel verilerin yasadışı olarak işlenmiş olması gibi durumları örnek olarak verilebilmektedir.

Unutulma hakkının düzenlendiği ikinci fıkraya göre ise, veri sorumlusunun kamuya açıkladığı kişisel verileri birinci fıkra uyarınca silmek zorunda olduğu hallerde veri sorumlusu, veri işleyenleri söz konusu kişisel verilere yönelik her türlü bağlantının ve bu verilerin her türlü nüshasının söz konusu veri işleyenlerce silinmesi için teknik tedbirlerin de alınması dahil olmak üzere gerekli bilgilendirmeyi yapması gerektiğine yöneliktir.

Üçüncü fıkra da silme hakkının istisnaları düzenlenmiştir. Unutulma hakkı; ifade özgürlüğü ve bilgi edinme hakkının kullanılması, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi, halkın sağlığı kapsamında kamu yararı sebeplerinin olması, kamu yararına arşivleme, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya yasal iddialarda bulunulması durumunda bu iddiaların uygulanması veya savunulması açısından sınırlandırılabildiği ifade edilmiştir.

Silme hakkı bahsinde, ABAD'ın 2014 tarihli Google Kararı'nda[113] verdiği internet ortamındaki kişisel verilere yönelik linklerin, bireylerin talebi halinde kaldırılmasına ilişkin önemli kararında "unutulma hakkı" kavramından bahsedilmiştir. İnternet tarayıcıları içerisinde en önemli firmalar arasında yer alan Google; her gün dünyanın dört bir yanından yapılan milyarlarca aramayla internetin neredeyse her yerine erişim imkânı sağlamaktadır. Mario Costeja Gonzalez isimli İspanyol bir avukat ise 1998 yılında evinin icra yoluyla açık artırmaya çıkarıldığına dair bir gazete ilanının, kişilik hakkını ihlal ettiğini ileri sürerek bu ilanı yayınlayan *La Vanguardia* isimli gazeteyi ve bu ilana arama motorlarında yer veren Google şirketini 2010 yılında İspanyol Ulusal Veri Koruması Otoritesi'ne şikâyet etmiştir. Otorite, gazete hakkındaki şikâyeti, mevzuat hükümleri çerçevesinde cebri icra yoluyla açık artırmada ilan verilmesinin zorunlu olduğu ve ilanın mümkün olabildiğince fazla kişinin bilgisine sunulmasında menfaat bulunduğu gerekçesiyle reddederken, Google hakkındaki şikâyeti ise Google'ın bir veri sorumlusu olduğunu belirterek kabul etmiştir.

Google, davayı İspanya İstinaf Mahkemesi'ne taşımıştır. Yüksek Mahkeme, bu hususta unutulma hakkını barındıran Direktif'in yorumlanması için ABAD'dan görüş almak istemiştir. ADAB bu olayda; geçersiz, eksik, tamamen ilgisiz veya sonradan ilgisiz hale gelmiş bir verinin kişilerin unutulma hakkına saygı gösterilerek ilgili kişinin talebi halinde silinmesi gerektiği yönünde bir yorumla oldukça önemli bir karara imza atmıştır.

Ancak önemle belirtmek gerekir ki unutulma hakkı kapsamında ilgili kişinin verilerinin tamamen arama motorunda çıkan sonuç listesinden silinmesi mümkün değildir. Bahsi geçen kararda verinin tamamen yok edilmesi değil ancak verilerin artık görünmesinin engelleneceği, değiştirilebileceği veya gizlenebileceğinden bahsedilmiştir zira, verinin kaldırılması esasen verinin bilinmez/karanlık hale getirilmesi şeklinde anlaşılmalıdır.

Blokzincir ağında ise yukarıda belirtildiği üzere verilerin silinmesi, imha edilmesi ve yok edilmesi teorik olarak mümkün olsa da pratik ve teknik olarak imkânsızdır. Bu sebeple silinme hakkının öne sürülüp verilerin silinmesi için ilerleyen bölümlerde aslında verilerin bilinmez/karanlık hale getirilmesi veya ilgili kişi ile ilişkisinin koparılması gibi detaylı olarak anlatılacağı üzere çözüm önerileri sunulmuştur.

iv. İşleme faaliyetini kısıtlama hakkı

GDPR'ın 18'inci maddesindeki belirtilen koşullardan birinin gerçekleşmesi halinde, ilgili kişinin veri sorumlusundan işleme faaliyetinin kısıtlanmasını talep etme hakkı bulunur. Örneğin; veri işleme faaliyetinin mevzuata aykırı olması ve ilgili kişinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi hali için geçerlidir.

[113] ABAD, 25 Haziran 2013, C-131/12, Google Spain SL-Google Inc./Agencia Española de Protección de Datos-Mario Costeja González, <http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN> s.e.t. 27.06.2019.

v. Kişisel verilerin düzeltilmesine ya da silinmesine veya işleme faaliyetinin kısıtlanmasına ilişkin kişisel verilerin paylaşıldığı üçüncü taraflara bildirim yükümlülüğü

Veri sorumlusu, imkânsız olmaması veya ölçüsüz bir çabayı gerektirmemesi şartıyla, 16'ncı madde, 17'nci maddenin 1'inci fıkrası ve 18'inci madde uyarınca gerçekleştirilen her türlü kişisel verilerin düzeltilmesi veya silinmesi işlemi veya işleme faaliyetini kısıtlama işlemini kişisel verilerin aktarıldığı her alıcıya bildirmelidir. İlgili kişinin bu yönde bir talebinin bulunması halinde, veri sorumlusu ilgili kişiyi bu alıcılar hakkında bilgilendirmelidir.

Blokzincir teknolojisinde Açık ve İzin Gerektirmeyen Ağlar'da herkesin veriye erişimi olduğu düşünüldüğünde bu bildirim nasıl yapılacağı sorun teşkil etmektedir.

vi. Veri taşınabilirliği hakkı

GDPR'ın 20'nci maddesinde yer alan hallerde, ilgili kişinin kendisi ile ilgili olarak bir veri sorumlusuna sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan şekilde ve makine tarafından okunabilecek bir formatta alma hakkı ve kişisel verilerin sağlandığı veri sorumlusunun herhangi bir engellemesi olmaksızın bu verileri başka bir veri sorumlusuna iletme hakkı bulunmaktadır.

vii. İtiraz hakkı

İlgili kişinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı mevcuttur. Veri sorumlusu ilgili kişinin menfaatleri, hakları ve özgürlükleri nedeniyle ağır basan veri işleme faaliyetlerine yönelik gerekçeler veya yasal iddialarda bulunulması ve bu iddiaların savunulması açısından zorlayıcı meşru gerekçeler göstermediği sürece, veri sorumlusu artık bu talebin ardından kişisel verileri işleyemeyecektir.

Kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, ilgili kişinin doğrudan pazarlama ile alakalı olduğu ölçüde profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine herhangi bir zamanda itiraz etme hakkı bulunmaktadır.

İlgili kişinin doğrudan pazarlama amaçlarına yönelik olarak işleme faaliyetine itiraz etmesi halinde, kişisel veriler artık bu amaçlarla işlenememektedir.

viii. Profilleme de dahil olmak üzere otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı

İlgili kişi kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profilleme de dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkına sahiptir. Başka bir ifade ile, erişim haklarının bir parçası olarak, ilgili kişi, veri sorumlusundan otomatik işlenmesine bağlı olarak gerçekleşen yapay zeka gibi otomatik karar verme faaliyetleri için verilerinin kullanılıp kullanılmadığı hakkında bilgi talep etme hakkına sahiptir.

GDPR çerçevesinde "otomatik karar verme" kapsamında kişilerin rastgele profillerinin oluşturulması veya yalnızca bir makine tarafından verilen bir karar temelinde, bazı yasal sonuçlara maruz kalınmasına karşı ilgili kişilerin korunması hedeflenmektedir. Bu doğrultuda GDPR hükümleri uyarınca, ilgili kişilerin bu işlemlerin gerçekleştirildiği konusunda bilgilendirilmeleri gerekmekte olup; ilgili kişiler, insan müdahalesini talep etme veya karara itiraz etme hakkına sahiptir. İlgili kişinin haklarını düzenleyen KVK Kanunu'nun 11'inci maddesi ise, GDPR düzenlemesine göre daha dar olmakla birlikte; söz konusu madde kapsamında ilgili kişilere, kendisiyle ilgili işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilerek aleyhine bir sonucun ortaya çıkması halinde söz konusu sonuca karşı veri sorumlusuna itiraz etme hakkı tanınmıştır.

Gerek GDPR gerekse de KVK Kanunu uyarınca, belirtilen bu itiraz hakkının uygulanmasının, blokzincir altyapısı kullanan sistemler için ne şekilde işleyeceği hukuken net olmamakla birlikte, bu hakkın kullanımının teknik olarak mümkün olmadığı değerlendirilmektedir.

✣ Blokzincir Teknolojisi ile KVK Kanunu'ndan ve GDPR'dan Doğan Hakların İlişkisinin Değerlendirilmesi

Blokzincir teknolojisinin ana prensipleri olarak (i) dağıtık veri tabanı (*distributed database*), (ii) eşler arası aktarım (*peer-to-peer transmission*), (iii) şeffaflık, (iv) değişmez kayıtlar (*static records*) ve (v) sayısal/hesaba dayalı mantık (*computational logic*) kavramları sayılabilmektedir. Blokzincir teknolojisi bahsi geçen ana prensiplerin yanı sıra, veri bütünlüğü (*data integrity*) ve kimlik doğrulama (*identity authentication*) özellikleri üzerine inşa edilmiştir.[114] Blokzincir teknolojisinin aradığı veri bütünlüğü özelliğini şifreleme fonksiyonu ile karşılarken, kimlik doğrulama özelliğini ise açık

[114] Bacon, Jean ve Michels, Johan David ve Millard, Christopher ve Singh, Jatinder, Blockchain Demystified, Sayı 1, <https://jolt.richmond.edu/blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers/> s.e.t. 27.06.2019.

anahtar alt yapısı (*public key infrastructure*) ile karşılamaktadır. Blokzincir teknolojisi bu iki özelliği bünyesinde barındırarak ilgili işlemlerin kalıcı ve bozulmamış kaydını oluşturmayı ve her işlemle ilişkili taraf veya tarafları doğrulamayı hedeflemektedir.

GDPR ve KVK Kanunu gibi veri koruma düzenlemeleri, ilgili kişilere kişisel verileri üzerinde daha kapsamlı kontrol imkânı sağlamak üzere tasarlanmıştır. Özellikle GDPR, AB ülkelerinin veri koruma düzenlemeleri arasındaki çelişkilerin ortadan kaldırılarak veri koruma mevzuatı birliğinin sağlanması; kişisel verilere daha kolay erişim hakkı; düzeltme hakkı; daha açık bir silme hakkı düzenlemesi ve veri taşınabilirliği gibi birtakım haklar öngörmektedir. Bu çerçevede GDPR ve KVK Kanunu, merkezi sistemlerin hakimiyette olduğu bir dünyada veri işleme faaliyetlerinin çoğunlukla merkezi yapılar tarafından gerçekleştirilmesi nedeniyle, bu yapılar tarafından gerçekleştirilen veri işleme faaliyetleri sırasında uyulması gereken usul ve esasları düzenlemektedir.

Blockzincir teknolojisi ise önceki bölümlerde detaylı şekilde açıklandığı üzere, merkezi değil, dağıtık bir yapıya sahiptir ve merkezi bir yapı üzerine inşa edilen GDPR ve KVK Kanunu gibi veri koruma düzenlemeleri ile arasındaki bu temel farklılık nedeniyle blokzincir teknolojisi ile veri koruma düzenlemeleri belirli noktalarda çelişmektedirler. Bu çelişkiler blokzincir teknolojisinin geliştirilmesi sırasında blokzincir geliştiricileri, regülatörler, bu alanda faaliyet gösteren firmalar ve bunların kişisel veri uzmanları ile karar mekanizmalarını aşılması gereken birtakım önemli engellerle karşı karşıya bırakmaktadır.

Yukarıda bahsi geçtiği üzere, genellikle blokzincir ağları, bir kez zincire yazılan verilerin değiştirilemeyeceği şekilde tasarlanmıştır. Bu değişmezlik blokzincir teknolojisinin önemli bir özelliği ve bu teknolojisinin güvenilirliğini sağlamaktadır. Bu çerçevede verisi işlenen ilgili kişinin verilerinin silinmesini talep etmesinin üzere, söz konusu blokzincir ağının veri sorumlusu tespit edilse dahi, zinciri yok etmeden bir işlemin kaydını silmek veya güncellemek mümkün değildir. Bu koşullar altında, ilgili kişinin silme veya düzeltme hakkını nasıl kullanacağı cevaplanması gereken önemli bir soruyu ortaya çıkarmaktadır. Blokzincir teknolojisinin yapısında yer alan bu değiştirilememe özelliğinin amacı, işlemlerin merkezi bir yapı olmadan gerekli güven ortamı oluşturularak gerçekleştirilmesini sağlamaktır.

Veri koruma düzenlemeleriyle gelen yükümlülüklerin genel olarak Kapalı ve İzin Gerektiren Blokzincir Ağları'nda geliştirilmesi ve uygulanmasının, Açık ve İzin Gerektirmeyen Blokzincir Ağları'na kıyasla daha kolay olduğu düşünülmektedir. Ancak, yukarıda da bahsedildiği üzere düzeltme ve silme haklarına ilişkin problemlerin söz konusu ağın Kapalı ve İzin Gerektiren Blokzincir Ağı'na taşınması suretiyle dahi çözülemeyeceği öngörülmektedir. Zira, Özel ve İzin Gerektiren Blokzincir Ağları ilgili kişinin düzeltme ve silme haklarını kullanabileceği şekilde tasarlanmadığı sürece bu problemler

ortadan kalkmayacaktır. Blokzincir teknolojisinin doğası nedeniyle, kişisel verilerin blokzincir teknolojisi kullanılan ağlarda saklanması halinde, bu verilerin değiştirilmesi, güncellenmesi ve silinmesinde çeşitli zorluklarla karşılaşılması muhtemeldir.

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan ilgili kişinin hakları bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

- Blokzincir teknolojisinde ilgili kişi kimden ve nasıl bilgi talep edecektir?
- Aktarım yapılan alıcı grupları nasıl tespit edilecektir ve nasıl bildirilecektir?
- Aktarım yapılacak yabancı ülkede yeterli koruma bulunmuyosa bu ülkeler nasıl tespit edilecek ve yükümlülükler nasıl yerine getirilecektir?
- Düzeltme hakkı ve silinme hakkı (unutulma hakkı) değiştirilemez olduğu kabul edilmiş olan blokzincir teknolojisinde nasıl kullanılacaktır?
- Veri işleme amaçları ve söz konusu amaçlara uygun işlemenin gerçekleştirilip gerçekleştirilmediği nasıl tespit edilecektir?
- Veri sahibi itiraz hakkını nasıl ve kime karşı kullanacaktır?

VIII. KVK Kanunu ve GDPR Uyarınca Temel/Genel İlkeler

a. Giriş

Kişisel verilerin işlenmesine ilişkin temel ilkeler, KVK Kanunu'nun *'Genel İlkeler'* başlığını taşıyan 4'üncü maddesinde düzenlenmiştir. İlgili düzenlemede yer alan ilkeler, tüm kişisel veri işleme faaliyetinin temelini oluşturmaktadır ve tüm kişisel veri işleme faaliyetlerinin bu ilkelere uygun olarak gerçekleştirilmesi gerekmektedir.

Bilindiği üzere, taraflar Blokzincir teknolojisinin, hangi şekillerde çalışacağı ve mutabakata varmak için hangi mekanizmaların kullanacağı konularını tasarlayabilirler. Böylece merkezi olmayan bu ağ üzerinde tarafların mutabık kaldıkları şartlar, işlemler ve bunlar doğrultusunda işlenen kişisel veriler geriye doğru değiştirilemeyecek bir şekilde tutulmaktadır. Dolayısıyla Blokzincir teknolojisi vasıtasıyla oluşturulan uygulamalar aynı zamanda yoğun şekilde özel nitelikli kişisel veri de dâhil olmak üzere çok sayıda kişisel veri işlemektedir.

Blokzincir teknolojisinin yukarıda kısaca açıklanmış olan sui generis yapısı, KVK Kanunu'nda düzenlenen kişisel verilerin işlenmesine ilişkin genel ilkeler kapsamında çeşitli zorlukları da beraberinde getirmektedir.

Raporumuzun bu başlığı altında Blokzincir teknolojisi vasıtasıyla kişisel veri işleme faaliyetlerinde *Genel İlkelere* uygunluk değerlendirmesinde karşılaşılan sorunlara değinilecek olup bu sorunlara ilişkin üretilebilecek çözüm önerilerinin ortaya konulması hedeflenmektedir.

Kişisel veri işleme faaliyetlerinin temelinde yer alan genel ilkeler, aynı zamanda tüm düzenlemelerin de çıkış noktasını oluşturmaktadır. Bu doğrultuda, genel ilkelere ilişkin düzenlemeler, kişisel verilerin koruması ve gizliliğini düzenlemekte olan bütün uluslararası metinlerde yer edinmiştir. Genel ilkelere ilişkin düzenlemeler ile birlikte öncelikli olarak ilgili kişi haklarının başlangıç noktası belirlenmekte ve ardından gelen bütün özel düzenlemelerin de çerçevesini çizmektedir. Bu nedenle bu genel ilkelere uygunluk, kişisel verilerin en etkili şekilde de korunması için temel yapı taşı niteliğindedir.[115]

Kişisel verilerin korunması ve gizliliğin sağlanmasında kılavuz niteliği taşıyan genel ilkeler, Blokzincir teknolojisinin getirdiği sistemin ve uygulamalarda da yerine bulabiliyor olması önem arz etmektedir. Raporun ilerleyen bölümlerinde de öncelikli olarak Türk ve Avrupa Birliği mevzuatında yer alan genel ilkeler kısaca incelenecek olup ardından Blokzincir teknolojisine uyum sorunu ile çözüm önerileri ele alınacaktır.

[115] Bkz. Information Commissioner's Office, 'The Principles', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (son erişim tarihi: 06.03.2019)

b. KVK Kanunu Kapsamında Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler

Kişisel veri işleme faaliyetlerinin özünde bulunması ve bu faaliyetlerde dikkate alınması gereken genel ilkeler Kanun'un 4'üncü maddesinde şu şekilde düzenlenmektedir:

"Kişisel veriler, ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme."

108 sayılı Sözleşme[116] ve 95/46/EC sayılı Avrupa Birliği Direktifi'ne paralel olarak düzenlenen bu ilkeler, Kanun'da yer alan düzenlemelerinin yanı sıra özel kanun düzenlemelerinde de yer alan kişisel veri işleme düzenlemelerine uygun işleme faaliyetlerini gerekmektedir. KVK Kanunu düzenlemeleri, Kurul Kararları ve ilgili diğer düzenlemeler incelendiğinde ilgili ilkeler kısaca aşağıda yer alan değerleri ifade etmektedir.[117]

i. Hukuka ve dürüstlük kurallarına uygun olma ilkesi

Mevzuata uygunluğun yanı sıra hukuk normları ve evrensel hukuk ilkelerine uygunluğu ile tüm hukuk sistemlerine uygunluğu ifade eden bu ilke, diğer ilkeleri de kapsayıcı niteliktedir. Hukuka uygun işleme faaliyeti, KVK Kanunu düzenlemelerinin yanı sıra özel düzenlemelere de uygunluğu beraberinde getirirken; dürüstlük kuralına uygun işleme faaliyeti ise veri sorumlularının veri işleme amaçlarının yanı sıra ilgili kişilerin çıkarlarını ve makul beklentilerini de dikkate almayı gerektirir. Dürüstlük kuralı, aynı zamanda kişilere kendilerine veri işleme konusunda izin ya da emir veren hukuk kurallarına dayanarak gerçekleştirdikleri fiillerde ilgili amaç gereği mümkün olan en az miktarda veri işlemelerini de gerektirmektedir.

İlkenin gereklilikleri göz önünde bulundurulduğunda, kişisel veri işleme süreçlerinin yönetiminde, sürece dâhil olan veri sorumlusu ve beraberinde veri işleyene birçok yükümlülük getirilmektedir. Blokzincir teknolojisi vasıtasıyla gerçekleştirilen bir kişisel veri işleme faaliyetinin de şüphesiz öncelikli olarak hukuka ve dürüstlük kuralına uygun olup olmadığı tespit edilmelidir.[118]

[116] 17.03.2016 tarihli 29656 sayılı Resmî Gazete'de yayınlanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", http://www.resmigazete.gov.tr/eskiler/2016/03/20160317-2.pdf (son erişim tarihi: 06.03.2019)

[117] Kişisel Verileri Koruma Kurumu, 'Kişisel Verilerin İşlenmesine İlişkin Temel İlkeler', https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/d0fbca08-30af-41fe-a7c9-65663b9c5231.pdf (son erişim tarihi: 06.03.2019)

[118] Ayözger Öngün, Dr. Çiğdem, "Kişisel Verilerin Korunması Hukuku", İstanbul, 2019 s.134.

ii. Doğru ve gerektiğinde güncel olma ilkesi

Veri sorumlusu, her daim ilgili kişinin bilgilerini doğru ve güncel olmasını temin etmekle yükümlü olup ilgili kişiyle ilgili aynı zamanda bir sonuç ortaya koymayı hedefliyorsa aktif özen yükümlülüğünü de yerine getirmesi beklenmektedir. Böylece, bu ilke ile ilgili kişinin temel hak ve özgürlükleri korunduğu gibi beraberinde veri sorumlusunun menfaatleri de gözetilmektedir. İlkenin gerekliliklerinin yerine getirilebilmesi için kişisel verilerin elde edildiği kaynaklarının güncel olması, bu kaynakların doğruluğunun test edilmesi ve bu kapsamda makul önlemlerin alınmış olması gerekmektedir.

Blokzincir teknolojisi vasıtasıyla işlenen verilerin değiştirilmesinin mümkün olmadığı göz önünde bulundurulduğunda; Blokzincir vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetlerinde zincirde yer alan her bir verinin doğru ve gerektiğinde güncel olduğunun da temini gerekmektedir ve sorun teşkil eden bir husus da bu ilkeden kaynaklanmaktadır.[119]

iii. Belirli, açık ve meşru amaçlar için işlenme ilkesi

Veri sorumlusu tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinde, veri işleme amacının açık ve kesin olarak belirlenmesi ve aynı zamanda bu amacın meşru olmasını ifade etmektedir. Bu kapsamda amacın meşru olması; kişisel veri işleme faaliyetlerinde işlenen verilerin yapılan iş veya sunulan hizmetle bağlantılı ve aynı zamanda bu iş veya hizmetle alakalı olmasını gerektirmektedir. Bir yandan dürüstlük kuralıyla da ilişkili olan bu ilke gereği; kişisel veri işleme amaçları, belirli ve açık bir şekilde ortaya konulmalıdır.

Blokzincir teknolojisi ile gerçekleştirilen kişisel veri işleme faaliyetlerinde veri sorumlusunun zincirde yer alan ve işlemeye tabi tutulan verilerin meşru amaçlar doğrultusunda işlendiğini belirli ve açık bir şekilde ortaya koyması beklenmektedir. Bir anlamda kişisel veri işleme faaliyetlerinde veri sorumlusunun ilgili kişiye karşı yükümlülüğünü ortaya koyan bu ilke; Blokzincir'in kurgulanma yapısına göre veri sorumlusu kişilerin mutabakat yapılarını oluşturma aşamasındaki saiklerine göre değerlendirilebilecektir. Zira belli bir mutabakat yapısı ile kurgulanan dağıtık defter sistemi ile tüm paydaşların uyduğu kurallar mutabakat süreci ile birlikte sisteme eklenmesi istenen her verinin geçerli bir standarda sahip olması beklenmektedir.[120]

[119] Ayözger Öngün, Dr. Çiğdem, "Kişisel Verilerin Korunması Hukuku", İstanbul, 2019 s.144.

[120] Usta, Ahmet, Doğantekin, Serkan, 'Blokzincir 101', https://www.bkm.com.tr/wp-content/uploads/2018/06/Blokzincir-101-v2.pdf (son erişim tarihi: 06.03.2019)

iv. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ilkesi:

Kişisel veri işleme faaliyetlerinin belirlenen işleme amacının gerçekleştirilebilmesine elverişli olmasını, amaçla ilgili olmayan kişisel veri işleme faaliyetlerinden kaçınılmasını ifade etmektedir. Ayrıca amaç için gerekli olanın dışında kişisel veri işleme faaliyeti yürütülmesi aynı zamanda sınırlılık ilkesine de aykırılık arz edecektir. İlkenin ölçülülük boyutu ise veri işleme ile hedeflenen amaç arasında makul bir dengenin kurulmuş olmasını ifade eder. İlkenin bir gereği olarak; 'muhtemel' amaçlar için kişisel veri işleme faaliyeti yürütülmesi ise KVK Kanunu kapsamında tamamen yeni bir kişisel veri işleme faaliyeti olarak kabul edilmektedir.

İlkenin getirileri göz önünde bulundurulduğunda; Blokzincir teknolojisi vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetlerinin ilgili zincirin kullanım amacıyla bağlantılı, sınırlı ve ölçülü bir şekilde veri barındırmasını gerektirmektedir. Blokzincir her ne kadar çeşitli senaryolar ile kurgulanabilecek olsa da bu noktada kişisel verilerin işlenmesine ilişkin ilkelerden Blokzincir prensipleri ile en çok örtüşen ilke olarak da değerlendirilebilir.[121]

v. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme ilkesi

Yukarıda açıklamış olduğumuz "amaçla sınırlılık" ilkesinin bir gereği, işleme amacı için gerekli olan süreye uygun olarak kişisel verinin muhafaza edilmesini gerektirmektedir. Bu kapsamda, kişisel verinin amaca uygun bir süreyle muhafazasını sağlamak amacıyla veri sorumlusu tarafından uygun teknik ve idari tedbirler alınmalıdır. Amaçla sınırlılık ilkesi uyarınca veri sorumlusunca belirlenen saklama süresinin yanı sıra ayrıca veri sorumlusunun tabi olduğu ilgili mevzuatın gereği bir saklama süresi de mevcut olabilir. Bu halde, veri sorumlusunun ilgili mevzuatın getirdiği saklama süresine öncelikli olarak riayet etmesi beklenmektedir.

Bu anlamda, "değiştirilemezlik" ve "silinemezlik" prensipleri üzerine kurulu Blokzincir sisteminde kişisel verilerin belli bir noktadan sonra sistem dışına çıkarılması, diğer bir ifadeyle imha ediliyor olması gerekmektedir. Bu sebeple, Blokzincir teknolojisinin KVK Kanunu ile en ters düştüğü ilke olarak da değerlendirilebilir.

KVK Kanunu ile ortaya konulmuş olan genel ilkeler, aynı zamanda birçok uluslararası belgelerde de kabul görmüş olup pek çok ülke uygulamasına da yansımıştır.[122] Buna göre kişisel veri işleme faaliyetleri, KVK Kanunu düzenlemelerinin yanı sıra özel kanun düzenlemelerinde de yer alan kişisel veri işleme düzenlemelerine uygun olarak işlenmesini gerekmektedir. Bu

[121] Ayözger Öngün, Dr. Çiğdem, "Kişisel Verilerin Korunması Hukuku", İstanbul, 2019, s.138
[122] Ayözger Öngün, Dr. Çiğdem, "Kişisel Verilerin Korunması Hukuku", 2019, İstanbul, s. 134 vd.

doğrultuda, Blokzincir teknolojisi vasıtasıyla gerçekleştirilen kişisel veri işleme faaliyetlerinde madde düzenlemesinde sıralanmış olan ilkelere uygun hareket etmek önem arz etmektedir.

Bu anlamda Blokzincir teknolojisi ile gerçekleştirilen kişisel veri işleme faaliyetlerinin bu ilkelere uygun olarak gerçekleştirilmesi veri sorumluları bakımından kanuni bir yükümlülük arz etmektedir. Bu sebepledir ki raporun sonraki bölümlerinde yukarıda bahsi geçen sorunlara/çelişkilere yönelik çözüm önerileri sunulmuştur.

c. GDPR Kapsamında Kişisel Verilerin İşlenmesine İlişkin Genel İlkeler

Kişisel veri işleme faaliyetlerinde veri sorumlusunun yükümlülüklerini belirleyen ve ilgili kişiler ile veri sorumluları arasında menfaat dengesini kurmakta olan ilkeler, KVK Kanunu'nda olduğu gibi 95/46/EC sayılı Avrupa Birliği Genel Veri Koruma Direktifi'nin de temelini oluşturmaktadır. Kişisel verilerin işlenmesine ilişkin temel ilkeler GDPR'ın 5. madde hükmünde şu şekilde düzenlenmiştir:

*1. **Kişisel veriler:***

(a) ilgili kişi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir (hukuka uygunluk, adalet ve şeffaflık);

(b) belirtilen açık ve meşru amaçlara yönelik olarak elde edilir ve bu amaçlara uygun olmayan bir şekilde işlenemez; madde 89/(1) uyarınca kamu yararı, arşivleme, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyeti, baştaki amaçlara aykırı değerlendirilmez ('amacın sınırlandırılması');

(c) işlendikleri amaçla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır ('veri minimizasyonu');

(d) doğru ve, gereken şekilde, güncel tutulur; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili tüm makul adımlar atılmalıdır ('doğruluk');

(e) yalnızca işlenme amaçlarının gerektirdiği sürece veri sahiplerinin teşhis edilmesini sağlayacak şekilde tutulur; madde 89/(1) uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece ve veri sahibinin hakları ve özgürlüklerinin güvence altına alınması için bu Direktif uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirler alınarak, kişisel veriler daha uzun süre boyunca saklanabilir ('saklama süresinin sınırlandırılması');

(f) yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dâhil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirleri almak suretiyle güvenliğini sağlayacak şekilde işlenir ('bütünlük ve gizlilik').

2. Veri sorumlusu, 1. paragrafa uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir. ('hesap verebilirlik').

Düzenleme kapsamında sıralanan temel ilkelerin KVK Kanunu ile hemen hemen benzer nitelik taşıdığı görülmektedir. GDPR düzenlemelerinin de bir gereği olarak Blokzincir teknolojisi vasıtasıyla işlenen kişisel veriler;

- Adil ve yasal işlemeye tabi tutulmalı,
- Belirlenen amaç ile sınırlı olarak işlenmeli,
- Elde etme ve işleme amaçlarıyla ilgili ve orantılı olmalı,
- Güncel ve doğru tutulmalı ve
- Süreyle sınırlı olarak işlenmelidir.

GDPR'da yer edinmiş olan temel ilkeler, KVK Kanunu'nda yer alan temel ilkelerle benzer olmakla birlikte ilgili kişilere tanınan haklar ve veri sorumlularına getirilen yükümlülükler bakımından birtakım farklılıkları da içermektedir. Bu farklılıklardan önemli olan birkaçına değinmek gerekirse; GDPR'ın getirmiş olduğu temel ilkelerden 'güncel ve doğru tutulma' ilkesi aynı zamanda GDPR'da ilgili kişilere tanınan 'düzeltme hakkı' (*right to amendment*) ve 'silme hakkı' (*right to erasure*) da beraberinde getirmektedir. Kısaca işlenmesinde yasal ya da meşru bir amacın bulunmadığı kişisel verilerin, ilgili kişilerin talebi halinde ilgili mecralardan silinmesini düzenleyen silme hakkı veya unutulma hakkı (*right to be forgotten*) GDPR'ın 17. maddesinde düzenlenmektedir. Buna göre, silme hakkı veri sahibinin rızasıyla işlenen verinin toplanma amacının gerçekleştirilmiş ve daha fazla tutulmasının gereksiz olması ya da rızasını geri almış olması veyahut verinin işlenmesine itiraz etmiş olması halinde başvurabilecek bir hak olarak düzenlenmiştir.[123] İlgili kişinin bu hakkı 2014 yılında Avrupa Birliği Adalet Divanı'nın verdiği Google Kararı[124] ile gündeme gelmiştir. Veri sorumlusunun silme hakkına ilişkin yükümlülüğüne aynı maddenin üçüncü fıkrasında, ifade özgürlüğü ve bilgi edinme haklarının kullanılması, bir yasal yükümlülüğün gerektirmesi, kamu sağlığı kapsamında kamu yararı gereklilikleri gibi istisna haller de düzenlenmiştir. GDPR açık bir şekilde silme hakkı (unutulma hakkını) düzenlerken, KVKK'da bu yönde detaylı bir düzenleme bulunmamaktadır. Öte yandan, unutulma hakkının Yargıtay[125] ve Anayasa Mahkemesi[126] kararlarına konu edildiğini görmekteyiz.[127]

Temel ilkeler ve ilgili kişilere tanınan bu haklar göz önüne alındığında Blokzincir teknolojisi 'değiştirilemezlik' prensibi ile öne çıkarken, GDPR'ın ilgili kişilere tanıdığı haklar çerçevesinde da soru işaretleri yaratacağı açıktır.

[123] Ayözger Öngün, Dr. Çiğdem Kişisel Verilerin Korunması Hukuku", 2019, İstanbul, s. 155

[124] Google Spain SL and Google Inc. v. Agencia Española de Protección de Datoand Mario Costeja González, (C-131/12, 13.05.2014).

[125] A Yargıtay HGK, E. 2014/4-56, K. 2015/ 1679, K.T., 17.06.2015.

[126] N.B.B. Başvurusu, , E. 2014/4-56, K. 2015

[127] Ayözger Öngün, Dr. Çiğdem, "İlgili Kişinin Kişisel Verilerin Korunması Kanunu'ndan Doğan Hakları", Prof. Dr. Hüseyin Hatemi'ye 80. Yıl armağanı (80. Yıl sempozyumu tebliğleri), İstanbul, 2018, s. 374.

GDPR ilgili düzenlemesinde; KVK Kanunu düzenlemesinden farklı olarak aynı zamanda veri sorumlularına hesap verme yükümlülüğü de getirilmektedir. Dolayısıyla, Blokzincir sistemi üzerinden kişisel veri işleme faaliyetinde bulunan veri sorumlusu, kişisel verilerin işlenmesine ilişkin ilkelere uyum sağlamakla yetinmeyecek aynı zamanda uyumluluğunu ispatlaması da gerekecektir. Hesap verilebilirlik sistemi ise hiç şüphesiz Blokzincir sistemi üzerinde karşımıza çıkan bir diğer sorun olarak değerlendirilebilir.

Kanuni bir hesap verilebilirlik prensibi iki unsura sahip olmalıdır:

I. **İlkelere uyum yükümlülüğü:** Veri sorumluları, kişisel verilerin korunması prensiplerinin ve yükümlülüklerinin yerine getirilmesi için gerekli tüm önlemleri almalıdır.

II. **Gerektiğinde hesap verebilme:** Veri sorumlusu bu yükümlülüğü yerine getirdiğini, talep edilmesi durumunda düzenleyici otoriteye ispatlayabilmeli/gösterebilmelidir.

Ancak, hesap verilebilirlik yeni bir kişisel veri koruma prensibi getirmemekte veya mevcut ilkeleri değiştirmemektedir. Yalnızca mevcut ilkelerin daha etkin şekilde uygulamaya yansımasını amaçlamaktadır. Blokzincir ağı üzerinden kişisel veri işleme faaliyetinde bulunan veri sorumlusu, kişisel verilerin işlenmesine ilişkin ilkelere uyum sağlamakla yetinmeyecek aynı zamanda uyumluluğunu ispatlaması da gerekecektir.

Her ne kadar yukarıda bahsi geçtiği üzere uygulanacak hukuk anlamında tartışmalar mevcut olsa da genel/temel ilkelerin evrensel nitelikte olması sebebiyle blokzincir teknolojisinde genel/temel ilkeler büyük öneme sahiptir. Blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da bahsedilen temel/genel ilkeler bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

Blockchain ağındaki verilerin değiştirilemez olarak kabul edilmesinden dolayı verilerin güncellenmesi nasıl sağlanacaktır?

Verilerin güncel ve doğru olduğunun teyidini kim sağlayacaktır?

Veri işleme amacı ile bağdaşmayan veriler nasıl imha edilecektir?

IX. Veri Sorumlusunun Yükümlülükleri

a. Aydınlatma Yükümlülüğü

KVK Kanunu'nda veri sorumlusuna getirilen en temel yükümlülüklerden biri ilgili kişiyi aydınlatma yükümlülüğüdür. KVK Kanunu 10'uncu madde uyarınca yapılacak olan bilgilendirme asgari olarak aşağıdaki hususları içermesi gerekmektedir.

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi ve
- KVK Kanunu'nun 11'inci maddesinde sayılan diğer hakları (örneğin; kişisel veri işlendiğini öğrenme, işlenmişse bilgi talep etme, verilerin aktarıldığı 3'üncü kişileri öğrenme).

Ayrıca, 10 Mart 2018 tarihli "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ" (**"Tebliğ"**) uyarınca aydınlatma yükümlülüğü yerine getirilirken aşağıda sayılan usul ve esaslara uyulması da gerekmektedir:

- Kişisel verilerin işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir,
- Kişisel verinin işlenme amacı değiştiğinde, veri işleme faaliyetinden önce ilgili kişiye bilgi verilmelidir,
- Kişisel verilerin farklı birimlerde farklı amaçlarla işlenmesi söz konusu ise, her bir birim tarafından ayrı ayrı aydınlatma yükümlülüğü yerine getirilmelidir,
- Sicile kayıt yükümlülüğü var ise, sicile verilen bilgiler ile ilgili kişiye verilecek bilgilerin uyumlu olması gerekmektedir,
- İlgili kişinin talebinden bağımsız olarak aydınlatma yükümlülüğü yerine getirilmelidir,
- İspat veri sorumlusundadır,
- Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olması halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemleri ayrı ayrı yerine getirilmelidir,
- Kişisel veri işleme amacının belirli, açık ve meşru olması gerekmektedir,
- İlgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil ile yapılması gerekmektedir,
- Yükümlülüğün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir,
- Kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir,

>> Kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir ve

>> Eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir.

GDPR'da da yukarıdaki usul ve esaslara benzer yükümlülükler getirilmekle beraber iki ayrım yapılmıştır;

>> Verilerin doğrudan ilgili kişiden alınması ve

>> İlgili kişinin 16 yaşından küçük olup olmadığıdır.

GDPR'ın 13'üncü maddesi uyarınca, verilerin direkt veri sahibinden alındığı durumlarda KVK Kanunu'nda ve Tebliğ'de yer alan yükümlülüklerle neredeyse aynı yükümlülüklere hükmedilmiştir. Ancak GDPR'ın 14'üncü maddesi ise, verilerin ilgili kişiden başka bir kişi vasıtasıyla alındığı durumları düzenlemektedir. Bu durumda 13'üncü maddede belirtilen kriterlere ek olarak, (i) ilgili kişisel veri kategorileri ve (ii) kişisel verilerin hangi kaynaktan alındığı ve uygun olduğu hallerde kişisel verilerin kamunun erişebileceği kaynaklardan elde edilip edilmediğinin bilgileri de aydınlatma yükümlülüğü kapsamındadır.

İlgili kişinin 16 yaşından küçük olması (çocuk) durumunda ise, çocuğun kişisel verilerinin hukuka uygun olarak işlenmesi, çocuk üzerinde velayet hakkı bulunan kişinin rızası veya onayına tabi tutulmuştur. Veri işleme faaliyeti, velinin rıza verdiği veya onaylandığı ölçüde hukuka uygundur. Bu sebepledir ki, aydınlatma metni hazırlanırken, 16 yaşından küçük çocuklar için hazırlanan aydınlatma metnini çocuğun velisinin onaylaması/imzalaması gerekmektedir.

b. Açık Rıza/Rıza

Kişisel verilerin işlenebilmesi için KVK Kanunu kapsamında açık rızanın temin edilmesi gerekmektedir. KVK Kanunu çerçevesinde açık rıza, kişinin sahip olduğu verinin işlenmesine, kendi isteği ile ya da karşı taraftan gelen istek üzerine, onay vermesi anlamını taşımaktadır. Açık rıza, ilgili kişinin, işlenmesine izin verdiği verinin sınırlarını, kapsamını, gerçekleştirilme biçimini ve süresini de belirlemesini sağlayacaktır.

Açık rızanın bu anlamda, rıza veren kişinin olumlu irade beyanını içermesi gerekmektedir. Diğer mevzuattaki düzenlemeler saklı kalmak üzere, açık rızanın yazılı şekilde alınmasına gerek yoktur. Açık rızanın elektronik ortam ve çağrı merkezi vb. yollarla alınması da mümkündür, ancak açık rızanın ispat yükümlülüğü veri sorumlusuna ait olacaktır.

KVK Kanunu'nun 3'üncü maddesi açık rızanın 3 unsuru mevcuttur:

>> Belirli bir konuya ilişkin olması,

>> Rızanın bilgilendirmeye dayanması ve

>> Özgür iradeyle açıklanması.

Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar "şemsiye rızalar" olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Örneğin; "her türlü ticari işlem, her türlü bankacılık işlemi, blokzincir ağında gerçekleştirilen her türlü işlem ve her türlü veri işleme faaliyeti" gibi belirli bir konu ve faaliyeti işaret etmeyen rıza beyanları şemsiye rıza kapsamında değerlendirilebilecek durumlardır.

Açık rıza vermek, kişiye sıkı sıkıya bağlı bir hak olduğundan, verilen açık rıza geri alınabilmektedir. Bu bağlamda kişisel verilerin geleceğini belirleme hakkı ilgili kişiye ait olduğundan, kişi dilediği zaman veri sorumlusuna vermiş olduğu açık rızasını geri alabilmektedir. Yukarıda sayılan esaslar çerçevesinde veri sorumlusunun ilgili kişinin açık rızasını her zaman geri alabileceğine ilişkin bilgi vermesi oldukça önemlidir. Nitekim bu bilgilendirmenin yapılmaması halinde ilgili kişiden alınan açık rıza da hukuka uygun olmayacaktır.

KVK Kanunu bakımından bir kişisel verinin işlenebilmesi için belirli şartları barındırması gerekmektedir. KVK Kanunu 5'inci maddesi uyarınca, kural olarak kişisel veriler ilgili kişinin açık rızası olmaksızın işlenememektedir.

Ancak, aynı maddenin 2'nci fıkrası uyarınca aşağıda yer alan şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerin işlenmesi mümkündür:

- Kanunlarda açıkça öngörülmesi,
- Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
- Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
- Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
- İlgili kişinin kendisi tarafından alenileştirilmiş olması,
- Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması ve
- İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Ayrıca, yukarıda değinildiği üzere, özel nitelikli kişisel verilerin işlenmesi bakımından da kural ilgili kişinin açık rızasının temin edilmesidir. Ancak, KVK Kanunu'nun 6'ncı maddesinin 3'üncü fıkrası uyarınca:

- sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler, kanunlarda öngörülen hallerde,

>> sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilmektedir.

Eklemek gerekir ki, KVK Kanunu'nun 7'nci maddesi uyarınca kişisel veri işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel verilerin resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hale getirilmesi gerekmektedir. KVK Kanunu'nun 8'inci maddesi uyarınca ise kişisel veriler kural olarak ilgili kişinin açık rızası olmaksızın aktarılamazken, yukarıda bahsi geçtiği üzere KVK Kanunu'nun 5'inci maddesinin 2'6'nci fıkrası veya yeterli önlemler alınmakta kaydıyla KVK Kanunu'nun 6'ncı maddesinin 3'üncü fıkrası uyarınca belirtilen şartlardan birinin bulunması halinde ilgili kişinin açık rızası aranmaksızın kişisel veriler aktarılabilmektedir.

>> **Örneğin;** hastaların sağlık geçmişlerinin görüntülenmesini sağlayacak bir blokzincir ağı oluşturulacaktır. Hastaların sisteme katılabilmeleri için sağlık verilerinin işlenmesine açık rıza göstermeleri gerekmektedir. Bu örneği üç ihtimalde ele aldığımızda;

1. Ağa katılmak tamamen gönüllülük esasına dayanmaktadır. Her ihtimalde hasta gerekli tedaviyi görecektir ve rıza göstermesinin buna hiçbir etkisi olmamalıdır. Bu durumda rıza özgür iradeye dayanmaktadır.

2. Ağa katılmak için maddi bir teşvik uygulanmakta (ağa katılanların %20 indirimli hizmet alması gibi) ancak ağa katılmayanlardan standart ücret alınmaktadır. Bu durumda da rızanın özgür olduğu kabul edilecektir, çünkü ilgili kişi açısından ortaya çıkan olumsuz bir durum mevcut değildir.

3. Sisteme katılmayı reddedenlerden önemli miktarda ek ödeme yapması istenmekte ve dosyalarının işleme alınması gecikmektedir. Bu durumda ilgili kişinin rıza göstermemesi kayda değer olumsuzluklara sebebiyet verdiğinden göstereceği rızanın özgür iradeye dayandığı kabul edilmeyebilir.

GDPR'da ise "rıza"nın (*consent*) koşulları KVK Kanunu ile benzerlik göstermektedir. Direktif'in tersine, GDPR açıkça verilmiş olan rızayı benimsemekte ve ilgili kişinin "açıkça ifade etmek ya da açık bir onaylayıcı eylemde bulunma" suretiyle rıza verdiğinin anlaşıldığını ifade etmesini şart koşmuştur. Rıza; ilgi kişinin beyanı veya onayladığını belirten bir davranışı (onaylayıcı eylem) yoluyla kişisel verilerinin işlenmesini özgür iradesiyle, belirli bir konuda, aydınlatılmış olarak ve rızanın açıkça, kesin bir biçimde verilmiş olması halinde geçerlidir. Bu sebepledir ki, zımni veya varsayılan rıza kişisel verilerin işlenmesi için meşru bir zemin oluşturmamaktadır.

Özetle, KVK Kanunu ve GDPR; rızanın açık ve anlaşılır olmasını şart koşarak verilerin işlenebileceğini ifade etmektedir. Bu noktada, blokzincir ağlarında rızanın alınıp alınmadığının tespiti, ispatı veya diğer hukuka uygunluk şartlarının varlığı bakımından belli kriterlerin önceden belirlenmesi gerekmektedir.

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan açık rıza kavramı bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

- İlgili kişi açık rızasını blokzincir ağında nasıl verecektir?
- Açık rızasını veren ilgili kişi blokzincir ağında verdiği rızayı nasıl geri çekecektir?
- Blokzincir ağında açık rıza kim tarafından temin edilecektir (özellikle İzin Gerektirmeyen Blokzincir Ağları'nda durum ne olacaktır)?
- Blokzincir ağında açık rıza nasıl temin edilecektir?

c. Veri Güvenliği/Denetim Yükümlülüğü:

KVK Kanunu uyarınca veri sorumlusu; (i) kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, (ii) kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve (iii) kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. Ayrıca kişisel verilerin veri sorumlusu adına 3. kişiler tarafından işlenmesi halinde veri sorumlusu bu kişilerle birlikte müştereken sorumludur.

Veri güvenliğinin sağlanabilmesi adına ayrıca veri sorumlusu tarafından gerekli denetimlerin yapılması, öğrenilen kişisel verilerin başkalarına açıklanmaması ve işleme amacı dışında kullanılmaması gerekmektedir. Bu yükümlülük veri sorumlusu ve/veya veri işleyen kişilerin görevlerinden ayrılmalarından sonra da devam etmektedir. KVK Kanunu'nun 12'nci maddesi uyarınca verilerin kanuni olmayan yollarla elde edilmesi halinde ise veri sorumlusu bu durumu en kısa sürede ilgili kişiye ve Kişisel Verileri Koruma Kurul'a ("**Kurul**") bildirmekle yükümlüdür.

Bu noktada, özel nitelikli kişisel verilen işlenmesine ilişkin alınması gereken önlemler bakımından ise Kurul'un 31 Ocak 2018 tarihli ve 2018/10 sayılı kararının[128] incelenmesi de yerinde olacaktır. Söz konusu kararın 3'üncü maddesi uyarınca, özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise:

- verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi,
- kriptografik anahtarların güvenli ve farklı ortamlarda tutulması,
- veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması,
- verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,
- verilere bir yazılım aracılığı ile erişiliyorsa bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması ve
- verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması

gerekmektedir.

Kurul'un yukarıda bahsi geçen 2018/10 sayılı kararında belirtilen özel nitelikli kişisel verilerin kriptografik yöntemler kullanılarak muhafaza edilmesi ve güvenlik önlemlerinin alınmasına ilişkin yükümlülükler, blokzincir teknolojisi ile çok daha kolay yerine getirilebilecektir.

d. Anonimleştirme/Silme/Yok etme:

KVK Kanunu uyarınca kişisel verilerin işlenmesini gerektiren hallerin ortadan kalkması halinde veri sorumlusu resen veya ilgili kişinin talebi üzerine kişisel verileri anonim hale getirmek, silmek veya yok etmekle yükümlüdür. Veri sorumlusu aksine bir karar alınmadıkça bu yöntemlerden kendisine uygun olanı seçmektedir. Bu kapsamda yapılan bütün işlemlerin kayıt altına alınması ve diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanması gerekmektedir.

Belirtilen yöntemleri açıklamak gerekir ise, 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliği[129] uyarınca;

- silme; kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi,

[128] Kişisel Verileri Koruma Kurulu, Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı, <https://www.kvkk.gov.tr/Icerik/4110/2018-10> s.e.t. 27.06.2019.

[129] Kişisel Verileri Koruma Kurumu, 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, <http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm> s.e.t. 27.06.2019, s. 31 ve 32.

>> yok etme; kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi ve

>> anonim hale getirme; kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi

olarak tanımlanmıştır.

KVK Kanunu'nun 11'inci maddesi uyarınca veri sorumlusu yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinmeli, yok edilmeli veya anonim hale getirilmelidir. Bu sürenin herhalükarda altı ayı geçmemesi gerekmektedir. Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlusunun ise, yükümlülüğün ortaya çıktığı tarihi takip eden üç ay içinde kişisel verileri silmesi, yok etmesi veya anonim hale getirmesi gerekmektedir.

Kurum tarafından yayınlanan rehberlerde anonimleştirmeye ilişkin aşağıdaki teknikler belirlenmiştir:[130]

MASKELEME:
Kişisel verilerin belli alanlarının silinerek veya yıldızlanarak kişinin belirlenemez hale getirilmesidir.

>> Örneğin, kişinin kredi kartı numarasının bir kısmının yıldızlanması durumunda maskeleme söz konusudur. (6698 **** **** 0006)

TOPLULAŞTIRMA/KÜMÜLATİF DATA YARATMA:
Verilerin kümülatif hale getirilerek toplam değerlerinin yansıtılmasını ifade eder.

>> Örneğin, şirkette kadın çalışan sayısının Z adet olması ve sayının %40'ının üniversite mezunu, %60'ının yüksek lisans mezunu olmasına ilişkin veriler anonim hale getirilmiştir.

VERİ TÜRETME:
Mevcuttaki detay verilerin daha genel karşılıklarıyla değiştirilmesidir.

>> Örneğin, doğum tarihi bilgisinin Gün/Ay/Yıl detaylarının yerine kişinin direkt yaşının yazılması durumunda veri türetmek suretiyle anonimleştirme yapılmıştır.

VERİ KARMASI:
Veri kümesi içinde değerlerin karıştırılarak toplam faydaya zarar vermeden kişilerin tespit edilebilirlik özelliğinin yok edilmesini ifade eder.

>> Örneğin, yaş ortalaması alınmak istenen bir sınıfta kişilerin yaşlarını gösteren değerlerin birbirleriyle değiştirilmesi durumunda veri karması yapılmıştır.

[130] Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi> s.e.t. 27.06.2019, s. 31 ve 32.

İlgili kişi, KVK Kanunu'nun 13'üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir,
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde gerekli işlemlerin yapılmasını temin eder ve
- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

Sonuç olarak, farklı blokzincir ağları olmakla birlikte blokzincir teknolojisi, kayıtların herkes tarafından incelenebilmesi, kopyalarının paylaşılır olması, değiştirilemez ve aracısız olması gibi özellikleri de içermektedir.[131] Nitekim blokzincir teknolojisinin tercih edilmesinin ve blokzincir teknolojisine güvenilmesinin en büyük sebeplerinden biri "değiştirilemezlik" özelliğinin olmasıdır. Ancak bu halde ilgili kişinin taleplerinin veri sorumlusu tarafından yerine getirilebilmesi ve mevzuata uyum sağlanması oldukça güçtür.

Örneğin, ilgili kişi verilerinin silinmesi talep edildiğinde, her bir bloğun bir önceki bloğa bağlı olması sebebiyle, blokta yapılan ufak bir değişiklik bile bütün yapıyı etkileyecektir. Bu sebeple blokzincir teknolojisi kullanılmadan önce gerekliliklerin ve hangi tür blokzincir ağının kullanılmak istendiğinin başlangıçta değerlendirilmesi gerekmektedir.

Ayrıca eklemek gerekir ki, KVK Kanunu'ndan farklı olarak bu aşamada GDPR uyarınca aşağıda çok daha detaylı bahsedileceği üzere veri koruma etki değerlendirmesi (*data protection impact assessment*) de yapılması gerekmektedir.

[131] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019, s. 1.

e. Sicile Kayıt Yükümlülüğü:

KVK Kanunu uyarınca veri sorumluları kişisel verileri işlemeye başlamadan önce Veri Sorumluları Sicili'ne ("**VERBİS**") kayıt olmakla yükümlüdür.

KVK Kanunu'nun 16'ncı maddesi uyarınca yapılacak bildirimin aşağıdaki hususları içermesi gerekmektedir:

- Veri sorumlusu ve varsa temsilcisinin kimlik ve adres bilgileri,
- Kişisel verilerin hangi amaçla işleneceği,
- Veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar,
- Kişisel verilerin aktarılabileceği alıcı veya alıcı grupları,
- Yabancı ülkelere aktarımı öngörülen kişisel veriler,
- Kişisel veri güvenliğine ilişkin alınan tedbirler ve
- Kişisel verilerin işlendikleri amaç için gerekli olan azami süre.

Blokzincir teknolojisinde ise bu kişisel verilerin kayıt altına alınması ve bir ihlal durumunda bu bildirimin nasıl yapılacağı konusunda boşluklar mevcuttur. Sicile kayıtla yükümlü olan veri sorumluları, kişisel veri işleme envanteri hazırlamakla yükümlü olmalarıdır. Bu süreçler kapsamında işlenen kişisel verilerin niteliklerinin tespiti, tespit edilen kişisel verilerin niteliklerinin belirlenmesi, işlenen kişisel verinin hukuki sebebinin tespiti, kişisel veri işlemem amaçlarının tespiti, işlenen kişisel verilerin saklama süresinin belirlenmesi, işlenen kişisel verilerin aktarıldığı alıcı/alıcı gruplarının belirlenmesi, yurt dışına aktarılan kişisel verilerin belirlenmesi ve işlenen kişisel veriler için alınan teknik ve idari tedbirlerin belirlenmesi gerekmektedir. Özellikle, Açık ve İzin Gerektirmeyen Blokzincir Ağları'nda tüm verilerin işlendiği süreçlerin envantere işlenmesi oldukça zor olacaktır. Aynı zamanda bir veri ihlali veya sızıntısı ile ilgili olarak bu durumlarda kime/kimlere ve hangi kurumlara/kuruluşlara nasıl haber verileceği de sorun teşkil etmektedir.

f. Yapılan Başvuruların Cevaplanması Yükümlülüğü:

KVK Kanunu'nun 11'inci maddesi uyarınca; kişisel verileri işlenen ilgili kişiler veri sorumlusuna başvurarak kendisiyle ilgili aşağıdaki hususları öğrenme hakkına sahiptir:

- Kişisel verisinin işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

>> Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

>> Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,

>> 7'nci maddede öngörülen şartlar[132] çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

>> Kişisel verilerin eksik veya yanlış işlenmiş olması halinde ve 7'nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini istemeleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

>> İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme ve

>> Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etmedir.

Bu kapsamda ilgili kişinin talebini veri sorumlusuna yazılı olarak veya Kurul'un belirleyeceği diğer yöntemlerle iletir. Veri sorumlusu ise talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde ücretsiz olarak talebi sonuçlandırmakla yükümlüdür. Veri sorumlusu talebi kabul eder veya gerekçesini açıklayarak reddeder ve cevabını ilgili kişiye yazılı olarak veya elektronik ortamda bildirir. Başvuruda yer alan talebin kabul edilmesi halinde veri sorumlusunca gereği yerine getirilir.

g. Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü:

Yukarıda ayrıntılı olarak bahsedildiği üzere, veri sorumlusu ilgili kişinin başvurusunu cevaplamakla yükümlüdür. Bu kapsamda veri sorumlusu tarafından başvurunun reddedilmesi, cevabın yetersiz bulunması ya da süresinde cevap verilmemesi hallerinde, ilgili kişi cevabı öğrendiği tarihten itibaren 30 gün ve her halde başvuru tarihinden itibaren 60 gün içinde Kural'a şikâyette bulunabilir. Bu halde ise Kurul gerekli incelemeyi gerçekleştirir.

Kurul tarafından hukuka aykırı bir işlem tespit edilmesi halinde, veri sorumlusu kendisine yapılacak tebliğe istinaden gecikmeksizin ve en geç tebliğden itibaren otuz gün içerisinde aykırılığı gidermekle yükümlüdür. Aksi halde veri sorumlusuna idari para cezası yaptırımı uygulanmaktadır.

Yukarıda belirtilenlere ek olarak; GDPR ile KVK Kanunu arasında aşağıda açıklandığı üzere bazı farklılıklar da mevcuttur.

[132] KVK Kanunu ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

i. Veri Koruma Etki Değerlendirmesi (Data Protection Impact Assessment) - Veri Koruma Görevlisi (Data Protection Officer)

GDPR uyarınca kişisel verilerin işlenmesi aşamasında, gerçek kişilerin hak ve özgürlüklerinin ihlal edilmesinin yüksek risk taşıdığı hallerde veri koruma etki değerlendirmesi yapılması zorunludur. Veri sorumlusu tarafından ilgili değerlendirme yapılırken veri koruma görevlisine danışılması öngörülmüştür ancak KVK Kanunu'nda her iki düzenlemeye benzer bir hüküm yer almamaktadır.[133]

Veri koruma görevlisi ise yine aynı şekilde GDPR'ın 37'nci ila 39'uncu maddelerinde düzenlenen bir pozisyondur. Sağlık verileri, dini veya siyasi inançlar gibi özel nitelikli kişisel verileri işleyen tüm kurumlar için zorunlu olması gerektiği belirtilmektedir. Veri koruma görevlisi veri sorumlularının yükümlülükleri konusunda bilgilendirme yapmak, tavsiyelerde bulunmak ve uyumluluğu denetlemekle yükümlüdür.

>> İlgili kişinin kapsamlı olarak izlenmesini gerektiren veri işleme faaliyetlerinin varlığı veya veri sorumlusu veya veri işleyenin esas faaliyetlerinin kapsamlı olarak özel nitelikli kişisel verilerin işlenmesinden oluşması durumunda, veri koruma görevlisi atanma zorunluluğu getirilmiştir.

>> Veri koruma görevlisi doğrudan üst yönetimi raporlayan, gerekli bağımsızlık teminatlarına sahip, GDPR'a şirketin uyumu, ilgili kişiyle otoriteyle iletişim noktasında sorumlulukları olacaktır.

>> Veri koruma görevlisi istihdam edilebileceği, hizmet alma yoluyla da (hukuk firmaları, danışmanlık şirketleri ve benzeri) bu sorumluluk yerine getirilebilecektir. Grup şirketlerinde tek bir görevli atanabilir.

ii. Başlangıçtan İtibaren Veri Koruması (Data Protection by Default) ve Tasarımdan İtibaren Veri Koruması (Data Protection by Design)

GDPR ile KVK Kanunu arasındaki önemli farklılıklardan bir diğeri de başlangıçtan itibaren tasarımdan itibaren veri koruması yaklaşımı kavramlarıdır.[134] Her bir projeye özel olarak veri koruma yöntemleri belirlenmeli ve kişisel veriler gerekli olduğu ölçüde işlenmelidir.

>> Her türlü yeni ürün ve servisin tasarlanması aşamasında veri koruması hukuku hükümleri ile uyumluluğun gözetilmesi tasarımdan itibaren veri koruması ilkesine işaret etmektedir.

>> Başlangıçtan itibaren veri koruması ilkesi ise birtakım ürün ve hizmetlerin (örneğin, otomatik kredi verme süreçleri) oluşturulmasının ancak "gizlilik" konuları dikkate alınarak gerçekleştirilebileceğini düzenlemektedir.

[133] Intersoft Consulting, GDPR, Privacy Impact Assessment, <https://gdpr-info.eu/issues/privacy-impact-assessment/> s.e.t. 27.06.2019.

[134] Intersoft Consulting, GDPR, Privacy by Design, <https://gdpr-info.eu/issues/privacy-by-design/> s.e.t. 27.06.2019.

Blokzincir teknolojisi geliştiricilerinin GDPR'da yer alan başlangıçtan ve tasarımdan itibaren veri koruması prensipleri çerçevesinde süreçlerini tasarlamaları (*kişisel verileri koruma mevzuatı düzenlemelerini geliştirilen teknolojik süreçlerin başlangıç aşamasında söz konusu düzenlemeleri hesaba katarak bu geliştirmelerin merkezine veri koruma düzenlemelerini koymaları*) büyük önem arz etmektedir.

Blokzincir teknolojisi düşünüldüğünde KVK Kanunu'nda bu düzenlemeler yer almasa bile Kurul tarafından gerekli düzenlemelerin yapılması gerektiği görüşündeyiz.

✣ Blokzincir Ağlarında Veri Sorumlusunun Yükümlülüklerinin KVK Kanunu ve GDPR Bakımından Değerlendirilmesi

Sonuç olarak, blokzincir teknolojisinin uygulama alanı bulduğu durumlarda, KVK Kanunu ve GDPR'da tanımlanan veri sorumlusunun yükümlülükleri bakımından aşağıdaki hususlara ilişkin olası soru(n)ların ortaya çıkabileceği değerlendirilmektedir.

- Blokzincir teknolojisinde aydınlatma yükümlülüğü nasıl yerine getirilecektir?
- Blokzincir ağındaki verilerin anonimleştirilmesi nasıl olmalıdır?
- Blokzincir ağındaki verileri silmek mümkün müdür?
- Kişisel verilerin kayıt altına alınması ve bir ihlal durumunda bildirim nasıl olacaktır? (ör. VERBİS)
- Veri sorumlusunun denetim yükümlülüğünün sınırları blokzincir teknolojisinde nasıl olmalıdır? Yükümlülüklerin daraltılması mümkün müdür?

h. Yaptırımlar

KVK Kanunu'nun "Suçlar" başlıklı 17'nci maddesi uyarınca TCK'nın 135 ila 140'ıncı maddelerine atıfta bulunulmuştur.[135] Bu maddelere göre suç teşkil eden ve cezaları aşağıdaki şekilde öngörülmüştür:

>> **TCK 135 –** Kişisel verilerin hukuka aykırı olarak kaydedilmesi

Kişisel verileri hukuka aykırı olarak kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Özel nitelikli kişisel veri işlenmesi halinde ceza yarısı oranında artırılır.

>> **TCK 136 –** Verileri hukuka aykırı olarak verme veya ele geçirme

Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

>> **TCK 137:** Bu suçlar, kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle veya belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle işlenirse ceza yarı oranında artar.

>> **TCK 138 –** Verileri yok etmeme

Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

>> **TCK 140 –** Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Yukarıdaki suçların işlenmesi dolayısıyla tüzel kişiler hakkında onlara özgü güvenlik tedbirlerine hükmolunacağı belirtilmiştir.

>> **KVK Kanunu Madde 17/f.2:** KVK Kanunu'nun 7'nci[136] maddesine aykırı olarak kişisel verilerin silinmemesi veya anonim hale getirilmemesi halinde bir yıldan iki yıla kadar hapis cezası verilir.

KVK Kanunu'nun 18'inci maddesi uyarınca yer alan kabahatler aşağıda belirtilmiştir:

>> Aydınlatma yükümlülüğünü yerine getirmeyenler: 5.000 ila 100.000 TL

>> Veri güvenliğine ilişkin yükümlülükleri yerine getirmeyenler: 15.000 ila 1.000.000 TL

>> Kurul kararını yerine getirmeyenler: 25.000 ila 1.000.000 TL

>> Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğüne aykırı hareket edenler: 20.000 ila 1.000.000 TL idari para cezası verilir.

[135] KVK Kanunu Madde 17- "(1) Kişisel verilere ilişkin suçlar bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun 135 ila 140'ıncı madde hükümleri uygulanır.
(2) Bu Kanun'un 7'nci maddesi hükmüne aykırı olarak; kişisel verileri silmeyen veya anonim hale getirmeyenler 5237 sayılı Kanun'un 138'inci maddesine göre cezalandırılır."

[136] KVK Kanunu Madde 7- "(1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.
(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.
(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir."

Ayrıca KVK Kanunu'nun 18'inci maddesinin 2'nci fıkrası uyarınca, 18'inci maddede öngörülen idari para cezaları veri sorumlusu olan gerçek kişiler ile özel hukuk tüzel kişileri hakkında uygulanır. 3'üncü fıkrası uyarınca da fıkrada sayılan eylemlerin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi halinde, Kurul'un yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurul'a bildirilir.

Bunların yanı sıra idari yaptırımlara Kurul tarafından karar verileceği hükme bağlanmış olup madde gerekçesinde idari para cezalarının alt ve üst sınırlarının kanun koyucu tarafından bilinçli olarak geniş tutulduğu belirtilmiştir. Kurul, idari yaptırımlara karar verirken kabahatin haksızlık seviyesini, failin kusurunu ve ekonomik durumunu dikkate alacaktır. Dolayısıyla Kurul'un yetkisinin çok geniş olduğu görülmektedir, miktarları çok yüksek olan idari para cezalarına hükmedilmesinin önlenebilmesi açısından veri sorumlularının söz konusu yükümlülükleri yerine getirmesi büyük derecede önem taşımaktadır.

GDPR'da ise AB'de yer alan ülkeleri değil, bu ülkelerle iş ilişkisi kuran kişi ve kurumları da temelinde etkilemektedir. Yukarıda bahsedildiği üzere GDPR, şirketlerin fiziksel konumundan bağımsız olarak, AB'de yaşayan bireylerin kişisel bilgilerini toplayan ve işleyen tüm organizasyonları kapsamaktadır. Avrupa'ya gerek e-ticaret gerek ilgili ülkelerdeki fiziksel mağazaları/ofisleri üzerinden ürün veya hizmet satışı yapan tüm firmaların, kişisel veri ile ilgili işlem yapmadan önce bu verileri nasıl kullanacağıyla ilgili sıkı bir inceleme yapması gerekmektedir. GDPR ile birlikte şirketler, herhangi bir AB ülkesinde faaliyet göstersin ya da göstermesin, AB vatandaşlarına hizmet sunuyorlarsa GDPR yükümlülüklerini yerine getirmek zorundadır.

GDPR yükümlüklerini yerine getirmeyen şirketleri, yıllık global cirolarının %4'üne denk gelen veya 20 milyon Euro'ya kadar olan para cezasına hükmedebilmektedir. Veri işleme konusunda yeterli müşteri iznine sahip olmama veya temel gizliliğin ihlali gibi durumlarda azami yaptırımlar yürürlüğe girmektedir. Ancak para cezalarında kademeli bir yaklaşım sergileyen GDPR, kayıtları belirlenen standartlarda tutmayan şirketlere cirolarının %2'si gibi bir yaptırım uygulayabilmektedir. Bu kuralların hem veri sorumluları hem de veri işleyen için geçerli olduğunu ve bulut hizmetlerinin uygulamadan muaf tutulmadığını unutmamak gerekmektedir.

GDPR: 20.000.000 Euro'ya kadar veya global cironun %4'üne kadar idari para cezaları.

X. Hukuki Sorunlar ve Teknik Çözüm Önerileri

a. Giriş

Blokzincir teknolojisi, dağınık paydaşlar arasında doğrulanabilir ve değiştirilemez yapısıyla merkezi bir odak olmadan paydaşlar arasında güven yaratmayı hedeflemektedir. Blokzincir teknolojisi, yakın geçmişte giderek önem kazanmış olup; dijital olan ve dijitalleşen birçok sektörde ön plana çıkarak bunlar içerisinde değer yaratmaya başlamıştır. Kullanım alanları finans sektöründen lojistiğe kadar oldukça geniş olan bu teknoloji, aynı zamanda tek bir zincir üzerinde sayısız paydaş arasında kişisel veri işleme faaliyetlerinin gerçekleşmesini de sağlamaktadır. Blokzincir, zincirde yer alan katılımcıların gizlilik ve mahremiyetini koruyarak zincirde yer alan tüm katılımcılar için hesap verebilir ve şeffaf bir ortam sağlamaktadır. Bu nedenle, blokzincir teknolojisinin tamamen KVK Kanunu'na ve GDPR'a aykırı olduğu veya bütünüyle uyuşmadığını söylemek tutarsız olacaktır. Elbette ki, hem KVK Kanunu hem de GPDR ile uyuşmadığı düşünülen noktalar mevcuttur ancak tüm mevzuata veya tüm teknolojiye bu uyuşmazlıklar atfedilmesi hatalıdır. Bu anlamda, KVK Kanunu ve GDPR ile belirlenen temel kişisel veri işleme ilkelerine ve ilgili kişinin haklarına aykırılık taşıdığı noktalar olduğu gibi; veri sorumlularının yükümlülüklerini yerine getirmelerinde kolaylık sağlayacak birçok imkân da sunmaktadır. Bu nedenle, blokzincir teknolojisinin kişisel verileri koruma düzenlemelerindeki tüm sorunlara çözüm olmadığı açıkça söylenebilecek olmakla birlikte, gerekli çabaların gerçekleştirilmesi halinde blokzincir teknolojisinin kişisel verilerin kullanımını kontrol etmeye yardımcı bir mekanizma olabileceği söylenebilecektir.[137]

Rapor'un işbu başlığı altında hem KVK Kanunu hem de GDPR kapsamında düzenlenen hükümlerin blokzincir teknolojisi kullanılarak gerçekleştirilen kişisel veri işleme faaliyetlerinde doğurabileceği sorunlar ortaya koyulacak olup; takiben söz konusu sorunların giderilmesi için birtakım çözüm önerileri sunulacaktır. Bu noktada belirtmek gerekir ki, blokzincir teknolojisi ile ilgili mevzuat arasında uyumsuzluk yaratan hususlar, henüz herhangi bir veri koruma otoritesi veya mahkemeler tarafından çözüme kavuşturulmamış olup; regülatörlerin blokzincir teknolojisinin önemi ve unsurlarını göz önünde bulundurularak değerlendirme ve gerekli ise mevzuat değişikliği yapmaları isabetli olacaktır. Önemle vurgulamak gerekir ki, aşağıda yer verilen çözüm önerileri, blokzincir teknolojisinin mevcut uygulamalarına ilişkin olarak yaptığımız araştırmalar ve incelediğimiz kaynaklarda yer alan değerlendirmelerden yola çıkarak hazırlanmıştır.

Büyük bir potansiyeli de beraberinde getirmekte olan blokzincir teknolojisinin hayatımızda varlığını ne şekilde sürdüreceği, ilerleyen süreçlerde uygulamalar ile şekillenecek olup; bu kapsamda getirilen çözüm önerileri çeşitlendirilebilecektir.

[137] IBM Security, White paper: Blockchain and GDPR, How blockchain could address five areas associated with GDPR compliance, <https://www.ibm.com/downloads/cas/2EXR2XYP> s.e.t. 27.06.2019.

b. Blokzincir Teknolojisinde Kişisel Verilerin Korunmasına İlişkin Ortaya Çıkabilecek Hukuki Sorunlar

Rapor'un işbu bölümünde, yukarıda ilgili bölülerde detaylı şekilde açıklanan, KVK Kanunu ve GDPR kapsamında düzenlenen hükümlerin blokzincir teknolojisi kullanılarak gerçekleştirilen kişisel veri işleme faaliyetlerinde doğurabileceği soru ve sorunlara özet şekilde yer verilmektedir.

Öncelikle, blokzincir ağındaki tüm verilerin kopyasına sahip olan ana işlevli düğümlerin (masternode) dünyanın her yerinde olabileceği göz önünde bulundurulduğunda, söz konusu tam işlevli düğümlerin hangi ülkede oldukları ve/veya hangi ülkenin mevzuatının bölgesel alanı/tabiiyeti içerisinde olduklarının tespiti oldukça güçtür. Bu noktada, blokzincir ağ yapılarına hangi ülke hukukunun uygulanacağı ve birden çok ülke hukukunun aynı anda uygulanmasının mümkün olup olmadığı soruları gündeme gelmektedir.

Ek olarak, bir kişisel veri ihlali durumunda veya diğer farklı kayıt ve bildirim yükümlülükleri bakımından hangi ülke hukukunun uygulama alanı bulacağının belirsizliği nedeniyle, söz konusu yükümlülüklerin gerçekleştirilmesi de farklı bir sorun olarak karşımıza çıkmaktadır.

Ayrıca, hangi ülkelere aktarım yapıldığının tespitinin güçlüğü nedeniyle, ilgili ülkelerin yeterli koruma bulunan ülkeler olup olmadığının belirlenmesi ve Türkiye ve AB dışına kişisel veri aktarımlarında KVK Kanunu ve GDPR'da düzenlenen güvenlik önlemlerinin alınması ve benzeri yükümlülüklerin yerine getirilmesi de oldukça güç olacaktır.

Öte yandan, merkezi bir sistem üzerine kurgulanmış kişisel verilerin korunmasına ilişkin mevzuat hükümlerinin blokzincir teknolojisinin merkeziyetsiz yapısı ile örtüşmemesi nedeniyle, ağ üzerinde veri sorumlusu/sorumluları ve veri işleyenleri tespit etmek oldukça güçtür. Bu noktada, farklı blokzincir ağ türlerinde farklı değerlendirmelerin yapılabileceği de unutulmamalıdır.

Veri sorumlusunun tespitinin güçlüğü, ilgili mevzuat hükümlerinde veri sorumlusuna getirilen yükümlülüklerin nasıl yerine getirileceği noktasında da sorunlara sebebiyet vermektedir. Örneğin, ilgili kişilere tanınan haklar kapsamında ilgili kişilerin kişisel verileri hakkındaki bilgi taleplerini (örn. verilerinin aktarıldığı alıcı gruplarını öğrenme) ve itiraz, düzeltme ve silinme haklarını yönelticeleri veri sorumlusu ile veri sorumlusunun denetim yükümlülüğünü nasıl gerçekeştireceği de mevcut sistemde belirsizliğini korumaktadır. Bu noktada ayrıca, veri sorumlusunun ilgili kişileri aydınlatma ve gerekli ise açık rızalarını temin etme yükümlülüklerini nasıl yerine getirecekleri ve ilgili kişilerin açık rızalarını nasıl geri çekeceklerine dair soruların yanıtları da henüz verilememiştir.

Veri sorumlusunun belirsizliği nedeniyle söz konusu yükümlülüklerin yerine getirilip getirilmediğinin ilgili otoriteler tarafından denetlenebilirliği de değerlendirilmesi gereken ayrı bir konu olarak yerini korumaktadır.

Blokzincir teknolojisinin temel unsurları arasında yer alan değiştirilemezlik prensibi ise, ilgili kişilerin hakları arasında yer alan düzeltme hakkı ve silinme hakkının değiştirilemez olduğu kabul edilmiş olan blokzincir teknolojisinde nasıl kullanılacağı problemini doğurmaktadır. Benzer şekilde, değiştirilemez verilerin doğruluğunun ve güncelliğinin nasıl sağlanacağı ve işleme amacı ile bağdaşmayan/sona eren kişisel verilerin ilgili ağ üzerinde nasıl silineceği ise henüz yanıt bulamamış sorular arasındadır.

Yukarıda bahsi geçen hususlara ilişkin teknik çözüm önerileri üretilmeye devam ederken, ilgili otorite ve kanun koyucuların da sürece dahil olarak değerlendirmelerini sunmaları ve gerekli ise mevzuat değişikliklerini uygulamaya koymaları, ilgili teknolojinin hukuka uygun biçimde kullanımının önünün açılmasında büyük bir rol oynayacaktır.

c. Blokzincir Teknolojisinde Kişisel Verilerin Korunmasına İlişkin Teknik Çözüm Önerileri

i. Blokzincir Teknolojisinin Kullanılması Gerekliliğinin Sorgulanması

Veri sorumlularının sürecin en başında blokzincir teknolojisini kullanma kararı vermeden önce, oluşturmak istedikleri yapı ve geliştirmenin blokzincir teknolojisini gerektirip gerektirmediğini kapsamlı bir şekilde değerlendirmesi gerekmektedir. Eğer aranan çözüm, yaratılacak değer ve verilerin kullanım şekli bakımından blokzincir teknolojisinin kullanımı mantıklı ve gerekli bir çözüm ise, blokzincir teknolojisinin kullanılması isabetli olacaktır. Bu doğrultuda, ilk adımda blokzincir teknolojisini kullanma gerekliliği mutlaka sorgulanmalıdır. Takiben, blokzincir ağının kullanılacağı iş modelinde hangi blokzincir ağ türünün daha etkin, işlevsel ve mevzuata uygun olduğunun tespit edilmesi gerekmektedir. Bu değerlendirmeler ve tespitler ışığında seçilecek olan blokzincir ağı olarak, genellikle pek çok mevzuat ile uyumlaştırılması daha kolay ve kontrolün daha sıkı olduğu Kapalı ve İzin Gerektiren Blokzincir Ağları tercih edilmektedir.

ii. Blokzincir Üzerinde Kişisel Veri Saklanmaması ve Yalnızca Anonim Verilerin Saklanması

Veri sorumlusunun blokzincir teknolojisinin ilgili kişinin haklarının sağlanması ve genel kişisel veri düzenlemeleri bakımından ortaya çıkarabileceği zorlukların önüne geçmek amacıyla, blokzincir üzerinde kişisel veri saklamaktan kaçınması ve bu kapsamda blokzincir üzerinde yalnızca anonim verilerin saklanmasını sağlamak için uygulanabilir tüm veri gizleme (data obfuscation), şifreleme, birleştirme tekniklerinin kullanılması isabetli olacaktır.

Bu doğrultuda, gerçekleştirilen faaliyet kapsamında faaliyeti gerçekleştiren kişi veya kurumun veri sorumlusu sıfatına haiz olacağı değerlendiriliyorsa, bu kişi veya kurumun herhangi bir blokzincir ağında kişisel veri saklamaktan kaçınması gerekmektedir. Kişisel verilerin maskeleme tekniği ile blokzincir üzerinde saklanması hallerinde bile, maskelemenin esasen geri döndürülebilir bir şifreleme tekniği olması ve bir anonimleştirme işlemi olmaması nedeniyle bu öneri geçerliliğini koruyacaktır.

Yukarıdaki açıklamalar ışığında, GDPR uyumluluğunu sağlayabilmek adına bazı geliştiriciler, farklı yöntemler geliştirmeye başlamıştır. Bir görüş ise bir defalık anahtarlara dayanan ve bir defalık bir işlem gerçekleştiren gizli bir adresin kullanılmasını önermektedir.[138]

>> **Örneğin;** kripto para birimi Monero, yeni bir özel adres ve bir "gizli anahtar" oluşturarak işlemin alıcısını gizlemeyi başarmıştır.[139] İşlemler için tek seferlik hesapların kullanılması, her işlemin bir veya daha fazla hesabı tamamen boşaltması ve bir veya daha fazla yeni hesap oluşturması gerekliliğini ortaya çıkarmıştır.[140] Bahsi geçen yönteme, "birleştirmenin önlenmesi" (merge avoidance) denilmektedir.[141]

>> **Başka bir örnek olarak;** en yüksek günlük hacme sahip olan coinlerin başında gelen Zcash ("ZEC"), kullanıcılarına Bitcoin gibi diğer kripto para birimleri ile karşılaştırıldığında daha fazla gizlilik sağlamak için kriptografi kullanmayı amaçlayan bir kripto para birimidir. Zcash'i diğer sanal paralardan ayıran yönü ise protokol yapısıdır. Zk- SNARK ismi verilen bu protokol ile Zcash kullanıcılarının, yaptıkları bütün işlemlerde kimlikleri gizlenebilmektedir. Bitcoin'den farklı olarak ise tüm işlemlerin değerleri blokzincir içerisinde saklanabilmektedir ve yalnızca görmesi gereken kişiler görebilmektedir. Bitcoin ve Etherium'da kullanıcılar gizli kalırken, bütün işlemler görülebilmekteydi ancak Zcash ile hem kişiler hem de işlemler gizli kalabilmektedir.

Diğer bir olası çözüm önerisi ise verilere "gürültü" (noise) eklenmesidir. İlgili çözüm önerisi, birkaç işlem kaydını gruplandırmış ve böylece bir işlem kaydının dışarıdan bu işlemin göndereninin/gönderenlerinin ve alıcısının/alıcılarının kimliğinin belirlenmesini imkânsız kılmıştır. Bu modele benzer algoritmalar, Bitcoin ve Ethereum blokzincir teknolojilerinde halihazırda tanımlanmıştır.Gürültü ekleme tekniğinin 29. Madde Çalışma Grubu'nun belirlediği kriterlerin sağlanması ile kabul edilebilir bir anonimleştirme tekniği olabileceği düşünülmektedir.[142] Gürültü

[138] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s. 25.

[139] Monero, Stealth Address, The Basic, <https://www.getmonero.org/resources/moneropedia/stealthaddress.html> s.e.t. 27.06.2019.

[140] Buterin, Vitalik (2016) Privacy on the Blockchain, <https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/> s.e.t. 27.06.2019.

[141] Hearn, Mike (2013) Merge Avoidance, A note on privacy-enhancing techniques in the Bitcoin protocol, <https://medium.com/@octskyward/merge-avoidance-7f95a386692f> s.e.t. 27.06.2019.

[142] 05/2014 sayılı Anonimleştirme Tekniklerine İlişkin Görüş (2014), Çalışma Grubu 29, Executive Summary, <https://www.pdpjournals.com/docs/88197.pdf> s.e.t. 27.06.2019, s. 12 ve 13
(İlgili raporda teknik hakkında genel açıklamalar yapılmıştır, blokzincir nezdinden özel olarak yorum yapılmamıştır.)

ekleme tekniğinin anonimleştirme tekniği olabilmesi için belli niteliklerin ve yarı-tanımlayıcıların kaldırılması gibi gizliliği sağlayan ek tekniklerle birleştirilmesi gerekmektedir.[143]

CNIL, blokzincir teknolojisinin günümüzde bulunduğu noktada ilgili kişinin veri sorumlusundan kişisel verilerinin silinmesini talep etmesi halinde bu talebin karşılanmasının imkânsız olduğunu belirterek, ilgili kişinin haklarını kullanabilmesi için teknik çözümler bulunması gerektiğini belirtmektedir. Bununla birlikte, CNIL, veri sorumlusunun blokzincir ağına kaydettiği kişisel verileri maskelenmesi ve maskelemede kullanılan anahtarın veya şifreli metnin (ciphertext) silinmesi ile birlikte verilerin pratik olarak erişilemez hale getirilmesinin veri silinmesi etkisine benzer bir etkinin ortaya çıkarabileceğini belirtmektedir.[144] CNIL, blokzincir ağı üzerinde ilgili verinin hâlâ saklanıyor olması nedeniyle, bu işlemin bir veri silme işlemi olmadığını kabul etmekle birlikte, bu yöntemin ilgili kişilerin silme haklarını kullanabilmeleri noktasında efektif bir çözüme yaklaşılmasını sağladığını belirtmektedir.

iii. Zincir dışı (off-chain) Veri Saklama

Yukarıda belirttiğimiz üzere, veri sorumlularının, veri koruma düzenlemelerinin ilgili kişiye tanıdığı düzeltme ve silme hakkının kullanılabilmesini sağlaması gerekmektedir. Kişisel verilerin açık veya maskelenmiş bir şekilde blokzincir ağına kaydedilmesi halinde, teknik olarak blokzincir üzerinde yer alan verilerin değiştirilmesi veya silinmesinin mümkün olmaması nedeniyle, mutlaka zorunlu olmayan hallerde kişisel verilerin blokzincir üzerine kaydedilmemesi önemle tavsiye edilmektedir. Blokzincir teknolojisinden faydalanarak bir sistem oluşturulurken, ilgili kişinin haklarının dikkate alınması, yani sistemin kurgulanmasından önce, veri koruma düzenlemelerinin getirdiği kısıtlamalar ve ilgili kişi taleplerinin yerine getirilmesi gerekecek haller göz önüne alınarak oluşturulması önemlidir. Bununla birlikte, veri koruma düzenlemelerinin öngördüğü kişisel verilerin saklama sürelerinin belirlenmesi, bu saklama sürelerinin sonunda kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hususları da göz önünde bulundurulmalıdır.

Blokzincir teknolojisinin günümüzde bulunduğu noktada, teknolojinin bütünlüğü bozulmadan bu hakların sağlanmasının güç olmasından dolayı, kişisel verilerin blokzincir ağının dışında gizli ve özel bir ağda yani "zincir dışı" (off-chain) saklanması/depolanması ve blokzincir üzerinde yalnızca bu zincir dışı tutulan verinin ispatının (örneğin şifrelemeye ilişkin kriptografik özetlenmiş veri) yer alması önerisi ön plana çıkmaktadır.[145] İlgili verinin şifreli özetinin yer aldığı

[143] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, GDPR's Material Scope: Does Data Stored on a Blockchain Qualify as Personal Data, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s.25 ve 26.

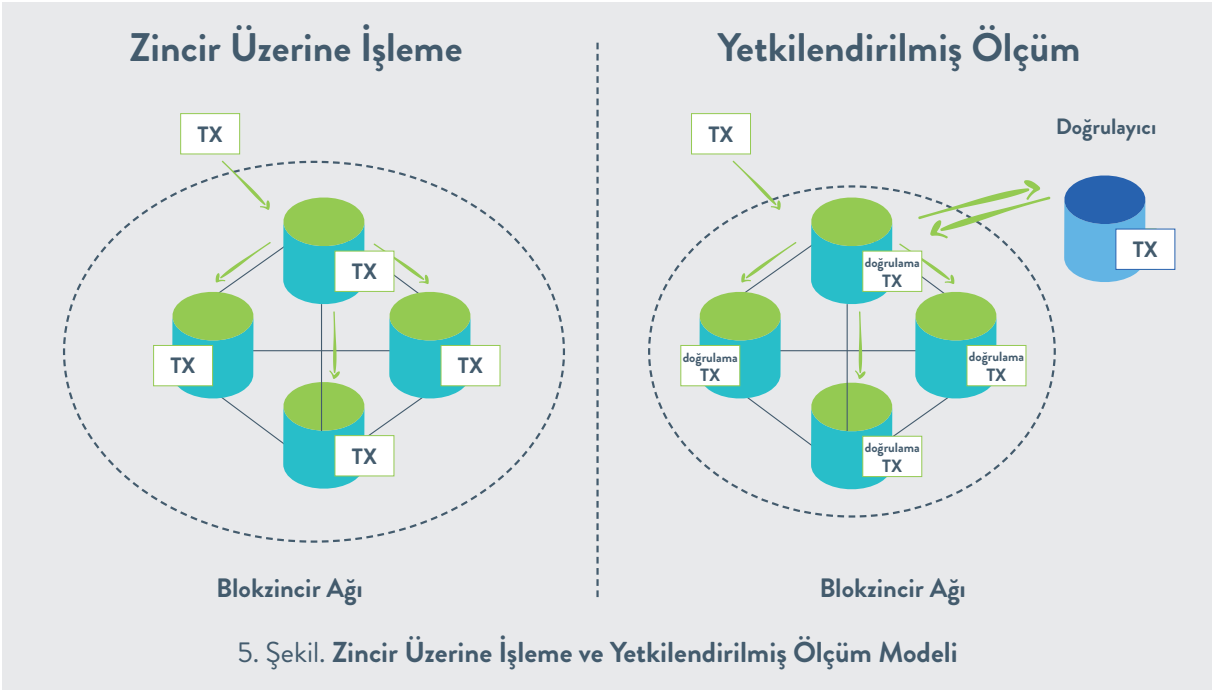
[144] CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data, <https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> s.e.t. 27.06.2019.

[145] IBM Security, White paper: Blockchain and GDPR, How blockchain could address five areas associated with GDPR compliance, <https://www.ibm.com/downloads/cas/2EXR2XYP> s.e.t. 27.06.2019.

kriptografik özet göstergesi (hash pointer) ile veriler zincire bağlanmaktadır. Bu yöntem ile kişisel veriler blokzincir üzerinde değil, referans verilen şifrelenmiş ve değiştirilebilir veri tabanına kaydedilmektedir.

Blokzincir teknolojisinin kullanımı sırasında kişisel verilerin işlenmesi gerekli ise, bu verilerin blokzincir dışında işlenmesi ve saklanması, veri koruma düzenlemeleri ve ilgili kişinin haklarını kullanabilmesi açısından çözüm olabilecektir. Ancak bu tür çözümler üzerinde çalışan geliştiriciler, "meta verinin" kişisel bilgilerin doğrudan zincirde depolanmadığı durumlarda bile kişisel bilgileri açığa çıkarılabileceğinden, dikkatli olmalıdırlar.[146] Zincir dışı depolama yöntemlerine başvurulması DLT'ye olan güveni azaltabileceği gibi güvenilir bir üçüncü tarafın katılımını da gerekli kılmaktadır. Bu durum, blokzincir teknolojisinin merkeziyetsiz ve aracıları ortadan kaldıran özelliklerini göz ardı etmeye neden olacaktır.

>> **Örneğin;** bir hastanenin hasta kayıtlarını tuttuğu sistemin blokzincir teknolojisi üzerinden yürütüldüğü durumda hastaların tıbbi kayıtları, işlem kayıtları olarak sisteme eklenecektir. Kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetleri gibi ilgili mevzuat uyarınca istisna tutulmuş durumlarda sağlık kayıtları ilgili kişinin açık rızası olmadan işlenebilmektedir. Özel nitelikli olan bu verilerin, işlenmesine gerek duyulmaması veya ilgili kişinin talebiyle silinmesinin istenmesi gibi hususlarda, blokzincir yerine kriptografik özet göstergesi ile referans olarak şifrelenmiş şeklide bir veri tabanına kaydedilmesi durumunda, zincirde herhangi bir işlem gerçekleştirilmesi gerekmeden veriler silinebilecektir.[147]



5. Şekil. **Zincir Üzerine İşleme ve Yetkilendirilmiş Ölçüm Modeli**

[146] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, GDPR's Material Scope: Does Data Stored on a Blockchain Qualify as Personal Data, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019, s. 23.

[147] Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, The Right to be Forgotten, EDPL, <https://edpl.lexxion.eu/article/edpl/2018/1/6> s.e.t. 27.06.2019.

Blokzincir ağı üzerindeki bir veriye ilişkin olarak düzeltme veya silme hakkının kullanılması mümkün değilken, kişisel verilerin zincir dışında tutulması halinde bu hakların ilgili kişi tarafından kullanılmak istenmesi durumunda, veri sorumlusu tarafından ilgili düzeltme veya silme işlemi zincir dışında gerçekleştirilebilecektir. Bu durumda, zincir dışı ağda yer alan kişisel verilerin silinmesi ile birlikte, blokzincir ağı üzerinde yalnızca kişisel verinin zincir dışında saklandığını teyit eden kriptografik özetlenmiş veri "silinememiş" şekilde kalmış olacak olup, kişisel verilerin blokzincir ağı üzerinde ağ hayatta olduğu sürece saklanması problemi çözülmüş olacaktır.

iv. Hata Kaydının Zincire Eklenmesi

İlgili kişi tarafından verilerin düzeltilmesine ilişkin talebin veri sorumlusuna iletilmesinde; talebe konu verinin düzeltildiğine dair zincire kayıt eklenmektedir. Bu kayıt ile önceki verinin silindiği, hata olduğu ve/veya düzeltildiğine ilişkin bilgilendirme mevcuttur ancak bu yöntem ile birlikte her ne kadar zincirde ilgili verinin değiştirildiğine dair bir beyan mevcut olsa da doğru olmayan verinin hâlâ zincirde görünüyor olması sebebiyle eleştiriler de mevcuttur.[148]

[148] Ibáñez, Luis-Daniel ve O'Hara, Kieron ve Simperl, Elena (2017) On Blokzincirs and the General Data Protection Regulation, University of Southampton, <https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf> s.e.t. 27.06.2019.

d. Sonuç

Yukarıda yer alan açıklamalar ışığında, KVK Kanunu ve GDPR hükümleri ile blokzincir teknolojisinin çeliştiği alanların mevcut olduğu değerlendirilebilecek olsa da, söz konusu uyumsuzlukların giderilmesi için her geçen gün yeni hukuki ve teknik çözüm önerileri sunulmaya devam etmektedir. Öte yandan blokzincir teknolojisinin, kişisel verilerin korunmasına ilişkin mevzuat düzenlemelerinde yer verilen yükümlülüklerin daha sağlıklı ve kolay şekilde yerine getirilmesini sağlayan pek çok pozitif katkısı olabileceği de göz ardı edilmemelidir. Bu nedenle, blokzincir teknolojisinin bütünüyle KVK Kanunu'na veya GDPR'a aykırı olduğuna ilişkin tespitlerin hatalı olduğu değerlendirilmektedir.

Ayrıca, kişisel verilerin korunması mevzuatına uyumluluk, teknoloji ile ilgili olmayıp; teknolojinin nasıl kullanıldığına ilişkindir. Nasıl ki kişisel verilerin korunması mevzuatı ile uyumlu internet yok ise, kişisel verilerin korunması mevzuatı ile uyumlu bir blokzincir teknolojisi de bulunmamaktadır. Bu nedenle, ilgili mevzuat ile uyumlu blokzincir uygulamaları ve kullanım senaryoları oluşturulmalıdır.[149]

Dolayısıyla, ilgili otorite ve yargı koyucuların konuya ilişkin değerlendirmelerinin devam ettiği ve farklı çözüm önerilerinin üretilmeye devam ettiği içinde bulunduğumuz bu ara dönemde, blokzincir teknolojisi kullanılmaya başlanmadan önce öncelikli olarak blokzincirin kullanılacağı alanda ilgili teknolojinin kullanımının gerekli olup olmadığının değerlendirilmesi yapılmalıdır. Eğer blokzincir teknolojisinin kullanılması zorunlu/gerekli ise, kullanılacak alana özgü olarak hangi blokzincir ağ türünün daha etkin ve mevzuat ile uyumlu olduğu tespit edilmeli; oluşturulacak kullanım senaryoları ise mevcut mevzuat hükümleri ile uyumlu olacak şekilde tasarlanmalıdır.

[149] The European Union Blockchain Observatory and Forum (2018) Blockchain and the GDPR, European Commision, <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf> s.e.t. 27.06.2019, s. 20.

KAYNAKÇA

a. Mevzuat ve Kararlar

YABANCI

1. 27 Nisan 2016 tarihli 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü
2. İnsan Hakları Evrensel Bildirgesi
3. İnsan Hakları Evrensel Beyannamesi
4. İnsan Hakları ve Temel Özgürlüklerin Korunmasına İlişkin Sözleşme
5. 2016/8576 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi
6. 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi
7. 3/2018 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Bölgesel Kapsamı Hakkındaki Rehber
8. Çalışma Grubu 29, 04/2014 sayılı Anonimleştirme Tekniklerine İlişkin Görüş (2014)
9. Çalışma Grubu 29, 8/2010 sayılı ABAD'ın Google Spain kararının ışığındaki yürürlükteki yasalarla ilgili görüşünün güncel versiyonu
10. Judgment of the Court, 1 Ekim 2015, C-230/24, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság
11. 25 Haziran 2013, C-131/12, Google Spain SL-Google Inc./Agencia Española de Protección de Datos-Mario Costeja González
12. ABAD, 12 Mayıs 2016, C 582/14, Patrick Breyer ve Bundesrepublik Deutschland
13. ABAD, 6 Ekim 2015, C-362/14, Maximillian Schrems ve Data Protection Commissioner

YEREL

14. 18 Ekim 1982 tarihinde kabul edilen 9 Kasım 1982 tarihinde yayımlanan 2709 kanun numaralı Türkiye Cumhuriyeti Anayasası
15. Kişisel Verilerin Korunması Kanunu Tasarısı
16. 6698 sayılı Kişisel Verilerin Korunması Kanunu
17. Kişisel Verileri Koruma Kurumu, 6698 Sayılı Kanun'da Yer Alan Terimler
18. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Yurt Dışına Aktarılması Rehberi
19. Kişisel Verileri Koruma Kurulu, "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı
20. Kişisel Verileri Koruma Kurumu, 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
21. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi

b. Makale ve Kitaplar

1. Usta, Ahmet ve Doğantekin, Serkan (2018), Blockchain 101, İkinci Baskı (güncellenmiş versiyon), Bankalararası Kart Merkezi
2. Ayözger Öngün, Dr. Çiğdem Kişisel Verilerin Korunması Hukuku, İstanbul, 2019
3. Unal, Engin (2018), Bitcoin ve Blockchain Nedir? Nasıl Çalışır?
4. Blok Zinciri Teknolojisi Temelli, Sağlık Verilerinize Hızlı ve Güvenli Erişimi Sağlayacak ve Hayat Kurtarabilecek Yeni Bir ICO: MEDICHAIN (2018), Criptotürk
5. Koinbülteni, KYC (Know Your Client) Nedir?, Know Your Client – Müşterini Tanı
6. The European Union Blockchain Observatory and Forum (2018), Blockchain and the GDPR, European Commision
7. OECD, İstatistik terimler sözlüğü, Otomatik Veri İşleme

8. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, İlk (Orijinal) Versiyonu
9. Information Commissioner's Office, Guide to the General Data Protection Regulation (GDPR), The Principles
10. IBM Security, White paper: Blockchain and GDPR, How blockchain could address five areas associated with GDPR compliance
11. CNIL (2018) Blockchain Solutions for a responsible use of the blockchain in the context of personal data
12. Brito, Jerry ve Castilllo, Andrea, Bitcoin A Primer for Policymakers (2013), 1. Basım, Virginia, Mercatus Center George Mason University
13. Woolf, Nicky (2017), Everything You Need to Know About Blockchain But Were Too Embarrassed to Ask
14. Song, Jimmy (2018), Why Blockchain is Hard
15. Organization for Economic Co-Operation and Development, The OECD Privacy Framework (2013)
16. Dr. Munz, Martin, Hickman, Tim ve Goetz Matthias, (2016), Court confirms that IP addresses are personal data in some cases, White and Case
17. Maldoff, Gabe (2016), Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization, iapp
18. Dr. Finck, Michéle (2018), Blockchains and Data Protection in the European Union, EDPL
19. Transactional Data, What does Transactional Data mean?
20. Biryukov, Alex, Khovratovich, Dmitry ve Pustogarov, Ivan (2014), Deanonymisation of Clients in Bitcoin P2P Network, University of Luxemburg
21. Torre, Lydia F de la (2019), Blockchain: Challenges and solutions for compliance with the GDPR
22. Kunde, Elke ve Dr. Kaulartz, Markus ve Naceur, Med Ridha Ben ve Liban, Samater ve Kunz, Matthias ve Prof. Dr. Skwarek, Voler ve Prof. Dr. Adam, Kataria ve Weiß, Rebekka ve Liesenjohann, Marco (2018) Blockchain und Datenschutz, Faktenpapier, bitkom
23. Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254)
24. Dr. Kaufmann, Jörg, Blockchain meets Data Privacy, Blockchain and the Data Controller
25. The European Union Blockchain Observatory and Forum (2018), Blockchain and the GDPR, European Commision
26. CMS Law and Tax (2019), The tension between GDPR and the rise of blockchain Technologies
27. Humbeeck, Van Andries (2017), The Blockchain – GDPR Paradox
28. S. Jimi (2018), Blockchain: What are nodes and masternodes?
29. Hajdarbegovic, Nermin (2014), Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack, coindesk
30. De la Torre, Quora, May 25, 2016, What are the differences between a Bitcoin exchange vs a Bitcoin wallet Website
31. Bacon, Jean ve Michels, Johan David ve Millard, Christopher ve Singh, Jatinder, Blockchain Demystified: A Technical Sayı Issue
32. Intersoft Consulting, GDPR, Privacy Impact Assessment
33. Intersoft Consulting, GDPR, Privacy by Design
34. Golaw (2018), Blockchain and data protection- Does the Blockchain technology adequately protect personal data?
35. Belic, Ivana (2018), Tilburg University, 'Data Protection Challenges of public permissionles Blockchains in relation to the GDPR'
36. Hogan Lovells (2017), A guide to Blockchain and data Protection
37. Monero, Stealth Address, The Basic
38. Buterin, Vitalik (2016), Privacy on the Blockchain
39. Hearn, Mike (2013), Merge Avoidance, A note on privacy-enhancing techniques in the Bitcoin protocol
40. Eberhardt, Jacob ve Tai, Stefan (2017), On or Off the Blockchain? Insights on Off-Chaining Computation and Data, Information Systems Engineering
41. Ibáñez, Luis-Daniel ve O'Hara, Kieron ve Simperl, Elena (2017), On Blokzincirs and the General Data Protection Regulation, University of Southampton
42. Ayözger Öngün, Dr. Çiğdem, "İlgili Kişinin Kişisel Verilerin Korunması Kanunu'ndan Doğan Hakları", Prof. Dr. Hüseyin Hatemi'ye 80. Yıl armağanı (80. Yıl sempozyumu tebliğleri), İstanbul

KATKI SAĞLAYAN KİŞİLER

Av. Burcu Çavdar

Bankalararası Kart Merkezi A.Ş.

Av. Zeynep Aga Tevetoğlu

Av. Dr. Mete Tevetoğlu

Stj. Av. Elvan Sunar

Boğaziçi Ventures A.Ş.

Av. Selin Başsimitci

Av. Ayça Aktolga Öztürk

BtcTurk (Eliptik Yazılım ve Ticaret Anonim Şirketi)

Stj. Av. İlayda Gedik

Av. Tuğçe Gelir

BTS&Partners

Av. A. Ülkü Solak

Av. Nihan Akkaş

Nazalı Avukatlık Ortaklığı

Av. Yaşar K. Canpolat

Canpolat Legal

Av. Çiğdem Ayözger Öngün

Av. Begüm Hande Ertürk

Av. Güneş Yılmaz

SRP-Legal - Dr. Av. Çiğdem Ayözger Öngün Hukuk Ofisi

Av. Özcan Kemer

Av. Didem Kalaycıoğlu Birol

Av. Özlem Akay

Turkcell İletişim Hizmetleri Anonim Şirketi

BLOCKCHAIN

TÜRKİYE

TBV

TÜRKİYE BİLİŞİM VAKFI