SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 08.03.2023
Kabul | Accepted: 29.05.2023
doi 10.15337/suhfd.1262158

BULUT BİLİŞİMDE GİZLİLİK SÖZLEŞMESİ

Dr. Öğr. Üyesi Emin GİTMEZ*

Öz

Yeni teknolojiler geleneksel uygulamalarda köklü değişikliklere neden olmaktadır. Bilgiyi saklamak, transfer etmek, korumak önceleri bilgisayarlara bağlanabilen taşınabilir araçlarla mümkün iken günümüzde kullanıcılar istedikleri yerde ve zamanda herhangi bir araca ihtiyaç duymadan internet ağının olduğu her ortamda bilgiye ulaşabilmektedir. Bu imkân internet çağında bulut bilişim teknolojisinin ortaya çıkmasıyla geçerli olmuştur. Bulut bilişim bilgiyi depolamak ve bilgiye ulaşmayı kolaylaştırmakla birlikte bilginin ifşası riskini de beraberinde getirmektedir. Her bilgi, gizli bilgi niteliğine sahip değildir. Ancak bazı bilgilerin gizliliğinin sağlanması mutlak surette gerekli olabilir. Bu durumda, gizli bilginin 3. kişilerle paylaşılmasının engellenmesine dönük birtakım hukuki mekanizmaların devreye alınması düşünülebilir. Bu amaçla, gizlilik sözleşmesi bilginin gizliliğinin korunmasını sağlamak noktasında caydırıcı bir etki ortaya koyabilir. Bu etkinin ortaya çıkmasını sağlamak için gizlilik sözleşmesinin geçerli ve yasal bir belge olmasını sağlayıcı tüm unsurların göz önünde bulundurulması gerekir.

Anahtar Kelimeler

Teknoloji ve Hukuk • Bulut Bilişim • Mahremiyet • Gizlilik • Gizlilik Sözleşmesi

* Dr. Öğr. Üyesi. İnönü Üniversitesi, İİBF Siyaset Bilimi ve Kamu Yönetimi Bölümü, Hukuk Bilimleri Anabilim Dalı, Malatya, Türkiye | Asst. Prof., İnönü University, Faculty of Economics and Administrative Sciences, Department of Political Science and Public Administration, Department of Legal Sciences, Malatya, Turkey.
emin.gitmez@inonu.edu.tr • ORCİD 0000-0002-6678-2506.

Atıf Şekli ⚜⚜**Cite As**: **GİTMEZ**, Emin: "Bulut Bilişimde Gizlilik Sözleşmesi", SÜHFD, C. 31, S. 2, 2023, s. 629-663.

İntihal ⚜⚜**Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. ⚜⚜This article has been scanned via a plagiarism software and reviewed by at least two referees.

NON DISCLOSURE AGREEMENT IN CLOUD COMPUTING

Abstract

New technologies cause radical changes in traditional practices. While it was possible to store, transfer and protect in formation with portable devices that can be connected to computers, nowadays users can access information wherever and whenever they want, without the need for any tool, in any environment where there is an internet network. This possibility became valid with the emergence of cloud computing technology in cyber age. While cloud computing makes it easier to store and access information, it also brings the risk of information disclosure. Not all information is classified as confidential information. However, it may be absolutely necessary to ensure the confidentiality of some information. For this purpose, a non disclosure agreement can have a deterrent effect in ensuring the confidentiality of information. In order for this effect to occur, all the factors that make the non-disclosure agreement a valid and legal document must be taken into account.

Key Words

Technology and Law • Cloud Computing • Privacy • Confidentiality • Non-Disclosure Agreement

GİRİŞ

Günlük hayatta birçoğumuz dijital kaynaklarımızı bilgisayara bağlanabilen flash disk veya harici harddisk gibi araçlar aracılığıyla taşırız. Bu araçlar nispeten fiziki olarak küçük boyutta olduğundan çoğu zaman birçok insan bu araçların kaybolması durumuyla yüzleşir. Bu durum belki günlük hayatta en sık yaşanılan ve sonuçları itibariyle en sinir bozucu olayların başında gelir. Bununla birlikte veriyi taşıdığımız bu araçlarda yer alan verilerin fiziki müdahalelerle tahrif edildiği de hayatın olağan akışı içerisinde sıkça karşılaşılan bir durumdur.

İnternet teknolojisinin geçirdiği baş döndürücü dönüşüm iletişim ve veriye erişim konusunda ilerleme sağlamıştır. Veri bütünlüğü, güvenliği ve gizliliği konusunda ilerleme ise ağır aksak olmaktadır. Her gün internet platformlarına farklı amaçlar için zaman ve mekândan bağımsız olarak erişim sağlamaktayız. Her erişim çeşitli uygulamalar üzerinden internet dünyasına veri aktarımını da beraberinde getirmektedir. Bu veriler ağırlıklı olarak kişisel verilerimizdir. İnternetin sağladığı imkânlarla git-

mek istediğimiz adresleri bulabilir, herhangi bir konuya ilişkin yorumumuzu paylaşabilir, karnımız acıktığında yemek bile sipariş edebiliyoruz. Fakat her defasında veri stokladığımız bu sanal alanda acaba verilerimiz yok oluyor mu? Silinebiliyor mu? Verilerimiz kimlerle paylaşılıyor? Veri mahremiyetimiz sağlanıyor mu? Verilerimizin gizliliği nasıl korunuyor? Ya da verilerimiz birileri tarafından kazanç amaçlı kullanılıyor mu düşüncesi kafa karışıklığına neden olmaktadır. Ancak, bulut bilişimdeki gelişmelere rağmen verilerimiz halen silinmekte, kaybolmakta, bozulmakta ve çalınabilmektedir.

İnternet teknolojisindeki gelişmeler yeni uygulamaları da beraberinde getirmiştir. Bulut bilişim de bu yeni uygulamalardan bir tanesi olup özellikle verinin paylaşılması ve erişimi noktasında sağladığı kolaylıkla internet kullanıcıları açısından tercih edilmektedir. Bulut bilişim sağladığı imkânların yanı sıra çok çeşitli riskleri de beraberinde getirmiştir. Bu risklerin başında gizli verinin sahibinin izni olmadan 3. kişilerle paylaşılması gelmektedir. Uygulamada bulut bilişim hizmeti kapsamında servis sağlayıcı ile hizmet faydalanıcısı arasında paylaşılan bilgilerin gizliliğinin sağlanması amacıyla birtakım araçlar geliştirilmiştir. Gizlilik sözleşmesi, veri ifşasının bertaraf edilmesi amacıyla en sık kullanılan güvenlik aracıdır.

Bulut bilişimde gizlilik sözleşmesi çok önemlidir. Bu sözleşme, bulut hizmet sağlayıcısı ile müşteri arasındaki gizliliği, veri koruma beklentilerini ve yükümlülüklerini tanımlar. Gizlilik sözleşmesi, müşterinin verilerinin güvenliğini ve gizliliğini garanti eder, bulut hizmet sağlayıcısının verilerin kullanımına, paylaşımına veya satışına izin vermeyeceğini ortaya koyar. Bu çalışmada bulut bilişimde kullanılan gizlilik sözleşmesi hukuki açıdan ele alınmıştır.

I. BULUT BİLİŞİM

Bulut bilişim ağ içi veya ağlar arası veri paylaşımını mümkün kılan bir sistemdir. Esasen bulut kavramı ilk olarak interneti sembolize etmek için kullanılmıştır. Fakat zaman içerisinde farklı formlara bölünmüştür. Bulut bilişimle ilgili ilk çalışmalar 1950'lere dayanmaktadır. Bu dönemde yüksek kapasiteli bilgisayarları edinmek çok pahalı bir amaç olduğundan

sayısı az olan bu bilgisayarlardan maksimum faydayı elde etmek tüm hizmet sağlayıcılar ve hizmet alanlar için çok önemlidir. Bir ticari girişim olarak başlatılan bu çalışmalarda girişimci sayısı birden fazladır. Fakat gerçek anlamda bir bulut hizmetinin sağlanması 2000li yıllarda mümkün olmuştur. Bu minvalde gerçek anlamda ilk bulut bilişim hizmeti 2006 yılında Amazon S3 tarafından sağlanmıştır Başlangıçta kapalı kaynak kodlu tasarlanan servisler sonradan açık kodlu servislerin de hizmete girmesi ile yaygınlaşmıştır.

Bulut bilişim özelinde konunun uzmanlarınca uzlaşılan ortak bir tanımlama bulunmamaktadır. Herkes sağladığı fayda bağlamında bir tanımlama yapabilmektedir. Amerika Birleşik Devletleri'ndeki Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından bulut bilişim, ağlar, sunucular, depolama, uygulamalar ve hizmetler gibi yapılandırılabilir bilgi işlem kaynaklarının minimum yönetim çabası veya hizmet sağlayıcı etkileşimi ile isteğe bağlı ağ erişimi sağlayan bir model olarak tanımlanmaktadır[1]. Bu modelde hızla sağlanabilen ve yayınlanabilen paylaşıma açık bir kaynak havuzu yer almaktadır. Bulut bilişimin en esaslı özelliği paylaşılan bir kaynak havuzuna sahip olmasıdır. Bu kaynak havuzu, veri depolama ve veriyi paylaştırma konularında uzmanlaşmış şirketler aracılığıyla üçüncü kişilerin hizmetine sunulmaktadır.

A. Bulut Bilişim Mimarisi

Bulut bilişim farklı hizmet modelleri ile kullanıcılara fayda sağlamaktadır. Bu modellerin bölümlendirilmesi kullanıcı sayısı, gizlilik ve güvenlik açısından kapsam olarak farklılık gösterebilmektedir. Bununla birlikte sunulan hizmet modeline bağlı olarak yazılım geliştirmeden altyapı hizmetlerinin sağlanmasına kadar çok çeşitli amaçlarla servis hizmetleri kullanıcılara sunulmaktadır.

Basitleştirilmiş bir bulut bilişim iş akışı sürecinde, bulut bilişim hizmeti alan kişi istemini sisteme gönderir, ardından sistem yönetimi istem çerçevesinde doğru kaynakları bulur, doğru kaynakların bulunmasıyla

---

1 **BADGER**, Lee/**GRACE**, Tim/**PATT-CORNER**, Robert/ **VOAS**, Jeff: "Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology". (Special Publication No 800-146, National Institute of Standards and Technology: United States Department of Commerce, May 2011) 2-1.

müşteri isteği yürütülür. Son olarak da hizmet taleplerinin sonuçları istemcilere gönderilir[2]. Kullanıcılar bulut bilişim servisleri üzerinden internet ortamında neredeyse ihtiyaç duyulan tüm ürünlere erişebilmektedir. Bu hizmet ürünleri analiz ve blok zincir uygulamaları, iş uygulamaları, yazılım geliştirme araçları, mobil aplikasyonlar ve oyun teknolojisi, yapay zekâ ve robotik uygulamalar ile makine öğrenimi, nesnelerin interneti, sanal ve arttırılmış gerçeklik uygulamaları vb. uygulamaları içermektedir.

Bulut bilişim servislerinin sunduğu çözümler kullanım örneğine, sektöre ve kurum türüne bağlı olarak farklılık göstermektedir. Kullanım örneğinde arşivlemeden blokzincirine, veri tabanı geçişlerinden nesnelerin internetine kadar onlarca çözüm sunulmaktadır. Sektörel çözüm hizmetlerinde reklam ve pazarlama, otomotiv, eğitim, enerji, finansal hizmetler, oyun teknolojileri, telekomünikasyon, seyahat ve konaklama vb. sektöre yönelik iş çözümleri sunulmaktadır. Bulut bilişimde, kurum türüne bağlı olarak başta uluslararası/ulusal özel büyük ölçekli işletmelerin gizlilik, güvenlik, mevzuat uyumluluğu ile yönetimsel gereklilikler için tasarlanmış bir dizi hizmet yer alır. Bunun dışında henüz emekleme aşamasında olan startuplar için geliştirme ve büyümeye dönük sunulan hizmetler de bulunmaktadır. Ayrıca, kamusal otoriteler ile kar amacı gütmeyen kuruluşlar için toplumsal fayda düzeyini arttırıcı nitelikte inovatif çözümler geliştirilmektedir[3].

İnternet dünyasında dört temel bulut mimarisi konumlandırılmaktadır. Bu konumlandırma bulut hizmetlerinden yararlanan tarafların içinde bulundukları çevreye göre yapılmaktadır. Örneğin genel bulutta bulut hizmetlerinden milyonlar faydalanırken topluluk bulutlarında yararlanıcı düzeyi rakamsal yönde düşük kalmaktadır. Dört temel bulut bilişim türünden bahsedebiliriz.

---

2 **ERTAUL**, Levent/ **SİNGHAL**, Saurabh/ **GÖKAY**, Saldamli: "Security challenges in Cloud Computing, Thesis", California StateUniversity, EastBay, vol. 2, no. 06, 2009, s. 625–626, https://aws.amazon.com/tr/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/ (Erişim Tarihi: 30.12.2022).

3 Bulut Bilişim için bkz. Amazon, "Bulut Bilişim Nedir?", https://aws.amazon.com/tr/what-is-cloud-computing/?nc2=h_ql_le_int_cc# (Erişim Tarihi: 30.12.2022).

1. Genel Bulut (Public Cloud)

Genel bulut bilgi işleminde bulut hizmeti sağlayıcısı, internet ağı üzerinden hizmet modeli uygulamalarını yürütür. Kullanıcılara sunulan hizmet modeli içerik açısından zengindir. Herkes bilgi işlem hizmetlerinden faydalanabilir. Sunulan hizmetler ücretsiz olabilir ancak kullanılan depolama alanı ve ağ bant genişliğine bağlı olarak ücretli de olabilir. Genel bulut, bireysel sanal makineler ile bilgi işlem donanımının satın alınmasını ortadan kaldırır. Kurumsal düzeyde şirket bilgi işlem altyapısı ile geliştirme platformlarının kurulması ihtiyacına çözüm üretir. Genel bulut sağlayıcısı işlem kayıtlarının yer aldığı veri merkezleri ile donanım ve teknik altyapının tüm sorumluluğunu üstlenir. Böylece şirket maliyetlerinin düşürülmesine katkı sağlar. Ayrıca, genel bulut ölçeklendirme açısından sonsuz işlem yapma kapasitesine sahip olduğundan verilere hızla erişim sağlamak mümkündür. Genel bulut, çok kiracılı bir ortamdır; bulut sağlayıcısının veri merkezi altyapısı, tüm genel bulut müşterileri tarafından paylaşılır. Küresel ölçekte bulut bilişim hizmeti sunan Amazon Web Services (AWS), Google Cloud, IBM Cloud, Microsoft Azure ve Oracle Cloud gibi şirketler genel bulut hizmetleriyle milyonlarca müşteriye ulaşabilmektedir[4].

2. Özel Bulut (Private Cloud)

Özel bir bulutun kaynaklarını ve depolamasını yalnızca bir kişi veya işletme kullanır. Kullanıcılar, özel bulut hizmetlerine, başkalarının genel internetten erişemediği özel bir ağ üzerinden erişir. Özel bulutlar, bir şirketin tesislerinde fiziksel olarak bulunabilir. Bazı üçüncü taraf bulut sağlayıcıları, müşterilere genel buluttan daha yüksek bir fiyata özel bulut seçeneği de sunabilir. Özel bulutlar kaynaklarını internet üzerinden birden fazla müşteriyle paylaşmadığından, özel bulutlar kuruluşlara genel

[4] **PETER**, Mell/**TİMOTHY**, Grance: "The NIST Definition of Cloud Computing", NIST, 2011, s. 1-7, https://www.ibm.com/cloud/learn/cloud-computing. (Erişim Tarihi: 02.01.2023).

buluttan daha fazla güvenlik sunabilir. Ancak, özel bir bulut genellikle genel bir buluttan daha pahalıya mal olur[5].

3. Hibrit Bulut (Hybrid Cloud)

Bilgi işlem, depolama ve hizmetlerin bir kombinasyonunun kullanılmasıyla çalıştırılan genel ve özel bulut ortamlarından oluşan karma bir bilgi işlem platformudur. Tek bir genel bulut kullanmak güven açısından risk içerdiğinden günümüzde hibrit bulut bilgi işlem hizmetlerinden faydalanmak daha sık görülmektedir. Hibrit bulutun amacı, bir kuruluşa ait her tür uygulama veya iş yükü için koşullara bağlı olarak en uygun bulutu seçmektir. Böylece genel ve özel bulut kaynaklarının bir karışımı ile eşanlı bir senkronizasyon düzeyi sağlanarak verilerin depolanması ve taşınması daha esnek bir yapıya kavuşturulur. Birçok kuruluş, maliyetleri azaltmak, riski en aza indirmek, dijital dönüşüm çabalarını desteklemek ve mevcut yeteneklerini genişletmek için hibrit bulut platformlarını benimsemektedir. Hibrit bulut yaklaşımı, günümüzün en yaygın altyapı kurulumlarından biridir. Kuruluşların genellikle uygulamaları ve verileri yavaş ve sistematik bir şekilde geçirmesi gerektiğinden, bulut geçişleri genellikle hibrit bulut uygulamalarına yol açmaktadır[6].

4. Çoklu Bulut (Multi-clouds)

İki veya daha fazla farklı bulut sağlayıcısından iki veya daha fazla bulutun kullanılmasıdır. Bazı kuruluşlar, siber güvenlik sistemlerini geliştirmek için birden çok bulut sağlayıcısı kullanmayı tercih eder. Çoklu bulut ortamları, şirketleri içindeki farklı iş akışları, departmanlar veya şubeler için ayrı bulutların korunmasına da yardımcı olabilir. Ancak, çoklu bulut sistemiyle, tüm bulut kaynakları ve verileri ayrı altyapılarda çalışır ve bu da kaynakları bulutlar arasında paylaşmayı daha zor hale getirebilir. Tüm hibrit bulutlar çoklu bulutlardır, ancak tüm çoklu bulutlar hibrit

---

5 Genel Bulut için bkz. İndeed, "9 Types of Cloud Computing (With Definition and Tips)", https://www.indeed.com/career-advice/career-development/what-is-cloud-computing. (Erişim Tarihi: 02.01.2023).

6 Çoklu Bulut için bkz. İbm, "What is cloud computing?", https://www.ibm.com/cloud/learn/cloud-computing (Erişim Tarihi: 02.01.2023)

bulutlar değildir. Çoklu bulutlar, birden çok bulut bir tür entegrasyon veya düzenleme ile birbirine bağlandığında hibrit bulutlar haline gelir[7].

Teknolojinin sürekli olarak gelişmesine bağlı olarak kullanıcıların ihtiyaçları doğrultusunda yüksek performanslı bilgi işlem (high-performance computing cloud) bulutları da hizmet vermektedir. Bu kapsamda, bazen süper bilgisayarlar olarak adlandırılan yüksek performanslı bilgisayar uygulamaları ve cihazları için özel olarak bulut hizmetleri sağlanmaktadır. Bazı kuruluşlar, hava durumunu tahmin etmek veya kimyasal molekülleri modellemek gibi karmaşık hesaplama görevlerini gerçekleştirmek için süper bilgisayarlar kullanmaktadır[8].

B. Bulut Bilişimde Hizmet Modelleri

Bulut bilişimin sağladığı hizmet modelleri üç temel başlık altında kategorilendirilebilir. Bu sınıflandırma bulut bilişimin ilk keşfedildiği dönemden bugüne aynı şekilde kabul görmektedir.

1. Hizmet İçin Altyapı (IaaS)

Kullanıcının donanım ve depolama ihtiyacını karşılamak üzere sanallaştırma teknolojisi ile sağlanan bir servis türüdür. Bu modelde bulut sağlayıcı, depolama, sunucu ve ağ kaynakları gibi bilgi teknolojisi altyapılarını yönetir ve bunları internet üzerinden erişilebilen sanal makineler aracılığıyla abone kuruluşlara sunar. Model, iş yüklerini potansiyel olarak daha hızlı, daha kolay, daha esnek ve daha uygun maliyetli hale getirmek gibi kuruluşlar için birçok avantaja sahiptir. Hizmet modelinde, bir bulut sağlayıcı, şirket içi bir veri merkezinde geleneksel olarak bulu-

---

7 Çoklu Bulut için bkz. Red Hat, "Types of cloud computing", https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud#:~:text=There%20are%20four%20main%20types,a%2DService%20(SaaS); https://www.indeed.com/career-advice/career-development/what-is-cloud-computing. (Erişim Tarihi: 02.01.2023).

8 Çoklu Bulut için bkz. İndeed

nan altyapı bileşenlerini barındırır. Buna sunucular, depolama ve ağ donanımı ile sanallaştırma veya hiper yönetici katmanı da dahildir[9]. Bu model modern işletmelere hız, performans, güvenilirlik, yedekleme ve kurtarma ile rekabetçi bir fiyatlandırma hizmeti sunmaktadır[10].

2. Hizmet Olarak Platform (PaaS)

Müşterilere, genellikle işletme içinde sürdürüldüğünde ortaya çıkacak maliyet ve karmaşıklığı ortadan kaldırarak uygulamaları geliştirmek, çalıştırmak ve yönetmek için eksiksiz bir bulut platformu (donanım, yazılım ve altyapı) sağlayan bir bulut bilgi işlem modelidir. Bu bilgi işlem modelinde geliştirme araçları, veri tabanı yönetimi, ara yazılım, işletim sistemleri, teknik altyapı hizmetleri sunulabilir[11].PaaS ayrıca iş akışı ve tasarım araçları gibi tümü iş kullanıcıları ve geliştiricilerini memnun eden onların uygulamalar oluşturmasına yardımcı olmayı amaçlayan bir dizi ek hizmet sunar. PaaS ile geçmişte işletmelerin kendileri geliştirmek zorunda olduğu uygulamalar ile ortaya çıkan karmaşık yazılım yığınları, sık güncellemeler, donanım bakımından kaynaklı maliyetler ortadan kaldırılmıştır. Zaman ve maliyet açısından daha avantajlı bir çözüme kavuşulmuştur.

3. Hizmet Olarak Yazılım (SaaS)

Bulut sağlayıcının bulut uygulama yazılımı geliştirdiği, sürdürdüğü, otomatik yazılım güncellemeleri sağladığı ve kullandığın kadar öde sistemiyle internet aracılığıyla müşterilerine yazılım sunduğu bulut tabanlı bir yazılım sağlama modelidir. Tüketicilerin yazılım mimarisini, yazılım bakımını ve temel altyapıyı yönetmesine gerek yoktur. Son kullanıcılar, web tarayıcısı gibi bir istemci kullanarak SaaS uygulamasına erişir[12]. Büyümeyi, erişimi ve yeniliği destekleyen bir iş stratejisinin temel direkleri olarak çevikliğe ve operasyonel verimliliğe dayanır. Hem teknik hem de finansal açıdan çok çeşitli avantajları barındırır.

---

9 **MILLARD**, Christopher: Cloud Computing Law, Croydon 2013, sh. 6.

10 Hizmet Altyapı için bkz. Amazon, "Hizmet Olarak Altyapı (IaaS) nedir?", https://aws.amazon.com/tr/what-is/iaas/ (Erişim Tarihi: 05.01.2023)

11 Hizmet Platform için Bkz. İbm "What is PaaS?", https://www.ibm.com/cloud/learn/paas (Erişim Tarihi: 06.01.2023)

12 Mahremiyet için Bkz. Alibaba Cloud, "What Is SaaS?", https://www.alibabacloud.com/tr/knowledge/what-is-saas. (Erişim Tarihi: 07.01.2023)

Modern işletmeler üretim, yönetim, pazarlama benzeri gereksinimlerine göre bulut bilişim sağlayıcılarının sunmuş oldukları hizmetlerin bir ya da birkaçını kullanabilmektedir. Bulut bilişim şirketleri bu hizmetleri sunma aşamasında sanallaştırma teknolojisini kullandıklarından bu hizmetlerin farklı sağlayıcılardan aynı anda tedarik edilmesi de mümkündür.

C. Mahremiyet ve Gizlilik

Mahremiyet kavramı kişilerin kendileri ile baş başa kalabildikleri, düşünceleri, eylemleri ve duyguları ile şekillenen diğer kişilerin müdahil olamadıkları ve onlardan soyutlanmış sınırlı bir alandır. Bunun sınırlarını çizecek olan da insanın kendi iradesidir[13]. Zira mahremiyetin kapsamına kişinin çok yakınında olan değer verilen kişiler veya onlarla paylaşılan her türlü sır ve bilgi girebilir. Neyin aşılması durumunda mahremiyetin ihlal edileceği hususu kişilere göre farklılık gösterebilir. Modern dünyada mahremiyetin önemi teknolojik gelişmeyle birlikte daha değerli bir noktaya evrilmiştir. Özellikle veri kavramının ortaya çıkması ile gerçek dünyada yapılan birçok işlemin dijital alana taşınmasına bağlı olarak ihtiyaç duyulan kişisel veriler, mahremiyet konusunun tartışılma boyutunu da değiştirmiştir. Gelecek, mahremiyet açısından karanlık bir önerme sunsa da aslında mahremiyetin gerekli olduğu ve hatta en çok değer verilmesi gereken bir insan hakkı olduğu da göz önünde tutulmalıdır. Nitekim Amerikalı yargıç Brandeis tarafından ortaya atılan "yalnız bırakılma hakkı veya yalnızlık hakkı" hukukun üstünlüğü ve insan hakları açısından en temel haklar arasında kabul görmektedir[14].

Hem teknik hem de hukuki boyutuyla tartışıldığında genel olarak birbirinin yerine kullanılan mahremiyet ve gizlilik kavramlarının kullanımı doğru mudur? Gizlilik kavramsal olarak her zaman için mahremiyetin yerine kullanılabilir mi? Esasında gizlilik ve mahremiyet benzeşik anlamlara sahiptir fakat gizlilik karşıladığı anlamın kapsamı itibariyle mahremiyete göre daha geniştir. Mahremiyet bireye özeldir. Mahremiyet,

---

13 **YÜKSEL**, Mehmet: "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", Ankara Üniversitesi SBF Dergisi, C. 58, S. 1, 2003, s.185.

14 **BENNETT**, Louise: "Reflections on privacy, identityandconsent in on-lineservices", Information Security Technical Report, C. 14, S. 3, 2009, s. 119- 123.

kişinin kendisiyle veya sevdikleriyle başbaşa kalması veya onlarla herhangi bir konuda ortaklaşması, varoluşsal etkiler karşısında kabuğuna çekilmesi, ötekilere kapalı olmasını ifade eder. Bu anlamda mahremiyetin ortaya çıkması kişilerin kendileri hakkındaki bilgilere erişimi kontrol ettikleri sosyal düzenin bir sonucudur. Bu kontrolün bireylere nasıl verildiği ve mahremiyet kavramını ifade eden sosyal yapıları meydana getirmenin yolları doğrudan ilgi konusu olmamıştır. Açıkça, kişilerin başkalarının mahremiyetine saygı duyduklarını ifade ettikleri sosyal yapıların çoğu gayri resmi ve örtüktür.

Hukuk kuralları, mahremiyetin sosyal bağlamını oluşturmada da büyük bir rol oynar[15]. Bu kurallar, bir kişiye ait belirli alanları, evini, iletişim numarasını vb. kontrol etme iddiasını garanti eder ve bu garantiyi uygulanabilir yaptırımlarla destekler. Örneğin kişiye ait ırk, etnik köken, dini inanç, cinsel tercih, biyometrik verilerinden bahsederken kişisel verilerin mahremiyeti kavramını kullanabiliriz. Gizlilik ise kişinin yalnızlığı üzerinden değil, ortak olandan ve kamusal olandan kaçma üzerinden tanımlanabilir[16]. Bir şirkete ait ticari sırlar veya şirket içerisinde gizlilik gerektiren hususların dışarıya aktarılmaması, korunması söz konusu olduğunda genellikle gizlilik kavramı kullanılmaktadır.

Hukuk uygulamalarında bu ayrım gözönünde bulundurulmuş, dolayısıyla kişiye ait olmayan özel nitelikteki her türlü verinin korunması için gizlilik kavramı kullanılmıştır. Bu açıdan gizlilik sözleşmesi kavramsal olarak da doğru bir kullanımdır. Uygulamada da mahremiyet sözleşmesi değil gizlilik sözleşmesi şeklinde bir adlandırma yapılmaktadır. Gizlilik sözleşmesinin önemi verinin paylaştırılması, yaygınlaştırılması sürecinde önem arz etmektedir. Veri kavramının fazlasıyla önem kazandığı bir teknolojik dönemde verinin saklanması, gizlenmesi gerekmektedir. Bunun için de özellikle şirket dışından bulut bilişim hizmetinin alınması durumunda hizmet sağlayıcı ile yapılacak sözleşmelerde gizlilik şartlarının sözleşmelere konulması gerekir. Bu gizlilik şartları sadece hizmet sağlayıcı ile yapılacak sözleşmelerde dikkate alınmamalı aynı şekilde hizmet

---

15 **CHARLES**, Fried: "Privacy", Yale LawJournal, C. 77, 1968, s. 475–493.

16 **YILMAZ**, Latif: "Kayıp Kamusallığın İzinde: Mahremiyet, Gizlilik ve Kamusallık Üzerine", https://birikimdergisi.com/guncel/10472/kayip-kamusalligin-Izinde-mahremiyet-gizlilik-ve-kamusallik-uzerine (Erişim Tarihi: 10.01.2023)

sağlayıcıya bağlı aracı bir kurumdan alınması durumunda da gizliliğin sağlanmasına dikkat edilmelidir. Bunun yanında şirket içi bilgilerin, ticari sırların şirket dışına aktarılması riski de gizlilik politikası çerçevesinde önlenmelidir. Bunun içinde işletmede farklı pozisyonlarda çalışan yardımcıişçi, vekil gibi kişilere gizliliğe ilişkin bilgilendirme yapılması gerekir. Özellikle işletmeler açısından ticari sır niteliğindeki bilgilere erişimi olan çalışanlara bu bilgilerin ifşasının meydana getireceği olumsuz sonuçlar hususunda gerekli uyarıların yapılması gerekir[17]. Gerektiğinde personelin bu konuda eğitilmesini sağlayan bilinçlendirici faaliyetler de yürütülmelidir.

II. GİZLİLİK SÖZLEŞMESİ

Bulut bilişimde verilerin izin verildiği taktirde erişim sağlayan kişilerle paylaşımı mümkün olabilir. Bu konuda izin verme yetkisi verinin sahibine aittir. Her veri gizli değildir. Örneğin herkesçe bilinen bir bilgi, yasal olarak açıklanması zorunda olan bir bilgi veya hayatın olağan akışı içinde normal makul bir insanın sahip olduğu bilginin gizli bilgi olduğu değerlendirilemez[18]. Ancak, bazı bilgilerin gizli olması zorunluluk gerektirebilir. Bilginin açık veya gizli olmasının ayrımı bilgiye verilen değerle ölçülür. Her türlü özneye ait ticari sır, know-how, marka, fikir, icat, telif hakkı, teknik bilgi, patent vb. bilgilerin gizli olduğu söylenebilir. Bu bilgiler bir şirkete atfedildiğinde eşsiz bir değere sahiptir ve o şirketi diğerlerinden farklı kılan değerlerdir. Bu bilgilerin ifşa edilmesi söz konusu şirketi değersizleştirir. Bu nedenledir ki gizli bilginin korunması gerekir. Gizli bilginin kapsamı ve ifşası durumunda meydana gelecek mağduriyetlerin hukuk düzleminde ortadan kaldırılması ya da bir cezalandırmanın yapılması için gizlilik sözleşmesinin taraflar arasında yapılması mutlak anlamda bir gereklilik ortaya koymaz. Çünkü karşılaştırmalı hukukta zaten her ülkenin gizliliğin korunmasına dönük iç hukuk metinlerinde kapsayıcı düzenlemeler yer almaktadır. Örneğin Türkiye'de münhasıran

---

17 **YÜKSEL**, Armağan/**BOZKURT**, Ebru: "Ticari Sırların Dijital Ortamda Korunması", TAAD, C. 9. S.33, 2018, s. 157.

18 **KOWALSKİ**, Stanley P./**KRATTİGER**, Anatole: Intellectual Property Management in Health and Agricultural Innovation a handbook of best practices, Volume 2, California, 2007, s.693.

gizliliğin korunması kusur sorumluluğu[19], özen ve sadakat borcu[20], haksız rekabet hükümleri[21] ile ceza sorumluluğu[22] kapsamında yasal olarak düzenlenmiştir[23]. Durum bu olmakla birlikte uygulamada gizlilik arz eden bilgilerin korunmasının sözleşme sorumluluğu kapsamına alınması için gizlilik sözleşmesinin yapılmasının da özellikle ispat sorumluluğu açısından önem arz ettiği değerlendirilmektedir.

Gizli bilginin korunması paylaşılmaması ile mümkün olabilir. Dijitalleşme ile ortaya çıkan bilgiye kolay erişim gizli bilginin ifşa edilmesi yönüyle riskli bir durum meydana getirmektedir. Bu nedenle gizli bilginin gizli kalması için gizli bilgiye sahip olanların bir takım yükümlüler üstlenmesi gerekmektedir. Gizlilik sözleşmesi uygulamada gizliliğin taraflarca sağlanması için bir hukuki güvence sağlamaktadır. Gizlilik sözleşmesi, sözleşmeye taraf olanların hangi bilgilerin gizli olduğu konusunda mutabakata vardıkları ve bunu üçüncü kişilerle paylaşılmaması konusunda karşılıklı rıza uyumunun sağlandığı iki taraflı sözleşmedir. Bu sözleşmede gizli bilginin gizliliğini korumak isteyen taraf karşı tarafa

---

19 Hukuka aykırı ve kusurlu bir eylemi ile bir kişinin kişi ve malvarlığında bir zarara neden olma durumunda söz konusu olur. Örneğin gizlilik sözleşmesinde gizli bilginin korunması için gerekli dikkat ve özeni göstermeme ya da gizli bilgiyi ifşa ederek kusurlu bir eylem ile bilerek ve isteyerek zararlı bir sonucun meydana gelmesinin sözkonusu olması durumunda geçerlidir

20 6098 sayılı Türk Borçlar Kanunun 396. maddesinde "……. İşçi, iş gördüğü sırada öğrendiği, özellikle üretim ve iş sırları gibi bilgileri, hizmet ilişkisinin devamı süresince kendi yararına kullanamaz veya başkalarına açıklayamaz. İşverenin haklı menfaatinin korunması için gerekli olduğu ölçüde işçi, hizmet ilişkisinin sona ermesinden sonra da sır saklamakla yükümlüdür" hükmü yer almaktadır.

21 6102 sayılı Türk Ticaret Kanunun 55. Maddesinde sayılan haksız rekabet hallerinden " d) Üretim ve iş sırlarını hukuka aykırı olarak ifşa etmek; özellikle, gizlice ve izinsiz olarak ele geçirdiği veya başkaca hukuka aykırı bir şekilde öğrendiği bilgileri ve üretenin iş sırlarını değerlendiren veya başkalarına bildiren dürüstlüğe aykırı davranmış olur" şeklinde hüküm yer almaktadır.

22 5237 sayılı Türk Ceza Kanunun 239. madde hükmü "Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır" şeklindedir. Madde hükmünün devamında nitelikli hallerden bahsedilmektedir.

23 **ŞENBAŞ**, Pınar: Bilgi Teknolojileri Dış Kaynak Alımında (Outsourcing) Kişisel Verilerin Korunması ve Gizlilik Sözleşmeleri, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2013.

bu bilginin gizliliğinin sağlanması koşuluyla bu bilgiye erişim imkânı tanımaktadır[24] . Gizlilik sözleşmesinde edimin konusu gizli bilgidir, edimin ifası ise bu bilginin gizliliğinin sözleşme şartlarına uygun bir şekilde sağlanmasıyla mümkün olabilecektir.

Bulut bilişim hizmetlerinde gizlilik sözleşmesi, taraflarca ayrı bir sözleşme şeklinde düzenlenebilir. Bununla birlikte taraflar ayrı bir sözleşme yapmak yerine anlaşabildikleri ölçüde temel sözleşme içeriğine gizliliğin sağlanmasına dönük kişilere hak ve yükümlülükler de tanımlayabilirler[25]. Dolayısıyla yapılacak sözleşmenin şeklini belirleyecek olan şey taraf iradeleridir. Bu açıdan gizlilik sözleşmelerinin yapılış şekline ilişkin şekil serbestisinin var olduğu söylenebilir.

Taraflarının kim olduğuna bakılmaksızın bütün gizlilik sözleşmelerinde sözleşmeye konu olan ortak unsurlar bulunmaktadır. Sözleşmenin konusu, gizli bilginin tanımı, taraf yükümlülükleri, süre, ihlal durumunda karşılaşılacak hükümler tüm gizlilik sözleşmelerinde yer alan ortak unsurlardır. Gizlilik sözleşmenin konusu, gizli bilgilerin korunması gerektiğini ortaya koyan tarafın rızası alınmadıkça, bilginin diğer gerçek ve/veya tüzel kişiye verilmemesini, açıklanmamasını temin edecek olan gizliliğin sınırlarının ve koşullarının belirlenmesidir. Bir gerçek veya tüzel kişiye ait tüm bilgiler gizli değildir. Dolayısıyla bu noktada hangi bilgilerin gizli olduğunun ortaya konulması gerekir. Bu noktadan hareketle ilk olarak gizli bilginin tanımlanması zorunludur. Gizli bilginin tanımı tarafların kişisel, kurumsal ve sektörel pozisyonlarına göre değişebilir. Örneğin bir kişiye ait telefon bilgisi kişisel veridir ve kişinin rızası alınmadıkça 3. kişilerle paylaşılmaması gerekir. Oysaki bir şirkete ait iletişim numarası gizlilik içermez. Aksine daha fazla kişiyle paylaşılması şirketin arzu ettiği bir durumdur.

A. Gizlilik Sözleşmelerinde Taraflar

---

[24] **SIAS**, Suzanne L: " Confidentiality and Nondisclosure Agreements ", Buisness Law, vol. iv., 2008, s. 3-4.

[25] **BİLGE**, Mehmet Emin: Ticari Sırların Korunması, Asil Yayınları, 2. Baskı, Ankara 2005, s.100; **BAĞRIAÇIK**, Safiye Nur: Üretim ve İş Sırlarının Korunması (Özellikle Haksız Rekabet Hukuku Açısından), On İki levha Yay., 1.Baskı, İstanbul 2017, s.9; **SAATCIOĞLU**, Onur Can: Kanunlar İhtilâfı Hukukunda Ticari Sırların İhlali, Yetkin Yay., 1. Baskı, Ankara 2020.

Bulut bilişim hizmetlerinde gizliliğin her durumda sağlanması gerekir. Gizli verinin korunması ve güvenli kılınması hukuki ilişkinin taraflarının değişmesine bağlı olarak mahiyete uygun hükümlerin her seferinde sözleşme içeriklerine yerleştirilmesiyle mümkün olabilir. Aksi durumda gizli bilgilerin ifşası, telafisi mümkün olmayan zararların ortaya çıkmasına yol açabilir. Örneğin bulut hizmeti sağlayıcısından alınan bir hizmetin karşılığında hizmet sağlayıcının şirketin gizli bilgilerinin üçüncü kişilerle paylaşılmaması konusunda yükümlendirilmesi gerekir. Bu gizli bilginin ifşa edilmesi riskini azaltır fakat riski tamamen ortadan kaldırmaz. Çünkü, bu aşamada hizmet sağlayıcı ile bir gizlilik sözleşmesi yapılırken bulut hizmeti faydalanıcısının kendi çalışanıyla şirkete ait ticari sırların başkasıyla paylaşılmaması yönünde bir gizlilik sözleşmesi yapmaması bilginin korunması açısından riskli durumun devam ettiği gerçeğine karşılık gelir. Bu nedenle gizliliğin tam anlamıyla sağlanması gizli bilginin paylaşıldığı tüm aktörlerle her aşamada gizlilik sözleşmesinin yapılmasıyla mümkün olabilir.

Bulut servis sağlayıcısı, bulut hizmeti faydalanıcısına donanım, yazılım veya altyapı desteği sunan bulut bilişim hizmetinin baş aktörüdür. Bulut hizmeti sağlayıcısının olmaması durumunda bulut bilişimden bahsetmek mümkün olmayacaktır[26]. Bu nedenle bulut hizmet sağlayıcısı ile hizmet faydalanıcısı arasında yapılan gizlilik sözleşmesi en temel sözleşmedir. Bu sözleşmede düzenleyici tarafta teknolojik düzeyin her aşamasında ve alanında hizmet veren genel itibariyle Amazon AWS, Microsoft Azure, Google Drive gibi küresel şirketler, karşı tarafta ise gerçek kişiler ile kamu/özel tüzel kişileri yer almaktadır. Bu sözleşmede düzenleyici tarafından önceden tek taraflı olarak belirlenmiş genel sözleşme hükümleri ile ücret, süre vb. hükümleri içeren, hükümlerinin karşı tarafla müzakere edildiği özel sözleşme hükümleri yer alır. İmzalanacak sözleşmenin tüm hükümlerinin düzenleyici tarafından karşı tarafla müzakere edilmemesi teknolojik hayatın bir gereğidir. Zira bulut şirketleri çok sayıda kişiye benzer hizmetler sunmakta olup sürecin en az maliyetle en hızlı şekilde

---

[26] **CAVE**, Jonathan/**ROBINSON**, Neil/**KOBZAR**, Svitlana/**SCHINDLER**, Helen Rebecca: Regulatingthe Cloud: More, Lessor Different Regulation and Competing Agendas, https://ssrn.com/abstract=2031695 (Erişim Tarihi: 01.01.2023), s. 2; **HILBER**, Marc: Handbuch Cloud Computing, Köln, 2014, s. 3.

tamamlanması ticari/kamusal hayatın sürdürebilirliği için elzem görülmektedir.

Bulut bilişimde ana servis sağlayıcısı, bazı hizmetlerin yerine getirilmesini alt servis sağlayıcılardan tedarik edebilir. Alt servis sağlayıcısı, bulut bilişim kapsamında faydalanıcıya sağlanan bazı hizmetleri hizmet sağlayıcısına karşı yerine getiren alt yüklenicidir. Bu durumda da bulut hizmet sağlayıcısı ile alt servis sağlayıcısı arasında bir gizlilik sözleşmesinin yapılması gerekir. Gizlilik sözleşmesinin verinin dağıtılmasının her aşamasında yapılması kanuni bir gereklilik değildir. Ancak, verinin gizliliğini ihlal etme teşebbüsünde bulunacak taraf açısından caydırıcı bir yönünün olduğu söylenebilir. Peki, bütün güvenlik tedbirlerine rağmen yine de gizli verinin alt servis sağlayıcısı tarafından izinsiz paylaşılması durumunda sorumluluk kime ait olacaktır? Sorumluluk hukuku çerçevesinde sözleşmenin tarafı olan bulut bilişim servis sağlayıcısı ihlalden açık bir şekilde sorumludur. Hizmet faydalanıcısının servis sağlayıcı ile alt servis sağlayıcı arasındaki sözleşme ilişkisini bilmesi, servis sağlayıcı tarafından kurulan ilişkiye dair bildirimde bulunulmaması durumunda servis sağlayıcının sorumlu tutulması mümkün değildir. Hizmet faydalanıcısı, servis sağlayıcı ile alt servis sağlayıcı arasındaki sözleşme ilişkisini biliyorsa gizlilik hükümlerinin alt servis sağlayıcısını da içerecek şekilde genişletilerek bir sözleşme ilişkisinin kurulması veri güvenliği açısında yararlı olur. Bu durumda bile ihlal durumunda asıl sorumlu bulut hizmet sağlayıcısıdır. Bulut hizmet sağlayıcısının gizlilik hükümlerine uymaması durumunda meydana gelecek zararın tazminat sorumluluğu çerçevesinde karşılanması gerekir. Bu açıdan gizlilik sözleşmesinin varlığı tazminatın ödenmesi noktasında ispat hukuku açısından delil niteliğindedir[27]. Tazminatın miktarında taraflar uzlaşabilir, uzlaşmama durumunda mahkemenin vereceği karar kesin hüküm niteliğindedir. Bununla birlikte, bu-

[27] **TUNÇ**, Aybike: Bulut Bilişim Sözleşmelerinin Hukuki Yapısı, Yayımlanmış Doktora Tezi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara, 2020.

lut bilişim hizmet sözleşmesinin herhangi bir şekilde sona ermesi durumunda hizmet faydalanıcısına ait verilerin de silinmesine ilişkin hükümlere de gizlilik sözleşmesinde yer verilmelidir[28].

B. Gizlilik Sözleşmelerinin Hukuki Niteliği

Gizlilik sözleşmesi gizli bilginin olduğu ve korunması gerektiği her türlü hukuk ilişkide söz konusu olabilir. Bu hukuki ilişki bir satım, eser, vekâlet, devir veya hizmet ilişkisi olabilir. Bulut bilişimde hizmet sağlayıcı ile faydalanıcı arasında geçerli bir hizmet ilişkisi söz konusudur. Gizlilik sözleşmesi asıl borç ilişkisine bağlı bir sözleşme olabileceği gibi, asıl borç ilişkisinden bağımsız bir sözleşme olarak da düzenlenebilir. Bazı durumlarda ise bağımsız bir sözleşme olarak düzenlenmesine gerek duyulmaz, taraflar asıl borç ilişkisini doğuran sözleşmeye gizliliğe ilişkin hükümlerin konulmasını yeterli görebilir. Bu durumda taraf iradelerinin birbiriyle uyumlu olması gizliliğe ilişkin şeklin belirlenmesi için yeterli görülmüştür.

Sözleşme ve şekil serbestisi 6098 sayılı Türk Borçlar Kanuna hâkim olan temel ilkeler arasında yer alır. Gizlilik sözleşmesinin de kurulmasında şekil serbestisi geçerlidir. Gizlilik sözleşmesi hukuki sonucuna göre taraflar arasında borç ilişkisi kuran bir borçlandırıcı sözleşmedir. Gizlilik sözleşmesi, Türk Borçlar Kanununda ve diğer özel kanunlarda düzenlenmemiştir. Bu açıdan gizlilik sözleşmesi isimsiz bir sözleşmedir. Gizlilik sözleşmesi kendisine göre özgü bir yapısı olan suigeneris bir sözleşmedir[29]. Tarafların bir araya gelerek sözleşme içeriğini kendi rızalarına göre ortaya koydukları, kanunda düzenlenmiş sözleşmelerin unsurlarını içermeyen, sözleşme konusuna bağlı gizliliğe ilişkin hükümleri bir bütünlük içinde bir araya getirdikleri bir isimsiz sözleşmedir[30]. Gizlilik sözleşmesi edimin süresine göre, borçlunun ediminin süreklilik teşkil ettiği, sürekli borç ilişkilerinin düzenlendiği sözleşmelerdir. Sürekli sözleşmelerde asli

---

28 **SPLITTGERBER**, Andreas/**ROCKSTROH**, Sebastian: Sicherdurchdie Cloud navigieren – Vertragsgestaltungbeim Cloud Computing, BB 2011, Heft 36, s. 2182.

29 **TANDOĞAN**, Haluk: Borçlar Hukuku Özel Borç İlişkileri Cilt I/1, İstanbul 2008, sh. 68; **DONAY**, Süheyl: Meslek Sırrının Açıklanması Suçu, Sulhi Garan Matbaası, İstanbul 1978, s. 54.

30 **EREN**, Fikret: Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, Ankara, 2012, s. 107;**OĞUZMAN**, M. Kemal/ **ÖZ**, M. Turgut: Borçlar Hukuku Genel Hükümler, Cilt-I, Vedat Kitapçılık, İstanbul, 2012, s. 12.

edim, taraflar arasında sözleşme ilişkisi sona erinceye kadar sürekli olarak ifa edilir[31].

Edim ilişkisine göre gizlilik sözleşmesi bir tarafa borç yükleyen veya iki tarafa borç yükleyen sözleşme olarak kurulabilir. Tek tarafa borç yükleyen gizlilik sözleşmelerinde taraflardan yalnız biri gizliliğin sağlanması taahhüdüyle borç altına girmektedir. Diğer tarafın yerine getireceği herhangi bir borç yükümlülüğü bulunmamaktadır. Örneğin bulut bilişim hizmeti alan bir hizmet faydalanıcısının şirkete ait ticari sırların 3. kişilerle paylaşılmaması konusunda hizmet sağlayıcı ile yapmış olduğu gizlilik sözleşmesinde sadece hizmet sağlayıcı borcu yüklenmiştir. Bu ilişkide gizlilik sözleşmesi tek taraflı bir hukuki işlem olmayıp tek tarafa borç yükleyen iki taraflı bir sözleşme niteliğindedir. Tarafların ikisinin de gizli veriyi saklı tutma yükümlülüklerini karşılıklı olarak yerine getirmeyi taahhüt etmiş olması durumunda ise iki tarafa borç yükleyen gizlilik sözleşmesi söz konusudur. Bu durumda karşılıklı edimlerin değer açısından eşit olması gerekli değildir. Önemlilik arz eden husus gizli verinin ifşasının sözleşme hükümleri kapsamında her iki tarafça sağlanmasıdır. Örneğin bulut bilişim hizmeti alan faydalanıcının ticari sırlarının 3. kişilerle paylaşılmaması durumuna karşılık, hizmet faydalanıcısının da sadece kendisine sağlanan verileri başka kişilerle paylaşmaması bu duruma karşılık gelmektedir. İki tarafa borç yükleyen gizlilik sözleşmeleri tam ve eksik iki taraf borç yükleyen sözleşme şeklinde olabilir. Gizlilik sözleşmesi asıl borç ilişkisini düzenleyen sözleşme ile birlikte yapılabileceği gibi asıl borç ilişkisini düzenleyen sözleşmeden önce de yapılabilir. Bu bağlamda gizlilik sözleşmesinin hangi aşamada düzenleneceği tarafların iradeleri ile belirlenir. Bu noktada edimin konusunun değer açısından ortaya koyduğu nitelik önemlidir. Gizliliğin ihlal edilmesi telafisi mümkün olmayacak sonuçların veya yüksek maliyetlerin ortaya çıkmasına neden oluyorsa bu durumda gizlilik sözleşmesinin asıl borç ilişkisini düzenleyen sözleşmeden önce yapılması gerekir. Örneğin Amerika Birleşik Devletleri Savunma Bakanlığı tarafından yürütülen Ortak Kurumsal Savunma Altyapısı (JEDI) projesi bir bulut bilişim projesidir. Bu kapsamda Bakanlık

31 **EREN**, s. 213.

Amazon ve Microsoft'dan bulut bilişim hizmeti almaktadır. Asli edim konusunun askeri güvenlik olduğu bu tür durumlarda gizliliğin sağlanması bulut hizmet sözleşmesinin objektif esaslı noktası haline gelecektir.

Gizlilik sözleşmelerinin yeni bir hukuk alanı olan Start-up hukukunda kullanımı önem arz etmektedir. Start-up hukuku, teknolojinin desteği ile kurucuların başlattıkları ve büyüttükleri yeni bir iş girişimini bir temel oluşturmak için çeşitli yasal uygulama alanlarına verimli ve metodik olarak özenli bir şekilde entegre etme uygulamasıdır[32]. Start-up hukukunda gizlilik sözleşmesinin asıl borç ilişkisini düzenleyen sözleşmeden önce yapılması gizliliği sağlanması açısından önemli görülmektedir.

C. Gizlilik Sözleşmelerine Uygulanacak Hukuk Alanının Tespiti

Gizlilik sözleşmesi, taraflar arasındaki gizlilik yükümlülüklerini tanımlayan bir belgedir. Sözleşmenin uygulanacağı hukuk alanı, tarafların anlaştığı veya sözleşmenin yapıldığı yer olarak belirlenir. Örneğin, bir Türk şirketi ile bir Alman şirketi arasında yapılan bir gizlilik sözleşmesi olduğunu varsayalım, bu durumda hangi ülke hukuku uygulama imkânına sahiptir. Türk hukuku veya Alman hukuku gibi iki farklı hukuk sistemi arasındaki uyuşmazlıklarda hangi hukuk sisteminin uygulanacağını belirlemek için hukuk alanının belirlenmesi gerekir.

Bulut bilişimde gizlilik sözleşmelerine uygulanacak hukuk, tarafların hangi ülkeye mensup olmasına göre değişmektedir. Sözleşmenin her iki tarafının tabi olduğu hukukun aynı olması durumunda uygulanacak hukuka ilişkin bir ihtilaf söz konusu olmaz. Bu durumda taraflar uyuşmazlık durumunda tabi oldukları ülke hukukunun dışında diğer bir ülkenin hukuk hükümlerinin geçerli olacağına dair bir yetki anlaşması yapsa dahi, bu anlaşma geçersizdir. Ancak taraflardan bir tanesinin başka bir ülkenin hukuk düzenine tabi olması durumunda hangi ülke hukukunun öncelikli olarak uygulanacağına dair taraflar arasında bir anlaşmanın olması mümkün olabilir. Gizlilik sözleşmeleri bulut servis ana sözleşmelerinin bir parçası olduğundan uygulanacak hukuk da ana sözleşmede ortaya konulan hükümlere göre belirlenmektedir. Bulut bilişim hizmeti

---

[32] Gizlilik Sözleşmesi için bkz. Berkeley Law, "Startup Law Initiative", https://www.law.berkeley.edu/experiential/pro-bono-program/slps/current-slps-projects/startup-law-initiative/ (Erişim Tarihi: 15.01.2023)

sağlayan firmalar ağırlıklı olarak yabancı menşeli olduklarından uygulamada kanunlar ihtilafı hükümlerine başvurulduğu sıklıkla görülmektedir.

Avrupa Birliği Hukuku'nda bulut bilişim sözleşmelerinde taraflara diledikleri hukuku seçme hakkı tanınmıştır. Bu tanınma Avrupa Parlamentosunun 1215/2012 numaralı düzenlemesi mümkün olmuştur. Uluslararası Hukuka ilişkin Avrupa yasal çerçevesi, yani Brüksel I[33] ve Roma I[34] düzenlemeleri, belirli koşulların geçerli olması koşuluyla, yani sağlayıcının tüketiciye yönelik hedeflenen faaliyetinin geçerli olması koşuluyla devreye giren, tüketici sözleşmelerinde yargı yetkisi ve geçerli yasa hakkında özel kurallar içeren düzenlemelerdir. Dolayısıyla taraflar sözleşmede hangi hukukun geçerli olacağına dönük rızaları uyuştuğu sürece bir seçimde bulunabilirler ve sözleşme ilişkisi devam ederken mevcut hükümlerde değişiklik de yapabilirler.

Bulut bilişim hizmetleri ağırlıklı olarak ABD menşeli firmalar tarafından tüm dünyada küresel olarak sağlanmaktadır. Bu bağlamda CLOUD Act (Bulut Yasası) telekomünikasyon hizmet sağlayıcılarının depoladığı verilere yönelik yasal çerçeveyi güncellemiştir. Bu güncellemenin yapılmasında tamamen Amerika Birleşik Devletleri kolluk kuvvetlerinin istekleri esas alınmıştır. Böylelikle esasında CLOUD Act, başka bir ülkenin yasaları veya ulusal çıkarlarıyla çakışması durumunda, bulut hizmeti sağlayıcılarına istekleri reddetme hakkı tanımaktadır[35]. Bu yasa ABD düzenlemelerine tabi olmayan harici olarak yönetilen bulut hizmetleri sağlayıcılarına ABD dışında ikamet eden kuruluşlar için gerçek anlamda veri gizliliği sağlama fırsatı sağlar, Google veya Microsoft gibi küresel oyuncular için nerede olursa olsun bulut altyapılarını konumlandırmak veya verilerini barındırmak, ABD mevzuatına tabidir. Bir barındırma sağ-

---

33 Regulation (EC) 44/2001 of 22 December 2000

34 Regulation(EC) 593/2008 of 17 June 2008

35 Gizlilik Sözleşmesi Hukuk Alanı Tespiti için Bkz. Amazon, "Clarifying Lawful Overseas Use of Data (Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi – CLOUD) Yasası", https://aws.amazon.com/tr/compliance/cloud-act/ (Erişim Tarihi: 16.01.2023)

layıcısının ABD ile herhangi bir bağlantısı yoksa, ABD hükümetine verilere erişim izni vermek zorunda değildir. Tek yükümlülükleri verilerin bulunduğu yerdeki yargı yetkisine uyumu sürdürmektir.

Türk Hukuku'nda milletlerarasılık unsuru taşıyan sözleşmelerde uygulanacak hukukun tespitine dönük hükümler 5718 sayılı Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanunda (MÖHUK) düzenlenmiştir. Bu kanunda tarafların yapacakları yetki anlaşmaları düzenlenmiş ve bu yetki anlaşmalarının sınırları belirlenmiştir. Kanunun 47. Maddesinde "Yer itibariyle yetkinin münhasır yetki esasına göre tayin edilmediği hâllerde, taraflar, aralarındaki yabancılık unsuru taşıyan ve borç ilişkilerinden doğan uyuşmazlığın yabancı bir devletin mahkemesinde görülmesi konusunda anlaşabilirler" şeklinde bir hüküm mevcuttur. Bulut bilişim hizmetleri uygulamada rekabet avantajına sahip belli başlı yabancı menşeli küresel birtakım şirketler aracılığıyla yerine getirilmekte ve yabancılık unsuru içermektedir. Gizlilik sözleşmesi de bulut bilişim faaliyetlerinin bir tamamlayıcısı olup içeriğinde borçlandırıcı birtakım hükümler barındırır[36]. Sonuç olarak MÖHUK hükümleri esas alındığında taraflar gizlilik sözleşmelerinde diledikleri şekilde hangi yer hukukunun geçerli olacağına dair yetki anlaşması yapabilirler. Ancak bu gizlilik sözleşmesinin geçerli olabilmesi yazılı delille mümkün olacaktır. Uygulamada da görülmektedir ki gizlilik sözleşmesi her ne kadar şekil serbestisi söz konusu olsa da yazılı yapılmaktadır.

D. Gizlilik Sözleşmelerinde Görevli ve Yetkili Mahkemenin Tespiti

Gizlilik sözleşmesi yapılırken bir yetki alanın seçilmesi önemlidir. Bu yetki alanında iki temel unsur bulunmaktadır. Bu unsurların ilki gizlilik sözleşmesine aykırı bir fiil neticesinde veri gizliliğinin ihlali durumunda hangi ülkenin mahkemesinde dava açılabileceğidir. Diğeri ise hangi ülke hukukunun geçerli olacağıdır. Yargı yetkisi ile hukuk seçiminin eşleşmesi zorunlu değildir. Örneğin Kanada'da bulunuyorsanız, yargı yetkisinin Kanada'da olmasını ancak İngiliz yasalarının geçerli olmasını isteyebilirsiniz. Bu, taraflardan herhangi birinin herhangi bir davanın bir Kanada mahkemesinde açılmasını ve Kanada mahkemesinin

---

36 **TUNÇ**, s. 117.

önlerindeki davayı değerlendirirken İngiliz yasasını uygulamasını istediğiniz anlamına gelir.

Tek yönlü gizlilik sözleşmelerinde yargı yetkisi ve hukuk seçimi normalde ifşa eden tarafça belirlenir. Bunun nedeni, ifşa eden tarafın aynı zamanda normalde gizlilik sözleşmesinde ısrar eden, sözleşmenin hazırlanması ve oluşturulması için ödeme yapan ve ilk yer seçimini yapan taraf olmasıdır. İfşa eden tarafça yeri seçtikten sonra, alan tarafın yeri değiştirmek için güçlü gerekçeler bulması normalde daha zordur. Bununla birlikte, her iki tarafın da açıklamalarda bulunduğu ve diğer taraftan gizlilik talep ettiği karşılıklı gizlilik sözleşmelerinde, en büyük pazarlık gücüne sahip taraf yargı ve hukuk seçimine karar verir[37].

Gizlilik sözleşmeleri oldukça uzmanlaşmış telif hakkı ve fikri mülkiyet konularını ele alma eğiliminde olduğundan, belirli bir mahkemenin veya hukuk seçiminin, bu tür bir konuda karar vermek için gerekli yargı yetkisine ve deneyime sahip olup olmadığını dikkate almak önemlidir. Bazı mahkemeler, dava konusunun tespiti konusunda kendilerini yetersiz görebilir ve görevsizlik kararı verebilir. Örneğin, ABD'de patent ihlalleri, eyalet yasalarının değil, federal mahkemelerin münhasır yargı yetkisine girer. Bir yargı yerini belirlemek ve hukuk seçimi basit bir iş değildir. Hangi kanunlar ihtilafının geçerli olabileceği ve belirli bir ülke ve eyaletin sonucunuz için olumlu olup olmayacağı da dahil olmak üzere dikkate alınması gereken çok sayıda karmaşık konu söz konusudur. Dolayısıyla, bir hata ek yasal maliyetlere ve daha da kötüsü istenmeyen bir sonuca yol açabilir.

Uygulamada bulut bilişim hizmet sözleşmelerinde uygulanacak hukuk ve yargı yerinin genel işlem koşulları şeklinde servis sağlayıcı tarafından muhatapla müzakere edilmeden tek taraflı belirlendiği görülmektedir. Servis sağlayıcı gizlilik sözleşmesi yapıldığı anda genel itibariyle daha güçlü bir konumda olduğundan uygulanacak hukukun tespiti de onun iradesi yönünde belirlenmektedir. Örneğin Microsoft Azure ağırlıklı olarak gizlilik sözleşmelerinde uygulanacak hukukun tespiti ve

---

[37] EveryNDA, "Choice of law and jurisdiction in NDAs", https://www.everynda.com/blog/choice-law-jurisdiction-nda/ (Erişim Tarihi: 30.01.2023)

yargı yerinin belirlenmesinde Birleşik Devletler hukukunun geçerli olacağını de faktör kabul etmektedir[38].

Amazon AWS ise münhasır yargı yetkisini kabul etmektedir. Münhasır yargı yetkisi, tarafların gizlilik sözleşmesinde belirtilenler dışında başka bir mahkeme veya kanunun dâhil olmasını istemedikleri anlamına gelir. Sözleşmede adı geçmeyen diğer mahkemelerin, sözleşmede adı geçen münhasır bir yargı yetkisinin olduğu durumlarda yargı yetkisini kabul etme olasılığı daha düşüktür. Uygulamada Amazonun dünyanın farklı bölgelerinde kurduğu bulut merkezlerinin konumlandığı yere göre hangi ülke hukukunun uygulanacağı ve hangi yargı yerinin görevli olduğu değişmektedir[39]. Sorunların çözümü noktasında tahkim uygulaması da yer bulabilmektedir.

Genel işlem koşulu niteliğinde yetki anlaşmasının varlığı durumunda uygulanacak hukuk bu hükme göre belirlenecektir. Sözleşmede belirlenen hükmün uygulanacak hukuka aykırı olması durumunda yetki

---

38 "Bu sözleşme, yasaların ihtilafı hükümleri dikkate alınmadan, şu istisnalar dışında Washington hukukuna tabidir: (i) ABD Hükümeti'ne bağlı bir kurum iseniz, bu sözleşme Birleşik Devletler yasalarına tabidir ve (ii) Birleşik Devletler'de bulunan bir eyalet veya yerel kamu kurumu iseniz bu sözleşme o eyaletin yasalarına tabidir. Bu sözleşmeyi uygulamaya yönelik tüm davalar, Washington Eyaleti mahkemelerinde açılmalıdır. Bu yetki anlaşması, taraflardan herhangi birinin, fikri mülkiyet haklarının ihlali konusunda uygun bir yetkili mahkemede ihtiyati tedbir aldırmasını önlemez" Bkz., Microsoft, "Microsoft Çevrimiçi Üyelik Sözleşmesi – ABD Kamu Bulut", https://azure.microsoft.com/tr-tr/support/legal/subscription-agreement/government/ (Erişim Tarihi: 01.02.2023)

39 "İlgili AWS Sözleşme Tarafı, Amazon AWS ServiçosBrasilLtda. ise taraflar işbu Madde 13.5(c) hükümlerinin geçerli olacağını kabul eder. İhtilaflar, Uluslararası Ticaret Odasının o tarihte geçerli olan Tahkim Kurallarına uygun olarak, mahkemeye götürmek yerine, taraflar arasında bağlayıcı olan tahkim yoluyla çözülecektir ve hakem kararına ilişkin karar, yargı yetkisine sahip herhangi bir mahkeme tarafından verilebilir. Tahkim, Brezilya'nın São Paulo Eyaleti, São Paulo Şehrinde yapılacaktır. Üç hakem olacaktır. Hakemlerin ve, varsa, idare makamının ücret ve masrafları taraflarca eşit oranda ödenecektir. Taraflar, bu tür tahkim davasının varlığının ve bunlarla ilgili bilgilerin taraflardan herhangi biri tarafından ifşa edilmeyeceğini ve bunların gizli bilgi oluşturacağını kabul eder. Yetkili Mahkemeler, yalnızca (i) tahkim davasının başlamasını sağlamak; ve (ii) tahkim mahkemesinin kurulmasından önce koruyucu ve geçici tedbirler vermek üzere münhasır yargı yetkisine sahiptir".
Bkz.,Aws, "Aws Müşteri Sözleşmesi", https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_Turkish_Translation.pdf (Erişim Tarihi: 02.02.2023)

anlaşmasının uygulanması hukuka aykırılık teşkil eder[40]. Eğer sözleşmenin karşı tarafı genel işlem şartını kabul etmez ve sözleşme hükmü olmasına rıza göstermezse Roma I Tüzüğü md. 10/I hükmü gereğince kendi mutat meskeni hukukuna dayanabilir[41]. Ancak, bulut bilişim sözleşmeleri yabancılık unsuru içermelerine binaen her ülke için belirlenen genel işlem koşullarının değiştirilmesi uygulamada çok mümkün görülmemektedir[42].

E. Gizlilik Sözleşmelerinde Genel İşlem Koşulları

6098 sayılı Türk Borçlar Kanunun md.20/1 hükmü gereğince genel işlem koşulları, bir sözleşme yapılırken düzenleyenin, ileride çok sayıda benzer sözleşmede kullanmak amacıyla, önceden, tek başına hazırlayarak karşı tarafa sunduğu sözleşme hükümleridir. Genel işlem koşulları hızla gelişen teknolojinin iş hayatında meydana getirdiği zorunlu bir yeniliktir. Genel işlem koşulları sözleşmelerde standardizasyon ve rasyonalizasyon sağlamaktadır. Bununla birlikte zaman yönünden sözleşmelerin hızlı ve kolay yapılması ile iş hayatında uzmanlaştırmayı da beraberinde yerine getirmektedir[43]. Gizlilik sözleşmesine Türk hukukunun uygulanacağı durumlarda yürürlük, yorum ve içerik denetiminin yapılması kanuni bir gerekliliktir. Gizlilik sözleşmesinin içeriğine ilişkin düzenleyen taraf, sözleşmenin yapılması sırasında karşı tarafa sözleşmede yer alan genel işlem koşullarının varlığı hakkında açıkça bilgi vermelidir. Aynı şekilde düzenleyen taraf karşı tarafa genel işlem koşullarının içeriğini öğrenme imkânı sağlamalıdır. Bu durum şartların okunması, değerlendirilmesi ve kabulüne ilişkin makul bir süreyi tanımayı içerir. Gizlilik sözleşmelerinde genel işlem şartlarının denetimi kapsamına yorum denetimi girer. TBK md. 23 gereğince sözleşmede yer alan bir hüküm, açık ve anlaşılır değilse veya birden çok anlama geliyorsa, düzenleyenin aleyhine ve karşı tarafın lehine yorumlanır. Gizlilik sözleşmesinde yer alan genel işlem koşulları hu-

---

40 **BORGES**, George/**MEENTS**, Jan Geert: Cloud Computing Rechtshandbuch, München 2016, s. 42.

41 **SÄCKER**, Franz Jürgen/**RIXECKER**, Roland/**OETKER**, Hartmut/**LIMPERG**, Bettina: MünchenerKommentar zum BGB 7. Auflage 2018, Band 12, Rn. 11; https://beckonline.beck.de/?vpath=bibdata/komm/MuekoBGB/cont/MuekoBGB%2Ehtm (Erişim Tarihi: 05.02.2023)

42 **EREN**, s. 215.

43 **EREN**, s. 215.

kuki niteliği itibari ile sözleşme hükmüdür fakat emredici nitelikte değildir. Bu hükümler sözleşmenin asli hükümleri şeklin de yorumlanamaz. Bunlar arızi hükümlerdir[44]. Çünkü sözleşmenin asli hükümlerinin genel işlem koşulları şeklinde düzenlenmesi mümkün değildir. Asli hükümlerin sözleşmenin tarafları arasında müzakere edilerek hükümler üzerinde bir uzlaşmanın sağlanması gerekir.

Genel işlem koşullarına ilişkin Alman Medeni Kanununda da hükümler bulunmaktadır. Alman hukukuna göre genel işlem koşulları sözleşme metnine dahil edildiği taktirde karşılık bulacaktır. Başka bir deyişle, genel işlem koşulları açısından sözleşme metninin önceden kaleme alınması başlı başına hukuki bir işlem olarak nitelendirilemez. Bu hükümlerin hukuk düzenince kabul görmesi için sözleşmenin karşı tarafının kendisine sunulan bu koşulları kabul etmesi gerekir[45]. Aslında Türk hukukunda var olan genel işlem koşullarına ait hükümlerin kaynağı Alman Medeni Kanunun 305-310 arası madde hükümleridir. Bu nedenle, Türk ve Alman hukuku açısından genel işlem koşullarının içerik denetimlerinin aynı olduğu söylenebilir. Yine Avrupa Birliği Konseyi' nin de 05.04.1993 tarihli Tüketici Sözleşmelerinde Kötüye Kullanılabilir Sözleşme Şartları Hakkında 93/13 No'lu Konsey Yönergesi tüketicileri konu alan bir yönerge olup uygulanma alanı sadece genel işlem koşullarıyla sınırlı olmayıp bireysel sözleşme hükümlerini de kapsamaktadır[46]. Bu düzenlemelerde yer alan genel işlem koşullarına ilişkin hükümler mahiyetine uygun olması koşuluyla bulut bilişim gizlilik sözleşmelerin de uygulama alanı bulur.

Gizlilik sözleşmesinde taraflara ait isim, adres, e-mail adresleri ile birlikte sözleşmenin akdedildiği tarih dışında neredeyse sözleşmenin tamamı bulut servis sağlayıcısı tarafından tek taraflı olarak düzenlenmektedir. Sözleşmede, gizli bilginin tanımı ve kapsamı, hangi bilgilerin gizli bilginin kapsamı dışında olduğu, gizli bilginin kullanımı ve ifşasına ilişkin hükümler, ifşa durumunda uygulanacak hukuk alanının seçimi, gizli bilgilerin sahipliğine ilişkin açıklamalar, yetkisiz kullanım durumunda

---

44 **HAVUTÇU**, Ayşe: Açık İçerik Denetimi Yoluyla Tüketicinin Genel İşlem Şartlarına Karşı Korunması, İzmir 2003, s. 179; **EREN**, s.218-220.

45 **GEZDER**, Ümit: Tüketici Kredisi Sözleşmeleri, İstanbul 1998, s. 145.

46 **HAVUTÇU**, s. 65.

bildirim, sözleşmenin sona ermesi durumunda gizli bilgilerin iadesi, ihtiyati tedbir hükümleri, kapsam ve sözleşme süresinin dolması ile çeşitli hükümler yer almaktadır. Bu başlıklara ait hükümler genel işlem koşulları şeklinde bulut bilişim servis sağlayıcısı tarafından önceden belirlenmiştir[47]. Uygulamada bulut bilişim gizlilik sözleşmeleri katılmalı sözleşme niteliğindedir. Sözleşme içeriğinin tamamı veya belirli bir kısmı önceden bulut servis sağlayıcısı tarafından düzenlenmiştir. Bu nedenle sözleşmenin karşı tarafı açısından tek bir alternatif durum söz konusudur. Sözleşmeyi kabul etmek veya reddetmek. Bulut bilişim hizmetinin ağırlıklı olarak yabancı menşeli firmalarca yerine getirildiği göz önüne alındığında gizlilik sözleşmesinde hangi ülke hukukunun geçerli olacağına dair açık bir hüküm varsa, uygulanacak hukuk hükümleri ilgili ülkeye ait olacaktır.

F. Gizlilik Sözleşmelerinde Sorumsuzluk Antlaşması

Sorumsuzluk anlaşması veya hükümleri sözleşmenin ihlalinden doğan zararın gerçekleşmesinden önce taraflar arasında açık veya örtülü yapılır. Bu anlaşma ileride ortaya çıkması muhtemel durumların varlığında, alacaklının tazminat talebinin tamamen veya kısmen ortaya çıkmasını engelleyen bir tür anlaşmadır[48]. Bulut bilişimde gizlilik sözleşmesinin tarafları aralarında anlaşmak suretiyle gizli bilginin ifşası nedeniyle tam bir sorumsuzluk anlaşması yapabilecekleri gibi, sınırlı bir sorumluluk anlaşması da yapabilirler. Burada gizlilik ihlalinden doğan sorumluluğu çerçevesi tarafların iradesine bağlıdır. Ancak ister kişisel ister ticari sır niteliğinde olsun gizlilik sözleşmesinin asıl edim yükümlülüğü taraflar açısından gizli bilginin ifşasını engellemek olduğundan kasti bir eylemden kaynaklı gizlilik ihlalinin sorumsuzluk anlaşması kapsamına alınması mümkün değildir. Nitekim TBK mad. 115'e göre borçlunun kasıt ve ağır ihmalden kaynaklı kusurundan doğacak zarardan sorumlu olmayacağına ilişkin sorumsuzluk anlaşması kesin hükümsüzdür. Bu bağlamda TBK 116 kapsamında sorumsuzluk anlaşması yapmak mümkün iken borç ilişkisinin konusunun bulut bilişim hizmeti olması durumunda

---

47 Gizlilik Sözleşmesinde Genel İşlem için bkz. Amazon, "Mutual Non-Disclosure Agreement", https://s3.amazonaws.com/cdn.prpl.rs/docs/PRPL-NDA.pdf (Erişim Tarihi: 07.02.2023)

48 **EREN**, s. 1108.

akdedilecek bir gizlilik sözleşmesinde gizliliğe ilişkin sorumsuzluk hükümlerine yer verilmesinin uygun olmayacağı kanaatindeyim. Örneğin aynı şirkette birlikte çalışan sistem güvenliği konusunda yetkilendirilmiş bir kişinin ihmalinden kaynaklı olarak diğer çalışanın gizli bilgileri ifşa etmesi durumunda, şirketin bu durumdan sorumluluk duymayacağına ilişkin gizlilik sözleşmesine hüküm konulması mümkün görülmemektedir. Bununla birlikte, bir hizmet, meslek veya sanat uzmanlık gerektiriyorsa ve kanun ya da yetkili makamlarca verilen bir izinle faaliyetler yürütülebiliyorsa, borçlunun hafif kusurundan sorumlu olunmayacağına ilişkin akdedeceği anlaşma kesin olarak hükümsüz olacaktır. Örnek vermek gerekirse sistem güvenliği konusunda hizmet veren bir siber güvenlik şirketinin hizmet verdiği şirketin hafif bir kusuruyla meydana gelen bir güvenlik ihlalinden sorumluluk duymayacağına ilişkin sözleşme kesin hükümsüzlük yaptırımına tabi olacaktır. Çünkü bulut bilişim hizmetlerinde işin doğası gereği sistemin arızalanması, yavaşlaması, performans kaybı veya veri kaybı gibi risklerle karşılaşılması her zaman mümkündür. Bu tür durumların varlığında elbette ki bulut hizmet sağlayıcısının sorumluluğu sözkonusu olacaktır. Bu nedenle örneğin, sistem altyapısının hafif bir kusur davranışı nedeniyle arızalanması, veri kaybının oluşması veya gizli bilgilerin ifşası durumunda hizmet sağlayıcının sorumlu olmayacağına dair gizlilik sözleşmesinde hükümlere yer verilmesi durumunda sözleşme hükmü yukarıda açıklandığı gibi geçersiz olacaktır.

Bulut hizmet sözleşmelerinde öngörülen sorumsuzluk hükümleri ağırlıklı olarak genel işlem şartı niteliği taşımaktadırlar. Uygulamada hem bulut bilişim ana hizmet sözleşmeleri hem de gizlilik sözleşmeleri düzenleyen tarafından önceden hazırlanmıştır, sözleşmede yer alan hükümler çoğunlukla karşı tarafla müzakere edilmeden sözleşmeye konulmuştur.

"Kullanıcıların …….. tarafından sunulan hizmetlerden/servislerden yararlanabilmek amacıyla kendilerine verilen bilgilerin (Kullanıcı ismi, şifre, e-posta, doğum tarihi, cinsiyet, telefon vb.) güvenliği, saklanması, bunların 3. kişilerin bilgisinden ve kullanımından beri tutulmasıyla ilgili hususlar tamamen kullanıcıların sorumluluğundadır. Kullanıcıların web sitesine giriş bilgilerinin güvenliği, saklanması, 3. kişiler tarafından kullanılması ve benzeri husus-

lardaki tüm ihmal ve kusurlarından dolayı kendilerinin ve/veya 3. kişilerin uğradığı veya uğrayabileceği zararlar nedeniyle …….. doğrudan veya dolaylı herhangi bir sorumluluğu bulunmamaktadır"[49].

Türk hukukunda yer alan genel işlem koşullarına ilişkin hükümlerin benzeri Avrupa Birliği komisyon raporlarında da yer almaktadır[50]. Bu raporlarda sorumsuzluk anlaşmalarının genel işlem şartı niteliğinde olduğu belirtilmiştir. Dolayısıyla sorumsuzluk anlaşması hükümleri ve genel hükümler çerçevesinde içerik, yorumlama ve yürürlük denetimine tabi tutulmaktadır. Örneğin mücbir sebep, düzenli aralıklarla yedekleme yapmama, mahremiyeti güçlendirmeye dönük altyapı yatırımları yapmama gibi hizmet sağlayıcı tarafından kusur sorumluluğu kapsamında değerlendirilmeyecek durumlarda sorumsuzluk anlaşmalarının geçerli olabilmesi için bulut hizmet faydalanıcısının sözleşme kurulmadan önce bu hususta açıkça bilgilendirilmiş olması, içeriğini okuma ve öğrenme imkânı tanınmış olması ve kabulü yönünde rızasının olması gerekmektedir[51].

G. Gizlilik Sözleşmesinin Sona Ermesi

Gizlilik sözleşmeleri kural olarak sürenin dolması ile sona erer. Bun durum belirli süreli gizlilik sözleşmeleri için geçerlidir. Belirsiz süreli gizlilik sözleşmeleri ise bulut bilişim servis sunucusu ile faydalanıcısı arasındaki sözleşme ilişkisi devam ettiği sürece geçerliliğini korur. Gizlilik sözleşmesi asıl borç ilişkisi başlamadan önce de akdedilebilir. Bu durumda asıl borç ilişkisinin başlamasıyla birlikte mevcut gizlilik sözleşmesinin yerine yeni bir sözleşmenin yapılması veya mevcut sözleşmenin yeni koşullara göre yenilenmesi mümkündür. Asıl borç ilişkisini düzenleyen ana bulut bilişim sözleşmesi kapsamında düzenlenen gizlilik sözleşmelerinde asıl borç ilişkisini düzenleyen sözleşmenin sona ermesi ile gizlilik sözleşmesinin geçerlilik süresi de dolacaktır. Gizlilik sözleşmesinin sona ermesi

---

49 Gizlilik Sözleşmesinde Sorumsuzluk Antlaşması için bkz. Geminilab, "Hizmet ve Gizlilik Sözleşmesi" https://geminilab.co/tr/hizmet-ve-gizlilik-sozlesmesi (Erişim Tarihi: 07.02.2023)

50 EUCommission, ComparativeStudy on cloudcomputingcontractsfinal report,https://doi.org/10.2838/16333 (Erişim Tarihi: 13.02. 2023)

51 **SCHÖTTLER**, Ingo/**DIEKMANN**, Christian: TypischeHaftungsklauseln in IT-AGB, ITRB 2012, Heft 4, s. 86; **BORGES**/**MEENTS**, s. 165.

gizli bilgiyi ifşa etmeme yükümlülüğü altında olan tarafın ifa yükümlülüğünü her zaman için tam olarak ortadan kaldırmayabilir. Bu nedenle bazı durumlarda taraflar arasında akdedilen gizlilik sözleşmesinin süresi dolsa da tarafların gizli bilgiyi paylaşmama yükümlülüğü belli bir süreliğine veya belirsiz süreli devam eder. Bu durum sözleşmede taraf iradelerine bağlı olarak değişkenlik gösterebilir. Bu noktada bulut bilişimin mimarisine bağlı olarak kullanıcıların görevlerinin niteliği önem arz eder. Örneğin, kamuya ilişkin gizli bilgilere erişimi olan bir devlet görevlisinin gizli bilgileri ifşa etmeme yükümlülüğü, belirsiz süreli olarak devam eder. Fakat bulut servis sunucusu ve hizmet yararlanıcısının özel işletme veya gerecek kişi olduğu durumda genel olarak özel kanunlarca belirlenmiş süreler kullanılır. Örneğin, gizlilik sözleşmesinde yer alacak bir hükümle işçinin iş ilişkisinin sona ermesi akabinde gizlilik özelliğine sahip belge veya bilgileri işçinin hem kendi çıkarları doğrultusunda kullanması hem de 3. kişilerle paylaşması yasaklanabilir[52]. Bununla birlikte, gizli bilgiye erişimle yetkilendirilen kişilerin görevlerinin sona ermesi durumunda gizli bilgi içeren tüm belgeler ve konuya yönelik bütün malzemeleri gizli bilgi sahibine teslim edilmesi gizli bilgiye erişimle yetkilendirilen kişinin borçları arasında yer alır[53].

Gizlilik sözleşmesi asıl bulut bilişim sözleşmesinin esaslı unsurları[54] arasında yer aldığından gizlilik sözleşmesinde yer alan hükümlere uyulmaması asıl sözleşme ilişkisinin tamamen ortadan kalkmasına sebep olabilir. Bulut bilişimde gizlilik sözleşmesi yürürlük tarihinde ve sonrasında eklenen bütün gizli bilgileri kapsar. Sözleşmede veri ifşasının zorunlu olduğu durumlara ilişkin hükümlere de yer verilmelidir. Zira bu tür bir durumun varlığında gizliliğin ifşasından bahsedilemez. Örneğin gizli veriyi ifşa etmemekle yükümlenen taraf üzerinde yargı yetkisine sahip devlet kurumlarının emirlerine veya diğer yasal olarak bağlayıcı talimatlarına

---

52 **KAYASOYLU**,Damla: Haksız Rekabet Hükümlerine Göre Üretim ve İş Sırlarının Korunması, 1. Baskı, Seçkin Yay., İstanbul 2020, s. 76;

53 **USLUEL**, Aslı E.: Anonim Şirketlerde Ticari Sırrın Korunması, Vedat Kitapçılık, İstanbul 2009, s. 151.

54 **SPLITTGERBER/ROCKSTROH**, s. 2182.

uymak için gerekli olduğu veya yasaların gerektirdiği şekilde gizli bilgileri ifşa edebilir[55]. Bu durumun varlığında gizlilik sözleşmesinin ihlaline bağlı olarak asıl hizmet sözleşmesinin tek taraflı feshi haklı bir neden teşkil etmeyecektir.

"Bu Sözleşme, İfşa Eden Tarafça yürürlük tarihinde ve sonrasında ifşa edilecek gizli bilgileri kapsar. Bu Sözleşme, (i) Taraflar veya bağlı kuruluşları arasında belirtilen amaçla ilgili tüm yazılı sözleşmelerin feshi veya(ii) herhangi bir anlaşma yapılmaması halinde, taraflar veya bağlı kuruluşları arasında belirlenen amaç ile ilgili tartışmaların sona erdirilmesi veya bu sözleşmeyi sona erdiren yazılı bildirimin teslimi, ancak (a) her bir tarafın diğer tarafın gizli bilgileri ile ilgili yükümlülükleri feshedildikten sonra üç (3) yıl boyunca geçerliliğini koruyacak ve (b) 6, 9, 10 ve 11. Bölümler süresiz olarak geçerliliğini koruyacaktır"[56].

Gizlilik sözleşmesinin sona ermesi asıl sözleşme ilişkisinin ortadan kalkması ile mümkündür. Bazı hükümlerin gizli bilginin sağlanmasını isteyen taraf açısından sahip olduğu yüksek önemi nedeniyle belirli süreli veya süresiz olarak gizli tutulması zorunlu kılınabilir.

SONUÇ

Bulut bilişimde gizlilik sözleşmesi önemlidir. Siber dünyaya angaje olmuş her gizli veri 3. kişilerle paylaşılma riskli ile karşı karşıyadır. Bu nedenle, veri paylaşımının yapıldığı borç ilişkisi sayısı kadar gizlilik sözleşmesinin de sayıca yapılması gerekir. Gizlilik sözleşmesinde asıl amaç veri gizliliğinin sağlanmasıdır. Bu nedenle başta bulut servis sağlayıcısı olmak üzere sözleşmenin her iki tarafı verilerinin gizliliğini korumalı ve gerektiğinde şifrelenmelidir. Gizliliğin sağlanması, veri erişim kontrolü ile mümkün olabilir. Bir başka deyişle bulut hizmet sağlayıcısı, hizmet faydalanıcısına ait verilere erişimi sadece yetkilendirilmiş kişilere vermeyi taahhüt etmelidir. Hiçbir veri sürekli olarak kullanılmaz. Veriler belirli bir süre boyunca hizmet sağlayıcı tarafından saklanmalı ve belirli bir zaman dilimi sonunda veriler silinmelidir. Veri güvenliği her ne kadar bulut hizmet sağlayıcısı tarafından birincil olarak sağlanması gereken bir

---

55 https://www.buyingfor.vic.gov.au (Erişim Tarihi: 13.02. 2023)

56 https://www.buyingfor.vic.gov.au (Erişim Tarihi: 13.02. 2023)

önlem olsa da faydalanıcıların da sorumluluk bağlamında hareket etmesi önemlidir.

Gizlilik sözleşmeleri için kanunda belirtilen bir şekil şartı söz konusu değildir. Ancak, adi yazılı şekilde yapılması ispat kolaylığı bakımından her iki taraf açısından bir avantaj sağlayacaktır. Taraflar isterlerse nitelikli yazılı şekle çevirebilirler. Gizlilik sözleşmesi tek taraflı olabilir ancak ivazlı olması her zaman için gizliliğin sağlanması açısından daha yararlı sonuçlar doğurur. İfanın sağlanması her iki taraf açısından eşit düzeyde olmayabilir. Ancak gizlilik sözleşmesinde yer alan taraf yükümlülüklerinin sözleşmeye uygun yerine getirilmesini sağlamak için gizlilik ihlalinin bir yaptırıma bağlanması caydırıcılık açısından kayda değer sonuçlar üretebilir. Bu yaptırımlar gizlilik sözleşmesinin ihlali durumunda faydalanıcının hizmet sağlayıcıya tazminat talebinde bulunması olabileceği gibi sözleşmenin feshedilmesi ile yasal işlem başlatılması da olabilir. Burada belirleyici unsur kuşkusuz taraf iradeleridir.

Bulut bilişim asıl sözleşmelerinde bir başka sözleşme olarak gizlilik sözleşmesinin yapılması zorunlu değildir. Uygulamada ayrı bir sözleşme şeklinde gizlilik sözleşmesi akdedilmese bile asıl sözleşme içeriğine gizliliği sağlayıcı hükümlerin eklendiği çokça görülmektedir. Ancak bu yeterli değildir. Gizlilik sözleşmesinin ayrı yapılması gizli bilginin ifşası durumunda öngörülmeyen zararların ortaya çıkmasına neden olabilir. Bu nedenle gizlilik sözleşmesi taraflar arasında yapılmalı ve gizlilik sözleşmesi hazırlanırken gizliliği teminat altına alacak tüm önlemler de alınmalıdır.

KAYNAKLAR

Alibaba Cloud, "What Is SaaS?", https://www.alibabacloud.com/tr/knowledge/what-is-saas (Erişim Tarihi: 07.01.2023).

Amazon, "Bulut Bilişim Nedir?", https://aws.amazon.com/tr/what-is-cloud-computing/?nc2=h_ql_le_int_cc# (Erişim Tarihi: 30.12.2022).

Amazon, "Hizmet Olarak Altyapı (IaaS) nedir?", https://aws.amazon.com/tr/what-is/iaas/ (Erişim Tarihi: 05.01.2023).

Amazon, "Clarifying Lawful Overseas Use of Data (Verilerin Denizaşırı Ülkelerde Kullanım Şeklinin Netleştirilmesi – CLOUD) Yasası", https://aws.amazon.com/tr/compliance/cloud-act/ (Erişim Tarihi: 16.01.2023).

Amazon, "Mutual Non-Disclosure Agreement", https://s3.amazonaws.com/cdn.prpl.rs/docs/PRPL-NDA.pdf (Erişim Tarihi: 07.02.2023)

Aws, "Aws Müşteri Sözleşmesi", https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_Turkish_Translation.pdf (Erişim Tari-hi: 02.02.2023).

BADGER, Lee/GRACE, Tim/PATT-CORNER, Robert/ VOAS, Jeff: "Cloud Com-puting Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology". (Special Publication No 800-146, National Institute of Standards and Technology: United States Department of Commerce, May 2011) 2-1.

BAĞRIAÇIK, Safiye Nur: Üretim ve İş Sırlarının Korunması (Özellikle Haksız Rekabet Hukuku Açısından), On İki levha Yay., 1.Baskı, İstanbul 2017.

Berkeley Law, "Startup Law Initiative", https://www.law.berkeley.edu/experiential/pro-bono-program/slps/current-slps-projects/startup-law-initiative/ (Erişim Tarihi: 15.01.2023)

BİLGE, Mehmet Emin: Ticari Sırların Korunması, Asil Yayınları, 2. Baskı, Ankara 2005.

BENNETT, Louise: "Reflections on privacy, identityandconsent in on-lineservices", Information Security Technical Report, C. 14, S. 3, 2009, s. 119- 123.

BORGES, George/MEENTS, Jan Geert: Cloud Computing Rechtshandbuch, München 2016.

CAVE, Jonathan/ROBINSON, Neil/KOBZAR, Svitlana/SCHINDLER, Helen Rebecca: Regulatingthe Cloud: More, Lessor Different Regulation and Compe-ting Agendas, https://ssrn.com/abstract=2031695 (Erişim Tarihi: 01.01.2023).

CHARLES, Fried: "Privacy", Yale LawJournal, C. 77, 1968, s. 475–493.

DONAY, Süheyl: Meslek Sırrının Açıklanması Suçu, Sulhi Garan Matbaası, İstanbul 1978.

EREN, Fikret: Borçlar Hukuku Genel Hükümler, Yetkin Yayınları, Ankara 2012.

ERTAUL, Levent/ SİNGHAL, Saurabh/ GÖKAY, Saldamli: "Security challenges in Cloud Computing, Thesis", California StateUniversity, EastBay, vol. 2, no. 06, 2009, s. 625–626, https://aws.amazon.com/tr/about-aws/whats-new/2009/08/26/introducing-amazon-virtual-private-cloud/ (Erişim Tarihi: 30.12.2022).

EveryNDA, "Choice of law and jurisdiction in NDAs", https://www.everynda.com/blog/choice-law-jurisdiction-nda/ (Erişim Tarihi: 30.01.2023)

EUCommission, ComparativeStudy on cloudcomputingcontractsfinal report,https://doi.org/10.2838/16333 (Erişim Tarihi: 13.02. 2023)

Geminilab, "Hizmet ve Gizlilik Sözleşmesi" https://geminilab.co/tr/hizmet-ve-gizlilik-sozlesmesi (Erişim Tarihi: 07.02.2023)

GEZDER, Ümit: Tüketici Kredisi Sözleşmeleri, İstanbul 1998.

HAVUTÇU, Ayşe: Açık İçerik Denetimi Yoluyla Tüketicinin Genel İşlem Şartlarına Karşı Korunması, İzmir 2003.

HILBER, Marc: Handbuch Cloud Computing, Köln, 2014.

İndeed, "9 Types of Cloud Computing (With Definition and Tips)", https://www.indeed.com/career-advice/career-development/what-is-cloud-computing (Erişim Tarihi: 02.01.2023).

İbm, "What is cloud computing?", https://www.ibm.com/cloud/learn/cloud-computing (Erişim Tarihi: 02.01.2023)

İbm "What is PaaS?", https://www.ibm.com/cloud/learn/paas (Erişim Tarihi: 06.01.2023)

KAYASOYLU,Damla: Haksız Rekabet Hükümlerine Göre Üretim ve İş Sırları-nın Korunması, 1. Baskı, Seçkin Yay., İstanbul 2020.

KOWALSKİ, Stanley P./KRATTİGER, Anatole: Intellectual Property Manage-ment in Health and Agricultural Innovation a handbook of best practices, Volu-me 2, California, 2007.

PETER, Mell/TİMOTHY, Grance: "The NIST Definition of Cloud Computing", NIST, 2011, s. 1-7, https://www.ibm.com/cloud/learn/cloud-computing (Erişim Tarihi: 02.01.2023).

MILLARD, Christopher: Cloud Computing Law, Croydon, 2013.

Microsoft, "Microsoft Çevrimiçi Üyelik Sözleşmesi – ABD Kamu Bulut", https://azure.microsoft.com/tr-tr/support/legal/subscription-agreement/government/ (Erişim Tarihi: 01.02.2023)

OĞUZMAN, M. Kemal/ ÖZ, M. Turgut: Borçlar Hukuku Genel Hükümler, Cilt-I, Vedat Kitapçılık, İstanbul 2012.

SAATCIOĞLU, Onur Can: Kanunlar İhtilâfı Hukukunda Ticari Sırların İhlali, Yetkin Yay., 1. Baskı, Ankara 2020.

SÄCKER, Franz Jürgen/RIXECKER, Roland/OETKER, Hartmut/LIMPERG, Bet-tina: MünchenerKommentar zum BGB 7. Auflage 2018, Band 12, Rn. 11; https://beckonline.beck.de/?vpath=bibdata/komm/MuekoBGB/cont/MuekoBGB%2Ehtm (Erişim Tarihi: 05.02.2023)

SCHÖTTLER, Ingo/DIEKMANN, Christian: Typische Haftungsklauseln in IT-AGB, ITRB 2012, Heft 4.

SPLITTGERBER, Andreas/ROCKSTROH, Sebastian: Sicherdurchdie Cloud navigieren – Vertragsgestaltungbeim Cloud Computing, BB 2011, Heft 36.

SIAS, Suzanne L: "Confidentiality and Nondisclosure Agreements", Buisness Law, Vol. iv., 2008, s. 3-4.

ŞENBAŞ, Pınar: Bilgi Teknolojileri Dış Kaynak Alımında (Outsourcing) Kişisel Verilerin Korunması ve Gizlilik Sözleşmeleri, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2013.

TANDOĞAN, Haluk: Borçlar Hukuku Özel Borç İlişkileri Cilt I/1, İstanbul 2008.

TUNÇ, Aybike: Bulut Bilişim Sözleşmelerinin Hukuki Yapısı, Yayımlanmış Doktora Tezi, Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, Ankara, 2020.

USLUEL, Aslı E.: Anonim Şirketlerde Ticari Sırrın Korunması, Vedat Kitapçılık, İstanbul 2009.

YILMAZ, Latif: "Kayıp Kamusallığın İzinde: Mahremiyet, Gizlilik ve Kamusallık Üzerine", https://birikimdergisi.com/guncel/10472/kayip-kamusalligin-Izinde-mahremiyet-gizlilik-ve-kamusallik-uzerine (Erişim Tarihi: 10.01.2023).

YÜKSEL, Armağan/BOZKURT, Ebru: "Ticari Sırların Dijital Ortamda Korunması", TAAD, C. 9. S.33, 2018, s. 143-192.

YÜKSEL, Mehmet: "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", Ankara Üniversitesi SBF Dergisi, C. 58, S. 1, 2003, s. 182-213.

https://www.buyingfor.vic.gov.au (Erişim Tarihi: 13.02. 2023)