TİCARİ SIRLARIN DİJİTAL ORTAMDA KORUNMASI

Protecting Trade Secrets In Digital Media

Yrd. Doç. Dr. Armağan Ebru BOZKURT YÜKSEL*

Geliş Tarihi: 16.06.2017 Kabul Tarihi: 29.09.2017

ÖZET

Ticari sırların saklanmasında son dönemde teknolojinin getirdiği olanaklardan yararlanılmaktadır. Teknoloji ticari sır niteliğindeki bilgilerin saklanmasında pek çok kolaylık sağlamaktadır. Bununla birlikte ekonomik değere sahip bu bilgilerin üçüncü kişilerce ele geçirilmesi yine teknolojinin sağladığı imkânlar yüzünden daha kolay hale gelmektedir. Tacir ticari sırlarını ister kendi işletmesindeki veri merkezinde (bilgisayar sistemlerinde) ister bulutta saklasın teknik ve hukuki bazı önlemleri almak zorundadır. Türk Ticaret Kanunu'nun 18(2). maddesi gereğince her tacirin, ticari faaliyetlerinde basiretli bir işadamı gibi davranma yükümlülüğü bulunmaktadır. Bu düzenleme de tacirin ticari sırlarının korunması için önlemler almasını gerektirmektedir. Şirket yöneticilerinin de ticari sırların korunmasında özenli davranması gerekmektedir. Ticari sırların dijital ortamda saklanması haksız rekabet hukukunu da ilgilendiren bir konudur.

Anahtar Kelimeler: Ticari Sır, Haksız Rekabet, Veri Koruma, Bulut Bilişim, Veri Güvenliği

ABSTRACT

Technology has been used for storing trade secrets recently. Technology provides many convenience for storing information qualified as trade secret. However it is also getting easier for the third parties to get to these economically valuable information due to the possibilities of the same technology. Whether the merchant stores his/her trade secrets in the datacenter (computer systems) of his/her business or in cloud, he/she must take some technical and legal measures. According to article 18(2) of Turkish Commercial Code all the merchants has the obligation of acting as a prudent businessman in his/her commercial activities. This regulation also requires merchants to take measures to protect his/her trade secrets. Company executives also need to be careful about protecting trade secrets. The storage of trade secrets in digital media is also an issue of unfair competition law.

Keywords: Trade Secret, Unfair Competition, Data Protection, Cloud Computing, Data Security .

GİRİŞ

Teknolojinin gelişmesiyle birlikte işletmelerde ticari sır niteliğindeki bilgiler artık kâğıtlardan oluşan arşivler yerine bilgisayarlarda veya diğer dijital depolama aygıtlarında (USB, DVD, harici hard disk vb.) ya da bulutta[1] saklanmaya

* Dokuz Eylül Üniversitesi, İİBF, Ticaret Hukuku ABD Öğretim Üyesi, armagan.bozkurt@deu.edu.tr, http://debis.deu.edu.tr/akademiktr/index.php?cat=3&akod=20014460.

1 Bulut; donanım, ağ, depolama ve bilişim hizmetine ulaşabilmek için arayüzlerden oluşan bir kümeyi ifade etmektedir. Bulut bilişim ise bir ağ üzerinden tipik olarak İnternet üzerinden

başlanmıştır. Ticari sırların saklanmasında teknolojiden yararlanılması veri depolama için ayrılan yerin azalması nedeniyle geleneksel kâğıt arşiv yerine daha ekonomik bir yöntemdir. Ayrıca teknolojiden yararlanılması bu bilgilere erişim kolaylığı sağlamaktadır. Bununla birlikte ticari sırların dijital ortama taşınması bunların üçüncü kişilerce ele geçirilmesini de kolaylaştırmıştır. Artık ticari sırlar fiziksel olarak işletmenin bulunduğu yere girmeye gerek kalmaksızın işletmenin bilgisayarlarına ya da kullanılan buluta erişilerek ele geçirilmeye çalışılmaktadır[2].

Uygulamada özellikle ticari sır sahibi şirketler tarafından yetkili otoritelere ticari sırlara yönelik saldırılara ilişkin durum rapor edilmemektedir. Çünkü şirketler, mevcut durum üzerindeki kontrolü kaybetmek istememektedir. Şirketlerin, hukuk davasının sonucunun ceza davasını beklemesi ve ceza yargılaması sürecinde ticari sırların ortaya çıkmasından endişelendikleri görülmektedir. Özellikle halka açık şirketler ticari sırların bilgi sistemine yönelik saldırı neticesinde ele geçirildiğinin duyulması üzerine borsada hisse senedi fiyatlarının düşmesinden endişe etmektedir[3]. Nitekim ticari sırların ele geçirilmesi ülkemizde de en sık rastlanılan adli bilişim fiilleri arasında yer almaktadır[4].

Ticari sırların ele geçirilmesinin ceza hukuku yönünden incelenmesi ayrı bir çalışma konusu olabilir. Ancak burada konunun cezai yönü[5] ele alınmayacaktır. Konunun bir diğer boyutu da ekonomik casusluktur *(cyber espionage)*. Devletlerin şirketlerin veri merkezlerinden siber saldırılar vasıtasıyla şirketler için büyük mali değeri olan ticari sırları ele geçirmesi söz konusu olabilmektedir[6].

---

bilişim kaynaklarının sağlanması hizmetidir. Kullanıcılar bilişim teknolojilerini kendileri satın almak yerine bulut bilişim sayesinde bunları üçüncü kişilerden temin etmektedirler. Bulut bilişim konusunda teknik ve hukuki geniş açıklama için bkz. **BOZKURT YÜKSEL, Armağan Ebru**, Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing), Yetkin Yayınları, Ankara 2016, s.21-23, ve dn.1-15'te anılanlar.

2 **GRUNFELD, Gay/FISCHER**, **Aaron,** "How Businesses Protect Their Valuable Trade Secrets", San Francisco Daily Journal, Monday, September 26, 2011, www.dailyjournal.com (Erişim 29.07.2016).

3 **ROWE, Elizabeth A.**, "RATs, TRAPs, and Trade Secrets", 57 B.C.L. Review, Y.2016, s.389.

4 En sık rastlanan adli bilişim fiilleri şu şekilde sayılmaktadır: *"Ticari sırların çalınması, çalışanların suiistimalleri, İnternet üzerinden uzaktan ağa sızma girişimleri, kredi kartı sahtekârlıkları, bankaların İnternet şubelerine sızarak kullanıcı hesaplarındaki paraların çalınması, eşlerin İnternet üzerinden birbirlerini aldatmaları, İnternet ve telefon yoluyla hakaret ve taciz olayları, çocuk pornografisi".* **YURDAKUL, Çiğdem,** "Türkiye'de Adli Bilişim Uzmanlığı/Gereksinimleri/Kriterler/Kimler Olmalı", Adli Bilişim Dergisi, Sayı 3, Nisan 2016, s.12.

5 Bilişim suçlarıyla ilgili ayrıntılı bilgi için bkz. **DÜLGER, Murat Volkan,** Bilişim Suçları ve İnternet İletişim Hukuku, 6.B., Seçkin Yayınevi.

6 **ROWE,** RATs, s.381-382; Amerikan hukukunda ticari sırların çalınması ve ekonomik casusluk ile ilgili hazırlanan kanunda elektronik ortamda depolanmış olan ticari sırların ele

Ekonomik casusluğun tanımı ticari sırların yabancı bir devlet yararına çalınması şeklinde yapılmaktadır[7]. Örneğin, hem özel sektörde hem de kamu sektöründe Amerika Birleşik Devletleri'nde ekonomik casusluk nedeniyle milyonlarca dolar kayıp yaşanmaktadır[8]. Yine ekonomik casusluk konusunda Almanya'da şirketler arasında yapılan bir araştırmada katılımcıların yarısının en az bir kez casusluğa, sabotaja ya da veri hırsızlığına maruz kaldığı belirlenmiştir. Ekonomik casusluğa en çok maruz kalan şirketlerin başında otomotiv sektöründeki şirketlerin geldiği, onu kimya ve ilaç şirketleri ile finans ve sigorta şirketlerinin takip ettiği belirlenmiştir. Ekonomik casusluk için şirket binalarına, bürolarına, laboratuarlarına ya da araştırma merkezlerine girmeye gerek kalmamıştır. Zira günümüzde teknolojik yöntemlerle her yerden şirketlerin bilgi işlem sistemlerine girilmesi mümkündür. Şirketlerin çalışanlarının da şirkete ait verileri kopyalayarak dışarıdaki rakiplere sızdırması söz konusu olabilmektedir. Ekonomik casuslukta hedeflenen sadece şirketlere ait ticari sırların, know how'ın ya da fikri mülkiyet konusu bilgilerin ele geçirilmesi değildir, ihalelerde izlenecek stratejiye ilişkin bilgiler de hedeflenmektedir[9]. Şirketlerin genellikle bu konuda yeterince dikkatli ve bilinçli olmadıkları, hatta ekonomik casusluk mağduru olduklarını ve tam olarak ne kadar zarara uğradıklarını bile belirleyemedikleri görülmektedir[10]. Bu konu ticari sırlarla ilgili ve son dönemde gündemde olan bir konu olmakla birlikte devletler genel hukukunu ilgilendirdiğinden yine bu çalışmanın konusu dışında kalmaktadır.

Bu çalışmada öncelikle ticari sır kavramı genel olarak açıklanmıştır. Daha sonra işletmelerin kendi veri merkezlerinde ve bulutta ticari sırları saklaması durumunda dikkat edilmesi gereken teknik ve hukuki hususlara değinilmiştir. Çalışmada ayrıca ticari sırların bulutta saklanması durumunda bulut bilişim sözleşmelerinde dikkat edilmesi gereken hususlar incelenmiştir.

---

geçirilmesinin cezaları düzenlenmiştir. Kanun uyarınca yabancı bir kuruluş yararına ticari sırların çalınması ekonomik casusluk *(economic espionage)*, maddi kazanç elde etmek için yapılan hırsızlık ise ticari sır hırsızlığı *(theft of trade secrets)* olarak adlandırılmaktadır. **DOYLE, Charles**, "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act", Congressional Research Service, August 19, 2016, s.1, https://www.fas.org/sgp/crs/secrecy/R42681.pdf (Erişim 27.09.2016).

7 **FBI,** "Economic Espionage", Inside the FBI, https://www.fbi.gov/audio-repository/news-podcasts-inside-economic-espionage.mp3/view, Yayınlanma Tarihi 23.06.2015 (Erişim 21.10.2016).

8 **MARIN, Mauricio**, "Economic Espionage Threat Rising in America", http://www.lasvegasnow.com/news/economic-espionage-threat-rising-in-america (Erişim 21.10.2016).

9 **HEIN, Matthias**, "Ekonomi Casusluğu Yayılıyor", Deutsche Welle Türkçe, http://www.dw.com/tr/ekonomi-casuslu%C4%9Fu-yay%C4%B1l%C4%B1yor/a-18452902, Yayınlanma Tarihi 15.05.2015 (Erişim 21.10.2016).

10 **ROWE,** RATs, s.386.

I.TİCARİ SIR KAVRAMI

A. Türk Hukukundaki Düzenlemeler

Sır, Türk Dil Kurumu'nun sözlüğünde *"varlığı veya bazı yönleri açığa vurulmak istenmeyen, gizli kalan, gizli tutulan şey*" olarak tanımlanmaktadır[11]. Ticari sırrın tanımı için mevzuata baktığımızda değişik düzenlenmeler görülmektedir.

4982 sayılı Bilgi Edinme Kanunu'nun 23. maddesinde ticari sır *"Kanunlarda ticari sır olarak nitelenen bilgi veya belgeler ile kurum ve kuruluşlar tarafından gerçek veya tüzel kişilerden gizli kalması kaydıyla sağlanan ticari ve mali bilgiler"* şeklinde tanımlanmaktadır[12].

Türk Ceza Kanunu'nun "ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması" kenar başlıklı 239. maddesinde ise *"Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya m*üşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikâyet üzerine, bir yıldan üç yıla kadar hapis ve beş *bin güne kadar adlî para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi hâlinde de bu fıkraya göre cezaya hükmolunur."* hükmü yer almaktadır[13].

4054 sayılı Rekabetin Korunması Hakkında Kanun'da ticari sırrın tanımı yapılmamakla birlikte 25. maddede*"Kurul üyeleri ve personeli Kurumla ilgili gizlilik taşıyan bilgileri ve bu Kanunun uygulanması sırasında öğrendikleri teşebbüs ve teşebbüs birliklerinin ticari sırlarını görevlerinden ayrılmış olsalar bile ifşa edemezler, kendilerinin veya başkalarının menfaatine kullanamazlar"* hükmü yer almaktadır[14].

5411 sayılı Bankacılık Kanunu'nun "sırların saklanması" kenar başlıklı 73. maddesi şu şekildedir: *"Kurul başkan ve üyeleri ile Kurum personeli, Fon Kurulu başkan ve üyeleri ile Fon personeli görevleri sırasında öğrendikleri bankalara ve bunların bağlı ortaklık, iştirak, birlikte kontrol edilen ortaklıkları ve m*üşterilerine ait sırları bu Kanuna ve özel kanunlarına göre yetkili olanlardan başkasına açıklayamaz ve kendilerinin veya başkalarının yararlarına

---

11 http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.56b0d6fd7f16b1.70263308 (Erişim 02.02.2016).

12 RG., T.24.10.2003, S.25269.

13 TCK madde 239'da düzenlenen bu suç hakkında geniş açıklama için bkz. **TEKŞEN, Mustafa Gökhan**, Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu, Yetkin Yayınları, Ankara 2012.

14 RG., T.13.12.1994, S.22140.

kullanamazlar."[15]

Ticari Sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısının 2. maddesinde ticari sırrın tanımı *"bir ticari işletme veya şirketin faaliyet alanı ile ilgili yalnızca belirli sayıdaki mensupları ve diğer görevlileri tarafından bilinen, elde edilebilen, özellikle rakipleri tarafından öğrenilmesi halinde zarar görme ihtimali bulunan ve* üçüncü *kişilere ve kamuya açıklanmaması gereken, işletme ve şirketlerin ekonomik hayattaki başarı ve verimliliği için b*üyük *önemi bulunan, iç kuruluş yapısı ve organizasyonu, mali, iktisadi, kredi ve nakit durumu, araştırma ve geliştirme çalışmaları, faaliyet stratejisi, hammadde kaynakları, imalatının teknik özellikleri, fiyatlandırma politikaları, pazarlama taktikleri ve masrafları, pazar payları, toptancı ve perakendeci müşteri potansiyeli ve ağları, izne tabi veya tabi olmayan sözleşme bağlantılarına ilişkin veya bu gibi bilgi veya belgeler"* şeklindedir[16].

Türk Ticaret Kanunu'nun 55(1). maddesinde başlıca haksız rekabet hâlleri sayılmıştır. Bununla birlikte buradaki sayım sınırlayıcı değildir[17]. Bunlardan (b) bendinde yer alan 3 numaralı cümle şu şekildedir: *"*İşçileri, vekilleri veya diğer yardımcı kişileri, işverenlerinin veya *müvekkillerinin üretim ve iş sırlarını ifşa etmeye veya ele geçirmeye yöneltmek"* haksız rekabet teşkil edecektir. (c) bendinde başkalarının iş ürünlerinden yetkisiz yararlanmanın haksız rekabet teşkil edeceği belirtilmiş ve özellikle *"1. Kendisine emanet edilmiş teklif, hesap veya plan gibi bir iş* ürününden *yetkisiz yararlanmak, 2.* Üçüncü *kişilere ait teklif, hesap veya plan gibi bir iş* ürününden, *bunların kendisine yetkisiz olarak tevdi edilmiş veya sağlanmış olduğunun bilinmesi gerektiği hâlde, yararlanmak, 3. Kendisinin uygun bir katkısı olmaksızın başkasına ait pazarlanmaya hazır çalışma* ürünlerini *teknik çoğaltma yöntemleriyle devralıp onlardan yararlanmak"* haksız rekabet teşkil eden davranış olarak sayılmıştır. (d) bendinde ise *"*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"* hükmü yer almaktadır.

5809 sayılı Elektronik Haberleşme Kanunu'nda ticari sır ile ilgili düzenlemelerden bir tanesi 6(h) maddesinde yer almaktadır. Buna göre, *"işletmecilerin ticari sırları ile kamuoyuna açıklanabilecek bilgilerinin kapsamını belirlemek, işletmecilerin ticari sırları ile yatırım ve iş planlarının gizliliğini korumak ve bunları adli makamların talepleri dışında muhafaza etmek"* Bilgi Teknolojileri ve İletişimin Kurumu'nun görev ve yetkileri arasındadır. Kanun'un

---

15 RG., T.01.11.2005, S.25983 (Mükerrer).

16 Tasarıda ayrıca banka sırrı ve müşteri sırrının da tanımı yapılmıştır. http://www2.tbmm.gov.tr/d24/1/1-0483.pdf (Erişim 02.02.2016).

17 ŞENER, Oruç Hami, Ticari İşletme Hukuku, Seçkin Yayınevi, Ankara 2016, s.610.

18(4) maddesinde ise erişim anlaşmalarının ticari sırlar dışında aleni olduğu düzenlenmiştir[18].

B. Amerikan Hukukunda, Avrupa Birliği Hukukunda ve Milletlerarası Metinlerde Yer Alan Düzenlemeler

Amerika Birleşik Devletleri'nde Yeknesak Ticari Sırlar Kanunu'nda *(Uniform Trade Secrets Act)* ticari sır, herkes tarafından bilinmemesi, kolaylıkla bulunamaması nedeniyle ekonomik değer taşıyan, başkalarının ekonomik değerini açıklandığında veya uygulandığında anlayabildiği ve gizliliğinin devam etmesi için makul bir çabaya konu olan formül, model, derleme/liste, program, plan, yöntem, teknik veya süreci içeren bilgi şeklinde tanımlanmıştır[19](Uniform Trade Secrets Act Section 1(C)(4)).

Amerika Birleşik Devletleri'nde Yeknesak Ticari Sırlar Kanunu eyaletlerin çoğu tarafından iktibas edilmiştir. Örneğin Kaliforniya'da Medeni Kanun içinde yer alan ticari sır ile ilgili düzenleme uyarınca ticari sır, başkaları tarafından öğrenildiğinde veya kullanılması bakımından ekonomik değeri olan bir formül, metod veya bir bilgidir. Bu bilgi gizliliğinin korunması için makul bir gayret gösterilen bilgidir (Civil Code §3426.1)[20].

Avrupa Birliği hukukunda ticari sırrın üzerinde anlaşılmış bir tanımı bulunmamaktadır. Üye devletlerin milli hukuk sistemlerinde ticari sır değişik şekillerde tanımlanmakta ve düzenlenmektedir. Bununla birlikte, düzenlemelere bakıldığında ticari sır ile ilgili ortak bazı noktalar bulunmaktadır. Buna göre bir bilginin ticari sır olarak değerlendirilmesi için iş ile ilgili ticari veya teknik bir bilgi olması gerekmektedir. Bu bilginin herkes tarafından bilinmeyen veya kolaylıkla erişilemeyen ve sahibine rekabet avantajı sağlayan bir ekonomik değere sahip olması gerekmektedir. Ayrıca bu bilginin gizli tutulması için makul tedbirler alınması gerekmektedir[21].

---

18 RG., T.05.11.2008, S.5809.

19 Maddenin metni şu şekildedir: *""Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."*, http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (Erişim 02.02.2016).

20 CA Civ Code § 3426 (2016)'daki düzenleme ve geniş açıklama için bkz. **POOLEY, James H.,** "The Uniform Trade Secrets Act: California Civil Code 3426", Santa Clara High Technology Law Journal, Volume I, Issue 2, Article 3, s.196.

21 Study on Trade Secrets and Confidential Business Information in the Internal Market, Final Study, April 2013, Prepared for the European Commission, Contract Number MARKT/2011/128/D, s.5, http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (Erişim 02.02.2016).

Avrupa Birliği'nin 2016/943 sayılı Açıklanmamış Know-how ve Ticari Sırların Hukuka Aykırı Olarak Elde Edilmesine, Kullanılmasına ve Açıklanmasına Karşı Korunması Direktifi'nin *(Directive (EU) 2016/943 of The European Parliament and of The Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure)* 2. maddesinde ticari sır kavramı tanımlanmıştır.[22] Buna göre ticari sır, aşağıdaki özellikleri taşıyan bilgidir: a) söz konusu bilginin türü ile normal olarak ilgilenen kişiler arasında genellikle bilinmeyen veya bu kişilerin kolayca erişebildiği bir yapı veya bileşen olmayan, b) ticari sır olması itibarıyla ticari değeri olan, c) hukuken bilgiyi kontrolünde tutan kişi tarafından bir sır olarak kalabilmesi için makul önlemlerin alındığı bilgidir.

Direktif'te ticari sır sahibi, aynı maddenin devamında ticari sırrı hukuken kontrol eden gerçek veya tüzel kişi olarak tanımlanmıştır. Ticari sırrı ihlal eden kişi ise ticari sırrı hukuka aykırı olarak elde eden, kullanan veya açıklayan gerçek veya tüzel kişi olarak tanımlanmıştır.

Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması'nda *(The Agreement on Trade-Related Aspects of Intellectual Property Rights-TRIPS)* açıklanmamış bilgi kavramından söz edilmektedir. 39. maddenin metni şöyledir: *"1. Üyeler Paris Sözleşmesi'nin (1967) 10 uncu Maddesinde öngörüldüğü gibi haksız rekabete karşı etkin koruma sağlarlarken, açıklanmamış bilgileri 2nci paragrafa uygun olarak ve hükümetlere veya hükümet kuruluşlarına sunulmuş verileri 3ncü paragrafa uygun olarak koruyacaklardır. 2. Gerçek ve tüzel kişiler yasal olarak kendi kontrolleri altındaki bilgilerin kendi izinleri olmadan, dürüst ticari uygulamalara aykırı, başkalarına ifşa edilmesini veya başkaları tarafından elde edilmesini veya kullanılmasını engelleme olanağına sahip olacaklardır, ancak bu koşulla ki, bu tür bilgiler; (a) bir bütün olarak veya unsurlarının kesin konfigürasyonunda veya grubunda, normal olarak söz konusu türde bilgilerle uğraşan çevrelerdeki şahıslarca genelde bilinmeyen veya bu şahısların kolaylıkla elde edemeyeceği anlamda gizli olmalıdır; (b) gizli olduğu için ticari değeri olmalıdır ve (c) yasal olarak bu bilgileri kontrol eden şahıs tarafından, gizli kalması için, ilgili koşullar altında makul önlemler alınmış olmalıdır…..*[23]*"* Anlaşma metninde ticari sır yerine açıklanmamış bilgi terimi kullanılmıştır. Ancak açıklanmamış bilgi terimi ticari sır kavramı ile karşılaştırıldığında aynı unsurların arandığı görülmektedir[24].

---

[22] Direktif'in tam metni için bkz. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN (Erişim 15.05.2017).

[23] TRIPS'in Türkçe tam metni için bkz. http://teftis.kulturturizm.gov.tr/Eklenti/34660,ticaretle-baglantili-fikri-mulkiyet-anlasmasi-trips-199-.doc?0 (Erişim 15.05.2017).

[24] **BİLGE, Mehmet Emin,** Ticari Sırların Korunması, Asil Yayın Dağıtım Ltd.Şti., 2.Bası, Ankara 2005, s.15; Ernie Linek, "A Brief History of Trade Secret Law, Part 1", BioProcess International, s.2, http://bannerwitcoff.com/_docs/library/articles/briefhistory1.pdf (Erişim 03.02.2016).

C. Ticari Sırrın Tanımı

Ticari sır gizli, ticari değeri olan ve bir işletmeye rekabet gücü sağlayan, müşteri listesi, üretim metodları, pazarlama stratejileri, fiyatlandırma bilgisi ve kimyasal formül gibi bir bilgidir. Cola Cola'nın formülü, Kentucky Fried Chicken'in tarifi, Google arama motorunun algoritması ticari sırra örnek olarak sayılabilir. Ticari sır bir işletmenin en değerli gayri maddi mallarındadır[25].

Amerikan Temyiz Mahkemesi'nin bir kararında ticari sır şu şekilde tanımlanmıştır: *"ticari sır müşteri listesi, üretim usulü, bir içeceğin gizli formülü gibi bir bilgidir. Ticari sır sahibi bu bilgiyi çalışanları ile veya diğer kişilerle gizlilik anlaşması yaparak ve koruyarak, şifreleyerek ve başka usullerde gizleyerek gizli tutmaktadır. Öyle ki, ticari sırrın açığa çıkması sözleşmenin ihlali veya haksız fiil teşkil etmektedir[26]".*

Doktrinde ticari sırrın bizim de katıldığımız *BİLGE* tarafından yapılan tanımı ise şu şekildedir: ticari sır*"bağımsız ekonomik bir değeri olan veya iktisadi faaliyetlerde sahibi lehine bir rekabet avantajı sağlayan, aleni olmayan (sadece sınırlı bir çevrede bilinen) ve sahibinin gizli kalmasını istediği her türlü bilgi"*dir[27].

D. Ticari Sırrın Benzer Kavramlardan Farkı

Ticari sırrın gizli bir bilgi olması itibarıyla başka bazı kavramlara benzetilmesi söz konusu olabilir. Bunlardan bir tanesi devlet sırrıdır. Ticari sır gibi devlet sırrında da gizlilik unsuru olmasına rağmen ikisi farklıdır. Devlet Sırrı Kanunu Tasarısı'na göre devlet sırrının tanımı şu şekildedir: *"Devlet sırrı; açıklanması veya öğrenilmesi, Devletin dış ilişkilerine, milli savunmasına ve milli güvenliğine zarar verebilecek; anayasal düzeni ve dış ilişkilerinde tehlike yaratabilecek ve bu nedenlerle niteliği itibarıyla gizli kalması gereken bilgi ve belgelerdir."* Tasarı'da devlet sırrı niteliği taşımayan diğer gizli bilgi ve belgeler de düzenlenmiştir. Devlet Sırrı Kanunu Tasarısı'nın 4. maddesinde devlet sırrı

---

[25] **YEH, Brian T.,** "Protection of Trade Secrets: Overview of Current Law and Legislation", Congressional Research Service, April 22, 2016, s.II, https://www.fas.org/sgp/crs/secrecy/R43714.pdf (Erişim 23.10.2016); Ticari sır üretimle ilgili, endüstriyel ya da ticaretle ilgili bir bilgi olabilir. Bu bağlamda ticari sır kapsamına satış yöntemleri, dağıtım yöntemleri, tüketici profilleri, reklam stratejileri, tedarikçi ve müşteri listeleri, üretim usulleri dâhildir. Hangi bilginin ticari sır teşkil edeceği somut olayın özelliğine göre belirlenecektir. **WIPO,** "What is a Trade Secret?", http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm (Erişim 23.10.2016).

[26] ConFold Pac. v. Polaris Indus., 433 F.3d 952, 959 (7th Cir. 2006) (**YEH,** s.2).

[27] **BİLGE,** s.5; *"Ticari sırrın, bir ticari işletme ve şirketin faal olduğu alanla ilgili olarak belli sayıdaki mensuplarınca bilinen, rakiplerince bilinmemesi gereken ve üçüncü kişilere (kamuya) açıklanmaması gereken, işletmenin başarısı için gerekli olan bilgi"* şeklindeki tanımı ve diğer açıklamalar için bkz. **TURANBOY, Asuman,** "Ticari Sır", Prof.Dr. Tuğrul ANSAY'a Armağan, Turhan Yayınevi, Ankara 2006, s.368.

niteliği taşımayan diğer gizli bilgi ve belgeler tanımlanmıştır. Buna göre *"devlet sırrı niteliği taşımayıp da*, açıklanması veya öğrenilmesi halinde ülkenin ekonomik çıkarlarına, istihbarata, askeri hizmetlere, idari soruşturmaya ve adli soruşturma ve kovuşturmaya zarar verebilecek nitelikteki veya yetkili makamlar tarafından gizlilik derecesi verilmiş bilgi ve belgeler, gizli bilgi ve belge olarak kabul edilir." Bu itibarla ticari sır da bu gizli bilgi ve belgeler arasında sayılabilecektir[28]. Özellikle günümüzde teknolojideki gelişmeler karşısında ve ülkeler arasında teknoloji transferinin önemi düşünüldüğünde ticari sırların ele geçirilmesi ülkenin ekonomik çıkarlarına zarar verecektir.

Ticari sırdan farklı bir başka kavram da meslek sırrıdır. Kişilerin mesleklerini icra ederken öğrendikleri gizli bilgilere meslek sırrı denmektedir. Bu bilgiler iş sahibinin zamanla mesleğini icra ederken öğrendiği ve geliştirdiği gizli bilgiler olabileceği gibi, müşterilerle ilgili özel bilgiler de olabilir[29]. Bazı mesleklerdeki sırlar özel olarak düzenlenmek suretiyle koruma altına alınmıştır[30]. Örneğin, Avukatlık Kanunu'nda[31] (m.36), Tıbbi Deontoloji Tüzüğü'nde[32] (m.4), Noterlik Kanunu'nda[33] (m.54) mesleğin icrası sırasında öğrenilen sırların ifşası yasaklanmıştır. İş Kanunu'nda[34] ise işçinin, işverenin meslek sırlarını ifşa etmesi doğruluk ve bağlılığa uymayan davranış teşkil ettiğinden, işverenin iş sözleşmesini haklı nedenle feshedebileceği düzenlenmiştir (İş K.m.25/II(e)).

İş sırrı ise iş ve işyeriyle ilgili aleniyet kazanmamış ve sadece işyerinde çalışanlarca bilinen bilgidir[35]. Türk Borçlar Kanunu'nun 396/IV ve 444/I maddelerinde geçen üretim sırrı ile iş sırrı birbirinden çok uzak kavramlar değildir. Nitekim Türk Ticaret Kanunu'nun 55(1)(b)(3) maddesinde üretim ve iş sırlarından bahsedilmektedir. Her iki kavram da ticari sır altında değerlendirilebilir. Hatta hem üretim hem de iş sırrı know how kavramı ile de yakından ilgilidir[36]. İngilizce bir kelime olan know how yerine Türkçe'de teknik bilgi denilebilirse de aslında know how teknik bilgiden daha geniş bir kavramdır. Know how, sınaî alanda özellikle ticari ve ekonomik faaliyetlerde kullanılan teknik veya işletmeyle ilgili bilgi ve tecrübeleridir[37]. Bu bilgi ve

---

28 **SULU, Muhammed**, Ticari Sırların Korunması, On İki Levha Yayınları, İstanbul 2016, s.19.

29 **BİLGE,** s.34.

30 Diğer açıklamalar için bkz. **SULU,** s.20.

31 RG., T.07.04.1969, S.13168.

32 RG., T.19.02.1960, S.10436.

33 RG., T.05.02.1972, S.14090.

34 RG., T.10.06.2003, S.25134.

35 İş sırrı hakkında daha fazla bilgi için bkz. **UŞAN, Fatih**, İş Hukukunda İş Sırrının Korunması, Ankara 2003.

36 **SULU,** s.21.

37 **KIRCA, Çiğdem,** "Know-How Sözleşmesinin Hukuki Niteliği", Prof.Dr.Ali Bozer'e Armağan, Ankara 1998, s.245; **BİLGE,** s.36; **KÖSEALİOĞLU, Ebru,** "Know-How Sözleşmesinin Tanımı, Unsurları ve Patentten Farkları", Hukuk Gündemi, Yaz 2007, Sayı 8, s.135; Rekabet Kurulu'nun 2003/3 ve 2007/2 sayılı Rekabet Kurulu Tebliğleri ile Değişik, Dikey Anlaşmalara İlişkin Grup

tecrübeler genellikle gizli olmakla birlikte, böyle olması zorunlu değildir[38]. Örneğin, işletmenin yönetilmesi, ürünün üretim tarzı know how kapsamına girer[39].

Müşteri sırrı, işletmenin ticari faaliyetleri sırasında müşterileriyle ilgili öğrendiği ve gizli tutmak zorunda olduğu bilgiler şeklinde tanımlanmaktadır. Müşteri sırları özellikle müşterilerin ekonomik durumlarına ilişkindir[40]. Ticari sır, Banka Sırrı ve Müşteri Sırrı Hakkında Kanun Tasarısı'nın 2(c) maddesi uyarınca müşteri sırrı, *"ticari işletme ve şirketlerin, bankaların, sigorta şirketlerinin, sermaye piyasasında ve mali piyasalarda faaliyet gösteren aracı kurumların kendi faaliyet alanlarıyla ilgili olarak m*üşteriyle ilişkilerinde, müşterinin şahsi, iktisadi, mali, nakit ve kredi durumuna ilişkin doğrudan ve dolayısıyla edindikleri tü*m bilgi ve belgeleri"* ifade etmektedir. Görüldüğü üzere müşteri sırrı ile ticari sır aynı değildir[41].

Şirket sırrı, iş sırrından daha dar kapsamlıdır. İş sırrı genel iş ile ilişkilendirmektedir. Oysaki şirket sırrı sadece şirketin işleyişiyle, menfaatiyle ilgilidir[42].

II. TİCARİ SIRRIN UNSURLARI

Ticari sır korumasının konusunu bir bilgi oluşturmaktadır. Ticari sır kavramının tanımlanması için öncelikle ortada bir bilgi olmalıdır. Bilginin yazılı olması veya olmaması burada önem arz etmez. Bilginin fikri mülkiyet hakkı korumasından yararlanıp yararlanmaması da ticari sır olarak nitelendirilmesinde rol oynamaz. Bilginin karmaşık ya da basit olması da önemli değildir. Bilgi pozitif olabileceği

---

Muafiyeti Tebliği, Tebliğ No : 2002/2'de know how'un tanımı şu şekilde yapılmaktadır: *"Know-how: Sağlayıcının tecrübe, denemeleri sonucu elde ettiği ve patentli olmayan, uygulamaya yönelik, gizli, esaslı ve belirlenmiş bilgi paketi anlamına gelir. Bu tanımdaki; 1) "Gizli" kavramı, know-how'ın bir bütün halinde veya parçaları tam olarak biraraya getirildiğinde ve birleştirildiğinde dahi herkes tarafından bilinmemesini ya da kolaylıkla erişilebilir olmamasını, 2) "Esaslı" kavramı, know-how'ın, anlaşma konusu malların veya hizmetlerin kullanılması, satımı veya yeniden satımı bakımından alıcı için vazgeçilmez bilgiler içermesini,3) "Belirlenmiş" kavramı, know-how'ın, gizli ve esaslı olma şartlarını taşıdığını doğrulayabilmek için, yeterince geniş kapsamlı ve ayrıntılı bir şekilde tanımlanmış olmasını ifade eder."*

38 *KIRCA* know how'un unsurlarını şu şekilde sıralamaktadır: 1) teknik ve ticari alandaki bilgilerden oluşması, 2) herkesin kolaylıkla elde etmesi mümkün olmayan bilgilerden oluşması, 3) know how'u oluşturan bilgilerin patent alınarak korunmamış olması, 4) üçüncü kişilere aktarılabilir bilgiler olması. Kırca, s.245 vd.

39 **YASAMAN, Hamdi,** "Patent Hukukunda Ticari Sırların Korunması", Fikri Mülkiyet Hukuku Yıllığı 2009, XII Levha Yayınları, İstanbul 2009, s.368.

40 **BİLGE,** s.34; **SULU,** s.22.

41 **SULU,** s.22.

42 **SULU,** s.22; **USLUEL, Aslı E.**, Anonim Şirketlerde Ticari Sırrın Korunması, Vedat Kitapçılık, İstanbul 2009, s.53-54.

gibi negatif de olabilir. Örneğin belli bir usulün işe yaramadığı, başarısız olduğu yönünde bir bilgiden rakipler haberdar olurlarsa artık o yönde para ve zaman harcamayacaklardır. Bilginin fiilen kullanılması gerekmez. Potansiyel olarak kullanılabilme olanağının olması yeterlidir[43].

Bir bilginin ticari sır niteliğinde olabilmesi için ikinci unsur ticari nitelikte olmasıdır. Bir başka deyişle bilginin tacirin ticari faaliyetleri ile ticari işletmesi ile ilgili olması gerekmektedir[44].

Bilginin, ticari sır niteliğinde olabilmesi için üçüncü unsur herkese açık olmamasıdır. Eğer ticari nitelikteki bilginin sır olma özelliği ortadan kalkarsa ticari sır özelliği de kaybolacaktır[45]. Buradaki bilinmeme unsuru patent hukukundaki yenilikten (Sınaî Mülkiyet Kanunu[46] m.83(1), (2)) farklıdır. Ticari sırrın konusu patent hukuku anlamında yenilik özelliğini içeren bir buluş olabileceği gibi yenilik özelliği taşımayan, stok durumu, yatırım planları gibi başka bilgiler de olabilir[47].

Bilginin ticari nitelikte olabilmesi için aranan dördüncü unsur ise ticari sır sahibinin sır tutma iradesinin olmasıdır. Buna göre ticari sır, sahibinin normalde bilinmeyen ancak gizli kalması yönünde bir isteğinin de olmadığı olay ve bilgilerden ayrıdır[48]. Ticari sır sahibinin sır tutma iradesinde sırrın korunmasında ekonomik bir yararının olması ticari sırrın varlığına karar verilmesinde etkilidir. Sır tutma iradesi sır korumaya yönelik tedbirlerin alınmış olmasıyla görünür. Örneğin, gizlilik sözleşmelerinin yapılması, belgelerin gizlenmesi için güvenlik sistemlerinin kurulması, bilgisayarlara şifreler konması şeklinde tedbirler alınması bu kapsamda sayılabilir[49]. Herkesçe bilinen bir bilgi ticari sır niteliğinde olmadığından ticari sır sahibinin bilginin sır niteliğinin korunması hususunda davranışlarına dikkat etmesi gerekir[50]. Örneğin Amerika'da mahkemece verilen bir kararda yer aldığı üzere bir iş için gelen bir ziyaretçinin imalathanede gezdirilirken gizli bir üretim sürecini görmesi bilginin ticari sır olma niteliğini ortadan kaldıracaktır[51]. Bununla birlikte bir bilginin ticari sır

---

43 **BİLGE,** s.17-18.

44 **BİLGE,** s.18.

45 **INTERNATIONAL CHAMBER of COMMERCE,** "Trade Secrets: Tools for Innovation and Collaboration", Innovation and Intellectual Property Series", By Jennifer Brant and Sebastian Lohse, 2014, s.5.

46 RG., T.10.01.2017, S.29944.

47 **BİLGE,** s.19-21.

48 **INTERNATIONAL CHAMBER of COMMERCE,** s.5.

49 **BİLGE,** s.27-28.

50 **ROWE, Elizabeth A.**, "Saving Trade Secret Disclosures on the Internet Through Sequential Preservation", Wake Forest Law Review, Volume 42, 2007, Number 1, s.17.

51 77 Wn. App. 20, Precision Moulding v. Simpson Door, No. 33315-1-I. Division One. February 21, 1995, http://courts.mrsc.org/appellate/077wnapp/077wnapp0020.htm (Erişim 07.08.2016).

niteliğinin kaybedilmesi için herkesçe bilinmesi değil o bilgiden ekonomik yarar sağlayacak kişilerce bilinmesi yeterlidir[52].

III. TİCARİ SIRRIN SAKLANMASINDA TEKNOLOJİDEN YARARLANILMASI

Ticari sırların teknolojinin gelişmesiyle birlikte elektronik ortamda saklanması giderek daha çok tercih edilmektedir. Ticari sır niteliğindeki bilgilerin kâğıt şeklinde arşivlerde depolanması yerine işletmelerin veri merkezlerinde ya da bulutta saklandığı görülmektedir[53]. Teknoloji bu bağlamda bir yandan erişim ve saklama kolaylığı sağlamakta diğer yandan ticari sırların ele geçirilmesini veya üçüncü kişilere aktarılmasını kolaylaştırmaktadır.

A. Ticari Sırların İşletmenin Veri Merkezinde Saklanması

1. Genel Olarak

Tacir işletmesinin içinde veya işletmenin merkezinden başka bir yerde bulunan bilgisayarlarda ya da sunucularda[54] ticari sır niteliğindeki verilerini saklayabilir. İşletmenin büyüklüğüne göre daha isabetli bir şekilde ifade etmek gerekirse sahip olunan verilerin hacmine göre tek bir bilgisayarın kullanılması söz konusu olabileceği gibi bir odayı ya da bir fabrika binasını doldurabilecek kadar büyüklükte sunucular da kullanılabilir. Burada ifade etmek istediğimiz tacirin herhangi bir dış kaynaktan yardım almaksızın kendi imkânlarıyla sahip olduğu bilgisayarlarda ya da sunucularda ticari sırlarını ya da daha kapsayıcı şekilde ifade etmek gerekirse işletmeye ilişkin tüm verilerini muhafaza etmesidir.

2. İşletmenin Veri Merkezinde Ticari Sırların Saklamasında Dikkat Edilecek Hususlar

Tacirin, ticari sırlarını işletmenin veri merkezinde saklaması durumunda karşılaşabileceği çeşitli sorunlar söz konusudur. Bunlara karşı alınabilecek teknik ve hukuki önlemler vardır.

Tacirin ticari sırlarını veri merkezinde saklaması durumunda dikkat etmesi gereken hususlardan ilki çalışanlarla ilgilidir. İşletmenin veri merkezinde

---

[52] **DHULIA, Khyati**, Trade Secrets in Cloud Computing, University of Washington School of Law, Final Thesis Paper, Spring 2010, s.29.

[53] **ALMELING, David,** "Seven Reasons Why Trade Secrets Are Increasingly Important", Berkeley Technology Law Journal, Vol.27, Issue 2, Fall 2012, s.1117.

[54] Sunucu da bir bilgisayardır. Ancak kişisel bilgisayarlardan farklı olarak sunucular daha gelişmiş bilgisayarlardır ve bilgisayarın bilgisayarla iletişimi için tasarlanmıştır. Sunucular, merkezi olarak yönetilebilir, uzun ömürlüdür ve yüksek işyüküne dayanıklıdır. Kişisel bilgisayarlar ise bilgisayar insan iletişimi için tasarlanmıştır. Daha kısa ömürlüdür. Daha geniş teknik açıklama için bkz. https://www.quora.com/What-is-the-difference-between-servers-and-desktops-workstations (Erişim 12.06.2017).

saklanan ticari sırların üçüncü kişilerce öğrenilmesine çalışanların neden olabildikleri bilinmektedir. Şöyle ki, çalışanların, üçüncü kişilere ticari sırları elektronik ortamda göndermesi veya kopyaladıkları ticari sır niteliğindeki dosyaları işten ayrılmalarından sonra yanlarında götürmeleri ihtimal dâhilindedir. Çalışanların ticari sırları üçüncü kişilerle paylaşmasına bir örnek 2010 yılında General Motors Şirketi'nin hibrid motorlarla ilgili değeri milyonlarca dolarla ölçülen planları içeren bilgisayardaki 16.262 dokümanının iki çalışan tarafından kopyalanarak bir Çinli otomobil üreticisine verilmesi gösterilebilir[55]. Bir başka örnek olarak *Charles Schwab&Co. v. Carter* davasına konu olan olay gösterilebilir. Dava, satış teklifi rakibi tarafından reddedilen şirketin rakibin çalışanına maddi karşılık sağlamak suretiyle rakibin finansal yazılım modelini ele geçirmesine ilişkindir. Bu çalışanın şirketteki görevi bilgi işlem merkezi yöneticiliği olduğundan görevi nedeniyle şirkette bulunan on beş gizli bilgisayar dosyasına erişmesi mümkün olmuştur. Olayda çalışan bütün bu dosyaları elektronik posta yoluyla rakibe göndermiştir[56].

Çalışanların sosyal medyada aslında kötüniyetli olmaksızın ticari sırları arkadaşları ile paylaşması da ihtimal dâhilindedir. Tacir işletmedeki çalışanların sosyal medya kullanımıyla ilgili bir politika geliştirmeye dikkat etmelidir. Örneğin işletmede sosyal medya kullanımıyla ilgili kurallar tespit edilerek çalışanların hiçbir şekilde işletmeden ya da ticari sırlardan bahsedemeyeceği yer alabilir. Çalışanların sosyal medya hesaplarında örneğin Facebook, Twitter gibi sitelerde herhangi bir ticari sırrı paylaşmaları bu sitelere o bilgiye bağlantı *(link)* verme ya da o bilgiyi kullanabilme imkânı doğurabilir. Elbette bu sitelerin üyelik sözleşmelerindeki şartlar gereği başka haklara sahip olmaları da gündeme gelebilir. Bu itibarla çalışanların sosyal medya kullanımı konusunda eğitilmesi gerekir[57].

Günümüzün teknolojik imkânlarıyla evden çalışanların *(home office)* ya da tatilde veya işyerinden uzakta olan çalışanların bilgilere ulaşabilmesi sağlanmaktadır. Çalışanlar bu durumda ticari sır niteliğindeki dosyaları işletmedeki bilgisayarlardan kendi bilgisayarlarına aktarabilmektedirler. Başka bir ihtimal çalışanların işletmedeki bilgisayarlardan ticari sır niteliğindeki dosyaları kendilerine ait buluta aktarmaları olabilir. Burada da çalışanların

---

55 **BOND Jr., Vince,** "U.S. Judge Sentences Couple to Jail for Stealing GM Trade Secrets", Automative News, Yayınlanma tarihi 01 Mayıs 2013, http://www.autonews.com/article/20130501/OEM06/130509970/u.s.-judge-sentences-couple-to-jail-for-stealing-gm-trade-secrets (Erişim 21.10.2016).

56 Charles Schwab & Co., Inc. v. Brian D. Carter, Acorn Advisory Management, L.L.C., et al. (Internet Library of Law and Court Decisions), http://www.internetlibrary.com/cases/lib_case403.cfm (Erişim 13.11.2016).

57 **MILLIGAN, Robert M./SALINAS, Joshua,** "A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media", NYSBA Bright Ideas, Spring/Summer 2012, Vol.21, No.1, s.7.

bulut kullanımında bulut bilişim sözleşmesini dikkatle incelemeleri ve bulutta saklanan bilgilerin ticari sır niteliğini kaybetmediğinden emin olmaları gerekmektedir[58].

İşletmenin veri merkezinde saklanan ticari sırların üçüncü kişilerce virüs içeren elektronik postalar gönderilmek suretiyle işletmenin bilgisayarlarına virüs bulaştırılarak ele geçirilmeleri söz konusu olabilir. Örneğin, Amerika Birleşik Devletleri'nde davaya konu olan bir olayda alüminyum üreticisi Alcoa Şirketi'nin ticari sırlarını ele geçirebilmek için çalışanlarına virüs içeren elektronik postalar gönderilmiştir. Bu yönteme oltalama *(phishing)* denilmektedir[59].

İşletmedeki bilgisayarlarda saklanan ticari sırların ele geçirilmesine *Physicians Interactive v. Lathian Sys.* davası da örnek verilebilir. Bu davada, davalı şirket ve bir çalışanı hakkında rakip davacı şirketin İnternet sitesine elektronik robot yazılımlar göndermek suretiyle saldırı düzenledikleri ve gizli kaynak kodlarını ve gizli müşteri bilgilerini çaldıkları ileri sürülmüştür[60].

Tacir eğer ticari sır niteliğindeki verileri kendi imkânlarıyla işletmesindeki veri merkezinde saklıyorsa siber saldırılara karşı gerekli teknik altyapıyı kurmalı ve çalıştırmalı ve teknolojik önlemleri almalıdır. Bu kapsamda düzenli olarak güncellenen virüs yazılımlarının kullanılması gerekmektedir. Ayrıca bilgisayarlarda güvenlik duvarının bulunmasına dikkat edilmelidir. Veri merkezi ile ilgilenecek teknik personelin çalıştırılması veya işletmenin büyüklüğüne göre dışarıdan bu konuda hizmet alınması gerekebilir. Teknik hususlarla ilgilenen bir personelin olması durumunda ticari sır niteliğindeki verilere erişimin sadece yetkili kişilere tanınması gerekir. Dışarıdan hizmet alınması durumunda bu kişilerle yapılacak hizmet sözleşmelerinin şartlarına dikkat edilmesi, sözleşmelere gizlilik şartı konulması düşünülebilecektir. Tacirin işletmede çalışan yardımcı, işçi, vekil gibi kişilere ve özellikle ticari sır niteliğindeki bilgilere erişimi olan çalışanlara bunların korunması hususunda dikkatli davranmaları konusunda gerekli uyarıları yapması, gerekirse eğitim vermesi ve bilinçlendirmesi gerekmektedir. Bunun için kitapçıklar, broşürler hazırlanabilir. İşe yeni alınan çalışanlar için tanıtım ve bilgilendirme toplantıları yapılabilir. Çalışanların ticari sır niteliğindeki bilgileri, tedarikçilerle

---

58 **WARE, James,** "IP, Trade Secrets and Employee Mobility", Essential California Legal Content, Week of November 25, 2013, Vol. 137, No.46.

59 **U.S. DEPARTMENT of JUSTICE,** "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Yayınlanma tarihi 19 Mayıs 2014, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage (Erişim 09.11.2016).

60 **ROWE,** RATs, s.405.

ya da başkalarıyla paylaşmaları ihtimaline karşılık teknik personel dışındaki çalışanlarla da gizlilik sözleşmesinin yapılmasına ya da hizmet sözleşmelerinde gizliliğin korunmasına ilişkin şartların bulunmasına dikkat edilmelidir. Özellikle bir şirket bünyesinde veya bir araştırma geliştirme laboratuarında çalışacak olan kişilerle yapılacak işe alım sözleşmelerinde rekabet yasağına, ticari sırların rakiplere açıklanmamasına ilişkin şartların yer alması gerekmektedir[61].

Elektronik ortamda bulunan ticari sır niteliğindeki veri ele geçirildiğinde genellikle bir kopyası alınmakta orijinal dosya yerinde bırakılmaktadır. Dolayısıyla ticari sır niteliğindeki verinin kopyalandığının anlaşılması bazen haftalar hatta çok daha uzun zaman alabilmektedir. Bu nedenle ticari sırrı ele geçiren kişinin eğer bir çalışan değilse kimliğinin tespiti de zordur[62]. Bir çalışan işten ayrıldığında onun kullandığı bilgisayar içinden herhangi bir dosyanın alınıp alınmadığı bakımından incelenebilir. İşletme bilgisayarlarında ticari sır niteliğindeki dosyaların isimlerinin "gizlidir" ve "ticari sır içerir" gibi ifadeleri içerir şekilde olması bunların izinsiz bir şekilde ele geçirilmesine engel olamayacaksa da yargılama sırasında çalışanın bu dosyaların gizliliği konusunda uyarıldığı yönünde yeterli çabanın gösterildiğinin ispatı açısından faydalı olacaktır[63]. Ticari sırlarla ilgili uyuşmazlıklarda ticari sır olduğu iddia edilen bilginin niteliğinin belirlenmesi için çaba harcandığından davacının ticari sır olduğunu iddia ettiği bilginin bu niteliğini kanıtlayamaması nedeniyle reddedilen davalar olabilmektedir[64]. Bu itibarla tacirlerin ticari sırlarını çalışanları bakımından belirgin hale getirilmesi önemlidir.

Ticari sırların saklandığı bilgisayarların bilgisayar korsanlarının *(hacker*[65]*)* saldırılarına karşı korunması gerekecektir. Bilgisayar korsanlarının veya rakiplerin ticari sırları ele geçirmek üzere teknolojiyi kullanarak birtakım girişimlerde bulunmaları söz konusu olabilir. Günümüzde teknolojinin geldiği düzey dikkate alındığında bu hususta bir uyarı mekanizmasının geliştirilmesi de önemlidir. Bunun için sadece yetkili personelin ticari sır niteliğindeki bilgilere erişiminin teknik olarak sağlanması, güvenilir parola veya şifrelerin

---

61 **KUMAR, Ranjeet/TRIPATHI, R.C./TIWARI, M.D.,** "Trade Secrets Protection in Digital Environment A Global Perspective", International Journal of Economics and Management Sciences, Vol.2, No.4, 2012, s.2.

62 **ROWE,** RATs, s.393.

63 **BRADFORD, Benjamin J./MALESON, Justin A./WERNER, Micheal T.,** "Protecting Trade Secrets Stored in the Cloud", American Bar Association, Section of Litigation Intellectual Property, March 28, 2014.

64 All Business Solutions, Inc., 629 F. Supp. 2d 553 (W.D. va. 2009) davası (**WARE**).

65 *Hacker* ya da bilgisayar korsanı, bir bilgisayar sistemine bilgi edinmek, bilgileri çalmak, bilgilere zarar vermek gibi amaçlarla yetkisiz olarak giren kişidir. http://www.merriam-webster.com/dictionary/hacker (Erişim 17.02.2016); http:// www.webopedia.com/TERM/H/hacker.html (Erişim 17.02.2016); Hacktivizmin hukuki açıdan değerlendirilmesi hakkında bkz. **DÜLGER,** 184 vd.

kullanılması, herhangi bir veri[66] ihlali ya da şifrenin ya da parolanın kırılması durumunda uyarı veren sistemin geliştirilmesi gerekmektedir[67].

Ticari sırların üçüncü kişilerce ele geçirilmesinde sadece bilgisayarlar değil veri saklayabilen, bilgi işleme özelliği olan diğer cihazlar da saldırıya uğrayabilir. Örnek olarak akıllı otomobiller, uçaklar, tıbbi cihazlar bu kapsamda sayılabilir. Nitekim nesnelerin İnterneti teknolojisi sayesinde ileride tüm akıllı cihazların birbirleriyle bağlantılı olması ticari sırların ele geçirilmesi bakımından saldırılara açık ağlar yaratacaktır[68].

Tacirlerin özellikle ticaret şirketlerinin İnternet üzerinden birbirleriyle bağlantı kurmalarının her geçen gün artması nedeniyle elektronik ortamda saklanan ticari sırların daha da saldırıya açık hale geldiği bilinmektedir. Bu itibarla siber güvenlik konusuna önem verilmesi, bu alanda gerekli harcamaların yapılması ve önlemlerin alınması gerekmektedir. Ancak uygulamada bu konuda işletmelerin yeterince farkındalık taşımadığı ve bu konuda yeterli yatırımda bulunmadığı gözlemlenmektedir[69].

Bir işletmede veri merkezi ayrı bir binada kapısında bir güvenlik görevlisi olan bir şekilde yapılandırılmış olsa da her zaman için doğal afet riski ya da güvenlik görevlisinin kablolara basma riski, bilgisayarlara sıvı dökme riski vardır. Bu nedenle verileri yedekleme düzenli olarak yapılmalıdır.[70]

---

66 Veri ve bilgi aynı değildir. Bilgi verinin analiz edilmesiyle elde edilir. http://www.business2community.com/strategy/difference-data-information-0967136 (Erişim 17.11.2016).

67 **GOWEN, Nicholas A./SCHWARTZ, Honigman Miller /Cohn LLP,** "Protecting Trade Secrets in the Cloud", The National Law Review, October 20, 2014, s.2.

68 Nesnelerin İnterneti hakkında açıklamalar ve konuyla ilgili hukuki sorunlar için bkz. **BOZKURT YÜKSEL, Armağan Ebru,** "Nesnelerin İnternetinin Hukuki Yönden İncelenmesi", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 17, Sayı 2, Y.2015, Basım Yılı Nisan 2016, s.113-139, http://hukuk.deu.edu.tr/wp-content/uploads/2016/05/arma%C4%9Fan_bozkurt_y%C3%BCksel.pdf (Erişim 14.11.2016); Bazı şirketler güvenlik açıklarının olup olmadığını tespit edebilmek için *hacker* (bilgisayar korsanı) kiralamakta ve ondan sistemde bir açık var mı diye test etmesini istemektedir. Bazı şirketler ise kendilerine yönelik bir *hacker* saldırısı olduğunda karşı saldırıda bulunmayı tercih etmektedir. **ROWE,** RATs, s.405-413.

69 ÖZDEN, Serkan, "Bilgi Güvenliği Konusunda Firmalar Ne Kadar Bilinçli?", http://wise.web.tv/video/bilgi-guvenligi-konusunda-firmalar-ne-kadar-bilincli__atblx3js2es (Erişim 14.11.2016).

70 İşletmenin merkezinden uzakta bir veri merkezinde ticari sırlar saklanabilir. Bunlara *lights out datacenter* denmektedir. Karanlık veri merkezi olarak tercüme edilebilecek bu terim, içinde personel bulunmayan, her işin uzaktan bağlanılarak yapıldığı veri merkezi anlamındadır. Veri merkezinin işletmenin ya da şirketin merkezinden başka bir binada, başka bir yerde, başka bir ülkede olması dahi mümkündür. Hiçbir insan hatasının oluşmaması için (kabloların üzerine basılması, cihazların üzerine içecek dökülmesi, kapının açılması gibi hatalar) her şey uzaktan kontrol edilmektedir. http://www.techopedia.com/definition/26965/lights-out-data-center (Erişim 07.03.2015); Konu ile ilgili diğer bilgiler için bkz. **BOZKURT YÜKSEL,**

İşletmedeki veri merkezinde saklanan ticari sır niteliğindeki dosyaların ele geçirilmesi ya da zarar görmesi durumunda tacirin maddi zarara uğraması söz konusu olabilir. Tacirin ticari sırlarını içeren dosyalar dışında elektronik ortamda tutulan ticari defterlerinin de ele geçirilmesi ya da zarar görmesi söz konusu olabilir. Bu itibarla siber risk sigortası yapılması düşünülebilir. Siber risk sigortası, kişisel veya kurumsal verilerin ihlali nedeniyle doğabilecek zararları, ağ güvenliğine yapılan saldırılar veya ağ kesintisi nedeniyle yaşanan aksaklıklardan doğabilecek net kâr kaybını, yaşanan bu tarz durumların itibar kaybına neden olmaması için yapılması gereken masrafları karşılayan sigortadır[71].

Günümüzde işletmeler ve şirketler rekabette geri kalmamak için teknolojiyi yakından takip etmek, getirdiği kolaylıklardan yararlanmak durumundadır. Bununla birlikte teknolojinin getirdiği risklere karşı yine teknik ve hukuki imkânları kullanarak kendilerini koruyabilirler[72].

B.Ticari Sırların Saklanmasında Bulut Bilişim Teknolojisinin Kullanılması

1. Genel Olarak Bulut Bilişim

Ticari sırların bulutta saklanmasından bahsetmeden önce genel olarak bulut bilişimin ne olduğu ve nasıl kullanıldığı hakkında bilgi vermek isabetli olabilir.

Bulut bilişim veri depolamanın ve diğer imkânların uzaktaki üçüncü bir kişiden alınmasını *(outsource)* sağlamaktadır. Bulut bilişim teknolojisi işletme sahiplerine pek çok kolaylık sağlamaktadır. Gün geçtikçe daha çok işletme bilgi teknolojileri uygulamalarını ve verilerini buluta taşımakta, böylelikle müşterilerinin yeni taleplerini karşılayabilmektedir. Bilgi teknolojileri altyapısının yönetimi ve işletilmesi bulut bilişim sayesinde dış kaynaktan temin edilebilmektedir. Bu sayede işletmeler kendi asıl uzmanlık alanlarına daha fazla yoğunlaşabilmektedir[73].

Bulut Bilişim, s.127.

71 https://sigortateklif.net/siber-risk-sigortasi.php (Erişim 10.11.2016); **SADIÇ, A.Burak**, "Siber Risk Sigortaları Nasıl Ele Alınmalı?", Siber Bülten, Yayınlanma Tarihi 04.10.2015, https://siberbulten.com/makale-analiz/siber-risk-sigortalari-nasil-ele-alinmali/ (Erişim 10.11.2016).

72 Gelişen teknolojilerin geleneksel iş modellerini nasıl değiştirdiği hakkında bkz. **BUGHIN, Jacques/CHUI, Michael/MANYIKA, James,** "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch", McKinsey Quarterly, http://www.mckinsey.com/industries/high-tech/our-insights/clouds-big-data-and-smart-assets-ten-tech-enabled-business-trends-to-watch (Erişim 04.12.2016).

73 **KERTESZ**, **Attila/VARADI, Szilvia,** "Legal Aspects of Data Protection in Cloud Federations", Security, Privacy and Trust in Cloud Systems, Editors Surya Nepal, Mukaddim Pathan, Springer, Verlag Berlin Heidelberg 2014, s.433.

Bulut hizmeti, kullanıcı taleplerine göre artırılabilen ya da azaltılabilen oranda, bir ağ üzerinden –tipik olarak İnternet üzerinden- bilişim kaynaklarının sağlanması hizmetidir. Kullanıcılar ihtiyaç duyduklarında bu hizmetten yararlanarak bilişim teknolojilerini kendileri satın almak yerine üçüncü kişilerden kiralamaktadırlar[74]. Bulut hizmeti tacirler açısından bakıldığında işletmelerinde yer, zaman, güç ve maliyet tasarruf yapmalarını sağlamaktadır[75].

Bulut hizmetini sunan kişi ya da kuruluş bulut hizmeti sağlayıcı *(cloud service provider)* ya da bulut sağlayıcı*(cloud provider)* olarak ifade edilebilir. Bulut hizmeti sağlayıcı gerçek kişi olabileceği gibi bir şirket veya gelir elde etme amacı olmayan bir kuruluş, bir devlet kuruluşu ya da başka bir kuruluş olabilir. Bulut hizmeti sağlayıcı başka bir kişi ya da kuruluş adına veri saklayan kişidir[76]. Bulut hizmeti sağlayıcı hizmet verirken kullandığı yazılım veya donanımların sahibi olmayabilir. Bulut hizmeti sağlayıcı yazılım veya donanım kaynaklarını üçüncü kişilerden temin etmek suretiyle de kullanıcıya veri işleme[77] hizmeti verebilir[78]. Bulut bilişimde kullanıcı/müşteri, bulut bilişim hizmetinden yararlanan kişidir. Kullanıcı bir gerçek kişi, bir tüzel kişi, bir devlet kuruluşu ya da başka bir kuruluş olabilir[79].

Kullanıcı, bulut hizmeti sağlayıcı ile bir bulut bilişim sözleşmesi yapmak suretiyle bulut hizmetinden yararlanabilmektedir. Bazı bulut hizmeti sağlayıcılar kullanıcılardan ücret almakta, bazıları ise almamaktadır. Buradaki ücretin bir kira bedelinden ziyade hizmet sağlayıcının işgörme edimi karşılığında olduğu belirtilmektedir[80].

---

74 **HON, W. Kuan/MILLARD, Christopher**, "Cloud Technologies and Services", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.3.

75 **HURWITZ, Judith/BLOOR, Robin/KAUFMAN, Marcia/HALPER, Fern,** Cloud Computing for Dummies, Wiley Publishing, Inc., Indianapolis 2010, s.10.

76 **GELLMAN, Robert,** "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", World Privacy Forum, February 23, 2009, s.7, http://www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf (Erişim 17.03.2015).

77 Veri işleme, *"verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder."* Kişisel Verilerin Korunması Kanunu madde 3(e)'de kişisel verilerin işlenmesi tanımlanmıştır. 6698 sayılı Kanun, RG., T.07.04.2016, S.29677.

78 **WEICHERT, Thilo,** "Cloud Computing & Data Privacy", The Sedona Conference Working Group Series, February 2011, s.2, https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-conputing-and-data-privacy.pdf (Erişim 24.11.2016).

79 **GELLMAN,** s.5.

80 **BAŞGÜL, Mürsel/CHOUSEİNOGLOU, Oumot,** "Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukuki Sorunlar", 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, Ankara 2013, s.212.

2. Bulut Bilişim Sözleşmesinin Hukuki Niteliği

Bulutta verilerin saklanması nedeniyle bulut bilişim sözleşmesinin bir saklama sözleşmesi olabileceği ileri sürülebilir. Doktrinde *BAŞGÜL ve CHOUSEİNOGLOU* saklama sözleşmesinin tam olarak bulut bilişim sözleşmelerinin özelliklerini karşılamayabileceğini belirtmektedirler. Buna gerekçe olarak da saklama sözleşmesinin konusunun bir taşınırın güvenli bir yerde saklayan tarafından koruma altına alınmasını göstermektedirler (TBK m.561). Kullanıcının verileri taşınır olarak nitelendirilse dahi bulut bilişim sözleşmesinin saklama sözleşmesi olarak değerlendirilmesinin mümkün olmayacağını belirten yazarlar, bulut bilişim sözleşmelerinde sadece verilerin saklanması değil, yazılım, bakım hizmetlerinin verilmesi edimlerinin de bulunduğunu da ifade etmektedirler. Ancak sonuç olarak yazarlar saklama sözleşmesine ilişkin klasik hukuk ilkelerinin bilişim hukukuna da uygulanabilecek evrensel kurallar olduğu görüşünü ifade etmektedirler[81].

FISCHL ve *WEIMER,* birden fazla sözleşmenin özelliğini taşıyan karma sözleşmelerden bahsederek, karma sözleşmelerde sözleşmedeki temel unsurun, hangi sözleşmenin özelliği daha ağır basıyorsa onun sözleşmenin hukuki niteliğini belirleyebileceğini ifade etmektedirler. Bu bakımdan bulut bilişim sözleşmesini de karma sözleşme olarak görmektedirler. Bulut bilişim sözleşmesinde saklama, kira, hizmet sözleşmesinin özelliklerinin görüldüğünü belirtmektedirler[82].

Bulut bilişim sözleşmesinde kiralama, saklama, satış dışında eser ve vekâlet sözleşmesine ait unsurlar da yer alabilir. Bulut bilişim sözleşmesinde değişik sözleşmelerin unsurları veya değişik sözleşmelerin tarafların iradesi ile bir araya getirilmesi söz konusudur[83]. *BOZBEL* bulut bilişim sözleşmesinin karma sözleşme niteliğinde olduğu görüşündedir. Yazar, hafıza kapasitesinin kullanıma hazır tutulmasının bir kira sözleşmesi olarak nitelendirilmesi gerektiğini, erişim sunma, bakım ve bulutun kullanımında destek verilmesi edimlerinin hizmet sözleşmesi niteliğinde olduğunu belirtmektedir. Uygulama yazılımlarının kurulumu ve uyarlanması ise eser sözleşmesi vasıflarını taşımaktadır[84].

---

81 **BAŞGÜL/CHOUSEİNOGLOU,** s.212.

82 **FISCHL, Thomas/WEIMER, Katharina A.,** "Cloud Computing-A German Perspective", Transcending the Cloud, A Legal Guide to the Risks and Rewards of Cloud Computing, ReedSmith, s.3, http://www.reedsmith.com/files/Publication/cf6df614-498c-4c92-979c-454346c15369/Presentation/PublicationAttachment/131ec3c6-65ff-45e4-bca1-f5628e478465/Cloud%20Computing%20-%20Germany%20Chapter%20ONLY%20-%2008.12.10.pdf (Erişim 04.01.2015).

83 **BAŞGÜL/CHOUSEİNOGLOU,** s.212; **WEICHERT,** s.3.

84 **BOZBEL, Savaş,** Fikir ve Sanat Eserleri Hukuku, XII Levha Yayınları, İstanbul 2012, s.476.

Esasen burada Türk hukuku açısından kanunun çeşitli sözleşme tiplerinde öngördüğü unsurların kanunun öngörmediği tarzda bir araya getirilmesi söz konusudur[85]. Dolayısıyla kanaatimizce de birden fazla sözleşmenin özelliğini taşıyan bulut bilişim sözleşmesinin hukuki niteliği için karma sözleşmedir denebilir.

3. Bulut Hizmeti Modelleri

Bulut hizmetinde hizmet modelleri temel olarak üç çeşittir[86]. Bulut hizmet modelleri en dar kapsamlı olandan en geniş kapsamlı olana doğru sıralanacak olursa:

- Bir hizmet olarak Altyapı *(IaaS-Infrastructure as a Service)*: ham bilişim kaynaklarının müşteriye sağlandığı hizmet modelidir; veri işleme, depolama, ağ gibi temel bilişim kaynakları sunulur. Örnek olarak Amazon S3, SQL Azure verilebilir[87].
- Bir hizmet olarak Platform *(PaaS-Platform as a Service)*: yazılım uygulamalarının geliştirilmesi ve dağıtımı için platformların sağlandığı hizmet modelidir; hizmet sağlayıcının programlama dili, kütüphanesi veya araçları kullanılarak uygulamalar yaratılır ve dağıtılır. Örnek olarak Force.com, Google App Engine, Windows Azure (Platform) verilebilir[88].
- Bir hizmet olarak yazılım *(SaaS-Software as a Service)*: son kullanıcılar hizmet sağlayıcının bulut altyapısında sunduğu uygulamaları kullanmaktadır[89]. Örnek olarak Google Docs, Salesforce CRM, SAP Business by Design verilebilir[90].

---

85 Karma sözleşmeler hakkında ayrıntılı bilgi için bkz. Cevdet Yavuz, Borçlar Hukuku Dersleri (Özel Hükümler), Beta Yayınevi, İstanbul 2013, s.13; Elektronik ortamda hizmet sunumunu konu eden elektronik sözleşmelerin genellikle hazır olmayanlar arasında yapıldığı ve hukuki niteliği itibarıyla katılmalı ve mesafeli sözleşmeler olduğu hakkında bkz. **AKKURT, Sinan Sami**, "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri", AÜHFD, 60(1), 2011, s.30.

86 **TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE),** Yakup Korkmaz, "Bulut Bilişim: Türkiye İçin Fırsatlar", http://www.tubitak.gov.tr/tubitak_content_files/bilgiguvenligi/sunular/Korkmaz_Bulut_Bilisim.ppt (Erişim 22.11.2014).

87 **European Commission Information Society and Media,** "The Future of Cloud Computing - Opportunities for European Cloud Computing Beyond 2010", Expert Group Report, s.9, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (Erişim 22.01.2015).

88 **European Commission Information Society and Media,** s.10.

89 *SaaS* şeklindeki bulut bilişim hizmeti en çok tercih edilen modeldir. Kullanıcıların herhangi özel bir yazılım indirmeden bulut yazılım uygulamasını kullanmalarına imkân sağlamaktadır. 2011 yılında Birleşik Krallık merkezli 300 işletme arasında yapılan bir ankette kullanıcıların en çok kullandıkları uygulamaların elektronik posta, yedekleme/kurtarma, depolama ve ağ sayfalarını barındırma *(web hosting)* hizmetleri olduğu görülmüştür. **HON/MILLARD,** s.4; *SaaS* modelinde bulut bilişim hizmeti örneği olarak Facebook verilebilir. *SaaS* modelindeki bulut ile paylaşım uygulamaları da dâhil sosyal ağ sağlanmaktadır. Facebook hizmet sözleşmesi için bkz. https://www.facebook.com/legal/terms (Erişim 25.11.2014).

90 **European Commission Information Society and Media,** s.10.

Bulut bilişimde kullanıma göre kurulum modelleri Amerika'da bulunan Ulusal Standartlar ve Teknoloji Enstitüsü'nün *(NIST-National Institute of Standards and Technology)* yaptığı[91] sınıflandırmada dört tanedir[92]. Bunlar:

- Özel Bulut *(Private Cloud)*: Tipik olarak farklı farklı kullanıcılar bulunmaktadır[93]. Bu kurulum modeli daha çok bir hizmet olarak yazılım *(SaaS)* şeklindedir[94]. Örneğin alışveriş hizmeti sunan eBay Şirketi bu kurulum modelini kullanmaktadır[95]. Özel bulut aynı zamanda devlet veya bir şirketler grubu içinde kurulmuş bilgisayar ağlarını da içermektedir[96].
- Topluluk Bulutu *(Community Cloud)*: Bu modelde altyapı ortak menfaatleri olan özel bir grup kullanıcıya aittir ya da onlar tarafından işletilmektedir ve paylaşılmaktadır. Örneğin bir devletin organları tarafından kullanılan ya da finansal hizmet veren şirketlerin birlikte kullandıkları bulut bu modeldir[97]. Topluluk bulutunda değişik kuruluşlar altyapılarını bir özel veya kamu bulutu için birleştirmektedir[98].
- Genel bulut *(Public Cloud)*: Altyapının aynı donanım veya yazılımı kullanan farklı kullanıcılar arasında kullanıldığı kurulum modelidir[99]. Bu bulutu kullanan işletmeler maliyetleri azaltmak için hizmetlerini dışarıdan sağlamaktadır. Genel bulut daha çok büyük ve dünya çapındaki

---

91 **NIST,** The NIST Definition of Cloud Computing, Special Publication 800-145, s.3, http//csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Erişim 24.11.2016).

92 HON/MILLARD, s.4.

93 **European Commission Information Society and Media,** s.10.

94 **HON/MILLARD,** s.4; Bu modele örnek Amerika Birleşik Devletleri'nin Alaska Eyaleti'nin uygulaması verilebilir. Alaska Eyaleti verilere daha hızlı ulaşabilmek, bölümlerdeki usuli uygulama farklılıklarını gidermek, bilgi merkezlerinde çalışanların hepsini aynı seviyeye getirmek için bulut bilişimi desteklemiş özel bulut uygulamasını başlatmıştır. **CISCO,** "State Government Deploys Private Cloud to Provide Services to Agencies", http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/state_of_alaska_cs.pdf (Erişim 22.11.2014).

95 **VENKATRAMAN, Archana,** "Case Study: How eBay Uses Its Own OpenStack Private Cloud", Computer Weekly, 18 June 2014, http://www.computerweekly.com/news/2240222899/Case-study-How-eBay-uses-its-own-OpenStack-private-cloud (Erişim 20.01.2015).

96 **WEICHERT,** s.2.

97 **HON/MILLARD,** s.4; Örneğin, Amerika Birleşik Devletleri Kaliforniya Eyaleti'nde tüm devlet organları Kaliforniya'da yerleşik vatandaşların bilgileri konusunda aynı bulut bilişim altyapısını kullanmaktadır. http://thecloudtutorial.com/cloudtypes.html (Erişim 22.11.2014).

98 **KERTESZ/VARADI,** s.434.

99 Genel buluta örnek olarak Amazon Şirketi'nin sunduğu bir hizmet olan Amazon Elastic Compute Cloud (EC2), IBM Şirketi'nin sunduğu bir hizmet olan Blue Cloud, Google Şirketi'ne ait Google AppEngine ve Microsoft Şirketi'ne ait Windows Azure Services Platform verilebilir. http://searchcloudcomputing.techtarget.com/definition/public-cloud (Erişim 23.11.2014).

bilişim teknolojileri şirketleri tarafından hizmete sunulmaktadır. Amazon,[100] Google Apps,[101] Microsoft, IBM burada örnek olarak gösterilebilir[102].

- Karma/Melez bulut *(Hybrid cloud)*: Yukarıdakilerin karışımı olan kurulum modelidir. Hibrid bulut hem özel hem de genel bulutun özelliklerini taşımaktadır. Ancak şu anda hibrid bulut kullanımı diğerlerine nazaran daha azdır[103].

Bu modellere Avrupa Komisyonu özel amaçlı bulutu da eklemektedir[104].

- Özel Amaçlı Bulut (Special Purpose Clouds): Özel fonksiyonlara sahip bir modeldir[105]. Örnek olarak Google's App Engine verilebilir. Burada Google altyapısı kullanılarak çeşitli uygulamalar geliştirebilir veya çalıştırabilir. Özel amaçlı bulut kurulum modeli bir hizmet olarak platform *(PaaS)* modelidir[106]. Bu bulut kurulum modeli diğer modellere nazaran daha da ihtisaslaşmış bir kurulum modelidir[107].

Uygulamada bu modeller dışında bir bulut hizmeti sağlayıcının diğer hizmet sağlayıcılar ile müşterileri arasında hiç kendi bulutunu kullandırmadan aracı olabildiği de görülmektedir[108].

C. Ticari Sırların Saklama Alanı Olarak Bulut

1. Bulut Kullanımının Ticari Sırlar Açısından Avantajları ve Dezavantajları

a. Avantajlar

Bulut bilişim işletmelere pek çok kolaylık sağlayabilir. Buluta yüklenen verilerin kaybolmaya, bozulmaya karşı korunması avantajlardan ilki olarak sayılabilir. Bulut hizmeti sağlayıcılar buluta yüklenen verileri, bozulmaya, yazılım veya donanımla ilgili hatalara karşı yedekleyebilir. Hatta işleyişin aksamaması için depolanmış verileri aynı veri merkezinde ayrı bir donanımda kopyalayabilir. Bazı hizmet sağlayıcılar coğrafi olarak da farklı yerlerdeki sunucularda verileri kopyalayarak saklamaktadır. Böylelikle örneğin bir doğal afet durumunda bir

---

100 http://aws.amazon.com/ (Erişim 21.01.2015).
101 https://www.google.com/work/apps/business/ (Erişim 21.01.2015).
102 **WEICHERT,** s.2.
103 **KERTESZ/VARADI,** s.434.
104 **European Commission Information Society and Media,** s.11.
105 **European Commission Information Society and Media,** s.11.
106 https://cloud.google.com/appengine/docs/whatisgoogleappengine (Erişim 21.01.2015).
107 **KERTESZ/VARADI,** s.435.
108 Bulutların birbirleri ile etkileşimli çalışması hakkında geniş açıklama için bkz. **DMTF,** "Interoperable Clouds", A White Paper from the Open Cloud Standards Incubator, http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf (Erişim 23.01.2015).

veri merkezinde telafi edilemeyecek bir hasarın oluşması durumunda başka bir yerdeki veri merkezinde yer alan kopyalar kullanılabilmektedir[109].

Bulut bilişimin ikinci avantajı ekonomikliktir. Bulut bilişimde hizmet birden çok kişiye sağlandığı için sunucular, yazılımlar için yapılacak masraflar azalmaktadır. Dolayısıyla kullanıcıların ödediği ücret bireysel olarak bunları sağlamaya çalışsa yapacağı harcamaya göre düşük olmaktadır. Yazılımlar için ödeme sadece kullanılan kadar yapılmaktadır. Ayrıca bir lisans ücreti söz konusu değildir. İşletme bünyesinde bir veri saklama merkezi barındırmanın bakım ve güvenlik masrafları bulut bilişimin kullanılması ile ortadan kalkmaktadır[110].

Bulut bilişim hizmeti, bilişim sistemlerinin ve güvenlik altyapısının sağlanması konusunda profesyonel bir hizmettir. Dolayısıyla asıl işi bilişim alanının dışında olan bir tacirin iyi çalışan ve güvenliği sürekli olarak sağlanan bir bilişim altyapısını kurması ve sürekliliğini sağlaması için ayrı bir mesai ve kaynak ihtiyacı vardır. Ayrıca asıl işi bu olmadığından tam olarak bu konuya odaklanması da çoğu zaman mümkün olamamaktadır[111]. Oysa bulut bilişim hizmetinden yararlanmak suretiyle sürekli olarak işlerliği bulunan ve güvenliği sağlanan bir bilişim altyapısından yararlanmak mümkün hale gelmektedir.

b. Dezavantajlar

Bulut bilişim kullanıcılara pek çok kolaylık sağladığı gibi, teknik ve hukuki bazı sorunları da beraberinde getirmektedir. Bunlardan ilki İnternet'e bağlı olarak buluttaki kaynaklara ulaşıldığından eğer bağlantı kurulamazsa ya da uzun zaman alırsa bir yerde saklanan verilere başka bir yerden kullanıcının ulaşmasının zor olmasıdır[112]. Verilerine erişemeyen veya zamanında erişemeyen işletmelerin zarar görmesi söz konusu olabilecektir.

Bulut bilişimde veri güvenliğinin ve gizliliğinin korunması en büyük sorunlardan biridir. Bulut bilişim kullanımında bazı verilerin ülke sınırları dışındaki bulutta saklanması nedeni ile ticari sırların korunması ile ilgili sorunlar mevcuttur[113]. Zira yurt dışında yerleşik bir bulut hizmeti sağlayıcının

---

[109] **HON/MILLARD**, s.10; Örneğin Google Şirketi, Google Apps kullanıcılarının tüm verilerinin afet ve acil durumlar için yedeklediğini belirtmiştir. Kullanıcıların yaptıkları her işlem aynı anda iki veri merkezinde yedeklenmektedir. Eğer doğal afet durumunda bir veri merkezi zarar görürse veriler diğer merkezine de aktarılmış olduğundan kullanıcılar verileri kaybetmemiş olacaktır. http://googleforwork.blogspot.com.tr/2010/03/disaster-recovery-by-google.html (Erişim 23.11.2014).

[110] **MEMİŞ, Tekin,** "Bulut Bilişimde Fikri Hak Sorunları", Fikri Mülkiyet Hukuku Yıllığı 2013, Yetkin Yayınları, Ankara 2015, s.320.

[111] **MEMİŞ,** s.321.

[112] **WEICHERT,** s.3; **BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU,** Bulut Bilişim, Ankara 2013, s.10.

[113] **MEMİŞ,** s.322; **WEICHERT,** s.3.

yurtdışındaki sunucularında sakladığı ticari sırların söz konusu ülkedeki hukuk kuralları gereği yetkili otoriteler tarafından öğrenilmesi mümkündür.

2.Ticari Sırların Bulutta Saklanması ve Gizliliğin Korunması Sorunu

Teknoloji alanında büyük bir atılım olan bulut bilişim işletmeler için de büyük önem taşımaktadır. İşletmelerin bulut bilişimden yararlanmalarıyla birlikte artık kendi veri merkezlerinde verilerini saklamalarına gerek kalmamıştır. Bir işletmenin verilerini kendi bilgisayarlarında saklamak yerine uzakta bulunan üçüncü bir kişiye ait sunucularda saklaması bu verilerin gizliliği, güvenliği özellikle ticari sırlar bakımından ise bu sırların korunması ile ilgili hukuki sorunları gündeme getirmektedir[114]. Ticari sır niteliğindeki bilgilerin üçüncü kişilerle paylaşılması ve konumuz bakımından özellikle buluta yüklenmesinin bilgilerin ticari sır niteliğini ortadan kaldırıp kaldırmayacağı hususu öne çıkmaktadır. Ticari sır niteliğindeki bilginin üçüncü kişilere açıklanması ya da transfer edilmesi durumunda, söz konusu üçüncü kişilerin gizliliğin korunması hususunda göstereceği gayretin ticari sır sahibi tarafından gözetilmesi gerekir[115]. Bir ticari sır sahibinin bilginin ticari sır niteliğini ortadan kaldırabilecek nitelikteki davranışı üç şekilde olabilir. Bunlar: ticari sır sahibinin yayın, patent başvurusu yoluyla ticari sırrı duyurması ya da tersine mühendislik[116] yapılması mümkün bir ürün veya hizmet ile pazara sürmesi ve de herhangi bir gizlilik taahhüdü almadan başkalarına ticari sırrı açıklamasıdır[117]. Gizliliği koruma yükümlülüğünde bulunmayan bir üçüncü kişi ile ticari sır niteliğindeki bilgilerin paylaşılması durumunda paylaşımın niteliği dikkatle incelenmeli ve burada ticari sır niteliğini etkileyecek şekilde bir paylaşımın olup olmadığına bakılmalıdır. Bu itibarla ticari sırların nasıl ve nerede saklandığına, bu bilgilere kimlerin erişim yetkisinin bulunduğuna dikkat edilmesi gerekir. Ticari sırların korunması kapsamında bulut bilişimin sınırlı olarak kullanılması, buluta yüklenen diğer verilerle ticari sır niteliğindeki verilerin ayrılması gizliliğin

---

114 **DHULIA,** s.4.

115 **SANDEEN, Sharon K.,** "Lost in the Cloud? The Trade Secret Implications of Cloud Computing", 2011 MSBA Computer and Technology Law Institute, Minneapolis, October 20, 2011, s.59.

116 Tersine mühendislik, insan yapımı bir nesnenin/ürünün parçalara ayrılarak onun üretim ve çalışma prensiplerinin çıkarılması, belirlenmesi sürecini ifade etmek için kullanılmaktadır. **SAMUELSON, Pamela/SCOTCHMER, Suzanne,** "The Law and Economics of Reverse Engineering", Yale Law Journal, Vol.111, No.7, 2002, s.1575 vd.; Tersine mühendisliğin kullanım alalarından biri için bkz. **BOZKURT YÜKSEL, Armağan Ebru,** "Üç Boyutlu Yazıcıların Fikri Mülkiyet Hukukuna Etkileri", Fikri Mülkiyet Hukuku Yıllığı 2014, Editör Prof.Dr.Tekin Memiş, Yetkin Yayınevi, Ankara 2016, s.112; **BOZKURT YÜKSEL, Armağan Ebru,** Patent Uyuşmazlıklarının Çözüm Yolları – Milletlerarası Tahkim ve Devlet Yargısı, Yetkin Yayınları, Ankara 2009, s.254.

117 **SANDEEN,** s.61.

korunması yükümlülüğü kapsamında düşünülebilir[118].

Bulut bilişim teknolojisi kullanılmaksızın ticari sırların tacire ait bilgisayarlarda, harici hard disklerde yedeklenmesi ve saklanması durumunda üçüncü bir kişiye ticari sırların açıklanması söz konusu değildir. Bulut kullanılması durumunda ise başka bir kişiye ait donanım ve yazılımın kullanılması nedeniyle ticari sırların ticari işletmenin dört duvarının dışında saklanmasının makul olup olmadığı tartışmalıdır. Ayrıca tacirin ticari sırlarını bulutta saklamasının basiretli bir davranış teşkil edip etmediği de tartışma konusu olabilir[119]. Bu tartışmaların yanında tacirin kendi bilgisayarlarında ticari sır niteliğindeki bilgileri bulundursa bulut kullanmasa dahi ticari sırların tam anlamıyla güvende olduğu söylenemez. Zira tacir en üst seviyede güvenlik önlemlerini sağlayamayabilir[120]. Bu bakımdan tacirin gerekli özeni göstermek suretiyle güvenilir bir bulut hizmeti sağlayıcı seçmesi ve onunla sözleşme koşullarına özellikle sır saklama yükümlülüğüne ilişkin sözleşmede şart bulunmasına gayret ederek sözleşme yapması bir bakıma daha basiretli bir davranış olarak dahi nitelendirilebilir. Burada tacirin bulutu nasıl kullandığı önemlidir. Örneğin New York Bölge Mahkemesi'nin bir kararında bir şirketin bir müşteri listesini buluta herkes tarafından erişilebilecek şekilde yüklemesi durumunda artık bilginin ticari sır niteliğinin kalmadığı belirtilmiştir[121].

3. Basiretli Davranma Yükümlülüğü ve Tedbirli Bir Yöneticinin Göstereceği Özen Kapsamında Ticari Sırların Bulutta Saklanması

Bulut hizmetinden yararlanılması bir işletmenin bilişim teknolojileri için gerekecek harcama kaleminin azalmasını sağlayacaktır. Bununla birlikte ticari sırların korunması açısından bakıldığında verilerin buluta yüklenmesinin tacir açısından basiretli bir davranış (TTK m.18/II) olup olmadığı sorusu da gündeme gelebilecektir. Zira ticari sırların buluta yüklenmesi ile söz konusu bilgilere hem bulut hizmeti sağlayıcının hem de üçüncü kişilerin erişimi mümkün olabilir. Basiretli davranma yükümlülüğü gereğince tacir ticari işletmesiyle ilgili faaliyetlerinde, aynı ticaret dalında faaliyet gösteren tedbirli, öngörülü bir tacirden beklenen özeni göstermek zorundadır[122]. Bu itibarla ticari sırlarını buluta aktarmayı düşünen bir tacir bu durumun veri güvenliği açısından risklerini öngörmek, gerekli tedbirleri hem bulut bilişim sözleşmesinin

---

118 **SANDEEN,** s.90.

119 **THAYER, Linda J./YANG, Ming-Tao,** "Security and Privacy: Storing Trade Secrets in the Cloud-Bad Idea?", Cloud Computing Journal, December 4, 2015, s.2, http://finnegan.com/resources/articles/articlesdetail.aspx?news=450db577-3e55-43db-ad74-192fde3fd3f9 (31.07.2016).

120 **INTERNATIONAL CHAMBER of COMMERCE,** s.7.

121 **MILLIGAN/SALINAS,** s.4.

122 **ŞENER,** Ticari İşletme, s.191.

yapılması aşamasında, hem sözleşme içeriği düzenlenirken hem de bulutun kullanımı sırasında erişim güvenliğine dikkat ederek almak durumundadır.

Tacirlerin defter ve belgelerini bulutta saklamaları halinde bu verilerin güvenliğinin sağlanması gündeme gelecektir. Türk Ticaret Kanunu uyarınca her tacir; ticari defterlerini, envanterleri, açılış bilançolarını, ara bilançolarını, finansal tablolarını, yıllık faaliyet raporlarını, topluluk finansal tablolarını ve yıllık faaliyet raporlarını ve bu belgelerin anlaşılabilirliğini kolaylaştıracak çalışma talimatları ile diğer organizasyon belgelerini, alınan ticari mektupları, gönderilen ticari mektupların suretlerini, 64. maddenin birinci fıkrasına göre yapılan kayıtların dayandığı belgeleri, sınıflandırılmış bir şekilde on yıl süreyle saklamakla yükümlüdür. Açılış ve ara bilançoları, finansal tablolar ve topluluk finansal tabloları hariç olmak üzere, sayılan bu belgeler Türkiye Muhasebe Standartlarına da uygun olmak kaydıyla, görüntü veya veri taşıyıcılarda saklanabilirler. Ancak, okunur hâle getirildiklerinde, alınmış bulunan ticari mektuplar ve defter dayanaklarıyla görsel ve diğer belgelerle içerik olarak örtüşmelidir. Saklama süresi boyunca kayıtlara her an ulaşılabilmelidir ve uygun bir süre içinde kayıtlar okunabilir hâle getirilebiliyor olmalıdır. Görüldüğü üzere kanunda defter ve belgelerin bulutta saklanması ile ilgili herhangi bir sınırlandırma bulunmamaktadır (TTK md.82).

Şirket yöneticileri için söz konusu olan özen ve bağlılık yükümlülüğü çerçevesinde şirket verilerinin buluta yüklenmesi şirket menfaatlerini ön planda tutan, tedbirli bir yöneticinin göstermesi gereken bir davranış sayılabilir mi sorusu da burada gündeme gelebilir. Türk Ticaret Kanunu'nun "özen ve bağlılık yükümlülüğü" kenar başlığını taşıyan 369.maddesinde *"Yönetim kurulu üyeleri ve yönetimle görevli üçüncü kişiler, görevlerini tedbirli bir yöneticinin özeniyle yerine getirmek ve şirketin menfaatlerini dürüstlük kuralına uyarak gözetmek yükümlülüğü altındadırlar."* hükmü yer almaktadır. Yönetim kurulu üyelerinin ortaklığın menfaatlerini daima ön planda tutma yükümlülüğü şirkete sadakat borcu ile ilgilidir. Şirket ile yönetim kurulu üyeleri arasındaki vekâlet veya hizmet sözleşmesinden kaynaklanan sadakat borcu, sır saklama ve özen gösterme yükümlülüklerinin de temelini oluşturur[123]. 369. maddenin gerekçesinde belirtildiği üzere tedbirli yönetici ölçüsü basiretli işadamı kavramından farklıdır. Tedbirli yönetici ölçüsü, yönetim kurulu üyesinin kurumsal yönetim ilkelerine uygun olarak "işadamı kararı" *(business judgement rule)* verebileceğini kabul eder ve riskin bundan doğduğu hallerde üyenin sorumlu tutulmaması esasına dayanır[124]. Duruma uygun araştırmalar

[123] ÇAMOĞLU, **Ersin,** Anonim Ortaklık Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu, 2.B., Vedat Kitapçılık, İstanbul 2007, s.75-76.

[124] İşadamı kararı ilkesi, yönetim kurulu üyelerinin verecekleri kararlarda, tedbirli yönetici ölçüsünün belirlenmesinde bir kriter olarak benimsenmiştir. Yönetim kurulu üyeleri bu

yapılıp, ilgililerden bilgiler alınıp yönetim kurulunda karar verilmişse, gelişmeler tamamen aksi yönde olup şirket zarar etmiş olsa bile özensizlikten söz edilemez[125].

Dolayısıyla şirketin ticari sırlarını da içeren şirket verilerine hızlı bir şekilde, farklı yerlerden ulaşma imkânını sağlayan bulut teknolojisinin kullanılması için yönetim kurulunda alınacak karar, eğer öncesinde gerekli özen gösterilerek incelemeler yapılarak alınmışsa, bulut bilişim sözleşmesinin hazırlanmasında gerekli özen gösterilmişse, gerekirse veriler buluta şifrelenerek gönderilmişse, elde edilecek yarar ile risk dengesi göz önünde tutulmuşsa,[126] tedbirli ve özenli bir davranış teşkil edecektir. Buna rağmen bulutun siber saldırıya uğraması ve şirkete ait ticari sırların üçüncü kişilerce ele geçirilmesi nedeni ile şirket zarara uğrarsa yöneticilerin tazminat sorumluluğu gündeme gelebilecektir. Ancak burada tazminattan yöneticiler kusurları oranında sorumlu olacaktır[127]. Yönetim kurulu üyelerinin sorumluluğunu düzenleyen Türk Ticaret Kanunu'nun 553(1).maddesi uyarınca yönetim kurulu üyeleri kanundan ve ortaklık ana sözleşmesinden doğan yükümlülüklerini kusurlarıyla ihlal ettikleri takdirde, hem ortaklığa, hem pay sahiplerine hem de ortaklık alacaklılarına karşı verdikleri zarardan sorumludurlar. Yönetim kurulu üyelerinin sorumlulukları kusura dayanmaktadır. Türk Ticaret Kanunu'nun 557.maddesi uyarınca yönetim kurulu üyelerinin sorumluluğu bakımından farklılaştırılmış teselsül ilkesi söz kabul edilmiştir. Birden fazla yönetim kurulu üyesinin her birinin kusuruna ve durumun gereklerine göre, zarar kendilerine yükletilebildiği ölçüde zarardan birlikte sorumlu olmaları söz konusudur[128]. Ayrıca, yönetim kurulu üyelerinin isteğe bağlı sorumluluk sigortası yaptırmaları da mümkündür[129].

---

kritere uygun davrandıklarında tedbirli bir yöneticinin göstermesi gereken özeni göstermiş sayılır. Tedbirli yönetici, nesnel ve ideal değeri temsil eden ölçü kişidir. Özen ölçüsü tespit edilirken tedbirli ve akılı bir kişinin aynı durum ve koşullarda göstereceği davranışlar dikkate alınacaktır. **BOZKURT YAŞAR, Sevgi,** Anonim Şirketlerde İşadamı Kararı İlkesinin (Business Judgment Rule) Uygulanması, Beta Yayınevi, İstanbul 2015, s.167 vd., dn.470'de anılanlar.

125 Türk Ticaret Kanunu madde 369 gerekçe metni için bkz. http://www.ticaretkanunu.net/turk-ticaret-kanunu-madde-gerekceleri-ikinci-kitap-ticaret-sirketlerimadde-124-644/ (Erişim 03.01.2015); Konu ile ilgili açıklamalar için bkz. **DEDEAĞAÇ, Ender/SAPAN, Oğuzhan,** Anonim Şirketlerde Yönetim Kurulu ve Sorumluluğu, Ankara Barosu Başkanlığı, Ankara 2013, s.51-53.

126 **BOSTICK, Kenneth L.,** "Pie in the Sky: Cloud Computing Brings an End to the Professionalism Paradigm in the Practice of Law", Buffalo Law Review, Vol.5, s.1413.

127 **AKDAĞ GÜNEY, Necla,** Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu, Vedat Kitapçılık, İstanbul 2010.

128 **ŞENER,** Oruç Hami, Ortaklıklar Hukuku, 2.B., Seçkin Yayınevi, Ankara 2015, s.413 vd.

129 **BAŞGÜL/CHOUSEİNOGLOU,** s.213-214; **KÖSEKAYA, Fatih,** Anonim Şirket Yönetim Kurulu Üyelerinin Mesleki Sorumluluk Sigortası, Adalet Yayınevi, Ankara 2013.

Tedbirli bir yöneticinin göstereceği özen kapsamında şirket yöneticileri eğer ticari sırları şirketin kendi imkânlarıyla şirkette bulunan veri merkezinde saklıyorlarsa siber saldırılara karşı gerekli teknik altyapının kurulması ve çalıştırılması şeklinde teknolojik önlemleri almalıdırlar. Burada şirket yöneticilerinden tüm teknik hususları anlamaları beklenmemelidir. Ancak teknik konulardan anlayan şirket içinde bir personel oluşturmak ya da bu konuda dışarıdan destek almak şeklinde davranış beklenebilir. Bu noktada personel seçiminde ya da dışarıdan destek alınacak kişilerin seçiminde karar alabilmek için makul ölçüde bilgilenmiş olmaları gerekmektedir[130].

4. Bulut Hizmeti Sağlayıcı Seçiminde ve Sözleşme Şartlarında Dikkat Edilecek Hususlar

Ticari sırrın saklanması için bulut bilişim de dâhil herhangi bir dış kaynak kullanıldığında, ticari sırrı saklayacak olan kişinin güvenilirliği, devamlılığı ve ulaşılabilirliği ticari sır sahibi tarafından aranacak özelliklerdir. Bulut bilişim açısından bakıldığında ise özellikle hizmet sağlayıcının güvenirliği, sunucuların nerede olduğu, hizmet sözleşmesinin şartları çok önemlidir. Bulut bilişim sözleşmesinde hizmet sağlayıcının ticari sır niteliğindeki bilgilerin gizliliğini ihlal etmesi durumunda sorumlu olacağına ilişkin şartlar da dahil sözleşmede yer almasına dikkat edilmesi gereken hususlar vardır[131].

Ticari sırların bulutta saklanması durumunda ticari sır sahibinin gizliliğin korunması konusunda makul oranda gayret göstermesi gerekmektedir[132]. Bu noktada bulut bilişim sözleşmelerinin şartlarının hazırlanması ve sözleşme öncesi gerekli özenin gösterilmesi öne çıkmaktadır.

Tacirin ticari sırlarının korunmasında gerekli çabayı gösterdiğinin ispatı üç noktada yoğunlaşmaktadır. Bunlardan ilki ticari sırların saklanacağı bulut hizmeti sağlayıcının seçiminde özen gösterilmesidir. İkincisi bulut hizmeti sağlayıcı ile yapılan sözleşmenin şartlarıdır. Üçüncüsü de tacirin ticari sırların gizli kalmasında gösterdiği özendir[133].

a. Sözleşme Öncesi Dikkat Edilecek Hususlar

Sözleşme öncesinde bulut hizmeti sağlayıcının gerekli güvenliği sağlayabileceğinden emin olmak gerekir. Bunun için özenli inceleme ve değerlendirme yapılmalıdır *(due diligence).* Bu itibarla fiziksel olarak yapılan

---

130 **BOZKURT YAŞAR**, s.269; Yönetim kurulu üyelerinin toplantı dışında bilgi alma ve inceleme hakları vardır (TTK m.392). *"Her yönetim kurulu üyesi yönetim kurulu başkanından izin alarak, yönetim kurulu toplantılarının dışında yöneticilerden bilgi alabilir, defterleri, belgeleri, sözleşmeleri, dosyaları inceleyebilir."* **TEKİNALP,** Ünal, Sermaye Ortaklıklarının Yeni Hukuku, 3.B., Vedat Kitapçılık, İstanbul 2013, s.234.

131 **SANDEEN.**

132 **DHULIA,** s.18.

133 **THAYER/YANG,** s.2.

kontroller, bulut hizmeti sağlayıcının erişimleri nasıl kontrol ettiği, izinsiz erişimleri önlemek ve yakalamak için ne tür tedbirler aldığı incelenmelidir. Bu anlamda hizmet sağlayıcının sızma testleri *(penetration testing)* yapıp yapmadığına ve bunların sonuçlarını paylaşıp paylaşmadığına bakılmalıdır. Bulut hizmeti sağlayıcının yedekleme ve veri kurtarma konusunda planlamasının olup olmadığına bakılmalıdır[134]. Tüm bunların yanı sıra bulut hizmeti sağlayıcının piyasadaki tanınırlığı ve güvenirliliğine de bakılmalıdır[135]. Bulutta saklanan ticari sırların güvenliği hizmet sağlayıcının sağladığı güvenlik seviyesi kadardır. Dolayısıyla bulutta ticari sırların saklanması için teknik ve hukuki açıdan konunun dikkatlice araştırılması ve anlaşılmasından sonra bulut kullanımına yönelmek ve hizmet sağlayıcıyı seçmek gerekir[136].

Ticari sırların buluta yüklenmesi durumunda verilerin tam olarak nerede olduğunu tacir bilmek isteyebilir. Bu nedenle bulut bilişim sözleşmesinde verilerin saklanacağı yer ile ilgili olarak taahhütlerde bulunması hizmet sağlayıcıdan istenebilir. Zira herhangi bir veri ihlali olması durumunda örneğin bulut hizmeti sağlayıcının çalışanının kullanıcının verilerini ele geçirmesi durumunda verilerin saklandığı yerin hukukuna göre veri korumaya uygulanacak olan kurallar belirlenir[137].

Uygulamada yabancı bir ülkede yerleşik hizmet sağlayıcıların önceden hazırladıkları bulut bilişim sözleşmelerinde genellikle yabancı bir hukuku yetkili hukuk olarak tespit ettikleri görülmektedir. Bu bakımdan Türkiye'de yerleşik bir tacirin yabancı bir bulut hizmeti sağlayıcı ile sözleşme yapması ve sözleşmede yetkili hukuk tespiti yapılması durumunda tacir olan bulut kullanıcıları açısından sözleşmedeki hukuk seçimine ilişkin şart geçerli olacaktır[138]. Bu nedenle bulutta saklanan ticari sır niteliğindeki verilere yönelik herhangi bir ihlal durumunda sözleşmeye yetkili yabancı hukuk uygulanacaktır. Bulut kullanacak tacirlerin sözleşmeyi onaylamadan önce sözleşmeye hangi hukukun uygulanacağı hususunu da göz önünde tutmaları ileride herhangi bir mağduriyet yaşamamaları açısından önemlidir.

---

134 **GOWEN/SCHWARTZ/Cohn LLP,** s.2.

135 **GOTHING, Andrea A./NORTROP, Seth A./ZHU, Li,** "Keeping secrets in the cloud: Are storms ahead for trade secret protection?", InsideCounsel.com, February 26, 2015; Thayer/Yang, s.3.

136 **THAYER/YANG,** s.3.

137 **THAYER/YANG,** s.3.

138 Doktrinde *GÜNGÖR,* tıklanarak kabul yapılan sözleşmelerde kullanıcının hukuk seçimine yönelik gerçek anlamda iradesinin ve rızasının olduğundan söz edilemeyeceğini, kullanıcının esas sözleşmeye gösterdiği rızanın hukuki sonuçlarını bilmediği hukuk seçimi anlaşmasını da kapsayacak şekilde anlaşılmaması gerektiğini belirtmektedir. **GÜNGÖR, Gülin,** "Yeni Düzenleme Çalışmalarında Elektronik Akitlerin Kuruluşu ve Click-Wrap Yazılım Lisansı Sözleşmelerinde Hukuk Seçimi Kaydı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Y.2002, C.51, S.1, s.36-37.

Bulut hizmeti sağlayıcı ile sözleşme yapmadan önce dikkat edilmesi gereken bir diğer husus ise siber risk sigortasının olup olmadığıdır. Bulut hizmeti sağlayıcının siber risklere karşı sigortasının olması da değerli ticari sırların saklanması için seçilecek bulut hizmetinde belirleyici olabilir[139].

Ticari sırların bulutta saklanması tercih edilecekse gizliliğin korunması bakımından dikkat edilecek hususlardan biri de seçilecek bulut hizmetinin türüdür. Bulut kullanımında seçilecek bulut hizmet modelinin türü hizmet sağlayıcının buluttaki ticari sır niteliğindeki verilere erişimini etkilemektedir. Bazı bulut hizmeti sağlayıcılar kendi cihazlarında saklanan verilerin niteliğini, ne derece önemli olduğunu bilmeyebilir. Doktrinde bunları verilerin niteliğini bilen hizmet sağlayıcılar ile aynı yükümlülüklere tabi tutmanın isabetli olmayacağı belirtilmiştir[140].

Altyapı hizmeti veren (IaaS) bulut hizmeti sağlayıcılar genellikle veri depolama ve veri işleme donanımını kontrol edebilmektedir. Yazılım hizmeti (SaaS) veren bulut hizmeti sağlayıcılar kullanıcılar tarafından yürütülen temel uygulama kodlarını kontrol edebilmektedir. Bununla birlikte bulutta veriler şifrelenerek saklanabilir ya da parçalara ayrılarak saklanabilir. Sadece kullanıcının oturum açarak bunları birleştirebildiği durumda ticari sırrın gizliliğinin korunması bakımından gerekli önlemlerin alındığı düşünülebilir. Bir diğer husus da bulut hizmeti sağlayıcının alt hizmet sağlayıcılardan yardım almasıdır. Bulut hizmeti sağlayıcının depolamada veya diğer hizmetlerin sağlanmasında alt hizmet sağlayıcılardan yardım alıp almadığı da incelenmelidir. Örneğin verilerin saklanmasında bir alt hizmet sağlayıcının sunucuları kullanılabilir. Alt hizmet sağlayıcının kullanıcının hesabı üzerinde asıl hizmet sağlayıcıdan daha az kontrolü vardır. Bununla birlikte tacir, bulut bilişim sözleşmesinin yapılması sırasında alt hizmet sağlayıcılara ilişkin bir hükmün de sözleşmeye konulmasına dikkat edebilir[141]. Hangi hizmet modeli olursa olsun bulut hizmeti sağlayıcının aldığı güvenlik önlemleri, uygulamalar ve politikalar konusunda taciri bilgilendirmesi ticari sırların gizliliğinin sağlanması bakımından yardımcı olacaktır[142].

---

139 **THAYER/YANG,** s.3.

140 **HON, W. Kuan/HÖRNLE, Julia/MILLARD, Christopher,** Which Law(s) Apply to Personal Data in Clouds?, Cloud Computing Law, Editor Christopher Millard, Oxford University Press, Croydon 2013, s.244.

141 **BOZKURT YÜKSEL,** Bulut Bilişim, s.146-147, dn.25; **HON, W. Kuan/MILLARD, Christopher/ WALDEN, Ian,** "Who is Responsible for Personal Data in Clouds?", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.210.

142 Kişisel veriler bakımından durumun incelemesi için bkz. **HON/MILLARD/WALDEN,** s.215.

b. Sözleşmenin Şartlarında Dikkat Edilecek Hususlar

Bulut bilişim sözleşmeleri genellikle önceden hazırlanmış standart sözleşmeler şeklinde yapılmaktadır. Bu sözleşmeler uygulamada çoğunlukla elektronik ortamda ana sözleşme metni yanında müşterinin/kullanıcının ekranda gördüğü bir kabul et yazısı yanındaki kutucuğu işaretlemesi/ tıklaması ile gerçekleşmektedir[143]. Burada ana sözleşme metni dışındaki bu alt metinlerin ana sözleşmenin parçasını oluşturup oluşturmadığı sorunu gündeme gelmektedir. Eğer alt sözleşme metinleri ana sözleşmenin parçası olarak kabul edilebilirse burada yazılı standart şartların kullanıcıları bağlayıp bağlamayacağı sorunu bu sefer cevap beklemektedir[144].

Sözleşmedeki şartların hizmet sağlayıcı tarafından daha sonra tek taraflı olarak değiştirilebilmesi söz konusu olabildiğinden yeni şartların geçerliliği ile ilgili tartışmalar vardır. Zira genellikle genel işlem şartları şeklinde hazırlanan bu sözleşmelerdeki değişikliklerin kullanıcılar ile müzakere edilmeden tek taraflı olarak değiştirilmesi ile bu şartlar sözleşme içeriğine girmemiş sayılır. Ayrıca kullanıcının yeni durumu kabul ettiğine ilişkin bir kutucuğu tıklatması istenirse bunun da geçerliliğinin tartışmalı olacağı, hizmetten yararlanan müşteriler aleyhine değişikliklerin yazılmamış sayılmasının gerektiğine ilişkin görüşler de mevcuttur[145].

Standart sözleşmeler tacirin ticari sırlarının korunması bakımından yeterli görülmezse burada özel olarak bir sözleşme hazırlanması düşünülebilir. Tacirin bir bulut kullanıcısı olarak hizmet sağlayıcı ile sözleşme şartlarını müzakere etmesi, kullanıcıya özel sözleşme yapacak bir bulut hizmeti sağlayıcı ile çalışması durumunda ticari sır sahibi tacirin ihtiyaçlarına göre sözleşme şartları hazırlanabilir. Bulut bilişim teknolojisinde gelişmeler ve rekabet arttıkça bu alanda kullanıcıya özel sözleşmelerin kullanımının artması muhtemeldir. Elbette burada bulut hizmeti sağlayıcının güvenirliği, veri saklama hususundaki tecrübesi ve sektördeki bilinirliği de dikkate alınmalıdır[146]. Sözleşmeden doğacak uyuşmazlıklar için tahkim şartı da sözleşmeye konulabilir. Böylelikle bilişim ve teknoloji hukuku alanında uzman bir hukukçu ve/veya bulut bilişim

---

143 Tıklanarak yapılan sözleşmeler için *click wrap agreement* terimi kullanılmaktadır. Bir de *browse wrap agreement* denilen gözden geçirilerek yapılan sözleşmeler vardır. Gözden geçirilerek yapılan sözleşmelerin geçerliliği konusunda doktrinde tartışmalar vardır. **ORGAN, Shawn J./CORCORAN, Matthew C.,** "Your Web Site's 'Terms of Use': Are They Enforceable?", Privacy & Data Security Law Journal, 2008, http://www.jonesday.com/files/Publication/97a326a1-0077-4fc9-ac81-e82c265d0c82/Presentation/PublicationAttachment/a882327c-e026-49bf-91fb-ee3f9ca21ac0/Terms%20of%20Use.pdf (Erişim 05.01.2016).

144 **BAŞGÜL/CHOUSEİNOGLOU**, s.211.

145 **BAŞGÜL/CHOUSEİNOGLOU,** s.212.

146 **THAYER/YANG,** s.2.

alanında uzman bir teknisyen hakem olarak seçilebilir[147]. Ayrıca tahkimin özel bir yargılama olması ve tahkim yargılamasının gizlilik özelliği yargılama sırasında açığa çıkan ticari sırların korunması bakımından devlet yargılamasından daha avantajlıdır[148]. Burada tacirin bulut bilişim sözleşmesini yapmadan önce bilişim ve teknoloji hukuku alanında uzman bir hukukçudan görüş alması sözleşmenin olası sonuçları açısından isabetli olacaktır.

- Bulut Hizmeti Sağlayıcının Sorumluluğuna İlişkin Şartlar

Günümüzde dünya çapında en bilinen bulut hizmeti sağlayıcıları olan Amazon, Google, Microsoft, Dropbox'un sözleşme şartları incelendiğinde bulut hizmeti sağlayıcıyı oldukça koruyan şartlar içerdikleri görülecektir. Örneğin, bu standart sözleşmelerde genellikle, veri gizliliğinin ya da güvenliğinin garanti edilmediği, veri ihlali durumunda sorumluluğun bir şirketin riskini yeterli derecede karşılayamayacak olmakla birlikte sıklıkla bir aylık ya da bir yıllık hizmet değeri ile sınırlı olduğu görülmektedir[149].

Bulut hizmeti sağlayıcıları buluttaki verilerin üçüncü kişiler tarafından ele geçirilmesi ya da herhangi bir nedenle veri kaybı olmasında durumunda ya da hizmet kusuru durumunda sorumlu olmadıklarına ilişkin kayıtları sözleşmeye koyabilmektedirler[150]. Bulut bilişim sözleşmelerinde hizmet sağlayıcının sorumluluğunu ortadan kaldıran veya sınırlandıran sorumsuzluk anlaşmaları Türk Borçlar Kanunu'nun 115 ve 116. maddeleri karşısında geçersiz sayılabilir[151]. Ancak yine burada sözleşmeye uygulanacak hukuka göre yorum yapmak gerekebilecektir. Örneğin, Avrupa Birliği hukuk sistemi, Amerikan hukukuna nazaran taraflardan birinin özellikle daha güçlü olan tarafın sorumluluğunun sınırlandırılmasına ya da kaldırılmasına ilişkin sözleşme şartları konusunda daha az toleranslıdır. Bu durum özelikle 93/13 sayılı Haksız Sözleşme Şartları Direktifi *(Unfair Contract Terms Directive)* ve 97/7 sayılı Mesafeli Satış Direktifi'nde *(Distance Selling Directive)* tüketici işlemleri hakkında yer almaktadır[152].

---

147 **BOZKURT YÜKSEL, Armağan Ebru,** "Online International Arbitration", Ankara Law Review, Vol.14, No.1, Summer 2007, s.83-93, http://dergiler.ankara.edu.tr/dergiler/64/1542/16895.pdf (Erişim 25.11.2016); **BOZKURT YÜKSEL, Armağan Ebru**, "Elektronik Ticarette Elektronik Alternatif Uyuşmazlık Çözümü", Mevzuat Dergisi, Yıl 11, Sayı 123, Mart 2008, http://www.mevzuatdergisi.com/2008/03a/02.htm (Erişim 25.11.2016).

148 Tahkim yargılaması sırasında açığa çıkan ticari sırlar ve gizli bilgilerin durumu hakkında ayrıntılı açıklama için bkz. **BOZKURT YÜKSEL,** Patent Uyuşmazlıkları, s.256 vd.

149 **THAYER/YANG,** s.2.

150 **LAW SOCIETY,** http://lawsociety.org.uk/advice/practice-notes/cloud-computing/ (Erişim 18.11.2014).

151 **BAŞGÜL/CHOUSEİNOGLOU,** s.212.

152 **BRADSHAW, Simon/MILLARD, Christopher/WALDEN, Ian,** "Standard Contracts for Cloud Services", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.66.

Bulut hizmeti sağlayıcının ve onun alt hizmet sağlayıcılarının[153] sorumluluklarının kaldırılmasına ilişkin sorumsuzluk anlaşmalarının her zaman geçerli olmayacağını ifade etmek gerekir. Türk Borçlar Kanunu'nun 115. maddesi uyarınca borçlunun kast veya ağır kusurundan doğan sorumluluktan kurtulmasını öngören anlaşmalar kesin olarak hükümsüzdür. Ancak hafif kusurundan dolayı borçlunun sorumsuzluğu kararlaştırılabilir. Bulut bilişim açısından maddenin uygulanmasında bulut hizmeti sağlayıcıların verilerin ve sistemin korunmasına ilişkin kast veya ağır kusurundan sorumsuzluğuna ilişkin anlaşmalar geçersiz olacaktır. Herhangi bir uyuşmazlık durumunda kusurun derecesinin belirlenmesinde teknik bilirkişi raporu verilerin (buluttaki ticari sırların) korunması için gerekli ve yeterli önlemlerin alınıp alınmadığının değerlendirilmesinde yardımcı olabilir[154].

Türk Borçlar Kanunu'nun 116. maddesinde *"Borçlu, borcun ifasını veya bir borç ilişkisinden doğan hakkın kullanılmasını, birlikte yaşadığı kişiler ya da yanında çalışanlar gibi yardımcılarına kanuna uygun surette bırakmış olsa bile, onların işi yürüttükleri sırada diğer tarafa verdikleri zararı gidermekle yükümlüdür. Yardımcı kişilerin fiilinden doğan sorumluluk, önceden yapılan bir anlaşmayla tamamen veya kısmen kaldırılabilir. Uzmanlığı gerektiren bir hizmet, meslek veya sanat, ancak kanun veya yetkili makamlar tarafından verilen izinle yürütülebiliyorsa, borçlunun yardımcı kişilerin fiillerinden sorumlu olmayacağına ilişkin anlaşma kesin olarak hükümsüzdür."* hükmü yer almaktadır. Buradaki yardımcı kişi borcun ifasının veya borç ilişkisinden doğan hakkın kullanılmasının bırakıldığı bütün şahısları ifade etmektedir. Borçlunun emri altında çalışma ilişkisinin varlığı zorunlu değildir. Borcun ifasının kendisine bırakıldığı kişinin yardımcı kişi sayılması, bu kişi ile borçlu arasında sürekli bir ilişkinin varlığına da bağlı değildir. Borcun ifası geçici veya ücretsiz olarak kendisine bırakılan kimse de yardımcı şahıstır[155]. Borçlunun yardımcı kişilerin fiilinden –kast veya ihmalinden- doğacak zarardan kısmen veya tamamen sorumlu olmayacağına ilişkin önceden yapılan anlaşmalar geçerlidir[156]. Bulut hizmeti sağlayıcının alt hizmet sağlayıcıların fiillerinden sorumlu olmayacağına ilişkin kayıtlar bu madde kapsamında değerlendirildiğinde geçerlidir.

Türk hukukunda borçlu, ifa imkânsızlığının (TBK m.136), ifanın gereği gibi yapılmamasının, kendisine yüklenemeyecek hallerin yani sorumlu tutulamayacak sebeplerin sonucu olduğunu ispat edebilirse, borcun ifa

---

153 Bulut hizmet sağlayıcılar alt hizmet sağlayıcılardan yardım alabilirler. Örneğin bulut hizmet sağlayıcısı başkasına ait sunucuları kullanarak bulut hizmeti verebilir. Alt hizmet sağlayıcılar hakkında geniş bilgi için bkz. **BOZKURT YÜKSEL,** Bulut Bilişim, s.138 vd.

154 **BOZKURT YÜKSEL,** Bulut Bilişim, s.155-156.

155 **REİSOĞLU, Safa,** Türk Borçlar Hukuku Genel Hükümler, Beta Yayınevi, 23.B., İstanbul 2012, s.361 vd.

156 **REİSOĞLU,** s.364.

edilmemesinde kusursuzluğunu kanıtlamış olur ve sorumluluktan kurtulur. Borcun ifasını engelleyen ve borçluya yüklenemeyecek olaylar beklenmeyen hal veya mücbir sebep (önlenemez neden) sonucu olabilir. Mücbir sebep veya beklenmedik hal nedeniyle borç ifa edilemezse borçlu sorumlu değildir[157]. Örneğin bulut bilişimde verilerin saklandığı sunucuların depremde zarar görmesi nedeniyle kullanıcının verilerine ulaşamaması durumunda bulut hizmeti sağlayıcı mücbir sebep söz konusu olduğundan sorumluluktan kurtulabilir. Ancak burada da bulut hizmeti sağlayıcının verileri yedeklemesi gerektiğine ilişkin sorunlar gündeme gelebilir. Bu itibarla bulut bilişim sözleşmesinde verilerin yedeklenmesine ilişkin düzenlemenin yer alması yerinde olur[158].

Bir kişinin sorumlu olduğu fiil ile bir başkasına yansıyan zarar arasındaki sebep sonuç ilişkisi doğrudan varsa burada doğrudan zarar söz konusudur. Buna göre zarar veren fiille uygun nedensellik bağı içerisinde olan her zarar doğrudan zarardır. Dolaylı zarar ile bir fiil neticesinde kişinin dolaylı olarak uğradığı zarar ifade edilir[159].

Haksız fiilden ya da borca aykırılık nedeniyle oluşan doğrudan zarardan zarar veren sorumludur. Ancak dolaylı zarardan sorumluluk için uygun nedensellik bağının kurulması gerekir. Dolaylı zarardan sorumluluğun olup olmaması nedensellik bağıyla ilgili bir problemdir. Zarar veren fiil ile uygun sebep sonuç/nedensellik bağı varsa dolaylı zararın da giderilmesi gerekir[160].

Bulut bilişim açısından bakıldığında ise bulut hizmeti sağlayıcının sözleşmeyi ihlal etmesi durumunda bulut kullanıcısının uğradığı zarar doğrudan zarardır ve bu zarardan bulut hizmeti sağlayıcı sorumludur. Dolaylı zarar da bulut bilişimde söz konusu olabilir. Bulut hizmeti sağlayıcının sözleşmeyi ihlal etmesi halinde, örneğin bulutta saklanan İnternet üzerinden satış yapan bir şirketin perakende sisteminin işleyişi ile ilgili bir veri silinirse şirketin uğrayacağı ekonomik zarar dolaylı zarardır[161]. Burada verinin silinmesi ile sistemin işleyişinin kötüleşmesi ve şirketin satışlarının düşmesi arasında nedensellik bağı olduğundan bu dolaylı zarardan da bulut hizmeti sağlayıcı sorumludur.

---

157 Her mücbir sebep beklenmeyen haldir. Ancak her beklenmeyen hal mücbir sebep değildir. Mücbir sebepte ifayı engelleyen olay borçlunun işletme ve faaliyetleriyle ilgisi olmayan bir dış kuvvetin etkisiyle meydana gelir. Buna göre bir fabrikada kazanın patlaması ya da yangın çıkması olayda borçlunun kusuru yoksa beklenmeyen haldir. Ancak yıldırım düşmesi, deprem, kuraklık, fırtınada mücbir sebep söz konusudur. **REİSOĞLU,** s.357-358.

158 **BOZKURT YÜKSEL,** Bulut Bilişim, s.155-157.

159 ÖZEL, Çağlar, "Sözleşme Dışı Sorumlulukta Yansıma Zarar ve Giderimine İlişkin Bazı Düşünceler", AÜHFD, C.50, S.4, Y.2001, s.83.

160 ÖZEL, s.83.

161 Bulut hizmeti sağlayıcıların genellikle dolaylı zararlardan da sorumlu olmadıklarına ilişkin hükümleri sözleşmeye koyma eğiliminde oldukları uygulamada görülmektedir. **BRADSHAW/MILLARD/WALDEN,** s.60.

Bulut hizmeti sağlayıcı bulut bilişim sözleşmesinde veri kaybı veya veri ihlali durumunda belli bir miktar para ile sorumlu tutulabilir. Ancak hiçbir ücret ödenmeden yararlanılan bir bulut hizmeti neticesinde veri kaybı durumunda hizmet sağlayıcıyı yüksek meblağlar ile sorumlu tutmak pratik açıdan pek mümkün görünmemektedir.

- Gizliliğin Korunmasına İlişkin Şartlar

Ticari sırların bulutta saklanması için yapılacak sözleşmede dikkat edilmesi gereken hususlardan biri gizliliktir. Ticari sırların bulutta saklanması örneğin bir şirketin ticari sırrını içeren dosyayı buluta yüklemesi durumunda ticari sırrın gizliliğinin korunması için gerekli önlemlerin alınmasına tacir dikkat etmelidir. Ticari sırrın sahibi tacir, sırrı verdiği kişilere bilginin gizli olduğunu ve açıklanmaması gerektiğini bildirmelidir. Bir bulut bilişim sözleşmesi yapılacaksa hizmet sağlayıcının gizlilik yükümlülüğüne ilişkin düzenlemenin sözleşmede bulunmasına dikkat etmelidir. Bilginin gizliliğinin korunmaması bilginin ticari sır niteliğinin kaybedilmesine neden olabilecektir.

Ticari sırların bulut hizmeti sağlayıcıya açıklanmasının ticari sırların gizliliğinin korunması hususunda gerekli çabanın gösterilmemesi anlamına gelip gelmediği yargılama sırasında tartışma konusu olabilir. Bulut hizmeti sağlayıcıya bilgileri görme, kullanma veya açıklama yetkisi veren şartların bulunduğu sözleşmeler bakımından artık bir ticari sırrın varlığından söz etmek mümkün değildir. Bir başka husus ise üçüncü bir kişinin bulut hizmeti sağlayıcıdan kayıtları almak istemesi durumunda ne olacağı ile ilgilidir. Örneğin bulut hizmeti sağlayıcı ticari sırların açıklanmasını gerektiren bir mahkeme emri aldığında bulunduğu ülkenin kuralları uyarınca bunun gereğini yerine getirmek durumunda kalabilir[162]. Yurt dışında bulunan bir bulut hizmeti sağlayıcının hizmetinden yararlanılması durumunda yabancı devlet makamlarının o bulut hizmeti sağlayıcıdan verileri istemesi ve bu verileri elde etmesi söz konusu olabileceğinden yabancı hizmet sağlayıcı seçiminde bu hususu gözönüne tutmakta fayda vardır.

Ticari sır sahibinin ticari sır niteliğindeki verileri buluta yüklemeden önce gizlilik anlaşması yapması önerilmektedir. Bulut kullanıcısının hizmet sağlayıcıyla gizlilik anlaşması yapması karşısında verilerin buluta yüklenmesi artık ticari sırların herkesçe bilindiği anlamına gelmeyecektir[163]. Ayrıca ticari sır sahibinin gerek kendi çalışanları tarafından gerekse bulut hizmeti sağlayıcı tarafından gizliliğin korunması hususunda gerekli çabanın gösterildiğinden emin olması gerekir[164]. Üçüncü kişilere açıklanan ticari sırlar eğer üçüncü

[162] **GELLMAN,** s.16.
[163] **DHULIA,** s.29.
[164] **SANDEEN,** s.59.

kişinin gizliliği sağlama yükümlülüğü yoksa korumayı kaybeder. Ticari sırlar bulutta saklanacaksa bulut bilişim sözleşmesinde açıkça yazılı olarak bulut hizmeti sağlayıcının ticari sırları sakladığını bildiğinin ve bu bilgilerin gizliliğini koruyacağı hususunun yer alması gerekir. Bulut hizmeti sağlayıcının bunları kabul etmemesi durumunda tacirin riske etmek istemediği bilgileri belirlemesi ve onları bulutta saklamaması gerekir[165].

Ticari sırlarını bulutta saklamayı tercih eden ticari sır sahibinin bilgilerin gizliliği hususunda gerekeni yaptığı ancak gerekli güvenlik önlemleri alınmışsa söylenebilir[166]. Ticari sır sahibinin gizliliğin sağlanması için yaptığı harcamalar bu konuda gösterdiği gayretin bir ölçüsüdür. Ticari sırların korunması için son teknolojinin kullanılması örneğin şifreleme yöntemlerinin kullanılması veya güvenlik duvarı *(firewall)* kurulması için yapılan harcamalar son kullanıcının bu konuda gayretinin bir göstergesidir[167]. Bunların dışında bulut bilişim sözleşmesinde bulut hizmeti sağlayıcının tersine mühendislik yapmasını yasaklayan düzenlemeler olması da önerilmektedir[168]. Sözleşmede veri ihlali veya sistemin çökmesi durumunda tacirin derhal durumdan haberdar edileceğine ilişkin düzenlemenin olmasına da dikkat edilmelidir[169].

- Sözleşmenin Sona Ermesi Halinde Ticari Sırlara Ne Olacağına İlişkin Şartlar

Bulut sözleşmelerinin sona ermesi durumunda bulutta saklanan verilere ne olacağı ile ilgili sorunlar olabilir. Bu durumda saklanan verinin geri verilmesi veya silinmesi gündeme gelecektir. Özellikle bir hizmet olarak yazılım (SaaS) hizmet modelinde sözleşmenin sona ermesi ile birlikte hizmet sağlayıcının kullanıcıya sağladığı yazılım desteği de sona ereceğinden hizmet kullanıcısı ticari sır niteliğindeki verilerini alsa da kullanamama, görüntüleyememe, işleyememe riski ile karşılaşabilir. Bu nedenle bulut bilişim sözleşmesi sona erdiğinde bu verilerin en azından görüntülenebilmesi, yeni dosyalar oluşturulamasa da en azından değiştirilebilmesi imkânının sağlanacağının sözleşmeye konulması önerilebilir. Yine verilerin bulut bilişim sözleşmesi sona erdikten sonra başka bir hizmet sağlayıcının bulutunda saklanabilecek ve işlenebilecek formatta teslim edilmesine ilişkin düzenlemelerin de sözleşmede bulunması önerilebilir[170]. Sözleşme sona erdikten sonra da ticari sırların gizliliğinin korunmasına devam edilmesi gerekmektedir. Bu itibarla sözleşmenin sona ermesi durumunda bulutta saklanan verilerin silinmesine ilişkin sözleşmede düzenleme

165 **THAYER/YANG,** s.3.
166 **DHULIA,** s.32.
167 **DHULIA,** s.28.
168 **DHULIA,** s.41; Tersine mühendisliğin sözleşmeyle kaldırılması hakkında bkz.**BİLGE,** s.214.
169 **GOWEN/SCHWARTZ/Cohn LLP,** s.2.
170 **BAŞGÜL/CHOUSEİNOGLOU,** s.213-214.

olmalıdır[171]. Böyle olamıyorsa bulut hizmeti sağlayıcı ile yapılan sözleşmede gizliliğin korunması ile ilgili yükümlülüğünün sözleşmenin sona ermesinden sonra da devam edeceğine ilişkin düzenlemenin yer alması dikkat edilmesi gereken bir hususdur. Nitekim lisans sözleşmelerinden bir örnek vermek gerekirse *Cadbury Schweppes v. FBI Foods Limited* davasındaki olayda lisans veren lisans sözleşmesi kapsamında ticari sır teşkil eden domates kokteylinin tarifini vermiştir. Lisans sözleşmesinin sona ermesinden sonra lisans alan bu tarifi rakip teşkil edecek bir ürünün geliştirilmesinde kullanmıştır. Mahkemece lisans sözleşmesi süresince ve sona ermesinden sonra da lisans alanın ticari sırrın korunması yükümlülüğünün olduğuna hükmedilmiştir[172].

c. Bulut Kullanımında Gizliliğin Korunması Bakımından Dikkat Edilecek Hususlar

Bulut kullanırken ticari sır sahibi tacirin bir bulut kullanıcısı olarak dikkat etmesi gereken hususlar vardır. Parola seçimi ve parolanın korunması en başta gelen hususlardır. İşletmedeki yetkisiz çalışanlarca parolaların ele geçirilmesi veya başka şekilde ihlaller söz konusu olabilir. Bilgisayar korsanları da*(hacker)* özellikle zincirdeki en zayıf halkayı yakalamak suretiyle verileri ele geçirmeye çalışmaktadırlar. Bu itibarla işletme içinde güvenlik politikalarının oluşturulması gerekmektedir. Bu anlamda ticari sırların sadece bilmesi gereken personel tarafından erişimine izin verilmesi gerekmektedir. Bunun yanında işletmelerde akıllı telefonlar ve sosyal ağlarla ilgili politikalar oluşturulması ve bunların da çalışanlarla ilgili sözleşmelere yansıtılması gerekir. Böylelikle çalışanların işletmeyle veya şirketle ilgili bilgileri yetkisiz bir şekilde bulutta saklamasının ve paylaşmalarının önüne geçilmiş olur[173]. Ticari sırlar bulutta saklanacaksa ticari sır sahibinin bunları buluta yükledikten sonra buluta erişim yetkisine sahip çalışanların kim olduğuna ve bunların denetimine, ayrıca bunların verileri buluta yüklerken şifrelemelerine dikkat etmesi gerekir. Buluta erişen personel belirli, deneyimli kişiler olmalıdır. Bunların günlük olarak buluta girişlerinin kaydının tutulması, raporlanması gerekir. Buluttaki verilerde herhangi bir değişiklik yapmaları durumunda bunların dijital imzalarla gerçekleşmesi tavsiye edilebilir[174].

Ticari sır sahibinin bulutta saklanan verilere sadece yetkili kişilerin ulaşabilmesi için gerekli tedbirleri alması gerekir. Eğer bulut hizmeti sağlayıcı paylaşılan bir sunucuda saklanan ticari sır niteliğindeki verilere üçüncü kişilerin de erişimini mümkün kılarsa o veriler ticari sır niteliğini kaybedebilecektir.

---

171 **THAYER/YANG,** s.3.

172 Cadburry Schweppes v. FBI Foods Limited kararı için bkz. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1678/index.do (Erişim 24.11.2016).

173 **THAYER/YANG,** s.3

174 **THAYER/YANG,** s.3.

Erişim kontrol güvenliği bulut hizmeti sağlayıcıya düşen bir yükümlülüktür. Ancak ticari sır sahibinin de yeterli derecede erişim kontrolü sağlayan bir bulut hizmeti sağlayıcı seçme hususunda özen göstermesi gerekir. Her ne kadar taraflar arasında gizlilik sözleşmesi yapılmış olsa da kullanıcı olarak ticari sır sahibi hiçbir zaman tam olarak emin olmadıkça ticari sırrın korunmasını bulut hizmeti sağlayıcıya bırakmamalıdır[175].

D. Ticari Sırların Bulutta Saklanması ve Haksız Rekabet

Ticari sırların bulutta saklanması ve gizliliğinin korunması konusu haksız rekabet ile de ilgilidir. Bulutta saklanan ticari sırların bulut hizmeti sağlayıcı tarafından yetkisiz olarak kullanılması fiili haksız rekabet teşkil edebilir. Türk Ticaret Kanunu'nda düzenlenmiş olan haksız rekabet hallerinden madde 55(1)(c)(1)'de yer alan *"kendisine emanet edilmiş teklif, hesap veya plan gibi bir iş ürününden yetkisiz yararlanmak"* şeklindeki hüküm böyle bir durumda gündeme gelebilir. Bir teklif, hesap ya da planın teknik olarak ticari sır olmasına engel bulunmadığından, eğer bunlar buluta yüklendikten sonra, bulut hizmeti sağlayıcının saklaması için kendisine emanet edilen bu bilgilerden yetkisiz olarak yararlanması söz konusu olursa bu davranış haksız rekabet teşkil edebilecektir. Örnek olarak bu bilgilerin bulut hizmeti sağlayıcı tarafından rakip tacirlere satılması ya da kendisi için kullanması gösterilebilir.

Türk Ticaret Kanunu'nun 55(1)(c)(1) maddesindeki düzenlemenin uygulanması için iki koşul gerekmektedir. Bunlardan ilki iş ürünlerinin emanet olarak bırakılmasıdır. Buna göre iş ürünleri hukuka aykırı olarak elde edilmemiş olmalıdır[176]. Kanundaki emanet edilmiş ifadesinden saklama sözleşmesinin kastedilmediği, iş ürünlerinin hak sahibinin kendi iradesiyle ancak yararlanılmaması koşuluyla verdiği tüm durumların bu kapsamda değerlendirileceği belirtilmektedir[177]. İkinci koşul ise iş ürünlerinin emanet edildiği kişinin bunlardan yetkisiz olarak yararlanması, kendisine olan güveni kötüye kullanmasıdır[178]. Bu iki koşulun ticari sırların bulutta saklanması durumunda gerçekleşmesi mümkündür. Tacir teklif, hesap planı gibi ticari sırlarını bulutta depolamak isteyebilir. Bu itibarla bulut hizmeti sağlayıcıyla bir sözleşme yapmak suretiyle ticari sırlarını buluta gönderebilir. Bulut bilişim sözleşmesi saklama sözleşmesinin de unsurlarını içeren karma bir sözleşmedir. Bu itibarla ilk koşul gerçekleşmiştir. Bulut hizmeti sağlayıcı bu anlamda sakladığı ticari sırları hukuka uygun olarak elde etmiş bulunmaktadır. Yetkisiz kullanım

175 **DHULIA,** s.25.

176 ŞENER, Ticari İşletme, s.641; **KARAHAN, Sami,** Ticari İşletme Hukuku, 21.B., Konya 2011, s.217.

177 ŞENER, Ticari İşletme, s.641; ÇAPA, M.Sadık, "Haksız Rekabet Hukukunda Başkalarının İş Ürünlerinden Yetkisiz Yararlanma", Ankara Barosu Dergisi, 2014/2, s.365-366.

178 ÇAPA, s.367.

koşulu da yine hizmet sağlayıcı ile tacir arasında yapılan sözleşmenin içeriğine göre belirlenebilir. Bulutta saklanan verileri kullanma yetkisi bulut hizmeti sağlayıcıya verilmemişse bu durumda bulut hizmet sağlayıcının yetkisiz olarak ticari sır niteliğindeki verileri kullanmasıyla haksız rekabet gerçekleşmiş olur.

Tacirin bulut bilişim sözleşmesinde hizmet sağlayıcıya verilere erişim yetkisi vermediği halde, hizmet sağlayıcının buluttaki verilerinin içeriğini ifşa etmesi ya da tacirin şifreleyerek buluta yüklediği üretim ve iş sırlarını izinsiz olarak deşifre etmek suretiyle değerlendiren veya başkalarına bildiren bulut hizmeti sağlayıcının fiili Türk Ticaret Kanunu'nda düzenlenen haksız rekabet hallerinden madde 55(1)(d)'yi düşündürebilir. Zira madde 55(1)(d) maddesindeki hüküm "üretim ve[179] 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 davranışmış olur." şeklindedir. Türk Ticaret Kanunu'nun 55(1)(d) maddesi anlamında iş sırrı uzun ve masraflı bir çalışma sonucunda elde edilebilen bilgileri ifade eder. Sırrın mutlaka yeni olmasına gerek yoktur. Bu itibarla know-how niteliğindeki bilgiler, isim adres bilgileri yanında başka bazı bilgileri de içeren müşteri listeleri kanundaki iş sırrı kapsamına dâhil olacaktır[180]. Yargıtay, bir kararında bir çalışanın bir şirkette çalışırken müşteri potansiyeli ve pazarlama ağını öğrenip, şirketten ayrıldıktan sonra başka bir şirket kurarak bu bilgileri orada kullanmasını 55(1)(d) anlamında haksız rekabet olarak değerlendirmiştir[181]. Bulutta saklanan üretim ve iş sırları bakımından bulut hizmeti sağlayıcının tacir ile yaptığı bulut kullanımına ilişkin sözleşme sona erdikten sonra[182] bulutta saklanan üretim ve iş sırlarını kullanması bu madde kapsamında değerlendirilebilecektir. Yine bulut kullanımına ilişkin sözleşmede bulut hizmeti sağlayıcının bulutta

---

179 Maddede ve bağlacı kullanılmakla birlikte veya olması gerektiği hakkında ŞENER, Ticari İşletme, s.644.

180 **ARKAN, Sabih,** Ticari İşletme Hukuku, 23.B., Ankara 2017, s.349 ve dn.4'te anılanlar; ŞENER, Ticari İşletme, s.644.

181 Y.11.HD, T.07.10.2004, E.13172, K.9423 (ŞENER, Ticari İşletme, s.644, dn.354).

182 Bulut hizmeti sağlayıcı verinin kaybı riskine karşılık verinin pek çok kopyasını almış olabilir. Kullanıcının verileri buluttan başka bir yere aktarmak istemesi durumunda hizmet sağlayıcıya ait farklı yerlerdeki sunucularda saklanan verinin kopyaları otomatik olarak silinmez. Bu itibarla bulut bilişim sözleşmelerinde tarafların haklarının ve yükümlülüklerinin sözleşmeden sonra da devam edeceğine ilişkin bir hüküm sözleşmede yer almalıdır. Hatta sözleşmenin sona ermesinden sonra buluttaki verilerin kopyalarının otomatik olarak silinmesine ilişkin bir hükmün de yer alması gerektiği doktrinde önerilmektedir. Ancak unutulmamalıdır ki bilgisayar ortamında silinen bir verinin tekrar geri getirilmesi mümkündür. Dolayısıyla bir verinin kopyalarıyla birlikte tamamen silinmesi başka bulut kullanıcılarının aynı sunucuda verilerinin saklanıyor olması nedeniyle her zaman mümkün olmayabilir. Burada bulut hizmeti sağlayıcının teknik olarak birtakım özel usulleri uygulaması gerekebilir. **DHULIA,** s.24.

saklanan üretim ve iş sırlarına erişiminin yasaklanması kararlaştırılmış ve hatta bu bilgilerin şifrelenmek suretiyle buluta gönderilmiş olması durumunda, üretim ve iş sırlarını gizlice ve izinsiz olarak ele geçirerek başkalarına bildirmesi veya kendisinin değerlendirmesi de haksız rekabet teşkil edebilecektir.

Türk Ticaret Kanunu'nun 55(1)(e) maddesinde yer alan *"iş şartlarına uymamak; özellikle kanun veya sözleşmeyle, rakiplere de yüklenmiş olan veya bir meslek dalında veya çevrede olağan olan iş şartlarına uymayanlar dürüstlüğe aykırı davranmış olur"* şeklindeki hüküm bulutta ticari sırların saklanmasında söz konusu olabilir. Şöyle ki, Türk Standartları Enstitüsü bulut bilişimde güvenlik ve standart taslağı üzerinde çalışmaktadır[183]. Bulut bilişim için oluşturulacak standartların mecburi hale getirilmesi durumunda bu standartlara uyulmadan bulut hizmeti verilmesi haksız rekabet teşkil edebilecektir. Zira standartlara uygun olarak güvenli bulut hizmeti veren rakiplere karşı haksız rekabette bulunulmuş olunacaktır.

Türk Ticaret Kanunu'nun 55(1)(f) maddesi *"dürüstlük kuralına aykırı işlem şartı kullanmak; özellikle yanıltıcı bir şekilde diğer taraf aleyhine doğrudan veya yorum yoluyla uygulanacak kanuni düzenlemeden önemli ölçüde ayrılan veya sözleşmenin niteliğine önemli ölçüde aykırı haklar ve borçlar dağılımını öngören önceden yazılmış genel işlem şartlarını kullananlar dürüstlüğe aykırı davranmış olur"* şeklindedir. Bu hüküm de ticari sırların bulutta saklanması durumunda gündeme gelebilir. Uygulamada bulut bilişim sözleşmeleri genellikle hizmet sağlayıcı tarafından önceden hazırlanmakta ve karşı tarafa sunulmaktadır. Hatta bu sözleşmeler çoğunlukta çevrimiçi olarak bir kutucuğunun tıklanması veya "kabul ediyorum" seçeneğinin tıklanması ile yapılmaktadır. Dolayısıyla kullanıcıların sözleşme şartlarını değiştirmeleri ya da müzakere etmeleri mümkün olamamaktadır. Bu itibarla bulut bilişim sözleşmesinde yer alan bulut hizmeti sağlayıcının bulutta saklanan ticari sırları dilediği gibi kullanabileceği, isterse satabileceği, isterse başkalarına açıklayabileceği ve karşı tarafın buna hiçbir şekilde itiraz edemeyeceği şeklindeki hükümler bu madde kapsamında haksız rekabet teşkil edecektir. Zira böyle hükümler ticari sırların bulutta saklanması durumunda bulut bilişim sözleşmesinin ekonomik amacına önemli ölçüde aykırı haklar ve borçlar dağılımı öngörmüş olacaktır. Burada Türk Borçlar Kanunu'nun 25.maddesi de gündeme gelebilecektir. Dürüstlük kuralına aykırı olarak karşı tarafın aleyhine veya onun durumunu ağırlaştırıcı nitelikte hükümler Türk Borçlar Kanunu'nun 25.maddesine göre kesin hükümsüzlük yaptırımına tabi olacaktır. Aynı zamanda Türk Ticaret Kanunu'nun 55(1)(f) maddesindeki şartların oluşması durumunda haksız rekabet davaları da açılabilecektir[184].

---

[183] Bulut bilişimde standartlar ve alınabilecek diğer güvenlik önlemleri hakkında detaylı bilgi için bkz.**BOZKURT YÜKSEL,** Bulut Bilişim, s.150 vd.

[184] **ŞENER,** Ticari İşletme, s.650.

SONUÇ ve ÖNERİLER

Ticari sırlar ister bulutta istenirse tacirin işletmesinde bulunan veri merkezinde saklansın teknolojinin kullanıldığı her durumda üçüncü kişilerce ticari sırların ele geçirilmesi riski vardır. Herhangi bir veri ihlali neticesinde ticari sırların üçüncü kişilerce öğrenilmesi durumunda tacirin gerek Türk Ticaret Kanunu'ndaki haksız rekabete ilişkin hükümlerden gerekse Türk Ceza Kanunu'ndaki hükümlerden yararlanması mümkündür. Ancak burada önceden hem teknik hem de hukuki tedbirlerin alınması çok önemlidir.

Ticari sırların daha ekonomik ve pratik olması, İnternet üzerinden her yerden veriye erişimin kolay olması nedeniyle bulutta saklanması tercih edilirse, burada da dikkat edilmesi gereken hususlar vardır. Bulut hizmeti alınacak olan kişinin dikkatli ve özenli seçilmesi, bu alanda güvenilir, tanınır hizmet sağlayıcılarla çalışılması önemlidir. Buluttaki verilerin tamamen güvende olduğunu söylemek mümkün değildir. Ancak teknolojinin geldiği noktada bulut kullanımı giderek artacaktır. Burada önemli olan doğru hizmet sağlayıcıyı seçmek ve teknik ve hukuki tedbirleri elden bırakmamaktadır[185]. Bulut hizmeti sağlayıcılar arasında uluslararası standartlara uygun hizmet sunanlar, izinsiz erişime izin vermeyen bir sistem kuranlar, herhangi bir veri ihlali durumunda acil durum planı olanlar, ticari sırlarını bulutta saklamak isteyen tacirler için gelecekte ön plana çıkacaktır.

Ticari sırların özellikle kötüniyetli yazılımlarla, yetkisiz bir şekilde ağlara erişimle, mobil cihazlara yönelik saldırılarla ve bulut tabanlı saldırılarla ele geçirilmesi söz konusu olmaktadır. Bu itibarla tacirlerin siber güvenliğin sağlanmasına önem vermeleri gerekmektedir[186]. Siber güvenlik konusundaki yasal ve teknik gelişmeler tacirler tarafından yakından takip edilmeli, siber güvenlik ve bilgi güvenliği konusunda politikalar geliştirilmelidir. Ayrıca nesnelerin İnterneti gibi yeni teknolojiler daha fazla akıllı cihaz kullanımını getirerek ticari sırların kötüniyetli kişiler tarafından ele geçirilmesini kolaylaştırabileceğinden yeni teknolojilerin kullanımında farkındalığı elden bırakmamak gerekmektedir.

---

185 **YILDIZ, Özcan Rıza**, "Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim, Sayıştay Dergisi, Sayı 74-75, s.19.

186 İnternet güvenliğine yönelik tehditlerle ilgili detaylı bilgi için bkz. **SYMANTEC,** Internet Security Trade Report, Volume 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (Erişim 21.10.2016).

KAYNAKLAR

AKDAĞ GÜNEY, Necla, Anonim Şirket Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu, Vedat Kitapçılık, İstanbul 2010.

AKKURT, Sinan Sami, "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Özellikleri", AÜHFD, 60(1), 2011, s.19-46.

ALMELING, David, "Seven Reasons Why Trade Secrets Are Increasingly Important", Berkeley Technology Law Journal, Vol.27, Issue 2, Fall 2012, s.1091-1118.

ARKAN, Sabih, Ticari İşletme Hukuku, 23.B., Ankara 2017.

BAŞGÜL, Mürsel/CHOUSEİNOGLOU, Oumout, "Bulut Bilişim Kapsamında Ortaya Çıkabilecek Hukuki Sorunlar", 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, Ankara 2013, s.210-215.

BİLGE, Mehmet Emin, Ticari Sırların Korunması, Asil Yayın Dağıtım Ltd.Şti., 2.Bası, Ankara 2005.

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU, Bulut Bilişim, Ankara 2013.

BOND Jr., Vince, "U.S. Judge Sentences Couple to Jail for Stealing GM Trade Secrets", Automative News, Yayınlanma tarihi 01 Mayıs 2013, http://www.autonews.com/article/20130501/OEM06/130509970/u.s.-judge-sentences-couple-to-jail-for-stealing-gm-trade-secrets (Erişim 21.10.2016).

BOSTICK, Kenneth L., "Pie in the Sky: Cloud Computing Brings an End to the Professionalism Paradigm in the Practice of Law", Buffalo Law Review, Vol.5, s.1373-1414.

BOZBEL, Savaş, Fikir ve Sanat Eserleri Hukuku, XII Levha Yayınları, İstanbul 2012.

BOZKURT YAŞAR, Sevgi, Anonim Şirketlerde İşadamı Kararı İlkesinin (Business Judgment Rule) Uygulanması, Beta Yayınevi, İstanbul 2015.

BOZKURT YÜKSEL, Armağan Ebru, Bulut Bilişimde Kişisel Verilerin Korunması (Personal Data Protection in Cloud Computing), Yetkin Yayınları, Ankara 2016 (Bulut Bilişim).

BOZKURT YÜKSEL, Armağan Ebru, "Elektronik Ticarette Elektronik Alternatif Uyuşmazlık Çözümü", Mevzuat Dergisi, Yıl 11, Sayı 123, Mart 2008, http://www.mevzuatdergisi.com/2008/03a/02.htm (Erişim 25.11.2016).

BOZKURT YÜKSEL, Armağan Ebru, "Nesnelerin İnternetinin Hukuki Yönden İncelenmesi", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 17, Sayı 2, Y.2015, Basım Yılı Nisan 2016, s.113-139.

BOZKURT YÜKSEL, Armağan Ebru, "Online International Arbitration", Ankara Law Review, Vol.14, No.1, Summer 2007, s.83-93, http://dergiler.ankara.edu.tr/dergiler/64/1542/16895.pdf (Erişim 25.11.2016).

BOZKURT YÜKSEL, Armağan Ebru, Patent Uyuşmazlıklarının Çözüm Yolları – Milletlerarası Tahkim ve Devlet Yargısı, Yetkin Yayınları, Ankara 2009 (Patent Uyuşmazlıkları).

BOZKURT YÜKSEL, Armağan Ebru, "Üç Boyutlu Yazıcıların Fikri Mülkiyet Hukukuna Etkileri", Fikri Mülkiyet Hukuku Yıllığı 2014, Editör Prof.Dr.Tekin Memiş, Yetkin Yayınevi, Ankara 2016, s.101-147.

BRADFORD, Benjamin J./MALESON, Justin A./WERNER, Micheal T., "Protecting Trade Secrets Stored in the Cloud", American Bar Association, Section of Litigation Intellectual Property, March 28, 2014.

BRADSHAW, Simon/MILLARD, Christopher/WALDEN, Ian, "Standard Contracts for Cloud Services", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.40-72.

BUGHIN, Jacques/CHUI, Michael/MANYIKA, James, "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch", McKinsey Quarterly, http://www.mckinsey.com/industries/high-tech/our-insights/clouds-big-data-and-smart-assets-ten-tech-enabled-business-trends-to-watch (Erişim 04.12.2016).

CISCO, "State Government Deploys Private Cloud to Provide Services to Agencies", http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/state_of_alaska_cs.pdf (Erişim 22.11.2014).

ÇAMOĞLU**, Ersin,** Anonim Ortaklık Yönetim Kurulu Üyelerinin Hukuki Sorumluluğu, 2.B., Vedat Kitapçılık, İstanbul 2007.

ÇAPA**, M.Sadık,** "Haksız Rekabet Hukukunda Başkalarının İş Ürünlerinden Yetkisiz Yararlanma", Ankara Barosu Dergisi, 2014/2, s.359-373.

DEDEAĞAÇ, Ender/SAPAN, Oğuzhan, Anonim Şirketlerde Yönetim Kurulu ve Sorumluluğu, Ankara Barosu Başkanlığı, Ankara 2013.

DHULIA, Khyati, Trade Secrets in Cloud Computing, University of Washington School of Law, Final Thesis Paper, Spring 2010.

DMTF, "Interoperable Clouds", A White Paper from the Open Cloud Standards Incubator, http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0101_1.0.0.pdf (Erişim 23.01.2015).

DOYLE, Charles, "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act", Congressional Research Service, August 19, 2016, https://www.fas.org/sgp/crs/secrecy/R42681.pdf (Erişim 27.09.2016).

DÜLGER, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, 6.B., Seçkin Yayınevi.

European Commission Information Society and Media, "The Future of Cloud Computing - Opportunities for European Cloud Computing Beyond 2010", Expert Group Report, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf (Erişim 22.01.2015).

FBI, "Economic Espionage", Inside the FBI, https://www.fbi.gov/audio-repository/news-podcasts-inside-economic-espionage.mp3/view, Yayınlanma Tarihi 23.06.2015 (Erişim 21.10.2016).

FISCHL, Thomas/WEIMER, Katharina A., "Cloud Computing-A German Perspective", Transcending the Cloud, A Legal Guide to the Risks and Rewards of Cloud Computing, ReedSmith, http://www.reedsmith.com/files/Publication/cf6df614-498c-4c92-979c-454346c15369/Presentation/PublicationAttachment/131ec3c6-65ff-45e4-bca1-f5628e478465/Cloud%20Computing%20-%20Germany%20Chapter%20ONLY%20-%2008.12.10.pdf (Erişim 04.01.2015).

GELLMAN, Robert, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing", World Privacy Forum, February 23, 2009, http://www.worldprivacyforum.org/www/wprivacyforum/pdf/WPF_Cloud_Privacy_Report.pdf (Erişim 17.03.2015).

GOTHING, Andrea A./NORTHROP, Seth A./ZHU, Li, "Keeping secrets in the cloud: Are storms ahead for trade secret protection?", InsideCounsel.com, February 26, 2015.

GOWEN, Nicholas A./SCHWARTZ, Honigman Miller/Cohn LLP, "Protecting Trade Secrets in the Cloud", The National Law Review, October 20, 2014.

GRUNFELD, Gay/FISCHER, Aaron, "How Businesses Protect Their Valuable Trade Secrets", San Francisco Daily Journal, Monday, September 26, 2011, www.dailyjournal.com (Erişim 29.07.2016).

GÜNGÖR, Gülin, "Yeni Düzenleme Çalışmalarında Elektronik Akitlerin Kuruluşu ve Click-Wrap Yazılım Lisansı Sözleşmelerinde Hukuk Seçimi Kaydı", Ankara Üniversitesi Hukuk Fakültesi Dergisi, Y.2002, C.51, S.1, s.19-42.

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

HEIN, Matthias, "Ekonomi Casusluğu Yayılıyor", Deutsche Welle Türkçe, http://www.dw.com/tr/ekonomi-casuslu%C4%9Fuyay%C4%B1l%C4%B1yor/a-18452902, Yayınlanma Tarihi 15.05.2015 (Erişim 21.10.2016).

HON, W. Kuan/MILLARD, Christopher, "Cloud Technologies and Services", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.4-17.

HON, W. Kuan/HÖRNLE, Julia/MILLARD, Christopher, Which Law(s) Apply to Personal Data in Clouds?, Cloud Computing Law, Editor Christopher Millard, Oxford University Press, Croydon 2013, s.221-253.

HON, W. Kuan/MILLARD, Christopher/WALDEN, Ian, "Who is Responsible for Personal Data in Clouds?", Cloud Computing Law, Editör Christopher Millard, Oxford University Press, Croydon 2013, s.194-219.

HURWITZ, Judith/BLOOR, Robin/KAUFMAN, Marcia/HALPER, Fern, Cloud Computing for Dummies, Wiley Publishing, Inc., Indianapolis 2010.

INTERNATIONAL CHAMBER of COMMERCE, "Trade Secrets: Tools for Innovation and Collaboration", Innovation and Intellectual Property Series", By Jennifer Brant and Sebastian Lohse, 2014.

KARAHAN, Sami, Ticari İşletme Hukuku, 21.Bası, Konya 2011.

KERTESZ, Attila/VARADİ, Szilvia, "Legal Aspects of Data Protection in Cloud Federations", Security, Privacy and Trust in Cloud Systems, Editors Surya Nepal, Mukaddim Pathan, Springer, Verlag Berlin Heidelberg 2014.

KIRCA, Çiğdem, "Know-How Sözleşmesinin Hukuki Niteliği", Prof.Dr.Ali Bozer'e Armağan, Ankara 1998, s.243-268.

KÖSEALİOĞLU, Ebru, "Know-How Sözleşmesinin Tanımı, Unsurları ve Patentten Farkları", Hukuk Gündemi, Yaz 2007, Sayı 8, s.135-138.

KÖSEKAYA, Fatih, Anonim Şirket Yönetim Kurulu Üyelerinin Mesleki Sorumluluk Sigortası, Adalet Yayınevi, Ankara 2013.

KUMAR, Ranjeet/TRIPATHI, R.C./TIWARI, M.D., "Trade Secrets Protection in Digital Environment A Global Perspective", International Journal of Economics and Management Sciences, Vol.2, No.4, 2012, s.1-9.

LAW SOCIETY, http://lawsociety.org.uk/advice/practice-notes/cloud-computing/ (Erişim 18.11.2014).

LINEK, Ernie, "A Brief History of Trade Secret Law, Part 1", BioProcess International, http://bannerwitcoff.com/_docs/library/articles/briefhistory1.pdf (Erişim 03.02.2016).

MARIN, Mauricio, "Economic Espionage Threat Rising in America", http://www.lasvegasnow.com/news/economic-espionage-threat-rising-in-america (Erişim 21.10.2016).

MEMİŞ, Tekin, "Bulut Bilişimde Fikri Hak Sorunları", Fikri Mülkiyet Hukuku Yıllığı 2013, Yetkin Yayınları, Ankara 2015, s.315-346.

MILLIGAN, Robert M./SALINAS, Joshua, "A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media", NYSBA Bright Ideas, Spring/Summer 2012, Vol.21, No.1.

NIST, The NIST Definition of Cloud Computing, Special Publication 800-145, http//csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Erişim 24.11.2016).

ORGAN, Shawn J./CORCORAN, Matthew C., "Your Web Site's 'Terms of Use': Are They Enforceable?", Privacy & Data Security Law Journal, 2008, http://www.jonesday.com/files/Publication/97a326a1-0077-4fc9-ac81-e82c265d0c82/Presentation/PublicationAttachment/a882327c-e026-49bf-91fb-ee3f9ca21ac0/Terms%20of%20Use.pdf (Erişim 05.01.2016).

ÖZDEN, **Serkan,** "Bilgi Güvenliği Konusunda Firmalar Ne Kadar Bilinçli?", http://wise.web.tv/video/bilgi-guvenligi-konusunda-firmalar-ne-kadar-bilincli__atblx3js2es (Erişim 14.11.2016).

ÖZEL, **Çağlar,** "Sözleşme Dışı Sorumlulukta Yansıma Zarar ve Giderimine İlişkin Bazı Düşünceler", AÜHFD, C.50, S.4, Y.2001, s.81-106.

POOLEY, James H., "The Uniform Trade Secrets Act: California Civil Code 3426", Santa Clara High Technology Law Journal, Volume I, Issue 2, Article 3, s.193-216.

REİSOĞLU, Safa, Türk Borçlar Hukuku Genel Hükümler, Beta Yayınevi, 23.B., İstanbul 2012.

ROWE, Elizabeth A., "RATs, TRAPs, and Trade Secrets", 57 B.C.L. Review, Y.2016, s.381-426 (RATs).

ROWE, Elizabeth A., "Saving Trade Secret Disclosures on the Internet Through Sequential Preservation", Wake Forest Law Review, Volume 42, 2007, Number 1, s.1-47.

SADIÇ, A.Burak, "Siber Risk Sigortaları Nasıl Ele Alınmalı?", Siber Bülten, Yayınlanma Tarihi 04.10.2015, https://siberbulten.com/makale-analiz/siber-risk-sigortalari-nasil-ele-alinmali/ (Erişim 10.11.2016).

SAMUELSON, Pamela/SCOTCHMER, Suzanne, "The Law and Economics of Reverse Engineering", Yale Law Journal, Vol.111, No.7, 2002, s.1575-1663.

SANDEEN, Sharon K., "Lost in the Cloud? The Trade Secret Implications of Cloud Computing", 2011 MSBA Computer and Technology Law Institute, Minneapolis, October 20, 2011.

SULU, Muhammed, Ticari Sırların Korunması, On İki Levha Yayınları, İstanbul 2016.

SYMANTEC, Internet Security Trade Report, Volume 21, April 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (Erişim 21.10.2016).

ŞENER, **Oruç Hami,** Ortaklıklar Hukuku, 2.B., Seçkin Yayınevi, Ankara 2015.

ŞENER**, Oruç Hami,** Ticari İşletme Hukuku, Seçkin Yayınevi, Ankara 2016 (Ticari İşletme).

TEKİNALP, Ünal, Sermaye Ortaklıklarının Yeni Hukuku, 3.B., Vedat Kitapçılık, İstanbul 2013.

TEKŞEN, Mustafa Gökhan, Ticari Sır, Bankacılık Sırrı veya Müşteri Sırrı Niteliğindeki Bilgi veya Belgelerin Açıklanması Suçu, Yetkin Yayınları, Ankara 2012.

THAYER, Linda J./YANG, Ming-Tao, "Security and Privacy: Storing Trade Secrets in the Cloud-Bad Idea?", Cloud Computing Journal, December 4, 2015, http://finnegan.com/resources/articles/articlesdetail.aspx?news=450db577-3e55-43db-ad74-192fde3fd3f9 (31.07.2016).

TURANBOY, Asuman, "Ticari Sır", Prof.Dr.Tuğrul ANSAY'a Armağan, Turhan Yayınevi, Ankara 2006, s.349-369.

TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü (UEKAE), Yakup Korkmaz, "Bulut Bilişim: Türkiye İçin Fırsatlar", http://www.tubitak.gov.tr/tubitak_content_files/bilgiguvenligi/sunular/Korkmaz_Bulut_Bilisim.ppt (Erişim 22.11.2014).

U.S. DEPARTMENT of JUSTICE, "U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", Yayınlanma tarihi 19 Mayıs 2014, https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage (Erişim 09.11.2016).

UŞAN, Fatih, İş Hukukunda İş Sırrının Korunması, Ankara 2003.

VENKATRAMAN, Archana, "Case Study: How eBay Uses Its Own OpenStack Private Cloud", Computer Weekly, 18 June 2014, http://www.computerweekly.com/news/2240222899/Case-study-How-eBay-uses-its-own-OpenStack-private-cloud (Erişim 20.01.2015).

WARE, James, "IP, Trade Secrets and Employee Mobility", Essential California Legal Content, Week of November 25, 2013, Vol. 137, No.46.

WEICHERT, Thilo, "Cloud Computing & Data Privacy", The Sedona Conference Working Group Series, February 2011, https://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-conputing-and-data-privacy.pdf (Erişim 24.11.2016).

WIPO, "What is a Trade Secret?", http://www.wipo.int/sme/en/ip_business/trade_secrets/trade_secrets.htm (Erişim 23.10.2016).

YASAMAN Hamdi, "Patent Hukukunda Ticari Sırların Korunması", Fikri Mülkiyet Hukuku Yıllığı 2009, XII Levha Yayınları, İstanbul 2009, s.367-388.

YAVUZ, Cevdet, Borçlar Hukuku Dersleri (Özel Hükümler), Beta Yayınevi, İstanbul 2013.

YEH, Brian T., "Protection of Trade Secrets: Overview of Current Law and Legislation", Congressional Research Service, April 22, 2016, https://www.fas.org/sgp/crs/secrecy/R43714.pdf (Erişim 23.10.2016).

YILDIZ, Özcan Rıza, "Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim, Sayıştay Dergisi, Sayı 74-75, s.5-23.

YURDAKUL, Çiğdem, "Türkiye'de Adli Bilişim Uzmanlığı/Gereksinimleri/Kriterler/Kimler Olmalı", Adli Bilişim Dergisi, Sayı 3, Nisan 2016.

INTERNET SİTELERİ

http://aws.amazon.com/ (Erişim 21.01.2015).

http://courts.mrsc.org/appellate/077wnapp/077wnapp0020.htm (Erişim 07.08.2016).

http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (Erişim 02.02.2016).

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&from=EN (Erişim 15.05.2017).

http://googleforwork.blogspot.com.tr/2010/03/disaster-recovery-by-google.html (Erişim 23.11.2014).

http://searchcloudcomputing.techtarget.com/definition/public-cloud (Erişim 23.11.2014).

http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.56b0d6fd7f16b1.70263308 (Erişim 02.02.2016).

http://teftis.kulturturizm.gov.tr/Eklenti/34660,ticaretle-baglantili-fikri-mulkiyet-anlasmasi-trips-199-.doc?0 (Erişim 15.05.2017).

http://thecloudtutorial.com/cloudtypes.html (Erişim 22.11.2014).

http://www.business2community.com/strategy/difference-data-information-0967136 (Erişim 17.11.2016).

http://www.internetlibrary.com/cases/lib_case403.cfm (Erişim 13.11.2016).

http://www.merriam-webster.com/dictionary/hacker (Erişim 17.02.2016); http:// www.webopedia.com/TERM/H/hacker.html (Erişim 17.02.2016).

http://www.techopedia.com/definition/26965/lights-out-data-center (Erişim 07.03.2015).

http://www.ticaretkanunu.net/turk-ticaret-kanunu-madde-gerekceleri-ikinci-kitap-ticaret-sirketlerimadde-124-644/ (Erişim 03.01.2015).

http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (Erişim 02.02.2016).

http://www2.tbmm.gov.tr/d24/1/1-0483.pdf (Erişim 02.02.2016).

https://cloud.google.com/appengine/docs/whatisgoogleappengine (Erişim 21.01.2015).

https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/1678/index.do (Erişim 24.11.2016).

https://sigortateklif.net/siber-risk-sigortasi.php (Erişim 10.11.2016).

https://www.facebook.com/legal/terms (Erişim 25.11.2014).

https://www.google.com/work/apps/business/ (Erişim 21.01.2015).

https://www.quora.com/What-is-the-difference-between-servers-and-desktops-workstations (Erişim 12.06.2017).