Elektronik Bilgi Güvenliğinin Sağlanması ile İlgili Hukuki ve Etik Sorumluluklar

Legal and Ethical Responsibilities for Ensuring Electronic Information Security

Türkay HENKOĞLU ve Nazan Özenç UÇAK***

Öz

Zaman ve mekân sınırları olmaksızın herkesin bilgi ile buluşabildiği kültür merkezleri haline gelen bilgi merkezlerinde, yeni hukuki ve etik sorumluluklar kapsamında bilgi güvenliğinin sağlanarak gerekli ve yeterli önlemlerin alınması; yakın gelecekte bilgi merkezlerinde meydana gelebilecek birçok maddi ve manevi zararın önüne geçilmesini sağlayacaktır.

Bu çalışmada, bilgi merkezlerinin ve bilgi profesyonellerinin elektronik bilgi güvenliğinin sağlanması ile ilgili hukuki ve etik sorumlulukları, Türk Hukuk Mevzuatı ve mesleki etik kuralları kapsamında ele alınmıştır. Bu bağlamda ilgili konulardaki teknik ve idari eksiklikler irdelenmiş ve literatüre dayalı hukuki ve etik sorumlulukların çelişen noktalarına dikkat çekilerek uygulanabilir çözümler üretilmeye çalışılmıştır. Çalışmada ayrıca; konu ile ilgili hukuk alanında ihtiyaç duyulan düzenlemeler üzerinde durulmuş ve hukuk kuralları ile çelişmeyen etik değerlerin belirlenmesinde dikkate alınması gereken konulara değinilerek önerilerde bulunulmuştur. Çalışma sonucunda, bilgi profesyonellerinin bilgi güvenliği ile ilgili olarak farkındalıklarının arttırılması ve bu konuda görevlerini yaparken yükümlü oldukları hukuk kuralları ve mesleki etik değerler hakkında bilinçlenmelerinin sağlanmasının önemi vurgulanmıştır.

Anahtar sözcükler: *Bilgi güvenliği, Bilgi merkezleri, Bilgi profesyonelleri, Hukuk kuralları, Mesleki etik*

Abstract

Nowadays, information centers have become cultural centers where everyone could gain access to information without time and place limitations. This situation has made the information centers and professionals take some new legal and ethical responsibilities. If necessary precautions are taken, this will prevent information centers from facing serious problems in terms of both financial and ethical issues in near future.

In this study, both ethical and legal issues and responsibilities of information centers and professionals related to the security of electronic data resources are investigated within the scope

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

of Turkish Law Legislation and professional ethical rules. In this process, related literature was reviewed to discover the contradictions and administrative and technical deficiencies in terms of ethical and legal responsibilities of information centers and professionals, which in turn has resulted in new applicable solutions for this area. In addition, in scope of the current study, legal regulations related to this issue were discussed in order to propose new ethical practices which do not conflict with the legal ones. At the end of the study, importance of raising awareness of information managers about information security and make them more knowledgeable their legal and ethical responsibilities in this subject are emphasized.

***Keywords**: Information security, Information centers, Information professionals, Rules of law, Professional ethics*

Giriş

Bilişim teknolojilerinin ve kitle iletişim araçlarının zaman ve kaynakların daha etkin kullanımı yönünde sağladığı avantajlar, bilgi merkezlerinin sağladığı hizmetlerin bilişim sistemlerine daha fazla bağımlı hâle gelmesine neden olmuştur. Bilgi merkezlerinde bulunan bilgi varlığının sayısallaşmasıyla birlikte elektronik bilgilerin sayısının her geçen yıl katlanarak artması, yeni riskleri (verilerin elektronik ortamda izinsiz elde edilmesi, içeriğin değiştirilmesi vb.) beraberinde getirmiş ve bilgi merkezinin sorumluluğundaki bilgiler daha fazla dış tehdide açık hâle gelmiştir.

Bilgi güvenliğinin 2009 tarihli E-devlet ve Bilgi Toplumu Kanun Tasarısı Taslağındaki tanımı, bilgi merkezleri için bilgi güvenliğinin nasıl bir anlam taşıdığını en iyi ifade eden tanımlardan biridir. Buna göre bilgi güvenliği, "bilgi sistemlerinin ve bileşenlerinin hukuka aykırı veya yetkisiz her türlü müdahale veya etkiden korunması; bilgiyle ilgili yapılan her türlü işlemde bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin temini ve bu işlemlerin sadece yetkili kişiler tarafından yapılmasının sağlanması" (T.C. Başbakanlık, 2009) şeklinde tanımlanmıştır.

Bilgi iletişim teknolojilerindeki hızlı gelişim; önceleri bilgisayarların yaygın kullanımının, günümüzde ise taşınabilir iletişim teknolojilerinin ve cep bilgisayarlarının kullanımının yaygınlaşması ile devam etmektedir. Bilgi ortamlarındaki bilgisayar ve internet kullanımına bağlı değişimler toplumun tüm kesimlerinde olduğu gibi bilgi merkezlerinde de görülmektedir. Her yeni teknoloji zaman ve mekân sınırlarını genişleterek bir öncekine göre çok daha fazla bilgiye erişim kolaylığı sağlamakla birlikte, birçok yeni problemi de beraberinde getirmekte ve bilgi hizmeti sunan bilgi profesyonellerine yeni sorumluluklar yüklemektedir. Bilgi hizmetlerinin geleneksel yerel yapısı hızla değişmekte ve elektronik ortamdaki bilginin kontrolü her geçen gün daha fazla zorlaşmaktadır.

Bugün Türkiye'de bilgiye erişimde daha çok yabancı veri tabanlarından yararlanmakla birlikte, ulusal veri tabanlarının oluşturulması ve kullanımı da giderek artmaktadır. Bu durum, yakın gelecekte ulusal veri tabanlarının da çok daha yaygın hâle geleceği ve

bilgi merkezlerinin daha fazla elektronik bilgi kaynağını kendi bilgi bankasında (kendi sunucu bilgisayarında) bulundurmaya ihtiyaç duyacağını göstermektedir. Gerekli önlemler alınmadığı takdirde, bilgi merkezlerini yakın gelecekte maddi ve manevi zararların daha fazla görüldüğü sıkıntılı bir dönem beklemektedir.

Bilgi merkezlerinde bulunan elektronik bilgi kaynaklarının maddi ve manevi zarara neden olabilecek girişimlerden korunabilmesi; hukuki eksikliklerinin giderilmesi, etik değerlerin oluşturulması ve benimsenerek uygulanması ile mümkün olabilir. Türkiye'de bilişim suçları ve internet ortamında işlenen suçlarla ilgili kanun ve yönetmelikler düzenlenmiş olmakla birlikte; yeterliliği ne kadar sağlayabildiği ve bu konudaki eksikliklerin hangi etik değerlere sahip çıkılarak giderilmeye çalışıldığı tartışılması gereken konulardır. Bilgi merkezlerinde elektronik bilgi güvenliğinin ve kişisel verilerin gizliliğinin tam anlamıyla sağlanması sadece hukuk kuralları ya da bilişim teknikleri ile mümkün değildir. Bilgi güvenliğinin sağlanmasında bilgi profesyonellerinin konu ile ilgili farkındalıkları ve etik değerlere uyum konusundaki hassasiyetinin artmasının önemi büyüktür.

Bu çalışmada; bilgi merkezlerinde yeni olanaklarla bilgiye erişimde yer ve zaman sınırlarının ortadan kalkmasıyla birlikte sunulan hizmetlerdeki çeşitliliğin ve dönüşümün beraberinde getirdiği yeni risklere dikkat çekilmiş, elektronik bilgi güvenliğinin önemi ve yakın gelecekte oluşabilecek maddi ve manevi zararların boyutu vurgulanmıştır. Ayrıca çalışmada, bilgi merkezleri ve bilgi profesyonellerinin elektronik bilgi güvenliğinin sağlanması ile ilgili hukuki ve etik sorumlulukları irdelenmiş; alınması gereken hukuki ve etik boyuttaki önlemlerin neler olabileceği tartışılarak çözüm önerileri üretilmeye çalışılmıştır.

Elektronik Bilgi Güvenliğinin Bilgi Merkezleri Açısından Önemi Nedir?

Elektronik ortamda yer alan bilgi, günümüzde bir varlık olarak algılanmaktadır. Özellikle elektronik bilgilerin yoğun olarak toplandığı kütüphaneler, arşivler, dokümantasyon ve enformasyon merkezlerinde; bilginin gizliliğinin ve bütünlüğünün bir varlık olarak korunması bilgi profesyonelleri tarafından uyulması zorunlu yükümlülükler haline gelmiştir. Elektronik depolama ortamlarındaki binlerce önemli ve korunması zorunlu veri nedeniyle hemen her özel kuruluş ya da kamu kurumu gibi; bilgi merkezlerinin de günümüzde ve yakın gelecekte işlevsel doğası gereği siber saldırı denemelerinin öncelikli hedefleri arasında yer alacağı öngörülebilir. Bilgi merkezlerindeki dijitalleştirme çalışmalarının hız kazandığı ve elektronik ortamda oluşturulmuş bilgi oranının katlanarak arttığı düşünüldüğünde, bilgi merkezlerinin bilgi güvenliğinin sağlanması konusundaki sorumluluklarının da her geçen gün artmakta olduğu söylenebilir. Bilgi hizmetlerinde bilgi sistemlerine bağımlılığın artması, tehditlere daha fazla açık olma anlamına gelmektedir. Bilişim dünyasının gelişimi ile orantılı

olarak sürekli gelişen siber saldırı teknikleri ve bu tehditlere karşı eşzamanlı takip gerektiren bilgi güvenliği konusu, bilgi profesyonellerinin de zorunlu ilgi alanları arasına girmeye başlamıştır. Bilgi merkezlerinde elektronik ortamda bulunan bilgilerin ve elektronik ortamda bilgi depolayan veri tabanlarına erişim hizmetlerinin güvenli olarak gerçekleşmesi bilgi profesyonellerinin görev ve sorumluluk alanı içerisinde yer almaktadır. Bilgi merkezlerinde varlık bulan yazılı ve basılı bilginin seçilmesi, sağlanması, değerlendirilmesi, düzenlenmesi, depolanması, erişilmesi ve kullanılması için gerekli olan klasik güvenlik önlemleri; elektronik ortamlarda varlık bulan ve oranı artmakta olan bilginin korunması anlamında büyük oranda (fiziksel güvenlik haricinde) önemini kaybetmiştir.

Üzerinde bilgi bulunan bir bilgisayarın tamamen güvenli olduğundan söz edilebilmesi için; bilgisayarın kapalı ve fiziksel güvenliğinin sağlanmış olması gerekir. Fakat bilgi merkezleri, asıl amacı olan kullanıcı ile bilgiyi buluşturma noktasında 7/24 hizmet vermek ve internet gibi bilgi güvenliğini sağlamanın en zor olduğu bir bilişim ağında erişim yapılan sunucular üzerinde mümkün olan en üst düzey bilgi güvenliğini sağlamak zorundadırlar. Elektronik bilgilerin güvenliğinin sağlanması, güncellenen bilgi güvenliği politikalarına bağlı planlamaları, bilgi birikimini, aktif yönetimi ve sürekli mali kaynakları gerektirmektedir.

Elektronik bilgi yönetiminin bilgi merkezlerinde sunulan hizmetlerin içindeki payı, bilgi çağı sürecinin de doğal bir sonucu olarak artmaktadır. Son yıllarda üniversite kütüphanelerinde yapılan toplam kalite çalışmalarından ve performans ölçütü olarak kullanılan kriterlerden de anlaşıldığı gibi; elektronik bilgi, bilgi merkezlerinde yer alan koleksiyon ve kullanıcı hizmetlerinde artan bir öneme sahip olmaktadır. Koleksiyona eklenen elektronik dergi sayısı, abonelik yoluyla sağlanan elektronik referans kaynağı ve elektronik kitap sayısı, dijital ortamdaki tez sayısı; bunların kullanım sayıları ve bilgi merkezi web sayfasının kullanımı gibi kriterler, bilgi merkezlerinin performanslarını değerlendirirken kullandıkları ana ölçütlerden bazılarıdır (Karasözen ve Gürgüz, 2004). Daha kaliteli ve güvenli bilgi hizmeti sunabilmek için; yüksek kapasiteli bilişim teknolojilerinin yanı sıra, bilgi güvenliğinin sürekliliğinin sağlanabilmesi ve belirli bir bütçe gerektiği unutulmamalıdır. Nitekim arşiv ve kütüphane gibi bilgi kuruluşları bilgi-iletişim teknolojilerine uyum sağlarken sadece bilgiye erişimi sağlamaktan değil; bilgiye güvenli/yetkili erişimden ve bilgi bütünlüğünün korunması ile ilgili yasal yükümlülüklerin yerine getirilmesinden de sorumludurlar.

Her ne kadar bir bilişim sistemine hukuka aykırı olarak girme, sistemi engelleme, bozma, verileri yok etme veya değiştirmek suretiyle işlenen bilişim alanındaki suçlara karşı hukuksal düzenlemeler yapılmış olsa da; bu tür saldırılara maruz kalan bir bilgi merkezinin zararının hukuk kuralları ve yaptırımları çerçevesinde telafi edilmesi mümkün değildir. Ayrıca, uluslararası hukuktaki boşlukların varlığı ve uluslararası bilişim suçlarında bir noktadan takip edilmek suretiyle teknik olarak faile ulaşmanın

çoğu zaman imkânsız olması dikkate alındığında, bilgi güvenliği konusunda alınacak tedbirlerin önemi artmaktadır. Amerika Birleşik Devletlerinde Computer Security Institute (CSI) tarafından her yıl hazırlanan Bilgisayar Suçları ve Güvenlik Araştırması'nın (Computer Crime and Security Survey) 2011 yılı raporu (CSI, 2011); bilişim suçlarına maruz kalan kişilerin %95'inin, sorunun hukuksal süreç içerisinde çözülemeyeceğini düşünmesi nedeniyle herhangi bir girişimde bulunmadıklarını ortaya koymaktadır.

Türkiye'de bilgi merkezlerinde bilgi güvenliğinin sağlanması konusu ile ilgili yasal düzenlemeler Türk Ceza Kanunu'nun 243 ve 244. maddelerinde yer almaktadır (TBMM, 2004). Türk Ceza Kanunu'nun 243. maddesi bilişim sistemine hukuka aykırı olarak girme suçunu; 244. maddesi ise bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçunu düzenlemektedir. Fakat bu konuda kamu kurumlarına ve özel kuruluşlara yol gösteren ya da birtakım önlemlerin alınması konusunda zorunluluk getiren yasal düzenlemeler bulunmamaktadır. Bu konuda yol gösterici olarak nitelendirilebilecek en önemli çalışma ve aynı zamanda ilk uluslararası sözleşme, 2001 yılında kabul edilen Avrupa Konseyi Siber Suçlar Sözleşmesi'dir (Avrupa Konseyi, 2001). Avrupa Konseyi Siber Suçlar Sözleşmesi; siber suçları tanımlamakta, cezai soruşturma ve kovuşturma yöntemlerini belirlemekte ve üye ülkeler arasında işbirliği ve koordinasyonun geliştirilmesini sağlamayı amaçlamaktadır. Fakat Türkiye'nin 10 Kasım 2010 tarihinde imzalamış olduğu Avrupa Konseyi Siber Suçlar Sözleşmesi, TBMM tarafından onaylanmadığı için henüz yürürlüğe girmemiştir. Siber suçlar sözleşmesinin TBMM tarafından onaylanmasından sonra, iç hukuka uyum için gerekli düzenlemelerin de yapılması gerekmektedir (Bozkurt, 2010). Bilgi güvenliği konusunda 2000 ve 2007 yıllarında hazırlanan ulusal bilgi güvenliği yasa tasarıları da, kurulması öngörülen Ulusal Bilgi Güvenliği Teşkilatı'nın görev ve sorumlulukları konusunda kamuoyunun tepkisine maruz kalması nedeniyle geri çekilmiştir. Oysa Almanya'da 1990 yılında kurulan Bilgi Güvenliği Federal Ofisi (Bundesamt für Sicherheit in der Informationstechnik) (BSI, 2012); bilgi sistemleri üzerindeki risklerin tespit edilmesi, bilgi sistem cihazlarının güvenlik testlerinin yapılması, güvenlik sertifikalarının verilmesi, kurum ve kuruluşların bilgi güvenliği konusunda desteklenmesi ve bilişim suçları ile mücadelede kolluk kuvvetlerinin desteklenmesi konularında örnek olabilecek nitelikte hizmet veren bir kuruluş olarak varlığını devam ettirmektedir.

Bilgi Merkezleri ve Bilgi Profesyonellerinin Bilgi Sistemlerinin Kullanımıyla İlgili Hukuki ve Etik Sorumlulukları

Bilgi profesyonelleri, bilgisayar teknolojileri kullanarak sorumluluklarını yerine getirirken bilişim alanı ile ilgili hukuk kuralları çerçevesinde hizmetlerini yürütmek zorundadırlar. Bilgi profesyonellerinin sorumlulukları sadece bilgilerin düzenlenmesi, depolanması ve sunulması ile sınırlı değildir. Bilgi merkezleri ayrıca üyelerinin kişisel bilgilerinin güvenli olarak muhafaza edilmesine, üyelerin faydalandığı kaynaklardan elde edilebilecek özel hayatla ilgili bilgilerin gizliliğine özen gösterilmesi, meydana gelen bir suçun yetkili

makamlara iletilmesi konularında genel cezai sorumluluklara sahiptir. Bilgi güvenliğinin sağlanması konusu, hukuk ve bilişim alanlarının her ikisinin de ortak konusudur ve bu disiplinlerden bir tarafın eksik kalması halinde kalıcı ve sürekli başarıya ulaşmak mümkün olmamaktadır. Bu nedenle teknik önlemlerinin hukuk kurallarına uygun olarak alınması önemlidir.

Bilgi merkezlerinde elektronik bilgi kaynaklarının daha fazla kullanılması ve ödünç verme sistemlerine uzaktan erişimin mümkün olması, yeni etik problemlerin ortaya çıkmasına neden olmuştur. Bilgi kaynaklarına uzaktan erişim, fikri mülkiyet, kullanıcı gizliliği ve bilgi bütünlüğünün sağlanması konularında henüz bilişim dünyasındaki etik kurallar üzerinde dahi tam bir uzlaşı sağlanamamışken; bilgi merkezleri mevcut sorumluluklarının yanında, bilişim teknolojilerinin kullanılması ve elektronik bilgi kaynaklarının artmasından kaynaklanan bu yeni etik problemlerle karşı karşıya kalmışlardır. Bilgi profesyonelleri sansürsüz ve sınırsız olarak bilgi ile kullanıcıyı buluşturma sorumluluğunu, kullanıcı ile ilgili mümkün olan en az kayıt bilgisini tutarak yerine getirmeyi temel etik değer olarak kabul etmektedirler. Fakat dijital dünyada hukuksal düzenlemeler ve bilgi güvenliği (kullanıcı gizliliği, yetkisiz erişimin kısıtlanması ve erişim kayıtlarının detaylı olarak tutulması gibi) kapsamında kabul görmüş etik değerler, bilgi profesyonelleri tarafından benimsenen temel etik değerleri tartışılabilir hâle getirmiştir. Günümüzde bilgi merkezlerinde çelişki oluşturmayan etik değerlerden söz edilebilmesi için, geleneksel kütüphanecilik anlayışının dışında, hukuk ve bilişim alanlarında yer alan etik değerleri de dikkate alan ve birbirine ters düşmeyen yeni etik değerler ile farkındalığın oluşturulması gerekmektedir.

Bilgi merkezlerinde bilgi hizmetlerinin sunulmasında meydana gelen değişimler, öncelikli olarak kişisel bilgilerin ve elektronik kaynakların korunmasına yönelik olan etik değerlerin yeniden değerlendirilmesini zorunlu kılmaktadır. Dijital bilgi merkezlerinin ya da bilgi merkezlerinde sunulan elektronik bilgi kaynaklarına erişimin sağladığı faydalar, önlem alınmadığı için maddi ve manevi kayıplara neden olan bir araca dönüşebilir. Bilgi merkezlerinde bulunan ve kişisel ilgi alanlarını ortaya koyan kayıt bilgilerinin kişinin rızası dışında ifşa edilmesi, kişinin özel alanına müdahale olarak yorumlanabilir. Her ne sebeple olursa olsun, kullanıcılara daha iyi hizmet sunabilmek amacıyla kayıt altına alınan kişisel bilgi veya belgelerin ya da kullanıcıya ait sistem kullanım kayıtlarının açıklanmaması ve bilgi profesyonelleri tarafından titizlikle korunması gerekir.

5237 Sayılı "Türk Ceza Kanunu" Açısından Bilgi Merkezlerinin Sorumluluğu

Türk Ceza Kanunu'nda (TCK) bilgi merkezlerinde çalışan bilgi profesyonellerini doğrudan ilgilendiren birçok düzenleme bulunmaktadır. Bu düzenlemelerden bir kısmı meydana gelen olaylar karşısında bilgi profesyonelini sorumlu olarak tayin ederken, bazıları da gerçek failin ceza yükümlülüğü ile ilgili hususları içermektedir. Basılı kaynakların muhafaza edilmesi ve kullanıcıya sunulması konusundaki sorumluluğun yerine getirilmesinde problem bulunmazken; elektronik ortamdaki bilginin artmasıyla birlikte

daha fazla sorunlar olabileceği açıktır. Elektronik ortamlarda bilgi profesyonellerini sadece gerekli tedbirleri almamaları halinde bile zor durumda bırakabilecek birçok tehlike bulunmaktadır. TCK'nda yer alan ve bilgi profesyonellerine belirli oranlarda sorumluluk yükleyen ya da onları daha bilinçli olmaya zorlayan maddelerden ön plana çıkanlar şunlardır;

Verileri hukuka aykırı olarak verme veya ele geçirme

Verileri hukuka aykırı olarak verme veya ele geçirme ile ilgili hususlar TCK'nın 136. Maddesinde düzenlenmiştir. Bilgi merkezlerinde bulunan ve üyelerin kişisel bilgileri ya da meslek bilgileri gibi başkaları tarafından bilinmesini istemedikleri tüm bilgiler bu kapsamda yer almaktadır. Kişisel verilerin ne şekilde verildiğinin önemi yoktur. Suçun internet üzerinden işlenmesi durumunda "verme" ve "ele geçirme" fiillerinin hangi şartlarda kanuna aykırı sayılacağı da açık değildir (Doğan, 2005). Fakat kişisel verilerin bir zararlı kod aracılığıyla alınması halinde de bu madde dikkate alınabilecektir. Bu suçun kamu görevlisi tarafından işlenmesi suçun nitelikli halini oluşturmaktadır.

Bilişim sistemine girme

Bilişim sistemine girme ile ilgili düzenleme TCK'nın 243. maddesinde yer almaktadır. Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girilmesi ve orada kalmaya devam edilmesi ile suç gerçekleşir. Özel hayatın gizliliğinin korunması ile ilgili düzenlemeler sonrasında sisteme hukuka aykırı olarak girme suç olarak düzenlenmiştir. Fakat "Sisteme girilmesi ve orada kalmaya devam edilmesi" fiilleri birbirine bağlı olduğu için her ikisinin de gerçekleşme zorunluluğunun bulunması ve kalma ifadesinin açık olmaması, kanun maddesini uygulanamaz hâle getirmektedir. Bilişim sistemine girilmesi ve birkaç saniye sonra sistemden çıkılması suçu oluşturmamaktadır. Başka bir ifadeyle; hukuka aykırı olarak girilmemiş ya da kalmaya devam edilmemişse suç işlenmemiş olarak değerlendirilmektedir. Ayrıca; suçun içerisinde hukuka aykırılık olduğu halde birinci fıkrada "hukuka aykırılık" ifadesinin yer alması, "hukuka özel aykırılık halini" oluşturmaktadır. Hukuka özel aykırılık şartının oluşabilmesi için; failin fiili hukuka aykırı olduğunu bilerek ve isteyerek yapmış olması gerekmektedir. Bu ifadenin yer aldığı suçların işlenebilmesi daha zordur (Karagülmez, 2009). Bilgi profesyonellerinin bu madde ile ilgili olarak, sistem erişimlerini kontrol etmek ve meydana gelen hukuka aykırı fiili durumu fark ettikleri anda ilgili makamlara bildirme sorumlulukları bulunmaktadır. Yazılı sözleşmelere bağlı olarak yapılan sistem güvenlik testleri esnasındaki yetkisiz erişimler bu maddenin kapsamı dışında bulunmaktadır (Henkoğlu, 2011).

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Sistemi engelleme, bozma, verileri yok etme veya değiştirme ile ilgili uygulamalar TCK'nın 244. Maddesinde düzenlenmiştir. Konuyla ilgili suçun meydana gelmesi, veri sabotajı ya da sisteme doğrudan zarar verme şeklinde gerçekleşmektedir. Sisteme zarar

verme durumunda dahi dikkate alınacak olan değer sistem üzerindeki bulunan ve zarar gören bilgidir (Henkoğlu, 2011). Bilgi profesyonellerinin bu madde ile ilgili olarak, sistem erişimlerini ve veri bütünlüğünü kontrol etmek ve meydana gelen hukuka aykırı fiili durumu fark ettikleri anda ilgili makamlara bildirme sorumluluğu bulunmaktadır.

Kamu görevlisinin suçu bildirmemesi

Kamu görevlisinin suçu bildirmemesi ile ilgili hususlar TCK'nın 279. maddesinde düzenlenmiştir. Bilgi profesyonellerinin özellikle TCK'nın 243 ve 244. maddelerinde düzenlenen suçlar ile göreviyle bağlantılı olarak karşı karşıya kalmaları halinde, durumu en kısa zamanda ilgili makamlara bildirme yükümlülükleri bulunmaktadır. İhmal veya gecikme durumunda TCK 279. maddesinde yer alan "suçu bildirmeme" ile ilgili cezai yaptırım uygulanır.

Bilgi profesyonelleri için ayrı bir hukuki sorumluluk düzenlenmediği için, hukuki sorumluluklar tazminat sorumluluğu şeklindedir ve sebep olunan zararın karşılanması ile sonuçlanmaktadır. Bilgi profesyonellerin sebep olabileceği zararlar, bilgi merkezinde bulunan kaynak ve araçlara yönelik veya bilgi merkezinden yararlanan üçüncü kişilere yönelik zararlar olmak üzere iki grup altında toplanabilir. Bilgi merkezlerinde bulunan kaynaklara ya da bilgi merkezinden yararlanan üçüncü kişilere yönelik zarara sebep olan bilgi profesyoneli, "haksız fiil" durumunun koşullarının (hukuka aykırı fiil, zarar, kusur ve nedensellik bağı) sağlanmış olup olmamasına bağlı olarak, Borçlar Kanunu'nun 49. maddesi[1] gereğince zararı ödemekle yükümlü olmaktadır. Ancak bilgi profesyonelinin bilgi merkezinden yararlanan üçüncü kişilere karşı olan kusurlarının "hizmet kusuru" ya da "kişisel kusur" olması yönünden ayrımının yapılması gerekir. Zira bilgi profesyonelinin görevini yaparken verdiği zararlardan dolayı çalıştığı idare aleyhine dava açılması gerekmektedir. Yönetim bilgi profesyonelini tazminata mahkûm olunan konuda kusurlu buluyor ise ödediği tazminatın kusurlu bilgi profesyoneli tarafından kendisine ödenmesini (rücu davası ile) isteyebilir. Kişisel kusur nedeniyle meydana gelen zararlarda ise, kişilik hakları zedelenen kişi doğrudan bilgi profesyoneli aleyhine adli yargıya dava açabilmektedir (Ketizmen, 2008).

5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" Kapsamında Sorumluluk

2007 yılında yürürlüğe giren ve bilgi profesyonellerini birçok yönü ile yakından ilgilendiren 5651 sayılı kanunda yer alan cezai sorumlulukların birçoğu kabahat niteliğindedir. 5651 sayılı kanunun bilgi merkezleri ve bilgi profesyonelleri ile ilgili kısımları, "erişim sağlayıcılar", "içerik sağlayıcılar", "yer sağlayıcılar" ve "internet servis sağlayıcılar" ile ilgili düzenlemelerdir. Kütüphaneler başta olmak üzere, yapılan bir dizi

1 BORÇLAR KANUNU
Madde 49 - Kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür.

sözleşme çerçevesinde bilgi merkezlerinin büyük bölümü kullanıcılarına çeşitli veri tabanlarına erişim hizmeti sunmaktadır. Bir kullanıcı adı ve şifresi ile (ilgili kütüphane sunucusu üzerinden proxy servisi aracılığıyla) erişime sunulan veri tabanına ulaşımı sağlayan aracı konumundaki bilgi merkezi ya da bilgi işlem merkezi, 5651 sayılı kanun kapsamında erişim sağlayıcı rolünü üstlenmiş durumdadır ve kanunda tanımlanan erişim sağlayıcının yükümlülüklerini (örneğin trafik bilgisinin tutulması) uygulamalıdır. Üniversitelerin seçmiş oldukları veri tabanları ile anlaşmaların yapılması ve hizmetlerin sunulması ile ilgili olarak üniversite kütüphanelerinin sorumlu olduğu, fakat bilişim altyapı ve yer sunum hizmetlerinin üniversite bilgi işlem daire başkanlıkları tarafından yürütüldüğü üniversitelerde bu sorumluluğun nasıl paylaşıldığı ya da hangi birimin üstlendiği konusunda henüz fikir birliği olmadığı görülmektedir. Bilgi merkezlerinin 5651 sayılı kanun çerçevesinde yer, içerik ve erişim sağlayıcısı olarak kendi sorumluluk alanlarında bulunan sunum sağlayan bilgisayarların üzerinde gerçekleştirdiği eylemlerden, bilgi merkezinde görevli bilgi profesyonelleri sorumludurlar. Fakat 5651 sayılı kanun çerçevesinde ele alınan içerik sağlayıcının, yer sağlayıcının, erişim sağlayıcının sorumlulukları ve toplu kullanım sağlayıcılarının (örneğin; üniversite kütüphaneleri) yükümlülükleri; idari yapılanma ve görevlerin paylaşımına bağlı olarak bilgi merkezleri ve bilgi işlem merkezleri arasında farklılık gösterebilmektedir.

Üniversite kampüsleri ya da birden fazla coğrafi alanda faaliyet gösteren bilgi merkezlerinin; 5651 sayılı kanun uyarınca uyulması gereken kuralları yazılı olarak ilân etmelerinin, meydana gelebilecek birçok olayda sorumlulara daha kolay ulaşma ve görev/sorumluluk paylaşımında meydana gelebilecek ihmâllerin önüne geçmede etkili olacağı değerlendirilmektedir. 5651 sayılı yasanın uygulanmasına yönelik olarak az sayıda olsa da olumlu örnekler bulunmaktadır (ODTÜ BİDB, 2008a).

İçerik Sağlayıcı Olarak Sorumluluk

Bilgi merkezleri web sayfaları aracılığıyla sundukları içerikten 5651 sayılı kanun çerçevesinde "içerik sağlayıcı" sıfatıyla sorumludurlar. Kanunda *internet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler* şeklinde tanımlanan içerik sağlayıcı terimi, web sitesinin yönetim, yayın ve tasarım sorumlularını da içine almaktadır. Kullanıcılarının dışarıdan veri girişi yapabildiği web sitelerinde; başka bir kişiye ait içerikle ilgili olarak, içeriğin benimsendiğine dair açık bir ifade ve yönlendirme bulunması halinde de bilgi yöneticisinin sorumluluğu devam etmektedir.

İçerik sağlayıcının kim olduğuna karar verilebilmesi için; içeriği sağlayan, içerik üzerinde değiştirme ve içeriği kaldırma yetkisi olan kişiye bakılması gerekmektedir. Yetki paylaşımının yapıldığı kurumsal yapıda, idari yapılanma ve yetkilendirme hiyerarşisi de göz önünde bulundurulmalıdır. Örneğin; bir üniversitede bulunan ve kendi web sayfasına sahip olan her birim, personel ve öğrenci içerik sağlayıcı olarak değerlendirilebilir. İçeriği denetleme yetkisi bulunan bilgi profesyonelinin, içeriğin değiştirilmesi ile ilgili

tüm yetkileri devretmediği sürece içerik sağlayıcı olarak sorumluluğu devam edecektir. Bu nedenle bilgi profesyonelleri, bilgi merkezinin sorumluluğunda bulunan içeriğin denetimini, bilgi güvenliği kapsamında "içerik sağlayıcı" sıfatıyla yapmak zorundadır. Bilgi merkezleri kurumsal olarak, personel ise kendi web sayfalarının içeriğinden kişisel olarak yasalara karşı sorumludurlar.

Yer Sağlayıcı Olarak Sorumluluk

5651 sayılı kanunda yer sağlayıcı; "hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler" olarak tanımlanmıştır (TBMM, 2007). 5651 sayılı kanuna göre yer sağlayıcının tespiti için faaliyet belgesine bakılması gerekmektedir. Bilgi merkezleri ve üniversiteler Telekomünikasyon İletişim Başkanlığı'ndan (TİB) "Yer Sağlayıcı Faaliyet Belgesi" almalıdırlar. Bilgi merkezleri, üniversiteler ve kurumlarda sunucu bilgisayarların (e-posta, web, ftp, dosya sunumcu vb.) işletilmesinden sorumlu birimlerin ve personelin sorumlulukları yer sağlayıcı kapsamda değerlendirilmektedir.

Yer sağlayıcılar normal şartlarda içeriği kontrol etmekle yükümlü olmadıkları halde; hukuka aykırı içerik ile ilgili olarak haberdar edilmeleri halinde içeriği yayından kaldırma (teknik olarak mümkünse) yükümlülükleri bulunmaktadır. Koruma tedbiri olarak verilen erişimin engellenmesi kararlarının TİB aracılığıyla elektronik ortamda yer sağlayıcıya gönderilmesinden itibaren; yer sağlayıcı erişimi engellenen yayını kaldırmak ve kararla ilgili bilgi yazısına yönlendirme yapmakla yükümlüdür.

Yer sağlayıcı ile içerik sağlayıcı aynı kişi olabildiği gibi; farklı kurum, bölüm ve kişiler de olabilmektedir. Farklı kişilerin sorumlu olması halinde; yer sağlayıcının bilgi güvenliği kapsamında içeriğin güvenliğini sağlama yükümlülüğü bulunmakta, fakat içeriği kendi karar verme yetkisini kullanarak kontrol etme ya da içeriği değiştirmeye hakkı bulunmamaktadır. Yer sağlayıcının bu tür girişimleri de ayrıca TCK'nın bilişim alanındaki suçlarla ilgili düzenlemesi kapsamında değerlendirilebilir.

5651 sayılı yasa kapsamında 2007 yılında yayınlanan 26716 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmeliğin" 7/1c maddesi gereğince; "yer sağlayıcı trafik bilgisini 6 ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle" de yükümlüdür (T.C. Başbakanlık, 2007). Yer ve erişim sağlayıcıların farklı olması durumunda yer sağlayıcıların trafik bilgisi tutmasının ne kadar doğru olacağı ise tartışma konusudur. Zira 5651 sayılı kanun; trafik bilgisi tutma yükümlülüğünü sadece erişim sağlayıcıya vermiştir.

Erişim Sağlayıcı Olarak Sorumluluk

Erişim sağlayıcıların 5651 sayılı yasa kapsamında kullanıcısına ait hukuka aykırı içeriğe erişimi; kanuna uygun olarak haberdar edilmesi ve teknik imkânların bulunması halinde engelleme yükümlülüğü bulunmaktadır. Ayrıca; koruma tedbiri ve idari tedbir olarak verilen erişimin engellenmesi kararlarını uygulama ve trafik bilgilerini tutma

sorumlulukları da bulunmaktadır. Koruma tedbiri olarak verilen erişimin engellenmesi kararlarının uygulanması, yer sağlayıcılarda olduğu gibi kararın elektronik ortamda alınmasından sonra derhal yerine getirmesini gerektirir. Konusu suç teşkil eden bir yayını üzerinde bulunduran içerik ya da yer sağlayıcının yurt dışında olması halinde ise, TİB tarafından alınacak idari kararla erişimin engellenmesine karar verilerek en geç 24 saat içinde hâkim onayına sunulmaktadır.

Erişim sağlayıcı, 26716 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" gereğince; TİB'e gerektiğinde bilgi aktarımı yapmak, trafiğin izlenmesinde destek vermek, faaliyetleri hakkında bilgilendirme yapmak ve vekil (proxy) sunucu trafik bilgilerini tutmakla da sorumludur. Bilgi merkezlerinin önceden yapılmış anlaşmalara bağlı olarak kendi sunucuları üzerinden kullanıcıların veri tabanlarına erişimini sağlama hizmeti, erişim sağlayıcı özelliğine örnek olarak verilebilir.

İnternet Toplu Kullanım Sağlayıcı Olarak Sorumluluk

5651 sayılı yasada toplu kullanım sağlayıcı; "kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı" ifade etmektedir. Bilgi merkezlerinin büyük bölümünde tanımda belirtilen internet ortamı kullanım olanağı sağlanmaktadır. Bir kurumun yerel ağına ya da bir bilgi merkezi ağına, sabit ya da dinamik IP adresi kullanmak suretiyle (kablolu ya da kablosuz olarak) erişim sağlayan personel ve kullanıcılar, kurum ya da bilgi merkezi tüzel kişiliği altında faaliyet gösteren toplu kullanım sağlayıcı olarak değerlendirilmektedirler (ODTÜ BİDB, 2008b).

Toplu kullanım sağlayıcıların IP adresi dağıtım kayıtlarını elektronik ortamda kaydetme ve konusu suç teşkil eden içeriğe erişimi engelleyici önlemler alma yükümlülükleri bulunmaktadır. Hangi IP adresinin hangi bilgisayara (MAC[2] adresi eşleştirmesi ile) ve hangi zaman aralığında tahsis edildiği bilgisini içeren IP adresi dağıtım kayıtları, bilgi güvenliği kapsamında büyük öneme sahiptir. Şayet bir birim (örneğin; kütüphane), bilgi işlem merkezinden almış olduğu bir IP adres bloğunun yönetimini, kendi içindeki kullanıcılarına internet kullanımı için IP adresi tahsis ederek üstlenmiş ise, internet toplu kullanım sağlayıcının yükümlülüklerini yerine getirmek zorundadır.

5846 Sayılı Fikir ve Sanat Eserleri Kanunu Açısından Sorumluluk

Bilgi merkezlerinde telif haklarının korunması ile ilgili iki durum söz konusudur. Bunlardan birincisi herhangi bir sözleşme yapmaksızın bir elektronik bilgi kaynağına erişim sağlanması; diğeri ise bilgi merkezinde bulunan elektronik bilgi kaynağının güvenliğinin sağlanmasıdır.

İnternetin yaygınlaşmaya başladığı ilk dönemlerde yaygın bir anlayış olarak ortaya çıkan "erişilebilen her kaynağa erişim meşrudur" anlayışının, günümüzde bilgi merkezi

2 MAC (Media Access Control) Adresi: Bilgisayarın kendine özgü ağ kartı numarasıdır. Herhangi bir olay sonrasında MAC adres kayıtlarından kullanıcıya ulaşmada kolaylık sağlamaktadır.

hizmeti olarak kabul edilmesi mümkün değildir. Kısıtlı bütçeler nedeniyle başvurulan izinsiz erişim yöntemi, yasal düzenlemelerde yoruma yer vermeyecek kadar açık bir şekilde yasaklanmış ve eserin yayınlanmasıyla ilgili tüm haklar eser sahibine verilmiştir. Bilgi merkezleri de bu alandaki yasal düzenlemelere uymakla yükümlüdürler.

Bilgi merkezlerinde bulunan elektronik bilgi kaynaklarının kime, ne kadar süre ile ve nasıl sunulacağı konusu da telif hakları ile ilgili diğer bir sorunu oluşturmaktadır. Bilgi merkezinde bulunan tüm bilgi kaynaklarının telif haklarının korunmasından ilgili bilgi profesyoneli sorumludur (Toplu, 2007). Ulusal ve uluslararası boyutta, elektronik bilgi kaynaklarının yasa dışı çoğaltılması konusu henüz çözüm bulunamayan sorunlardan biri olarak varlığını devam ettirmektedir. Bu konuda bilgi merkezi yöneticileri ve bilgi profesyonelleri üzerine düşen sorumluluk; elektronik bilgi kaynaklarına yetkisiz erişimlerin ve kaynakların bilgi bütünlüğünün bozulmasına neden olabilecek girişimlerin bertaraf edilmesi amacıyla, bilgi güvenliği çerçevesinde birtakım önlemlerin alınmasını sağlamaktır.

Bilgi güvenliği ve 5846 sayılı yasa çerçevesinde bilgi merkezlerinde manevi ve mali hakların korunması amacıyla önlem alınması gereken konulardan bazıları; hak sahibinin yazılı izni olmaksızın eserlerin depolanması, değiştirilmesi, dağıtılması, hukuka aykırı olarak çoğaltılması ve umuma iletilmesidir.

İdari Sorumluluk

Bilgi profesyonellerinin genel ve bilgi teknolojilerini kullanarak yerine getirdikleri hizmetlerle ilgili olarak hukuki sorumluluklarının yanı sıra idari sorumlulukları da bulunmaktadır. İdari sorumluluklar kanun, tüzük, yönetmelik ve genelgelere bağlı olarak her bilgi merkezi tarafından kendi içerisinde belirlenmiştir. İdari sorumluluğun yerine getirilmemesi halinde, yetkili makamlar tarafından disiplin cezası gibi yaptırımlar uygulanır.

Bilgi profesyonellerinin 5651 sayılı kanundan kaynaklanan cezai sorumlulukları büyük ölçüde basit nitelikteki suçları düzenleyen 5326 sayılı "Kabahatler Kanunu" kapsamında yer almaktadır. Kabahatler kanunu genel ahlâk ve toplum düzenini koruyan düzenlemeler içermektedir. Kabahatin oluşabilmesi için; bilgi profesyonelinin yapması gereken bir hareketi yapmaması (ihmal yoluyla) ya da yapmaması gereken bir hareketi yapmış olması şartı gerekir. Kabahatin gerçekleştiği olaya bağlı olarak uygulanan idari para cezasının miktarı değişebilir. Şayet bir kişi, tüzel kişinin görevini üstlenmiş ya da temsilci sıfatıyla bir gerçek kişiyi temsil ederken kabahat işlemişse; bu durumda tüzel kişi ya da temsil edilen kişi hakkında idari yaptırım uygulanabilir.

Etik Olarak Kullanıcı Gizliliğinin Sağlanması ve Bilgi Merkezlerinin Sorumlulukları

Günümüzde bilgi merkezleri sadece bilgi kaynaklarının depolandığı alanlar olmanın ötesinde, farklı formatlarda (elektronik, görsel, işitsel vb.) bulunan ve sayısı katlanarak artan bilgi kaynaklarına erişim sağlayan, eğitim ve kültür merkezleri haline gelmiştir.

Bilgi teknolojilerinin son yıllardaki hızlı gelişimi ve bilgi merkezlerinde yoğun kullanımı; en önemli etik kurallarından biri olan "kullanıcı gizliliğinin sağlanması" konusunda bilgi profesyonellerinin sorumluluklarını arttırmıştır. Kullanıcı gizliliği; kullanıcıların bilgi merkezlerinde yapmış oldukları araştırmaların, faydalandıkları kaynakların, kütüphane web sayfası üzerinden yapmış olduğu aramalara ait kayıtların ve ulaştığı veri tabanlarının, kullanıcının onayı olmaksızın paylaşılmaması anlamında kullanılmaktadır. Gizlilik; kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleri anlamına gelmektedir (Winter, 1997). Bilgi merkezlerinin elektronik kaynaklara çok daha fazla yer veriyor olması, sunulan veri tabanı hizmetlerindeki artış ve kullanıcıların elektronik bilgi kaynaklarına olan ilgilerinin artması; bu alanda çalışan bilgi profesyonellerine yeni sorumluluklar yüklemiş ve bilgi güvenliği konusunun daha önemli hâle gelmesini sağlamıştır.

Anayasa, TCK, Türkiye'nin 1981 yılında imzaladığı Avrupa Konseyi tarafından hazırlanan Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması ile ilgili 108 sayılı sözleşme ve bu konuda yeni düzenlemeler içeren "Kişisel Verilerin Korunması" kanun tasarısı ile hukuksal olarak mahremiyetin korumaya alınmasına çalışılmış olsa da, sadece hukuksal düzenlemeler ile mahremiyete yönelik saldırının önüne geçilmesi mümkün değildir. Ayrıca; internet kullanıcılarının arama motorları aracılığıyla yapmış oldukları aramaların bir veri tabanına aktarılması ve Wikileaks olayları gibi örnekler, mahremiyeti korumanın kişilerin kendi elinde olmadığı gibi, özellikle uluslararası düzlemde hükümetlerin de çaresiz kalabildiğinin bir göstergesidir (Hürman ve Özmen, 2011). 1996 yılından beri bekleyen Kişisel Verilerin Korunması Kanun Tasarısı'nın en kısa zamanda yasa haline gelmesi ve bu alanda işlenen suçlarla bağlantılı olarak ticari hâle gelen "veri madenciliği" ile ilgili bilişim suçlarına yönelik yeni düzenlemelerin yapılması, mahremiyetin korunması ile ilgili hukuksal eksikliklerin giderilmesini sağlayacaktır. Fakat bilgi merkezlerindeki mahremiyete yönelik saldırıların azalması, bilgi profesyonellerinin mesleki bir ilke olarak benimsedikleri etik kuralları çerçevesinde bilgi güvenliği ile ilgili almış oldukları önlemlerin etkinliğine bağlıdır.

Bilgi merkezlerinde gizlilik konusu ilk olarak 1939 yılında Amerikan Kütüphane Derneği (American Library Association - ALA) tarafından ele alınmış ve Ahlak Kuralları (Code of Ethics) başlığı altında; kullanıcıların kütüphaneden edindikleri bilgilerin, danıştığı sorunların ve ödünç aldığı kitapların gizliliğinin sağlanması ile ilgili kurallar belirlenmiştir. Bu kurallar 1981, 1995 ve 2008 yıllarında tekrar gözden geçirilmiş ve bazı düzeltmeler yapılmıştır (ALA, 2008). ALA Konseyi'nin elektronik bilgi ve hizmetlerine yönelik 24 Ocak 1996 tarihinde yapmış olduğu yorumda; kütüphane ve kütüphanecilerin varlık nedeninin, "düşüncenin kaydedildiği format ve teknoloji ne olursa olsun bir düşünceyi tanımlama, düzenleme, hazırlama ve erişimi sağlamakla bu hakların kullanımını kolaylaştırmak olduğu" vurgulanmaktadır. Fakat elektronik bilgilere erişimin kolaylaşması, kişisel bilgilerin gizliliği ve güvenliğini önemli bir sorun olarak ortaya çıkarmıştır (Çelik ve Tonta, 1996).

1980'li yıllarda Federal Soruşturma Bürosu (Federal Bureau of Investigation – FBI) ve yerel kolluk kuvvetleri tarafından kütüphane kullanıcılarının kütüphane kullanım ve okuma alışkanlıklarının incelenmesi, 1990'lı yıllarda kullanıcıların internet üzerinden yapmış oldukları kütüphane işlemlerinin incelemeye alınması, 2001 yılında Amerika'da meydana gelen terör olayları sonrasında yapılan soruşturmalarda kütüphane kayıtlarına da herhangi bir gerekçe/şüphe olmaksızın başvurulması ve elde edilen bilgilere bağlı olarak soruşturmaya yön verilmesi ve 2002 yılında bu işlemlerin otomatik olarak yapılmasını sağlayan programların Amerika Savunma Bakanlığı tarafından uygulamaya konulması, kütüphane kullanıcılarına ait kayıtların ne kadar önemli olabileceğinin bir göstergesidir. Fakat kullanıcı gizliliği ve etik boyutu ile bakıldığında; hakkında soruşturma yapılan bir kullanıcının bilgilerinin verilmesi sonrasında, kütüphane tarafından kullanıcıya işlem hakkında bilgi verilip verilmemesi konusunda dahi Amerika'da ortak bir görüş hâkim değildir. Kullanıcı gizliliğinin sağlanması konusunda ALA, kullanıcı gizliliğinin benimsenmesi ve bu doğrultuda politikalar geliştirilmesi gerektiğini belirtmiştir. Bunun öncelikli adımlarından birinin de kullanıcıya ait gereksiz kayıtların tutulmaması olduğunun ve sadece kütüphane hizmetleri için zorunlu olan en az kişisel bilginin kaydedilmesi gerektiğinin altı çizilmiştir (ALA, 2007). Bilgi merkezlerinin kullanıcılar hakkında elektronik ortamda tuttukları ve bilgi güvenliği kapsamında gizliliğin korunmasına konu olan bilgiler genel olarak şunlardır;

- ◊ Üyelik esnasında alınan telefon, isim, ev/iş adresi, meslek bilgileri (personel, lisans öğrencisi vb.), elektronik posta adresi, vatandaşlık numarası, kurum kimlik (veya öğrenci kimliği) numarası,
- ◊ Ödünç alınan yayınlara ait bilgiler,
- ◊ Bağlantı kurulan veri tabanları ile ilişkilendirilmiş kullanıcı hesapları ve bağlanılan bilgisayara ait IP numaraları kayıtları,
- ◊ Kütüphane web sayfası üzerinden elde edilen; tarama geçmişi, erişim sağlanan IP adresi, ziyaret edilen tarih/zaman dilimi, kullanılan tarayıcı ve işletim sistemi gibi bilgiler.

Bu kayıtların bir bölümü (IP kayıtları, ziyaret edilen tarih/zaman dilimi vb.), hukuk kuralları ile etik değerlerin arasında çelişki oluşturmakta ve bu yüzden meydana gelen olaylarda bilgi merkezlerinin detaylı düşünülmüş ve dengelenmiş yazılı eylem planına ihtiyaç duymalarına sebep olmaktadır. Hukuk kuralları (örneğin 5651 sayılı kanun) meydana gelen olaylarda faile ulaşılabilmesi amacıyla bilgi merkezlerinde ve internet servis sağlayıcılarda birtakım kayıtların tutulmasını ve belirli bir süre muhafaza edilmesini zorunlu kılarken; bu alandaki evrensel etik değerler tek taraflı bakış açısıyla, mümkün olduğunca en az seviyede kişisel bilgi kaydının tutulmasını ve böylece erişim özgürlüğü ve gizliliğin zarar görmemesini savunmaktadır. Bu konudaki yasal düzenlemelerin henüz yeni yapılmış olması ve Türkiye'de bilgi merkezlerine yönelik siber tehditlerin diğer Avrupa ülkeleri ve ABD ile kıyaslandığında çok düşük seviyelerde olması, bilgi merkezlerinde bulunan elektronik verilerin durumunun hukuki ve etik boyutuyla değerlendirilmesinin ilgi ve çalışmaların dışında kalmasına neden olmuştur.

Türk Kütüphaneciler Derneği (TKD) tarafından 1996 yılında bilgi hizmetlerinde çalışanlara hitaben hazırlanan ve üyeler tarafından benimsenen etik ilkeleri, kütüphanelerle ilgili olarak bu konuda yapılan önemli bir çalışmadır (TKD, 1996). 1996 yılında yürürlüğe konulan Mesleki Etik İlkelerinin 2010 yılında elektronik ya da basılı-yazılı kaynak ayrımı yapmaksızın mevcut yasal düzenlemelerin de dikkate alınarak yeniden gözden geçirilmesi ile birlikte; çelişkilerden büyük ölçüde uzak ve kullanıcı gizliliğini ihlal etmeyen yeni etik değerler benimsenmiştir. Yeni etik kurallar içerisinde; kullanıcıların yaptığı araştırmaların, ödünç aldığı ve/veya yararlandıkları bilgi kaynaklarının neler olduğunun gizliliği güvence altına alınmakta ve kişisel bilgilerin yasal gereklilik dışında kimseyle paylaşılmayacağı belirtilmektedir (TKD, 2010). Bilgi edinme özgürlüğü, özel hayatın gizliliği ve kişilik haklarının korunması ile yakın ilişki içerisindedir. Batılı ülkelerde bilgi edinme özgürlüğü konusundaki sınırlar ortadan kaldırılırken, kişilik haklarının da korunması önemsenmektedir. TKD'nin de Mesleki Etik İlkelerini yeniden düzenlerken bu hassasiyeti göz önünde bulundurduğu ve hazırlanan yeni ilkelerin bilgi profesyonellerine rehber olabilecek nitelikte olduğu görülmektedir.

Hukuksal Düzenlemeler ve Etik Kurallarının Belirlenmesi Konusunda Neler Yapılmalıdır?

Mevcut hukuksal düzenlemeler içinde bilgi merkezlerini ve bilgi profesyonellerini ilgilendiren birçok konu bulunduğu gibi; bilgi merkezlerine yönelik olarak işlenen bilişim suçları içinde artan öneme sahip güncel tehditlerle ilgili yeni düzenlemelerin zaman kaybetmeksizin yapılması gerekmektedir. Yabancı hukuk mevzuatlarından uyarlanması, yeniden yapılması ya da onaylanarak yürürlüğe girmesi halinde birçok konuda belirsizliği gidereceği düşünülen düzenlemelerin bazıları şunlardır (TBD, 2012);

- 5237 sayılı TCK, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve 5070 sayılı Elektronik İmza Kanunu'nun altyapısını oluşturan "Ulusal Siber Güvenlik Yasa Tasarısı" yasalaştırılmalıdır.
- "Avrupa Konseyi Siber Suçlar Sözleşmesi" TBMM tarafından onaylanarak yürürlüğe girmeli ve iç hukuka uyum için gerekli düzenlemeler yapılmalıdır.
- "Kişisel Verilerin Korunması Yasa Tasarısı" yeniden değerlendirilerek ve farklı görüşler de dikkate alınarak yasalaştırılmalıdır.

Kullanıcı gizliliğinin etik olarak korunması ile ilgili, Türkiye'de henüz belirlenmiş politikaların bulunduğu ya da yaygın bir anlayış olduğunu söylemek yanıltıcı olabilir. Hukuksal düzenlemelerde olduğu gibi, etik kurallarının da oluşması meydana gelen olayları takip etmekte, bir başka ifade ile geriden gelmektedir. Bu yüzden; Türkiye'de henüz bilgi profesyonellerinin üzerinde kişisel bilgilerin korunması konusunda baskı ve stres olmaması, gizliliğin korunması ile ilgili problemlerle (Amerika'da olduğu gibi) sıkça karşılaşmamaları ile ilişkilendirildiğinde olumlu olarak yorumlanabilir.

Fakat bilgi teknolojilerinin kullanımının her geçen gün arttığı Türkiye'de özellikle elektronik ortamda bilgi erişimlerinin artmasıyla birlikte, bilgi merkezlerinde bulunan kişisel bilgilerin gizliliğine yönelik tehditlerin artacağı aşikârdır. Bu yüzden; Amerika örneğinde karşılaşılan problemlerin ve oluşturulan etik değerlerin önceden irdelenmesi ve uygulanabilir olanların benimsenmesi, meydana gelebilecek birtakım zorluklarla mücadelede bilgi profesyonellerine kolaylık sağlayacaktır. Etik açıdan değerlendirildiğinde; bilgi güvenliği ile ilişkili olarak düşünülmesi gereken dış tehditlere karşı gizliliğin muhafaza edilmesi ve soruşturma vb. nedenlerle kamu kurumları tarafından talep edilen bilgilerin verilmesine yönelik olarak iki farklı durum ortaya çıkmaktadır. Her iki durumu da göz önünde bulundurarak; gizliliğin korunması ile ilgili yerel olarak bir bilgi merkezinde alınması gereken önlemler konusunda, ALA'nın belirlediği şablon üzerinden aşağıda yer alan temel hususlar örnek alınabilir (ALA, 2007). Buna göre;

- ◊ Elektronik ortamda bulunan verilerin erişimi konusunu da içine alacak şekilde yazılı bilgi güvenliği ve gizlilik politikasının geliştirilmesi,
- ◊ Bilgi merkezinde çalışan tüm bilgi profesyonellerinin hukuksal ve etik sorumluluklar konusunda eğitilmesi,
- ◊ Bilgi profesyonellerinin yetkisiz erişimlerin tespiti ve gizliliğin ihlâl edildiği bu tür durumlarda hangi birimlerle (bilgi işlem ve savcılık gibi) koordineli olarak çalışacağı konusunda bilgilendirilmesi,
- ◊ Yapılan düzenlemelerle ilgili üyelik sürecinde ve sonrasında kullanıcıların bilgilendirilmesi. Bilgi güvenliği ve gizliliğin sağlanması konusunda kullanıcıların alacakları önlemlerin bildirilmesi,
- ◊ Yapılan sözleşmelerin kütüphane politikalarına, kullanıcı gizliliğinin korunması ile ilgili etik değerlere ve hukuksal düzenlemelere uygun olması,
- ◊ Küçük yaştaki bilgi merkezi kullanıcılarının ailelerinin de bilgi merkezinde geçerli olan gizlilik politikaları ile ilgili olarak bilgilendirilmeleri ve belirlenen politikalar dâhilinde belirli bir yaşın altında (örneğin; Amerika'daki "Çocukların Çevrimiçi Gizliliğini Koruma Yasası" içinde 13 yaş sınırı olduğu gibi) (COPPA, 1998) bulunan küçüklerden ailesinin bilgisi dışında kişisel bilgi alınmaması, yerel bir bilgi merkezinin alabileceği uygulanabilir önlemlerden bazılarıdır.

Değerlendirme ve Sonuç

Günümüzde bilgi merkezleri sadece yazılı basılı bilgi kaynaklarının bulunduğu bir bilgi deposu olmasının ötesinde, dünyanın her noktasından erişim sağlanabilen ve dünyanın hangi noktasında olursa olsun kullanıcılarına bilgi hizmetleri sunan küresel kültür merkezleri haline gelmişlerdir. Bilgi merkezleri, çeşitli elektronik kaynaklara erişim hizmeti sağlayarak ve koleksiyonlarını elektronik ortama aktararak; anlık bilgiye ihtiyaç duyan kullanıcılarına, gelişen bilgi teknolojileri ve internetin de yardımıyla cevap verebilme imkânına kavuşmuşlardır.

Bilgiye kesintisiz erişim, çağımızın en öncelikli konuları arasında yer almakta ve birkaç dakikalık kesinti dahi birçok meslek grubu için tahammül sınırlarını zorlamaktadır. Bu nedenle, kesintisiz bir bilgi hizmeti sunabilmek için gerekli tüm önlemleri almak, bilgi profesyonellerinin başlıca sorumluluklarından biridir. Bunun için; bilgi hizmetlerinin sunulduğu bilgi sistemlerini, elektronik bilgi kaynaklarını ve kullanıcı gizliliğini her türlü tehditten hukuk ve etik kuralları çerçevesinde korumak, gerekli güvenlik önlemlerini almak ve tüm önlemlere rağmen engel olunamayan sorunlar karşısında önceden belirlenmiş yazılı politikaların uygulanmasını sağlamak gerekir.

Yasal düzenlemelerle çelişmeyen kütüphane politikalarının geliştirilmesi ve benimsenmesi, kullanıcının özgür bir şekilde istediği tüm bilgi kaynaklarına erişiminin sağlanması, bilgi hizmetlerini sağlayan bilgi profesyonellerinin bilinçliliğinin artırılarak kullanıcı gizliliğinin sağlanması konusuna özen göstermeleri ve yasal zorunluluk nedeniyle tutulan kayıtların bilgi güvenliği ve kişisel bilgilerin gizliliği kapsamında korunması etik açıdan alınabilecek önlemlerin başında gelmektedir.

Kullanıcılara önceden bildirilmiş yazılı bilgi merkezi kuralları, kullanıcı ile bilgi merkezi arasındaki güven ortamının oluşmasına katkı sağlamaktadır. Kullanıcıların bilgi merkezlerinde bulunan yazılı-basılı kaynaklara ulaşırken kendilerini güvende hissetmelerini sağlayan güven ortamı, elektronik ortamda bulunan bilgi kaynaklarına ulaşırken de sağlanmalıdır. Kullanıcı gizliliği ve kullanıcıya ait bilgilerin güvenliğinin sağlanması, bilgi toplumlarının üzerinde hassasiyetle durduğu ve birçok meslek grubunun benimsediği etik değerlerin bir parçası haline gelmiştir. Bilgi profesyonelleri ile kullanıcılar arasındaki ilişki; avukat-müvekkil veya doktor-hasta arasında alışılagelmiş gizlilik ilişkisinden daha önemsiz değildir. Ayrıca kullanıcılar bilgi merkezlerine vermiş oldukları bilginin nasıl kullanılacağını bilme hakkına sahiptirler.

Bilgi profesyonellerinin bilgi merkezlerinin hizmetlerinin yürütülmesinde üstlendikleri sorumlulukların boyutu, bilişim ve hukuk alanlarının çözüm üretmeye çalıştıkları birçok hukuki ve etik konuyu ilgilendirir hâle gelmiştir. Bilgi merkezlerinde bilgi teknolojilerinin kullanımının artışına bağlı olarak, farklı disiplinler birbirine yaklaşmakta, ortak zemine dayalı çalışmalar hız kazanmaktadır. Sadece hukuksal düzenlemelerle suçun oluşumunun tamamen önüne geçilemediği ve sürekli olarak yeni suç modellerinin geliştirildiği bir alanda bilgi profesyonellerinin tam olarak başarılı olabilmeleri için, etik kuralları benimsemeleri ve diğer disiplinlerin uzmanlık alanına giren ortak ve temel mesleki bilgiye de yeterli seviyede sahip olmaları gerekmektedir. Şayet bir bilgi kaynağının yayınlanması ya da bilgi merkezlerinde bulundurulması yasal bir düzenleme ile yasaklanmış ise, düşünce özgürlüğü ve bilgiye erişim özgürlüğü gibi konularla ilgili olarak bir kütüphane görevlisinden beklenen geleneksel etik davranışın aksine, alınacak önlem bilgi kaynağına en azından uzaktan erişimin engellenerek yasanın uygulanmasıdır. Yasa ile yasaklanmış bir elektronik bilgi kaynağına erişimin teknik olanaklarla kısıtlanabilmesi ve yasal yükümlülüğün yerine getirilebilmesi için,

bilgi kaynağına bilgisayar ağları üzerinden erişimin kapatılması ve bulunduğu fiziksel ortamda çoğaltılmasının engellenmesi gerekmektedir. Bilgi-iletişim teknolojilerinin gelişimi ile beraber; herhangi bir erişim yasağı için istisnalara yer verilmesi ve açık kapı bırakılması halinde, erişimi yasaklanan bilginin hızla çoğaltılması ve bu nedenle yasağın uygulanamaz hâle gelmesi mümkün olabilmektedir.

Türkiye'de ulusal bir bilgi güvenliği politikası bulunmamaktadır. Özellikle bilgi merkezleri, kamu kurumları ve özel kuruluşlara önerilerde bulunabilecek ve koordinasyon sağlayacak bir teşkilatın (ulusal bilgi güvenliği teşkilatı) ve bilgi güvenliği konusunda belirli standartların uygulanmasını öngören yasal düzenlemenin bulunmaması; bilgi merkezlerini kendi sınırlı maddi imkân ve bilgi birikimlerini kullanarak çözümler üretmeye zorlamakta ve bu konuda yalnız kalmalarına neden olmaktadır. Bu eksikliğin bilgi merkezleri üzerindeki etkisinin en düşük seviyede hissedilmesi için; bir bilgi güvenliği politikasının oluşturularak bilgi profesyonellerinin sorumluluk ve görevlendirmelerinin bu çerçevede yazılı hâle getirilmesi gerekmektedir. Böylece; sorumluluk bilincinin hızla kazanılması sağlanacak ve bilgi profesyonelleri görevini yaparken, hukuk kuralları ile farklı kaynaklardan edinilen mesleki etik kurallarındaki çelişkiler arasında kalmamalarını sağlayacak bir kılavuza sahip olacaklardır.

Bilgi merkezlerinde bilgi güvenliğinin sağlanması; uluslararası standartlarda kesintisiz ve güvenilir bilgi hizmetini kullanıcılara sunabilmek için öncelikli olarak üzerinde durulması gereken konulardan biridir. Bilgi güvenliğinin sağlanması konusunun sadece bilgi teknolojilerinin ve onu programlayanların problemi gibi algılanması, olası sorunlara davetiye çıkarmaktadır. İnsan faktörü bilgi güvenliğinin en zayıf halkasını oluşturmaktadır. Bilginin nasıl korunacağı aşamasına geçmeden önce; neden korunacağı konusu üzerinde durulmalı ve tüm bilgi profesyonellerinde bu konu hakkında farkındalığın oluşması sağlanmalıdır. Bilgi güvenliği riski hiçbir zaman ortadan kaldırılamasa dahi; bilinçli (hukuki ve etik sorumluluklarını bilen) bilgi profesyonelleri ile kabul edilebilir seviyeye düşürebilir. Bilgi profesyonellerinin eğitimlerinde bilişim ve hukuk alanlarında konuyla ilgili soruları ortadan kaldıracak düzeyde bilgi almaları, ileride karşılaşacakları sorunların çözümünde yardımcı olacaktır. Bilgi güvenliği konusunda edinilen bilgiler; artık kaçınılmaz bir zorunluluk haline gelen diğer disiplinlerle koordinasyonun daha kolay kurulabilmesine, daha iyi bilgi hizmeti sunabilmek için gerekli teknik çözümlerin üretilmesine, mali kaynak gerektiren ihtiyaçların belirlenmesine ve bilgi merkezi politikalarının geliştirilmesine de ışık tutacaktır.

Kaynakça

ALA. (2007). *Privacy tool kit*. 17 Mart 2012 tarihinde http://www.ala.org/offices/oif/iftoolkits/toolkitsprivacy/introduction/introduction adresinden erişildi.

ALA. (2008). *Code of ethics of the American Library Association.* 17 Mart 2012 tarihinde http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf adresinden erişildi.

Avrupa Konseyi. (2001). *Convention on cybercrime*. 14 Temmuz 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm adresinden erişildi.

Bozkurt, A. (2010). Türkiye de "Sanal Suçlar Sözleşmesi"ni imzaladı. *Bilişim Dergisi*. *127*, 10-12.

BSI. (2012). *Bundesamt für Sicherheit in der Informationstechnik*. BSI-Informationen. https://www.bsi.bund.de/DE/Home/home_node.html adresinden erişildi.

COPPA. (1998). *COPPA - Children's Online Privacy Protection Act*. 17 Mart 2012 tarihinde Federal Trade Commission: http://www.ftc.gov/ogc/coppa1.htm adresinden erişildi.

CSI. (2011). *Computer crime and security survey.* 24 Mart 2012 tarihinde http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html adresinden erişildi.

Çelik, A. ve Tonta, Y. (1996). *Düşünce özgürlüğü, bilgi edinme özgürlüğü ve bilgi hizmetleri.* 17 Mart 2012 tarihinde http://yunus.hacettepe.edu.tr/~tonta/yayinlar/beozgur.html adresinden erişildi.

Doğan, Y. H. (2005). *Özel hayata ve hayatın gizli alanına karşı suçlar.* 17 Mart 2012 tarihinde http://www.ceza-bb.adalet.gov.tr/makale/146.doc adresinden erişildi.

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

Hürman, H. ve Özmen, S. (2011). *İnternette mahremiyet: başlangıcı ve sonu….* 17 Mart 2012 tarihinde http://siviltoplumakademisi.org.tr/index.php?option=com_content&view=article&id=809:internette-mahremiyet-&catid=65:mansetler&Itemid=121 adresinden erişildi.

Karagülmez, A. (2009). *Bilişim suçları ve soruşturma-kovuşturma evreleri.* Ankara: Seçkin Yayıncılık.

Karasözen, B. ve Gürgüz, E. (2004). *ODTÜ Kütüphanesi performans bütçeleme projesi ve toplam kalite çalışmaları.* Ankara: ODTÜ Kütüphane ve Dokümantasyon Daire Başkanlığı.

Ketizmen, M. (2008). *Türk Ceza Hukukunda bilişim suçları.* Ankara: Adalet Yayınevi.

ODTÜ BİDB. (2008a). *ODTÜ yerel alan ağında 5651 sayılı kanun uyarınca uyulması gereken kurallar.* 26 Mart 2012 tarihinde http://www.metu.edu.tr/5651/files/5651_sayili_kanunun_uygulanma_kurallari_v1.0.pdf adresinden erişildi.

ODTÜ BİDB. (2008b). *5651 Sayılı kanun ile ilgili sıkça sorulan sorular*. 26 Mart 2012 tarihinde http://www.metu.edu.tr/5651/sss.php adresinden erişildi.

TBD. (2012). Ulusal siber güvenlik yasa tasarısı acilen yasalaştırılmalı. *Bilişim Dergisi*. *141*, 14-15.

TBMM. (2004). *Türk Ceza Kanunu.* 30 Mart 2012 tarihinde http://www.tbmm.gov.tr/kanunlar/k5237.html adresinden erişildi.

TBMM. (2007). *İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun.* 26 Mart 2012 tarihinde http://www.tbmm.gov.tr/kanunlar/k5651.html adresinden erişildi.

T.C. Başbakanlık. (2007). *İnternet ortamında yapılan yayınların düzenlenmesine dair usul ve esaslar hakkında yönetmelik.* 26 Mart 2012 tarihinde http://www.mevzuat.adalet.gov.tr/html/27666.html adresinden erişildi.

T.C. Başbakanlık. (2009). *E-Devlet ve bilgi toplumu kanun tasarısı taslağı.* 16 Temmuz 2012 tarihinde http://akgul.bilkent.edu.tr/e-devlet/taslak.pdf adresinden erişildi.

TKD. (1996). *BBY Haber.* 18 Mart 2012 tarihinde http://www.bbyhaber.com/bby/wp-content/uploads/dosyalar/mevzuat/Mesleki-Etik-Kurallari.pdf adresinden erişildi.

TKD. (2010). *Türk Kütüphaneciler Derneği mesleki etik ilkeleri.* 18 Mart 2012 tarihinde http://www.kutuphaneci.org.tr/index.php?view=article&catid=45%3Atkd-bildirgeler&id=115%3Atkd-meslek-etik&format=pdf&option=com_content&Itemid=101 adresinden erişildi.

Toplu, M. (2007). Kütüphaneciliğin etik sorunu ve Türkiye yaklaşımı. *Türk Kütüphaneciliği*, *21*(2), 186-217.

Winter, K. (1997). *Privacy and the rights and responsibilities of librarians.* 17 Mart 2012 tarihinde http://www.cstone.net/~kwinter/articles/ksr4_winter.pdf adresinden erişildi.