Türk Arşivciler Derneği

Arşiv Dünyası Dergisi

The Journal of Archival World

Sayı/Number: 17-18, Sayfa/Pages: 46-56

İstanbul, İlkbahar-Kış/Spring-Winter 2017

ISSN: 2147-2599

KİŞİSEL VERİLERİNİZ NE KADAR GÜVENDE? BİLGİ GÜVENLİĞİ KAPSAMINDA BİR DEĞERLENDİRME

Are Your Personal Data Safe? An Assessment from an Information Security Perspective

Türkay HENKOĞLU

Adnan Menderes Üniversitesi, Söke İşletme Fakültesi, Yönetim Bilişim Sistemleri Bölümü

turkay.henkoglu@adu.edu.tr

Alındığı tarih: 20.12.2016; Kabul tarihi: 11.06.2017

Öz

Elektronik ortamda bulunan bilgi varlıklarındaki çeşitliliğinin artışına bağlı olarak veri depolama ortamlarına yönelik güvenlik endişelerinin artması ve bilgi yönetimi için kullanılan bilişim teknolojilerinin hedef haline gelmesi, günümüzde bilgi güvenliğinin sağlanması konusuna daha geniş bir çerçevede ve sistematik olarak bakmayı zorunlu hale getirmektedir. Özellikle kişisel verilerin korunması konusu hukuksal yönleriyle değerlendirildiğinde, bilginin gizliliğinin korunmasından farklı olarak daha etkin ve kapsamlı koruma önlemlerinin alınmasını gerektirmektedir. Bu konuda yapılan araştırmalar, hukuksal düzenlemelerin bazen dikkate alınmadığını, Türkiye'de bilgi güvenliğinin sağlanmasına yönelik önlemlerin, kişisel hak ve özgürlüğün korunmasına ilişkin risklerin artmasına neden olduğunu göstermektedir.

Bilgi saklama/depolama ve arşiv işlemlerinin "ayıklama" yerine bilginin elektronik ortamda doğuşu ile başlaması, klasik bilgi güvenliği anlayışındaki değişimi ve farklı disiplinlerin de bu konuya neden dâhil olması gerektiğini açıklamaktadır. Bilginin işlendiği/üretildiği andan imha edildiği ana kadar olan süreçte yer

alan tüm aktörlerin, bilgi güvenliğinin sağlanması konusunda sorumlulukları bulunmaktadır. Çalışmada, kişisel verilerin korunması çerçevesinde bilgi güvenliğinin sağlanmasına yönelik olarak uygulamada yapılan yanlışlar ve bu konudaki sorumluluklara değinilerek, teknik ve hukuksal açıdan ne gibi risklerle karşı karşıya olunduğuna dikkat çekilmesi amaçlanmaktadır. Uygulamadaki risklerin değerlendirilmesi ve daha geniş çerçevede sorumlulukların belirlenmesi ile birlikte, bilginin gizliliğinin ve kişisel hakların aynı anda korunması mümkün olabilecektir.

Anahtar Sözcükler: Kişisel veri, bilgi güvenliği, gizlilik, kişisel haklar.

Abstract

Nowadays, provision of information security from a wider perspective and more systematically has become compulsory due to the increased concern for data storage media as a result of the increase in variety of information assets in electronic environment and due to the information technologies used for more effective information management becoming a target. Especially when evaluating legal aspects of protecting personal data, it is required to take more effective and comprehensive protection measures unlike those of protection of information privacy. Research conducted in this regard shows that measures taken to provide information security in Turkey, where no legal arrangements are taken into account, lead to the increase in risks of protection of personal rights and freedom.

The fact that storage and archiving of information has started at the birth of electronic information rather than with the sorting explains the change in the understanding of classic information security and why different types of disciplines should involve in this issue. All of the persons who are involved in the process from the production / processing of information to the destruction of it have responsibilities for information security. In this study, it is aimed to draw attention to the risks both from technical and legal aspects by addressing the mistakes made in practice of providing information security for personal data and by addressing the responsibilities in this issue. It may be possible to protect both personal rights and information privacy by assessing the risks and determining the responsibilities together from a broader perspective.

Keywords: Personal data, Information security, Privacy, Personal Rights

1. Giriş

Elektronik ortamlarda saklanan bilgilerin güvenliğinin sağlanması, risk ve tehditlerdeki değişime bağlı olarak her geçen gün daha karmaşık hale gelmektedir. Bununla beraber, internet üzerinde sosyal ağlar ve e-ticaretin kullanımının daha yaygın hale gelmesiyle birlikte, kişisel verilerin korunması konusunda da endişeler artmaktadır. Bu durum, hukuksal dayanakları da bulunan bilgi güvenliği önlemlerinin dikkate alınmasını zorunlu hale getirmektedir.

Kişisel verilerin korunmasına yönelik bilgi güvenliği önlemleri, bilginin elde edilmesinden imha edilmesine kadar olan tüm süreçler içerisinde aktif olan ve bilginin işlenmesinde rol alan tüm aktörlere belirli ölçülerde sorumluluk yükleyen bir

güvenlik zincirini oluşturmaktadır. Bu nedenle etkin teknik önlemlerin yanı sıra, hukuksal sorumluluklar kapsamında veri sorumlusu olarak idari personelin de yükümlülüklerini yerine getirmeleri önem taşımaktadır. Bu sorumluluklar Kişisel Verilerin Korunması Kanunu (KVKK) içerisinde açıkça ifade edilmekle birlikte, uygulamaya yönelik eksikliklerin de ikincil mevzuat ile giderilmesi gerekmektedir.

Saklanan verinin niteliğinde bilgi teknolojilerindeki tarihsel sürece bağlı değişiklikler olmuş ve bu değişiklikler alınacak güvenlik önlemlerine ilişkin sorumlulukların paylaşılmasını zorunlu hale getirmiştir. Bilginin nasıl elde edildiği, kim tarafından ve hangi amaçla işlendiği, bu verilerin sahibinin ve güvenlik sorumlusunun kim olduğu, verilerin nerede ve nasıl saklandığı, süresi dolan verilerin kim tarafından ve nasıl imha edildiği gibi birçok sorunun cevabının açık olarak verilebiliyor olması, günümüzde bilgi güvenliğinin etkinliği açısından önem taşımaktadır. Bu süreçte yer alan tüm unsurların hukuksal sorumluluklarını ve belirlenen bilgi güvenliği politikası kapsamındaki yükümlülüklerini yerine getirmeleri halinde güvenlik zincirinin tüm halkaları aynı direnci gösterebilmektedir. Ancak kişisel veriler gibi önceden sınıflandırılmış ve daha üst seviyede korunacak bilgi varlıkları için, belirlenecek bilgi güvenliği politikalarında, uygulama yöntemlerine (kriptolama, sanallaştırma, anonimleştirme gibi) ve kişi haklarına ilişkin bilgilere de yer verilmesi önemlidir. Farklı güvenlik önlemlerini almakla yükümlü kişilerin sorumlulukları paylaşmaları ve aynı zamanda bir sistem yaklaşımı içerisinde birbirleri ile koordineli olarak bu sorumlulukları yerine getirmeleri sağlanmalıdır.

2. Saklanan Bilginin Dönüşüm Evreleri ve Etkili Bilgi Güvenliği İçin Gerekli Unsurlar

1951 yılında manyetik teyp kullanarak verileri depolayan UNIVAC adlı bilgisayarın üretimi, bilginin korunmasına yönelik önemli bir tarihsel dönüşüm noktasıdır. Bu tarihten itibaren gelecek kuşaklara aktarılması istenen bilgiler elektromanyetik saldırı gibi dış etkilere karşı daha duyarlı hale gelmiş ve ilâve güvenlik önlemlerinin alınması tartışılmaya başlanmıştır. Depolanan bilgilere ilişkin ikinci önemli dönüm noktası ise Amerikan Savunma Bakanlığı bünyesinde kurulan "ARPANET" ile başlayan internetin gelişim sürecidir. 1969-1995 yılları, elektronik ortamda saklanan bilgilerin transfer edilme risklerinin ve bu bilgilerin bütünlüğüne yönelik yeni tehdit unsurlarının dikkate alınmaya başlandığı tarih aralığıdır. Bilgisayar ağlarının yaygınlaştığı bu döneme kadar; en önemli güvenlik unsuru olarak ön planda olan fiziksel güvenlik koşullarının sağlanması şartı uygulamada alt basamaklara inmiştir. 1995 yılından günümüze kadar uzanan süreçte ise, bilgisayar ağları bilişim suçlarının işlenmesine yönelik altyapıyı sağlayan en önemli araç ve güvenlik risklerinin odak noktası olarak görülmektedir.

Bilgi güvenliğinde etkinliğin arttırılabilmesi için, bilgi yönetim süreçlerinin gözden geçirilmesi ve bu konudaki eksikliklerin giderilmesi önem taşımaktadır. Bu kapsamda bilgi güvenliğine yönelik olarak izlenmesi gereken aşamalar şunlardır (ISF, 2016):

- Öncelikle korunması istenen kritik bilgi varlıklarının tanımlanması gerekmektedir.

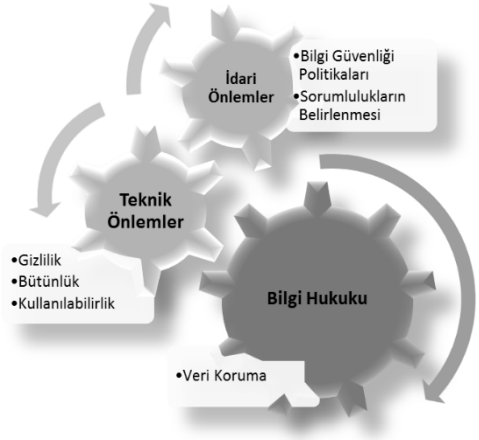
- Bu varlıklara karşı olabilecek tehditler değerlendirilmeli ve bu tehditler liste haline getirilmelidir.
- Bilgi varlıklarının korunması için en uygun metot belirlenmelidir.
- Kapsamlı ve "tutarlı" koruma sağlayacak yaklaşımlar belirlenerek uygulanmalıdır.

Korunması istenen bilgi varlıklarının tanımlanması, bilgi yönetim süreci içerisinde yer alan temel ve en önemli unsurdur. Olası tehditlerin tespit edilmesi ve bu tehditlere karşı idari, teknik ve hukuksal önlemlerin alınabilmesi için, kritik bilgi varlıklarının doğru tanımlanması ve gerekli güncellemelerin sık aralıklarla yapılması önem taşımaktadır. Son olarak, belirlenen güvenlik önlemlerinin uygulanması aşamasında, tutarlılık unsurunun mutlaka göz önünde bulundurulması gerekmektedir.

Bilginin korunan niteliği üç temel unsurdan oluşmaktadır. Bunlar; gizlilik, bütünlük ve kullanılabilirliktir. Başka bir ifade ile bilginin temel olarak gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunması hedeflenmektedir. Bilgi varlıkları genel olarak göz önüne alındığında, bilgi güvenliği kapsamında bu üç temel unsur arasında ortak bir denge noktasının belirlenmesi tercih edilmektedir. Ancak elektronik ortamda yer alan bilgilerin güvenliği söz konusu olduğunda, bu üç unsur arasındaki tutarlılık gizlilik ve bütünlük tarafına daha fazla yaklaşmaktadır. Bu noktada erişilebilirlik ve güvenlik dengesi üzerinde daha fazla durulması ve güvenlik stratejisinin bu çerçevede belirlenmesi önemlidir. Dijital üretimin ya da dijitalleşmenin bilgi erişimine sağladığı katkısının yanı sıra, siber saldırı riskleri ve elektromanyetik saldırı risklerini de göz önünde bulundurmakta fayda vardır. Bununla beraber, elektronik ortamda yer alan bilgilerin güvenliğinin sağlanması için en fazla kaynak ayrılan ve tam korumanın sağlanmasını imkânsız hale getiren bilginin bütünlüğünün korunması ihtiyacı, yazılı-basılı ortamlarda yer alan bilgiler için çok daha kolay yöntemlerle karşılanabilmektedir. Bu nedenle, elektronik ortamda üretilen bilgilerin orijinalliğinin korunarak yüzlerce yıl saklanması ve gelecek kuşaklara aktarılabilmesi konusunda şüpheler bulunmaktadır. Elektronik ortamda üretilen ve sadece elektronik ortamda saklanan bilgilerin bütünlüğünün korunmasına yönelik riskler, bazı kurumlarda tasarruf amacıyla uygulanan çıktı alma yasaklarını da (Henkoğlu, 2015, s. 141) tartışmalı hale getirmektedir. Çünkü korunması istenen bilgiler kapsamında sınıflandırılmış bu tür bilgilerin sadece belirlenen idari önlemler ve bilgi güvenliği politikaları kapsamında değil, hukuksal sorumluluklar kapsamında da korunması gerekmektedir.

Tarihsel süreç içerisinde bilginin karakteristik özelliğinin (gizlilik, bütünlük, kullanılabilirlik) temel olarak değişmemesine karşın, bilginin durumuna (bilginin işlenmesi, depolanması ve transferi) yönelik önemli değişiklikler olmuş ve bu kapsamda alınacak güvenlik önlemlerinin çeşitliliği ile birlikte ağırlığı da değişim göstermiştir. Bu çerçevede gelecek kuşaklara aktarılacak bilgi varlıklarının güvenliğinin sağlanması için dikkate alınması gereken unsurlar; teknoloji, bilgi güvenliği politikaları ve eğitim/farkındalıktır. Ancak bu üç önemli unsurun her birinin, ayrı ayrı değerlendirilmesi ve amaca yönelik güvenlik stratejisinin belirlenmesi gerekmektedir. Güvenlik önlemleri bir sistem yaklaşımı içerisinde değerlendirildiğinde ise, teknik önlemler, idari önlemler ve bilgi hukukunun birbiri ile bütünleşmiş bir sistemin parçalarını oluşturdukları söylenebilir. Bu parçaların her biri Şekil-1'de görüldüğü

gibi kendi içinde farklı güvenlik unsurlarını barındırmakta ve tüm unsurlar dikkate alınarak işlevsel hale getirildiklerinde bir bilgi güvenliği şemsiyesi oluşturulabilmektedir.



Şekil 1: Bilgi güvenliği önlemleri için başlıca unsurlar

3. Bilgi Güvenliği Kapsamında Neyi Korumalıyız?

Bilgi güvenliğinin sağlanması konusunda korunacak bilgi varlıklarının seçilmesi, sınıflandırılması ve uygun güvenlik önlemlerinin belirlenmesi işlemleri en önemli hususlardan biri olmasına karşın, bu konunun çoğu zaman dikkate alınmadığı görülmektedir (Henkoğlu, 2015, s. 134-148). Bilgi yönetiminin de temel iş süreçleri arasında yer alan bu faaliyetlerdeki eksiklikler, güvenlik zincirinin zayıf halkasını oluşturmaktadır. Çünkü bir bilginin gizliliğinin korunması ile kişisel hakların korunması farklı kavramlar olduğu gibi, farklı güvenlik önlemlerinin doğru ve zamanında uygulanması da ayrıca önem taşımaktadır. Çoğunlukla bilgi işlem merkezinin sorumluluğunda bulunan merkezi veri depolama ortamlarının korunmasına yönelik stratejiler, teknik önlemlerin ön planda olduğu, bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin dikkate alındığı önlemleri içermektedir. Oysa merkezi veri depolama ortamlarında bulunmakla birlikte sorumluluk paylaşımının yapılmadığı kişisel verilerin korunmasına ilişkin önlemler, hukuksal ve idari süreçleri de içine alan ve bilgi erişim hakları ile daha karmaşık hale gelmiş veri koruma önlemlerinin birleşimi ile oluşmaktadır. Çoğunlukla farklı bir kavram gibi algılanan kişi hak ve özgürlüğünün korunması, kişisel verilerin bilgi güvenliği önlemleri kapsamında korunması ile birlikte başlamaktadır (Henkoğlu ve Uçak, 2016, s. 31).

4. Kişisel Verilerin Korunması Neden Önemlidir ve Bu Konudaki Temel Sorunlar Nelerdir?

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi olarak tanımlanmaktadır (Avrupa Konseyi, 1995; KVKK, 2016). Hukuksal düzenlemelerde kişisel verilerin neler olabileceği konusunda bir liste sunulması yerine açık uçlu bir tanımın yapılması, kişisel hakların korunması konusunda herhangi bir eksikliğin oluşmaması açısından önemlidir. Ancak veri sorumlusu ve veriyi işleyen kişilerin bu konuda daha bilinçli olmaları da aynı derecede önemlidir. Veri koruma-

ya ilişkin hukuksal düzenlemeler ve uluslararası sözleşmeler incelendiğinde şu ortak unsurların ilke olarak benimsendiği görülmektedir (Avrupa Komisyonu, 1981; Avrupa Konseyi, 1995; KVKK, 2016; OECD, 2013):

- Bilginin hukuka uygun olarak elde edilmesi,
- Bilginin amacına uygun olarak kullanılması,
- Gereğinden fazla bilgi toplanmaması,
- Bilginin veri sahibi tarafından erişilebilir olması,
- Bilginin doğru ve güncel olması,
- Bilginin güvenli olarak tutulması,
- Kullanım süresi sona eren bilgilerin uygun yöntemlerle imha edilmesi.

Veri koruma konusunda tüm dünyada belirli ölçülerde hassasiyet bulunmaktadır. Almanya gibi bazı Avrupa ülkelerinin öncülüğünde atılan adımlarla, Avrupa Birliği'nin (AB) bu konuda belirlemiş olduğu standartlar ve hukuksal düzenlemelerin, diğer ülkeler üzerinde de etkili olduğu görülmektedir. Bunun temel nedeni, bir ekonomi topluluğu olarak kurulan AB'nin ekonomi odaklı bilgi politikalarıdır (Henkoğlu ve Yılmaz, 2013). Bu açıdan bakıldığında, kişisel verilerin korunması ile çevrimiçi ticaretin geliştirilerek ekonominin canlı tutulması hedefi birbirinden uzak konular değildir. Kişisel verilerin hukuksal düzenlemelerle korunarak kişilere çevrimiçi ticareti güvenle kullanabileceklerinin güvencesi verilmesi ise, transfer edilen bilgilere ilişkin etkin güvenlik önlemlerinin alınması ile bir sistem yaklaşımı içinde sağlanabilmektedir.

2015 yılındaki bilgi güvenliği ihlallerine ilişkin istatistikler incelendiğinde (Gemalto, 2016b); kaybedilen verilerin %43'ünün kamu kurumlarında ve %19'unun sağlık hizmetlerinde olduğu görülmektedir. Bu sonuçlar kişisel verilerin hedef olarak seçildiğini ve bilgi güvenliği önlemleri arasında kişisel verileri korumaya yönelik önlemlerin de dikkate alınması gerektiğini göstermektedir. Bu oranlar her ülkede küçük farklılıklar göstermekle birlikte, veri korumaya ilişkin temel sorunların değişmediği görülmektedir. Bu temel sorunlar (Henkoğlu ve Uçak, 2015, s. 69-72);

- Korunması istenen bilgiye ilişkin kavramlar üzerindeki belirsizlikler,
- Sorumlulukların paylaşılamaması ve
- Bilgi güvenliği stratejilerinin geliştirilememesidir.

Veri, bilgi ve bilişim kavramlarının farklı disiplinler tarafından farklı yorumlanması, korunacak bilgi varlığının sınıflandırılması konusunda ve hukuksal koşullar içindeki değerlendirmelerde farklılıklara neden olmaktadır. Başka bir ifade ile bilgi güvenliğinin sağlanmasına ilişkin teknik önlemleri alma sorumluluğunu taşıyan kişiler ile hukuksal koşulları sağlamakla yükümlü idari personelin kişisel veri ve hassas verilere bakış açısında farklılıklar bulunmaktadır (Henkoğlu, 2015, s. 31-33). Bu farklılık, veri koruma konusunun bir sistem yaklaşımı içerisinde bütünüyle değerlendirilmesi ve uygun stratejinin geliştirilmesine ilişkin eksikliklere neden olmaktadır.

Kişisel verilerin korunmasına ilişkin dikkate alınmayan bir diğer risk ise, bilgi işlem merkezlerinin önemli ölçüde kişisel veri içeren hizmetleri/servisleri (e-posta, depolama alanı vd.) sunan sunucuları devre dışı bırakarak, bu hizmetleri/servisleri ücretsiz olarak sunan bulut servis sağlayıcılara devretmeleridir. Bu dönüşüm ya da

servis hizmetlerinin herhangi bir bulut servis sağlayıcıya herhangi bir özel sözleşme olmaksızın devredilmesi ile birlikte, veri korumaya yönelik sorumluluklar tartışmalı hale gelmektedir. Bu konuya KVKK açısından bakıldığında öncelikle akla gelen şu sorulara tüm kullanıcılarda şüpheye yer bırakmayacak cevapların verilebilmesi gerekmektedir. Cevabı kesin bir şekilde verilmesi gerekli sorular şunlardan oluşmaktadır:

- KVKK'da tanımlanan veri sorumlusu ve KVKK'nın 12. Maddesi kapsamındaki veri sorumlusunun yükümlülükleri belirlenmiş midir?
- Verilerin farklı bir ülkede yer alan sunucu üzerinde işlendiği ve saklandığı konusunda veri sahibi aydınlatılıyor mu?
- İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği konusundaki açıklamaların ilgili servis sağlayıcının gizlilik sözleşmesinde yer aldığı ve bu sözleşmenin herhangi bir kullanıcı için de farklılık içermediği hakkında kurumsal kullanıcılar bilgilendiriliyor mu?
- Bu servisler üzerinden gizlilik derecesi bulunan kurumsal bilgilerin gönderilmesine ilişkin risk ve yasaklar hakkında kullanıcılar bilgilendiriliyor mu?
- KVKK'nın 11. Maddesinde yer alan ilgili kişinin hakları mevcut koşullar içinde sağlanabiliyor mu?
- Bu servisler üzerinde işlenen bilgilerin silinse dahi, kalıcı olarak silinip silinmediği konusunda risk ve belirsizliklerin olduğu bilgisi kullanıcıya veriliyor mu?
- Tüm bu belirsizliklerle birlikte, hangi koşulun sağlanması halinde ilgili kişinin rızası şüpheye yer bırakmayacak şekilde alınmış olarak kabul ediliyor?

Bu soruların bazıları ilgili kurumlar tarafından yapılacak olan kullanıcı aydınlatma metni ile birlikte cevaplanabilirken, bazıları tartışmalı olarak kalmaktadır. Örneğin, kurumsal e-posta adresinin ya da bulut veri depolama ortamının başka bir yerden edinilemeyeceği dikkate alındığında, bu koşullarda rızanın (şüpheye yer bırakmayacak şekilde) özgürce verildiğini söyleyebilmek için, ilgili kişiye gerçek bir seçim hakkı sunulmalıdır. İlgili kişi rıza göstermeye zorunlu bırakılmışsa veya üzerinde bu yönde bir baskı bulunuyorsa, bu durumda özgür iradesinin varlığı tartışmalı hale gelmektedir. Bununla beraber kurumların işledikleri kişisel verilere ilişkin olarak rıza kriterlerini karşılayabilmeleri için; hangi verilerin kaydının tutulacağı, verilerin nerede tutulacağı, ne kadar süre ile tutulacağı ve bu verilerin kullanım amacına ilişkin bilgilendirmeyi veri sahiplerine yapmaları gerekmektedir (AGIMO, 2013; University of London, 2015).

Kurum içinde işlenen kişisel verilerin korunması kontrolünün sağlanması için veri sorumlusu[1] ile birlikte bilgi güvenliği yetkilisinin de belirgin olması önem taşımaktadır. Ancak KVKK'da sadece veri sorumlusu tanımlanmış olup, bilgi güvenliği yetkilisinin ikincil mevzuatta düzenlenmesi öngörülmüştür. Bu nedenle bilgi güvenliği yetkilisi bazı örnekler de olduğu gibi (Sağlık Bakanlığı, 2016) ilgili yönetmeliklerle ya da bilgi güvenliği politikaları içinde tanımlanarak sorumluluk paylaşımı daha

[1] Veri sorumlusu, tek başına ticaretle uğraşanlar ve şirketler olabileceği gibi; okullar, yerel yönetimler, kolluk güçleri, hastaneler ve diğer devlet kurumları gibi ticaret dışı topluluklar da olabilir.

belirgin hale getirilmelidir. Böylece hiyerarşik yapı içinde sorumluluk alması gereken idari yöneticilerin de sorumluluğunun açıklanması sağlanabilecektir.

5. Kişisel Verilerin Korunması İçin Neler Yapılmalıdır?

Bilginin içinde bulunduğu duruma bağlı olarak uygulanacak güvenlik önlemleri farklılık göstermektedir. Bilgi bütünlüğünün tam olarak sağlanabilmesi için, bilginin işlenmesi esnasında mevcut hash değerlerinin değişmemesine özen gösterilmesi, veri iletim yolunun kriptolanması ve saklama ortamının kriptolanması en güvenli yöntemlerdir. Veri ihlallerine ilişkin raporlar da (Gemalto, 2016a) kripto kullanımının etkinliğini ortaya koymaktadır.

Bilgi yönetim süreçlerinin de başlangıç noktası olarak değerlendirilen bilginin sınıflandırılması aşamasında, bilgi güvenliği odaklı yaklaşımlara öncelik verilmelidir. Kritik bilgi ve anlık bilgilerin işlenmesi esnasında diğer bilgilerden ayrılması, güvenlik önlemlerinin sağlanmasına yönelik maliyetlerin düşmesine ve etkin bilgi güvenliği sağlanırken de genel sistem performansında hissedilir değişikliğin olmamasına katkı sağlayacaktır. Kişisel ve hassas verilerin bütünlüğünün korunması aynı zamanda hukuksal sorumluluklar arasında olmasına karşın, diğer düşük öncelikli iş kayıtlarının sadece varlığının korunması yeterli olabilmektedir.

Veri koruma konusunda faydalanılabilecek önemli araçlardan biri de sanallaştırmadır. Sanallaştırma, hangi verinin nerede ve nasıl tutulacağı ile bilginin güvenliğinin sağlanması konularının kesiştiği noktada yer almaktadır. Veri depolamaya ilişkin olarak kullanılan sanallaştırma yöntemi ile doğrudan disk üzerinden bilgiye erişim ve uzaktan erişim riskleri en düşük seviyeye indirilebilmektedir.

Bilgi profesyonellerinin sıklıkla uyguladıkları anonimleştirme işlemleri de kişisel verilerin korunmasına yönelik bilgi güvenliği önlemlerini zenginleştirmektedir. Ancak anonimleştirme işlemi ile kodlama ya da takma isim kullanma kavramlarının karıştırılmamasına özen gösterilmeli ve bilgi politikalarında kişisel verileri anonim hale getirme işlemi[2] açık olarak tanımlanmalıdır. Anonim hale getirme, KVKK'nın yürürlüğe girdiği tarih öncesinde kaydedilen ve KVKK hükümlerine aykırı olan kişisel veriler için de uygulanabilecek yöntemlerden biridir (KVKK, 2016).

Kullanım amacı sona eren verilerin imha edilmesi sadece maliyet açısından değerlendirilebilecek bir konu olmanın ötesinde, kişisel hakların korunması açısından da önem taşımaktadır. Kurumların tüm verileri saklama eğiliminin (Henkoğlu, 2015, s. 139) KVKK kapsamında değerlendirildiğinde değişmesi gerekmektedir. Kişisel verilerin korunması söz konusu olduğunda, kullanım amacı sona eren verilerin derhal imha edilmesi gerektiği KVKK'da açık olarak belirtilmektedir (KVKK, 2016).

Kişisel verilerin korunmasına ilişkin risklerin kabullenilmesi ya da transfer edilmesi, hukuksal sorumluluklar çerçevesinde mümkün değildir. Bu nedenle, risklerin azaltılması için gerekli güvenlik önlemlerinin alınması önemlidir. Bu kapsamda güvenlik önlemlerinin alınmasına yönelik olarak iç tehditlere daha fazla önem

[2] **Anonim hale getirme**: Kişisel verilerinin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

verilmesi gerekmektedir. Çünkü yapılan araştırmalar, bilişim sistemlerine yönelik en büyük tehdidin iç tehditler olduğunu ve bilişim sistemlerinin %68'inin iç tehditlere karşı daha zayıf olduğunu göstermektedir (CXO, 2015; Durbin, 2016).

Bilgi depolama alanlarının güvenliğinin sağlanması da kişisel verilerin korunması ve bilgi varlıklarının gelecek kuşaklara aktarılmasında önemli rol oynamaktadır. Bu kapsamda fiziksel güvenlik önlemleri ile beraber, elektromanyetik tehditlere karşı alınacak önlemler de dikkate alınmalıdır. Bu amaçla veri depolama merkezlerinin / felaketten kurtarma (disaster recovery) sistemlerinin birbirine yakın mesafede olmayan en az üç farklı coğrafi bölgede bulunması önerilmektedir (SFA, 2009). Ayrıca, merkezi veri depolama ortamlarında sistem üzerinde çalışmıyor olsa dahi, veri depolama aygıtlarının elektromanyetik tehditlere karşı koruma özelliği bulunan kılıf ya da koruyucu kafes içine alınması önem taşımaktadır (Emanuelson, 2016; Kessler, 2009).

Sonuç

Kişisel veri kavramı üzerindeki farklı algılara bağlı olarak bilginin işlenmesi, bir sistem yaklaşımı içerisinde değerlendirilmesi gereken bilgi güvenliği, bilgi erişimi ve hukuksal koşulların sağlanmasına yönelik riskleri oluşturmaktadır. Bu kapsamda uygulamada hukuksal koşulların da değerlendirilerek dikkate alınması gereken önemli noktalar şunlardır:

- Minimum veri kaydı ve depolama yapılması,
- Erişim yetkilendirmesinin yapılarak sadece bilmesi gerekenlerin bilgiye erişiminin sağlanması,
- Erişim kayıtlarının tutulması,
- Veri yedekleme planının oluşturulması,
- Veri değişikliklerinin izlenmesi,
- Veri kullanım/saklama sürelerindeki belirsizliklerin giderilmesi,
- Kriptolama ve sanallaştırma yöntemlerinin etkin olarak kullanımının sağlanması,
- Verilerin saklandığı ortamlar geleneksel fiziksel şartların yanı sıra elektromanyetik tehditler açısından da değerlendirilmesi,
- Felaket kurtarma planının oluşturulması,
- Veri sorumlusunun belirgin olması,
- Veri sahibinin yasal yükümlülükler çerçevesinde aydınlatılması,
- Verinin bulunduğu ortamın hukuksal etki alanının da göz önünde bulundurulması,
- Verilerin kimlerle paylaşılabileceğinin bilgi güvenliği politikalarında yer alması ve
- Sorumlulukların belirlenmesi.

Kaynakça

AGIMO. (2013). *Privacy and cloud computing for Australian Government Agencies*. 09 Kasım 2016 tarihinde http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf adresinden erişildi.

Avrupa Komisyonu. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 8 Kasım 2016 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm adresinden erişildi.

Avrupa Konseyi. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 03 Kasım 2016 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF adresinden erişildi.

CXO. (2015). *Insider threats and vulnerability*. 28 Ekim 2016 tarihinde http://www.slideshare.net/cxocommunity/vectranetworks-insider-threat-report adresinden erişildi.

Durbin, S. (2016). *Insiders are today's biggest security threat: The most fundamental element of threat is deeply human.* 24 Ekim 2016 tarihinde http://www.recode.net/2016/5/24/11756584/cyber-attack-data-breach-insider-threat-steve-durbin adresinden erişildi.

Emanuelson, J. (2016). *Getting Prepared for an Electromagnetic Pulse Attack or Severe Solar Storm*. 02 Kasım 2016 tarihinde http://www.futurescience.com/emp/emp-protection.html adresinden erişildi.

Gemalto. (2016a). *2015 Data Breach Statistics - Breach Level Index Findings*. 08 Kasım 2016 tarihinde https://safenet.gemalto.com/resources/data-protection/2015-data-breaches-infographic/ adresinden erişildi.

Gemalto. (2016b). *2015 Data Breach Statistics - Breach Level Index Findings.* 11 Kasım 2016 tarihinde https://safenet.gemalto.com/resources/data-protection/2015-data-breaches-infographic/ adresinden erişildi.

Henkoğlu, T. (2015). *Bilgi güvenliği ve kişisel verilerin korunması*. Ankara: Yetkin Hukuk Yayınları.

Henkoğlu, T. ve Uçak, N. Ö. (2015). Üniversite Kütüphanelerinde Kişisel Verilerin Korunması. *Bilgi Dünyası, 16*(1), 45-74.

Henkoğlu, T. ve Uçak, N. Ö. (2016). Information Security and the Protection of Personal Data in Universities. *International Journal of Business and Management Invention, 5*(11), 30-43.

Henkoğlu, T. ve Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği, 27*(3), 451-471.

ISF. (2016). *Protecting the Crown Jewels: How to Secure Mission-Critical Assets*. 03 Kasım 2016 tarihinde https://www.securityforum.org/tool/protecting-the-crown-jewels/ adresinden erişildi.

Kessler, R. (2009). *EMP Attack Could Wipe Out U.S.* 06 Kasım 2016 tarihinde http://www.newsmax.com/RonaldKessler/emp-attack/2009/09/09/id/334894/ adresinden erişildi.

KVKK. (2016). Kişisel Verilerin Korunması Kanunu. 07 Kasım 2016 tarihinde http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf adresinden erişildi.

OECD. (2013). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. 03 Kasım 2016

tarihinde http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf adresinden erişildi.

Sağlık Bakanlığı. (2016). *Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik*. tarihinde http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm adresinden erişildi.

SFA. (2009). *Digital Archiving Policy*. tarihinde https://www.bar.admin.ch/dam/bar/fr/dokumente/konzepte_und_weisungen/policy_digitale_archivierung.pdf.download.pdf/digital_archivingpolicyangl.pdf adresinden erişildi.

University of London. (2015). *Information security and records management*. 12 Kasım 2016 tarihinde http://www.london.ac.uk/fileadmin/documents/about/Records_Management/InfoSecurityandrecordsManagement.pdf adresinden erişildi.