GDPR'ın Blok Zinciri Üzerinde Etkisi

1. Giriş

Veri, onu erişilebilir ve saklanabilir kılan teknolojik gelişmeler sonucunda büyük maddi değer kazanmıştır. İnternetin yaygınlaşması ve veri bant genişliğinin yükselmesi verinin iletimini arttırmış, yüksek kapasiteli veri saklama üniteleri ile rahatlıkla depolanabilir hale gelmiştir. Verinin artan değeri, veriden yapabildiğimiz çıkarımlar ve bu çıkarımların ticari kazanımlara dönüşmesi sonucunda artmıştır. Bu durum da ekonomide yeni bir sürecin başlamasına sebep olmuştur. Ekonomideki bu değişim sosyal, siyasal ve hukuksal alanlarda da etkisini göstermiştir. Özellikle veri, gerçek kişiler ile ilişkilendirilerek bir anlam kazandığında kişiler üzerinde tüketim alışkanlıklarından siyasi ve ideolojik düşüncelerine yön veren sanal bir silah haline gelmiştir. Temel hukuk düzenlemeleri kapsamında öncelikle özel hayatın gizliliği ve kişilik hakları içerisinde ele alınan kişisel veri, kişi menfaat dengesini sağlama noktasında yeterli korumayı sağlayamamıştır. Bu doğrultuda kişisel verinin etki ettiği alanlar göz önünde bulundurularak yeni bir temel hak ve özgürlükler grubunda yerini alan *"Kişisel Veri Koruma Hakkı"* ulusal ve uluslararası birçok düzenlemeye konu olmuştur.

"Avrupa Veri Koruma Tüzüğü" (*General Data Protection Regulation, GDPR)* Avrupa Ekonomik Alanı *(European Economic Area, EEA)* sınırlarını aşan bir uygulama öngörerek kişisel verilerin hukuka uygun olarak işlenmesi, saklanması, silinmesi ve transferi noktasında birçok düzenlemeyi beraberinde getirmiştir. "Blok zinciri" *(Blockchain)* ise, merkezi otoritenin müdahalesinden uzaklaşmak adına geliştirilen, şifrelenmiş işlem takibi ile elektronik veri aktarımının sağlandığı ve doğrulanabildiği dağınık veri tabanı olarak teknolojik gelişmeler içerisinde yerini almıştır.

Blok zinciri hakkında işlenen verinin değiştirilemez ve herkes tarafından izlenebilir genel algısı GDPR uyumluluğunun sağlanamayacağı noktasında temel tartışmaları doğurmuştur. Değiştirilemez özelliğinin GDPR'da belirtilen veri sahibi haklarının kullanımını engelleneceği düşünülen bu durum, blok zinciri teknolojisi hakkında yanlış (kısmen eksik de denilebilir) bilgi oluşturmuştur. Veri sahibi haklarının kullanılmasının zorluklarının yanı sıra, halka açık blok zincirlerinde, GDPR genel ilkelerinde yer alan "hesap verilebilirlik" ilkesi gereğince veri sorumlularının tespiti, verinin anonim olarak kabul edilip edilemeyeceği tartışmaları da

gündeme gelmiştir. Bu noktada belirtmek gerekir ki blok zincirini kişisel verilerin korunması hedefi ile kullanılması neticesinde bilgi güvenliğinin ve veri işlemede şeffaflık ilkesinin sağlandığı bir sistemin oluşturulması, hukuksal düzenlemeler doğrultusunda etkin bir şekilde teknoloji kullanımının yolunu açacaktır.

Sonuç olarak her iki tarafın amacı da *"veri koruma"*dır. Blok zinciri, merkezi otoritenin gücünü kırarak veriler üzerinde güvenliği ve şeffaflığı öngörürken GDPR ise kişisel veri kullanımını merkezi otoritenin kendi amaçları doğrultusunda kullanmasını engelleyerek kişinin kendi verileri üzerindeki hakimiyetini sağlamayı hedeflemektedir. 2017'de Accenture tarafından yapılan araştırmaya göre blok zinciri ve akıllı sözleşmeler kullanan yatırım bankaları 12 milyar dolar tasarruf edebileceği belirtilen ve 2018 yılı itibari ile dünya çapında 150 milyar dolar değer sağlayan bu teknolojiyi tamamen yok saymak mümkün değildir. Yaklaşımımız teknolojinin GDPR uyumluluğunu eleştirmek yerine, teknolojiyi GDPR'a uygun olarak nasıl kullanılması gerektiği yönünde olmuştur. Unutulmamalıdır ki terazinin bir ucunda kişilerin temel hak ve özgürlükleri varken diğer bir ucunda ekonomiye yön veren ticari kaygılar barındıran şirketleri ve yeni teknolojilerin kullanımları vardır. Regülasyonlar ve teknolojik yenilikler terazinin dengesinin bozulmadan yeni ekosisteme entegre edilmelidir.

2. Kişisel Verilerin Korunması ve GDPR Düzenlemeleri:

GDPR, Avrupa Birliği (AB) vatandaşlarının kişisel verilerin işlenmesinin hukuksal düzenlemelerini konu alan ve kişisel verilerin sınır ötesi serbest dolaşımlarını düzenleme amacıyla oluşturulmuş, 2016 Mayıs ayında AB Komisyonu tarafından kabul edilerek 25 Mayıs 2018'de yürürlüğe girmiştir. Ancak 2012 yılından itibaren GDPR metin içeriği hazırlanmaya başlanmıştı. O süreçte mevcut teknolojik gelişmeler daha çok merkezi sistemli bulut altyapısı ile oluşturulan *(web-centric centralized cloud-based)* internet şeklinde olması GDPR içeriğini etkilemiştir. Blok zinciri kullanımı ise GDPR düzenlemelerini etkileyecek düzeyde olmaması bir nevi GDPR'ın dağıtık defter teknolojisi karşısında yetersiz bırakmıştır. Bu durumun yeni bir regülasyon yapılmasının zaruri olduğu, mevcut düzenlemenin asla yeni teknoloji karşısında yeterli olduğu çıkarımlarını yapmak isabetli olmayacaktır. Bu durum sadece alışılagelmiş bir sistem yorumundan uzaklaşılması gerektiği, merkezi otoriteli sistemler gibi blok zincirinin yorumlanmaması gerektiği noktasında ışık tutacaktır. Zira regülasyonların sürekli yenilenen teknolojilere uygun hazırlanması beklenemez. Teknolojinin regülasyonlara uygun olarak tasarlanması ve kullanılması gerekir.

GDPR'dan önce yürürlükte olan ve 25 Mayıs 2018 tarihi itibariyle geçerliliğini yitiren Direktif 95/46/EC yine veri koruma hakkına ilişkin olarak düzenlemeler getirmiştir. Ancak mevcut düzenlemelerin yetersizliği ve doğrudan hukuki bağlayıcılığı olmadığı için yeni bir regülasyonun yapılmasını zorunlu kılmıştır.

Bu noktada GDPR'ın getirdiği yenilikler arasında özellikle dikkat çeken ve blok zinciri tasarımında temel kavramlar;

- ***Etki Alanı (Terriorial Scope):*** genişletilmiş etki alanın olmasıyla sadece AB üye devletleri kapsamında değil aynı zamanda AB vatandaşı olmasa dahi AB yaşayan kişilere mal ve hizmet sunan ve bu aşamada veri işleyen herkes için GDPR uygulaması zorunluluğu getirilmiştir. Artık EEA'nın sınırlarını aşan bu regülasyonun veri sorumlusunun dünyanın neresinde ikamet ettiğine/merkezinin-şubesinin bulunduğuna bakılmaksızın Avrupa Birliği üye devlerinde ikamet eden bir vatandaşa mal veya hizmet sunulması durumunda GDPR uygulama alanı bulacaktır.
- ***Şeffaflık (Transparency):*** veri işlemeye ilişkin her aşamanın ulaşılabilir olması ve içeriğinin veri sahipleri tarafından kolayca anlaşılabilmesi, sade ve açık olması gerektiği belirtilmiştir.
- ***Unutulma Hakkı (Right to be Forgotten):*** Aşağıda da detaylı değinileceği üzere, unutulma hakkı ile birlikte kişilerin verileri üzerinde daha etkin kontrol hakkına sahip olabilmesi,
- ***Tasarım ile Gizlilik (Privacy by Design):*** Üzerinde durulması ve blok zinciri sisteminin GDPR'a uygun olarak kullanılmasında dikkat etmemiz gereken önemli prensiplerden biri de "Tasarım ile Gizlilik"'tir. Prensip doğrultusunda her türlü yeni ürün veya servisin tasarlanması aşamasında veri koruma ilkelerden:[1]
  - *Hukuka Uygun, Dürüst, Şeffaf (Lawfuness, Fairness, Transparency),*
  - *Belirli, Açık ve Meşru Amaçla Sınırlılık (Purpose Limitation),*
  - *Veri Minimizasyonu (Data Minimisation),* gerekli olduğu kadar; ilgili; ölçülü,
  - *Doğruluk (Accuracy),* gerekli olduğu hallerde; güncel olarak,
  - *Saklama Sınırlaması (Storage Limitation),* veri işleme amacının varlığı süresince,
  - *Bütünlük ve Gizlilik (Integrity and Confidentiality),* verinin güvenliğinin sağlanması gerekliliği,
  - *Hesap Verilebilirlik (Accounability),* veri sorumlusunun sorumluluğu,

[1] GDPR m. 5 (1).

ve GDPR hükümlerine uyumluluğun sağlanması hedeflenmiştir. Eş değişle gizliliğin sağlanamamasından sonra ortaya çıkan veri ihlallerine çözüm bulunmasından önce kişisel veri güvenliğini sağlayan sağlam bir sistemin kurulması zorunlu kılınmıştır. Ayrıca T*asarım ile Gizlilik* prensibi karşısında, yukarıda sayılan ilkelere ek olarak hesap verilebilirlik kriterine,

- Bulanıklaştırma/Takma Ad yöntemi *(Pseudonymization)* tercih edilmesi, verinin anonim halde tutulmasının mümkün olmadığı durumlarda bulanıklaştırma/takma ad yöntemini tercih etmek veri güvenliği açısından faydalı olacaktır.
- Veri sahiplerinin veri işleme süreçlerini denetlemesine imkân tanınması,
- Düzenli olarak veri güvenliğine ilişkin önemleri geliştirme, uygulamak ve var olanları da iyileştirmeleri gerekmektedir. Zira veri etki analizi *(Privacy Impact Assesment)* yapılmasının gerekliliği de bu noktada ortaya çıkmıştır.

GDPR md.24 kapsamında ele alınan ve 95/46 Direktif'den farklı olan prensiplerinden biri de "Risk Temelli Yaklaşım *(Risk Based Approach)*"dır. Madde iki ölçüt belirlemiştir;

1. Riskin gerçekleşme ihtimali *(Likelihood of Occurence)*
2. Riskin gerçekleşmesi durumunda kişilerin hak ve özgürlüklerine ne derece etki doğuracağı *(Severity of Impact)*

Risk ölçümü veri işlem faaliyetinden önce gerçekleştiği için Tasarımda Gizlilik (*Pravicy by Design*) prensibinin kapsamı içerisinde ele alınmalıdır.

Risk temelli yaklaşımla veri güvenliğinin sağlanmasına yönelik ne gibi önlemler alınabileceğine ilişkin GDPR m.32 ise;

- Kişisel verilerin bulanıklaştırma*(psedonymisation)* ve kriptolama yöntemleriyle korunmasını,
- Veri işleme sistemlerinin gizliliğinin, güvenliğinin, ulaşılabilirliğinin ve sağlamlığının gerçekleştirilmesi,
- Teknik veya fiziksel bir ihlalin meydana gelmesi durumunda sistemlerin tekrar eski hale getirilmesi için gerekli tedbirlerin alınması,
- Sistem güvenliğinin sağlanabilmesi için önlemlerin belirli aralıklarla kontrol edilmesi,
- Mesleki kuralların yerine getirildiği veya veri güvenliği sertifikalarının (ISO 27001) veri güvenliğini yükümlülüğünün yerine getirildiğine kanıt teşkil edeceği belirtilmiştir.

Verilen örnekler sınırlı sayıda olmayıp, örneklendirilmelerle yapılmıştır. Yukarıda ana hatlarıyla çizilen sistem, GDPR'ın kişisel verinin dijital ortamda işlenmesinde teknoloji kullanımı esnasında asgari düzeyde olan beklentileridir. Oluşturulacak herhangi bir sistemde, GDPR temel ilkelerine bağlı kalarak risk temelli yaklaşım ile kişisel verilerin işlenmesi gerekmektedir.

Yukarıda bahsedilen GDPR temel ilkeleri üzerine inşa edilen bir blok zincirinin kullanılmaması görüşü isabetli olmayacaktır. Özellikle aşağıda da değinileceği üzere farklı kullanım şekilleri olan blok zincirlerinden konsorsiyum blok zincirinin tercih edilerek kişisel veri işleme faaliyetinin GDPR'a uygun bir şekilde oluşturulması mümkündür. Son olarak vurgulanan risk temelli yaklaşım kapsamında, mesleki kuralların yerine getirilmesinin bir göstergesi olarak veri güvenliği sertifikaları yine blok zinciri için de uygulama alanı bulacaktır. Bu kapsamda blok zinciri ve "Dağınık Defter Teknolojisi *(Distributed Ledger Technology)*" için ISO/TC 307 oluşturulmuştur.

3. Veri Koruma Düzenlemeleri Karşısında Blockchain Kullanım Şekilleri

Basit ve genel olarak bir blok zinciri sisteminde her blok kendin önce gelen bloğun özet değerini *(hash value)* barındırmakta ve kendi özet değerini de bir sonraki bloğa aktarmaktadır. Bu durum zincirde bir değişiklik yapılmasının önüne geçerek verinin değiştirilemez oluşunu pratikte sağlamaktadır. Zira herhangi bir değişiklik, bütün zincirin baştan aşağı değişmesine sebep olacaktır. Bu durum merkezi otoritenin müdahalesi ile bir değişikliğin mümkün olmadığı dağınık uzlaşı sisteminde kişiden kişiye *(peer to peer)* işlemin gerçekleştiği bu platform oldukça güvenlidir. Ancak her blok zincirinin tamamen değiştirilemez yapısı olduğunu kabul etmek de isabetli değildir. Blok zincirleri, farklı şekillerde oluşturulmaktadır.

Blok zinciri her ne kadar herkesin erişebildiği ve bir parçası olarak yer alabildiği bir sistem olarak kabul edilse de kullanım amaçları ile kısmi merkeziyetçi-konsorsiyum *(partially decentralized, consurtium)* ve özel *(private)* blok zinciri yapıları da geliştirilmiştir. Konsorsiyum blok zincirleri *(Quorum, Hyperledger, Corda)* ve özel blok zincirlerinde algoritmaları daha önceden belirlenmiş sınırlı sayıda tarafın yönettiği bir sistemdir. Blok zincirini herkes görebileceği ancak veri işleyişi belirli kişiler tarafından sağlanan karma bir sistem olarak da meydana getirilebilir.

Halka Açık, İzin Gerektirmeyen *(Public, perminsonless)*: Blok zincirinde kayıtlı verileri okumak için herhangi bir izin gerekmediği ve "mutabakat sürecine" kuralları belirlenmiş olan mutabakat yapısına uyan herkesin dahil olabildiği; yeni veriler işlenmesi izninin herkese açık olduğu sistemdir. Ağa dahil olan herkes veriye ulaşabilmekte, veri üzerine eklemeler yapabilmekte, veriyi kendi bilgisayarında saklayabilmekte, tanımadığı kişiler ile etkileşimde bulunabilmektedir. Özellikle Bitcoin bu sistem üzerine kurulmuş olup genel algı olarak blok zinciri kullanım şeklinin sadece bu sistem olarak ele alındığı yanlış bir şekilde değerlendirilmektedir. Elbette ki böyle bir sistemde bloklara kişisel verilerin işlenmesi GDPR uyumluluğunda birçok sıkıntıyı (verilerin ilgisiz insanlar tarafından görülmesi, veri sahibinin veri üzerindeki haklarının uygulanmasının imkansızlığı, veri sorumlusu tespitinin oldukça zor olması ve bu sebeple hesap verilebilme ilkesinin uygulanamaması vb.) barındırmaktadır. Halka açık ve izin gerektirmeyen blok zincirleri GDPR'a uygun bir sistemin kurulması pratik ve teorik açıdan mümkün değildir.

Halka Açık, İzin Gerektiren *(Public, Permissioned)*: Verilerin herkese açık bir şekilde gözüktüğü ancak zincire katılarak yeni veri işleme ve eklemeler yapmanın izne tabi olduğu sistemlerdir.

Özel, İzin Gerektiren *(Private, Permissioned)*: Verilerin herkese açık bir platformda yer almadığı, veri işlenmesinde mutabakat sürecine dahil olabilmenin izin gerektirdiği sistemlerdir. Bu sistemler dağınık veri tabanı özelliğinden merkezi yapıya yaklaşmasına sebep olmaktadır. Ağı meydana getiren kişiler, katılımcıların görevlerini, kimlerin ağa katılabileceğini tayin edebilmekte ve aynı zamanda veri işleme kurallarını oluşturmaktadır. Bu doğrulta yukarıda detaylıca bahsedilen GDPR gereklilikleri doğrultusunda *tasarımda gizlilik* prensibini bir blok zincirinde oluşturulması mümkündür.

4. Blok Zincirinde GDPR Uyumluluğunun Sağlanmasındaki Problemler:

Teknolojinin nasıl kullanıldığı noktasında GDPR uyumluluğu yaklaşımını ele almak doğru olacaktır. Yukarıda da bahsedildiği üzer blok zinciri kullanım şekilleri farklılaşmaktadır. Blok zinciri hakkında ortaya çıkan sorunlar ise genel olarak halka açık ve izin gerektirmeyen sistemler üzerinden oluşmaktadır. Özel ve izne tabi sistemlerde ise veri sahibi haklarının kullanılmasının mümkün olamayacağı üzerinde tartışmalar yapılmaktadır.

GDPR ile blok zinciri arasında 3 temel noktada sıkıntının var olduğu genel olarak belirtilmiştir:

a. Veri sorumlularının ve veri işleyenlerin kimlik tanıma ve yükümlülüklerinin saptanması,
b. Kişisel Verilerin Anonimleştirilmesi,

c. Bazı Veri Koruma Haklarının Kullanılması.

a. Hesap Verilebilme İlkesinin Blok Zincirinde Uygulanması

Öncelikli olarak GDPR kapsamında temel terimlerden kişisel veri işleme faaliyetini, hesap verilebilirlik ilkesini ve bu doğrultuda veri sorumlusunu ve veri işleyeni tanımlamak gerekmektedir.

Kişisel Veri İşleme Faaliyeti *(Processing)*: *"Kişisel veri işleme faaliyeti, otomatik yöntemlerle olsun veya olmasın, kişisel veri veya kişisel veri setleri üzerinde gerçekleştirilen toplama, kaydetme, düzenleme, yapılandırma, saklama, uyarlama veya değiştirme, elde etme, danışma, kullanma, iletim yoluyla açıklama, yayma veya kullanıma sunma, uyumlaştırma ya da birleştirme, kısıtlama, silme veya imha gibi herhangi bir işlem veya işlem dizisidir"*[2]. Genel anlamda veri işleme faaliyeti, kişisel verinin ilk elde edilişinden başlayarak imhasına kadar olan bütün süreci kapsamaktadır. Ayrıca belirtmek gerekir ki, ticari ve mesleki amaç doğrultusunda işlenmeyen hane halkı aktiviteleri kapsamında kişiler veri işleme faaliyeti GDPR düzenlemeleri dışında yer almaktadır.

Veri Sorumlusu *(Data Controller)* : Veri sorumlusu, yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenmesine ilişkin amaçlar ve yöntemleri belirleyen gerçek veya tüzel kişi, kamu kuruluşu, kurumu veya diğer herhangi bir organdır[3]. Yani veri sorumlusu, kişisel veri işleme araç ve vasıtalarını belirleyen kişi olarak tanımlanmıştır. Bu durumda blok zinciri, bir araç veya vasıta olarak kabul edilebilecektir. Buradaki belirleme yetkisi, veri sorumlusu olarak tayin edilen kişiler tarafından verileceği için sorumluluk da onlara aittir.

Veri İşleyen *(Data Processor)* : Veri sorumlusu adına, onun çizdiği amaç ve yöntemler doğrultusunda kişisel veriyi işleyen gerçek veya tüzel işi, kamu kurum ve kuruluşları veya diğer bir organdır[4].

Temel sıkıntılardan biri de GDPR'ın veri işleme sürecindeki hesap verilebilme ilkesinin blok zinciri üzerinde nasıl uygulanabileceği sorunudur. Zira veri sorumlusu ve veri işleyenin veri sahibine karşı birçok sorumluluğu vardır. Bunlardan biri de hesap verilebilirlik ilkesidir. Klasik sistemde, veri işleyen ve veri sorumlusu rahatlıkla tayin edilebilirken, özellikle halka açık izinsiz blok zincirlerinde bu durumun nasıl tespit edileceği tartışmasıdır. Zira veri sahibi GDPR'dan

[2] GDPR m.4 (2).
[3] GDPR m.4 (7).
[4] GDPR m.4 (8).

kaynaklı haklarını kullanırken (unutulma hakkı/ itiraz hakkı) veri sorumlusu veya veri işleyen olarak kime yönelmesi gerekecektir? Hesap verilebilirlik ilkesinin aslında sorumlu tayini açısından büyük bir önemi olacağı için veri sorumlusunun da kimliğinin tespit edilmesi gerekmektedir. Hesap verilebilme ilkesi 95/46 Direktif'te üzerinde durulmayan bu ilkenin GDPR açısından beklentisi, GDPR uyumluluğunun gerçekleştirildiğinin ve denetleyici makamlara *("Supervisory Authorities")* ispatlamasıdır. Uyumluluğun sağlanmadığı veya veri ihlallerinin gerçekleşmesi durumlarda veri sorumlusu 20.000.000.00 veya bir önceki mali yılın cirosunun 4% 'üne kadar para cezası öngörmektedir[5].

Halka açık, izin gerektirmeyen blok zincirlerinde veri sorumlusunun tayin edilmesi de sıkıntı barındırmaktadır. Genel olarak blok zincirinin tanınma şeklini oluşturan bu durum için GDPR uyumluluğunun sağlanması mümkün değildir. Verinin kimin tarafından işlendiği mutabakat yapısına kimlerin katıldığı tespit edilemeyeceği için "veri işleyen" ve "veri sorumlusunun" tayini oldukça zordur.

Halka açık olmayan ve izne tabi olarak veri işlenebilen blok zinciri, mutabakat yapısına karar veren ve mutabakat sürecine dahil olan kişilerin belirlenebilmesi mümkündür. Daha önce kuralların konulduğu bu sistemde veri sorumlusu/veri işleyen yetkili kişiler veya yetkili kişilerin kontrolü altında olan kişilerdir. GDPR, hesap verilebilirlik ilkesi her ne kadar halka açık ve izin gerektirmeyen sistemler bakımından uygulanamasa da özel ve izne tabi sistemlerde uyumluluk gerçekleşmesi mümkündür.

Ulusal Bilgi ve Özgürlük Komisyonu (Commision Nationale Informatique and Libértes, National Commission on Informatics and Liberty, CNIL), blok zincirinde yazma hakkına sahip olan ve madenciler tarafından veri işleme onayı gereken mesleki veya ticari bir faaliyetle ilgili olan sistemde, bu kişileri veri sorumlusu olarak kabul etmektedir. Yine CNIL, veri işleyenleri ise, veri sorumlusunun verdiği yetkiye dayanarak veri işleme faaliyeti gerçekleştiren veya veri işlenmesinde onay veren madenciler *(manner)* olarak tanımlamıştır.

b. Anonimleştirme ve Kişisel Veri Tanımı *(Personally Identifiable Information (PII) Anonymisations)*

GDPR kapsamında korunmak istenen veri, "*tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir ('veri sahibi'); tanımlanmış bir gerçek kişi özellikle bir isim, kimlik*

[5] GDPR m.77-84.

numarası, konum verileri, çevrimiçi 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 tanımlanabilen bir kişidir" [6]**.** Bu doğrultuda yaklaşıldığında blok zinciri üzerinde işlenen her veri değil, GDPR'ın öngördüğü şekilde bir kişiyi işaret eden her türlü veriler bahse konu olmaktadır. Kişinin ad ve soyadı, eğitimi, dini ve felsefi görüşü hepsi birer kişisel veridir. Aynı zamanda kişinin ekonomik durumu, fiziki özellikleri de kişiyi işaret ettiği takdirde kişisel veri olarak kabul edilecektir. Bu sadece tek bir veri ile olabileceği gibi birçok verinin bir araya gelmesiyle de bir kişinin tanımlanabilir olması durumunda da GDPR uyumluluğunun sağlanması gerekliliği gündeme gelecektir.

Anonim veri ise, GDPR'ın uygulama alanı dışında kalmaktadır. Anonimleştirme, veri ile kişi arasındaki bağıntıyı kesen veri imha yöntemidir[7]. Anonim veri ise, doğrudan bir kişiyi işaret etmediği için veri tabanında sadece anonim veri tutan kişiler, veri sorumlusu olmayacaktır. Bu noktada tartışılan husus ise, özet değerler *(hash value)* doğrudan bir kişiyi işaret etmediği için anonim veri olarak kabul edilerek GDPR yükümlülüklerinden kaçınılabilecekleri düşünülmektedir. Ancak her zaman bu özet değerler, anonim halde kalmayabilir. Her ne kadar blok zinciri üzerinde yapılan işlemler uzun haneli şifreler olarak gözükse de veri sahipleri veya veri sorumluları özel anahtarlarının yazılı olduğu bir kağıt veya dijital ortamı üstün koruma yöntemlerini sağlamak zorundadırlar. Özellikle Bitcoin gibi kripto paralarla işlem yapan kişilerin dikkatsiz ve bilinçsiz davranışlarının önüne geçilmesi için özel anahtarı saklayan yazılımlar çıkarılmıştır. Ancak ve ancak söz konusu bu yazılımlarda eğer ki bir güvenlik açığı olması durumunda kişilerin tespit edilmesi mümkün olacaktır. Bu sebeple doğrudan blok zincirine girilen değerlerin, anonim olarak kabul edilmesi veri ihlalleri riskini oluşturacaktır.

Bulanıklaştırma, Takma Ad Yöntemi *(Pseudonymisation)*:

Bulanıklaştırma, bireyi tespit edilmesini engelleyici bir yol olarak karşımıza çıkmaktadır. Bu yöntem ne anonim veri gibi veri ile kişi arasındaki bağıntıyı tamamen ortadan kaldırmakta ne de doğrudan veri ile kişi arasındaki bağıntıyı gözler önüne sermektedir. Bulanıklaştırma, "*kişisel verilerin tanımlanmış veya tanımlanabilir bir gerçek kişiyle ilişkilendirilmemesinin*

[6] GDPR m. 4 (1).
[7] Gerekçe 26.

sağlanması amacı ile ek bilgilerin ayrı tutulması ve teknik ve düzenlemeye ilişkin tedbirlere tabi tutulması koşuluyla, kişisel verilerin söz konusu ek bilgiler kullanılmaksızın spesifik bir veri sahibiyle artık ilişkilendirilemeyecek şekilde işlenmesidir" şeklinde belirtilmiştir[8].

Potansiyel olarak tanımlamaya izin verecek ilave bilgiler ayrı tutulması gerekir. Kolay bir şekilde herkesin erişimine açık olmaktan daha ziyade belli kişilerin bu yetkiye sahip olması, veri ihlal riskinin önüne geçilmesine yarayacaktır. Ayrıca bu durum kriptografi yöntemleri gibi teknolojik imkanlar da oldukça önemlidir. Tam bu noktada blok zincirinde gerekli korumayı sağlayabilecek şekilde dizayn edilmesi mümkündür.

Bulanıklaştırma/takma ad kullanımının yararları:

1- GDPR'a uygun olarak veri saklama şekli olması,
2- Veri ihlal riskini düşürmesi,
3- Veri işleme amacının değiştiğinde doğrulama gerektirebilir, veri işleme amaçları keyfi olarak değiştirildiğinde bildirim yapılmasını sağlaması,
4- Veri Sorumlusu ile veri sahibi arasındaki menfaat dengesi oluşturması

şeklinde sıralanabilir.

Son olarak blok zincirinde bulanıklaştırma/takma ad kullanılması, GDPR'ın gerekliliklerini blok zinciri üzerinde sağlanmasında bir yöntem olarak tercih edilebilir. Blok zincirinde kullanımında en çok soru işaretlerini barındıran durum veri sahibinin "unutulma hakkını" kullanamayacağına ilişkindir. Aşağıda unutulma hakkı kısmında detaylıca belirtileceği üzere özel ve izne tabi blok zincirlerinde verinin silinmesi mümkündür. Ancak her zaman bu blok zincir ağı kullanılmadığı için kişisel verinin korunması noktasında takma ad verinin kullanım amacına göre veri güvenliği açısından sağlıklı olacaktır. Zira bulanıklaştırma/takma ad yöntemi kullanılarak, kişisel verilerin blok zinciri üzerinde tutulmasından ziyade, şifrelenerek bir özet değerinin elde edilmesiyle, bu özet değerlerin zincirde tutulması; verinin silinmesi talep edildiğinde de bu değer kaydının silinmesiyle veri ne tamamen anonim hale gelecektir ne de silinecek/yok edilecektir. Ayrıca veri üzerinde herhangi bir değişiklik yapıldığında özet değerler örtüşmediği için verinin keyfi değiştirilmesinin de önüne geçilecektir. Bu noktada istenilen menfaat aslında verinin değiştirilmediğine ilişkin ispat açısından blok zinciri kullanılması bir anlam ifade edecektir. Bu yorumun yapılabilmesi ise GDPR'ın silme

[8] GDPR m. 4 (5).

yönteminin nasıl olması gerektiği noktasında kesin bir tanım yapmamasından kaynaklanmaktadır. Amaç, kişiye ait verinin kimse tarafından ulaşılamaz hale gelmesi ise verinin değil de veriye ulaşmada kullanılacak şifrenin silinmesi ile de GDPR kapsamında silme faaliyeti olarak değerlendirebilecektir.

c. Veri Sahibi Haklarının Blok Zinciri Teknolojisi Karşısında Kullanımı

Erişim Hakkı (Right to Access)[9]:Veri sahibinin kendisine ait verilerin işlenip işlenmediğini teyit etme ve veri işlemesinin olması durumunda hangi kişisel verilerinin işlendiği, hangi amaç doğrultusunda işlendiği, veri transferinin yapılıp yapılmadığı, ne kadar süreye kadar verileri saklayacakları gibi veri üzerindeki denetimini sağlayabilir. Bu durumda blok zincirinde veri işleyen ve veri sorumlusunun tayin edilmesi gerekmektedir. Halka açık ve izin gerektirmeyen blok zincirlerinde erişim hakkı, halka açık olmasına rağmen talep edilmesi halinde yine de kişisel veri sahibine bilgilendirme yapılması zorunludur. Halka açık olmayan, izin gerektiren blok zincirlerinde ise, mutabakat yapısını oluşturan ve veri işleyeme izin veren ve veri işleyen kişilerin veri sorumlusu/veri işleyen olarak kabul edilmesi durumunda GDPR tarafından veri sorumlusuna tanınan erişim hakkı kullanılması mümkün hale gelecektir.

Düzeltme Hakkı (Right to Rectification)[10]: Veri sahibi kendisine ait verilerin, doğru veya güncel olmadığı iddiası ile kişisel verinin değiştirilmesini talep hakkına sahiptir. Verinin düzeltilmesi ve verinin silinmesi faaliyetleri blok zinciri üzerinde değişiklik yapılması genel anlamı altında toplanmaktadır. Aşağıda düzeltme hakkının blok zinciri üzerinde nasıl kullanılabileceğine ilişkin yorum birlikte ele alınacaktır.

Unutulma Hakkı (Right to Erasure, Right to Forgotten)[11]: Veri sahibi, kişisel verisinin toplanma ve işleme amaçlarıyla ilgisinin kalmaması, daha önce verinin işlenmesi için göstermiş olduğu rızayı geri çekmek istemesi, kişisel verisinin işlenmesine itiraz ettiği ve veri işlenmesinin meşru bir gerekçesi olmaması, kişisel verisinin yasa dışı işlenmesi gibi sebeplerden ötürü verisinin silinmesini talep edebilme hakkına sahiptir. Veri sorumlusunun, verinin işlenmesi için hukuka uygun bir sebebi yoksa en kısa sürede kişisel verinin silinmesi gerekmektedir. Silme yöntemi, GDPR kapsamında veri imha yöntemlerinden biri olup dijital

[9] GDPR m.15.
[10] GDPR m.16.
[11] GDPR m.17.

ortamda kayıt altında tutulan kişisel verilerin uygun teknoloji kullanılarak tamamen ortadan kaldırmayı hedeflemektedir.

Halka açık, izin gerektirmeyen blok zincirinde, bloklara işlenen verilerin silinemez özelliği "Unutulma Hakkı"nın etkin bir şekilde kullanımının önüne geçmektedir. Zira zincir şeklinde dizayn edilen bu sistemde, bir önceki blok ve bir sonraki blok verinin asıl işlendiği bloktaki özet değeri veya veriyi muhafaza etmektedir. Bu durum ise bir bloktaki herhangi bir değişikliğin yapılmak istenmesinde sistemin baştan aşağı tekrar dizayn edilmesi gerekliliği sonucunu doğuracak, pratik olarak mümkün olmayacaktır. Ancak buradaki ana hedefin veriye bir daha erişilemez hale gelmesi, kişi hakkının teorik anlamda silinmesinden daha çok hak ihlalinin önlenmesi olduğu unutulmamalıdır.

Tüm bunlarla birlikte GDPR md. 17/2'de "mevcut teknoloji ve maliyetin" dikkate alınması gerektiğidir. Teknolojinin izin vermemesi ve maliyetin yüksek olması durumunda -yoruma açık ve tartışmalı olan bu durum- silinmemesini haklı bir gerekçe olarak göstermektedir.

Kanaatimize göre, getirilen istisna hakkın kullanımını engelleyecek; kişinin Anayasal hakkının ihlaline yol açacaktır. Ancak yine teknolojik imkanlar göz önüne alındığında sistemin izin vermemesi haklı gerekçe olarak yorumlanmaktan çok, sorumluluk hukuku kapsamında tayin edilecek cezada indirim sebebi olarak ele alınması isabetli olacaktır.

Bu durumda unutulma hakkı hiçbir şekilde blok zinciri sisteminde etkin bir şekilde kullanılamaz sonucunu doğurmamaktadır. Bununla birlikte özel ve izne tabi blok zincirlerinde ise işleyiş farklıdır.

Düzenlenebilir Blok Zinciri (Blockchain Redaction)

Son olarak değinilmesi gereken bir husus ise "blok zinciri üzerinde verinin silinebilmesinin mümkün olduğu" durumlardır. Bu işlem Accenture firmasının 2016 yılında patent başvurusu ile gündeme gelmiştir. "Düzenlenebilir Blok Zinciri Buluşu", halka açık olmayan izne tabi blok zincirlerinde verinin değiştirilebilir, silinebilir olmasını mümkün kılmıştır. Sistemin oluşturulması aşamasında GDPR tasarımda gizlilik *(privacy by design)* ilkesinin uygulanarak bir blok zinciri değişime açık bir şekilde oluşturulmaktadır. Kodlama ve işlem hatalarından, verilerin tutulmasına yönelik kapasite ve maliyetlerin kontrol edilmesinden, hukuksal düzenlemelerden kaynaklı olarak blok zincirinde bir değişikliğin gerektiği durumlar bakımından bu buluş çözüm niteliğindedir. Klasik bir blok zincirinde, her blok kendisinden

önceki bloğun özet değerini barındırdığı için bir bloktaki değişiklik bütün zinciri etkileyeceğinden blok zincirinin değiştirilmez özelliği olduğu belirtilmektedir. Ancak düzeltme özelliği ile birlikte sadece belirli kişilerin kontrolü altındaki blokların değiştirilmesine yönelik bir tasarım oluşturulmuştur. Blok zinciri bağlantısında, bloklara *"Bukalemun Özet Değer (Chameleon Hash)"* adı verilen karma bir fonksiyon eklenerek bloklar arasındaki bağlantının kilidinin açılmasını sağlayan gizli bir anahtar sağlanmaktadır. Böylelikle bloklar gereklilikler doğrultusunda düzenlenebilecek ve tekrardan kilitlenerek yetkisiz kişiler tarafından değiştirilmesi engellenecektir. Değişiklik yapıldığı zaman ise, standart zincir bozulacak ve değişiklik ise blok üzerinde belli olacaktır. Ancak Bukalemun özet değeri bozulmadan kalacak ve düzenlenen yeni sistem birbiriyle uyumlu halde kalmaya devam edecektir.

Özel ve izne tabi blok zincirlerinde uygulanabilecek bu özellikte ise değişiklik yapma hakkı belli kişilere özgülenmektedir. Sistemi kullanan yani bloklara veri işleyen herkese bu yetki tanımlanmamıştır. Eş değişle bu sistemin halka açık ve izin gerektirmeye blok zincirinde kullanılması mümkün değildir. Buluş, blok zincirinin merkeziyetçi ve güvenilir sistem özelliğinin bozulması soru işaretlerini doğurmuş olsa da blok zincirinin kullanılmasındaki diğer faydaları ortadan kaldırmamaktadır. Hala merkezi bir sistem olma özelliğini korumakta ve keyfi değişiklik yapılmasının önüne geçmektedir. Daha önceden kuralları belirlenmiş mutabakat yapısına uygun olarak yetkili kişiler tarafından değişiklik işlemi gerçekleştirilecek ve gereklilik sebepleri de kayıt altında tutulacaktır. Böylelikle GDPR'ın getirdiği şeffaflık ilkesi de sağlanmış olacaktır. Zira hala bu sistem yine özel ve izne tabi olan sistemlerin genel özelliği kapsamı içerisinde varlığını koruyacaktır.

Kimlerin değişiklik yapma yetkisi olduğu da daha önce tayin edileceğinden veri işlemede sorumlunun tayin edilmesi mümkün olacağı için GDPR uyumluluğu hem veri işleyenin sorumluluğu hem de veri sahibi haklarının etkin bir şekilde kullanılması sağlanmış olacaktır. Diğer taraftan ise blok zincirinin olanaklarının kullanılması devam edecektir. Elbette bu sistem sadece hukuksal düzenlemeler için kullanılmakla sınırlı değildir. Akıllı sözleşmelerde *(Smart Contract)* taraflar arasında değişiklik yapılması istenilen durumlar için de kullanılması mümkün olacaktır.

5. Blok Zincirinin GDPR'a Uyumluluğu için Çözüm Önerileri ve Sonuç:

DLT sistemlerinin GDPR'a uyumlu olabileceği noktasında birçok projeler/görüşler mevcuttur. Ancak henüz netleşmiş ve nasıl uyumlu kullanılabileceğine ilişkin bir regülasyon yoktur. Bir regülasyonun oluşturulmasını beklemek ise teknolojinin sağladığı faydalardan uzaklaşmaya

sebep olacaktır. Zira regülasyonların teknolojiye uygun olarak sürekli olarak oluşturulması hukukun belirlenebilir olması ilkesine aykırılık teşkil edecektir. Bu sebeple ana hedeflerin belirtildiği temel normlara uygun olarak teknolojinin kullanılması mevcut ortamda en isabetli görüştür.

Blok zinciri kullanımı elbette ki ihtiyaçlara göre belirlenmektedir. Merkeziyetçi sistemden uzaklaşılması ve güvenli veri transferlerinin gerçekleşmesi için hazine değerinde olan bu teknoloji, bazı şirket politikaları gereği bu güven ilişkisine ihtiyaç duymayabilir. Veri sahibi açısından blok zincirinin kullanılması gerçekten de verinin bozulmaması ve transfer kontrolü açısından oldukça değerli olacaktır. Kaldı ki yukarda bahsedilen önlemler alındığında, özel ve izne tabi blok zinciri kullanıldığında hem veri sorumluları hem de veri işleyenlerin tespiti mümkün olacağı ve veri sahipleri haklarını kullanabileceği için oldukça elverişli bir yöntemdir.

Eğer ki kişisel veri koruma şeklini sağlanamıyorsa, kişisel verileri blok zincirinde tutmaktan kaçınmak gerekir. Zira yapılacak bir hatanın geri dönüşü olmadığı takdirde ciddi para cezaları ve itibar kayıpları söz konusu olacaktır. Bu noktada bahsedilen husus "Tasarımda Gizlilik" (*privacy by design)* prensibinin sağlanmasıdır. Veri sorumlularından veri güvenliğini ve veri sahibi haklarını gözeten bir sistemin oluşturmaları beklenmektedir. Tereddütlerin olduğu ve veri etki analizlerinin olumsuz sonuçlanması durumunda blok zinciri kullanmamakta fayda olacaktır.

Blok zinciri kullanılmasının faydası tespit edildiği ve gerekli risk değerlendirilmeleri yapılıp olumlu sonuçlar alındığı takdirde kullanıcılara olabildiğince şeffaf bir şekilde veri sorumluları tarafından veri sahiplerine karşı aydınlatmanın yapılması gerekmektedir. Kullandıkları veri tabanı, yazılımların neler olduğu, veri sahibi haklarını nasıl kullanmaları gerektiği ve diğer yükümlülüklerini ve yaklaşımlarını belirttikleri gizlilik sözleşmelerinde açıkça gösterilmelidir.

Son olarak değinmek gerekirse, GDPR uygulamasından önce blok zincirini kullanan ve işledikleri veriler üzerinde veri sahibi haklarının kullanılması mevcut sistemlerinde mümkün olmayan veri sorumluları için durum ne olacağıdır. Öncelikle imhası gereken bir verinin imhasının gerçekleşmediği, çok önceden ilgisiz üçüncü kişilerle paylaşıldığı -halka açık blok zincirinde bu durum ile karşılaşabiliriz- durumlarda, veri ihlalinden bahsetmek mümkündür. GDPR, iletilen, saklanan veya işlenen kişisel verilerin kazara yasadışı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik

ihlalini veri ihlali olarak tanımlamaktadır. Öncelikle bu olaylarda veri ihlaline ilişkin GDPR hükümleri uygulama alanı bulacaktır. Ancak yine GDPR'da belirtilen "*Veri sorumlusunun kişisel verileri kamuya açıklamış olduğu ve 1. paragraf uyarınca kişisel verileri silmek zorunda olduğu hallerde, veri sorumlusu, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin talep etmiş olduğu kişisel verileri işleyenlerin söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu veri sorumlularınca silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atar.*[12] *"* hükmü doğrultusunda yorumlandığında "mevcut teknoloji ve uygulama maliyeti göz önünde bulundurulması hususu muğlak kalmaktadır. Bu hüküm veri sorumlusu ve veri işleyenlerin sorumluluklarından kurtulacağı şeklinde yorumlanabilse de, tayin edilecek cezada indirim sebebi olarak ele alınması isabetli olacaktır.

[12] GDPR m.17 (2).

REFERANSLAR:

- Accenture “Editing The Uneditable Blockchain, Why Distributed Ledger Technology Must Adapt to An Imperfect World”, 2016.
- Christian Wirth, Michael Kolain, Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data, 2018.
- Claudio Lima, Blockchain- GDPR Privacy by Design, How Decentralized Blockchain Internet will Comply with GDPR Data Privacy ,2018.
- Commision Nationale Informatique and Libertes, Blockchain and the GDPR: Solutions for a Responsible Use Of the Blockchain in the Context of Personal Data, 2018.
- General Data Protection Regulation, 2018.
- Jana Moser, R3 Reports, The Application&Impact of the European General Data Protection Regulation on Blockchains, 2017.
- Michele Finck, Blockchain and Data Protection in the European Union, Max Planck Institute for Innovation & Competition Research Paper, 2017.
- Paul Voight,Axel von dem Bussche, The EU General Data Protection (GDPR) Practical Guide. 2017.
- The European Union Blockchain Observatory and Forum, Bockchain and the GDPR, 2018.