Finans Hukuku Gündemi Dergisi
Sayı 4, Temmuz 2020

KANUNUM

BLOKZİNCİR PROJELERİ ÖZELİNDE KİŞİSEL VERİLERİN KORUNMASI KANUNU'NA İLİŞKİN HUKUKİ DEĞERLENDİRMELER

Elçin Karatay
Mutlucan Solak
Begüm Ergin

Özet: "Blokzincir" teknolojisi kullanılarak geliştirilen projelerin sayısı her geçen gün artmakta ve merkezi bir otorite olmaksızın kişiler arasında elektronik veri aktarımının gerçekleştirilebildiği ve doğrulanabildiği güven sistemleri ile birçok sektörde yenilikçi çözümler üretilmektedir. Geliştirilen blokzincir tabanlı çeşitli projelerde dağıtık veri tabanlarında kişisel veriler işlenebilmekte ve saklanabilmektedir. Öte yandan, Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği'nde yürürlükte olan *General Data Protection Regulation* başta olmak üzere, kişisel verilerin korunması alanındaki birçok düzenleme merkezi gerçek veya tüzel kişilerin veri işleme, saklama, silme ve benzeri uygulamaları gerçekleştireceği yönündeki öngörü ile hazırlanmıştır. Bu bağlamda, bahsi geçen hukuki düzenlemelerde yer alan hükümlerin blokzincir tabanlı projelere uygulanması noktasında bazı uyumsuzluklar oluşacağı görülmektedir. İşbu çalışmada, blokzincir tabanlı projelerde kişisel verilerin işlenmesine ilişkin olarak Kişisel Verilerin Korunması Kanunu'nda öngörülen genel yükümlülüklerin uygulanmasındaki zorluklara değinilmiş ve bu yükümlülüklere uyum sağlanabilmesi için projelere adapte edilebilecek bazı çözüm önerileri hukuki olarak incelenmiştir.

I.Giriş

7 Nisan 2016 tarihinde yürürlüğe girmiş olan 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**"), kişilerin temel hak ve özgürlüklerini korumak amacıyla kişisel verilerin işlenmesine ilişkin esasları belirlemekte ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Blokzincir teknolojisi kullanılarak, merkezi bir otorite olmaksızın kişiler arasında elektronik veri aktarımının gerçekleştirilebildiği, dağıtık bir veritabanı ile "güven merkezleri"ni ortadan kaldıran güvenli, izlenebilir ve verimli projelerin hayata geçirilmesi için yapılan çalışmaların sayısı her geçen gün artmaya devam etmektedir.

Ancak, blokzincir teknolojisi kullanılarak geliştirilen projelerde kişisel verilerin saklanmasında; merkezi gerçek veya tüzel kişilerin veri işleme, saklama, silme ve benzeri uygulamaları gerçekleştireceği yönündeki öngörü ile hazırlanmış KVKK ve Avrupa Birliği'nde yürürlükte olan Genel Veri Koruma Tüzüğü'nde (*General Data Protection Regulation*, "**GDPR**") yer alan hükümlerin uygulanması bazı durumlarda uyumsuzluklar oluşturmaktadır. Yabancı hukuk doktrininde, konuya ilişkin tartışmalar özellikle iki temel eksende toplanmaktadır. Bunların ilki, "*immutable*" olarak ifade edilen değiştirilemez veri bütünü oluşmasını sağlayan *blokzincir*

teknolojisi kullanılarak dağıtık veri tabanlarına işlenen verilerde, GDPR kapsamında getirilen "silme" yükümlülüğüne uyumun sağlanabilmesine ilişkin; ikincisi ise "*public blockchain*" olarak adlandırılan ve "halka açık blokzincir", "herkese açık blokzincir" veya "ortak blokzincir" olarak nitelendirilebilecek, herkesin verilerin kopyasını bulundurma ve çoğu zaman yeni bloklar oluşturma yetkisine sahip otorite (blokzincir türüne göre "*node*" yani "bağlantı noktası" yahut "düğüm" veya "*miner*" yani "madenci" olarak adlandırılabilmekte ve farklı işlemler yapabilmektedirler) olarak görev yapabildiği durumlarda, veri sorumlularının tespit edilebilmesi ve sisteme veri işleyen kişiler ile veri sorumlularının sorumluluklarının belirlenebilmesine ilişkindir (Commission Nationale L'informatique et des Libértes, 2018; Finck, M., 2017; Toth, A., 2018; Ibanez, L. D. et al, 2018; Ferrari, V., 2018). Bunların yanında hukuka uygunluk sebepleri arasında yer bulan alenileştirme kavramının *blokzincir* projeleri ve dağıtık veri tabanı bakımından nasıl değerlendirilmesi gerektiği de tartışılabilmektedir.

Biz bu çalışmamızda KVKK ekseninde blokzincir ile geliştirilen projelerde verilerin saklanması, işlenmesi ve silinmesi gibi işlemlere ilişkin ortaya çıkabilecek hukuki problemlere değinmeyi; yabancı hukuk doktrini ve uygulamasında öngörülmüş çözüm önerilerini değerlendirmeyi ve bu kapsamda ilgili problemlere ilişkin hukuki çözüm önerilerimizi paylaşmayı amaçlamaktayız.

II. Blokzincir Projeleri Özelinde Kişisel Verilerin Korunması Kanunu'na İlişkin Hukuki Değerlendirmeler

KVKK'nin 1'inci maddesi ("**m.**") uyarınca, KVKK'nin amacı, kişisel verilerin işlenmesinde özel hayatın gizliliği ile birlikte kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülüklerini düzenlemektir. Bu kapsamda, KVKK'nin bütününde, "veri işleyen" ve "veri sorumlusu" tanımları altında üçüncü kişilerin kişisel verileri ile çeşitli ilişkiler kuran kişilere, bu kişisel verileri Anayasa'ya uygun olarak korumaları ve kendileri veya başka kişiler tarafından verileri işlenen kişilerin haklarına haksız olarak müdahalede bulunmamaları için yükümlülükler getirilmiştir.

KVKK'nin gözettiği kişisel verilerin korunması amacı, blokzincir temelli birçok projede de kendini göstermektedir; merkezi kuruluşlara ihtiyaç duymadan kişilerin kendi kişisel verilerini işleyebilmesi ve verilerin doğruluğunu teyit edebilmelerini sağlayan bu sistem, hem verilerin değiştirilmesinin önüne geçmekte, hem de verileri merkezi kurumlar da dahil üçüncü kişilerle doğrudan paylaşmadan işleme imkanı yaratmaktadır. Kişisel verilerin işlenmesi ve korunması noktasında sistemde çığır açıcı bir bakış açısı kazandıran blokzincir tabanlı projeler çoğu zaman; bu işlevlerin hayata geçirilebilmesi için (yeni geliştirilen ve bu kaygıları önleyen teknolojilerin kullanılmadığı projelerde) verilerin veya bunların şifrelenmiş "*hash* "lerinin (Bir değeri başka bir değere dönüştüren fonksiyonlar "özet fonksiyon" ve dönüşen değer ise "özet değer" olarak da ifade edilmektedir ve bir verinin ilgili fonksiyon tarafından belirli sayıda karakter içeren yahut belirli bir kurala uygun olan bir değere dönüşmesi ile dönüşen değer ifade edilmektedir) herkes tarafından görülmesine de sebep olmaktadır. Kişisel verilerin korunması açısından hem olumlu hem de olumsuz sonuçlar doğurabileceği söylenebilecek bu durum çalışma kapsamında ayrıntılı olarak incelenecektir.

Dağıtık bir sistemde, merkeziyetsiz olarak veri işlenmesi ve doğrulanması bakımından tartışma konularını belirleyebilmek için öncelikle KVKK sisteminin temelini oluşturan "kişisel veri", "kişisel verilerin işlenmesi", "veri sorumlusu" ve "veri işleyen" tanımları incelenmeli ve bunların uygulanabilirliği denetlenmelidir.

A. KVKK Sisteminde "Kişisel Veri" Tanımının Blokzincir Tabanlı Projeler Açısından İncelenmesi

KVKK m. 3/1(d) uyarınca "kişisel veri", kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. KVKK m. 3'ün gerekçesinde, kişisel verinin yalnızca bir bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgileri de kapsadığı ifade edilmiştir. Bu durumda, örneğin Bitcoin blokzinciri özelinde, bir kişinin sahip olduğu dağıtık veri tabanında saklanan bitcoin sayısı, hangi cüzdanlar üzerinden diğer hangi cüzdanlar ile kaç bitcoin üzerinden işlem yaptığına ilişkin veriler ilgili kişilerin kişisel verisi olarak nitelendirilecektir.

KVKK m. 3'ün gerekçesinde ayrıca bir kişinin belirli veya belirlenebilir olması, mevcut verilerin herhangi bir şekilde bir gerçek kişiyle ilişkilendirilmesi suretiyle, o kişinin tanımlanabilir hale getirilmesini ifade edeceği açıklanmıştır. Bu durumda, her ne kadar veri tabanında verilerin kendileri değil özet değerleri, yani bir algoritmadan geçirilerek "şifrelenmiş" izdüşümleri tutuluyor olsa da; ilgili özet değerlerin veya başka bir şekilde dağıtık veri tabanında tutulan bilgilerin o kişiyle ilişkilendirilebildiği durumlarda bu özet değerler veya diğer verilerin de kişisel veri olduğunun kabulü gerekecektir. Bu noktada, gerekçede örnek verilirken telefon numarası, motorlu taşıt plakası, özgeçmiş gibi verilere yer verilmiştir. Bitcoin veri tabanında bir kişinin ödeme aldığı bitcoin cüzdan numarasının bilinmesi durumunda ilgili cüzdandan yapılan her işlem takip edilebildiği için; gerekçedeki açıklamalar ışığında, her ne kadar kendiliğinden ilgili kişinin kimliğini ortaya çıkarmasa da karakterlerden oluşan bitcoin cüzdan numaralarının kişisel veri olduğu öne sürülebilecektir.

B. KVKK Sisteminde "Kişisel Veri İşlenmesi" Tanımının Blokzincir Tabanlı Projeler Açısından İncelenmesi

KVKK m. 3/1(e) 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 hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade etmektedir.

KVKK m. 3'ün gerekçesinde kişisel veri işlenmesi kavramının, verilerin ilk defa elde edilmesinden başlayarak veriler üzerinde gerçekleştirilen tüm işlem türlerini ifade ettiği açıklanmaktadır. Bu durumda, blokzincir ve dağıtık veri tabanları açısından hangi işlemlerin veri işleme olarak nitelendirilebileceği incelenirken genel olarak iki işlem türüne değinmek

gerekecektir. Bu işlem türlerini irdeleyebilmek için blokzincir projelerinde büyük oranda işlem gören iki tür düğümün (*node*) işlevleri açıklanmalıdır. Genel olarak blokzincir ağlarında "*validating nodes*" yani "onaylayıcı düğümler" olarak adlandırılan ve dağıtık deftere (*distributed ledger*) kuralları belirlenmiş olan bir algoritmaya göre veri eklemeye izni olan düğümler; ve "*participating nodes*" yani "katılımcı düğümler" olarak adlandırılan ve senkronize edilmiş veriyi (veya bu verinin bir bölümünü) kendi bünyesinde saklayan düğümler bulunmaktadır. Katılımcı düğümlerin de dağıtık deftere veri yüklemeleri mümkündür ancak bu verilerin öncelikle bir onaylayıcı düğüme gönderilmesi gerekmektedir (EU *Blockchain* Observatory and Forum, 2018, s. 14). Bitcoin blokzincirinde herkes her iki düğüm olarak da görev alabilmektedir, herhangi bir kişi ilgili yazılımı bilgisayarına yükleyerek tüm veri bütününü kopyalayabilir, saklayabilir ve inceleyebilir; bunun yanı sıra bilgisayarında çalıştırdığı program ile blok oluşturulmasına katkı sağlayabilir. Bu sebeple, Bitcoin blokzinciri halka açık veya herke açık ("*public*") ve izne gerek olmayan ("*permissionless*") bir ağ olarak adlandırılmaktadır. Ancak farklı teknolojiler ile geliştirilen blokzincir ağlarında herkesin verileri görmesine izin verilirken, dağıtık deftere veri ekleyen kişilerin sınırlandırılması veya gerek verileri gören, gerekse ekleyen kişilerin sınırlandırılması gibi örneklere rastlanmaktadır (EU Blockchain Observatory and Forum, 2018, s. 15).

Bu durumda, gerek dağıtık veri tabanında blok oluşturan ve veri ekleyen onaylayıcı düğümlerin, gerekse kendilerine ait veya başkalarının verilerinin onaylayıcı düğümlere gönderilmesine vesile olan katılımcı düğümlerin (ortada bir kişisel veri olması durumunda) bu verileri KVKK anlamında işledikleri iddia edilebilecektir.

Dikkat edilmesi gereken bir husus, GDPR m. 2 kapsamında "salt kişisel veya ailevi/evle ilgili faaliyetler kapsamında gerçek kişi tarafından gerçekleştirilen veri işleme" faaliyetlerinin ticari olmayan amaçlarla yapılması halinde GDPR'ın uygulama kapsamından istisna tutulmuş olmasına rağmen, benzer bir istisnaya yer veren KVKK'de ilgili istisnanın yalnızca m. 28/1(a) kapsamında "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" için verilmiş olmasıdır. Bu durumda, özellikle halka açık olan, yani verilerin tüm sistem kullanıcıları ile paylaşıldığı ve herkesin verileri kaydederek inceleyebildiği sistemlerde, kişisel verilerin "üçüncü kişilere verildiğinden" bahisle, GDPR kapsamında değerlendirilebilecek bu istisna KVKK kapsamında uygulanamayacaktır. Bu durumda, özellikle ilgili *blokzincir* ağını kullanan kullanıcıların veya kendi kişisel verileri ile işlem yapan ve bu kişisel verileri işlerken ticari bir amaç gütmeyen düğümlerin GDPR m. 2 kapsamında ilgili kanunların uygulanmasına tabi olmadıkları söylenebilecekse de (Commission Nationale L'informatique et des Libértes, 2018); aynı yorumun KVKK açısından yapılması mümkün olmayacaktır (Karatay, E ve Solak, M, 2019).

C. KVKK Sisteminde "Veri Sorumlusu" Tanımının Blokzincir Tabanlı Projeler Açısından İncelenmesi

KVKK m. 3/1(ı) uyarınca "veri sorumlusu", kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir. KVKK m. 3'ün gerekçesinde de ayrıntılı olarak belirtildiği üzere, veri sorumluları yalnızca tüzel kişiler değil gerçek kişiler de olabilmektedir. Bu durumda, 6098 sayılı Türk Borçlar Kanunu uyarınca bir adi ortaklığın varlığı halinde, temsile yetkili ve kişisel verilerin işlenme amaç ve vasıtalarını belirleyen adi ortaklık ortakları da veri sorumlusu olabileceklerdir.

Bir gerçek veya tüzel kişiyi veri sorumlusu olarak nitelendirebilmek için gerekli olan unsurların sayıldığı KVKK m. 3/1(ı) uyarınca, veri sorumlusunun kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen kişi olduğu söylenmiştir. GDPR'da da "*data controllers*" yani veriyi kontrol eden kişiler tanımı altında benzer bir açıklamaya yer verilmiştir. Kişisel Verileri Koruma Kurumu tarafından çıkarılmış olan kitapçıklarda (Veri Sorumlusu ve Veri İşleyen, 2018, s. 3) veri sorumlusunun tespiti için kişisel verilerin toplanması ve toplama yöntemi, toplanacak kişisel veri türleri, toplanan verilerin hangi amaçlarla kullanılacağı ve benzeri kriterlerin dikkate alınacağı belirtilmiştir. Bu durumda, veri sorumlularının belirlenebilmesi için *blokzincir* tabanlı sistemlerde kimlerin verilerin toplanması ve toplama yöntemlerine ilişkin karar verme yetkisine sahip olduğu ve verileri işleme amaç ve vasıtalarını belirlediği incelenmelidir.

Halka açık olmayan ve izne tabi olarak veri işlenmesine izin veren dağıtık veri tabanı sistemlerinde; ilgili verilerin nasıl işleneceğine karar veren kişilerin belirlenebileceği (örneğin sistemi işleten ve onaylayan düğümleri yöneten kişiler) iddia edilebilse de özellikle halka açık ve herhangi bir izin gerekmeksizin işleyen dağıtık veri tabanlarını kullanan sistemlerde verinin nasıl işleneceği noktasında karar veren kişi veya kişileri belirlemek çok güçtür. Nitekim, halka açık ve izin gerekmeksizin işleyen blokzincir sistemlerinde münferit bir kontrol noktası bulunmamakta, aksine, tüm ağ düğümler tarafından topyekûn işletilmektedir; herkes ilgili ağlara katılabilmekte, sistemleri kullanabilmekte ve tanımadığı veya güvenmediği kişiler ile etkileşimde bulunabilmektedir (Finck, 2018). Bu noktada, yabancı doktrinde GDPR özelinde, ilgili açık ve izne gerek olmaksızın çalışan sistemlerde protokolü geliştiren yazılımcılar, onaylayan düğümler (*validating nodes*) ve sisteme kendi verilerini işleyen yahut sistemin kopyalarını kendilerinde tutan kullanıcıların veri sorumlusu olup olamayacakları tartışılmıştır.

Protokolü geliştiren yazılımcılar açısından yapılan incelemede, her ne kadar ilgili protokol ve algoritmalar geliştirilirken yazılımcıların verileri işleme amaç ve vasıtalarını belirledikleri iddia edilebilse de; bu yazılımcıların özellikle açık kaynak kodlu, halka açık ve izin almaksızın kullanılabilen dağıtık veri tabanlarının işletilmesinde, yalnızca yazılımın ilk halini geliştiren kişiler oldukları ve ilgili kuralları uygulayan konumunda olmadıkları, onaylayan düğümlerin kendi aralarında bir uzlaşmaya vararak onay mekanizmalarında değişikliğe gidebildiği gerekçelerine dayanılarak, açık kaynak kodlu bu tür bilgisayar programları ortaya çıkaran yazılımcıların veri sorumlusu olarak addedilemeyecekleri iddia edilmiştir (Ibanez, L. D., O'Hara, K., Simperl, E., 2018, s. 5). Yine, ilgili yazılımcıların yalnızca bir araç ortaya

çıkardıkları ve bu aracın nasıl kullanılacağını tayin etmedikleri ve bu sebeple veri sorumlusu sayılmamaları gerektiği de ifade edilmektedir (EU *Blockchain* Observatory and Forum, 2018, s. 18)

Düğümlere yönelik olarak yapılan incelemelerde Finck (2018) ilgili düğümlerin veri işleme noktasında birlikte ancak birbirlerinden habersiz ve bağımsız olarak çalıştıkları düşünüldüğünde ya hiçbir düğümün işleme amaçları ve vasıtalarını belirlemediği veyahut tüm düğümlerin birlikte bu işleme amaç ve vasıtalarını belirlediği çıkarımının yapılabileceğini savunmuş; bu sebeple de ya hiçbirinin ya da hepsinin birlikte veri sorumlusu olması gerektiği açıklanmış ve ikinci durumun daha olası olduğu üzerinde durmuştur. GDPR açısından bu tez savunulurken, özellikle, ilgili düğümlerin protokollerin yeni sürümlerini yahut farklılaştırılmış hallerini uygulama noktasındaki serbest iradelerinin, blokzincir projelerinin gelişimi ve işleyişi üzerinde doğrudan etkili olduğu gerekçesine de dayanılmaktadır (EU Blockchain Observatory and Forum, 2018, s. 18). Bu fikrin kabulü halinde, her bir düğümün, özellikle bu düğümü kurma ve veri işleme noktasında serbestçe hareket ettiği düşünüldüğünde, KVKK'de veri sorumluları için gösterilen yükümlülüklere uyma noktasında sorumlu olacağı söylenebilecektir. Nitekim, GDPR açısından benzer bir sonuca varan Finck (2018), bu durumda, GDPR'da merkezi olarak veri işleme yöntemlerine karar veren kurumlar için öngörülmüş olan yükümlülüklere uyma noktasında birçok problemle karşılaşılacağını aktarmıştır. Bununla birlikte, düğümlerin veri sorumlusu olarak addedilemeyeceğini, düğümlerin bir ödül kazanmak, sistemin sağlıklı ve dengeli bir şekilde çalışmasına katkı sağlamak veya üçüncü kişi aracılar olmaksızın verilere ulaşmak ve doğrulamak için protokolleri çalıştırdıkları ve aslında verilerin işleme amaç ve vasıtalarını belirlemedikleri görüşü de savunulmaktadır (Commission Nationale L'informatique et des Libértes, 2018, s. 2; EU Blockchain Observatory and Forum, 2018, s. 18).

İlgili ağı kullanan ve ilgili işlemleri blokzincir ağına (düğümler tarafından işlenmesi veya onaylanması için) gönderen kullanıcılar açısından yapılan değerlendirmede ise, bu kişilerin veri sorumlusu olarak addedilmelerinin mümkün gözüktüğü savunulmaktadır (Commission Nationale L'informatique et des Libértes, 2018, s. 1). Nitekim, kendisine veya üçüncü kişilere ait kişisel verilerinin işlenmesi, işlenme amaçları ve vasıtalarını belirleme noktasında bu kişilerin söz sahibi olduğunun söylenmesi gerekir. Bununla birlikte, GDPR'ın ticari olmayan salt kişisel kullanım için veri işlenmesi durumunda bu işlemlerin GDPR uygulama kapsamında olmayacağına ilişkin getirdiği istisna doğrultusunda, ilgili kişilerin kendi verilerini işlemesinde yalnızca profesyonel veya ticari bir amaçla veri işlenmesi durumunda GDPR'da yer alan yükümlülüklere uyması gerektiği vurgulanmaktadır (Commission Nationale L'informatique et des Libértes, 2018, s. 1). Fakat, yukarıda da açıklandığı üzere, KVKK'de bu istisnanın yalnızca "üçüncü kişilere verilmemek kaydıyla" tanındığı düşünüldüğünde, üçüncü kişilerle verilerin paylaşıldığı blokzincir sistemleri için GDPR'da öngörülen istisnanın uygulanamayacağı sonucuna varılacaktır.

Bir kişinin veri sorumlusu olarak addedilmesi durumunda, diğer yükümlülüklerinin yanında, örneğin, KVKK m. 10'da gösterilen aydınlatma yükümlülüğüne (yani kendisinin veya temsilcisinin kimliği, kişisel verinin hangi amaçla işleneceği, işlenen kişisel verilerin kimlere

ve hangi amaçla aktarılabileceği, kişisel veri toplama yöntemi ve hukuki sebebi gibi konularda bilgi verme yükümlülüğüne); KVKK m. 11'de gösterilen kişilerin başvuru haklarını kullanmaları durumunda bunlara cevap verme veya uyumlu davranma yükümlülüklerine; KVKK m. 12'de gösterilen veri güvenliğine ilişkin yükümlülüklere; KVKK m. 16 ve devamında gösterilen veri sorumluları siciline kayıt yükümlülükleri uyması gerekmektedir.

D. KVKK Sisteminde "Veri İşleyen" Tanımının Blokzincir Tabanlı Projeler Açısından İncelenmesi

KVKK m. 3/1(ğ) uyarınca "veri işleyen", veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder. GDPR'da da "*data processors*" yani veri işleyenleri açıklamak için benzer bir tanım kullanılmıştır. KVKK m. 3'ün gerekçesinde bu kişilerin, kişisel verileri kendisine verilen talimatlar çerçevesinde işleyen çalışanlar olabileceği gibi, veri sorumlusunun hizmet satın almak suretiyle belirlediği ayrı bir gerçek veya tüzel kişi de olabileceği belirtilmiştir.

Bu noktada, blokzincir tabanlı sistemler açısından veri sorumlusunun verdiği yetkiye dayanarak veri işleyen kişilerin veri işleyen olabilecekleri ve bu kapsamda bazı durumlarda "akıllı sözleşme" yazan (başka bir ifade ile programlayan) ve bunları işleme koyarak veri sorumlusu adına veri işleyen kişilerin, bazı durumlarda ise ilgili algoritma ve dağıtık veri tabanı onay kurallarına göre ilgili verinin işlenmesinin uygun olup olmadığını denetleyen ve bu verinin işlenmesinde görev alan madenci ("*miner*") veri işleyen olarak addedilebileceklerine dikkat çekilmiştir (Commission Nationale L'informatique et des Libértes, 2018, s. 3).

Akıllı sözleşmelere ilişkin bilgisayar programları geliştiren ve yayımlayan kişiler açısından yapılan değerlendirmede, bu kişilerin gerçekten "kişisel veriyi işleyen" sıfatına haiz olup olmadıklarına yönelik bir tartışma bulunmakla birlikte, bu hususun somut olay özelinde çözülmesi gerektiği vurgulanmaktadır (EU *Blockchain* Observatory and Forum, 2018, s. 18).

Bir kişinin veri işleyen addedilmesi durumunda, bu kişi KVKK m. 12/4'te gösterilen verileri KVKK hükümlerine aykırı olarak başkasına açıklamama ve işleme amacı dışında kullanmama yükümlülüğüne uygun davranmak ile verilerin işleme amacı dışında kullanılmaması yükümlülüğüne uymak zorunda olacak; yani, veri işleyen kişiler, diğer yükümlülükleri yanında, öğrendikleri kişisel verileri KVKK hükümlerine aykırı olarak başkasına açıklayamayacak ve verilerin toplanması ve saklanması gibi işleme amaçları dışında kullanamayacaklardır.

E. Blokzincir Projelerinde KVKK Kapsamında "Kişisel Verilerin Silinmesi"ne İlişkin Yükümlülüklere Uyum

KVKK m. 7 uyarınca KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmeli, yok edilmeli veya anonim hâle getirilmelidir. KVKK m. 7'nin gerekçesinde silinme, yok edilme ve anonim hale getirmeye ilişkin tanımlar açıklanmıştır. Kişisel verilerin silinmesiyle, bu verilerin tekrar hiçbir şekilde kullanılamayacak ve geri getirilemeyecek şekilde imhasının ifade edildiği belirtilmiş ve

verilerin kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülemeyecek şekilde silinmesi gerektiği açıklanmıştır. Verilerin yok edilmesinde, bilgilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesinin ifade edildiği açıklanmıştır. Verilerin anonim hale getirilmesiyle ise, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesinin kastedildiği açıklanmıştır.

Kişisel Verileri Koruma Kurumu tarafından çıkarılmış olan 30224 sayılı ve 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("**Yönetmelik**") ise, KVKK m. 7'de öngörülen hükümleri ayrıntılı olarak düzenlemiştir. Yönetmelik m. 8 ile silinme, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini; m. 9 ile yok edilme, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini; ve m. 10 uyarınca anonim hale getirilme ise, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi işlemini ifade edecek şekilde tanımlanmıştır.

Yine, ilgili işlemlerin somut olay özelinde nasıl uygulanacağına ilişkin olarak Kişisel Verileri Koruma Kurumu tarafından Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi yayımlanmıştır (Kişisel Verileri Koruma Kurumu, 2018, Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi). İlgili rehberde, anonim hale getirmeye ilişkin olarak, aşağıdaki açıklamalara da yer verilmiştir:

"Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

...

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir. Bu şartların yerine getirilmiş olmasını veri sorumluları sağlamalıdır:

• Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulamaması,

• Bir ya da birden fazla değerin bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,

• Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Bu riskler sebebiyle veri sorumlularının, anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştikçe kontroller yapmaları ve anonimliğin korunduğundan emin olmaları gerekmektedir. (Kişisel Verileri Koruma Kurumu, 2018, Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi, s. 16 vd.).”

Bitcoin ve benzeri blokzincir ağlarının bloklar oluşturarak sağladıkları güven sisteminin çalışabilmesinin temel esaslarından biri ilgili bloklara işlenmiş verilerin “*immutable*” yani değiştirilemez olduğudur. Bu sistemde işlenen veriler veya bunların özet değerleri bloklarda saklanmakta ve oluşturulan her bir bloktan sonraki blok, önceki bloğa ilişkin verileri barındırmaktadır. Bu sebeple, herhangi bir bloktaki verinin silinememesi yahut değiştirilememesi mümkün olmamaktadır.

Sistemin işlemesinin verilerin değiştirilemez olmasına dayandığı bu sistemlerde, gerek KVKK gerekse GDPR’da tanınmış olan silinme, yok edilme veya anonimleştirme haklarının genel olarak blokzincir tabanlı projelerde dağıtık veri tabanında saklanan veriler için uygulanması mümkün gözükmemektedir. Bu noktada, GDPR’ın uygulanması açısından yapılan tartışmalarda özellikle GDPR m. 17/2’de gösterilen “silinme talebi halinde, veri sorumlusunun mevcut teknoloji ve uygulama maliyetini dikkate alacağı”na ilişkin madde kapsamında bir değerlendirme yapılıp yapılamayacağı üzerinde durulmaktadır; ve bu kapsamda, ilgili maddenin *blokzincir* kullanılarak dağıtık veri tabanında saklanan verilerde silinmenin gerçekleşemeyeceği şeklinde yoruma imkan verip vermediği tartışılmaktadır (Finck, 2018, s. 24). Ancak, ilgili maddenin izdüşümü KVKK’de bulunmadığı için, Türk hukuku kapsamında bu tartışmanın aynı kapsamda yapılması mümkün olmayacaktır (Karatay, E. ve Solak, M., 2019).

Bu noktada, Bitcoin blokzincir ağı özelinde, KVKK’de öngörülmüş olan silme, yok etme veya anonimleştirmeye ilişkin yükümlülüklerin uygulanması imkanı olmadığı görülmektedir. Bununla birlikte, tartışma ve sonuç bölümünde ayrıntılı olarak değinileceği üzere, GDPR ve dolayısıyla KVKK’deki yükümlülüklere uyumlu olacak blokzincir projelerinin geliştirilebileceğine ilişkin bazı öneriler ve görüşler bulunmaktadır.

F. Blokzincir Projeleri Bakımından KVKK Kapsamında “Alenileştirme” Kavramının Değerlendirilmesi

Blokzincir tabanlı projeler kapsamında kişisel veriler, çoğu zaman, veri sahibi ilgili kişi tarafından sisteme gönderildikten sonra onaylayan düğümler veya diğer üçüncü kişiler tarafından işlenerek bloklar oluşturulmakta ve işlemler gerçekleştirilmektedir. Ayrıca, dağıtık veri tabanı sistemine dayalı olan blokzincir tabanlı projelerde özellikle herkese açık sistemlerde şeffaflık ilkesi çerçevesinde bu veriler herkese açık tutulmakta ve üçüncü kişiler tarafından incelenebilmektedir. Bu kapsamda, tartışılması gereken bir diğer konu, kişisel verilerin

işlenmesi için açık rıza alınması gerekip gerekmediği ve bu kapsamda kişisel verilerin ilgili kişi tarafından alenileştirilmiş olup olmadığıdır.

KVKK m. 5 kapsamında kişisel verilerin işlenme şartları düzenlenmiştir. KVKK m. 5 uyarınca kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez. Ancak, KVKK'de sayılan şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür. KVKK m. 5 kapsamındaki hukuka uygunluk nedenleri arasında "*ilgili kişinin kendisi tarafından alenileştirilmiş olması*" yer almaktadır. Bu bağlamda ilgili kişinin kendisi tarafından alenileştirilen, bir başka ifadeyle herhangi bir şekilde kamuoyuna açıklanmış olan kişisel verileri, üçüncü kişilerce işlenebilecektir.

Ancak, alenileştirme kavramının GDPR'a da paralel olarak KVKK m. 4'te belirtilen genel veri işleme ilkeleri süzgecinden geçirilerek değerlendirilmesi gerekmektedir. Özellikle "*hukuka ve dürüstlük kurallarına uygun olma*" ve "*işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma*" ilkelerinin alenileştirmeye ilişkin istisnanın yorumlanması bakımından altının çizilmesi gerekmektedir.

Kişisel Verileri Koruma Kurumu tarafından yayımlanan Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi'nde yapılan alenileştirmeye ilişkin açıklamalar bu gerekliliği açıkça ortaya koymaktadır:

"Ancak, kişisel verinin aleni kabul edilebilmesi için ait olduğu kişinin aleni olmasını istemesi gerekir. Başka bir ifade ile, alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin varlığı gerekir. Yoksa bir kişinin kişisel verisinin herkesin görebileceği bir yerde olması aleni olmasını sağlamaz. Ayrıca, alenileştirme durumunda kişisel verinin amacı dışında da kullanılmaması gerekmektedir. Örneğin, ikinci el araç satışı yapılan internet sitelerinde aracını satmak isteyen ilgili kişinin iletişim bilgilerinin pazarlama amaçlarıyla kullanılması mümkün değildir. (Kişisel Verileri Koruma Kurumu, 2019, Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi, s. 76)"

Yine bu doğrultuda, Kişisel Verileri Koruma Kurulu 27 Ocak 2020 tarihli ve 2020/67 sayılı Karar Özeti'nde alenileştirmeye ilişkin aşağıdaki değerlendirmelerini ortaya koymuştur.

"Alenileştirmenin gerçekleştirilebilmesi için alenileştirme iradesinin ne olduğuna bakılması gerektiği, zira bir kişinin kişisel verisinin herkesin görebileceği bir yerde olmasının aleni olmasını sağlamayacağı, alenileştirme durumunda kişisel verinin alenileştirme amacı kapsamında kullanılması gerektiği, somut olayda, alenileştirme bulunuyor olsa dahi ilgili kişinin reklam faaliyetleriyle ilgili kendisiyle iletişim kurulması amacıyla söz konusu kişisel verileri alenileştirmemiş ise, gerçekleştirilecek olan kişisel veri işleme faaliyetinin hukuka uygun olmayacağının değerlendirildiği, …"

Kişisel Verileri Koruma Kurumu ve Kişisel Verileri Koruma Kurulu tarafından yayımlanan rehberler ve karar özetlerinden de açıkça ifade edildiği üzere, bir kişinin verilerini kamuya açıklamış veya herkesin görebileceği şekilde paylaşmış olması, ilgili kişisel verilerin her türlü amaçla kullanılabileceği ve işlenebileceği anlamına gelmeyecektir. Bu kişisel verilerin

alenileştirme amacı ile kullanılması gerekecektir. Örneğin Bitcoin blokzincirinde, ilgili kişi, kaç adet Bitcoin göndermek istediği, bu bitconleri hangi cüzdanından göndereceği gibi bilgileri, ilgili işlemleri gerçekleştirmek için paylaşmaktadır. Bu durumda, ilgili verilerin, yine bitcoin transferi ve Bitcoin blokzincirinin işlemesi için kullanılabileceği düşünülse de, bundan farklı bir amaçla işlenmesi için açık rıza alınması gerektiği savunulabilecektir. Kişisel verilerin blokzincir üzerinde kamuya açık olarak saklanması, ilgili kişinin açık rızasını almaksızın her türlü amaçla kişisel verilerin işlenebileceği anlamına gelmemektedir.

III. Tartışma ve Sonuç

Kişisel verilerin korunmasının, bireylere tanınmış bir Anayasal hak olması gözetildiğinde, ilgili Anayasal hakkın bireylere sağladıkları özgürlük alanlarının düşünülmesi ve amaçsal olarak yorumlanması zorunluluğu hasıl olmaktadır. Özel hayatın gizliliği gibi birçok temel ilkeye temas eden kişisel verilerin korunması hususu, kişisel verilerimizin işlenmesi ve paylaşılmasının her geçen gün arttığı, ilgili kişisel veri havuzlarının büyüdüğü ve dağıldığı dünyamızda kontrol edilmesi ve hukuki olarak düzenlenmesi çok zor bir süreç haline gelmiştir. Gerek KVKK'nin gerekse GDPR'ın kurduğu sistemin merkezi olmayan güven mekanizmaları ve merkeziyetsiz veri tabanları sistemleri ile uyumlu olarak çalışmak üzere hazırlanmamış olduğu gözetilmelidir.

Bu noktada, blokzincirin bireylerin kişilerin verileri üzerindeki kontrollerini arttırma ve veri işleme süreçlerini şeffaflaştırma noktasında devrim yaratabileceği iddia edilse ve bu kapsamda kanunların yorumlanmasında ilgili hükmün konuluş amacının da değerlendirilmesi gerektiği savunulabilse de; kanunun lafzı önünde yalnızca amaçsal yorum ilkeleri benimsenerek bir hukuki çıkarım yapılması mümkün değildir. Bu durumda, kanun koyucu tarafından gerekli önlemler alınıncaya kadar yukarıda öngörülen hukuki problemlerin, projelerin uygulanmasındaki yöntemlerdeki değişiklikler ile aşılarak halihazırdaki mevzuatımıza uyumlu hale getirilmesi için çözümler aranmalıdır.

KVKK m. 3/1(d) kapsamında kişisel veriler yalnızca gerçek kişiye ilişkin verileri ifade ettiğinden, anonim şirket ve benzeri tüzel kişilere ait verilerin saklanması noktasında KVKK uygulama alanı bulmayacaktır. Bu durumda, blokzincir projelerinde yalnızca tüzel kişilere ait verilerin saklanması ihtimali üzerinde durulabilir.

Blokzincir ağı kullanılan projelerde dağıtık veri tabanlarına kaydedilmiş verilerin silinmesi, yok edilmesi ve anonimleştirilmesi yükümlülüklerinin yerine getirilebilmesi için, ilgili verilerin şifrelenerek saklanması yahut belirli algoritmalardan geçirilmeleri sonucunda özet değerlerin (*hash*) saklanması ve veriler silinmek istendiğinde bu verilere ulaşılabilmesini sağlayan anahtarların silinmesinin bir çözüm önerisi olarak tartışmaya açılmıştır (Finck, 2018; Filippi, 2016). Bu noktada, Yönetmelik m. 8 kapsamında silinme ile, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi; m. 9 ile yok edilme ile, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işleminin ifade edilmiş olması kapsamında; ilgili yöntem ile yalnızca bu verilere ulaşılmasının engellendiği düşünüldüğünde, bu yöntem uygulanarak

KVKK ve Yönetmelik kapsamında silinme yahut yok edilme gerçekleştiğinden söz edilemeyecektir. Bununla birlikte, Yönetmelik m. 10 uyarınca anonim hale getirilmenin ise, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi olarak tanımlanması kapsamında bir değerlendirme yapıldığında, ilgili anahtarın silinmesinin bu verilere erişimi engellediği düşünülse dahi, Yönetmelik m. 10'da gösterilen "başka verilerle eşleştirilme" lafzının yorumlanmasındaki farklılıkların; ilgili işlemin anonimleştirme olup olamayacağı konusundaki görüşü değiştireceği düşünülmelidir. Nitekim, burada mutlak bir ilişkilendirilememe arandığı söyleniyorsa, anahtar verisi her ne kadar silinmiş bulunsa da, bir şekilde şifrelenmiş asıl veri ile eşleştirildiğinde ilgili veriye ulaşılabiliyor olması; Yönetmelik hükmünde öngörülen sonuca ulaşılmadığı çıkarımının yapılması sonucunu doğuracaktır.

GDPR ile uyumlu blokzincir projeleri geliştirilmesine yönelik olarak sunulan önerilerden bir diğeri ise kişisel veri niteliğindeki verilerin *off-chain* yani dağıtık veri tabanı ve blokzincir ağı dışında merkezi bir veri tabanında tutulması ve böylece dağıtık veri tabanı üzerinde kişisel verilerin saklanmaması yönündedir (Ibanez, L. D., O'Hara, K., Simperl, E., 2018, s. 8). Ancak, bu noktada, ilgili kişisel verinin ayrı olarak tutulduğu merkezi veri tabanından silinmesine rağmen özet değerin (*hash*) başlı başına bir kişisel veri oluşturabileceği üzerinde durulmakta (EU *Blockchain* Observatory and Forum, 2018; Finck, 2018) ve bu sistem benimsendiğinde *blokzincir* kullanmanın anlamsızlaştığına vurgu yapılmaktadır (Ibanez, L. D., O'Hara, K., Simperl, E., 2018, s. 8)

Halka açık ve izin verilmeden işlem yapılan blokzincir sistemlerinin aksine, izin verilmeden işlem yapılamayan blokzincir ağları bakımından problemin çözümüne daha ılımlı yaklaşılmaktadır. Nitekim, ilgili ağın veri işleme kurallarına göre bir mutabakat sağlandığında, temeldeki bir verinin değiştirilerek blokzincir ağının işlerliği bozulmadan kayıtlara devam edilebileceği ifade edilmektedir (Wirth, C. and Kolain, M., 2018).

Verilerin silinmesi yükümlülüğü dışında, blokzincir projeleri açısından değerlendirilmesi gereken KVKK kapsamındaki yükümlülüklerden bir diğeri; KVKK m. 11 uyarınca herkesin veri sorumlusuna başvurarak kendisiyle ilgili kişisel veri işlenip işlenmediğini öğrenme ve verisi işlenen kişinin, hangi kişisel verilerinin ne şekilde işlendiğine ilişkin olarak bilgi alma hakkının uygulanması noktasındadır. Nitekim, ilgili hükmün uygulanması, düğümleri yahut veri işleyen kullanıcıları veri sorumlusu olarak ele aldığımız noktada, bunların her birine başvurulabilecek olduğu sonucunu doğuracaktır. Yine, bu durumda, veri sorumluları açısından da ilgili kişilerin gerçekten kişisel veriye sahip olan kişi olup olmadıklarını anlama noktasında bir çözüm geliştirmeleri beklenecektir. Bu noktada, verilerin herkese açık olduğu halka açık blokzincirlerde verilerin hangi şekilde ve ne şekilde işlendiğine ilişkin bilgiler herkese açık olsa da KVKK m. 11 uyarınca gösterilen bilgilerin veri sorumlusu tarafından cevaplanması yükümlülüğü ortadan kalkmamaktadır. Bu durumda veri sorumlusu ilgili kişisel verilerin halka açık olduğunu öne sürerek, ilgili kişinin talebini geri çevirme hakkına sahip değildir. Yine bu problemlerin aşılması için, daha merkezi bir yapı tarafından işletilen ve izin alınarak veri kaydedilen blokzincir projelerinin geliştirilebileceği düşünülmektedir.

Halihazırda halka açık ve izin gerekmeksizin veri işlenebilen blokzincir sistemlerinde dağıtık veri tabanında kişisel verilerin işlenmesi ve saklanması durumunda KVKK'de gösterilen yükümlülüklere uyularak ilgili projenin hayata geçirilebilmesi mümkün gözükmemekle beraber, özellikle izin verilerek veri işlenen ve veri işleyenlerin belirli küçük bir gruptan oluştuğu sistemlerde KVKK ile uyumlu blokzincir projelerinin geliştirilebileceği düşünülmektedir. Bununla birlikte, merkezi otoriteleri ortadan kaldırmak suretiyle bireyselliği ön plana çıkaran bir felsefeyi yansıtan blokzincir tabanlı projelerde, temel olarak veri güvenliğini ve kişisel verilerin muhafazasında şeffaflığı sağlama amaçlarına hizmet etmektedir. Bu bağlamda, KVKK'nin Genel Gerekçesi'nde ortaya koyulan bireylerin aydınlatılması ve veri güvenliğine ilişkin tedbirlerin alınması yönündeki ana ilkeler de blokzincir tabanlı birçok projenin temelindeki felsefeyle paraleldir. Dolayısıyla, kişisel verilerin korunmasına ilişkin düzenlemelerin tatbiki esnasında blokzincir kapsam dışında bırakmaktansa blokzincir ve kişisel verilerin korunmasına ilişkin düzenlemeleri birbirleriyle uyumlu olabilecekleri bir eksene getirmek iki kurumun da temelinde yatan prensipleri nazara aldığımızda, daha makul çözümler üretebilmemizi sağlayacaktır.

KAYNAKÇA

Allen, D., Berg, A., Berg, C., Markey-Towler, B., Potts, J. (2018, Mayıs). **Some economic consequences of the GDPR.** 27 Eylül 2018 tarihinde SSRN veri tabanından erişilmiştir.

Commission Nationale L'informatique et des Libértes. (2018, Eylül). **Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles?.** [Çevrim-içi: https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles], Erişim tarihi: 09.10.2018.

EU Blockchain Observatory and Forum (2018, Ekim). **Blockchain and the GDPR.** [Çevrim-içi: https://www.eublockchainforum.eu/reports], Erişim Tarihi: 01.10.2018.

Ferrari, V. (2018, Eylül). **EU Blockchain Observatory and Forum Workshop on GDPR, Data Policy and Compliance. Institute for Information Law Research Paper No. 2018-04.** 27 Eylül 2018 tarihinde SSRN veri tabanından erişilmiştir.

Filippi, P. (2016). **The interplay between decentralization and privacy: the case of blockchain technologies. 9 Journal of Peer Production.** [Çevrim-içi: http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf], Erişim Tarihi: 17.09.2018.

Finck, M. (2017, Kasım). **Blockchain and Data Protection in the European Union. Max Planck Institute for Innovation & Competition Research Paper.** 12 Ocak 2018 tarihinde SSRN veri tabanından erişilmiştir.

Herian, R. (2018). **Regulating Disruption: blockchain, GDPR, and questions of data sovereignty. Journal of Internet Law,** 22(2), 8-18. 28 Eylül 2018 tarihinde The Open University veri tabanından erişilmiştir.

Ibanez, L. D.; O'Hara, K., Simperl, E. (2018). **On blockchains and the General Data Protection Regulation.** 8 Ağustos 2018 tarihinde University of Southampton Institutional Repository veritabanından erişilmiştir.

Karatay, E. ve Solak, M. (2019). **Tübitak 2. Ulusal Blokzincir Çalıştayı, Dijital Kimlik, Blokzincir ve Kişisel Verilerin Korunması Kanunu'na Uyum Üzerine Hukuki Düşünceler konulu bildiri sunumu.** 25 Eylül 2019 tarihli bildiride sunulmuş ve bildiri özeti paylaşılmıştır.

Kişisel Verileri Koruma Kurumu (2018). **Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi rehberi.** [Çevrim-içi: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf], Erişim Tarihi: 12.09.2018.

Kişisel Verileri Koruma Kurumu (2018). **Veri sorumlusu ve veri işleyen.** [Çevrim-içi: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf], Erişim Tarihi: 12.09.2018.

Kişisel Verileri Koruma Kurumu (2019). **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi.** [Çevrim-içi: file:///C:/Users/Beg%C3%BCm/Downloads/41784a70-2bac-4e4a-830f-35c628468646.PDF], Erişim Tarihi: 20.05.2020.

Kişisel Verileri Koruma Kurumu. **"İlgili kişiye rızası bulunmamasına rağmen bir gayrimenkul şirketi tarafından SMS aracılığıyla gönderilen reklam ve bildirimler hakkında"** Kişisel Verileri Koruma Kurulunun 27/01/2020 tarih ve 2020/67 sayılı Karar Özeti. [Çevrim-içi: https://www.kvkk.gov.tr/Icerik/6718/2020-67], Erişim Tarihi: 20.05.2020.

Lima, C. (2018, Haziran). **Blockchain-GDPR Privacy by Design.** [Çevrim-içi: https://blockchain.ieee.org/images/files/pdf/blockchain-gdpr-privacy-by-design.pdf], Erişim Tarihi: 12.09.2018.

Mainelli, M. (2017, Ekim). **Blockchain could help us reclaim control over our personal data. Harvard Business Review.** [Çevrim-içi: https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data], Erişim Tarihi: 10.09.2018.

Nakamoto, S. (2009). **Bitcoin: A Peer-to-Peer Electronic Cash System.** [Çevrim-içi: https://bitcoin.org/bitcoin.pdf], Erişim tarihi: 01.11.2018.

Serozan, R. (2013). **Hukukta Yöntem.** Yaşar Üniversitesi Dergisi 8 (Özel 2423-2440). [Çevrim-içi: https://journal.yasar.edu.tr/wp-content/uploads/2014/01/6-Rona-SEROZAN.pdf], Erişim Tarihi: 18.09.2018.

Toth, A. (2018, Mayıs). **Will GDPR block Blockchain?** [Çevrim-içi: https://www.weforum.org/agenda/2018/05/will-gdpr-block-blockchain/], Erişim Tarihi: 18.09.2018.

Wirth, C.; Kolain, M. (2018): **Privacy by blockchain design: a blockcchain-enabled GDPR-compliant approach for handling personal data.** Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies. 28 Eylül 2018 tarihinde EUSSET Digital Library veritabanından erişilmiştir.

Zarsky, T. (2017). **Incompatible: The GDPR in the age of big data.** Seton Hall Law Review, 47, Article 2. 9 Eylül 2018 tarihinde Seton Hall Law Review veritabanından erişilmiştir.

Zyskind, G., Nathan, O., Pentland, A. (2015). **Decentralizing privacy: using blockchain to protect personal data.** 2015 IEEE Security and Privacy Workshops, 180-184. 15 Mart 2018 tarihinde IEEE veritabanından erişilmiştir.