# Avrupa Birliği (AB) Bilgi Güvenliği Politikaları

## *European Union (EU) Information Security Policies*

**Türkay Henkoğlu[*] ve Bülent Yılmaz[**]**

***Öz***

*Avrupa ekonomisinin gelişimi, bilgi ve iletişim teknolojilerinin kullanımı ve bilgi toplumu dönüşüm süreci ile yakın ilişkilidir. Fakat bilgi ve iletişim teknolojilerinin kullanım riskleri, kullanıcıların teknolojinin kullanımına olan güvenini azaltmakta ve ekonominin canlanmasına engel olmaktadır. Bu nedenle; özellikle son 20 yıl içinde AB bilgi politikaları içinde bilgi güvenliğine büyük önem verilmiş ve birçok direktif ve tavsiye kararı yayımlanmıştır.*

*Bu çalışmada; AB bilgi güvenliği politikalarını şekillendiren unsurların, politikaların amaçlarının, nasıl uygulandığının ve etkilerinin değerlendirilmesi amaçlanmıştır. Bilgi güvenliği politikalarının kapsamı ve önemi, çok yönlü ve kapsamlı bir kuramsal bilgi güvenliği modeli olan McCumber bilgi güvenliği modeli üzerinde irdelenmiştir. Bilgi güvenliği ile ilgili olarak yayımlanmış AB direktifleri, AB komisyonu tarafından hazırlanan sözleşmeler, bilgi güvenliği politikalarının geliştirilmesinde etkili AB kuruluşları ve mevcut literatür incelenerek; AB bilgi politikaları içinde bilgi güvenliği konusunun yeri ve önemine dikkat çekilmiştir. Çalışma sonucunda; AB bilgi güvenliği politikalarının, ekonomi ve bilgi toplumu politikalarının önemli bir parçası olarak görüldüğü ve veri koruma direktifleri üzerinde güncelleme çalışmalarının 1995 yılından itibaren kesintisiz olarak yapıldığı anlaşılmıştır. Bu politikaların günün gereksinimlerine yanıt verebilecek nitelikte olduğu belirlenmiştir.*

***Anahtar Sözcükler:*** *bilgi güvenliği politikaları; kişisel verilerin korunması; AB veri güvenliği; siber suçlar; McCumber Modeli; ENISA; dijital ajanda*

***Abstract***

*The development of the European economy is strongly related to the use of information and communication technologies (ICT) and the transformation process of information society. However, because of the risks of ICT, people are anxious about using technology, which in turn retards the economic growth of countries all around the world. Therefore, especially in the last twenty years, information security issues have begun to gain importance in European Community (EC) information policies, and many suggestions have been made related to these issues.*

[*] Adli Bilişim Uzmanı, Hacettepe Üniversitesi. e-posta: henkoglu@hacettepe.edu.tr

[**] Prof. Dr., Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü. e-posta: byilmaz@hacettepe.edu.tr

*The purpose of this study is to examine the main issues in EC information policies, the aims and the effects of these policies, and how they are implemented. The importance and scope of these policies were examined based on the McCumber information security model, which is a comprehensive and multidimensional information security model. In order to draw attention to the importance of information security issues in EC policies, a wide range of information sources are reviewed, including EC directives and agreements related to information security, the EC organizations responsible for making information security policies, and the literature concerning these issues. The findings of the study show that EC information security policies are seen as a vital part of economy and information society policies. In addition, the study shows that data protection directives have been updated regularly since 1995, which makes them suitable for the needs of today's world.*

***Keywords:*** *information security policies; protection of personal data; EC information security; cybercrimes; McCumber Model; ENISA; digital agenda*

## Giriş

Bilgi güvenliğinin sağlanması; tüm dünyada yaşamın bir parçası haline gelen internet kullanımının yaygınlaşması, siber suç oranlarındaki artış, iş dünyası ve kişisel bilgi gizliliğini tehdit eden bilgi teknolojilerine bağlı unsurların etkisinin artması, yasal sorumlulukların artması, tehditlerin çoğalması ve daha karmaşık bir yapıya dönüşmesi nedeniyle zorunlu hale gelmiştir. Kişisel bilgisayarların yanı sıra merkezi veri depolama alanlarında korunmaya ihtiyaç duyulan bilgi; kullanıcıya ait kişisel bilgiler, bilgi merkezinin ya da kurum ve kuruluşların kendi idari yapısı ve işleyişi ile ilgili bilgiler ve erişime açılan bilgi kaynakları gibi çeşitliliğe sahip olabilir. Fakat genel anlamda bilişim sistemleri üzerinde bulunan tüm bilgiler, belirli sınıflandırma ve yetkilendirme işlemi sonrasında, yaygın olarak bilinen bilgi güvenliği önlemleri ile korunurlar. İş dünyası, bilgi merkezleri ve kişisel bilgisayarlara ilişkin tehditler; maddi kayıpların yanı sıra, zaman ve itibar gibi yeri doldurulamayacak kayıplara da neden olabilmektedir. Dünyanın önde gelen bilgi teknolojileri ve yazılım şirketlerinden biri olan Hewlett-Packard'ın yapmış olduğu Siber Güvenlik Riskleri Raporu'na göre; 2011 yılında yapılan siber saldırı sayısının iki kat (%56) arttığı ve web uygulamalarının %86'sının korumasız olduğu görülmektedir (HP, 2011). Dünyanın en büyük bilgi güvenliği yazılım üreticilerinden Symantec'in 2011 yılı tehdit raporu da; tehdit unsuru olarak zararlı kodların üretiminde 2010 yılına oranla %41 ve saldırı oranında %81 artış olduğunu göstermektedir (Symantec, 2012). Bu nedenle, uluslararası ve büyük boyutta zarara neden olan tehditlerle mücadele edebilmek için, uluslararası işbirliğine duyulan ihtiyaç ve verilen önem artmaktadır.

Bilgi ve iletişim teknolojilerinin kullanımından kaynaklanan riskler katlanarak artsa da, günümüzde bilgi ve iletişim teknolojilerinden yoksun olarak yaşamak hemen hemen olanaksız hale gelmiştir. Bu durumda izlenecek tek yol, bilgi güvenliği konusunda alınabilecek önlemleri en üst seviyeye çıkarmak ve kullanıcı bilinçliliğini sağlamaktır. Bilgi güvenliği konusunun birçok boyutu (teknik, hukuki vd.) bulunmaktadır. Ayrıca %100 güvenliğin sağlanması ve sürekli olarak üretilen yeni tehditlerin tamamının önceden tahmin edilerek önüne geçilmesi teknik açıdan mümkün değildir. Fakat yeni tehditlere karşı gösterilen tepki süresi azaltılarak, meydana gelebilecek büyük kayıpların önüne geçilebilmektedir. Bilgi güvenliği, çok geniş ve disiplinler arası boyutta ele alınması gereken bir konudur. Bu nedenle; bilgi politikasının alt unsuru olarak bilgi güvenliği politikalarının da teknik ve hukuki boyutlarıyla birlikte önceden geliştirilmesi ve uygulanabilir hale getirilmesi gerekmektedir. Bilgi güvenliği politikalarının oluşturulması, hassas ve kişisel verilerin de işlendiği bilgi merkezleri ve kurumlar için büyük

önem taşımaktadır[1]. Bilgi güvenliğinin sağlanması konusunda uygulanacak eylem planı ve teknik önlemleri içeren politikalar, meydana gelebilecek zararları önceden öngörmeye, önlem almaya ve tehditleri bertaraf etmeye yönelik olarak yapılırken; yasal düzenlemeleri içeren politikalar ise; caydırıcılık etkisi yaratabilmeye, meydana gelebilecek zararın boyutunu en düşük seviyede tutabilmeye ve en kısa sürede zararı gidermeye yönelik olarak yapılmaktadır. Bilgi güvenliği ile ilgili yasal düzenlemeler bilgi politikasının unsuru oldukları gibi; belirlenen politikalarının uygulanmasında da önemli bir rol oynamaktadır. AB'de bilgi güvenliği ile ilgili politikaların amacı ve uygulama yöntemi, bilgi merkezlerinde ya da kurum ve kuruluşlarda sorumluluğun paylaşımı ve risklerin azaltılması için geliştirilecek politikaların oluşturulması açısından önem taşımaktadır. Bu çalışmada, AB bilgi güvenliği politikaları, hukuki ve teknik boyutlarıyla, örnek kuramsal model çerçevesinde detaylı olarak irdelenerek; bilgi güvenliği politikalarının çok boyutluluğuna, konunun önemini vurgulayan çalışmalara ve bilgi güvenliği politikaları geliştirilirken atılması gereken adımlara dikkat çekilmesi amaçlanmaktadır.

## Bilgi Güvenliği

### *Bilgi Güvenliğinin Tanımı ve Önceliği*

Bilgi güvenliği; "güvenlik" kavramı içinde yer alan unsurlardan biridir. Genel anlamda güvenlik; fiziksel güvenlik, personel güvenliği, iletişim güvenliği, ağ güvenliği ve bilgi güvenliğini içeren geniş bir çerçeveyi oluşturmaktadır. Bilgi güvenliği 1990'lı yıllara kadar olan süreçte yazılı-basılı ortamlarda yer bulan bilgilerin daha çok fiziksel anlamda güvenliğinin sağlanmasını ifade eden bir olguydu. Bilgi ve iletişim teknolojilerinin gelişimine bağlı olarak elektronik ortamda üretilen ve muhafaza edilen bilginin miktarındaki artışla birlikte; bilgi yönetimi ve bilgi güvenliğinin sağlanması yeni bir boyuta taşındı. 1990'lı yılların başında bilgi yönetimi ve güvenliğinin sağlanması elektronik ortamda daha karmaşık hale gelmeye başladı. Fakat asıl büyük dönüşüm; "internet çağı" olarak da adlandırılan 1990'lı yılların sonlarında, bilgisayar ağlarının gelişimine bağlı olarak bilgi transferindeki artış ile gerçekleşmiş ve bu gelişmeler bilgi güvenliğinin tanımının da değişmesine neden olmuştur. Bu çerçevede McCumber'in "Bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa edilmesi, bozulması, değiştirilmesine veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma" şeklinde yapmış olduğu tanım, en kapsamlı ve bugünün koşullarını içine alan tanımlardan biridir (McCumber, 2005, s. xxiii).

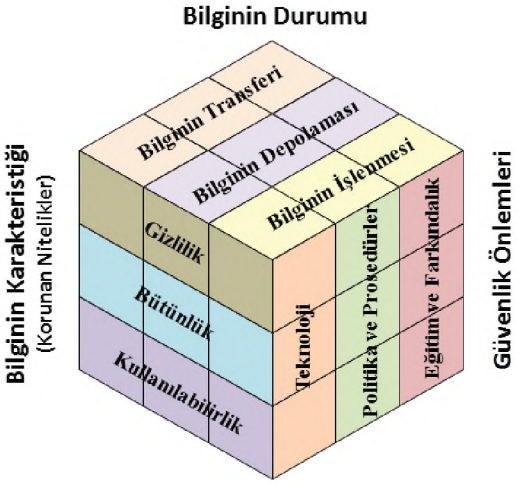
Bilgi güvenliği politikalarının oluşturulması ve bilgi teknolojileri kullanıcılarının bilgi güvenliğinin sağlanması hakkında bilinçlendirilmesi, bilgi güvenliği konusunun temel önceliğini oluşturmaktadır. Bilgi güvenliği politikasının oluşturulması ve bilinçlenme sürecinde, bilgiyi yöneten ve kullanan açısından bakıldığında iki farklı fakat birbiri ile ilişkili grubun rol aldığı görülmektedir. Elektronik bilgilerin miktar ve oranındaki artış, bilgi yönetiminin kullanıcı ile bilgi kaynağını buluşturmanın ya da başka bir ifade ile kullanıcının bilgiye erişimini sağlamanın ötesinde; kullanıcının bilgiye güvenli olarak erişiminin sağlanması sorumluluğunu da almasına neden olmuştur. Bilginin sahibi ve bilgiyi kullanan kadar, bilgi ve bilgi sistemlerini yönetenler de bilgi güvenliğinin sağlanmasından sorumludurlar. Bilgi ile ilişkili bu grupların içindeki en zayıf nokta ise "bilgi güvenliğinin seviyesi" olarak kabul edilmektedir. Bilgi güvenliğinin temel amacı; doğru kişinin en kısa sürede doğru bilgi ile buluşmasını sağlamaktır. Bilginin tanımı üzerinden bir yaklaşımda bulunulduğunda; insan (bilen) ile nesne (bilinen) arasında kurulan bağın güvenliğinin sağlanması, bilgi güvenliğinin temel amacı olarak ifade edilebilir.

[1] Bilgi güvenliğinin bilgi merkezleri açısından önemi ve hukuki sorumluluklara ilişkin ayrıntılı bilgi için bkz. (Henkoğlu ve Uçak, 2012).

Günlük yaşamda bilgi ve iletişim teknolojilerinin yaygın olarak kullanıldığı ve en fazla bilgi güvenliği ihlâlinin bulunduğu alanlar; kişisel bilgilerin yoğun olarak kullanıldığı bankacılık işlemleri, e-ticaret, hastane bilgi sistemi, eğitim sistemleri ve büyük veri depolama alanlarıdır. Bu nedenle; bilgi güvenliği politikaları oluşturulurken öncelikle bu alanlarda bilgi ve iletişim teknolojilerinin güvenli kullanımı ve alınacak önlemlerin uluslararası boyutta standartlaştırılması hedeflenmektedir. Veri koruma, kişisel bilgilerin gizliliği ve siber saldırılara ilişkin bilgi güvenliği politikalarının, ulusal ve uluslararası boyutta daha fazla üzerinde durulan konular olduğu görülmektedir. Bu alanlarda uygulanan teknik yöntemler her geçen gün güncellenmekte ve daha karmaşık hale gelmektedir. Fakat bu takibin sürekliliği ve yeterliliğinin sağlanabilmesi için; uygulanabilir bir bilgi güvenliği politikası ve kullanıcı/insan faktörünün de süreçten ayrı tutulmaması gerekmektedir.

### *McCumber Bilgi Güvenliği Modeli*

Bilgi güvenliği politikalarının oluşturulması ve politikaların uygulamaya dönüşmesi aşamasında, tüm yönleri ile birlikte değerlendirme yapılmadığı müddetçe, bilgi güvenliğinin sağlanmasında başarıya ulaşılması söz konusu değildir. Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin bilgi güvenliği içindeki rolü kadar, bu sürece etki eden insan faktörü ve uygulanan bilgi güvenliği politikalarının da büyük önemi bulunmaktadır. Şekil 1'de yer alan McCumber'in geliştirmiş olduğu model, bilgi güvenliği konusunda ulusal ya da uluslararası boyutta politika geliştirmek ve bilgi güvenliğini tüm yönleri ile uygulayabilmek için temel olabilecek en uygun bilgi güvenliği modelidir. Bilgi güvenliğinin unsurlarının farklı boyutlarını gösteren ve aynı zamanda kendi içinde gruplandıran McCumber'in bilgi güvenliği modeli, 1991 yılından bu yana geçerliliğini korumuş ve daha sonra geliştirilen modellere de temel olmuştur. Bilgi güvenliğini teknik boyutta en katı kurallarla uygulayan ve standartları belirleyen (CISCO gibi) kuruluşlar da temel bilgi güvenliği kavramları içerisinde McCumber modeline yer vermektedirler (CiscoLearning, 2009). AB bilgi güvenliği politikalarının değerlendirilmesinde çok boyutlu ve detaylı bakış açısı sunan McCumber modeli, bilgi merkezleri ve kurumlar için bilgi güvenliği politikası geliştirilirken de dikkate alınması gereken bir kuramsal modeldir. Model üzerinde bilgi güvenliğinin sağlanması ile ilgili olarak; bilginin üç farklı yüzü (karakteristiği/güvenlik servisleri, durumu ve güvenlik önlemleri) gruplandırılarak gösterilmektedir.




**(Şekil 1)**: McCumber Bilgi Güvenliği Modeli (McCumber, 1991).

*Kritik Bilgi Karakteristiği, Güvenlik Servisleri, Korunacak Nitelikler*

McCumber güvenliğin bileşenlerini tanımlarken; üç ana unsur üzerinden hareket etmektedir. Bunlar; gizlilik, bütünlük ve kullanılabilirliktir. Bu üç unsur, McCumber'in 1991 yılında geliştirdiği bilgi güvenliği modelinde, "bilginin karakteristiği" grubu altında da yer almaktadır. Sözü edilen üç unsura, daha sonra güvenlik politikaları geliştiren araştırmacılar ve güvenlik analizcileri tarafından yeni unsurlar (inkâr edememe gibi) eklenmiştir. Fakat McCumber, 1991 yılında geliştirmiş olduğu modelin 2005 yılında değerlendirmesini yaparken; ayrıca yeni unsurların eklenmesine ihtiyaç olmadığını ve yeni unsurlar olarak gösterilen "inkâr edememe" ve "kimlik doğrulama" unsurlarının bilgi bütünlüğünün bir yüzü olduğunu ifade etmiştir (McCumber, 2005). Bilgi güvenliği konusuna McCumber'in bakış açısıyla bakıldığında; McCumber modelinin hâlâ güncel ve uygulanabilir bir model olduğu söylenebilir. McCumber modelinde "bilginin karakteristiği" grubu altında yer alan gizlilik, bütünlük ve kullanılabilirlik unsurları; bilgi güvenliğinde en fazla üzerinde çalışılan unsurlardır. Solomon'un gizlilik, bütünlük ve kullanılabilirlik üçgeninde de (CIA Triad) ifade edildiği gibi; bilgi güvenliği bu üç unsurun birleşimi olarak kabul edilmektedir (Solomon ve Chapple, 2005). McCumber'in üzerinde ısrarcı olduğu ve McCumber'in modelini esas alan yeni modellerin güvenlik servisi içerisinde yer alan unsurları şunlardır;

- *Gizlilik:* Bilginin gizliliği, bir bilgiye erişmesi uygun görülen kişiler tarafından erişimin sağlanabilmesini ifade eder. Bilgi merkezlerinde ya da büyük verinin bulunduğu sistemler üzerindeki bazı bilgiler herkes tarafından ulaşıma açık olabildiği gibi, bazı bilgiler (örneğin veri tabanları) yapılan sözleşmeler çerçevesinde sadece belirli bir grup üyenin erişimine açıktır. Yetkilendirme, şifre ile erişim ve veri kriptolama işlemleri; bilgi gizliliğinin sağlanması için kullanılan başlıca yöntemlerdir. McCumber modelinde bilgi gizliliğinin sağlanması amacıyla, bilginin transferi ve depolanması süreçlerinde kripto kullanımı önerilmektedir (McCumber, 2005). Elektronik ortamdaki bilginin gizlilik etiketi ve bilgi güvenliği politikası kapsamında belirlenmiş "bilmesi gereken ilkesi[2]", bilgi gizliliğinin sağlanmasında dikkat edilen öncelikli unsurlardır (WBO, 2003). Bilgiye erişim esnasındaki gizliliğin, kişisel bilgilerin ve bireysel hakların korunması; bilginin gizliliği kapsamındaki başlıca konulardır.
- *Bütünlük:* Bilgi bütünlüğü, bilgi merkezlerinde ya da herhangi bir elektronik ortamda yer alan bilgi kaynaklarının yayıncı tarafından ulaştırılan orijinal halinin, yetkisiz kişiler tarafından değiştirilmemiş olması anlamını taşımaktadır. Bilgi bütünlüğü kasıtlı olarak bozulabileceği gibi, bilgi sistemlerindeki bazı eksiklikler nedeniyle kullanıcılar tarafından bilmeden ve istemeden de bozulabilir. Bilgi bütünlüğün korunması, aynı zamanda bilginin değerinin de korunması anlamını taşımaktadır. Bu nedenle bilgi güvenliği yatırımları içinde en fazla pay tahsis edilen alanlardan biri bilgi bütünlüğünün korunmasıdır. McCumber'e göre bilginin bütünlüğü; kripto çözümleri, karşılaştırmalı analiz, inkâr edememe, kimlik doğrulama ve erişim kontrolü süreçlerini de içine almaktadır (McCumber, 2005). Kimlik doğrulama ve erişim kontrolü ile ilgili yetkisiz erişimi tespit etme ve engelleme sürecinde; kimlik tanımlama, kimlik doğrulama ve yetkilendirme yöntemleri (kullanıcı adı, şifre, parmak izi, elektronik güvenlik sertifikaları, elektronik kart vd.) uygulanarak, kullanıcının önceden yetkilendirilmiş kaynaklara ihtiyaç duyabileceği en düşük yetki ile erişimi sağlanır.
- *Erişilebilirlik/Kullanılabilirlik/Süreklilik:* Bilginin kullanılabilirliği, kullanıcının ihtiyacı olan bilgiye yetki alanı sınırları içinde ve istediği anda ulaşabilmesidir. Başka bir ifade ile bilginin erişim yetkisi olan kişiler tarafından erişilebilmesi ve kullanılabilmesidir. Yer sağlayıcılar ve bilgi profesyonelleri açısından erişilebilirlik konusu mevcut bilgi sistemlerinin faal olmasının ötesinde birtakım sorumlulukları da içermektedir. Veri depolama

[2] Bilmesi Gereken İlkesi: Bir organizasyon/kurum içinde, personelin sadece görev ve sorumluluk alanı ile ilgili bilgiye erişiminin sağlanması, ihtiyacı olmayan bilgiye erişiminin engellenmesidir (WBO, 2003).

alanlarının her an güncel bilgi ile kullanıcıyı buluşturması noktasında üstlenilen kritik sorumluluk; aktif olarak hizmet veren cihazların altyapı yedekliliği ve yeterliliğinin yanı sıra veri yedekliliğinin de düzenli olarak yapılması ve gerektiğinde en kısa sürede hizmete sunulmasını zorunlu kılmaktadır. Erişilebilirlik ile ilgili olarak en fazla yaşanan sorun, uygulanan güvenlik önlemlerinin bilgiye erişimi gereğinden fazla zorlaştırmasıdır. Güvenlik önlemi ile erişilebilirlik dengesinin doğru biçimde kurulmaması, bilgi kaynaklarına erişimi kısıtlayabilmektedir.

*Bilginin Durumu*

McCumber'in modelinde bilginin durumu; bilginin işlenmesi, depolanması ve transferi şeklinde üç sınıf altında gösterilmiştir. Herhangi bir sistem üzerinde ve herhangi bir anda, bilgi bu üç durumdan bir veya birkaçının tanım alanına girecek şekilde bulunmaktadır. Bir bilginin bir yerden başka bir yere gönderilmesi esnasında; bilginin hem transfer edilen hem de asıl kopyası disk üzerinde olduğu için, depolanma durumunda olduğu söylenebilir. Bilginin durumu, değerinin belirlenmesi açısından önemlidir. Bilgi güvenliği modelinde bilgiye bir "değer" olarak yaklaşılmakta ve risk yönetimi esnasında buna bağlı olarak bilgi güvenliğinin sağlanması öngörülmektedir.

Yaşayan, büyüyen, diğer bilgilerle bir araya gelerek çoğalan ve değişen yapısı nedeniyle; bilginin, durumunun da dikkate alındığı güvenlik önlemlerinin uygulanması gerekmektedir. Bilgi güvenliğinin sağlanması amacıyla kullanılacak teknik yöntem belirlenirken; öncelikli olarak bilginin hangi durumda olduğuna bakılmaktadır. Örneğin transfer halinde ya da depolanmakta olan bir bilginin güvenliğinin sağlanabilmesi için en uygun yöntem, Roma İmparatorluğu döneminden günümüze kadar ulaşan yöntemlerden biri olan kripto kullanımıdır (McCumber, 2005). McCumber'in modelinden esinlenerek oluşturulan bazı yeni modellerde, bilginin durumunun dört sınıfta toplandığı ve "zaman" unsurunun da eklendiği görülmektedir. Zaman unsuru; bilginin durumundaki değişmenin başladığı zamanı ifade etmek için kullanılmaktadır (Maconachy, Schou, Ragsdale ve Welch, 2001).

*Güvenlik Önlemleri*

McCumber modelinde güvenlik önlemleri; politika ve prosedürler, teknik önlemler ve insan faktörü unsurlarını içermektedir. Güvenlik önlemleri, model üzerinde birleşen noktalarda tamamlayıcı unsur olarak uygulanabilecek yöntemlerdir. Örneğin; bilginin transferi esnasındaki güvenliğin sağlanabilmesi için kullanılacak önlem (bilginin kriptolanması gibi), güvenlik önlemi boyutuyla bilgi güvenliğini tamamlamaktadır. Bilgi güvenliği önlemleri, bilgi güvenliğinin diğer iki boyutunun (bilginin karakteristiği ve bilginin durumu) birleşimi ile elde edilen sonuca üçüncü boyut olarak eklenmek suretiyle, sürecin eksiksiz olarak tamamlanmasına katkı sağlamaktadır. Modelde yer alan üç boyuttan birinin uygulanmadığı alanlar, güvenlik açığını oluşturan noktalardır.

Güvenlik önlemlerinin uygulamadaki öncelikli unsuru teknik unsurdur. Güvenlik önlemlerinin teknik unsuru içerisinde, her geçen gün tehditlere bağlı olarak sayısı artan birçok önlem (güvenlik duvarı vd.) yer almaktadır. Teknik güvenlik önlemleri; bilginin kritik karakteristik özelliğini (gizliliği, bütünlüğü ve kullanılabilirliğini) korumak amacıyla, bilginin durumuna uygun olarak kullanılabilecek yazılım ya da donanım ile ilgili önlemlerdir. Fakat tüm bu önlemler içinde bilinen en eski ve aynı zamanda en güncel ve öncelikli yöntem bilginin kriptolanmasıdır. Güvenlik politikası unsuru ise; korunan sistem ve bilginin değerine ve kullanıldığı alana bağlı olarak farklılık göstermektedir. Yasal düzenlemeleri de kapsayan ulusal bilgi güvenliği politikalarından en alt seviyede detaylı kullanıcı şifre politikasına kadar tüm planlamalar bu kapsamda değerlendirilebilir. Doğru politikaların oluşturulması, bilgi

güvenliğinin sağlanması ile yakın ilişkilidir. Fakat güvenlik önlemleri unsurlarından olan insan faktörünün dikkate alınmaması halinde, diğer unsurların uygulanması yetersiz kalabilmektedir.

***Bilgi Güvenliği Politikalarını Yönlendiren Başlıca Risk ve Tehditler***

Ulusal ve uluslararası çapta bilgi güvenliği politikaları; korunması her geçen gün daha maliyetli hale gelen bilgi, bilgi sistemleri ve kullanıcılarını risk ve tehditlere karşı maliyet-etkin olarak korumayı hedeflemektedir. AB bilgi güvenliği politikalarının oluşturulmasında da, risk ve tehditleri esas alan bir metot izlenmektedir. Bilgi ve iletişim sistemlerinin kullanımına bağlı olarak yapılan analizler sonrasında; teknolojiye bağlı birçok tehdit (zararlı kodlar, gizlilik ihlalleri, telif hakları ihlali, servis ve yer sağlayıcı güvenilirliği vd.) belirlenmekte ve belirlenen politikalar yasalaştırılarak uygulamaya konulmaktadır (Feiler, 2011). Bilgi güvenliği politikalarının yapılması aşamasında gündemi belirleyen ana risk ve tehditler, genel olarak üç başlık altında sınıflandırılabilir. Bu risk ve tehditler;

- Bilişim Sistemine girme ve bilgiye yetkisiz erişim,
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme ve
- Kimlik hırsızlığı ve kişisel verilerin kötüye kullanımıdır.

Bu üç başlık altında sınıflandırılan risk ve tehditlerle mücadele edilirken; uygulanan teknik ve belirlenen amaca bağlı olarak bazı alanlar ve yöntemler ön plana çıkmaktadır. Bunlar; zararlı kodlarla mücadele, veri gizliliğinin sağlanması ve web tabanlı uygulamalarda güvenliğin sağlanmasıdır.

*Zararlı Kodlar ve Siber Suçlarla Mücadele*

Veri depolama alanlarını hizmet veremez duruma getirmek ya da verilere zarar vermek amacıyla yapılan saldırı ve girişimler, büyük oranda zararlı kodlar ile yapılmaktadır. Saldırgan için daha az riskli ve daha az maliyetli olması, zararlı kodlar kullanmak suretiyle gerçekleştirilen saldırıların daha yaygın olmasının öncelikli nedenidir. Veri depolama alanlarının ve kişisel verilerin gizliliğinin zararlı kodlardan etkili ve sürekli olarak korunabilmesi için; ulusal ve uluslararası boyutta, anlaşılır ve uygulanabilir yazılı bilgi güvenliği politikalarının oluşturulması gerekmektedir. Özellikle uluslararası hukukun konusuna giren bilişim suçlarının, bu tür suçlarla mücadelede işbirliği yapmayan ülkeler üzerinden (proxy sunucular aracılığıyla) gerçekleştirilmesi, hukuki boyutta zararlı kodlarla mücadeleye darbe vurmaktadır.

Zararlı kodlarla aktif mücadele, genel bilgi güvenliği önlemlerinin alınması, güvenlik duvarı, virüs önleyiciler ve casus yazılım önleyiciler ile teknik olarak yapılmaktadır. Zararlı kodların dağıtımını yapan ve bu yolla itibar ya da maddi güç kazanmak isteyen kişilerle mümkün olabilen her noktada hukuki mücadelenin de yapılması gerekmektedir. Teknik detaylara değinmeden zararlı kodlarla mücadele için belirlenecek bilgi güvenliği politikaları başlıklar halinde özetlenecek olursa; bir eylem planının oluşturulması, kullanıcıların nasıl hareket edecekleri (teknik ve hukuki anlamda) konusunda bilinçlendirilmesi, tüm zararlı kodlara karşı teknik önlemlerin alınması ve güncellemelerin takip edilmesi öncelikli ve mutlaka uygulanması gereken adımlar olarak sıralanabilir.

*Veri Gizliliğinin Sağlanması ve Önemi*

95/46/EC sayılı AB veri koruma direktifinde kişisel veri; kimliği belirli ya da belirlenebilir gerçek kişi ile ilgili her türlü veri olarak tanımlanmıştır (European Council, 1995). Kişisel veri; kişinin özel, iş hayatı ya da toplumsal hayatı ile bağlantısı olan ya da olmayan, kişi ile ilgili tüm bilgilerdir. Kullanıcı gizliliğine konu olan başlıca bilgiler arasında; telefon bilgisi, kimlik bilgileri, adres bilgileri, e-posta adresi, fotoğraf, vatandaşlık numarası, kurum/öğrenci kimlik numarası, çevrimiçi kullanıcı hesapları, sosyal paylaşım siteleri üzerinden yapılan gönderiler, banka bilgileri ile sağlık kayıtları bulunmaktadır (European Commission, 2012c).

Son yıllarda özellikle ticari amaçlı kişisel bilgilere (kimlik bilgileri, kredi kartı bilgileri vd.) ilişkin siber saldırıların artışı, bulut bilişim gibi yeni bilgi iletişim ve paylaşım hizmetlerinin yaygınlaşması ve bilgi iletişim teknolojilerindeki hızlı gelişime bağlı olarak güvenlik risklerinin artması; bilgi güvenliğinin sağlanması çerçevesinde kişisel verilerin korunması konusunu en çok tartışılan konular arasına taşımıştır (King ve Raja, 2012). Kişisel verilerin korunması, bilgi güvenliği kapsamında verilerin korunmasının ötesinde; bireylerin kişisel hak ve özgürlüğünü de korumayı hedefleyen bir güvenlik ağı içinde yer almaktadır.

Kamu kurum ve kuruluşları bilgi sistemleri üzerinden verdikleri hizmetlerde genellikle kimlik doğrulama amacıyla ya da takibinin sürekliliği gerektirdiği (meslek kuruluşları ve sağlık bilgileri gibi) alanlarda kişisel bilgilere ihtiyaç duymaktadırlar. Arama motorları ve e-ticaret şirketleri gibi özel kuruluşlar ise; hizmet kalitesini arttırmak amacıyla, kullanıcının bilgi sistemleri ile etkileşimi aşamasında kişisel bilgileri toplamaktadırlar. Bunun dışında; kimlik bilgileri ya da istihbarat amaçlı bilgileri elde etmek için kişisel bilgileri hedef alan kötü niyetli girişimler de bulunmaktadır. Elde edilme yöntem ve amaçlarında farklılık bulunan bu risk alanlarında kişisel verilerin etkin olarak korunabilmesi için; kişisel bilgileri toplama, kaydetme, kullanma ve açığa vurma konusunda kısıtlamalar getiren bilgi politikalarının oluşturulması gerekmektedir. Bu konuda örnek düzenlemelerden biri olan 95/46/EC isimli AB direktifinde; verinin nasıl işlendiği, nasıl saklandığı ve kim tarafından erişildiği konusunda veri sahibinin bilgilendirilmek zorunda olduğu açık olarak ifade edilmekte ve özünde bireyin korunması hedeflenmektedir. Bu düzenleme Winter'in yapmış olduğu gizlilik tanımıyla da örtüşmektedir. Winter'a göre gizlilik; kullanıcıların kendilerine ait kişisel bilgilerin ne zaman, nasıl ve ne kadarının başkalarının erişimine açılacağına karar vermeleridir (Winter, 1997).

*Web Tabanlı Uygulamalarda Güvenliğin Sağlanması*

Bilişim teknolojileri kullanılarak verilen hizmetler, günümüzde büyük ölçüde web tabanlı uygulamalar aracılığıyla sunulmaktadır. Özellikle 2006 yılı sonrası web 2.0 ve bulut bilişim alanındaki gelişmelere bağlı olarak, yeni bilgi güvenliği sorunları da gündeme gelmiştir. İnternet üzerinden yapılan saldırıların büyük bölümü, sunucu bilgisayarların işletim sisteminin ve web tabanlı uygulamaların açıkları kullanılarak yapılmaktadır (Belson, Möller ve Bergqvist, 2012). Sistemleri üzerinde büyük veri yığınları bulunduran birçok yer sağlayıcı, sunmuş olduğu bilgi kaynaklarına erişimi web sayfası aracılığıyla sağlamaktadır. Yer sağlayıcıların, web sayfası üzerinden erişime açılan bilgi kaynakları ve kullanılan web tabanlı uygulamalarla ilgili sorumlulukları bulunmaktadır. Bununla beraber, yeni web uygulamaları ile meydana gelen bilgi güvenliği sorunları; teknik ve hukuki boyutlarıyla farklı disiplinlerin de konusu haline gelmiş ve birçok boyutu ile mücadele edilmesi gereken karmaşık bir yapıya dönüşmüştür. Bulut bilişim ve Web 2.0 kullanımı ile iş dünyası ve e-ticaret alanında sağlanan avantajlar (maliyetlerin düşmesi vd.) bilgi güvenliği politikalarının üretilmesi noktasında söz sahibi olan kuruluş ve örgütleri de harekete geçirmiştir.

Elektronik bilgi kaynaklarını depolayan ve belirli anlaşmalara bağlı olarak erişim hizmeti sağlayan (veritabanları vd.) bilgi merkezleri ve bulut hizmet sağlayıcılarının, belirli güvenlik standartların sağlanması (ISO 27001-2005[3] gibi) ve mevcut güvenlik politikalarına (yasal düzenlemeler, AB direktifleri vd.) uyum konusunda sorumlulukları bulunmaktadır. Temel olarak web tabanlı hizmetlerin sunulması konusunda ulusal ve uluslararası bilgi güvenliği politikalarına yön veren ve özellikle AB ve ABD bilgi güvenliği politikaları üzerinde en fazla tartışılan bilgi güvenliği risk alanları ve açıklık kazanmamış konular şunlardır (Svantesson ve Clarke, 2010, s. 392);

[3] **ISO 27001-2005 (Bilgi Güvenliği Yönetim Sistemi):** Hassas verilerin güvenliğinin sağlanması konusunda sistematik bir yaklaşım ile gereksinimleri tanımlayan, her boyuttaki şirket ve kamu kuruluşuna uygulanabilecek uluslararası standarttır.

- Kişisel verilerin güvenliği ve denetim alanı dışındaki ülkelere taşınması konuları,
- Hizmet alınan firmaların güvenilirliği ve hizmet sözleşmelerindeki belirsizlikler,
- Veri bütünlüğünün sağlanması, erişim ve kimlik denetimi sorunları,
- Büyük veri alanlarının siber saldırıların hedefi haline gelmesi,
- Adli incelemelerin ve dijital delillerin elde edilmesi konusundaki belirsizlikler ve
- Yasal düzenlemelerdeki eksiklikler.

***Bilgi Güvenliği Politikasında Ulaşılmak İstenen Ana Hedefin Belirlenmesi***

Bilgi güvenliği politikaları bilgi ya da bilgiyi saklamak, işlemek ve iletmek amacıyla kullanılan bilgi sistemlerinin güvenliğini sağlamak amacıyla oluşturulmuş dokümanlardır (Loop Technology, 2010). Bilgi güvenliği politikalarına ihtiyaç duyulmasının başlıca nedenleri; bilişim teknolojileri kullanımının iş dünyası ve kişisel yaşam üzerindeki etkileri, tehditlerin artış hızındaki yükselme, tehditlerin çok yönlülüğü, siber suç oranlarındaki artış ve yasal yükümlülüklerdir. Bu risk alanlarında kullanıcıların güvenli bir şekilde bilgi ve iletişim teknolojilerini kullanabilmeleri için; bilginin gizliliği, bütünlüğü ve kullanılabilirliği çerçevesinde çok yönlü önlemlerin alınması gerekmektedir. Bu unsurların risk yönetimine bağlı olarak uygulanması farklı oranlarda olabilmektedir. Fakat birbirinden bağımsız ya da önemsiz olduğu düşünülmeksizin uygulanması, bilgi güvenliğinin sağlanabilmesi için zorunludur. Bilginin gizliliğinin sağlanması, onun erişilebilirliğinin ortadan kalkmasına ya da erişilebilirliğe daha fazla önem verilmesi, bilginin bütünlüğünün bozulmasına neden olmamalıdır.

Bilgi güvenliği politikalarında öncelikli hedef; bilginin karakteristik özelliğini korumak amacıyla alınan tüm güvenlik önlemlerinin planlanması, bilgi ve bilgi sistemleri güvenliğini tehdit eden her türlü zararlı girişime karşı yeterli bilinçlendirmenin sağlanması ve olabildiğince kapsamlı işbirliğinin geliştirilerek tüm alanlarda mücadele edilmesini sağlamaktır. Uygulanabilir bir bilgi politikasının geliştirilmesinde; teknik altyapı ve güvenlik önlemleri için yeterli bütçenin ayrılması, bilgi güvenliğinin en zayıf halkası olan kullanıcıların bilinçlendirilmesi ve gerekli yasal düzenlemelerin yapılması konuları öncelikli olarak değerlendirilmektedir. Bilgi güvenliğinde bilinçlendirme çalışmaları, ulusal ve uluslararası düzeyde çerçeve planları ve kalkınma planları içerisinde yer almaktadır. 2000 yılından itibaren bilgi toplumu ve bilgi okuryazarlığı kapsamında yapılan çalışmaların da bir bölümü bilinçlendirme çalışmalarına ayrılmıştır. Kullanıcı eğitimi ile birlikte yürütülen bilinçlendirme çalışmalarında; bilginin bütünlüğü, gizliliği ve kullanılabilirliği konuları temel alınmakta ve bilginin neden korunması gerektiği üzerinde ağırlıklı olarak durulmaktadır (Loop Technology, 2010). Kullanıcılardaki bilgi güvenliğinin bilgi ve sistem yöneticilerinin işi olduğu algısı, sosyal mühendisliğin hafife alınması, koruyucu yazılımların güncellenmesinde gerekli hassasiyetin gösterilmemesi ve bilgi kaynağına erişimde gerekli seçiciliğin gösterilmemesi, bilinçlendirme çalışmalarının kapsamını oluşturan ve sık karşılaşılan eksikliklerdir.

Bilgi güvenliği politikalarının, gerekli teknik altyapının oluşturulması ya da hizmet sağlayıcıların (kullanıcı sözleşmeleri ve uygulamalarında) belirli standartlara uyması konusunda zorlayıcı etkileri bulunabilmektedir. Bu tür zorlayıcı politikalar, kurum ve kullanıcıları korumayı amaçlamakta ve olası kayıpların önüne geçilmesinde önemli rol oynamaktadır. AB'nin kişisel verilerin korunması amacıyla belirlediği kurallara aykırı olduğu gerekçesiyle, arama motoru Google'dan gizlilik ilkelerini değiştirmesini istemesi; son yıllarda bilgi güvenliği politikalarının hayata geçirilmesi noktasındaki dikkat çekici örneklerden biridir (Arthur, 2012). Belirlenen bilgi güvenliği politikalarının hayata geçirilmesi amacıyla yapılan yasal düzenlemeler ve direktifler, standartların uygulanması amacıyla baskı oluşturan ve bu sayede kurum ve kullanıcıları korumayı sağlayan önemli bilgi güvenliği bileşenleridir. AB sınırları içinde bulut bilişim hizmeti sunan şirketlerin, kullanıcılara ait kişisel bilgileri AB sınırları dışına

taşımalarının yasaklanması, bilgi güvenlik politikalarının yasal düzenlemelerle uygulamaya dönüştüğü örneklerden biridir (Sultan, 2012, s. 161).

## Avrupa Birliği'nde Uygulanan Bilgi Güvenliği Politikaları

### *AB Hukuk Mevzuatı Çerçevesinde Uygulanan Bilgi Güvenliği Politikaları*

AB ülkelerinin bilgi güvenliği politikalarını en iyi ifade eden kaynaklar yasal düzenlemelerdir. Yasal düzenlemeler, üzerinde uzlaşı sağlanmış politikaların hayata geçirilmiş olması anlamına da gelmektedir. Bilginin meta olarak değerlendirildiği günümüzde ne zaman ve hangi boyutta tehdit ile karşı karşıya kalınacağının önceden tahmin edilmesi mümkün değildir. Bir zararlı kodun üretim ve dağıtımının tamamen engellenmesi, hukuken ya da tüm teknik önlemler alınmasına rağmen mümkün olamamaktadır. Fakat kodun kullanımı sonrasında meydana gelen fiilin nasıl değerlendirileceği konusunda, AB çatısı altında bilgi güvenliği politikaları belirlenmekte ve yasal düzenlemelerin toplumsal gelişmelerin gerisinde kalmaması amacıyla çalışmalar yapılmaktadır. Her ülke ayrıca direktifler ve uluslararası sözleşmelere bağlı olarak kendi iç hukukunu uyumlu hale getirmektedir.

AB tarafından kişisel verilerin korunması ve siber güvenliğin sağlanması öncelikli olmak üzere, bilgi güvenliğinin sağlanması konusunda birçok direktif ve tavsiye kararı hazırlanmış ve yayımlanmıştır. Bilgi güvenliği ile ilgili konuları içeren temel AB direktifleri ve tavsiye kararları şunlardır[4];

- Bilgi Güvenliği Alanındaki 92/242/EEC Sayılı Karar
- Kişisel Verilerin İşlenmesi ve Kişisel Verilerin Serbest Dolaşımına Dair Bireylerin Korunması Hakkındaki 95/46/EC Sayılı Direktif
- 97/66/EC Sayılı Telekomünikasyon Alanında Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Direktifi
- 2000/31/EC Sayılı Elektronik Ticaret Direktifi
- 2002/58/EC Sayılı Elektronik Haberleşme Sektöründe Kişisel Gizliliğin Korunması Direktifi
- 1151/2003/EC Sayılı Yasadışı ve Zararlı İçerikle Geniş Ağ Üzerinde Mücadele Kararı
- 854/2005/EC Sayılı Güvenli İnternet Kullanımına Geçiş Kararı
- 2006/24/EC Sayılı Kamusal Elektronik Haberleşme Hizmetlerinin Sunumu Sırasında veya Kamusal Haberleşme Şebekeleri Üzerinden Elde Edilen Verilerin Muhafazasına İlişkin Direktif

24 Ekim 1995 tarih ve 95/46/EC sayılı AB direktifi; veri koruma hukukunda temel direktiftir. 97/66/EC sayılı direktif, 95/46/EC sayılı direktifin telekomünikasyon alanındaki tamamlayıcısıdır. 95/46/EC sayılı direktifi elektronik alanında tamamlayan 2002/58/EC sayılı direktif ise, aynı zamanda 2000/31/EC sayılı elektronik ticaret direktifinden de daha güçlü koruma sağlamaktadır. Bunların dışında; kullanıcı bilinçliliğini artırmaya ilişkin hazırlanmış tavsiye kararları da bulunmaktadır. 1997 ve 1999'da internet üzerindeki yasadışı ve zararlı içerikler, 2003'te ağ ve bilgi güvenliği konusuna AB'nin yaklaşımı, 2005'te bilgi sistemlerine yönelik saldırılar, 2007'de güvenli bilgi toplumu oluşturma stratejisi ve 2008'de bilgi ve iletişim teknolojilerini kullanan çocukları korumaya ilişkin tavsiye kararları öne çıkan bazı tavsiye kararlarıdır.

Direktif, sözleşme ve tavsiye kararları dışında AB bilgi güvenliği politikalarına ışık tutan önemli belgelerden biri de "Yeşil Kitap (Green Paper)"tır. Yeşil kitap; AB Komisyonu tarafından belirli bir konuyu tüm AB genelinde tartışmaya açmak ve alınan fikirlerle konunun olgunlaşmasını sağlamak amacıyla hazırlanmaktadır. Yeşil kitabın bağlayıcılığı bulunmamaktadır. Fakat niyeti ortaya koyması nedeniyle, belirlenecek politikalar için önemli bir basamak niteliğindedir. 17

[4] Ayrıntılı bilgi için bkz. (http://europa.eu/legislation_summaries/index_en.htm)

Kasım 2005 tarihinde Avrupa Komisyonu tarafından yayımlanan Kritik Altyapıları Koruma Programı (Green Paper on a European Programme for Critical Infrastructure Protection) isimli yeşil kitap da bilgi güvenliği politikalarının oluşturulması ile ilgili önemli belgelerden biridir (European Commission, 2005). Bu belgede; kritik bilgi ve iletişim altyapısını (bilgi sistem ağ altyapısı, telekomünikasyon, internet, uydu, bilgisayar, yazılım vd.), meydana gelebilecek her türlü felaketin (doğal felaketler, terörizm, siber saldırı, zararlı kod girişimleri vd.) etkisinden korumayı ve bireylerin zararının en aza indirilmesini amaçlayan önlemlere geniş yer ayrılmıştır.

AB'de bilgi güvenliği politikaları bazı temel konular üzerinden şekillenmektedir. Bunlar; bilgi ve iletişim teknolojileri ile toplumun etkileşimi (e-ticaret vd.), internet üzerinden gerçekleştirilen faaliyetler, veri mülkiyet hakları ve kişisel verilerin korunması konularıdır. AB direktiflerden bazıları, bu temel konuların bilgi ve iletişim teknolojileri ile ilişkisi ve gelişen bilgi ve iletişim teknolojilerinin ekonomi alanında yaratmış olduğu etkiye de bağlı olarak daha fazla tartışılmakta ve gündemde kalmaktadır (King ve Raja, 2012, s. 312). AB bilgi güvenliği politikalarının ve yasal düzenlemelerin en önemli unsurlarından biri olan 95/46/EC sayılı veri koruma direktifinin ve yeni veri koruma direktifi taslağının içeriği, bu konuya genel yaklaşım hakkında önemli ipuçları vermektedir.

24 Ekim 1995 tarih ve 95/46/EC sayılı AB direktifi; kişilerin mahremiyetini en üst düzeyde korumayı ve aynı zamanda kişisel verilerin serbest dolaşımına da olanak sağlamayı hedefleyen bir düzenlemedir. Direktifte kişisel veriler, "belirli veya belirlenebilir gerçek kişilere ilişkin bütün bilgiler" olarak ifade edilmektedir. Ayrıca; "kişisel veri" olarak nitelendirilecek verilerin; üzerinde şifre taşıması, kimlik numarası bulundurması, fiziksel, zihinsel, fizyolojik, kültürel, ekonomik ya da sosyal kimliğe dair aidiyeti ifade etmesi ve belirli ya da belirlenebilir bir kişiye ait ayırt edici bilgiyi içermesi gerekmektedir. Direktifin amacı; kişisel verilerin işlenmesi ile ilgili olarak, kişisel mahremiyet, kişilerin temel hakları ve özgürlüklerinin üye devletler tarafından korunmasını sağlamaktır. Fakat üye ülkeler, direktife uygun olarak yapacağı koruma işlemleri esnasında, üye ülkeler arasında kişisel verilerin akışını engellemeyeceklerdir (European Council, 1995). Üye ülkeler arasında veri akışının engellenmesini yasaklayan maddeyle, bilgi güvenliğinin sağlanmasında temel prensiplerden biri olan güvenlik ve erişim dengesinin sağlanması amaçlanmıştır.

95/46/EC sayılı direktif ile hizmet sağlayıcılar belirli kurallara uymaya zorlanarak, kişisel verilerin korunması konusunda kullanıcılara temel haklar sağlamaktadır. Direktifte; şirket ve kuruluşların herhangi bir meşru ya da açık gerekçe olmadıkça, kişisel bilgileri toplama, kaydetme, kullanma ve açığa vurmaları kısıtlanmıştır. Veri öznesinin; verinin nasıl işlendiği, nasıl saklandığı ve kim tarafından erişildiği konusunda bilgilendirilmesi ve en az seviyede kişisel bilginin (sağlık bilgileri vd.) kaydedilmesi gerekmektedir. Ayrıca bilgilerin güvenliğinin sağlanması ve yetkisiz erişimlerden korunması zorunludur.

95/46/EC sayılı direktifin 25. Maddesi ile kullanıcıya ait kişisel bilgilerin, yeterli seviyede bilgi güvenliği sağlamayan AB ekonomik alanı dışındaki ülkelere transferi yasaklanmıştır. Koruma seviyesinin yeterliliğinin değerlendirilmesinin ise; veri transfer faaliyetini çevreleyen tüm güvenlik koşullarının dikkate alınarak yapılacağı belirtilmiştir. Değerlendirmede özel önem verilecek unsurlar arasında; verinin aktarılacağı ülke, yasal düzenlemeler, verinin yapısı ve faaliyetin amacı yer almaktadır. Komisyonun yeterli koruma seviyesini taşımadığını tespit ettiği üçüncü ülkeye karşı tüm üye devletler gerekli önlemleri almakla yükümlüdürler. 25. Maddenin bazı istisnaları bulunmaktadır. Bunlar (madde:26); veri öznesinin açık rızasının olması, kanuni hakların tesisi ya da kamu menfaatini gerektirmesi ve veri öznesinin hayati menfaatlerinin korunması için gerekli olması gibi özel durumları içeren istisnalardır. 95/46/EC sayılı direktife uygun olarak alınan 26 Temmuz 2000 tarih ve 2000/520/EC sayılı Avrupa Komisyonu kararında; Avrupa Ekonomik Alanı'ndan ABD›ye bilgi transferi yapılabilmesi

için, bilgiyi transfer edecek şirketin "Safe Harbour Agreement"[5] (Güvenli Liman Anlaşması) üyesi olma durumu istisnai bir durum olarak belirlenmiştir (European Commission, 2004). Güvenli Liman Anlaşması; gerekli şartları taşıyarak üye olan şirketin, kullanıcılarını topladığı kişisel veriler ve bu verileri hangi amaçla kullanacağı hakkında bilgilendirerek, gerekli tüm bilgi güvenliği önlemlerini almalarını zorunlu hale getirmiştir. Şirketlerin bu anlaşmanın üyesi olabilmek için tüm AB üyesi ülkelerden ayrı ayrı onay almak zorunda olmaları, saygınlık ve güvenilirliklerinin artmasına da destek olmaktadır.

AB sınırları içinde faaliyet gösteren tüm şirketler için, yasal yükümlülüklere uyma zorunluluğu bulunmaktadır. Bu bağlı olarak; bilgi işleme ve bilgiyi diğer şirketlerle paylaşma (AB alanı dışı dâhil) konusunda, kullanıcılar da veriler üzerinde hak sahibidirler (European Council, 1995). 95/46/EC sayılı direktif; veri öznesinin verileri hakkında bilgilendirilmesini sağlama ve AB sınırları içinde yeni sunucular tesis etme konusunda hizmet sağlayıcılara yeni sorumluluklar yüklemektedir. Verilen hizmetler üzerinden kişisel veri toplayan ve işleyen şirketler bu sorumlulukları yerine getirmek zorundadırlar.

AB sınırları içinde geçerli olan mevcut veri koruma ve tüketici koruma kanunları, özellikle gizliliğin sağlanması konusunda kaygıları gidermekte yetersiz kalmaktadır (Filippi ve Belli, 2012). Bilişim teknolojileri ve internetteki gelişime bağlı olarak sosyal paylaşım sitelerinin kullanımının yaygınlaşması ve bilgi depolama yöntemlerinde meydana gelen değişim, bilginin korunması konusunda güncellemelerin yapılmasını zorunlu hale getirmiştir. Günümüzde internet üzerinde yapılan birçok işlem (çevrimiçi rezervasyon, ürün alımı, çeşitli abonelikler vd.); ad-soyad, kimlik numarası, telefon, adres, e-posta, doğum tarihi gibi kişisel bilgiyi karşı taraf ile paylaşımı gerektirmekte ve bu yüzden yeni alanları da kapsayan yasal düzenlemelerin yapılmasına ihtiyaç duyulmaktadır. 95/46/EC sayılı direktifin güncellenmesi gerektiği ve bunun nasıl yapılacağı, 4 Kasım 2010 tarihinde yayımlanan IP/10/1462 referans numaralı "Kişisel Verilerin Nasıl Korunacağına İlişkin Strateji" (European Commission, 2010a) ve MEMO/10/542 referans numaralı bildirilerde (European Commission, 2010b) de ifade edilmiştir. Bu ihtiyaca bağlı olarak AB Komisyonu'nun çevrimiçi gizlilik haklarını kapsamlı olarak düzenleyen yeni kişisel verilerin korunması taslağı; 25 Ocak 2012'de AB Konseyi ve Parlamento'nun onayına sunulmuştur (European Commission, 2012b).

IP/12/46 referans numaralı yeni kişisel verilerin korunması taslağı; kullanıcıların çevrimiçi veri koruma risklerini yönetebilme imkânı sunan "unutulma hakkı", sahip olunan verilere kolay erişim, kişisel verilerin hizmet sağlayıcılar arasında transfer edilebilmesi, kişisel verilerin nasıl elde edilebileceği konusun (örneğin; 13 yaş üstü kısıtlaması gibi) daha açık ve anlaşılır olması, herhangi bir sebeple veri ihlali oluştuğunda kullanıcı ve ilgili güvenlik birimlerinin durum hakkında bilgilendirilmesi ve kişisel verileri işleyenlerin daha fazla sorumluluk alması gibi önemli yenilikler içermektedir (European Commission, 2012d).

AB Komisyonu "Dijital Ajandası (2010-2020)" içerisinde de bilgi güvenliği konusuna geniş yer ayrılmıştır. Dijital Ajanda; AB'nin 2020 stratejisinin bir parçasıdır. Dijital Ajanda'nın bilgi güvenliği konusundaki amacı; kişisel verilerin korunması ve siber saldırı konuları da dâhil olmak üzere, tehditlere karşı pratik çözüm önerileri üretmek ve bilgi güvenliği politikaları geliştirmektir (European Commission, 2012e).

[5] **Safe Harbour Agreement (Güvenli Liman Anlaşması):** ABD ticaret bakanlığı ile AB arasında 2000 yılında yapılan, AB sınırları içindeki ülke vatandaşlarının kişisel bilgilerinin ABD şirketleri tarafından transferini belirli şartlara bağlayan bir anlaşmadır.

## *Uluslararası Sözleşmeler Çerçevesinde Bilgi Güvenliği Politikaları*

### *Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkındaki Sözleşme*

Veri koruma alanında Avrupa Konseyi tarafından imzaya açılan ilk uluslararası hukuk düzenlemesi, 1981 yılında yapılan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunması Hakkındaki Sözleşme"'dir (European Commission, 1981). 108 sayılı sözleşme ile sözleşmeyi imzalayan ülkelerdeki gerçek kişilerin, yasal olarak temel hak ve özgürlüğü ve kişisel nitelikteki verileri güvence altına alınmaya çalışılmıştır. Sözleşmede yer alan kişisel nitelikteki verilerin tanımı günümüzde de geçerliliğini korumaktadır. 1995 yılında 95/46/EC sayılı AB direktifi ile birlikte, 108 sayılı sözleşmede yer alan bireylerin hak ve özgürlükleri ve kişisel mahremiyet hakkındaki esaslar genişletilmiştir. 2001 yılında 108 sayılı sözleşmeye ek olarak; bulut bilişim hizmetlerini de yakından ilgilendiren 181 sayılı Ek Protokol (Denetleyici Makamlar ve Sınırötesi Veri Akışına İlişkin Protokol) kabul edilmiştir (European Commission, 2001). 108 sayılı sözleşme ve 181 sayılı protokolü imzalayan 46 ülkeden 2 tanesi (Türkiye ve Rusya) hariç olmak üzere tüm ülkeler iç hukukta da onaylayarak uygulamaya başlamışlardır (European Council, 2012). AB bilgi politikalarının bir parçası olarak, yapılan yasal düzenlemeler ve sözleşmelerden taraf olan ülkelerin etkin olarak faydalanabilmeleri için; kişisel bilgilerin gizliliğinin sağlanması, elektronik bilgi kaynaklarının korunması ve bilgi sistemlerinin kesintisiz olarak hizmet verebilmesi konusunda iç hukuk düzenlemelerini yapmaları gerekmektedir.

108 sayılı sözleşmede ve 1995 yılında yayımlanan 95/46/EC sayılı direktifte; üye ya da sözleşmeye taraf ülkeler arasında kişisel nitelikteki verilerin transferinin yasaklanamayacağı hükmü bulunmaktadır. Bu hükümden, AB'nin bilgi güvenliği politikalarını geliştirirken; Avrupa Ekonomik Alanı'nı bir bütün olarak değerlendirdiği ve üye ya da taraf ülkeler arasında bütünleştirici bir tutumu benimsediği görülmektedir. Özellikle Ocak 2012 tarihli ve IP/12/46 referans numaralı yeni veri koruma direktifi taslağına ihtiyaç duyulmasının nedenleri arasında üye ülkelerin ulusal veri koruma düzenlemeleri arasındaki belirsizlik ve farklılıkların da gösterilmesi, bu düşünceyi doğrulamaktadır.

### *Avrupa Konseyi Siber Suçlar Sözleşmesi ve Ek Protokol*

Uluslararası bilişim suçları ve bilgi güvenliği politikaları ile ilgili olarak Avrupa Konseyi tarafından hazırlanan en önemli hukuki belgelerden biri 185 sayılı Siber Suçlar Sözleşmesi (SSS)'dir (European Council, 2001). 2001 yılında kabul edilerek 2004 yılında yürürlüğe giren ve sonradan Türkiye'nin de katıldığı (TBMM'de henüz onaylanıp yürürlüğe girmedi) 47 ülke tarafından (ABD, Japonya, Kanada, Güney Afrika, Avrupa Konseyi üyeleri ve diğer Avrupa ülkeleri) imzalanan SSS; bilgi merkezlerini ve bireyleri korumayı hedef almakta ve zararlı kodların üretilmesi/dağıtılması konusunda uluslararası bir çerçeve oluşturmaktadır (Bozkurt, 2010). SSS aynı zamanda, yetkisiz erişim ve fikri mülkiyet hakları ile ilgili düzenlemeler de içermektedir. SSS'in bilgi güvenliği politikaları açısından en önemli özelliği; içeriğinde yasal düzenlemeler, alınacak teknik önlemler ve uluslararası işbirliği seçeneklerinin harmanlanarak oluşturulmuş olmasıdır (Roscini, 2010). AB'nin siber suçlar konusunda düzenleme yapmaya zorlayan en büyük etken; uluslararası hukukta bilişim suçları ile ilgili boşlukların bulunması ve soruşturma, kovuşturma ve diğer adli işlemlerin nasıl yapılacağı konusundaki belirsizliklerdir.

SSS'nin 4. maddesi veriyi bozma, değiştirme ve silme işleminin haksız, bilerek ve isteyerek gerçekleştirilmiş olmasını; 5. maddesi ise, bilişim sistemine veri ilâve edilmesi, verilerin silinmesi, bozulması, değiştirilmesi ve başka bir yere aktarılmasını 4. maddede olduğu gibi (haksız, bilerek ve isteyerek gerçekleştirilmiş olmasını) yaptırıma bağlamıştır (Helvacıoğlu, 2004). SSS'nin zararlı kodlar, yetkisiz erişim ve fikri mülkiyet hakları konusundaki düzenleme-

leri, sözleşmeyi imzalayan ülkeler arasındaki uluslararası işbirliğini arttırmayı hedeflemektedir. Bilgi sistemlerine ve verilere yönelik saldırıların uluslararası bir sözleşmeyle de düzenlenmiş ve yaptırıma bağlanmış olması, AB'nin bilgi güvenliği politikası hakkında önemli ölçüde fikir vermektedir.

28 Ocak 2003 tarihinde; bilişim sistemleri aracılığıyla yapılan ırkçılık ve yabancı düşmanlığını tanımlayan ve bu tür içeriğin yayılmasını suç olarak nitelendiren ek protokol hazırlanmıştır (European Council, 2003). Türkiye SSS'yi 2011 yılında imzalamış, fakat ek protokolü imzalamamıştır. Türkiye'nin sözleşmenin yaptırım gücünden faydalanabilmesi için, sözleşmeyi iç hukuka uyarlaması ve TBMM onayından geçirmesi gerekmektedir. SSS'nin iç hukuka uyarlanarak yürürlüğe girmesi, emniyet teşkilatları arasında bilgi alışverişine imkân tanıması yönüyle de önemlidir. Fakat bu konuda yapılacak çalışmalar, "Kişisel Verilerin Korunması" kanunu ile ilgili çalışmalarla birlikte yürütülmelidir. Çünkü iç hukukunda kişisel verilerin korunması hakkında düzenlemeye sahip olmayan ve kişisel verilerin hangi şartlarda paylaşılacağını belirlemeyen ülkeler; SSS'yi uygulamaya başladıklarında, bireylerin kişisel verilerini sözleşmeyi onaylayan diğer ülkelerle paylaşmak zorunda kalmaları söz konusu olabilecektir.

### *Uluslararası Kuruluşların Öncü Olduğu Bilgi Güvenliği Politikaları*

*ENISA (AB - Avrupa Ağ ve Bilgi Güvenliği Ajansı)*

AB içinde özel bir görevi yerine getirmek, belirli bir alandaki sorunlara çözüm aramak ve kurumlar arasında koordinasyonu sağlamak amacıyla tüzel kişiliğe sahip ajanslar oluşturulmuştur. Bunlardan biri olan ve merkezi Yunanistan'da bulunan ENISA (European Network and Information Security Agency), AB içinde ağ ve bilgi güvenliğinin sağlanması amacıyla kurulan bir uzmanlık kuruluşudur. Avrupa Konseyi'nin 31 Mart 1992 tarihli ve 92/242/ECC sayılı kararı, üye ülkelerin bilgi sistemleri kullanımının güvenliğini sağlamak ve bilginin serbest dolaşımı ile ilgili politika geliştirme amacını taşımaktadır (European Council, 1992). Kararda, komisyona danışmanlık yapacak ve eylem planı hazırlayacak bir birimin kurulması da öngörülmektedir. 10 Mart 2004 yılında ENISA'nın kurulması ile ilgili 2004/460/EC sayılı tüzüğün de bu karar ile ilişkili olduğu söylenebilir.

2004/460/EC sayılı ve 10 Mart 2004 tarihli düzenleme ile kurulan ENISA, AB çatısı altındaki tüm kurum ve kuruluşların ağ ve bilgi güvenliği konusunda bilgi paylaşımında bulunduğu bir merkez konumundadır. ENISA'nın sorumluluğu, AB içinde en üst seviyede ve en etkin şekilde ağ ve bilgi güvenliğini tesis etmektir. AB enstitüleri ve üye ülkelerle de işbirliği yaparak; AB içinde yer alan tüm kullanıcılar, çeşitli organizasyonlar ve iş dünyasında bilgi güvenliği kültürü oluşturmayı hedeflemektedir. ENISA, bulut bilişim alanında hem kamu kurumlarına, hem de özel sektör temsilcilerine yeni bilişim teknolojileri ve servislerine güvenli geçiş için rehberlik hizmeti sunmaktadır (ENISA, 2009). ENISA, kurumlar arası koordinasyonu sağlama ve bilinçlendirme çalışmaları yapmanın yanı sıra; kullanıcılara uyguladığı anketlerle mevcut durumun analizini de sık aralıklarla yaparak, yeni bilgi güvenliği politikalarının üretilmesine katkı sağlamaktadır (ENISA, 2012).

AB veri koruma kanunu ve kişisel verilerin gizliliği ile ilgili tanım ve kapsamın gözden geçirilmesi konusunda AB Komisyonunun son yıllarda daha fazla çaba gösterdiği görülmektedir. Bunun nedeni; bilgi ve iletişim teknolojilerinin gelişimine bağlı olarak, ekonomi politikaları ile bilgi politikalarının önemli ölçüde kesişmesidir. AB, ekonomi politikaları ile bilgi ve bilgi güvenliği politikaları arasındaki ilişkiye bu nedenle daha fazla önem vermektedir. Bu alanlar arasında ortak politika geliştirilmesi ve uygulanmasında en büyük sorumluluğu ENISA üstlenmektedir (European Commission, 2011). AB veri koruma düzenlemelerinin gözden geçirilmesi kapsamındaki yeni çalışmaların temel gerekçesi olarak; AB içindeki her ülkede

farklılık gösteren ve anlaşılamayan veri koruma yasalarının, kullanıcılarda çevrimiçi alışverişe karşı güvensizlik yaratması ve bunun Avrupa çevrimiçi ekonomisini olumsuz etkilemesi gösterilmektedir (European Commission, 2012a).

ENISA, AB içerisinde ve üye ülkelerde oluşturulan "Bilgisayar Olaylarına Müdahale Ekipleri" (Computer Emergency Response Team, CERT) ile ortak çalışmalar da yürütmektedir. CERT, kritik bilgi altyapısının korunması ve danışmanlık hizmetleri konusunda önemli bir rol üstlenmektedir. ENISA'nın ülkeler arasındaki koordinasyonu sağlama görevini, her ülkenin CERT merkezi ile birlikte yürütmesi hedeflenmektedir. ENISA'nın, faaliyet alanlarının tümü göz önüne alındığında; McCumber Bilgi Güvenliği Modelinin "Güvenlik Önlemleri" altında yer alan sorumlulukları AB içinde gerçekleştiren bir kuruluş olduğu söylenebilir.

*Uluslararası Telekomünikasyon Birliği'nin (ITU - International Telecommunication Union) Çalışmaları*

Uluslararası Telekomünikasyon Birliği (ITU) ilk 20 kurucusu arasında Türkiye'nin de yer aldığı, Birleşmiş Milletler'in telekomünikasyon alanındaki ihtisas kuruluşlarından biridir. Merkezi İsviçre'de bulunan ITU tarafından oluşturulan bilgi güvenliği strateji ve politikalarına AB doğrudan katkı sağlamaktadır. ENISA ile ITU'nun ortak çalışmalarından biri olan ve yol haritasının birlikte çizildiği "ICT Security Standards" projesi bu kapsamda önemli örneklerden biridir (ITU, 2011). Uluslararası Telekomünikasyon Birliği'ne 193 ülke ve 700 özel sektör kuruluşu üyedir. Yürütmekte olduğu projelerle tüm dünya için iletişim standartlarının belirlenmesinde önemli bir kuruluş olma özelliği taşımaktadır.

ITU, internet ve bilgi politikaları üzerinde etkili kuruluşlardan biridir. ITU konseyi her yıl düzenli olarak toplanmakta ve mevcut durum değerlendirmesi ile birlikte, bir sonraki toplantının temasını da belirlemektedir. 21 Ekim 2011'de Cenevre'de yapılan toplantıda; bir sonraki "internet ve kamu politikaları" konulu forumun 2013 yılında yapılması kararı alınmıştır. ITU kuruluş yasası ve sözleşmede değişiklik yapan tam yetkili temsilciler konferansı sonuç belgeleri, üye ülkeler tarafından yasalaştırılmaktadır.

AB bilgi politikalarının gelişimi ve uygulanmasında önemli katkısı olan ITU temsilciler konferansının sonuç belgeleri Türkiye'de 5163 sayılı kanun ile 2004 yılında yasalaştırılmıştır. Bu yasanın içeriği; ITU'nun bilgi güvenliği politikaları üzerindeki belirleyiciliğinin görülebilmesi açısından önemlidir. "Bilgi ve iletişim teknolojilerinin kullanımında güven ve emniyet" başlığı altında, bilgi sistemleri ve bilgi kaynaklarına zararlı karışma ve bunların kötüye kullanılmasını içeren bilgi güvenliğinin değerlendirilmesine vurgu yapılmıştır (TBMM, 2004). ITU tarafından bilgi güvenliği konusunda onaylanan ve bilgi politikasına yön veren tavsiye niteliğinde birçok çalışma ve değerlendirme bulunmaktadır (Bertine, 2007).

ITU'nun internet politikaları ve yönetim ile ilgili olarak da çok geniş çalışma alanlarında faaliyetlerini yürütmektedir. Özellikle siber güvenlik, yeni nesil bilgisayar ağları ve çocukların çevrimiçi ortamda korunması (hukuki çözümler, teknik önlemler ve uluslararası boyutta önlemler kapsamında) ile ilgili güvenlik politikalarının belirlenmesi ve uygulanması konusundaki çözümler dikkate alınması gereken çalışmalardır (ITU, 2012).

## AB'de Bilgi Güvenliği Politikaları: Genel Değerlendirme

AB bilgi güvenliği politikalarının geliştirilmesinde; direktifler, uluslararası sözleşmeler, özel amaçlı kuruluşlar, yeşil kitap ve tavsiye kararları öncelikli ve etkili kaynaklardır. Direktifler, gelişen bilgi teknolojilerine bağlı olarak güncellenen ve politikaların uygulamaya dönüştüğü noktada bilgi güvenliği politikalarını en iyi ifade eden hukuk kaynaklarıdır. Uluslararası sözleşmeler ise; bilgi güvenliği politikalarının başarılı olabilmesi için, uluslararası boyutta işbirliğinin önemini ve güncel tehditlere karşı ne tür önlemler alınabileceğini göstermektedir.

Bilgi güvenliği politikalarının hayata geçirilmesi, uluslararası boyutta koordinasyonun sağlanabilmesi ve elde edilen sonuçlardan yeni politikaların üretilebilmesinde; bu özel amacı yerine getirmek için kurulmuş olan ajans ve uluslararası kuruluşların etkinliği önemlidir. Her ne kadar bağlayıcılığı ya da uygulanma zorunluluğu bulunmasa da; fikirlerin tartışılması ve olgunlaşmasına katkı sağlayarak, yeni bilgi güvenliği politikalarının oluşmasında tavsiye kararları ve yeşil kitabın da önemli başvuru kaynakları olduğu değerlendirilmektedir.

AB bilgi güvenliği politikalarının 1980'li yıllardan itibaren bilgi ve iletişim teknolojilerinin gelişiminin beraberinde getirmiş olduğu risklere bağlı olarak şekillendiği ve direktifler üzerinde güncellemeler yapıldığı görülmektedir. Fakat 1981 yılında imzalanan ilk uluslararası sözleşmenin, sözleşmeyi imzalayan üye ülkeler tarafından iç hukuka uygun hale getirilemediği ve her ülkenin kendi veri koruma kanununu hazırlamasının uygulamada farklılıklar yarattığı aşikârdır. Bilgi güvenliği politikalarının temel göstergelerinden biri olan veri koruma direktifinin 1990'lı yıllardaki hazırlanma nedeni ile 2012 yılında yeni ihtiyaçlara bağlı olarak güncellenme nedeninin odak noktasında; farklı uygulamalardan kaynaklanan sorunların ve ekonominin gelişimine ilişkin gerekçelerin bulunması dikkat çekicidir (European Council, 1995). Her iki direktif ve taslakta da, üye ülkelerin veri işleme ve koruma yöntemlerindeki (mahremiyet, bireysel haklar ve üye ülkeler arasında veri akışına farklı müdahaleler) farklılıkların, ekonomi faaliyetlerinin kısıtlanmasına neden olabileceği endişesi yer almaktadır.

AB bilgi güvenliği politikalarının oluşmasına etki eden unsurlar ve uygulanacak yöntemler; direktif ve sözleşmelerin amaçlarında açıkça ifade edilmektedir. Fakat mevcut düzenlemelerin yeterliliği, bilgi güvenliği politikalarının hangi yönde geliştiği ve gelecek ile ilgili beklentilerin en iyi okunabildiği kaynaklar; direktif taslakları, özel amaçlı kuruluşların projeleri ve yeşil kitaptır. Veri koruma ile ilgili mevcut direktifler, sözleşmeler ve yeni veri koruma direktifi taslağı (European Commission, 2012c) da dikkate alınarak, AB bilgi güvenliği politikaları ile ulaşılmak istenen temel hedefler şöyle özetlenebilir;

- Veri öznesinin veri üzerinde yönetim ve tam denetiminin (unutulma hakkı vd.) sağlanması,
- Verinin işlenmesi ile ilgili tüm aşamalarda (toplama, engelleme, kaydetme, depolama, değiştirme, silme, dağıtma vd.) veri öznesinin bilgilendirilmesi,
- Veri öznesinin veriye erişiminin kolaylaştırılması,
- Kişisel verilerin hizmet sağlayıcılar arasında transferinin yapabilmesi hakkının sağlanması ve hizmet sağlayıcılar arasında rekabetin arttırılması
- Verinin nasıl elde edildiği konusunda (özellikle çocuklar için 13 yaş sınırı ile ilgili olarak) açıklığın sağlanması
- Veri öznesini olumsuz etkileyebilecek güvenlik ihlalleri meydana geldiğinde; verinin AB dışında işlenmesi halinde dahi, hizmet sağlayıcıların veri öznesini ve yetkili birimleri bilgilendirmeleri
- Veri koruma haklarının ihlali konusu ile ilgili idari ve hukuki yapının geliştirilmesi
- Verinin işlenmesi ile ilgili sorumluluk ve denetimlerin arttırılması
- Siber suçlara karşı Avrupa dışından ülkelerin de katılımıyla uluslararası mücadelenin geliştirilmesi ve uluslararası veri koruma standartlarının oluşturulması
- AB sözleşmelerine taraf ülkelerde ENISA ile koordine halinde olan bir "Bilgisayar Olaylarına Müdahale Merkezi" (Computer Emergency Response Teams, CERT) kurulması
- Bireylerin müdahale olmaksızın her türlü bilgiyi arama ve iletme hakkının sağlanması
- AB kurallarının AB pazarı içinde faaliyet gösteren, fakat kişisel verileri AB alanı dışında bulunduran şirketlere de uygulanması ve böylece AB vatandaşlarının veri güvenliğinin dünyanın her yerinde sağlanması
- Ulusal bilgi koruma otoritelerinin güçlendirilerek, AB veri koruma düzenlemelerini ihlal eden şirketleri cezalandırabilmelerinin sağlanması

- Hizmet sağlayıcıların sadece AB ülkelerinde bulunan ulusal veri koruma otoritesi/kuruluşu ile bağlantılı olması ve bireylerin kişisel verilerini işleyen şirket AB alanı dışında olsa dahi, ihtilaf halinde kendi ulusal veri koruma otoritelerine bağlı olmalarının sağlanması
- Veri koruma kurallarının etkin olarak uygulanması ile AB pazarında ticaretin canlandırılması ve bu sayede (yıllık 2,3 milyar Euro) tasarruf sağlanması
- Yasal düzenlemeler ile tüketicilerin verilerinin korunduğu güvencesini verebilen AB şirketlerinin uluslararası rekabette avantaj sağlamaları ve böylece AB sayısal ekonomisinin hızlı büyümesinin gerçekleşmesi
- Hayatı kolaylaştıran ve aynı zamanda maliyetleri düşüren, yeni iş sahaları yaratan, ekonomiyi canlandıran, sayısal tek pazarın oluşumuna katkı sağlayan, açık ve güçlü bir hukuki altyapının oluşturulması.

**Sonuç**

AB bilgi güvenliği politikalarının ana hedefi, ekonomi alanında bilgi ve iletişim teknolojilerinin kullanım etkinliğini artırabilmek için gerekli güvenlik önlemlerinin belirli bir standart çerçevesinde sağlanması, başta kişisel mahremiyet olmak üzere temel hak ve özgürlüğün korunması ve bireylerin çevrimiçi ticarete karşı güven kazanmaları sağlanarak bireyin refahının artması ve ticari genişlemeye katkı sağlamaktır. AB'de bu hedefe ulaşmak için, uluslararası sözleşmeler ve direktiflerin temel araçlar olarak kullanıldığı görülmektedir. Uluslararası sözleşmelerle (SSS gibi); uluslararası bilişim suçlarının büyük bölümünü düzenleyerek, AB sınırlarının da ötesinde güvenlik şemsiyesi oluşturulması hedeflenmektedir. Veri koruma direktifleriyle de; "Avrupa Ekonomik Alanı" içerisinde bulunan tüm kurum ve bireylerin verilerinin en üst seviyede korunması hedeflenmektedir. Fakat sözleşme ve direktiflerin koruyuculuğu, üye ülkelerin bu sözleşme ve direktiflere uyumlu iç hukuk düzenlemelerini yapmaları ile mümkün olabilmektedir.

AB tarafından bilgi güvenliğinin sağlanması çerçevesinde oluşturulan politikalar ve politikaları uygulamaya ilişkin olarak yapılan uluslararası anlaşmalar ve direktiflerin etkileri; hizmet sağlayıcıların kullanıcı ile yapmış oldukları sözleşmelerde açıkça görülebilmektedir. Sözleşmelerde; AB üyesi ülkelerin, ABD'nin ve bazı ülkelerin (İsviçre ve Avusturalya gibi) kullanıcılarına ait verileri için yapılan anlaşmalara bağlı olarak gerekli güvenlik önlemlerinin alınacağı ifade edilmektedir. Bilgi güvenliği politikası ve bu kapsamda hazırlanmış yasal düzenlemeleri olmayan ülkelerin kullanıcılarına ait verilerin güvenliğinin sağlanması sorumluluğu kullanıcıya bırakılmıştır.

Bilgi ve iletişim teknolojilerindeki hızlı gelişim, mevcut veri koruma direktifinin (95/46/EC sayılı direktif) yerini alacak güncel bir direktif için hazırlıkların başlamasına neden olmuştur. AB Komisyonunun 2012 yılında yapmış olduğu çalışmalarda; çevrimiçi ekonominin canlanmasında büyük rol üstlenen bulut bilişim kullanımının önündeki en büyük engelin veri koruma kaygısının olduğu ve en kısa sürede (2013 yılı içinde) AB Konseyi ve Parlamentosu'nun düzenleme üzerinde çalışmasının önemli olduğu belirtilmiştir (European Commission, 2012f). AB bilgi güvenliği politikalarında; bireysel hakları koruyan yasal düzenlemelerle yeni bilgi ve iletişim teknolojilerinin kullanımını yaygınlaştırmak ve çevrimiçi ekonomiyi canlandırarak rekabetçi bir ortak pazarın oluşumunu hızlandırmak öncelikli hedef olarak görülmektedir. AB bilgi güvenliği politikalarının belirlenen hedefler çerçevesinde; bilgi kaynakları, bilgi sistem altyapısı, bilgi sistemleri ve bilgi hizmetlerinin tümünü kapsayacak şekilde çok yönlü olarak oluşturulduğu görülmektedir. Bu yönüyle, McCumber bilgi modelinde olduğu gibi; bilgi güvenliğinin sağlanabilmesi için gerekli olan çok boyutlu değerlendirme ve farklı alanların birleşme noktalarında da etkinliğin arttırılması hedefine ulaşılmaktadır. Bilgi merkezleri ya da kurum ve kuruluşlarda bilgi güvenliği politikaları geliştirilirken; kuramsal model

üzerinde irdelenen bilgi güvenliğinin tüm boyutlarının AB'nin bilgi güvenliği politikalarına yaklaşımında olduğu gibi çok yönlü olarak değerlendirilmesi, uygulanabilirliğin sağlanması açısından önemlidir. Özellikle son 20 yıl içerisinde uygulanan bilgi güvenliği politikaları, (her ne kadar yeterli seviyede olmasa da) dünyanın diğer bölgeleri ile kıyaslandığında; bireysel hakların ve mahremiyetin korunması konusunda AB sınırları içindeki bireyleri ayrıcalıklı bir noktaya taşımıştır.

## Kaynakça


Arthur, C. (2012). *EU justice chief warns Google over "Sneaking" citizens' privacy away*. 3 Kasım 2012 tarihinde http://www.gurdian.co.uk/technology/2012/mar/01/eu-warns-google-over-privacy adresinden erişildi.

Belson, D., Möller, R. ve Bergqvist, S. (2012). *The state of the internet.* 23 Mart 2012 tarihinde http://www.akamai.com/stateoftheinternet/ adresinden erişildi.

Bertine, H. (2007). *Telecommunication security.* 26 Ekim 2012 tarihinde http://www.itu.int/ITU-T/special-projects/security/presentations/Telecommunication_Security-GSC11.ppt adresinden erişildi.

Bozkurt, A. (2010). Türkiye de "Sanal Suçlar Sözleşmesi"ni imzaladı. *Bilişim Dergisi,* 127, 10-14.

CiscoLearning. (2009). *CCNA security.* 28 Ekim 2012 tarihinde http://www.cs.rpi.edu/~kotfid/secvoice10/powerpoints/CCNA_Security_01.ppt adresinden erişildi.

ENISA. (2009). *Cloud computing information assurance framework.* 25 Aralık 2012 tarihinde http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport adresinden erişildi.

ENISA. (2012). *An SME perspective on cloud computing - Questionnaire.* 05 Aralık 2012 tarihinde http://www.surveymonkey.com/s.aspx?sm=CZdVubBa9LIzYlR3KNeZIQ_3d_3d adresinden erişildi.

European Commission. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* 04 Aralık 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm adresinden erişildi.

European Commission. (2001). *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows.* 04 Aralık 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm adresinden erişildi.

European Commission. (2004). *Commission Staff Working Document.* 05 Aralık 2012 tarihinde http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf adresinden erişildi.

European Commission. (2005). *Green paper on a European programme for critical infrastructure protection.* 09 Aralık 2012 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF adresinden erişildi.

European Commission. (2010a). *European Commission sets out strategy to strengthen EU data protection rules.* 07 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_IP-10-1462_en.pdf adresinden erişildi.

European Commission. (2010b). *MEMO/10/542.* 07 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_MEMO-10-542_en.pdf adresinden erişildi.

European Commission. (2011). *Action 28: Reinforced network and information security policy*. 03 Aralık 2012 tarihinde Digital Agenda for Europe: http://ec.europa.eu/information_society/newsroom/cf/fiche-dae.cfm?action_id=186&pillar_id=45&action=Action%2028%3A%20Reinforced%20Network%20and%20Information%20Security%20Policy adresinden erişildi.

European Commission. (2012a). *Action 12: Review the EU data protection rules*. 03 Aralık 2012 tarihinde Digital Agenda for Europe: http://ec.europa.eu/information_society/newsroom/cf/fiche-dae.cfm?action_id=170&pillar_id=43&action=Action%2012%3A%20Review%20the%20EU%20data%20protection%20rules adresinden erişildi.

European Commission. (2012b). *Commission proposes a comprehensive reform of the data protection rules*. 26 Kasım 2012 tarihinde http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm adresinden erişildi.

European Commission. (2012c). *MEMO/12/41*. 07 Aralık 2012 tarihinde http://europa.eu/rapid/press-release_MEMO-12-41_en.pdf adresinden erişildi.

European Commission. (2012d). *How does the data protection reform strengthen citizens' rights?* 05 Aralık 2012 tarihinde http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf adresinden erişildi.

European Commission. (2012e). *Digital agenda for Europe*. 03 Aralık 2012 tarihinde http://ec.europa.eu/information_society/newsroom/cf/pillar.cfm?pillar_id=45&pillar=Trust%20and%20Security adresinden erişildi.

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

European Council. (1992). *92/242/EEC: Council decision of 31 March 1992 in the field of security of information systems*. 02 Kasım 2012 tarihinde http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31992D0242:EN:NOT adresinden erişildi.

European Council. (1995). *Directive 95/46/EC Of The European Parliament and of the Council*. 29 Ekim 2012 tarihinde http://idpc.gov.mt/dbfile.aspx/Directive%2095-46%20-%20Part%202.pdf adresinden erişildi.

European Council. (2001). *Convention on Cybercrime*. 29 Kasım 2012 tarihinde http://conventions.coe.int/treaty/en/treaties/html/185.htm adresinden erişildi.

European Council. (2003). *Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. 06 Aralık 2012 tarihinde http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm adresinden erişildi.

European Council. (2012). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 04 Aralık 2012 tarihinde http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG adresinden erişildi.

Feiler, L. (2011). *Information security law in the EU and the U.S.: A risk-based assessment of implicit and explicit regulatory policies*. 28 Ekim 2012 tarihinde http://fsi.stanford.edu/research/information_security_law_in_the_eu_and_the_us_a_riskbased_assessment_of_implicit_and_explicit_regulatory_policies adresinden erişildi.

Filippi, P. ve Belli, L. (2012). Law of the cloud v law of the land: Challenges and opportunities for innovation. *European Journal of Law and Technology*, 3(2), 1-23.

Helvacıoğlu, A. D. (2004). *İnternet ve hukuk* (Y. M. Atamer, Yay. Haz.). İstanbul: Bilgi Üniversitesi.

Henkoğlu, T. ve Uçak, N.Ö. (2012). Elektronik bilgi güvenliğinin sağlanması ile ilgili hukuki ve etik sorumluluklar. *Bilgi Dünyası,* 13(2), 377-396.

HP. (2011). *2011 Top cyber security risks report*. 06 Kasım 2012 tarihinde http://www.hpenterprisesecurity.com/collateral/report/2011FullYearCyberSecurityRisksReport.pdf adresinden erişildi.

ITU. (2011). *ICT security standards roadmap*. 21 Ekim 2012 tarihinde http://www.itu.int/ITU-T/studygroups/com17/ict/index.html adresinden erişildi.

ITU. (2012). *ITU Activities related to cybersecurity*. 22 Ekim 2012 tarihinde http://www.itu.int/cybersecurity/ adresinden erişildi.

King, N. ve Raja, V. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review*, 28(3), 308-319.

Loop Technology. (2010). *Information security policy review*. 19 Kasım 2012 tarihinde http://www.looptech.com.au/content_common/pg-security-policy-review.seo adresinden erişildi.

Maconachy, W., Schou, C., Ragsdale, D. ve Welch, D. (2001). *A model for information assurance: An integrated approach*. 14 Kasım 2012 tarihinde http://it210web.groups.et.byu.net/lectures/MSRW%20Paper.pdf adresinden erişildi.

McCumber, J. (1991). Information systems security: A comprehensive model. *Proceedings 14th National Computer Security Conference.* Baltimore: National Institude of Standarts and Technology. 18 Kasım 2012 tarihinde http://www.cryptosmith.com/sites/default/files/docs/MccumberAx.pdf adresinden erişildi.

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

Microsoft. (2012). *Microsoft Online Privacy Statement*. 30 Kasım 2012 tarihinde http://privacy.microsoft.com/TR-TR/fullnotice.mspx adresinden erişildi.

Roscini, M. (2010). World wide warfare - Jus ad bellum and the use of cyber force. *Max Planck Yearbook of United Nations Law* (A. Bogdandy, & R. Wolfrum, Yay. Haz.) içinde (ss. 85-130). Netherlands: Brill.

Solomon, M. ve Chapple, M. (2005). *Information security illuminated.* Boston: Jones and Bartlett Publishers.

Sultan, N. (2012). Knowledge management in the age of cloud computing and Web 2.0: Experiencing the power of disruptive innovations. *International Journal of Information Management*, 33(1), 160-165.

Svantesson, D., ve Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review*, 26(4), 391-397.

Symantec. (2012). *Internet security threat report - 2011 trends.* 06 Kasım 2012 tarihinde http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf adresinden erişildi.

TBMM. (2004). *Uluslararasi Telekomünikasyon Birliği Kuruluş Yasası ve Sözleşmesinde Değişiklik Yapan Marakeş Tam Yetkili Temsilciler Konferansı Sonuç Belgelerinin Onaylanmasının Uygun Bulunduğuna Dair Kanun.* 23 Ekim 2012 tarihinde http://www.tbmm.gov.tr/kanunlar/k5163.html adresinden erişildi.

WBO. (2003). *Information security assurance for executives.* Paris: The World Business Organization.

Winter, K. (1997). Privacy and the rights and responsibilities of librarians. *The Katharine Sharp Review, No:4.* 17 Kasım 2012 tarihinde http://mirrored.ukoln.ac.uk/lis-journals/review/review/winter1997/winter.pdf adresinden erişildi.

## Summary

As a result of the development of computer networks, the security and management of information has become more and more complex. While in the 1990s, the security of information in the form of printed materials could be achieved physically, security has now become a more complex, multi-directional, and—most importantly—necessary process for digital information in the 2000s. As a result of this necessity, new information security models, which take into account the characteristics, status, and security issues of information from all aspects, have been developed in order to provide high data security at information centers where huge amounts of information are available. In addition to technical measures, legislation and information security policies integrate security measures taken to provide privacy, integrity, and usefulness of information. Nowadays, the creation of information policies, which is one of the most important issues in information security, has become more and more important for information security models.

In the process of the creation of information security policy, risks and threats like unauthorized access and modification and misuse of data become the most important issues. Because of these risks and threats, both national and international studies on such issues as fighting against malicious code, maintaining the privacy of data, and ensuring security on web-based applications should be carried out corporately. In order to make applicable information security policies, it is necessary to set aside enough money for technical measures, to carry out studies on how to increase user awareness, and to make applicable legislation on these issues. In this study, EU information security policies are examined and evaluated from all aspects

in light of legal regulations, directives, and agreements related to information security, within the framework of the sample information security model and the organizations responsible for making information security policies.

One of the most important elements that has shaped EU information security policies in the last twenty years is the fact that people are anxious about using technology because of the risks of information and communication technologies (ICT); this anxiety in turn retards the economic growth of countries all around the world. Therefore, the creation of multidimensional and comprehensive information security policies should aim to increase the effective use of ICT in economic areas and to revive online economies. To achieve this goal, many directives have been issued and suggestions have been made to protect private data; international agreements have been implemented; and new organizations have been established to ensure international coordination and continuity. While through directives it is possible to ensure the protection of data of individuals and organizations located in the European Economic Area, through international agreements and private organizations a protection system can be created beyond EU borders.

The effectiveness of the directives and agreements formed within the framework of EU information security policies can be seen in the agreements between service providers and their customers. However, due to rapid developments in the use of information technologies, current directives related to data protection are evaluated as insufficient, and efforts to prepare drafts of new directives on data protection continue without interruption. In this study, EU data protection directives, recommendations, agreements, and activities of related organizations are examined in detail in the light of information security policies. This study shows that actions to provide data security have continued and expanded regularly since 1995. In addition, the findings of the study show that current policies are adequate and suitable for the needs of today's world, and this enables individuals in the EU to have higher standards in terms of protection of individual rights.