**ULUSAL BİLGİ GÜVENLİĞİ POLİTİKALARI AÇISINDAN KAMU KURUMLARININ İNCELENMESİ: KAYSERİ BAROSU ÖRNEĞİ**

***Ali KAYA[[1]](#footnote-1)***

***Damla MURSÜL[[2]](#footnote-2)\*\****

**Öz**

Küreselleşme süreciyle birlikte teknoloji, hayatımızın her alanına girmiştir. İçinde bulunduğumuz süreçte yaşanan gelişmeler, klasik yönetim anlayışının ötesine geçerek bilgi ve hizmetlerin kullanıcıya (vatandaş-müşteri) daha hızlı daha kolay ulaşması yönünde talepler doğurmuştur. Bilgi ve hizmete erişebilirlik, bilgi toplumunun en önemli güç kaynaklarından biridir.

Çalışma, ulusal bilgi güvenliği sisteminin temel mevzuatını oluşturan strateji belgeleri ve eylem planlarından yola çıkarak kamu kurumlarının bilgi güvenliği kültürüne yaklaşımını uygulamaya koyduğu politikalar çerçevesinde ortaya koymayı amaçlamaktadır. Güvenlik kültürü; yöneticilerin, çalışanların, hizmetten faydalananların ve tüm kamu üyelerinin karşı karşıya kalabilecekleri sorunların en aza indirilmesi ya da ortadan kaldırılmasına yönelik uygulamaları içermektedir. Günümüz bilgi toplumlarında bilgi güvenliği konusu, güvenlik kültürünün/güvenlik yaklaşımının önemli bir boyutudur. Gelişen teknolojiyle birlikte internet ortamında bireysel veya kamusal düzeyde çeşitli güvenlik riskleri ortaya çıkmakta, buna bağlı olarak kamu kurumları çeşitli önlemler almaya yönelmektedir. Kamu kurumlarında güvenlik kültürünün oluşturulabilmesi için bilgi güvenliği ve siber güvenlikle ilgili düzenlemeleri öngören mevzuat bilgi sistemi, çalışmanın ele aldığı kurumsal dokümanların kaynağını oluşturmaktadır.

Bu kapsamda çalışma, 2015-2018 arası dönemi içeren *Bilgi Toplumu Stratejisi ve Eylem Planının* ele aldığı ulusal bilgi güvenliği politikalarını; bu politikaların kamu kurumları için belirlediği hedefleri ve uygulama önerilerini, nitel araştırmalarda kullanılan veri toplama araçlarından biri olan doküman incelemesi yöntemiyle Kayseri Barosu özelinde analiz etmeye çalışmaktadır. Analiz sonucunda bilgi güvenliği ve güvenlik kültürü yaklaşımları çerçevesinde Kayseri Barosu’nun başlangıç düzeyinde birtakım faaliyetler yürüttüğü, çevrim içi ortamda kullanıcılarla bu bilgileri paylaştığı ancak bu girişimlerin henüz yetersiz olduğu sonucuna varılmaktadır. Eylem Planı’nda sorumlu kuruluş olarak belirtilen Adalet Bakanlığı’nın bu konularda tüm barolara daha fazla katkı sağlaması önerilmektedir.

**Anahtar kelimeler:** Kamu Kurumu, Bilgi Toplumu, Güvenlik Kültürü, Bilgi Güvenliği, Ulusal Bilgi Güvenliği Politikaları.

**A REVIEW OF PUBLIC INSTITUTIONS IN TERMS OF NATIONAL INFORMATION SECURITY POLICIES: SAMPLE OF KAYSERI BAR ASSOCIATION**

**Abstract**

Technology has entered every aspect of our lives with the globalization process. The developments in the current period led to the need for information and services to reach the user (citizen-customer) faster and more easily beyond the classical approach of management Accessibility to information and service is one of the most important sources of power in the information society.

The study aims to reveal approach of the public institutions about information security culture within the framework of the policies implemented by the strategy documents and action plans that constitute the basic legislation of the national information security system. Safety culture includes practices aimed at minimizing or eliminating the problems that managers, employees, service beneficiaries and all public members may face. In order to establish a security culture in public institutions, the legislation information system, which provides regulations on information security and cyber security, is the source of the institutional documents.

In this context, the study includes the national information security policies addressed by the *2015-2018 Information Society Strategy and Action Plan*; it tries to analyze the objectives and implementation proposals of these policies for public institutions specific to Kayseri Bar Association by document analysis method which is one of the data collection tools used in qualitative research. As a result of the analysis, it is concluded that Kayseri Bar Association carries out some activities at the beginning level within the framework of information security and security culture approaches, and shares the related information with users by online services, but these initiatives are not sufficient yet. It is recommended that the Ministry of Justice, which is mentioned as the responsible institution in the Action Plan, should contribute further to all bar associations on these issues.

**Keywords:** Public Institution, Information Society, Security Culture, Information Security, National Information Security Policy.

**1. Kavramsal Çerçeve**

Çalışma, bilgi toplumu kavramından hareketle güvenlik kültürü ve bilgi güvenliği kavramlarına öncelik vermekte ve bilgi güvenliğine ilişkin ulusal politikaları, bu kavramlar üzerinden incelemeye çalışmaktadır.

* 1. **Bilgi Toplumu**

Bilgi toplumu, küreselleşme sürecinin hız kazanmasıyla birlikte 20.yüzyılın sonlarına doğru sıkça duymaya başladığımız, son dönemde ise doğrudan içinde bulunduğumuz toplumla özdeşleştirdiğimiz bir kavramdır. Geray (1997), aslında bilgi toplumu kavramının henüz 20.yüzyıla gelinmeden ortaya atıldığını ve ilk kez, iletişim uzmanı Marshall McLuhan tarafından 1962 yılında kullanıldığını ifade etmektedir (Geray’dan akt. Yılmaz, 1998: 149).

Bilgi toplumu; küresel toplum, endüstri toplumu, enformasyon toplumu, post modern toplum gibi pek çok kavramla birlikte, çoğu zaman birbirlerinin yerine anılmaktadır. Literatürde bilgi toplumu kavramına karşılık gelen alternatif adlandırılmalar mevcuttur. İngilizce’deki ‘information society’ kavramını tam olarak karşılamadığı ve bu nedenle enformasyon toplumu olarak kullanılması gerektiği konusunda birtakım tartışmalar bulunmaktadır. Bu makalede farklı adlandırmalar üzerinde durmaktansa kavramdan ne anlamamız gerektiği üzerinde durulmaktadır.

Bilgi toplumu ya da bilgi toplumunun içinde bulunduğu bilgi çağı, internetin yaygınlaşması ve hem sunulan hizmetlerin hem de bu hizmetlere erişimin dijitalleşmesi süreciyle anlam kazanmıştır. İnsan zihninin de gücüyle beşeri sermayenin potansiyeline bağlı bir toplumsal dönüşüm olgusu, tüm dünyada yeni bir çağın başlangıcına vesile olmuştur (Meder, 2001: 73).

 Çoban (1997), içinde bulunduğumuz çağın bilgi toplumunun temel özelliklerini aşağıdaki maddeler çerçevesinde sıralamaktadır;

-Bilgi, merkezi önemdedir,

-İşletmenin mantığı küreseldir,

-Bilgi sektörü kurumsallaşmıştır,

-Çevre koruma bilinci yüksektir,

-Sivil toplum etkindir,

-Birey, merkezi öneme sahiptir,

-Yoğun bilgisayarlaşma hakimdir,

-Toplum, örgütlü bir yapıdadır (Çoban’dan akt. Meder, 2001: 73).

 Bilgi çağı, bilgiyi referans noktası olarak alan, üretim ve iletişimin yaygınlaşması ile değişim ve gelişimin kaçınılmaz olduğu yeni bir toplumsal ve ekonomik yapıyı ifade etmektedir (Öğüt’ten akt. Balay, 2004: 66). Günümüzde bilgi; doğal kaynaklar, sermaye, emek ve girişimci gibi adeta üretim unsurlarından biri haline gelmiş ve yaşamın merkezine oturmuştur. Sanayi sonrası toplumlarının geçirdiği dönüşüm sürecinde üretimi mümkün ve sürekli kılan, standart-rasyonel-kontrollü bilgi yığını ve bunun yön verdiği işbölümüdür (Meder, 2001: 74). Bilgi ve bilgi toplumunun öneminin temel göstergeleri, yukarıda sıralanan özelliklerin de birer yansıması olarak küresel güvenlik, insan hakları, sivil toplum, teknoloji, ekonomi, ekoloji, siyaset vb. konuların ya da sorun alanlarının doğrudan ulus üstü düzeyde çeşitli ortamlarda tartışılıyor olmasıdır (Çukurçayır ve Çelebi, 2009: 61).

 Kuşkusuz bilgi toplumunun temel özelliklerine ilişkin pek çok eleştiri getirilebilir ancak burada önemli olan bilginin etkilediği ve yönlendirdiği bir kurumsallaşma ve buna bağlı olarak yaşanan toplumsallaşma sürecidir. Her iki süreçte de en önemli konuların başında güvenlik kültürü yaklaşımı gelmektedir.

**1.2.Güvenlik Kültürü**

 Güvenlik kültürü kavramı, 1986 yılında yaşanan Çernobil faciasından sonra ortaya atılmış bir kavramdır (Cox ve Flin, 1998: 190). Uluslar arası Atom Enerjisi Kurumu (IAEA), 1991 yılında güvenlik kültürü kavramını şu şekilde tanımlar: ‘Kurumun sağlık ve güvenlik programlarının yeterliliğine, tarzına ve uygulamadaki ısrarına karar veren birey ve grupların değer, tutum, yetkinlik ve davranış örüntülerinin bir ürünüdür’ (Özkan ve Lajunen, 2003: 3).

Risk düzeyinin fazla olduğu durumlarda ya da olaylarda güvenliğin sağlanmasında insan faktörü, büyük önem taşımaktadır. Güvenlik kültürü, insanların güvenliğe dair tutumları, değerleri ve davranışlarını ifade etmekle birlikte; güvenliğin sağlanması, sürdürülmesi, kontrolü ve bu yöndeki her türlü politikayla ilgili uygulamaları içermektedir.

 Geleneksel hizmet sunumunun elektronik ortama taşınması, yalnızca hizmeti sunan ya da hizmetten faydalananlar açısından değil; ülkeler açısından da önemli bir duruma gelmiştir. Hem kamu sektörünün hem özel sektörün bilgi alt yapılarını kapsayan güvenlik endişesi, zaman içerisinde güvenlik yaklaşımlarının geliştirilmesine ve bu konuda politikalar ve eylemler oluşturulmasına neden olmuştur. Güvenlik, yalnızca fiziki koşulların iyileştirilmesi olarak algılanmamalı, bu konuda bilinçli bireyler olabilmek adına farkındalığın arttırılması ve kullanıcıların kişisel ve daha büyük çapta bilgilerinin/verilerinin korunması yönünde yeterli donanıma sahip olması şeklinde ele alınmalıdır. Bilgi eksikliği, kuşkusuz bu konudaki en önemli engellerden biridir (Dursun, 2011; Akalp ve Yamankaradeniz, 2013).

 Katılımcılığın arttırılması, kamu**-**özel işbirliğinin sağlanması, kurumsal yapılanma, ulusal bir stratejinin izlenmesi, yasal çerçeve oluşturulması, siber tehditlerle mücadele gibi pek çok girişim, güvenlik kültürünün birer bileşeni konumundadır. Hem kullanıcıların hem de bu teknolojileri kullanarak hizmet sunan yönetimlerin eğitilmesi, sorumluluk ve görevlerine dair bilgilendirilmesi gerekmektedir. Ülke genelinde olabileceği gibi meslek içi ya da kurum içi eğitimler aracılığıyla da eksiklikler giderilebilir. Bu konuda OECD ve AB tarafından bağlayıcı olmasa da rehber niteliği taşıyan birtakım ilkeler güncellenerek yayınlanmaktadır.

Benzer şekilde son olarak 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Eylem Planı’nda da ulusal düzeyde tüm kullanıcıların (yöneticiler ve bilgisayar kullanan herkes) siber güvenlik kültürüne sahip olması, bu bilincin kazandırılması ve alanda uzman personel yetiştirilmesi yönünde girişimlerde bulunulmuştur (<https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>, 2016).

**1.3.Bilgi Güvenliği**

Bilgi, artık günümüz toplumlarında en merkezi konumda yer almaktadır (Meder, 2001: 72). Ulusal bilgi güvenliği konusu, günümüzde neredeyse her ülkede odak noktası haline gelmiş ve büyük önem kazanmıştır. Gelişmiş ülkelerden ziyade az gelişmiş ya da gelişmekte olan ülkeler açısından da bilgi güvenliği konusuyla ilgili birtakım politikaların hayata geçirildiği, mevzuat ve uygulama örnekleri aracılığıyla bilgi çağının gereği olan güvenlik ağının geliştirilmeye çalışıldığı görülmektedir.

Bilgi güvenliği; bilginin tutulduğu bilgi sistemlerindeki her türlü bilginin kullanımını, korunmasını, değiştirilmesini, incelenmesini, ortadan kaldırılmasını ya da yetkisiz erişime karşı korunmasını ve buna ilişkin tüm önlemleri içermektedir. Kişisel bilgisayarlardan kurumsal ve ulusal çaptaki tüm bilgi sistemlerini kapsayan geniş bir güvenlik yönetimi anlayışı olarak karşımıza çıkmaktadır.

 Türkiye de bilgi güvenliği konusunda gereken teknolojinin yalnızca tüketicisi değil, aynı zamanda üreticisi konumunda yer almalıdır. Teknolojik yenilikler, eğitimden bilime, yönetimden üretime pek çok alt yapı çalışmasının sağlıklı ve uyumlu bir şekilde yürütülmesiyle mümkün olabilecektir (Yılmaz, 1998: 155).

 Bilgi güvenliği açısından bakıldığında dijital ortamda verilerin, kötü niyetli kullanıcılara açık olduğu ve dolayısıyla tehlike altında olduğu açıktır. Diğer adıyla dijital güvenlik, ‘yeni’ bir tehlike formu olarak adlandırılmakta; gerçek dünyadaki tehditlerden farklı olarak bir de sanal dünyadaki tehdit unsurunun varlığıyla karşı karşıya kalındığını göstermektedir (Karabulut, 2015: 117). Bilgisayar teknolojileri açısından bilgi güvenliğinin amacı, kişi ve kurumların sahip oldukları bu teknolojileri kullanırken karşı karşıya kalabilecekleri tehdit ve tehlike unsurlarına yönelik gerekli tedbirlerin alınmasını ve ilgi faaliyetlerin tümünün önceden planlanmasını ifade etmektedir (Canbek ve Sağıroğlu, 2006: 169).

**1.3.1.Bilgi Güvenliğinin Unsurları**

Çağımızın önemli sorun alanlarından biri haline gelen bilgi güvenliği, bilginin üç ana unsuru üzerinde durulmasını gerekli kılmaktadır.

* Gizlilik,
* Bütünlük,
* Kullanılabilirlik (Güngör, 2015: 8).

Gizlilik, bilginin yalnızca yetki verilen; bilginin korunması, işlenmesi vb. süreçlerin yönetiminde sorumlu kılınan kişilerin erişimine açık olmasını sağlayarak; yetkisiz kişilerin tehdit oluşturmasını önleme amacını ifade etmektedir. Diğer yandan kaydedilen ya da girilen herhangi bir bilginin içeriğinin korunması, bütünlüğünün bozulmamasının sağlanması bütünlük; kullanıma hazır durumda muhafaza edilmesi ise kullanılabilirliğini (erişilebilirlik) içermektedir.

Bilgi güvenliğinin göz önünde bulundurulması gereken diğer ilkeleri ise kayıt altına alma, kimlik tespiti, güvenirlik ve inkar edememe (sayısal imza yöntemiyle gönderici ve alıcı arasındaki işlemler) şeklinde sıralanabilir (Tekerek, 2008: 133-134).

 Söz konusu unsurlar ve temel ilkeler çerçevesinde gerek ulusal gerek uluslar arası düzeyde bilgi güvenliğine dair politika araçları geliştirilmekte ve çeşitli politika önerileri hayata geçirilmektedir.

**1.3.2.Bilgi Güvenliği Politika Alanları**

Bilgi güvenliğinin temel unsurlarından hareketle ihtiyaç duyulan çok çeşitli alanlarda politika geliştirilmesi ihtiyacı kaçınılmazdır. Gerek özel gerek kamu sektörünü ilgilendiren bu alanlar;

* Bilgisayar ve ağ güvenliği,
* Bilgi güvenliği yönetim sistemi,
* Bilgi güvenliği yönetişimi,
* Kriptoloji,
* Siber güvenliği,
* Bilişim suçları,
* Veri mahremiyeti ve korunması,
* Ulusal güvenlik ve
* Uluslar arası işbirliği şeklinde sıralanabilir (Güngör, 2015: 13-24)

Bilgi teknolojilerinin hayata geçirilmesinde insan faktörü olduğu için bu alandaki güvenlik kaygılarının da dayandığı temel sorun, özünde insandır. Bilinçli olarak ya da bilinçsizce ihmaller neticesinde bazı riskler ve tehdit unsurları (kötüye kullanma, çalma, izinsiz alma, etkisiz kılma vb.) ortaya çıkabilir. Kısacası hayata geçiren de ortadan kaldıran da aynı faktördür, insan (Güngör, 2015: 2).

İnsan faktörünün etkisiyle gerek teknik gerek sosyal ve kültürel açıdan pek çok konu, politika alanlarına dahil edilebilir. İlk aşamada uygulama alanlarının çoğu, teknik ya da fiziki özellikler göstermektedir. Ancak bu durum, toplumsal ve kültürel açıdan bilgi güvenliği yaklaşımını göz ardı etmemize engel değildir.

**2.Türkiye’de Ulusal Bilgi Güvenliği Politikaları**

Kamu yönetiminde bilgi teknolojilerine dayalı uygulamaların kullanımı, son dönemde giderek yaygınlaşmaktadır. Özellikle ticaret, bankacılık, ulaştırma ve haberleşme gibi pek çok sektörde internet kullanımı, vatandaş ve müşteriye çeşitli kolaylıklar (*hız, basitlik, şeffaflık, maliyet, etkinlik gibi*) sağlamaktadır. Hizmet sunumunda internetten faydalanılması, bilgi sistemlerinin güvenilir olmasını ve risklere karşı korunmasını zorunlu kılmaktadır. Bu alandaki uluslar arası düzenlemelerin, ulusal düzeyde uyumlaştırılması ve Türkiye’nin ihtiyaçlarına cevap verebilecek şekilde düzenlenmesi kaçınılmazdır.

**2.1.Ulusal Bilgi Güvenliğinin Stratejik Unsurları**

* Siyasi sahiplenme: Politika yapıcıların ve ilgili kamu yöneticilerinin bilgili olması, önlem alınması konusunda kararlılık göstermesi ve ulusal bir strateji oluşturulması yönündeki faaliyetlerin tümünü içerir.
* Kurumsal Yapılanma: Ulusal strateji çerçevesinde kurumlar arasında eşgüdüm ve koordinasyon sağlanmasıdır.
* Suçla Mücadelede Yasal Altyapı: Bilişim suçlarının ve bunlara yönelik cezai yaptırımların belirlenmesi, siber suçla mücadele edilmesidir.
* Kritik Bilgi Altyapılarının Korunması: Bir ülke açısından önem arz eden bilgilerin korunması için ayrı bir strateji oluşturulmasını gerekli kılan durumdur.
* Bilgisayar Olaylarına Müdahale Ekipleri: Güvenlik tehditlerini takip eden, bilgilendirme ve önlemeye yönelik faaliyetleri yürüten yetkili birimlerdir.
* Kamu Bilgi Sistemleri Güvenliği,
* Kamu-Özel Sektör Koordinasyon ve İşbirliği,
* Eğitim, Farkındalık ve AR-GE Çalışmaları,
* Uluslar Arası İşbirliği (ITU, 2011).

Ulusal anlamda örgütlenme ve yapılanma açısından yukarıda sayılan stratejik unsurlar, bilgi güvenliğini sağlama konusunda özen gösteren ülkeler açısından önem taşımaktadır. Bu ülkeler arasında AB’ye üye ülkeler, ABD, Çin ve Japonya dikkatleri çekmektedir. Özellikle e-devlet uygulamalarında güvenli bir ortamda zaman ve maliyet tasarrufu ile hizmet sunumu öne çıkmaktadır (Efendioğlu ve Sezgin, 2007: 222-226).

Türkiye de söz konusu unsurlar çerçevesinde birtakım politikalar geliştirmiştir ve de geliştirmeye devam etmektedir.

**2.2.Türkiye’de Ulusal Bilgi Güvenliği Konusunda Yapılanlar**

Türkiye’de ulusal bilgi güvenliği konusunda 90’lı yılların başlarından bu yana hayata geçirilen ve uygulamaya geçirilemese de planlama aşamasında kalan birtakım düzenlemeler aşağıda sıralanmıştır:

1. Bilişim ve Ekonomik Modernizasyon Raporu: 1993 yılında Türkiye ve Dünya Bankası işbirliğinde hazırlanmıştır. Ulusal bilgi güvenliğine ilişkin ilk çalışmadır. Türkiye’nin bilgi toplumuna geçiş sürecindeki ihtiyaçları belirlenerek eylem planı oluşturulması yönünde öneriler sunmuştur ancak uygulanamamıştır. Kişisel verilerin korunması, bilgisayar güvenliği konularıyla sınırlı kalan çalışmanın şu anki algıdan oldukça farklı ve basit düzeyde olduğu belirtilmelidir.
2. Güvenlik Çalışma Grubunun kurulması (1996) (kanun tasarısına dönüşmemiştir)
3. E-Türkiye Girişimi ve taslak eylem planlarının hazırlanması
4. Başbakanlık Müsteşarının başkanlığında kamu kurum ve kuruluşlarının katılımı ile Kamu-Net Üst Kurulu ve Kamu-Net Teknik Kurulu oluşturulması (1998): Bilişim güvenliğine yönelik çalışmalar yaparak eylem planı önerisi getirilmiştir. E-Türkiye Girişiminin hayata geçirilmesine dek kurullar faaliyet göstermiştir.
5. Türkiye Enformasyon Politikası ve Enformasyon Altyapısı Ana Planı (TUENA-1999): Bilgi güvenliği kavramına değinen önemli raporlardan biridir. Bilgi Toplumu Bakanlığına dönüşmesi öngörülen Bilgi Toplumu Kurumu şeklinde bir kurumsal yapılanma modeli önerilmiştir. Ulusal Bilgi Güvenliği Kanun Taslağı ile eş zamanlı çalışmalar yürütmüştür.
6. Ulusal Bilgi Güvenliği Kanun Tasarısı: Kanun tasarısında ulusal bilgi güvenliği, haberleşme güvenliği, personel güvenliği, kriptoloji gibi konularda düzenlemeler yapılmış; çalışmaları yürütecek yönetsel örgütler oluşturulmuştur. Bu amaçla Ulusal Bilgi Güvenliği Üst Kurulu ve Ulusal Bilgi Güvenliği Kurumu Başkanlığı kurulması hedeflenmiştir. Tasarı halen yasalaşmamıştır. Halen bu konuda ciddi bir boşluk bulunmaktadır (Kırışık, 2016: 118).
7. E-Dönüşüm Türkiye Projesi (2003): Projenin başlıca hedefleri; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olan bir devlet yapısı geliştirmek, bilgi ve iletişim teknolojileriyle ilgili AB ile uyumlu mevzuat ve politikaları hayata geçirmek, aday ülkeler için öngörülen eylem planlarını Türkiye’ye uyarlamaktır.
8. 2003-2004 Yıllarını Kapsayan Kısa Dönemli Bir Eylem Planı
9. 2006-2010 Yıllarını Kapsayan Bilgi Toplumu Stratejisi ve Eki Eylem Planı: En kapsamlı ulusal politika metnidir. Adalet Bakanlığı’na ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi için düzenleme yapma ve Kişisel Verilerin Korunması Hakkında Kanun Tasarısı Taslağını yasalaştırma görevleri verilmiştir. 2016 yılı itibarıyla Resmi Gazetede yayımlanmıştır (<https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>, 2019).
10. 8. Kalkınma Planı: Ulusal düzeyde yasal düzenlemelere yer veren ilk kalkınma planıdır, 2001-2005 yıllarını kapsamaktadır. Son olarak da
11. Siber Güvenlik Kurulunun Oluşturulması (2012) gibi pek çok faaliyet sıralamak mümkündür.

**3. 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı**

Çalışmanın ele aldığı temel politika dokümanı, 2015-2018 yıllarını kapsayan ve en son uygulanan Bilgi Toplumu Stratejisi ve Eylem Planı’dır. Söz konusu Eylem Planı, 2014 yılı Aralık ayında Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı tarafından yayınlanmıştır. 204 sayfadan oluşan raporun temel stratejiler ve 2018 yılı hedeflerinin yer aldığı bölümdeki ana başlıkları (sekiz eksenden oluşmak üzere) şöyledir:

**1.**Bilgi Teknolojileri Sektörü

**2.**Genişbant Altyapısı ve Sektörel Rekabet

**3.**Nitelikli İnsan Kaynağı ve İstihdam

**4.**Bilgi ve İletişim Teknolojilerinin Topluma Nüfuzu

**5.**Bilgi Güvenliği ve Kullanıcı Güveni

**6.**Bilgi ve İletişim Teknolojileri Destekli Yenilikçi Çözümler

**7.**İnternet Girişimciliği ve e-Ticaret

**8.**Kamu Hizmetlerinde Kullanıcı Odaklılık ve Etkinlik.

Yukarıda yer verilen strateji ve hedef başlıkları arasında Bilgi Güvenliği ve Kullanıcı Güveni başlığı, çalışmanın özellikle üzerinde durmayı hedeflediği başlığı oluşturmaktadır. 5 numaralı eksen çerçevesinde *Adalet Bakanlığı*, *sorumlu kuruluş* olarak raporda yer almıştır. Bakanlığın sorumluluğuna verilen strateji ve 2018 hedefleri kapsamında yürütülmesi planlanan eylemler ise şöyledir:

**Eylem 1:** Siber Güvenlik Kanunu’nun çıkarılması,

**Eylem 2:** Kişisel verilerin korunması mevzuatının çıkarılması,

**Eylem 3:** Siber suçla mücadele stratejisi ve eylem planının oluşturulması,

**Eylem 4:** Bilişim suçları ihtisas mahkemelerinin kurulması.

**3.1. Adalet Bakanlığı Ayağı: Bakanlık Tarafından Verilen Elektronik Hizmetler**

Bakanlık ve ilgili teşkilat yapısı içerisinde verilen e-hizmetlere bakıldığında ilk sırada UYAP (Ulusal Yargı Ağı) Bilişim Sistemi’nin yer aldığı görülmektedir. Bu uygulamayı, UYAP Uzaktan Eğitim Bilgi Sistemi, SMS Bilgi Sistemi, İcra Malları e-Satış Portalı, Vatandaş Portalı, Avukat-Bilirkişi-Kurum Bilgi Sistemleri, SEGBİS (Ses ve Görüntü Bilişim Sistemi) gibi çeşitli uygulamalar takip etmektedir (<http://afyonluoglu.org/e-devlet/tr-edevlet/#ADALET>, 2019)

Kamu sektöründe bilgi teknolojileri kullanımı konusunda öne çıkan önemli ve de ilk uygulamalardan biri, UYAP’tır. Uygulama ile adli işlemler açısından hem zaman hem de maddi tasarruf yapılmış, adli hizmetlerin görülmesinde mahkemeye gidilmesine gerek kalmamıştır. UYAP sistemi, Adalet Bakanlığı ile pek çok kamu kurumu arasında uyumlu çalışan bir altyapıya sahiptir. Bu kurumlar: Maliye Bakanlığı, Sosyal Güvenlik Kurumu, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Türkiye Cumhuriyeti Merkez Bankası, Vakıf Bank, PTT, Türk Telekom, Tapu ve Kadastro Genel Müdürlüğü, E-Devlet Kapısı ve Ulusal Baro Ağı Projesi’dir (<http://www.edevlet.gov.tr/wp-content/uploads/2017/08/03.08.2017-Koordinasyon-e-Devlet-Adalet-Bakanligi.pdf>, 2019). 1998 yılından bu yana devam eden çalışmalar sonucunda UYAP, yargı birimlerinin tamamını kapsar hale getirilmiştir.

UYAP, vatandaşlara ve avukatlara çeşitli adli hizmetlerin elektronik ortamda sunulmasını sağlayan bir sistemdir. Sistemde çalışan portallar; avukat, vatandaş, kurum, bilirkişi portalları, SMS bilgi sistemi ve e-satış portalıdır (Taş ve Uçacak, 2018: 507). UYAP’ın çok yönlü ve farklı toplumsal kesimlerin adli ihtiyaçlarına yönelik ortaya konan bir uygulama olduğunu söylemek mümkündür. UYAP, şemsiye bir oluşum olarak pek çok hizmeti bünyesinde barındırmaktadır.

UYAP öncesi ve sonrası ile hız kazanan işlemlerle ilgili olarak Adalet Bakanlığı’ndan edinilen bazı bilgiler şu şekildedir;

-Dosyanın başka birime gönderilme işi, yarım günden 0-1 dakikaya,

-Nüfus kaydı alma, 1 haftadan 0-1 dakikaya,

-Adli sicil kaydı alma, 1 haftadan 0-1 dakikaya,

-Dosya aşamalarını görme 10 günden 0-30 saniyeye,

-Matbu evrakların hazırlanması 5 dakikadan 0-30 saniyeye düşmüştür.

-Diğer istatistikler ise aşağıdaki gibidir (<http://www.edevlet.gov.tr/wp-content/uploads/2017/08/03.08.2017-Koordinasyon-e-Devlet-Adalet-Bakanligi.pdf>, 2019):

**Tablo1:** UYAP ve Sunulan e-Hizmetlerle İlgili Bazı Sayısal Bilgiler

|  |  |
| --- | --- |
| 2016 Yılında Üretilen Evrak Sayısı | 780 milyon (adet) |
| 2016 Yılında Günlük Okunan Evrak Sayısı | 13 milyon (adet) |
| 2016 Yılında Günlük Eklenen Evrak Sayısı | 3 milyon 600 bin (adet) |
| 2016 Yılında Güncellenen Evrak Sayısı | 1 milyon 200 bin (adet) |
| Gönderilen e-Tebligat Sayısı (01.01.2016-15.07.2017 tarihleri arasında) | 1 milyon 406 bin 824 (adet) |
| Avukat Portalı Aktif Kullanıcı Sayısı (2017)  | 72 bin 17 kişi |
| Avukat Portalı Günlük İşlem Sayısı (2017) | 8 milyon 338 bin 31 (adet) |
| Vatandaş Portalı Aktif Kullanıcı Sayısı (2017) | 1 milyon 640 bin 125 kişi |
| Vatandaş Portalı Günlük İşlem Sayısı (2017) | 41 bin 212 (adet) |
| UYAP SMS Üye Sayısı (2017) | 1 milyon 514 bin 80 kişi |

**Kaynak:** <http://www.edevlet.gov.tr/wp-content/uploads/2017/08/03.08.2017-Koordinasyon-e-Devlet-Adalet-Bakanligi.pdf>, 2019.

 Tablo 1’de de görüldüğü üzere 2017 yılı itibarıyla avukat ve vatandaş portallarındaki kullanıcı ve günlük işlem sayıları giderek artmaktadır. 2016 yılında üretilen evrak sayısı, 780 milyon civarındayken; bu sayının günümüzde mümkün olduğunca e-hizmetler üzerinden yürütüldüğü açıkça görülmektedir. E-hizmetlere yönelim, yargıdaki bürokratik ağırlığın da azalmasına yol açmış ve işlem hızını arttırmıştır.

**3.3.Kayseri Barosu Kapsamında Hayata Geçirilen e-Hizmetler ve Bilgi Güvenliği**

Kayseri Barosu, tüzel kişiliğe sahip kamu kurumu niteliğinde bir meslek kuruluşu olarak 1926 yılında kurulmuştur (<http://www.kayseribarosu.org.tr/Detay.aspx?ID=9009>, 2019). Baro bünyesinde pek çok komisyon görev almakla birlikte konumuz gereği bilgi güvenliği ve kullanıcı güveni konularında doğrudan sorumlu ve görevli birim olan Mevzuat İçtihat ve Bilişim Komisyonu’nun yer aldığını ayrıca belirtmek gerekir. Komisyon, 2013 yılında Kayseri Barosu’na üye olan sekiz avukat tarafından kurularak faaliyete geçmiştir.

Aşağıda Kayseri Barosu tarafından verilen e-hizmetlerden bazılarına yer verilmektedir;

**-Türkiye Barolar Birliği Kimlik Doğrulama Sistemi**

**-Baro Levhası Sorgulama:** Avukat adı ya da soyadıyla bölgedeki kayıtlı avukatların iletişim bilgilerine (eğer avukatın izni varsa telefon numaraları da dahil olmak üzere) erişim imkanı tanınmaktadır.

**-Baro TV:** Baro web sayfasından canlı yayına erişim olanağı bulunmaktadır.

**-UHAP:** Türkiye Barolar Birliği tarafından hazırlanan çevrimiçi bir otomasyon sistemidir. Barolar, TBB ve Adalet Bakanlığı arasındaki işleyişin hızlanması adına faaliyete geçirilmiştir.

Barolar; bilgi akışını arttırmak, süreç ve kaynaklarını denetim altında tutmak, bunları etkin şekilde planlamak ve bunu düşük maliyetle gerçekleştirmek, ayrıca iş bilgilerini güncelleştirememe kaynaklı problemleri en aza indirebilmek için içerik yönetim sistemi kullanımının avantajlarını göz önüne almalıdır. Devlet hizmetlerinin tümü elektronik ortamdan verilmeye başlandığında ulusal, kurumsal veya kişisel olarak verilen kararlar, yürütülen süreçler ve yapılan anlaşmaların tek ve en önemli kanıtı elektronik ortamda tutulacak olan belgeler olacaktır. Bu yeni sürece uyum sağlayabilmek ve bu değişimi yönetebilmek sağlam temellere oturtulmuş bir Web Tabanlı İçerik, Kaynak, Proje, Süreç, İş Akışı, İletişim ve Elektronik Belge Yönetim Sistemi ile mümkündür (<https://www.uhap.com.tr/#/bilgi/tanitim>, 2019).

Güvenlik ve gizlilik politikası gereği, kullanıcıların sisteme girdiği bilgiler, sadece kullanıcılara aittir. Bu verilerin güvenliğinin sağlanması için endüstri standardı önlemler uygulanır. Sitede yer alan bilgiler için veri güvenliği maksimum düzeyde tutulur. Site üzerinde yapılan sayfa gezinme işlemleri kayıt altına alınmaktadır. Bu bilgiler kullanıcı ayırt edici değildir, sitenin geliştirilmesi ve daha iyi hizmet vermesi amacıyla toplanmaktadır. Olası kötü niyetli kullanımı önlemek için siteye giriş ve çıkış işlemlerinin yapıldığı tarih, saat ve IP (internet) adresi kaydedilmektedir ve ortaya çıkabilecek kötü niyetli kullanımda, bu bilgiler olası bir hukuki süreçte delil olarak kullanılabilecektir. Kişisel bilgileriniz internet güvenlik standardı olan SSL Secure sistemi ile 128 mbit şifrelenmiştir. Bu şekilde internet üzerindeki dolaşımları sırasında herhangi bir şekilde bu bilgilerinizin istenilmeyen kişi veya kurumlarca ele geçirilmesi önlenmiştir (<https://www.uhap.com.tr/#/bilgi/yasaluyari>, 2019).

**-İlan Panosu:** Stajyer avukatlar da dahil iş arayan/ortak çalışabilecekleri diğer avukatları arayan tüm avukatların yer aldığı ilanlara çevrimiçi ortamda paylaşılmaktadır.

**-İcraTek – BüroTek – KararTek Uygulamaları:**

**İcraTek,** Türkiye Barolar Birliği tarafından avukatlar için özel olarak hazırlanmış bir online icra takip sistemidir. İcraTek programının marka ve isim hakkı Türkiye Barolar Birliği’ne aittir. Program, kullanımının kolay olması, her yerden ulaşılabilmesi, her bilgisayardan kullanılabilmesi konularına özellikle dikkat edilerek hazırlanmıştır (<https://www.icratek.com.tr/hakkimizda>, 2019).

SMS (kısa mesaj) modülü, İcraTek ile icra takibi ile ilgili herkese kısa mesaj gönderme işlemini kolaylıkla gerçekleştirebilirsiniz. Sistem üzerinden yüklenecek kredi ile sistem üzerinden istenilen numaraya kısa mesaj gönderimi yapılabileceği gibi, TC Kimlik Numarası ile telefon numarası sorgulaması ve TC Kimlik Numarasına kısa mesaj gönderimi yapılabilmektedir. İcraTek SMS modülü komple bir modül olup, sistem üzerinden yeni eklenecek telefon numarasına hızlı SMS, belirlenecek gruplara toplu SMS gönderilmesi, istenilen numaralar ile adres defteri oluşturulması, daha önce gönderilmiş mesajlara ait gönderme zamanı, iletim durumu, mesaj içeriği gibi kayıtlara ulaşılması mümkündür.

**BüroTek,** Türkiye Barolar Birliği tarafından Avukatlar için özel olarak hazırlanmış bir Online Büro Yönetimi Sistemi’dir. BüroTek programının marka ve isim hakkı Türkiye Barolar Birliği’ne aittir. Program, bir avukatlık bürosunun temel ihtiyaçlarını karşılaması, kullanımının kolay olması, her yerden ulaşılabilmesi, her bilgisayardan kullanılabilmesi konularına özellikle dikkat edilerek hazırlanmıştır (<https://www.burotek.av.tr/#/bilgi/hakkimizda>, 2019).

BüroTekmodülleri; Kişi İşlemleri; büro ile ilgisi olabilecek her kişiye ait kişisel bilgilerin ve iletişim bilgilerinin kaydedilebileceği, kişinin büro ile ilişki biçimine göre türünün belirlenebileceği modüldür. Kişi bilgileri sistemin diğer modüllerinde kullanılabileceği gibi ve kişi bilgilerinin sorgulanması, raporlanması ile kişilerle iletişim araçlarında kullanılması mümkündür. Notlar; danışma, icra, dava gibi büro işlerine ait dosyalar içinden işlerle ilgili notların, doğrudan alınacak notların, takvim üzerinden alınacak notların kaydedilebildiği modüldür. Kaydedilen notların takvime eklenmesi, notlara hatırlatıcı eklenmesi, hatırlatıcı eklenen notların yapılacak işler listesi olarak raporlanabilmesi mümkündür.

Evrak; büroya gelen ve bürodan gönderilen tüm evrak, yazışma ve belgelerin kaydedilebileceği modüldür. Danışma; büronun verdiği hukuki danışma hizmeti olarak değerlendirilebilecek işlerin ve görüşmelerin kaydedilebileceği modüldür. Danışma kaydında danışma içeriği yanında, danışma hizmetine ait notlar ve yapılacak işler, gelir ve gider kaydının yapılabileceği alanlar bulunmaktadır.

Dava; dava dosyalarına ait bilgilerin kaydedilebildiği modüldür. Dava kaydında dava içeriği yanında, dava dosyası tutanak ve belgelerinin, duruşma tarihlerinin, dava dosyasına ait notlar ve yapılacak işlerin, dava dosyasına ait gelir ve gider kaydının yapılabileceği alanlar bulunmaktadır.

İcra; icra dosyalarına ait bilgilerin kaydedilebildiği modüldür. İcra kaydında icra içeriği yanında, icra dosyası tutanak ve belgelerinin, haciz, satış tarihlerinin, icra dosyasına ait notlar ve yapılacak işlerin, icra dosyasına ait gelir ve gider kaydının yapılabileceği alanlar bulunmaktadır.

Cari/muhasebe işlemleri; büro gelir ve giderlerinin kaydedilebildiği modüldür. Yapılan kayıtlara ilişkin hesaplamalar, not ve hatırlatmalar ile raporlamalar yapılabilmektedir. e-Arşiv; büro ile ilgili her türlü belge, evrak, tutanak gibi dosyaların tüm program kullanıcılarının kullanımına sunulmak üzere çeşitli formatlarda yüklenebildiği modüldür. Bilgilendirmeler; kullanıcının programa kayıtlı kişilere ya da rehberine ekleyeceği kişilere SMS ya da ses SMS (sesli mesaj) gönderebileceği modüldür.

Sorgulama hizmetleri; GSM operatörlerinin sunduğu sorgulama hizmeti seçeneklerinin program üzerinde kullanılabildiği modüldür. Demirbaş; büro demirbaşlarının ve bulunduğu yerlerin ve kimin kullanımına tahsis edildiği bilgilerinin girilebildiği modüldür. Kütüphane; bürodaki her türlü yayının kütüphaneler, yayın grupları oluşturarak tüm bilgileri ile kaydedilebildiği ve gerek duyulursa hareketlerinin izlenebildiği modüldür.Araçlar; mevzuat, dilekçeler, hesaplama araçları, standart faiz oranları gibi büro içindeki işleyiş sırasında faydalanılabilecek pratik araçların kullanılabildiği modüldür.İletişim; destek taleplerinin girişinin yapılabildiği modüldür (BüroTek modülleri hakkında bilgi için; <https://www.burotek.av.tr/#/bilgi/tanitim>, 2019).

**KararTek İçtihat Bilgi Bankası**, Türkiye Barolar Birliği tarafından avukatlar için özel olarak hazırlanmış bir çevrimiçi içtihat programıdır. Program ile yüksek yargı kararlarına interneti olan her cihazdan erişilmesi, kararlarda detaylı sorgulama yapılabilmekte, seçilen kararlar daha sonra ulaşılmak üzere karar havuzuna kaydedilebilmekte, programa üye olan kullanıcılar programa kendi ad ve soyadları ile karar ve karara ait yorum ekleyebilmektedir (<https://www.karartek.com.tr/#/kullanici/hakkimizda>, 2019).

SMS (kısa mesaj) modülü; KararTek üzerinden rehbere kaydedilecek kişilere kısa mesaj ve SesSMS gönderme işlemi kolaylıkla yapılabilmektedir. Sistem üzerinden yüklenecek kredi ile istenilen numaraya kısa mesaj gönderimi yapılabileceği gibi, yazılan metnin ses dosyası haline getirilerek karşı tarafa robot aracılığıyla okunduğu SesSMS de gönderilebilmektedir.

TC Kimlik Numarası ile telefon numarası sorgulaması ve TC Kimlik Numarasına kısa mesaj gönderimi yapılabilmektedir. KararTek SMS modülü komple bir modül olup, sistem üzerinden yeni eklenecek telefon numarasına hızlı SMS, belirlenecek gruplara toplu SMS gönderilmesi, istenilen numaralar ile adres defteri oluşturulması, daha önce gönderilmiş mesajlara ait gönderme zamanı, iletim durumu, mesaj içeriği gibi kayıtlara ulaşılması mümkündür.

Sorgulama modülü; TC Kimlik Numarası ile GSM Numarası Doğrulama, TC Kimlik Numarası ile GSM Numarası Sorgulama, Kurumsal ve Bireysel Abonelik Sorgulama, Faturalı ve Faturasız Abonelik Sorgulama, Müşterim Bu Ülkede mi Sorgulama, SIM Kart Değişikliği Sorgulama, IMEI Aktiflik Sorgulama, Cihaz Değişikliği Sorgulama, Cihaz Modeli Sorgulama, Müşterim Yurtdışında mı Sorgulama Servisleri ile sorgulamalar KararTek üzerinden yapılabilmektedir. KararTek sorgulama modülü ile yapılacak işlemler GSM operatörlerine ve verdikleri hizmetlerin çeşidine göre değişebilmektedir (KararTek modülleri hakkında bilgi için; <https://www.karartek.com.tr/#/kullanici/tanitim>, 2019).

**3.4.Bilgi Güvenliği Konusunda Yürütülen Çalışmalar**

Kayseri Barosu, Adalet Bakanlığı ile koordineli bir çalışma yürüterek sunulan elektronik hizmetler konusunda gerek avukatlara gerek aktif kullanıcılara ve vatandaşlara yönelik pek çok eğitim semineri, panel ve staj programları sunmaktadır. Kayseri ölçeğinde üniversitelerle de işbirliği içerisinde bulunan Kayseri Barosu, avukatlara UYAP çerçevesinde yaşanan gelişmeler ve uygulama örnekleri hakkında da zorunlu eğitim ve bilgilendirme programları organize etmektedir.

 Kişisel verilerin korunmasına yönelik bilginin güvence altına alınması, saklanması ve koruma sürekliliğinin sağlanması gerekliliği günümüzde artık sıklıkla dile getirilen ve bu konuda özenli çalışmaların yürütüldüğü bir alandır. Yargı kararlarına erişim imkanı, kayıtlı avukatların (izin verilenlerin) bilgilerinin herkese açık olması ve yukarıda sayılan pek çok e-hizmetle ilgili bilgiler, güvenlik programları aracılığıyla korunmaktadır.

 Baro’nun resmi internet sayfasında yukarıda bahsedilen İcraTek, Bürotek ve KararTek uygulamalarının 24 saat hizmet verdiği belirtilmekle birlikte; bilgi kaybı, bilginin izinsiz kullanılması ya da izinsiz değiştirilmesi gibi konularda ilgili güvenlik firmasının teminatına yer verilmiştir. Alınan güvenlik önlemleri kapsamında güvenlik sertifikalarına ait bilgiler, işlem anına dair kart bilgilerinin korunması ve takip sistemine dair bilgiler de kullanıcılarla çevrim içi ortamda açıkça paylaşılmıştır.

 UYAP aracılığıyla (güvenlik standartlarına uyma şartıyla) avukatlar, dava açma, harç yatırma, dilekçe verme, icra takibi, temyiz ve yetkileri çerçevesinde dosya açma işlemlerini elektronik ortamda yapabilmektedir. Vatandaşlar ise dosyalarının bulunduğu aşamaları öğrenebilir, örnek kararlara erişebilir, duruşma günlerini internet üzerinden takip edebilir.

Mevzuat İçtihat ve Bilişim Komisyonu’nun görev alanları ve bilgi güvenliği konusunda yürütülen faaliyetlere ilişkin olarak ilgili komisyonda yetkili olan bir avukat ile görüşülerek bilgi temin edilmiştir. Bu bağlamda güncel ve avukatlar için faydalı olan içtihatların derlenip paylaşıldığı, yasa değişikliklerinin takibinin mümkün olduğunca kolaylaştırıldığı ve Kayseri Barosu resmi internet sayfasında da duyurulduğu belirtilmiştir.

Ayrıca Baro tarafından çıkarılan ‘Duruşma Arası’ hukuk dergisinde de güncel içtihat ve önemli yasa değişikliklerine yer verilmektedir. Bunun yanında hukuk alanındaki teknolojik ve sanal değişikliklere; internet, UYAP, e-tebligat, ofis ve bilişim alanındaki güncel sorunlarla ilgili konularda etkili çözümler sunmak amacıyla e-imza,
e-tebligat, e-dosyalama, e-duruşma, e-ödeme, e-makbuz, e-ofis ve
e-güvenlik konularında seminer ve çeşitli bilgilendirme toplantıları düzenlendiği ifade edilmiştir.

Düzenlenen seminerlerde bilişim, internet, teknoloji ve sanal hukuk, UYAP, siber güvenlik ve sosyal medya konularında uzman olan katılımcılar tarafından sunumlar yapılmış; eğitimlere ve seminerlere katılan avukatlarla güncel gelişmeler ve günden güne değişen teknolojik koşullar çerçevesinde planlanan hedefler paylaşılmıştır. Kısacası Baro üyelerinin bilgi teknolojileri, bilgi güvenliği ve hukuk alanındaki elektronik hizmetler konusunda bilgilendirildiğini ve böylece bir anlamda güvenlik kültürünün oluşturulması adına da peyderpey adımlar atıldığını söylemek mümkündür. Ancak şu aşamada ne derece yeterli olduğunu net olarak söylemek mümkün değildir.

**Sonuç**

Tek ve bütünleşmiş bir sistem olarak UYAP, Adalet Bakanlığı ve bağlı kuruluşlar bünyesinde yürütülen faaliyetlerin otomasyon sistemine geçirilmesi, yurttaşın bilgiye erişimini kolaylaştıran sorgulama sistemleri içermesi ve birim bazlı değil de fonksiyon bazlı geliştirilen modüllerle her yeri kapsayan, her yerden ulaşılabilecek şekilde geliştirilmesi, adalet sistemi açısından geliştirilen elektronik hizmetlerin olumlu yanları olarak karşımıza çıkmaktadır.

Diğer yandan bilgi güvenliği konusu, halen tartışmalı bir konudur. UYAP örneğinden hareketle hakim, Cumhuriyet Savcısı, adliye personeli, dosyadaki taraflar ve vekilleri kendilerine verilen yetkiler doğrultusundaki bilgileri görebilmektedir. Ancak bilgi güvenliğinin nasıl sağlanacağı, hangi sistemlerin kullanıldığı detaylı şekilde paylaşılmamış ve güvenlik koruması konusunda tartışmalara neden olmuştur.

Veri güvenliği konusunda gerek mevzuat gerek uygulama pratiklerinin geliştirilmesi ile günümüzde iç ve dış güvenlik sistemleri güçlendirilmiş; yardım masası oluşturulmuş, parola seçimi konusunda düzenlemeler yapılmış, pek çok teknik düzenleme ile güvenlik duvarları geliştirilmiştir.

Nitekim Kayseri Barosu’nun resmi internet sayfasında güvenlikle ilgili düzenlemeler ve yazılımlar hakkında açık şekilde bilgi paylaşılıyor olsa da tam anlamıyla bilgi güvenliği yönetim sistemi oluşturulduğuna dair bilgi paylaşılmadığı görülmektedir. Bilgi güvenliğine dair paylaşımların da kullanıcıların algılayabileceği düzeyde olmadığı, teknik birtakım ifadelerle geçiştirildiği gözlemlenmektedir.

Kurumların internet üzerinden akan verilerinin güvenliğinin sağlanmasında pek çok teknoloji bulunsa da yalnızca teknolojik ürünler ve bunların sunduğu önlemlerle iş süreçlerinde bilgilerin güvenliğini sağlamak imkansızdır. Bu nedenle güvenliği sağlamak için öngörülen ve planlanan yönetsel çerçevelerin belirlenmesinde kurumsal süreçlerin, bilgi toplumu ve ayrıca güvenlik kültürünün önemli bir parçası olduğu unutulmamalıdır.

Bu anlamda iş ve yönetim anlayışı çerçevesinde bilgi güvenliği konusundaki çağa uygun yönetim standartlarının oluşturulması ve bu standartların/bilgilerin her türlü ortamda şeffaf olarak vatandaş-kullanıcı odaklı olacak şekilde açık, net ve basit ifadelerle ortaya konması gerekmektedir. Diğer yandan 2015-2018 Bilgi Toplumu ve Eylem Planı’nda bilgi güvenliği ve kullanıcı güveni konularında doğrudan sorumlu kuruluş olarak ifade edilen Adalet Bakanlığı’nın, diğer ilgili kuruluşlarla işbirliği ve uyum içerisinde olması gerektiği; barolar ve diğer adli birimler ile kullanıcı arasındaki iletişim kanallarının daha şeffaf ve vatandaşa yönelik planlanması gerektiği vurgulanmalıdır.

**KAYNAKÇA**

2015-2018 Bilgi Toplumu ve Stratejisi Eylem Planı, <http://www.bilgitoplumustratejisi.org/tr> (Erişim Tarihi: 20.04.2019).

2016-2019 Ulusal Siber Güvenlik Stratejisi, <https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf> (Erişim Tarihi: 01.09.2019).

Akalp, G. ve Yamankaradeniz, N. (2013). İşletmelerde Güvenlik Kültürünün Oluşumunda Yönetimin Rolü ve Önemi. *Sosyal Güvenlik Dergisi*, Cilt 3, Sayı 2, 96-109.

Balay, R. (2004). Küreselleşme, Bilgi Toplumu ve Eğitim. *Ankara Üniversitesi Eğitim Fakültesi Dergisi*, Cilt 37, Sayı 2, 61-82.

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi,* Cilt 9, Sayı 3, 165-174.

Cox S. and Flin, R. (1998). Safety Culture: Philosopher’s Stone or Man of Straw?. *Work and Stress*, 12(3), 189-201.

Çukurçayır, M. A. ve Çelebi, E. (2009). Bilgi Toplumu ve e-Devletleşme Sürecinde Türkiye. *ZKÜ Sosyal Bilimler Dergisi*, Cilt 5, Sayı 9, 59-82.

Dursun, S. (2011). *Güvenlik Kültürünün Güvenlik Performansı Üzerine Etkisine Yönelik Bir Uygulama*. Yayınlanmamış doktora tezi, Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Bursa.

Efendioğlu, A. ve Sezgin, E. (2007). E-devlet Uygulamalarında Bilgi ve Paylaşım Güvenliği. *Ç. Ü. Sosyal Bilimler Enstitüsü Dergisi,* Cilt 16, Sayı 2, 219-236.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı (Uzmanlık Tezi), Yayın No: 2919.

International Telecommunication Union (ITU), (2011), ‘‘National Cybersecurity Strategy Guide’’,<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>, (Erişim Tarihi: 01.05.2019).

Karabulut, B. (2015). Bilgi Toplumu Çağında Dijital Yerliler, Göçmenler ve Melezler. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Sayı 21, 11-23.

Kayseri Barosu Resmi İnternet Sayfası, <http://www.kayseribarosu.org.tr/Detay.aspx?ID=9009>, (Erişim Tarihi: 01.05.2019).

Kırışık, F. (2016). *Yönetsel Dönüşüm Sürecinde Şeffaflık ve Bilgi Edinme Hakkı.* Ankara: Ekin Yayınları.

Kişisel Verilerin Korunması Kanunu, <https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf>, (Erişim Tarihi: 01.05.2019).

Meder, M. (2001). Bilgi Toplumu ve Toplumsal Değişim. *Pamukkale Üniversitesi Eğitim Fakültesi Dergisi*, Sayı 9: 72-81.

Özkan, T. ve Lajunen, T. (2003). Güvenlik Kültürü ve İklimi. *Pivolka*, Yıl: 2 Sayı: 10, 3-4.

Taş, İ. E. ve Uçacak, K. (2018, Ocak). Türk Kamu Yönetiminde Bürokratik İşlemlerin Azaltılmasında UYAP Uygulamasının Önemi, *Sosyal Bilimler Dergisi*, Yıl:5 Sayı: 19, 492-513.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 11 (1), 132-137.

Türkiye’de e-Devlet Hizmetleri Hakkında; <http://afyonluoglu.org/e-devlet/tr-edevlet/#ADALET>, (Erişim Tarihi: 20.04.2019).

Yılmaz, B. (1998). Bilgi Toplumu: Eleştirel Bir Yaklaşım. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, 15 (1), 147-158.

UHAP ve ilgili internet adresleri;

<http://www.edevlet.gov.tr/wp-content/uploads/2017/08/03.08.2017-Koordinasyon-e-Devlet-Adalet-Bakanligi.pdf>, (Erişim Tarihi: 20.04.2019).

<https://www.uhap.com.tr/#/bilgi/yasaluyari>, (Erişim Tarihi: 01.05.2019).

<https://www.uhap.com.tr/#/bilgi/yasaluyari>, (Erişim Tarihi: 01.05.2019).

<https://www.uhap.com.tr/#/bilgi/tanitim>, (Erişim Tarihi: 01.05.2019).

BüroTek hakkında;

<https://www.burotek.av.tr/#/bilgi/hakkimizda>, (Erişim Tarihi: 01.05.2019).

<https://www.burotek.av.tr/#/bilgi/tanitim>, (Erişim Tarihi: 01.05.2019).

İcraTek hakkında;

<https://www.icratek.com.tr/hakkimizda>, (Erişim Tarihi: 01.05.2019).

KararTek hakkında;

<https://www.karartek.com.tr/#/kullanici/hakkimizda>, (Erişim Tarihi: 01.05.2019).

<https://www.karartek.com.tr/#/kullanici/tanitim>, (Erişim Tarihi: 01.05.2019).

1. *Prof. Dr., Nuh Naci Yazgan Üniversitesi İktisadi ve İdari Bilimler Fakültesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, akaya@nny.edu.tr* [↑](#footnote-ref-1)
2. \*\* *Dr. Öğr. Üyesi, Nuh Naci Yazgan Üniversitesi İktisadi ve İdari Bilimler Fakültesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, dkabakusak@nny.edu.tr* [↑](#footnote-ref-2)