Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme

Cloud Computing as an Information Access Platform: A Study on Threats and Legal Requirements

Türkay HENKOĞLU[*] ve Özgür KÜLCÜ[**]

Öz

Bulut bilişim, bilgiye her yerden ve her an erişebilme kolaylığı ile internet üzerinden sunulan çok yönlü ve hızlı gelişen servis araçlarından biridir. Ancak bu yeni teknoloji servisi birçok faydasının yanı sıra; göz ardı edilmesi halinde büyük kayıplara neden olabilecek riskleri de içermektedir. Çalışma genelinde, küresel çapta yoğun olarak tartışılmakta olan "Bulut üzerinde bulunan bilgilerin sahibi kim? Kişisel verilerin korunmasından kim sorumlu? Kayıp ve zararların telafi edilmesi mümkün mü?" gibi birçok sorunun yanıtı literatür ve mevcut uygulamalar içinde aranarak; bulut bilişimde verilerin güvenliği ve gizliliği konusunda toplumda bilinçlenmenin artırılması hedeflenmiştir.

Bu çalışmada, bulut bilişimin faydalı ve olumsuz yönleri ile birlikte; mevcut ABD hukuk mevzuatı, AB direktifleri ve AB sözleşmeleri kapsamlı olarak incelenerek, tüm hukuksal risk ve problemlere dikkat çekilmiştir. Çalışma sonunda, mevcut bulut hizmet sözleşmeleri ve yasal düzenlemeler çerçevesinde; Türkiye'de bulut bilişim kullanıcılarının veri güvenliğini ve gizliliğini yeterli seviyede koruyan bir hukuksal düzenlemenin bulunmadığı ortaya konulmuştur. Ayrıca; veri öznelerinin bulut bilişime olan güveninin sağlanabilmesi ve kişisel verilerin korunabilmesi amacıyla temel olarak kabul edilebilecek güvenli bulut bilişim modeli önerisinde bulunulmuştur.

Anahtar sözcükler: *AB veri güvenliği, ABD veri güvenliği, Bulut bilişim, Bulut bilişim modeli, Bulut bilişim riskleri, Kişisel verilerin korunması,*

Abstract

Cloud computing is one of the services that are delivered over internet for transmission and access to user data at anytime from anywhere. In spite of numerous advantages provided with cloud computing, it is important to recognize the potential threats, including loss of user data, when disregarded. In scope of the study, it is aimed to raise public awareness on cloud computing by investigating security and privacy issues related to user data stored on remote servers based on the questions like "Who is the owner of the data?", "Who is responsible for protection of the data?", "Is it possible to compensate for the data loss?", in the current cloud computing systems and literature review.

* Adli Bilişim Uzmanı, Hacettepe Üniversitesi, Beytepe, Ankara. (henkoglu@hacettepe.edu.tr)
** Doç. Dr., Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, Beytepe, Ankara. (kulcu@hacettepe.edu.tr)

In addition to the pros and cons of cloud computing; the current law of United States and all directives and agreements in European Union are examined in order to draw attention to all legal risks and problems in the study. This study shows that there are no legal regulations relating to security and privacy issues of cloud computing in Turkey in scope of the current cloud computing service agreements and the legalities. At the end of the study, a new cloud computing security model is proposed, by which it is aimed to increase users' trust towards the system and to ensure the security of user data.

Keywords: *EU data security, USA data security, Cloud computing, Cloud computing risks , Cloud computing model, Protection of private data*

Giriş

Bulut bilişim, dijital yaşamın ve bilgi ve iletişim teknolojilerinin en önemli dönüm noktalarından birini oluşturmaktadır. Sosyal paylaşım sitelerinin gelişimi ile birlikte kullanıcıların ilgisini çekmeye başlayan bulut bilişim; iş dünyasında maliyetleri düşürmesi, e-ticaretin gelişimine katkıda bulunması ve istihdama olan etkisi nedeniyle, büyük şirketlerin ve devlet yönetimlerinin bilgi politikaları arasında öncelikli yerini almıştır. Avrupa Birliği (AB) Komisyonu başkan yardımcısı ve Dijital Ajanda üyesi Needie Kroes'in "bulut bilişim ve veri koruma reformu" ile ilgili açıklamaları, AB'nin ekonomiye bulut bilişim stratejisi ile yön vermekte olduğunu göstermektedir (Kroes, 2012). Küresel bulut bilişim pazarının 2010 yılındaki değeri 21,5 milyar dolar iken, 2015 yılı için gerçekleşmesi beklenen değer 73 milyar dolar seviyesindedir. Microsoft'un açıklamasına göre; 2014 yılında bulut bilişim sayesinde 11,3 milyon yeni istihdam oluşması beklenmektedir. Bu açıklama da, bulut bilişimin ulaştığı boyutu tanımlamak açısından dikkat çekicidir (Fox, 2012).

Bulut bilişim sistemlerinin gelişimi bankacılık sisteminin gelişimi ile bazı benzerlikler göstermektedir. Bankacılık sektörünün gelişmeye başladığı ilk dönemlerde, yasal düzenlemelerin yetersizliğinden kaynaklanan belirsizlikler, birikimlerin bankaya güvenle yatırılması konusunda çekimserlik yaratmaktaydı. Benzer durum, günümüzde bulut bilişimin kullanılması noktasında görülmektedir. Bilginin en önemli değer olarak ifade edildiği bilişim çağında; mobil iletişim ve bilgi transfer işlemlerinin yoğun olarak yapıldığı bulut sistemlerinin bilgi güvenliğini sağlama noktasındaki yetersizliği, kullanıcıların endişe duymaları için geçerli bir neden olarak görülebilir. Bilgi güvenliğinin sağlanması, kişisel bilgilerin kaydedilmesi ve bilgilerin nerelerde bulunacağı ile ilgili konular; bilgi yönetiminin teknik zorlukları ile birlikte, hukuksal düzenlemelerle de yakından ilgilidir (Varadi, Kertesz ve Parkin, 2012). AB ve ABD'de bulut bilişimin risklerinin ve bilgi güvenliği kapsamında alınabilecek hukuksal önlemlerin yoğun olarak tartışıldığı görülmektedir (Paquette, Jaeger ve Wilson, 2010). Hukuki boyutun tartışıldığı başlıca konular; verilerin farklı bir ülkeye transferi, kişisel bilgilerin korunması ve güvenlik ihlali durumunda neler yapılabileceği hakkında kullanıcının bilgilendirilmesidir.

Türkiye'de de genel bulut bilişim hizmetlerinden faydalanma oranının hızla arttığı, fakat kullanıcıları meydana gelebilecek zararlar karşısında korumaya alan kişisel verilerin

korunması kanunu vb. hukuksal düzenlemenin olmadığı görülmektedir. Bu durum bulut sistemi üzerine aktarılan tüm verilerin sorumluluğunun, bulut hizmeti alan kullanıcı üzerinde bulunduğu anlamını taşımaktadır. Bu nedenle bulut sisteminin sunmuş olduğu kolaylık ve imkânlardan faydalanan kullanıcıların; bulut sisteminin kullanımı esnasında ve sonrasında oluşabilecek riskler ve bu konudaki hukuksal eksiklikler hakkında bilinçli olmaları önem taşımaktadır. Bu çalışmada; küresel çapta e-posta ve veri depolama hizmetinin yaygın kullanımı ile öne çıkan ve aynı zamanda ücretsiz bulut bilişim hizmeti sunan Google, Microsoft ve Yahoo gibi bulut hizmet sağlayıcıların (Kaufman, 2009) hizmet sözleşmeleri esas alınarak değerlendirmeler yapılmıştır. İçeriğinde farklılık olabilecek diğer hizmet sağlayıcı sözleşmeleri bu değerlendirme kapsamının dışında tutulmuştur.

Bulut Bilişimin Tanımı ve Kapsamı

Bulut bilişim üzerinde uzlaşı sağlanmış açık bir tanım bulunmamakla birlikte; uygulamaların internet ortamında bulunan bir uzak sunucu üzerinden çalıştırılması ya da kullanıcıya ait verilerin uzak sunucu üzerinde her an erişilebilir şekilde bulundurulmasını sağlayan bir servis yapısı olarak tanımlanabilir. Web ara yüzü bilgiyi her yerde ve herkes için ulaşılabilir hale getirirken; bulut bilişim, bilgi işlem gücünü her yerde ve herkes için kullanılabilir hale getirmiştir (European Commission, 2012a). Uygulamaların kullanıcı bilgisayarı üzerinden çalıştırılarak ve bilgilerin yerel bilgisayar diskinde bulundurularak yapılan uzak erişimler, merkezi bilgisayar ve ona bağlı terminal yapısıyla 2000'li yılların başından itibaren kullanılmaktadır (Salesforce, 2012). Bu yönüyle bulut sistemi; geçmişte kullanılmış bir yöntemin günümüzün ekonomik şartlarına uyarlanarak ve geliştirilerek, tüm internet kullanıcılarının kullanımına olanak sağlayacak şekilde yeniden sunulmasıdır.

Bulut bilişim sayesinde, istenilen bilgiye her yerden ve her türlü bilgi iletişim cihazı (PC, Mac, iPhone, Android veya BlackBerry) kullanarak ulaşmak mümkün olabilmektedir. Donanım kaynaklı problemlerin bulunmaması, fiziksel sunuculardan daha hızlı çalışan sanal bilgisayar ile yüksek erişilebilirlik imkânının sunulabilmesi, bellek ve disk değişikliği gerektirmeyen esnek yapının kullanılması ve doğa dostu (elektrik ve yer tasarrufu) olması, bulut bilişimin ilk bakışta dikkati çeken avantajları arasında görülmektedir.

Bütün bu avantajlı yönleri göz önüne alındığında; bilgi iletişim teknolojilerindeki gelişimin yansıması olan bulut bilişimden uzak durmak ya da alternatif yöntemlerde ısrarcı olmak akılcı bir çözüm olarak görülmemektedir. Fakat bulut bilişimin beraberinde getirdiği riskler de yok sayılamayacak kadar önemlidir.

Bulut Bilişim Hizmet Modelleri ve Kullanım Biçimleri

Kullanım biçimine göre bulut bilişim dört sınıfta toplanmaktadır (Mell ve Grance, 2011). Bunlar;

Genel Bulut (Public Cloud)

İnternet üzerinden web ara yüzü aracılığıyla genel kullanıma sunulan hizmetlerdir. (Google Apps, Amazon, Windows Azure)

Özel Bulut (Private Cloud)

Belirli bir kurum ya da kuruluşa sunulan bulut hizmetidir. Bulut hizmet sağlayıcı, kurumun kendisi olabileceği gibi, üçüncü bir bulut hizmet sağlayıcı da olabilir. Kurum dışından tüm erişim yolları kapatılarak sadece kurum içi hizmet verilir.

Melez Bulut (Hybrid Cloud)

Genel ve özel bulut hizmetlerinin birlikte kullanıma sunulmasıdır. Bir kurumun verileri özel bulut içinde yer alırken, bazı servisleri genel bulut üzerinden halkın kullanımına açılabilir. Melez bulut henüz yaygın olarak kullanılan bir kullanım biçimi değildir. (IBM, Juniper)

Topluluk Bulutu (Community Cloud)

Belirli bir topluluk ya da gruba sunulan bulut hizmetidir. Topluluğu oluşturan unsurlar, ortak çalışma alanında bulunan kurumlar da olabilir.

Bulut bilişim hizmet sağlayıcıları, bulut hizmeti sağlarken yazılım, platform ve alt yapı hizmet modellerinden birini ya da aynı anda birkaçını kullanmaktadırlar. Fakat bazen bulut hizmet sağlayıcıların uyguladığı roller karışıklık yaratabilmektedir.

Servis Olarak Yazılım (SaaS - Software as a Service)

Uygulama bulutu olarak da adlandırılmaktadır. Bulut alt yapısı kullanılarak, web tabanlı çeşitli yazılım ve uygulamaların (örneğin e-Posta) bulut sistemi kullanıcısına sunulmasıdır. Kullanıcının sunucu, işletim sistemi, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır. Kullanıcı, bulut hizmeti almakta olduğu sunucu bilgisayar üzerindeki yazılımı çalıştırmak suretiyle dosyaları üzerinde çalışabilmektedir (Schubert, 2010). Ayrıca bilgisayarın yerel sabit sürücüsü üzerine herhangi bir yazılım kurulumuna ihtiyaç duyulmaz. Google Drive ve Salesforce CRM servis olarak yazılım hizmeti örnekleridir.

Servis Olarak Platform (PaaS - Platform as a Service)

Kullanıcıya yönetilebilir yeni uygulamalar geliştirmesi ve sunabilmesi için sanal servis ortamı sağlar. Geliştirilen uygulama ile ilgili alt yapı, ortam ve diğer servisler bulut hizmet sağlayıcı tarafından sağlanır (Schubert, 2010). Kullanıcının sunucu, işletim

sistemi, veri depolama alanı üzerinde yönetim işlevi bulunmamaktadır. Sadece geliştirilen uygulamalar üzerinde kontrol sağlayabilmektedir. Bir bulut hizmet sağlayıcısı (örneğin Force.com, Google App Engine, Windows Azure) üzerinde geliştirilen uygulama, standartların bulunmaması nedeniyle sadece geliştirilen platform üzerinde kullanılabilmektedir.

Servis Olarak Altyapı (IaaS - Infrastructure as a Service)

Kaynak bulutu olarak da ifade edilmektedir. Ağ üzerinden güvenli erişim imkânı sunan dinamik veri depolama alanı (örneğin; Amazon S3, SQL Azure), işlemci kaynaklarının sanal olarak sunulması (örneğin; Amazon EC2, Zimory, Elastichosts) ve ağ hizmetleri gibi servisler, bulut bilişim alt yapı servisi örnekleridir (Schubert, 2010). Kullanıcının bulut alt yapısında yönetim işlevi bulunmamaktadır. Fakat işletim sistemi, veri depolama alanı ve sınırlı olarak ağ bileşenleri (güvenlik duvarı gibi) üzerinde kontrol sağlayabilmektedir.

Bulut Bilişimin Sağladığı Teknik Faydalar

Donanım ve Yazılım Maliyetinin Azalması

Bulut sisteminde hizmet sunmak için kullanılan tüm donanım, bakım ve güncellemeleri hizmet sağlayıcı tarafından yapılmaktadır. Kullanıcı sayısı ve sunulan hizmetin niteliğine bağlı olarak, donanım ölçeklendirilerek maliyetler yönetilebilir. Kullanıcı tarafında herhangi bir yazılım ücreti ödemeksizin bulut hizmetlerinden faydalanılabilir. Yazılım maliyeti kullanıcı sayısına bağlı olarak hizmet sağlayıcı tarafından karşılanır. Kullanıcının sadece üyelik başlatması yeterlidir. Kullanıcı tarafında veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç yoktur. Avrupa ekonomik alanı içerisinde 2011 yılında yapılan araştırmalar; bulut sistemini kullanmaya başlayan şirketlerin %80'inin, %10-20 oranında tasarruf sağladığını göstermektedir. Ayrıca; tüm ekonomik veriler, bulut bilişimin önemini doğrulamakta ve bulut bilişim kullanım oranlarının küresel olarak hızlı bir artış göstermesi beklenmektedir. Bulut bilişim; mobil çalışmayı %46, üretimi %41 ve standartlaşmayı %35 oranında artırmaktadır (European Commission, 2012a).

Uzaktan Erişim Kolaylığı Sağlaması

Bulut bilişimin temel işlevi, kullanıcıya ait verilerin internet üzerindeki bir sunucuya aktarılması, depolanması ve gerektiğinde uzaktan erişilerek bilgiler üzerinde değişikliğin yapılmasını sağlamaktır. Bulut hizmet sağlayıcıların her an kullanıcının isteklerine cevap verecek durumda ve yeterlilikte olması gerekir. Bu özelliği ile bulut bilişim, mobil yaşamı destekleyen en önemli bilgi ve iletişim teknolojileri hizmetlerinden biri haline gelmiştir. Bulut bilişim kullanımıyla, internete erişim sağlanabilen her noktadan bilgilere ve uygulama programlarını kullanma imkânına sahip olunabilmektedir. Uzaktan erişim kolaylığı, hırsızlık ya da fiziksel disk problemleri gibi nedenlerle verinin kaybedilmesi risklerini de azaltmaktadır.

Depolama Kapasite Sınırlamalarının Ortadan Kalkması

Kullanıcılara tahsis edilmiş özel bir disk alanı kullanılmadığı için, veri depolama alanının yönetimi daha etkin olarak yapılabilmektedir. Kullanıcılar, depolama alanı kullanımı konusunda, sanal disk üzerinde yazılım ile kısıtlanırlar ve tüm kullanıcılara ait veriler aynı ortamda bulunmaktadır. Kullanıcı bilgisayarında veri depolamak için yüksek kapasiteli veri depolama birimlerine ihtiyaç duyulmamaktadır. Bulut bilişimde kullanılan bilgi ve veri alanı yönetim araçları, eşit seviyede maliyet ile daha geniş veri alanında daha güçlü veri koruma imkânı sunar (ENISA, 2009).

Bulut Bilişim Sorunları ve Yeni Hukuksal Koşullar

Uygulamaların Yavaş Çalışması ve Düşük Hızlarda Servis Sorunları

Web tabanlı bulut hizmetleri, geniş bant internet ile çalışacak şekilde tasarlanmıştır. Bu nedenle; kullanılan internet bağlantısının indirme ve yükleme hızları bulut hizmetlerinin kullanımında etkilidir. İndirme hızı 1 Mbps ve yükleme hızı 256 Kbps'e kadar olan geniş bant internet bağlantılarında büyük boyuttaki verilerin bulut üzerine transferi uzun zaman alabilmektedir. Geniş bant internet alt yapısı, küresel dijital ekonominin gelişiminde önemli rol oynamaktadır. Türkiye İstatistik Kurumu (TÜİK) tarafından yapılan "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması – 2012" araştırma sonuçlarına göre; Türkiye'de hanelerin %43,2'sinde geniş bant internet erişim imkânı bulunmaktadır (TÜİK, 2012).

AB'nin 2020 stratejisi içinde yer alan ana hedeflerden biri de; ekonomik büyümeyi sağlayacak etkin ve yaygın internet kullanımını sağlamaktır. Bu nedenle; geniş bant stratejisinin uygulanması ve geniş bant internet alt yapısının AB genelinde hızla yaygınlaştırılması hedeflenmektedir. IP/10/1142 referans numaralı AB Dijital Ajandası'nda yer alan 2020 yılı hedefine göre; 2020 yılına kadar AB alanı içerisinde tüm internet erişim hızının 30 Mbps'in üzerinde olacağı ve en az %50'sinin 100 Mbps hızında erişim hızına sahip olacağı belirtilmektedir (European Commission, 2010a). Kısa vadede ise (2013 yılına kadar) temel geniş bant alt yapısının (2 Mbps) AB genelinde yaygınlaştırılması öngörülmektedir (Digital Agenda, 2010). Türkiye'de internet kullanımı ve geniş bant internet erişim imkânının artmakta olduğu görülse de; AB ülkeleri ile kıyaslandığında hâlâ sayısal uçurumun bulunduğu söylenebilir (DPT, 2011).

Uzaktan Erişim ve Güvenlik Sorunları

Özellikle kullanıcıya ait kişisel bilgilerin de bulunduğu veri merkezi olarak hizmet sunan bulut hizmet sağlayıcıların veri koruma yükümlülüğünü yerine getirebilmesi için yetkisiz erişimlere karşı verileri korumaya ilişkin önlemler alması ve verilerin kriptolanabilmesi için ek bütçe ayırması gerekmektedir. Bulut bilişim üzerinde bulunan verilerin dış tehditlere karşı daha fazla hedef durumunda olması nedeniyle; internet

üzerinde bulunan sıradan bir veri bankasına göre daha fazla teknik önlem alınması önemlidir. Herhangi bir veri kaybının telafi edilebilmesi için yapılacak veri yedekleme işlemlerinin de maliyetleri oldukça yüksektir. Bu nedenle genellikle ücretsiz olarak hizmet sunan bulut hizmet sağlayıcılar, veri güvenliğinin sağlanması ya da herhangi bir saldırı sonucu kaybolan verilerin geri getirilmesi konusunda bildirimde bulunarak sorumluluk almamaktadırlar.

Bulut bilişimin internet teknolojisine bağlı olarak kullanılabilen bir hizmet olması nedeniyle güvenli bir internet bağlantısına ihtiyaç duyulmaktadır. Bulut hizmetlerini kullanan kullanıcıların internete bağımlı olması; önemli bilgilerin buluta aktarılması esnasında bilgi güvenliği kapsamında düşünülebilecek tüm güvenlik önlemlerini gözden geçirmesini gerektirecektir. Herhangi bir şifre dahi kullanılmadan bağlantı yapılabilen kafe, restoran, otobüs gibi ortamlarda kullanıcı şifreleri ve kişisel bilgilerin gizliliğinin korunmasına ilişkin riskler bulunmaktadır. Ayrıca bulut hizmetleri kullanımı esnasında uzaktan erişime bağlı güvenlik riskleri de bulunmaktadır. Koklama (sniffing), yanıltma (spoofing) ve araya girme (man-in-the-middle) yöntemleri ile yapılan saldırılar; bulut hizmetlerinde yönetim ara yüzü kullanımı esnasında veri güvenliğine yönelik en önemli tehditlerdir.

Verilerin Nerede Olduğunu Bilmeme Sorunu

Bulut bilişimin, verilere her yerden ulaşabilme özelliği daha fazla öne çıktığı için, hizmet kalitesi ve erişim olanakları üzerinde daha fazla durulmakta; diğer hususlar genellikle hizmet alan kullanıcılar tarafından ihmal edilmektedir. Fakat verilerin denetimi ya da hukuksal sorunların çözümü esnasında verilerin nerede bulunduğu konusu önem kazanmaktadır. Bu konuda bazı ülkeler kendi vatandaşlarına konuyu ihmal etme şansı tanımamışlar ve uygulamaya koydukları bilgi güvenliği politikalarında gerekli önlemleri almışlardır. Örneğin, Avrupa Birliği'nin verilerin korunması hakkındaki direktifine (EU Data Protection Directive) (European Council, 1995) göre; bulut bilişim hizmeti sunan şirketlerin, kullanıcılarına ait verilerin bulunduğu sunucuları AB ülkeleri dışında kurmaları ya da kiralayabilmeleri için bu ülkelerin AB yasalarının belirlemiş olduğu bilgi güvenliği seviyesinde olmaları gerekmektedir (Turan, 2010).

Türkiye'nin de aralarında bulunduğu birçok ülkede; bu konuda karşılaşılabilecek hukuksal sorunların çözümünde, verilerin nerede bulunacağı ile ilgili detaylar, hizmet alan kullanıcının yapacağı sözleşmede yer alması gereken önemli hususlardır. Fakat genellikle ücretsiz olarak bulut hizmeti sunan birçok hizmet sağlayıcı, kullanıcılara sözleşme üzerinde değişiklik yapma seçeneği sunmamaktadır. Bu tür bulut hizmet sağlayıcıların çevrimiçi gizlilik bildirimlerinde; kullanıcıya ait kişisel bilgilerin dünyanın herhangi bir yerinde depolanabileceği ve işlenebileceği açık olarak belirtilmektedir (bkz. Microsoft Çevrimiçi Gizlilik Bildirimi) (Microsoft, 2012). Bulut üzerinde bulunan verilerin gizliliği, bütünlüğü ve kullanılabilirliği ile ilgili olarak meydana gelebilecek zararlarda yasal hakların takip edilebilmesi için, hizmet sağlayan sunucuların belirli bir bölge

içinde bulunması istenmelidir. Mevcut yasal düzenlemelerin bulut hizmetleri kullanımı konusundaki bireysel hakları koruyuculuğu göz önüne alındığında; sözleşmede özel bir madde yer almadığı sürece Türkiye dışına taşınan verilerle ilgili tüm sorumluluğun, veriyi bulut ortamına taşıyan kullanıcıya ait olduğu söylenebilir.

Hizmet Alınan Firmaların Güvenilirliği, Yeterliliği ve Denetlenmesi Sorunları

Hizmet alınan firmanın doğru seçimi, bulut bilişimin sağladığı maliyet avantajının sürdürülebilirliği açısından önemlidir. Seçilen firmanın; istenilen güvenlik, kullanılabilirlik ve veri bütünlüğünün sağlanması konusunda taahhütte bulunması ve aynı zamanda bunu yerine getirecek teknik alt yapıya sahip olması gerekmektedir. Verilerin herhangi bir nedenle kaybolması, bütünlüğünün bozulması veya yetkisiz erişime karşı gerekli önlemlerin alınmamış olması gibi nedenlerle oluşabilecek zararların telafisi her an mümkün olamamaktadır. Ayrıca; bulut hizmet sağlayıcının en alt düzeyde gerekli teknik alt yapıya sahip olması ve sistemi işleten sistem yöneticilerinin bu konudaki yeterliliği de önem taşımaktadır. Bulut hizmet sağlayıcıların programlama ara yüzlerinde standardın olmaması ve verilerin tutulduğu veri tabanı şemalarındaki farklılıklar nedeniyle; kullanıcıların verilerini farklı bir bulut hizmet sağlayıcıya taşımasında problemler olabilmektedir. Hizmet yeterliliğinin bulunması; bulut hizmet sağlayıcının varlığını sürdürebilmesi ve aynı zamanda kullanıcının güvenini kazanabilmesi açısından da önemlidir. Türkiye'de bulut bilişim hizmeti verebilmek için sağlanması gereken standartlara ilişkin uyulması zorunlu düzenleme bulunmamaktadır.

Bilgi ve iletişim teknolojilerinin gelişimi; kişisel verilerin gizliliği konusunda her geçen gün daha fazla risk oluşturmaktadır. Anlık dikkatsizlik, yanlış işlem ya da hizmet sağlayıcısının kusuru sonucunda açığa çıkan kişisel bilgi, dünyanın her tarafına hızla yayılarak; telafisi mümkün olmayan kayıplara neden olabilmektedir. Hizmet alan bir tüketici olarak veri öznesinin bulut bilişim üzerindeki sorumluluğu; bir uçakta seyahat eden yolcunun, uçağın güvenli olarak kalkışından inişine kadar olan süreçteki sorumluluğu eşdeğerinde olmalıdır. Ayrıca; bulut bilişim hizmeti almak isteyen bir kullanıcı, bulut bilişim hizmet sağlayıcısı seçerken; hava yolu firması seçerken olduğu kadar kararlı olabilmelidir. Bir hava yolu şirketinin pilotlarının ne kadar tecrübeli oldukları hava yolu şirketine olan güvenin altında ayrıca sorgulanmamaktadır. Bulut bilişimde de güvenlik konusunda belirli standartların uygulanması ve düzenli olarak denetlenmesi gerekmektedir. Böylece kullanıcılar tercihlerini yaparken, bilgilerinin güvenliğinin sağlanıp sağlanmayacağı konusunda, hizmet sağlayıcılara yeterlilik sertifikasını veren kuruluşları göz önüne alabileceklerdir.

Bulut bilişim hizmeti verecek girişimciler için herhangi bir izin ya da yeterlilik (yeterli alt yapı, sermaye, kalifiye personel vd.) ön şartı bulunmamaktadır. Bu konuda herhangi bir yasal düzenleme ve denetim (internet toplu kullanım sağlayıcılarda olduğu gibi) olmadığı ve üyelik işlemleri sanal ortamda yapıldığı için; hizmet alan kullanıcıların birçok konuda (hizmete son verilmesi, veri kaybı, kişisel verilerin gizliliği vb.) mağdur olabilecekleri ortam oluşmaktadır.

Hizmet Sağlayıcıların Bilgi Güvenliği, Veri Bütünlüğü ve Erişim Denetimi ile İlgili Taahhütte Bulunamamaları

Bilgi güvenliği oldukça kapsamlı ve farklı boyutları ile birlikte değerlendirilmesi gereken bir alandır. Bilgi güvenliği önlemleri kapsamında sadece bilginin korunacak nitelikleri (gizliliği, bütünlüğü, kullanılabilirliği) değil; McCumber Bilgi Güvenliği Modeli'nde belirtildiği gibi, bilginin durumu (transferi, depolanması, işlenmesi), güvenlik önlemleri (teknoloji, politikalar, farkındalık) ve risk yönetimi etkenlerinin de göz önünde bulundurulması gerekmektedir (McCumber, 2005). Bulut sistemi üzerinde alınacak teknik güvenlik önlemleri de, benzer şekilde birçok farklı etken (politikalar, kullanıcı ihtiyaçları vd.) göz önüne alınarak belirlenmektedir. Aynı alt yapıyı kullanan kullanıcılardan biri güvenlik duvarından sadece güvenli protokolleri (SSH) kullanan veri paketlerinin geçişine izin verilmesini isterken; diğer kullanıcı web sunucusu çalıştırdığı için tüm http ve HTTPS paketlerinin geçişine izin verilmesini isteyebilmektedir (ENISA, 2009). Bu nedenle; bulut hizmet sağlayıcıların erişilebilirliği göz ardı ederek ve en katı güvenlik önlemlerini uygulayarak veri güvenliğini sağlamaları beklenmemelidir.

Bulut hizmet sağlayıcılar, kullanıcı ile yapmış oldukları sözleşmelerde; bilgi güvenliğinin sağlanması ve veri bütünlüğünün korunmasına ilişkin tüm sorumluluğun kullanıcıya ait olduğunu ve hizmetin kullanımı ile bu şartın kabul edilmiş olduğunu belirtmektedirler (bkz. Microsoft Hizmetler Sözleşmesi) (Microsoft, 2012). Bu tür hizmet sözleşmeleri karşısında kullanıcı haklarını koruyan yasal düzenlemeler olmaması nedeniyle bulut sistemi üzerine aktarılan verilerin kaybolma riskinin kullanıcı tarafından göze alınabilir nitelikte olması gerekmektedir.

Hizmet Sağlayıcıların Kesintisiz Hizmet Garantisi Verememeleri

Bulut hizmet sağlayıcılar meydana gelebilecek tüm felaket senaryolarına karşı hazırlıklı olmalı ve herhangi bir felaket durumunda kullanıcıya kesintisiz olarak hizmet sağlayabilmelidirler. Kullanıcıların bulut sistemini öncelikli olarak kullanmalarının ilk şartı, istenilen zamanda ve istenilen bilgiye erişebilme güvencesine sahip olmalarıdır.

Bulut servis hizmetlerinde meydana gelen kesintiler, kullanıcıların kendisine ait bilgilere erişiminin kısıtlanması ve bazen iş akışının kesintiye uğraması anlamına gelebilmektedir. Uluslararası Bulut Bilişim Esnekliği Çalışma Grubu (International Working Group on Cloud Computing Resiliency, IWGCR) tarafından yayınlanan rapora göre; 2007 yılından itibaren 13 büyük bulut hizmet sağlayıcının hizmet kesintileri nedeniyle 5 yılda meydana gelen zarar miktarı 45 milyon sterlin olmuştur (Bourne, 2012). Microsoft, Google, Yahoo, BlackBerry ve Amazon gibi büyük bulut hizmet sağlayıcılarının da aralarında bulunduğu birçok büyük şirketin hizmetlerinde kesintiler olabilmektedir (Perlin, 2012).

Bulut hizmet sağlayıcılar, hizmetlerde meydana gelen kesintiler ya da hizmet sağlayıcı tarafından hizmetin herhangi bir sebep gösterilmeksizin sonlandırılması durumunda meydana gelebilecek kayıplar ve bulut sistemi üzerinde bulunan bilgilerin iade edilmesi konusunda sorumluluk almamaktadır (bkz. Microsoft Hizmetler Sözleşmesi) (Microsoft, 2012).

İçeriğin Kullanımı ve Mülkiyet Hakkı ile İlgili Belirsizlikler

Hizmet sözleşmelerinde, kullanıcıya ait verilere sadece kendisinin erişebileceğine dair açıklık bulunmamaktadır. Ayrıca sözleşmeler herhangi bir yasal düzenlemeye dayanmadığı için, sadece hizmet sunan tarafın lehine olacak şekilde hazırlanmaktadır (Wyld, 2009). Herhangi bir felaket durumunda sistemin ne kadar sürede tekrar aktif hale gelerek hizmet vermeye başlayacağı konusunda da sözleşmelerde açıklık bulunmamaktadır.

Bulut sistemine aktarılan ya da bulut üzerinde bulundurulan verilerin kime ait olduğu konusu yeterince açık değildir. Bazı hizmet sözleşmelerinde, hizmetler aracılığıyla yüklenen içeriğin sahibinin kullanıcı olduğu ve içeriğin tümüyle kullanıcının sorumluluğunda olduğu belirtilmektedir. Fakat farklı bir maddede; hizmet sağlayıcının hizmet kalitesini geliştirmek amacıyla; içeriği kullanılabileceği, değiştirilebileceği, uyarlanabileceği, kaydedilebileceği, yeniden üretilebileceği, dağıtılabileceği ve görüntülenebileceği ifade edilmektedir (bkz. Google Hizmet Şartları veya Microsoft Hizmetler Sözleşmesi) (Google, 2012; Microsoft, 2012). Bu kapsamlı izin ve yetkinin sözleşme ile hizmet sağlayıcıya verilmesi, içeriğin kullanıcıyı korumak için alınacak önlemlerin (kötü amaçlı yazılım tespiti vb.) dışında kullanımına da imkân tanımaktadır. Bazı bulut son kullanıcı lisans sözleşmelerinde ise, sunulan hizmetler üzerinden gönderilen içeriğin tüm lisans haklarının (çoğaltma, aktarma, yayınlama ve saklama hakkı) daimi olarak hizmet sağlayıcı şirkete (hizmetleri sunması amacıyla) devredilmiş olduğu ifadesi yer almaktadır (Acer Inc., 2012). Bulut hizmet sağlayıcıların hizmetlerini sunmak amacıyla almış olduğu bu yetkinin de kullanım alanının çok geniş olduğu değerlendirilmektedir (Svantesson ve Clarke, 2010).

Bulut Alanlarının Saldırıların Hedefi Haline Gelmesi

Bulut bilişim sistemi üzerinde bulunan bilgilerin siber saldırı gibi nedenlerle kaybedilme riski olduğu gibi; kişisel bilgisayarlar üzerinde depolanan bilgilerin de zarar görme olasılığı bulunmaktadır. Fakat nasıl bir bankada müşterinin parasının yok olduğu kabul edilemez bir durum ise; kullanıcı için bedeli daima paha biçilemez olarak değerlendirilen bilgilerin bulut üzerinden kaybolması da kabul edilebilir değildir. Tüm internet teknolojisi kullanan servislerde olduğu gibi; bulut bilişim servislerinin de klasik internet saldırılarına (ortam dinleme, yetkisiz erişim, verilerin değiştirilmesi vd.) karşı savunmasız yönleri bulunmaktadır (Bisong ve Rahman, 2011). 2011 yılında meydana gelen büyük siber saldırılar ve veri kayıpları göz önüne alındığında; özellikle bulut sistemi gibi büyük verilerin bulunduğu alanların ve kişisel bilgilerin bulunduğu sistemlerin hedef olarak seçilmesi dikkat çekicidir (Lemos, 2011).

Bulut hizmeti alınan hizmet sağlayıcıların herhangi bir felaket durumunda sistemi ve verileri en kısa süre içerisinde tekrar erişilebilir hale getirmeleri ve bulut sistemi üzerinde bulunan kişisel verileri kriptolu olarak saklamak suretiyle mahremiyetin korunmasına özen göstermeleri önemlidir.

Adli İncelemelerin ve Dijital Delillerin Elde Edilmesi Konusundaki Belirsizlikler

Bir dijital bilginin delil olarak değerlendirilebilmesi için birtakım şartların yerine gelmiş olması gerekmektedir. Bulut sisteminde bilgilerin sanal ortamda bulunması, farklı kişilere ya da kurumlara ait bilgilerin aynı ortamda şifreli olarak bulunması, bu konuda nasıl bir yol izleneceği konusunda herhangi bir hukuksal düzenlemenin bulunmaması ve sistem yöneticilerinin verilere müdahale imkânının bulunması, ilk bakışta göze çarpan sorunlardır.

Bulut sistemi üzerinde yapılacak dijital delillerin incelenmesi esnasında; aynı ortamda bulunan ve suç konusu olmayan verilerin de açık hale gelmesi, farklı bir hukuksal problemin oluşmasına neden olabilecektir. Diğer taraftan, inceleme esnasında herhangi bir suç ile ilişkisi bulunmayan dosyaların yapısında da (son erişim zamanı vd.) değişiklik meydana geleceği için, daha sonra yapılacak herhangi bir incelemede delil niteliğinde değerlendirilemeyecektir.

Adli açıdan diğer önemli sorun ise; kullanıcının bulut sistemi üzerinden silmiş olduğu verilerin tamamen silindiğinden emin olamaması durumudur (Privacy Rights Clearinghouse-PRC, 2012). Bulut sistemi üzerinde bulunan verilerin silinmesi, kullanılan sistemin özelliğine bağlı olarak verinin geri dönüşümünün mümkün olmadığı anlamına gelmemektedir. Bu durum, kullanımdan yıllar sonra dahi kullanıcı ile silinmiş dosyalar arasında bağ kurulmasına neden olabilecektir (Henkoğlu, 2011). Ayrıca son kullanıcı gizlilik sözleşmelerinde, silinen bilgilerin yedeği alınan bilgi ortamlarından aynı anda silinemeyeceği açıkça ifade edildiği halde (bkz. Google Gizlilik Politikası) (Google, 2012), en fazla ne kadar süre sonra tamamıyla silinme işleminin gerçekleşmiş olacağına dair bilgi yer almamaktadır.

Kişisel Verilerin Gizliliği ve Korunması Konusunda Hizmet Sağlayıcıların Hukuksal Sorumlulukları: ABD, AB ve Türkiye Örneklerinin Değerlendirilmesi

Son kullanıcı sözleşmelerinde açıkça ifade edildiği gibi herhangi bir saldırı girişimi sonrası meydana gelen veri kaybı ve gizliliğin korunamaması ile ilgili olarak bulut hizmet sağlayıcılar sorumluluk almamaktadırlar. Fakat bulut bilişim endüstrisinin gelişebilmesi, gizliliğe hassasiyet göstermesi ve kullanıcıların güveninin kazanılmasına bağlıdır. Türkiye'de henüz bireylerin bulut bilişim veri alanları üzerindeki bireysel haklarını koruma altına alan ya da Türkiye sınırları içinde faaliyet gösteren bulut hizmet sağlayıcılarının verilerin korunması ile ilgili sorumluluk almalarını sağlayacak bir yasal düzenleme bulunmamaktadır.

ABD ve AB'nin bilgi politikaları içinde, bilgi güvenliği ve özellikle kişisel verilerin korunması konusuna geniş yer ayrılmaktadır. Çevrimiçi ekonominin canlandırılarak ekonomik büyümenin sağlanması hedefinin gerçekleştirilebilmesi için kişisel verilerin korunduğu bir bulut bilişim ortamının oluşturulması gerektiği bilinci oluşmuş ve bu konudaki sorunlar tartışılmaya başlanmıştır. Bireylerin etkin olarak kullanabilecekleri güvenli bir bulut ortamının oluşturulabilmesi ve hizmet sağlayıcıların kişisel verileri koruma konusunda sorumluluk almalarını zorunlu hale getirebilmek için verilerin korunması ile ilgili yasal düzenlemeler hızla güncellenmektedir.

Bulutun dünyanın her yerinden erişilebilir olması, kişisel verilerin gizliliği ve güvenliği konusunda da tehditlere açık olması anlamına gelmektedir. Kişisel Verilerin İşlenmesi ve Kişisel Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayılı AB Direktifi'nde kişisel veriler; "belirli veya belirlenebilir gerçek kişilere ait bütün bilgiler" olarak ifade edilmektedir. Direktifin 2. Maddesine göre; "Kişisel veri" olarak nitelendirilecek verilerin; üzerinde şifre taşıması, kimlik numarası bulundurması, fiziksel, zihinsel, fizyolojik, kültürel, ekonomik ya da sosyal kimliğe dair aidiyeti ifade etmesi ve belirli ya da belirlenebilir bir kişiye ait ayırt edici bilgiyi içermesi gerekmektedir (European Council, 1995). AB tarafından veri koruma direktifinde yapılması planlanan reform çalışmaları hakkında bilgiler içeren 25 Ocak 2012 tarihli bildiride de; kişisel veri "kişinin özel, iş hayatı ya da toplumsal hayatı ile bağlantısı olan ya da olmayan, kişi ile ilgili tüm bilgiler" olarak ifade edilmiş ve ayrıca kullanıcı gizliliğine konu olabilecek bilgilerin neler olduğu açıklanmıştır (European Commission, 2012b). Bu tanım ve belirtilen özellikler, Avrupa ve ABD'de yapılan yerel bilgi koruma kanunlarında ve bilgi güvenliği politikalarında da benzer şekilde yer almaktadır. AB hassas veriler içinde; ırk, politik düşünce, din vd. inançlar, sağlık bilgileri, adli bilgiler ve özel yaşam bilgilerini tanımlamaktadır. Fakat bazı üyeler kişisel bilgilerin de bu tanım içerisine dâhil edilmesi gerektiğini düşünmektedirler. Coğrafi yer bilgileri de hassas veri tanımlaması içinde olmadığı halde, AB'de kaygı duyulan konulardan biridir (King ve Raja, 2012).

ABD'de Bulut Bilişime Dönük Hukuksal Koşullar

ABD'de henüz hassas verinin tanımının açık bir şekilde yapıldığı ya da kişisel bilgilerin gizliliğini koruyan ve verilerin başka ülkelere transferini kısıtlayan kapsamlı bir düzenlemenin (AB Veri Koruma Direktifi gibi) bulunmadığı görülmektedir. Fakat federal kanunda hassas veri olarak nitelendirilebilecek verilerin neler olabileceği (sağlık, finansal vb.) belirtilmiş ve gizlilik gereksinimi için belirli kısıtlamalar getirilmiştir (King ve Raja, 2012). Hassas veri olarak nitelendirilen verilerin bulunduğu alanlar;

- ◊ Web sitelerinin 13 yaş altındakilerden kişisel bilgi toplaması (FTC, 1998),
- ◊ Finansal kuruluşların müşterileri ile ilgili kişisel bilgi toplaması (U.S.C., 1999),
- ◊ Sağlık kuruluşlarının hastaları ile ilgili toplamış oldukları sağlık bilgileri (U.S.C., 1996),
- ◊ Kredi ajanslarının müşteri kredi geçmişleri ile ilgili bilgileri toplamasıdır (FTC, 2011).

Federal Ticaret Komisyonu (FTK)[1] tarafından hazırlanan Tüketici Koruma Yasası da ABD'de kişisel bilgilerin korunması konusunda rol üstlenmiştir. FTK, her ne kadar hassas verinin tanımını yapmamış olsa da; finansal verileri, çocuklara ait verileri, sağlık bilgilerini, coğrafi yer bilgilerini ve kurumlar tarafından verilen kimlik numaralarını (Sosyal güvenlik numarası) bu kapsamda değerlendirmektedir (King ve Raja, 2012). ABD'de kullanıcıların, sağlık kayıtları, etnik bilgileri, inançları, cinsel tercihleri, coğrafi yer bilgileri, finansal bilgileri, biyometrik verileri ve sosyal güvenlik numarası gibi hassas verileri tanımlayan ve kişisel bilgileri korumak üzere hazırlanmış yasa önerileri de bulunmaktadır (U.S.C., 2011).

Genel olarak belirtilen bu alanlardaki verilerin bulut üzerinde bulunması halinde hukuksal açıdan gizlilik ve güvenliğin dikkate alınacağı görülmektedir. Ayrıca; bu dört alanda toplanan kişisel bilgilerin sadece kendi alanında kullanılması ve başka hiçbir suretle ifşa edilmemesi gerekmektedir. Federal düzenlemeler, şirketlerin minimum güvenlik kurallarına uymalarını istemekte ve bu konuda onları özendirmektedir. Örneğin sağlık kuruluşları kişisel sağlık bilgilerinin güvenliğini sağlamak zorunda iken; bilgileri kriptolayarak saklamak zorunda değillerdir. Fakat bilgiler yeterli seviyede kriptolanarak saklanırsa, bilgiye yetkisiz erişim olması halinde bunu kamuoyuna duyurmak zorunda kalmayacaklardır. Böylece gereksiz masraf, müşteri kaybı ve itibar kaybı oluşmayacaktır. Bu yüzden birçok sağlık kuruluşu verileri kriptolamayı tercih etmektedir. Eğer sağlık kuruluşu hastaların bilgilerini farklı bir ülkede bulunan bulut sistemi üzerine taşırsa ve bu sistem üzerinde bilgi güvenliği ihlali gerçekleşirse; bu durumda (sağlık kuruluşunun sorumluluğu devam ederken) bulut hizmeti sağlayıcısı ABD yasaları gereğince sorumlu tutulmamakta ve sadece yapılmış olan sözleşme çerçevesinde sorumluluk taşımaktadır. Ayrıca; sağlık kuruluşu meydana gelen bilgi güvenliği ihlalini duyurmak zorundadır. Bu konuda genel bir yasal düzenleme bulunmasa da, her eyalet kendi sınırları içinde meydana gelen güvenlik ihlallerinden kullanıcıların haberdar edilmesini, belirlemiş olduğu "veri güvenliği ihlali bildirim kuralı" çerçevesinde şirketlerden istemektedir (King ve Raja, 2012). Bu kurala uymamanın cezai yaptırımları da bulunmaktadır.

AB'de Bulut Bilişime Dönük Hukuksal Koşullar

AB, kişisel verilerin korunması amacıyla birçok alanda yasal düzenlemeler yapmıştır. Fakat 95/46/EC sayılı direktif, geçerli veri koruma direktifi olması ve yeni gelişmelere uygun olarak hazırlanan direktif taslaklarının da temelini oluşturması yönüyle önem taşımaktadır. 95/46/EC sayılı direktif, bulut bilişim ve bireylerin korunmasına ilişkin şu noktalara açıklık getirmektedir (European Council, 1995):

◊ Hizmet sağlayıcılar, içeriğe bakmaksızın veri işleme yükümlülüklerini yerine getirerek ve belirli kurallara uyarak; kişisel verilerin korunması konusunda kullanıcıların temel haklarını korumak zorundadırlar.

1 Federal Ticaret Komisyonu (FTC - U.S. Federal Trade Commission): Kredi kartı ve güvenlik kodları gibi kişisel bilgilerin korunmasını inceleyen ve önlemler alan kuruluştur.

- ◊ İşyerleri herhangi bir meşru ya da açık gerekçe olmadıkça, kişisel bilgileri toplama, kaydetme, kullanma ve açığa vurma konusunda kısıtlanmışlardır.
- ◊ Veri sahibi; verinin nasıl işlendiği, nasıl saklandığı ve kim tarafından erişildiği konusunda bilgilendirilmek zorundadır. Şirketlerin işlediği verileri amacı dışında sonradan kullanımı yasaklanmıştır.
- ◊ Veri sahibi hakkında, konu ile ilgili olarak (sağlık bilgileri vd.) en az seviyede kişisel bilgi kaydedilmelidir. Bu bilgilerin güvenliğinin sağlanması ve yetkisiz erişimlerden korunması zorunludur.
- ◊ AB sınırları içinde faaliyet gösteren şirketler, bilgi işleme ve bilgiyi diğer şirketlerle paylaşma (AB alanı dışı dâhil) konusunda yasal yükümlülüklere uymak zorundadırlar. Kullanıcılar da söz konusu veriler üzerinde hak sahibidirler.
- ◊ Bulut üzerinden kişisel veri toplayan ve işleyen şirketler, bulut alt yapısının kendisi ya da farklı bir hizmet sağlayıcı tarafından sağlandığına bakılmaksızın bilgi güvenliği sorumluluğunu yerine getirmek zorundadırlar.

Bulut sisteminin karakteristiği, kullanıcı bilgilerinin sunucu üzerinde bulunmasını gerektirmektedir. Fakat 95/46/EC sayılı direktifte; kullanıcıya ait kişisel bilgilerin transfer edilen ülke tarafından yeterli seviyede güvenliği sağlamadığı müddetçe, AB ekonomik alanı dışına transferi yasaklanmıştır. Bu nedenle bulut hizmeti sağlayıcılar; AB alanı içinde yeni sunucular tesis etmek ve kullanıcıların her konuda bilgilendirilmesi gibi normalde uygulamadıkları işlemleri yaparak, bilgi ve erişim güvenliğini sağlamak için daha fazla sorumluluk almak zorunda kalmışlardır. 95/46/EC sayılı direktife uygun olarak alınan 26 Temmuz 2000 tarih ve 2000/520/EC sayılı Avrupa Komisyonu kararında; AB'den ABD'ye bilgi transferi yapılabilmesi için; bilgiyi transfer edecek şirketin "Safe Harbour Anlaşması"[2] üyesi olma durumu istisnai bir durum olarak belirlenmiştir (European Commission, 2004). Anlaşmanın üyesi olan şirket, üye olabilmek için gerekli şartları taşıdığı için ayrıca saygınlık kazanmaktadır.

AB İçindeki Bulut Bilişime Dönük Farklı Yaklaşımların Bütünleştirilmesi ve Yeni Eğilimler

Kişisel verilerin gizliliği konusu, internetin gelişim süreci ile birlikte farklı platformlarda en fazla tartışılan konuların başında gelmektedir. AB Komisyonu'nun özellikle 2009 yılından itibaren, AB veri koruma kanunu ve kişisel verilerin gizliliği ile ilgili tanım ve kapsamın gözden geçirilmesi konusunda daha fazla çaba gösterdiği görülmektedir. 95/46/EC sayılı direktifin neden güncellenmesi gerektiği konusu ve bu konuda izlenecek yöntemler 2010 yılında AB gündemine taşınmıştır. 4 Kasım 2010 tarihinde

2 Safe Harbour Agreement (Güvenli Liman Anlaşması): ABD ticaret bakanlığı ile AB arasında 2000 yılında yapılan, AB sınırları içindeki ülke vatandaşlarının kişisel bilgilerinin ABD şirketleri tarafından transferini belirli şartlara bağlayan bir anlaşmadır. Anlaşma gereğince; şirketler topladığı veriler ve bu verileri hangi amaçla kullandığı konusunda kullanıcıyı bilgilendirmek ve aynı zamanda gerekli tüm bilgi güvenliği önlemlerini almak zorundadır. Şirketlerin bu anlaşmanın üyesi olabilmeleri için, tüm AB üyesi ülkelerden ayrı ayrı onay almak zorundadırlar.

yayınlanan IP/10/1462 referans numaralı "Kişisel Verilerin Nasıl Korunacağına İlişkin Strateji" (European Commission, 2010b) ve MEMO/10/542 referans numaralı bildiriler (European Commission, 2010c), veri koruma direktifinde yapılacak reformlar hakkında fikir veren önemli belgelerdir.

Tam olarak anlaşılamayan ve AB içindeki her ülkede farklılık gösteren veri koruma yasalarının, kullanıcılar arasında çevrimiçi alışverişe karşı güvensizlik yaratması ve bunun Avrupa çevrimiçi ekonomisini olumsuz etkilemesi, çalışmaların temel gerekçesi olarak gösterilmektedir (European Commission, 2012c). Dijital Ajanda içerisinde yer alan AB Sayısal Tek Pazar Projesi ile ilgili olarak atılacak adımların içinde bulut-dostu politikalara da yer verilmiş ve bu politikaların uygulanması halinde 2,5 milyon fazladan iş olanağı yaratılarak ekonomiye 2020 yılına kadar olan süreçte önemli katkı sağlanacağı ifade edilmiştir. AB Komisyonu'nun Ocak 2012 yılında yapmış olduğu çalışmalarda; bulut bilişim kullanımının önündeki en büyük engelin veri koruma kaygısının olduğu ve en kısa sürede (2013 yılı içinde) AB Konseyi ve Parlamentosu'nun düzenleme üzerinde çalışmasının önemli olduğu belirtilmiştir. Fakat yapılacak olan düzenlemede, AB üyesi olmayan bir ülkeden hizmet veren bulut hizmet sağlayıcıların ve AB üyesi olmayan ülke kullanıcılarının nasıl tanımlanacağı konusunda belirsizlikler devam etmektedir (European Commission, 2012a).

AB'nin bilgi politikaları içinde bulut bilişime yaklaşımı ve ulaşılmak istenen hedef, veri koruma direktifleri ile ilgili çalışmalarda açıkça görülebilmektedir. Bilgi ve iletişim teknolojilerinin kullanılarak çevrimiçi ekonominin canlandırılması, bulut bilişimin etkin kullanımı ile yakın ilişkilidir. Fakat bireylerin bulut bilişimin kullanımı ile ilgili olarak bireysel haklarının yeterince korunup korunmadığı konusundaki çekinceleri, bu süreci olumsuz etkileyen etkenlerden biri haline gelmiştir. Mevcut 95/46/EC sayılı veri koruma direktifinin yeni internet servislerinin (bulut bilişim, sosyal paylaşım siteleri vd.) kullanımı ve sunulması konusunda yetersiz kalması ya da belirsizlikler bulunması; 2010 yılında başlayan çalışmaların da şekillendirilerek, veri koruma kanununda kapsamlı bir reform niteliğinde olan IP/12/46 referans numaralı yeni kişisel verilerin korunması taslağının oluşmasını sağlamıştır (European Commission, 2012d). 25 Ocak 2012'de AB Konseyi ve Parlamento'nun onayına sunulan IP/12/46 referans numaralı yeni kişisel verilerin korunması taslağı; bulut bilişim üzerinde meydana gelebilecek birçok risk ile ilgili yenilikler içermektedir. Bunlardan ön plana çıkan bazı konular; kişisel verilerin hizmet sağlayıcılar arasındaki transferi, kişisel verilerin hangi şartlarda elde edilebileceği konusuna açıklık getirilmesi, veri öznesinin çevrimiçi veri koruma haklarını yönetebilmesini sağlayan "unutulma hakkı", bilginin işlenmesi ile ilgili her aşamada ve oluşan güvenlik ihlali ile ilgili durumlarda veri öznesinin bilgilendirilmesidir (European Commission, 2012e).

AB'de hukuksal düzenlemelerin yanı sıra, uygulamaya ilişkin bilinçlendirme çalışmalarının da eş zamanlı olarak yürütülmesine özen gösterilmektedir. Bu konuda yeni politikalar üretmek ve kurumlar arası koordinasyonu sağlamak için Avrupa

Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency–ENISA) kurulmuştur. ENISA, bilinçlendirme çalışmaları yapmak ve bilgi güvenliği üzerinde politikalar üretmekle sınırlı kalmayıp, kullanıcılara uyguladığı anketlerle mevcut durumun analizini de sık aralıklarla yapmakta ve bu alandaki çalışmalara yön vermektedir (ENISA, 2012).

Türkiye'de Bulut Bilişime Dönük Hukuksal Koşullar

Bulut bilişimin hukuk alanında birçok kargaşaya sebep olacağı ve bankacılık sektörünün internet alt yapısını kullanarak hizmet vermeye başladığı ilk dönemlerde olduğu gibi, hak aramak için yeterli güce sahip olamayanların mağdur olabilecekleri, mevcut yasal düzenlemelerin yetersizliği karşısında öngörülebilir bir durumdur. Bulut bilişimde hizmet sağlayıcılar ile kullanıcılar arasındaki ilişki, sadece hizmet sözleşmeleri ile sınırlı olup, özellikle hizmet sağlayıcıdan kaynaklanan ihtilafın giderilmesi konusunda kullanıcının tutunabileceği hukuksal dayanaklar bulunmamaktadır.

Türkiye'de bulut bilişimde kişisel bilgilerin gizliliği ve verilerin korunması ile ilgili herhangi bir yasal düzenleme bulunmamaktadır. Bu koşullar altında kişisel bilgileri dilediği gibi toplayan, kullanan ve korumak için yeterli önlemi almayan hizmet sağlayıcılara dava açılabilmesi mümkün değildir. Mevcut "Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı" üzerinde ise 15 yıldır değişiklikler yapılmaktadır. AB veri koruma direktifleri ile uyumlu olarak hazırlanan son tasarı da henüz yasalaştırılamamıştır (KVKKT, 2012). Tasarının yasalaşması; bilişim sektörünün ihracatının büyümesi, AB ülkeleri ile bilgi alış-verişini sağlayan ilişkilerde Türkiye'nin güvenli ülke olarak görülmesi ve bireylerin anayasal haklarını koruyarak bilgi teknolojilerini kullanmalarını sağlaması açısından da önem taşımaktadır.

Türk hukuk mevzuatında kişisel bilgilerin gizliliğinin korunması konusuna, Anayasa'nın 20. Maddesi (2010 yılında Ek yapılarak) (T.C. Anayasası, 1982) ve Türk Ceza Kanunu'nun (TCK) 135 ve 136. Maddelerinde (Türk Ceza Kanunu, 2004) yer verildiği görülmektedir. Fakat Anayasa ve TCK'daki düzenlemelerin AB sınırları içinde 1998 yılından itibaren uygulanan ve yeni teknolojiler karşısında yetersiz olduğu düşünülen veri koruma yasasının koruma düzeyinde dahi olmadığı değerlendirilmektedir. Ayrıca bulut bilişim hizmet sağlayıcılarının kullanıcı ile yapmış oldukları hizmet sözleşmelerinde herhangi bir ihtilaf olması halinde hangi mahkemenin yetkili olacağı ve hangi durumlarda hukuksal hak iddia edilemeyeceği belirtilmektedir. Bu durumun aşılarak kullanıcı haklarının korunabilmesi için konu ile ilgili yasal düzenlemelerin yapılması gerekmektedir. Los Angeles şehri kamu yöneticilerinin, Google uygulamalarını kullanmaya başladıklarında verilerin ABD içinde kalmasını öngören sözleşmede ısrarcı olmaları ve bununla herhangi bir ihtilaf durumunda ABD dışındaki mahkemelere gitme olasılığını ortadan kaldırmaları, konunun uygulamadaki örneklerinden biridir (Thibodeau, 2011).

Hizmet sözleşmelerinde yetkili mahkeme olarak Türkiye sınırları dışında bulunan bir mahkemenin adres gösterilmesi, herhangi bir ihtilaf halinde hak iddia edebilmek için uluslararası boyutta ve maliyetli bir hukuk mücadelesinin gerekeceği anlamına gelmektedir. Hizmet sözleşmelerinde yetkili mahkemenin yer almaması ve hizmet sağlayıcının sunucularının farklı bir ülkede bulunması halinde ise bu tür hizmet anlaşması ve yabancı ülkede işlenen suçlar konusunda bireylerin başvurmayı düşünebileceği sadece TCK'nın 12. ve 13. Maddelerinin bulunduğu görülmektedir (Türk Ceza Kanunu, 2004). Ancak mağdura karşı Türkiye dışında işlenen suçlarda, mağdurun korunmasını esas alan TCK'nın 12. Maddesinde, suçu yabancı ülkede işleyen failin Türkiye'de bulunması şartı yer aldığı için bulut bilişim konusunda bu maddenin koruyucu olabilmesi, hizmet sağlayıcının Türkiye'de temsilcisinin bulunmasına bağlıdır. TCK'nın 13. Maddesinde ise yabancı ülkede işlenen diğer suçlar yer almaktadır. Fakat bu maddede yer alan katalog suçlar arasında da bilişim suçları yer almadığı için, bulut ile ilgili ihtilaflarda çözüm maddesi olmaktan uzaktır. Yetkili mahkemenin belirtilmediği ve hizmet sağlayıcıların üçüncü bir ülkeden veri alanı kiralayan farklı ülkelerdeki hizmet sağlayıcılar ile anlaşarak hizmet sunması durumu ise uluslararası hukukta ihtilaflara karşı henüz çözüm üretilemeyen konular arasında yer almaktadır.

Türkiye'nin kişisel verileri ve bireysel hakları korumak amacıyla Avrupa Konseyi tarafından yapılan önemli sözleşmelerde imzası bulunmaktadır. Fakat bunların hiçbiri iç hukuka uyumlu hale getirilerek uygulamaya geçirilememiştir. Avrupa Konseyi tarafından imzaya açılan veri koruma alanında yapılan ilk uluslararası hukuk düzenlemesi, 108 no'lu sözleşme (Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkındaki Sözleşme)'dir (European Commission, 1981). 2001 yılında bu sözleşmeye ek olarak, bulut bilişim hizmetlerini de yakından ilgilendiren 181 no'lu Ek Protokol (Denetleyici Makamlar ve Sınır Ötesi Veri Akışına İlişkin Protokol) kabul edilmiştir (European Commission, 2001). Türkiye'nin 28 Ocak 1981 tarihinde imzalamış olduğu 108 no'lu sözleşmenin onaylanabilmesi için iç hukuka uyumlu hale gelmesini sağlayacak "Kişisel Verilerin Korunması Kanun Tasarısı"nın yasalaşması gerekmektedir. Başka bir ülkeye veri transferinin standartlaştırılması, kişisel verilerin korunması ve bağımsız bir denetim kurumunun oluşturulması amacıyla imzaya açılan 181 Ek Protokol de 8 Kasım 2001 tarihinde Türkiye tarafından imzalanmış, fakat iç hukukta onaylanmamıştır. 108 no'lu sözleşmenin onaylanması, 181 no'lu Ek Protokolün de onaylanmasının ön şartıdır. Türkiye, 46 ülke içerisinde 108 no'lu sözleşme ve 181 no'lu protokolü iç hukukta onaylamayan Rusya ile birlikte 2 ülkeden biridir (European Commission, 2012f). Fakat Rusya'da veri koruma ile ilgili ulusal yasa ve bilgi güvenliği politikaları bulunmaktadır. Rusya, AB'nin 1995 tarihli Veri Koruma Kanunu'nu da kapsayan 108 no'lu sözleşmeyi 20 Aralık 2005 tarihinde onaylayarak iç hukukta uygulamaya başlamıştır. Rusya Federasyonu, kişisel verilerin korunması ile bilgi ve bilgi teknolojilerinin korunması hakkında kapsamlı uyum yasasını da Haziran 2006'da çıkarmıştır (Hohlov ve Shaposhnik, 2006).

Uluslararası bilişim suçları ile ilgili olarak Avrupa Konseyi tarafından hazırlanan en önemli hukuki belgelerden biri de 185 no'lu Siber Suçlar Sözleşmesi'dir (European Commission, 2001). Uluslararası hukukta bilişim suçları ile ilgili boşlukların bulunması ve soruşturma, kovuşturma ve diğer adli işlemlerin nasıl yapılacağı konusundaki belirsizlikler, Avrupa Konseyi'ni siber suçlarla mücadele konusunda harekete geçirmiştir. ABD'nin de katkısıyla hazırlanarak 23 Kasım 2001 tarihinde imzaya açılan 185 no'lu Siber Suçlar Sözleşmesi'ni, Türkiye 10 Kasım 2010 tarihinde imzalamıştır. Fakat henüz iç hukukta gerekli yasal düzenlemeler yapılarak Siber Suçlar Sözleşmesi uygulamaya geçirilememiştir.

Bulgular Çerçevesinde Bulut Bilişim Sistemlerinde Temel Bilgi Güvenliği Uygulama Modeli

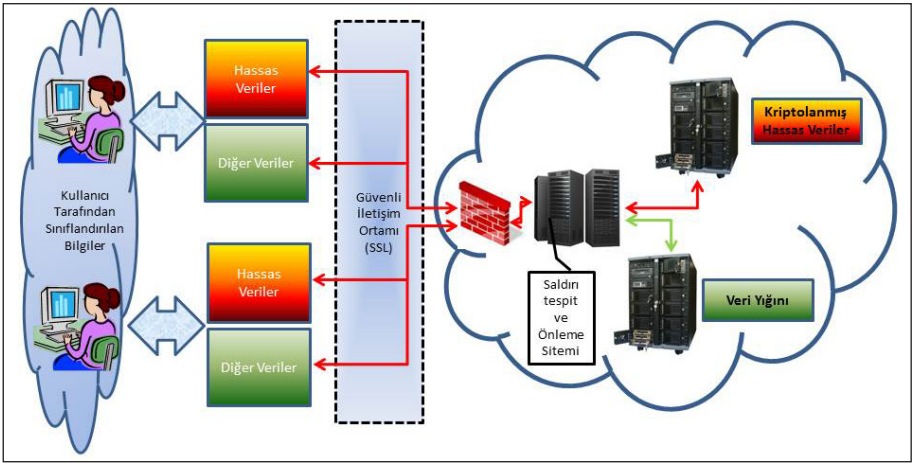
Bilginin sınıflandırılması, bulut bilişim güvenliğinin en öncelikli adımlarından biridir. Çünkü bilginin herhangi bir elektronik ortamda güvenliğinin ve gizliliğinin korunabilmesi için öncelikle o bilginin değerinin ortaya konulması gerekmektedir. Örneğin, bir bilginin "hassas bilgi"[3] olarak tanımlanması, o bilginin güvenliğinin ve gizliliğinin nasıl ve hangi yükümlülüklerle ilgili olarak korunacağı konusunda ayrıcalık yaratmaktadır. Zira bulut üzerinde bulunan tüm verilerin en üst seviyede teknikler (kriptolama vd.) kullanılarak koruma altına alınması, günlük bilgi üretim miktarı göz önüne alındığında, maliyetleri çok yüksek seviyelere çıkaracağı için tercih edilebilir ya da gerçekçi bir yaklaşım olmayacaktır.

Bilginin sınıflandırma işleminin, kullanıcı tarafında bulut sistemine transferi öncesinde yapılması ve bulut hizmet sağlayıcılarının bu sınıflandırmayı dikkate alarak hizmet sunması; bulut bilişim üzerinde alınabilecek en etkili önlemlerden biridir. Bu yapının sağlıklı çalışabilmesi için Şekil1'de gösterilen basit model önerilebilir.

Şekil 1'de sunulan modelde, bulut sistemine ulaşıncaya kadar olan süreçte bilginin izlediği yol, bankacılık sisteminde uygulanan güvenlik tedbirleri ile benzer niteliktedir. Bu modelde, kullanıcıların bankacılık hizmetlerinde olduğu gibi, hizmet aldıkları sunucuların nerede olduğu ve hangi seviyede güvenli hizmet verildiğini bilmedikleri; fakat belirli bir standardı sağlamayan bir hizmet sağlayıcının faaliyet gösteremeyeceği öngörülmektedir. Güvenli iletişim ortamında kullanılacak güvenlik protokolleri (SSL[4]-Secure Socket Layer), giriş kısıtlamaları, kimlik doğrulama ve tek kullanımlık şifre uygulaması; bulut hizmeti veren hizmet sağlayıcı tarafından uygulanmalı ve yeterli bilgi güvenliği standardını karşılayacak düzeyde olmalıdır. Şekil-1'deki model üzerinde; kullanıcı tarafından sınıflandırılan tüm bilgiler, çeşitli güvenlik protokolleri kullanılarak

3 Hassas Bilgi: Gizli tıbbi gerçekler, ırklar veya etnik kökenler, siyasi veya dini inançlar ya da cinsellikle ilgili belirli bir kişisel bilgi kategorisidir (Google, 2012).

4 Secure Socket Layer (Güvenli Yuva Katmanı): 1994 yılında Netscape tarafından geliştirilen ve internet üzerinden şifreli veri iletişimi sağlayan güvenlik protokolüdür. SSL 3.0 sürümü tüm web tarayıcılar tarafından desteklenmektedir.



Şekil 1. Güvenli Bulut Bilişim Modeli

sağlanan güvenli iletişim ortamından geçerek, bulut hizmetinin sunulduğu alana ulaşır. Bu alana ulaşan bilgiler, güvenlik duvarı ve saldırı tespit/önleme sistemleriyle zararlı kodların tespiti ve sonrasında kimlik denetimi gibi bir dizi güvenlik kontrolünden geçirilir. Kullanıcı tarafından sınıflandırılan veriler, iki farklı sunucu ya da depolama alanına yönlendirilir. Hassas bilgilerin bulunduğu alan kriptolanmak suretiyle üst seviyede bilgi güvenliği önlemi alınır. Böylece, bu alana ilişkin olarak yapılan zararlı kod saldırıları ve yetkisiz erişimler sonucunda veri bütünlüğü ve gizliliğin sağlanması konusunda meydana gelebilecek zafiyetlerin önüne geçilir. Bu model, minimum seviyede bulut bilişim bilgi güvenliğini standart hale getirmeyi öngördüğü için hassas bilgilerin üzerinde bulunduğu veri depolama alanında kullanılacak sanal depolama alanı işlemleri ve dosya sistemi güvenliği ile ilgili detaylara yer verilmemiştir. Paylaşılan veri depolama alanlarında bilgi güvenliği risklerinin bulunması her zaman mümkündür.

Bu modelin en basit düzeyde dahi uygulamaya geçirilebilmesi noktasında, yasal düzenlemeler ve bilgi güvenliği politikalarına ihtiyaç duyulmaktadır. Bankacılıkla ilgili 5411 Sayılı Bankacılık Kanunu çerçevesinde hazırlanmış düzenlemelerde (Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ) olduğu gibi (BDDK, 2007); belirli kriterlerin belirlenmesi, belirli aralıklarla bilgi güvenliği denetimlerinin yapılması ya da sertifikalandırma sisteminin oluşturulması, bu alanda faaliyet gösteren şirketlerin gerekli sorumluluğu almaları için zorlayıcı bir unsur olacaktır. Bankacılık sektöründe ve hatta internet toplu kullanım sağlayıcılarının faaliyet alanlarındaki sınırları belirleyen yönetmelikler dahi yapılmış ve uygulanıyorken; bulut bilişim hizmeti verecek olan şirketlerin faaliyetlerini icra ederken kullanacakları bilgi sistemlerinin yönetimi amacıyla uymak zorunda oldukları usul ve esasları gösteren bir düzenlemenin bulunması da aynı derecede önem taşımaktadır.

Sonuç ve Öneriler

Bilgi güvenliğinin sağlanması öncelikli olmak üzere bulut bilişim üzerinden hizmet alan kullanıcıları bekleyen birçok risk bulunmaktadır. Bulut bilişime geçiş aşamasının sorunları olarak nitelendirilebilecek bu risklerden uzak kalınabilmesi için, sürecin iyi yönetilmesini sağlayacak birtakım kuruluşlara ihtiyaç duyulmaktadır. Her yeni teknolojinin günlük hayata girişinde birtakım problemlerin olması normal karşılanmakla birlikte, mümkün olan en az olumsuz etkiye maruz kalınabilmesi için kullanıcıların en doğru aşamada bilinçlendirilmesi önemlidir. AB ve ABD'de bu tür bilinçlendirme çalışmalarını yapmak ve kurumlar arası koordinasyonu sağlamak için bazı kuruluşlar oluşturulmuş ve çeşitli çözüm politikaları üretilmeye başlanmıştır. AB ve ABD'de bulut bilişim, bilgi ve iletişim teknolojilerinin yöneldiği odak nokta olarak görülürken; bulut bilişimin beraberinde getirdiği sorunlar da en az faydaları için olduğu kadar irdelenmiş ve geçiş süreci adı altında bir dizi bilgi güvenliği politikası ve proje uygulamaya konulmuştur. Fakat kullanıcılara ait hassas bilgilerin bulut ortamında yeterince korunabilmesi için gizlilik ve güvenlik ile ilgili AB ve ABD yasalarının da gözden geçirildiği görülmektedir.

Bulut bilişim, mobil iletişim çağı olarak da nitelendirilebilecek hızlı bir dönüşümün en popüler bilgi ve iletişim araçlarından biri haline gelmiştir. Günlük yaşamda maliyetlerin düşürülmesi, erişim ve kullanım kolaylığı noktasında sunduğu avantajlarının yanı sıra; bulut bilişimin beraberinde getirdiği riskler de küçümsenemeyecek kadar önemlidir. Bulut stratejisi geliştirirken; kullanıcı dostu olduğu kadar, aktif olarak kullanılan bir bulut için düzenleme ihtiyacı öngörülmektedir.

Türkiye'de bilgi güvenliğinin sağlanması ve kişisel verilerin korunması konusunda hukuksal alt yapının oluşmadığı ve kullanıcıların siber ortamda bilgi güvenliğine ilişkin önlemleri ve sorumluluğu alma konusunda yalnız bırakıldığı görülmektedir. AB içerisinde yapılan birçok çalışma ve sözleşmede (108 ve 185 no'lu sözleşmeler vd.) Türkiye'nin de imzası bulunmasına rağmen, iç hukukta gerekli düzenlemeler yapılamadığı için uygulamaya geçirilememektedir. Bulut hizmet sözleşmelerinde yer alan ve sadece belirli ülkelerin (ABD, Avusturalya, AEA ve İsviçre gibi) kullanıcılarını kapsayan güvenlik maddelerinin (tüketici yasal hakları ve verilerin aktarılması ile ilgili) Türkiye'de bulut hizmetlerini kullanan kullanıcılar için de uygulanabilmesi için, gerekli yasal düzenlemeler yapılmalıdır.

Türkiye'de de bulut bilişim hizmetlerinden faydalanan kullanıcıların veri güvenliği ve gizliliklerinin bulut üzerinde korunduğundan emin oldukları bir reform yapılması gerekmektedir. Bulut bilişim, çok geniş bir hukuki sorumluluk alanı içinde yer almaktadır. ABD'de federal yasa ile korunmaya çalışılan ve Avrupa Konseyinin 108 sayılı Sözleşmesi ve 181 sayılı ek Protokolü ile belirli bir çerçeveye alınan kişisel verilerin korunması kavramı, Türkiye'de henüz hukuksal boyutuyla ilgi ve gündemden uzaktır. Bulut bilişim hizmetinden faydalanan kullanıcıların kişisel verilerinin etkin bir şekilde korunması ve aynı zamanda bulut bilişim hizmet sağlayıcılara olan güvenin artması için, Kişisel Verileri Koruma Kanun Tasarısının en kısa zamanda yasalaşması önemlidir.

Bulut bilişim alanında var olan riskleri en aza indirerek, bilgi ve iletişim teknolojileri kullanımının yükselen değeri olan bulut sisteminin azami ölçüde ve güvenle kullanabilmesini sağlamak için alınması gereken öncelikli önlemler şu şekilde sıralanabilir;

◊ Ulusal bilgi güvenliği politikası geliştirilmeli ve içinde bulut bilişim konusuna özel olarak yer verilmelidir.

◊ Hassas bilgilerin neler olduğunun da açıkça belirtildiği kişisel verileri koruma ile ilgili yasal düzenleme yapılarak yürürlüğe konulmalıdır.

◊ Bulut bilişim hizmeti sunacak hizmet sağlayıcıların, hizmet alanında faaliyet gösterebilmek için gerekli ön şartların veya uluslararası standartların (ISO 27001-2005[5] vb.) belirlenerek sağlaması zorunluluğu getirilmeli ve bir sertifikasyon sistemi içinde derecelendirilmelidir.

◊ Veri güvenliğinin ve kişisel bilgilerin korunabilmesi için en temel çözüm, güvenli iletişim ve verilerin kriptolanmasıdır. Bu nedenle; bulut bilişim hizmeti sunacak hizmet sağlayıcıların, örnek modelde yer alan temel güvenlik önlemlerini standart olarak kullanmalarını sağlayacak yasal düzenlemeler ve denetimleri yapılmalıdır.

◊ Bulut bilişim hizmeti sunan hizmet sağlayıcılarının, belirlenen bilgi güvenliği kriterleri çerçevesinde denetimi yapılmalıdır.

◊ Kullanıcılar tarafından hizmet alacakları bulut hizmet sağlayıcıların özenle seçilmesi ve kullanıcı hizmet sözleşmelerinin içeriğinden haberdar olmaları için farkındalığı artırmaya ilişkin eğitim programların düzenlenmesi gerekmektedir .

◊ Kullanıcı verilerinin ve meydana gelebilecek felaketler sonrası mahremiyetin korunabilmesi için güvenli iletişim protokolleri ve üst seviyede kimlik doğrulama standartlarını kullanım zorunluluğu getiren yasal düzenlemeler yapılmalıdır.

◊ Türkiye'de bulunan bulut sistemi kullanıcılarının uluslararası ihtilaf, bilişim suçları ve kişisel verilerin korunması kapsamında haklarının korunması ya da haklarını arama imkânının sağlanabilmesi için uluslararası düzeydeki çalışmalara (AB sözleşmeleri gibi) ortak olunmalı ve işbirliğini geliştirici uyum sağlama çalışmaları hızlandırılmalıdır.

Kaynakça

Acer Inc. (2012). *AcerCloud Son Kullanıcı Lisans Sözleşmesi.* 1 Kasım 2012 tarihinde https://www.cloud.acer.com/ops/showEula adresinden erişildi.

BDDK. (2007). *Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ.* 11 Kasım 2012 tarihinde http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=9.5.11621&MevzuatIliski=0&sourceXmlSearch=banka adresinden erişildi.

5 ISO 27001-2005: Bilgi Güvenliği Yönetim Sistemleri, hassas ve gizli verilerin güvenliğinin sağlanması konusunda sistematik bir yaklaşım ile gereksinimleri tanımlayan uluslararası standarttır.

Bisong, A., ve Rahman, S. (2011). An overview of the security concerns in enterprise cloud computing. *International Journal of Network Security & Its Applications (IJNSA), 3*(1), 30-45.

Bourne, J. (2012). *Cloud downtime cost £45m over five years, IWGCR claims*. 24 Kasım 2012 tarihinde http://www.cloudcomputing-news.net/news/2012/jun/20/cloud-downtime-cost-45m-over-five-years-iwgcr-claims/ adresinden erişildi.

Digital Agenda. (2010). *Digital agenda: Commission outlines measures to deliver fast and ultra-fast broadband in Europe.* 15 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_IP-10-1142_en.pdf adresinden erişildi.

DPT. (2011). *Bilgi toplumu istatistikleri - 2011.* Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı.

ENISA. (2009). *Cloud computing - benefits, risks and recommendations for information security*. 26 Kasım 2012 tarihinde http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport adresinden erişildi.

ENISA. (2012). *An SME perspective on cloud computing exit this survey* . 29 Ekim 2012 tarihinde http://www.surveymonkey.com/s.aspx?sm=CZdVubBa9LIzYlR3KNeZlQ_3d_3d adresinden erişildi.

European Commission. (1981). *Convention for the protection of ındividuals with regard to automatic processing of personal data*. 27 Kasım 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm adresinden erişildi.

European Commission. (2001). *Additional protocol to the convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and transborder data flows*. 27 Kasım 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm adresinden erişildi.

European Commission. (2001). *Convention on cybercrime*. 27 Kasım 2012 tarihinde http://conventions.coe.int/treaty/en/treaties/html/185.htm adresinden erişildi.

European Commission. (2004). *Commission staff working document.* 4 Aralık 2012 tarihinde http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf adresinden erişildi.

European Commission. (2010a). *European broadband: Investing in digitally driven growth.* 15 Aralık 2012 tarihinde http://ec.europa.eu/information_society/activities/broadband/docs/bb_communication.pdf adresinden erişildi.

European Commission. (2010b). *European Commission sets out strategy to strengthen EU data protection rules.* 12 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_IP-10-1462_en.pdf adresinden erişildi.

European Commission. (2010c). *MEMO/10/542.* 12 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_MEMO-10-542_en.pdf adresinden erişildi.

European Commission. (2012a). *Unleashing the potential of cloud computing in Europe.* Brussels: European Commission.

European Commission. (2012b). *MEMO/12/41*. 12 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_MEMO-12-41_en.pdf adresinden erişildi.

European Commission. (2012c). *Action 12: Review the EU data protection rules*. 23 Kasım 2012 tarihinde Digital Agenda for Europe: http://ec.europa.eu/information_society/newsroom/cf/fiche-dae.cfm?action_id=170&pillar_id=43&action=Action%2012%3A%20Review%20the%20EU%20data%20protection%20rules adresinden erişildi.

European Commission. (2012d). *Commission proposes a comprehensive reform of the data protection rules*. 13 Aralık 2012 tarihinde http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm adresinden erişildi.

European Commission. (2012e). *How does the data protection reform strengthen citizens' rights?* 13 Aralık 2012 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf adresinden erişildi.

European Commission. (2012f). *Convention for the protection of individuals with regard to automatic processing of personal data*. 27 Kasım 2012 tarihinde http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG adresinden erişildi.

European Council. (1995). *Directive 95/46/EC Of The European Parliament and of the Council.* 30 Kasım 2012 tarihinde http://idpc.gov.mt/dbfile.aspx/Directive%2095-46%20-%20Part%202.pdf adresinden erişildi.

Fox, B. (2012). *Cloud computing a "Game Changer" for EU economy, Kroes Saays*. 06 Kasım 2012 tarihinde euobserver.com/news/117695 adresinden erişildi.

FTC. (1998). *Children's online Privacy Protection Act of 1998 (COPPA)*. 28 Kasım 2012 tarihinde http://www.ftc.gov/ogc/coppa1.htm adresinden erişildi.

FTC. (2011). *The Fair Credit Reporting Act*. 18 Kasım 2012 tarihinde http://www.ftc.gov/os/statutes/031224fcra.pdf adresinden erişildi.

Google. (2012). *Gizlilik politikası*. 12 Kasım 2012 tarihinde http://www.google.com/policies/privacy/ adresinden erişildi.

Google. (2012). *Google Hizmet Şartları*. 12 Kasım 2012 tarihinde http://www.google.com/policies/terms/ adresinden erişildi.

Henkoğlu, T. (2011). *Adli bilişim - dijital delillerin elde edilmesi ve analizi.* İstanbul: Pusula Yayıncılık.

Hohlov, Y. ve Shaposhnik, S. (2006). *Russia.* 27 Kasım 2012 tarihinde http://ec.europa.eu/information_society/activities/internationalrel/docs/pi_study_rus_ukr_arm_azerb_bel_geor_kaz_mold/2_russia.pdf adresinden erişildi.

Kaufman, L. (2009). Data security in the world of cloud computing. *IEEE Computer and Reliability Societies*, 61-64.

King, N. J. ve Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *ElsevierComputer Law & Security Review*, 308-319.

Kroes, N. (2012). *Cloud computing and data protection reform*. 3 Ocak 2013 tarihinde http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection/print/ adresinden erişildi.

KVKKT. (2012). Kişisel Verilerin Korunması Kanunu Tasarısı. 22 Mart 2013 tarihinde http://www.kgm.adalet.gov.tr/Tasariasamalari/Basbakanlik/Kanuntas/kisiselveriler.pdf adresinden erişildi.

Lemos, R. (2011). *Ten big breaches in 2011*. 13 Kasım 2012 tarihinde http://www.darkreading.com/taxonomy/index/printarticle/id/232200377 adresinden erişildi.

McCumber, J. (2005). *Assessing and managing security risk in IT systems.* Washington: CRC.

Mell, P. ve Grance, T. (2011, Eylül). *The NIST definition of cloud computing.* Gaithersburg: U.S. Department of Commerce.

Microsoft. (2012). *Microsoft Hizmetler Sözleşmesi.* 28 Kasım 2012 tarihinde http://windows.microsoft.com/tr-TR/windows-live/microsoft-services-agreement adresinden erişildi.

Microsoft. (2012). *Microsoft Online Privacy Statement*. 27 Kasım 2012 tarihinde http://privacy.microsoft.com/TR-TR/fullnotice.mspx adresinden erişildi.

Paquette, S., Jaeger, P. ve Wilson, S. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 245-253.

Perlin, M. (2012). *Downtime, outages and failures - understanding their true costs*. 25 Kasım 2012 tarihinde Evolven: http://www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html adresinden erişildi.

Privacy Rights Clearinghouse (PRC). (2012). *Personal data retention and destruction plan.* 12 Kasım 2012 tarihinde Privacy Rights Clearinghouse: https://www.privacyrights.org/print/fs12a-personal-data-retention-and-destruction-plan adresinden erişildi.

Salesforce. (2012). *Complete history of cloud computing.* 5 Ocak 2012 tarihinde http://www.salesforce.com/uk/socialsuccess/cloud-computing/the-complete-history-of-cloud-computing.jsp?d=70130000000sC08&RRID=469645998 adresinden erişildi.

Schubert, L. (2010). *The Future of cloud computing.* European Commission.

Svantesson, D. ve Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law And Security Review*, 391-397.

T.C. Anayasası. (1982). *Türkiye Cumhuriyeti Anayasası.* 13 Aralık 2012 tarihinde http://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf adresinden erişildi.

Thibodeau, P. (2011). *Congress urged to leave cloud computing alone*. 18 Kasım 2012 tarihinde Computerworld: http://www.computerworld.com/s/article/print/9215750/Congress_urged_to_leave_cloud_computing_alone_?taxonomyName=Cloud+Computing&taxonomyId=158 adresinden erişildi.

Turan, S. (2010). *Bulut bilişimi (cloud computing) teknolojisi ve güncel hukuki problemler*. 24 Ekim 2012 tarihinde Bilişim Hukuku Bülteni: http://www.bilisimhukuk.com/2010/02/bulut-bilisimi-cloud-computing-teknolojisi-ve-guncel-hukuki-problemler/ adresinden erişildi.

TÜİK. (2012). *Hanehalkı bilişim teknolojileri kullanım araştırması.* Ankara: Türkiye İstatistik Kurumu.

Türk Ceza Kanunu. (2004). *Türk Ceza Kanunu.* 13 Aralık 2012 tarihinde http://www.tbmm.gov.tr/kanunlar/k5237.html adresinden erişildi.

U.S.C. (1996). *Health Insurance Portability And Accountability Act of 1996.* 28 Kasım 2012 tarihinde http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/downloads/hipaalaw.pdf adresinden erişildi.

U.S.C. (1999). *Gramm-Leach-Bliley Act.* 18 Kasım 2012 tarihinde http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf adresinden erişildi.

U.S.C. (2011). *In the house of representatives.* 19 Kasım 2012 tarihinde http://www.gpo.gov/fdsys/pkg/BILLS-112hr611ih/pdf/BILLS-112hr611ih.pdf adresinden erişildi.

Varadi, S., Kertesz, A. ve Parkin, M. (2012). The necessity of legally compliant data management in European cloud architectures. *Computer Law & security Review*, 577-586.

Wyld, D. C. (2009). *Moving to the cloud: an introduction to cloud computing in government.* 21 Ekim 2012 tarihinde http://faculty.cbpp.uaa.alaska.edu/afgjp/PADM601%20Fall%202010/Moving%20to%20the%20Cloud.pdf adresinden erişildi.