DERLEME

GELİŞ TARİHİ: 27 ŞUBAT 2021 / KABUL TARİHİ: 25 AĞUSTOS 2021

2010 ANAYASA DEĞİŞİKLİĞİNİN BİLİŞİM SUÇLARIYLA MÜCADELE POLİTİKASI BAKIMINDAN ETKİLERİNİN ANALİZİ VE BU AMAÇLA KURULAN KURULUŞLARIN İNCELENMESİ

Analysis of The Effects of The 2010 Constitutional Amendment in Terms of Cyber Crime Policy and Analysis of the Organizations Established for This Purpose

Hakan YILDIRIM[*] - Volkan KAPLAN[**]

Öz

2010 yılında gerçekleşen Anayasa değişikliği ile ilk kez kişisel verilerin korunması Anayasa metnine girmiştir. Dolayısıyla bilişim suçlarıyla mücadele anlamında Türk kamu politikaları açısından bu değişimin öncesi ve sonrasının değerlendirilmesi özel bir önem arz etmektedir. Önceki mevzuatımızda bilişim suçlarıyla mücadele ile ilgili hükümler mevcuttur. Ancak ilk defa en üst norm olan Anayasamızda bir değişiklik sonucu yer almış ve hem de bu değişiklik bir halk oylaması (referandum) ile olmuştur. Günümüzde bilişim suçlarıyla mücadele, hükümetler ve kamu idarelerince yönetilmesi gereken bir olgudur. Bilişim suçlarının ilk defa görülmeye başlandığı yıllarda doğrudan polisiye yöntemlerle bu suçlarla mücadele edilmiştir. Ancak giderek artan bilişim temelli suç oranları ve bunların toplumda meydana getirdiği huzursuzluk ve etki gücü konuyu toplumsal bir sorun haline getirmiştir. Bu alanda kamu politikası belirlemek de zorunluluk haline gelmiştir. Bu olgu özetle 'polisiye tedbirlerden politikalara dönüşüm' olarak adlandırılır. 2010 Halkoylaması (referandum) ile Anayasamızda yer alan değişiklikler sonucu bilişim suç-

Abstract

With the Constitutional amendment made in 2010, the subject of protection of personal data was included in the Constitution text for the first time. Therefore, regarding combating cybercrimes, the evaluation of this change before and after is of special importance in terms of Turkish public policies. Previously, there were provisions regarding the fight against IT Crimes in our legislation. However, for the first time, it took place as a result of an amendment in our Constitution which is the highest norm, and this change was made by a referendum. Today, the fight against cybercrimes is a phenomenon that should be managed by governments and public administrations. In the years when IT Crimes started to be seen for the first time, these crimes struggled with direct police methods. However, the increasing rates of informatics-based crime and the unrest and power of influence caused by these in the society have made the issue a social problem. It has also become a necessity to determine a public policy in this area. This phenomenon is called "transformation from police measures to policies" in summary. As a result of the

[*] Dr. Öğretim Üyesi, Antalya Akev Üniversitesi, hakanyildirim72@gmail.com, ORCID: 0000-0002-5959-2691

[**] Bağımsız Araştırmacı, volkankaplan@gmail.com, ORCID: 0000-0002-1979-319X

larıyla ilgili olarak devlet kurumlarının yapısal ve işlevsel olarak çok önemli değişiklikler olmuştur. Yeni ihdas edilen birimler olduğu gibi var olan kurumlarda ise isim ve görev değişiklikleri görülmüştür. Yeni kurulan kamu organları bir politika değişikliğinin de göstergesidir. Örneğin Kişisel Verileri Koruma Kurumu'nun kurulması için gerekli kanun, 2010 Anayasa Değişikliğinden 4 yıl sonra, 2014 yılında tasarı haline getirilerek TBMM Başkanlığına sunulmuştur. 24 Mart 2016 tarihinde yasalaşmıştır. Ancak kurumun faaliyete başlaması 2017 yılını bulmuştur. Bu sırada doğrudan veya dolaylı olarak kişisel veri güvenliğini ilgilendiren başka kurumlar da kurulmuş veya var olan kurumların görev alanları kişisel veri güvenliği kavramını ilgilendirecek şekilde genişletilmiştir. Bu yazıda 2010 yılı Anayasa değişikliğinden sonra, başlıca bu değişikliğe bağlı olarak meydana gelen değişiklikler kamu politikaları bağlamında ele alınmıştır.

Anahtar Kelimeler: Bilişim Suçları, Siber Suçlar, Kamu Politikası Analizi

changes in our Constitution with the referendum of 2010, there have been very important changes in the structure and function of state institutions regarding Information Crimes. There have been changes in the names and duties of the existing institutions as well as the newly created units. For example, the law required for the establishment of the Personal Data Protection Board was brought into a draft form in 2014, 4 years after the 2010 Constitutional Amendment, and submitted to the Presidency of the Turkish Grand National Assembly. It became law on March 24, 2016. However, it was not until 2017 that the institution started its operations. Meanwhile, other institutions that are directly or indirectly related to personal data security have been established or the duties of existing institutions have been expanded to concern the concept of personal data security. In this article, the changes that occurred after the Constitutional amendment in 2010, mainly due to this amendment, are discussed in the context of public policies.

Keywords: IT Crimes, Cyber Crimes, Public Policy Analysis

1. GİRİŞ

Günümüzde bilgi ve iletişim teknolojileri, sosyal ve ekonomik hayatın vazgeçilmez bir parçası haline gelmiştir. Kamu hizmetlerinin ise ayrılmaz bir parçasıdır. Özellikle internet, bireysel kullanımdan, kamu kurumlarına ve şirketlere kadar geniş bir yelpazede bilişim teknolojileri ve internet insan hayatının büyük bir bölümünü kapsamakta ve vazgeçilmez bir rol üstlenmektedir.

Bilişim teknolojileri ve özellikle internetin varlığı her geçen gün artmakta ve insan hayatını kolaylaştırma adına önemli katkılar vermektedir. İnternetin toplumun her katmanında yaygınlaşması, güvenlik boyutunda da yeni kaygıların gelişmesine sebep olmuştur. Her geçen gün internet dünyasının yeni teknolojik, sosyal ve hukuksal sorunları ortaya çıkmaktadır. İnternetin küresel manada yaygınlık kazanması ise mekân kavramı bir anlamda ortadan kaldırmıştır. Yeni dijital dünyada, fiziksel temas olmaksızın veya mağdurla aynı mekânı paylaşmaksızın uzak mesafeden bile hırsızlık, dolandırıcılık ve kişisel verilerin ihlali gibi suç fiilleri mümkün hale gelmiştir. Özellikle organize suç örgütleri, terör örgütleri ve art niyetli kişiler gelişen bu teknolojiyi yakından takip etmektedir. Dijital dünyanın siber terörizmini ve daha karışık yeni suç türlerini kendi çıkarları için kullananlar; bireyleri, kurumları ve hatta devletleri mağdur edebilmektedir. Ülkelerinin tecrübelerinden de istifade etmek suretiyle gerekli önlemlerin alınması ile birlikte yeni bir güvenlik konsepti olan Bilişim Suçlarına karşı izlenecek politikaları belirleyen siber güvenlik anlayışının geliştirilmesi büyük önem taşımaktadır.

Bilişim Suçlarıyla mücadele kamu politikasının 2010 Anayasa değişikliği ile birlikte çeşitli açılardan etkileri olmuştur. Anayasa değişikliği, ulusal uygulamaların, bilişim suçlarıyla mücadele aktörleri ve mağdurları yönünden değişmesine neden olmuştur.

Kamu politikası geliştiricileri aldıkları kararları ve geliştirdikleri politikaları etki analizi ve geri besleme yöntemleri ile ölçebilirse bu durum yeni gelişecek politikalara da ışık tutacak en azından eksik veya yanlışlar varsa düzeltilebilecektir.

Teknolojinin hızlı değişimi ile birlikte bilişim suçları mücadelesi, dünyaca kabul edilen ve tarafları doğrudan etkileyen yasaların ve uygulamaların yürürlüğe girmesi ile değişmektedir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile Kişisel Verileri işlenen bireyler hakkında uygulanan kanun bilişim suçlarıyla mücadele kapsamını değiştirmektedir. Bu makalede bireysel, örgütsel veya ulusal bilgilerin ve bilgi iletişim sistemlerinin güvenliğine yönelik saldırıları ve tehditleri kapsayan "bilişim suçları" ve bunlara karşı, Türkiye'nin 12 Eylül 2010 Anayasa değişikliği öncesi ve

sonrası bilişim ile mücadele politikaları incelenmiş ve karşılaştırılmıştır. Türkiye'de Bilişim Suçlarıyla Mücadele Kamu Politikasının 2010 Anayasa değişikliği öncesi ve sonrası karşılaştırılmış, bilişim suçlarıyla mücadeleyi etkileyen kamu politikaları merkeze alınmıştır.

Bilişim suçları ile mücadele alanında farklılıklar incelenirken birey, grup, sistem ve düzeyler arası kıyaslamalar kullanılmıştır. Sanal alemin ve bilişim suçlarının önlenmesi adına geliştirilen kamu çalışmamızda sıklıkla yer alan kavramlardan ikisi bilişim suçlar ile siber suçlarıdır. Ancak doğası gereği bu kavramlar iç içedir. Gerek konuyu kavramsal olarak sarihleştirmek ve gerekse de çalışmanın izahı açısından bu kavramların kullanımı şu şekildedir: *Siber Suç*; bilişim sistem güvenliği ve kullanıcısını hedef alan bilişim sistemi vasıtasıyla işlenen suçlar olarak tanımlanırken, *Bilişim Suçu*; bilgisayar ağı kullanılarak işlenen suç olarak tanımlanmaktadır.

Bilişim suçlarının uluslararası ve ulusal hukuktaki durumu, bu suçlarla mücadele politikalarının temel prensipleri ortaya konulmuştur. Bilişim suçları ile mücadeleye yönelik Türk Kamu Politikasında 12 Eylül 2010 Anayasa değişikliği ile hayatımıza giren ve önemli rol alan Kişisel Verileri Koruma Kurumu, Siber Güvenlik Kurulu, Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Bilgi Teknolojileri İletişim Kurumu, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Emniyet Genel Müdürlüğü, Milli İstihbarat Teşkilatı ve Türk Silahlı Kuvvetleri gibi önemli aktörler ve bunların konumları incelenerek Türkiye bağlamında konuyla ilgili genel bir değerlendirme yapılmıştır.

2. KAVRAMSAL ARKA PLAN

Özel hayatın gizliliği ve mahremiyet gibi kavramlar yeni kavramlar değildir. Uzun bir geçmişe sahiptir ve yasal düzenlemelerle koruma altına alınmıştır. Ancak internetin ve yeni nesil bilgi ve iletişim araçlarının yaygınlaşması sonucu bu mahremiyet alanının daha önce görülmedik şekilde ihlali kafa karışıklıklarına sebep olmuştur. Mevcut düzenlemeler yetersiz kalmıştır. Telekomünikasyon alanında yapılan düzenlemeler yönetmelik ve yönerge düzeyinde kalmıştır.

Kişisel bilgilerin korunması yönünde ortaya çıkan bu eksikliklerin giderilmesi için 2010 yılında yapılan halk oylaması ile Anayasanın 20. maddesine bir fıkra eklenmiştir. Böylece ilk kez kişisel mahremiyet alanı anayasal güvenceye kavuşmuştur.

İlgili fıkra şöyledir; *'Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultu-*

sunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.' hükmüne yer verilmiştir. (Oğuz, 2018)

İlgili Anayasa hükmüne göre;

1. Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu anlamda bireyler temel olarak, kendileri ile ilgili kişisel verilerin ilgisiz üçüncü kişilerin eline geçmemesi konusunda gerekli tedbirlerin alınmasını isteme hakkına sahiptirler.

2. Anayasa metnine dercedilen bu hakkın kapsamı kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme olarak belirlenmiştir.

3. Yine aynı kapsamda kişisel verilerin işlenebilmesi ancak kanunda öngörülen hallerde veya kişinin açık rızası ile mümkün hale gelmiştir. Bunun dışında kalan durumlarda ya da bireyin kendisine ait kişisel verilerin işlenmesi yönünde açık bir irade beyanının olmaması durumunda kişisel verilerin işlenebilmesi açık bir Anayasa ihlali haline gelmiştir. (Kişisel Verileri Koruma Kurumu, 2018)

Şüphesiz 2010 yılında gerçekleşen Anayasa değişikliğinin ardından kişisel veri güvenliğinin anayasal bir güvenceye alınmış olması tek başına yeterli değildir. Bu değişikliklerin uygulanabilir olması gerekli alt düzenlemeleri ve kurumsal değişikliklerin yapılması gerekmiştir. Ancak kamu alanında yapılacak değişikliklerin köklü, etkili ve sürekli olabilmesi için öncelikle kamu politikalarının belirlenmesi gerekmektedir.

Kamu politikası, politika aktörleri tarafından geliştirilen istikrarlı ve belirli bir hedef merkezli karar verme sürecinin sonucudur (Anderson, 1990). Kamu politikası kamunun isteklerine ve beklentilerine cevap niteliğinde olan bir tercihtir. Olumlu/olumsuz aksiyonları birlikte içerebilir. Geliştirilen ve uygulanan politikadan toplumun bir kesimi olumlu, bir diğer kesimi de olumsuz etkilenebilir. En ideal politika yaklaşımını, çözümünü ve/veya adımını atabilmek karar verme mekanizmalarının buradaki süreci ne derece etkili bir şekilde yönetildikleri ile doğru orantılıdır. Aynı zamanda üzerinde çalışılan politikanın da başarısını etkileyebilmektedir. Karar sürecinin yönetilmesi sırasında atılan (ya da atılmayan) adımlar ise, kamu politikası için yaptığı tanımdaki karar vericilerin yaptığı ya da gerçekleştiremedikleri şeklinde anlaşılmalıdır. (Dye, 2002)

Politika geliştirilmesi aşamasında en uygun yaklaşımın geliştirilebilmesi için toplumun ortak müştereklerinin belirlenebilmesi ve politika problemleri için alternatifli düşünebilme gerekmektedir. Bu bakımdan, uygulanabilir bir kamu politikası toplumun nabzını mümkün olan en üst düzeyde tutabilmeli ve onların ihtiyaçlarını ve isteklerini karşılayabilen en uygun alternatifleri hazırlayabilmelidir. Bununla birlikte karar verme mekanizmasında bulunanların kendi norm ve değerlerinden tamamen soyutlanarak bir kamu politikasına karar vermeleri de çok zordur. Bu nedenle; bir kamu politikası ürünü siyasilerin öznel tutumları ile doğrudan ilintili olabilir, etkilenebilir ve şekillenebilir (Çavuş, 2008). Kamu politikasının yukarıda tanımı ve özellikleri dikkate alındığında, karar vermeden daha kapsamlı ve geniş bir kavram olduğu anlaşılmaktadır.

Güçlü sosyal unsurların etkisiyle kamu politikasını geliştirmek ve uygulamak, politika analistinden ziyade karar vericinin görevidir. Bir politika analisti aslında bir karar verici değildir. Karar vericiye yardımcı olmak için nitelikli veriler sağlamak ilke olarak politika analistinin görevidir. Politika analisti tarafından nitelikli veri olarak sunulan öğeler bazen çok karmaşık ve hatta zıt olabilir. Çünkü bir kamu politikasını etkileyen tüm olası faktörleri dahil etmek genellikle mümkün değildir (Nacak, 2014). Sosyal bilim araştırma yöntemlerinin sınırlamalarına ek olarak karışıklık artabilir. Bu bağlamda, politika analizinin sonucunun ne kadar net olduğu önemli olmasa da karar vericilerin kendi durumları altında kararlar almak için öznellik ve tarafsızlık arasında en uygun kararı vermeleri gerekir.

Kamu politikası belirlemesi gereken bu alan bilgi ve iletişim teknolojilerinin büyük bir hızla gelişmesi ve hayatımızın her alanına girmesi sonucu tehdit altına giren kişisel veri güvenliği ile ilgilidir. Bireylerin evlerine girerek fiziksel bir dosyayı almak ne kadar zor ise elektronik ortamda bulunan bilgilerine erişmek ve bunların istismarı ise bir o kadar kolaydır. Bu bakımdan öncelikle bilişim (bilgi ve iletişim) teknolojilerinin kişisel veri güvenliğini ilgilendiren kamu politikalarının belirlenmesindeki rol ve boyutlarının anlaşılması ve ele alınması gerekmektedir.

Bilişim teknolojileri her türlü mekanik hesaplama ve bilgiyi analiz etme ve elektronik cihazlar vasıtasıyla düzenli olarak işlemeye dayanır. Bilişimciler elde edilen bilgileri oluşturur, tanımlar ve kullanılabilir formlara dönüştürür. Süreç ifadelerini algoritmik olarak bir temele oturtur ve karmaşık sistemler tasarlarlar ve soyutlamaları formüle ederler (Alan, 2019). Temelde hesaplamanın ve bilginin teorik temeli olarak tanımlanabilir olması, bilginin uygulanması ve kurulumunu ve pratik tekniklerle hesaplamayı ele alan bilim dalıdır. Bilişim, donanım ve yazılım olmak üzere iki alt bölüme altında incelenmektedir. Donanım alt başlığından bilgisayarların yapımı fiziksel geliştirilmesi anlaşılırken, yazılım alt başlığından donanımın üzerin-

de çalışacak programlar ve algoritmalar anlaşılmaktadır. Bilgisayarın ve dolayısıyla bilişim teknolojileri alanındaki gelişmeler donanım ve yazılım alanındaki rekabet ile ilerleme kaydetmiştir. Donanım üzerinde çalışacak yazılımlar geliştirilirken, yazılımların donanım teknolojisinin sınırlarını zorlamasıyla gelişme hız kazanmıştır.

Donanım ve yazılım teknolojilerinin gelişmesiyle internet, internetin gelişmesiyle sosyal medya yazılımları ortaya çıkmıştır. İnternet ve sosyal medya ile birlikte bilişim suçları da farklı bir boyut kazanmıştır. Eskiden suç işlemek için fiziksel olarak ulaşılması gereken cihazlar, internetin tüm dünyayı bir ağ gibi sarmasından sonra daha ulaşılabilir hale getirmiştir. Bilişim alanındaki gelişmelerle modemlerin taşınabilir hale gelmesi ve mobil cihazların yaygınlaşması ile birlikte kontrol mekanizmaları azalmış ve suç daha kolay işlenebilir hale gelmiştir. Bilişim üzerinden işlenen suç bireye, topluma ve devlete karşı kanun ile yasaklanmış fiiller olarak karşımıza çıkmaktadır (Bahar, 2018).

Bilişim suçlarıyla ilgili birçok tanım bulunmaktadır ve ülkemizde "internet suçları, siber suçlar, bilgisayar suçları, dijital suçlar, yüksek teknoloji suçları" vb. olarak da tanımlanmaktadır. Başka ülkelerde bu suçlara Siber Suçlar, Bilgisayar Suçları, Ağ Suçları, Bilişim (Bilgi Teknolojileri) Suçları, isimleri verilmiştir (Tulum, 2006). Bu çerçevede, bilişim sistemlerine ilişkin suçlar bu tezde "bilişim suçları" olarak adlandırılmaktadır. Teknolojinin gelişmesiyle artan bilişim suçları, "teknoloji yardımıyla ve genellikle sanal ortamda kişi veya kurumlara maddi veya manevi zarar vermek" olarak açıklanabilir.

Güvenlik sorunlarıyla mücadele etmek için "Adli Bilişim" konusu günümüzün olmazsa olmazlarından biridir. Dijital delillerin mahkemeler ve soruşturma birimleri tarafından delil olarak değerlendirilebilmesi için belirlenen kurallara göre uygun koşullarda toplanması, saklanması ve incelenmesi gerekmektedir. Adli bilişim, soruşturma birimi için dijital kanıtların hazırlanmasında ve sunulmasında, bütünlüğünün ve güvenilirliğinin sağlanmasında da çok önemli bir rol oynamaktadır (Başlar, 2020).

Alınacak önlemler sadece enstitülerin veya özel şirketlerin endüstriyel kontrol sistemleri için değil, aynı zamanda ulusal kritik altyapıların güvenliğini sağlamak ve korumak için de önemlidir. Ulusal güvenlik bağlamında siber güvenliğin böylesine bir risk potansiyeli barındırması ona yönelik politikaların benimsenmesini gerekli kılmaktadır. Sanal ağların resmî kurumlar için vazgeçilmez hale gelmesi, bu sistemlerin her an saldırılara maruz kalma riskini artırmaktadır. Özellikle son yıllarda The National Aeronautics and Space Administration – NASA (Amerikan Havacılık ve Uzay Ajansı), North Atlantic Treaty Organization - NATO (Kuzey

Atlantik işbirliği Paktı) ve benzeri kuruluşlara yapılan saldırılar sonucunda sistemler ciddi zararlar görmüştür. Bazı büyük BT kuruluşlarına ait siteler tahrip olmuş ve kullanılamaz hale getirilmiştir.

Bilgi güvenliği yetkisiz kişilerin erişiminden, ifşa edilmesinden, imha edilmesinden, değiştirilmesinden veya yetkisiz kişilerin bilgisine vereceği zararlardan korunma işlemidir. Buna göre, siber alemin güvenli olması için bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak gerekir (Hekim ve Başıbüyük, 2013). Bilgi güvenliğini etkileyen üç kavram öne çıkmaktadır. Gizlilik, bilgi sistemleri ve bilgilere yalnızca yetkili kişiler veya sistemler tarafından erişilebilir veya değiştirilebilir olmasıdır. Erişilebilirlik, gerekli olduğunda yetkili kişilerin erişebileceği depolanmış bilgiye duyulan ihtiyacı açıklar. Bütünlük, bilgi sistemleri aracılığıyla depolanan bilgiler değiştirilemez, kısmen veya tamamen silinemez veya imha edilemez demektir. Ticari amaçlı kişisel bilgilere (kimlik bilgileri, kredi kartı bilgileri vb.) yönelik siber saldırıların artmasıyla, bulut bilişim gibi bilgi iletişim ve paylaşım hizmetlerinin güvenlik riskleri ortaya çıkmıştır. Sektördeki hızlı gelişme nedeniyle artan bilgi iletişim teknolojileri; bilgi güvenliğinin sağlanması çerçevesinde kişisel verilerin korunması konusunu en çok tartışılan konular arasına girmiştir (Henkoğlu ve Yılmaz, 2013).

Günümüzde bireysel ve kurumsal anlamda sosyal, ekonomik-ticari, eğitim gibi pek çok alanda iş ve işleyişler giderek artan bir oranda sanal aleme geçmektedir. En az birkaç yönüyle bilişim teknolojilerine ve internete bağımlı olmayan bir sektör kalmamıştır. Bireysel alanda ise bu durum kendisini "ekran bağımlılığı" olarak göstermektedir. O kadar ki cep telefonları günlük kullanım oranlarını raporlamakta; araştırmalar ise bireylerin ekran bağımlılığının giderek arttığını ortaya koymaktadır. Öte yandan en hızlı büyüyen suçların başında ise siber alemde meydana gelen, siber dolandırıcılık, kimlik hırsızlığı, siber saldırılar ve sınır aşan suçlar gibi konuların geldiği görülmektedir. En kısa ve net ifadesi ile doğrudan veri ve bilgileri korumaya yönelik kavramsal bakış "bilgi güvenliği" kavramı altında ele alınmaktadır. Siber güvenlik alanı baş döndürücü bir ivmeyle değişmektedir. Öyle ki, Endüstri 4.0 veya 4. Sanayi Devrimi olarak tanımlanan gelişmelerden ilham alan "Siber Güvenlik 4.0" teriminin kullanımı bile güncellenmiştir. Endüstri 4.0, birçok modern otomasyon sistemini, veri alışverişini ve üretim teknolojisini içeren bir terimdir. Terim, siber-fiziksel sistemlerden oluşan bir dizi değeri ifade etmektedir. Nitekim Endüstri 3.0 sürecinde elektronik bilgi teknolojilerinin devreye girmesiyle başlayan kamu hizmeti üretim alanları ve bu alanların kritik altyapılarının oluşturulması ve korunması sürecinde devletler ve hükümetler büyük ölçekli önlemler almak zorunda kalacaklardır (Kutlu, Kahraman ve Dinçer, 2019)

Bilişim teknolojilerinin ve buna bağlı olarak iletişim imkanlarının artmasıyla bu alanda gelişen suç kavramı da farklı bir boyut almıştır. Hükümetlerin bilişim teknolojileri konusunda geliştirmekte oldukları kamu politikalarının isabet kaydetmesi ve sonuç verebilmesi kavramın doğru anlaşılmasına bağlıdır. Bu alandaki kavramların ifade ettikleri ile birlikte etki alanlarının da doğru tespit edilmesi gerekmektedir. Yapılan her bir değişiklik farklı alanları etkilediğinden ve sonuçlar ön görülmediğinden neticeleri çoğu zaman öngörülmemektedir.

Türkiye'de, bilişim suçları ile mücadele Devlet Güvenliği (Siber Savunma) odaklı birimler ve Kolluk Odaklı (Suç Tespit/Önleme) birimler tarafından icra edilmektedir. Özellikle kolluk odaklı çalışan Emniyet Genel Müdürlüğü bünyesinde bulunan Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığında mücadele şu şekilde başlamıştır: Bir daire başkanlığı bünyesinde Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü adı altında başlayan mücadele Bilişim Suçları ve Sistemleri Şube Müdürlüğüne dönüşmüştür. Sonrasında Emniyet Genel Müdürlüğüne bağlı olarak Bakanlar Kurulu Kararıyla Siber Suçlar Dairesi Başkanlığı olarak müstakil bir daire başkanlığı kurulmuş ve daha sonra Siber Suçlarla Mücadele Daire Başkanlığı olarak adı değiştirilmiştir. 2012 ve sonrasındaki bilişim suçları ile mücadele istatistikleri Emniyet Genel Müdürlüğü Stratejik faaliyet raporlarındaki sayıları yansıtmaktadır.

Emniyet Genel Müdürlüğünün siber suçlara ilişkin tuttuğu 2019 yılı istatistiklerine Tablo 1'de yer verilmiştir. Buna göre banka ve kredi kartı dolandırıcılığını da içinde barındıran ödeme sistemleri suçları ve çocuk istismarı suçları en sık rastlanan suç kategorilerini oluşturmaktadır. Yakalanan şüpheli sayılarında ise çocuk istismarı suçları ve ödeme sistemleri suçları başarının yüksek olduğu ve ön plana çıktığı alanlar olarak görülmektedir.

Tablo 1: 2019 Yılı Siber Suçları Olay ve Yakalanan Şüpheli Sayıları

Suç Türü	Olay Sayısı	Yakalanan Şüpheli Sayısı
Bilişim Suçları	10.260	541
Ödeme Sistemleri Suçları	21.978	3.590
Çocuk İstismarı Suçları	16.067	6.388
Yasadışı Bahis Suçları	1.546	1.926
Toplam	49.851	12.445

Kaynak: Emniyet Genel Müdürlüğü 2019 Yılı Faaliyet Raporu Siber Suçlar ile Mücadele Bölümü

2.1. İLGİLİ DÜZENLEME VE AKTÖRLER

2.1.1. Elektronik Haberleşme Güvenliği Yönetmeliği

Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan Elektronik Haberleşme Güvenliği Yönetmeliği 2008 yılı içerisinde yürürlüğe girmiştir. Bu Yönetmelik ile Bilgi Güvenliği Yönetim Sistemi standardı olan TS ISO / IEC 27001 veya ISO / IEC 27001 standardına uyma zorunluluğu, elektronik iletişim hizmeti veren ve elektronik iletişim altyapısı işletenlere uygulanmıştır. Bilgisayar Olaylarına Acil Müdahale Merkezi – BOME'nin kurulması ve operasyonel kabiliyet kazanması ile birlikte elektronik ortamda suç işlemeye yönelik eylem ve saldırılar önceden tespit edilip bunlara karşı önlemler alınabilmektedir ve bu yönetmeliğe uymayanlara cezai müeyyideler uygulanmaktadır. (Elektronik Haberleşme Güvenliği Yönetmeliği, 2008). Elektronik haberleşme güvenliği yönetmeliği 2010 yılı anayasa referandumu öncesi önemli bir kamu politikası uygulama aracı olmakla birlikte diğer tamamlayıcı yasal düzenlemeler ile birlikte etkili bir rol oynamıştır.

2.1.2. Bilgi Toplumu Stratejisi Eylem Planı

2006 yılında yürürlüğe giren eylem planı Millî Savunma Bakanlığı, İçişleri Bakanlığı, Devlet Planlama Teşkilatı (DPT), Türkiye Bilimsel Teknik ve Araştırma Kururmu (TÜBİTAK) ve ilgili kamu kurum ve kuruluşları tarafından uygulanmıştır. Bilgi Toplumu Stratejisi, yapısal ve ekonomik bir dönüşüm süreci yaşayarak "bilgiye dayalı ekonomi" sürecinde gelişmiştir. Bu sürecin başlıca yapısal özellikleri; üretimdeki bilgi ve iletişim teknolojilerine dayalı hizmetlerin ileri teknoloji, Ar-Ge ve yaşam boyu eğitimdir.

2.1.3. 5237 Sayılı Türk Ceza Kanunu

Türkiye'de ayrı bir bilişim ya da siber suçlar yasası mevcut değildir. Bu nedenle ilgili düzenlemeler genellikle olan 5237 sayılı Türk Ceza Kanunu'nda (TCK) ele alınmış ve elektronik ağlar vasıtasıyla işlenen klasik suçlar olarak zikredilmiştir. 2005 yılında yapılan yeni TCK'nın düzenlenmesinde, gelen eleştiriler dikkate alınarak korudukları hukuksal değer bakımından ilgili oldukları bölümlerde benzer suç tipleri ile birlikte değerlendirdikleri görülmektedir (Dülger, 2012). TCK'da bilişim suçları ile beraber bilişim sistemleriyle işlenebilecek suçlar da tasnif edilmiştir. Bundan doğrudan bilişim sistemlerinin hedef alındığı suçlar ile bilişim sistemlerinin suç işlemek için vasıta olarak kullanıldığı suçlar ayrımı da çıkabilmektedir. Elektronik ağlara ilişkin suçlarda ise TCK'da Onuncu Bölüm olarak "Bilişim Ala-

nında Suçlar" başlığı altında ele alınmıştır. TCK Onuncu Bölüm 'de bilişim sistemine girme fiilini tanımlayan 243. maddeyle başlamaktadır.

2.1.4. 5271 Sayılı Ceza Muhakemesi Kanunu

Ceza muhakemesi kanunun 134. maddesi, bilgisayarların, bilgisayar programlarının ve dosyalarının aranması, kopyalanması ve ele geçirilmesi, şüpheli ve bilgisayar dosyalarının kullandığı bilgisayar ve bilgisayar programlarının aranması, bilgisayar kayıtlarından kopyalanması, bu kayıtların kodunun çözülmesi ve metne dönüştürülmesi gerektiğini öngörülmektedir. Başka bir şekilde kanıt/delil elde etmek için bir fırsat bulunmaması halinde, bu kararlara hâkim tarafından karar verileceği ifade edilmektedir. Bilgisayar veya bilgisayar dosyalarının ele geçirilmesi sırasında, sistemdeki tüm veriler yedeklenmelidir. Bu madde bağlamında gerçekleştirilen incelemelerin ve prosedürlerin orijinal kanıtların bir kopyası ile yapıldığı bilinmektedir. Bu bağlamda, orijinal kanıt ile görüntünün özet çıktı değerlerinin aynı olması, kanıtlarda müteakip bir değişiklik olmadığı anlamına gelir. Bu bağlamda, söz konusu kanıt toplama işleminin bazı eksiklikleri ve hatalara konu olabileceği uzmanlar tarafından ifade edilmektedir. (Hekim ve Başıbüyük, 2013).

2.1.5. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun

Bu yasa, içerik sağlayıcıların, yer sağlayıcıların, erişim sağlayıcıların ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını ve içerik, konum ve erişim sağlayıcıları aracılığıyla internet ortamında işlenen belirli suçlarla mücadeleye ilişkin ilke ve prosedürleri düzenlemektir. 5651 sayılı İnternet Üzerinden İşlenen Suçların Düzenlenmesi ve Mücadelesi Hakkında Kanuna ek olarak 21 Temmuz 2020 tarihinde yurtdışında faaliyet gösteren içerik, yer veya erişim sağlayıcısına uygulanan idari para cezaları ve sosyal ağ sağlayıcılarının tanımlanması konusunda değişiklik yapılmıştır. Yapılan değişiklik ile birlikte erişim engelleme kararlarında ihlal edilen kişilerin haklarının ortaya çıkması durumlarında suçu oluşturan kısmi içeriklerin kaldırılması mümkün olabilmektedir. Türkiye kaynaklı olarak, günlük bir milyondan fazla içeriği olan yabancı kaynaklı sosyal ağ sağlayıcısının, Türkiye'deki temsilciyi belirlemesi ve bu yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcılarına uygulanacak yaptırımların belirlenmesi için kırk sekiz saatlik istatistiki ve kategorik olarak başvurulara cevap verilmesi zorunluluğu getirilmiştir. Cevap

başvuruları ile Türkçe olarak altı aylık dönemlerde bilgi içeren raporların hazırlanması ve raporlanması yükümlülüğünün sağlanması amaçlanmaktadır (Resmî Gazete Sayı 31202, 2020).

2.1.6. 5070 Sayılı Elektronik İmza Kanunu

Teknolojinin gelişmesi ile birlikte ticarete de olumlu yansımalar olmuştur. Bireyler veya kurumlar birbirlerini görmeden internet üzerinden alışveriş yapabilir hale gelmiştir. Bununla birlikte, anlaşmanın yerine getirilmesi için belirli koşulların sağlanması gerekmektedir. Yasal koşullarda ticaretin gerçekleşmesi için elektronik imza kavramı ortaya çıkmıştır. 5070 sayılı Elektronik İmza kanunu 23 Ocak 2004 tarihinde Resmî Gazete' de yayınlanmış ve 23 Temmuz 2004 tarihinde uygulanmaya başlanmıştır. Elektronik imza ıslak imza yerine geçmekte ve her türlü dijital işlemde kâğıt ve zaman tasarrufu sağlamaktadır. Elektronik imza kamu, bankacılık, sigorta, e-ticaret başta olmak üzere birçok alanda geçerliliğini ispatlamış ve ciddi depolama maliyetleri tasarrufu sağlamıştır.

2.1.7. Kişisel Verilerin Korunması Kanunu

Sosyal ve ekonomik yaşamı sürdürmek, kamu hizmetlerini etkin bir şekilde sağlamak, ekonominin gereksinimlerine uygun olarak mal ve hizmetleri geliştirmek, dağıtmak ve pazarlamak kaçınılmaz olsa da kişisel verilerin art niyetli olarak toplanması veya kötüye kullanılması sonucu kişisel hakların ihlali kaçınılmazdır (Mutlu, 2019). Tüm AB üye ülkelerdeki kişisel verilerin aynı standartlarda korunması ve karşılıklı standartların oluşturulması amacıyla Avrupa Konseyi tarafından hazırlanan, Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunmasına Dair 108 sayılı Sözleşme hazırlanmıştır. Sınır veri akışı ilkeleri, ülkemiz tarafından 28 Ocak 1981 tarihinde imzaya açılmıştır ve imzalanmıştır (Bozkurt, 2019). Anayasa hükmünde yasa ile izin verilen durumlarda kişisel verilerin işlenebileceği ön görülmesine karşın, özel sınırlama hallerine yer verilmemiştir. Bu nedenle 26 Aralık 2016 tarihinde verilen kanun tasarısının kabulü üzerine "Kişisel Verilerin Korunması Kanunu", 24 Mart 2016 tarihinde yasalaşmış ve 7 Nisan 2016 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

2.1.8. Cumhurbaşkanlığı İletişim Merkezi - CİMER

Önceleri Başbakanlık İletişim Merkezi (Bimer) ve (Cimer) olarak iki ayrı platformda hizmete girmiş ve elektronik yolla yapılan dilek, istek, şikayetlerin yapılabi-

leceği bir portaldir. 2017 Anayasa referandumunun ardından Başbakanlık kalktığı için Bimer kalkmış ve sadece Cimer portali olarak hizmet vermeye devam etmektedir. Özellikle ihbar özelliği ile bireyler; kişisel veri güvenliği konusunda yaşayabilecekleri sorunları ilgili devlet kurumlarına ve savcılıklara doğrudan iletebilmektedir. Elektronik yolla yapılan müracaatların da ıslak imzalı müracaatlar gibi muteber kabul edilebilmesi için dilekçe verenin kimliği ve adresinin belli olması gerekmektedir. Ayrıca dilekçe tarihi ve hangi kuruma hitaben yazıldığı gibi hususların da dilekçe üzerinde bulunması gerekmektedir. Sayılan tüm bu hususlar ve daha fazlası zaten otomatik olarak (e-devlet üzerinden ve/veya şifresi ile giriş sağlandığı için) doldurulmaktadır ve şekil şartları sağlanmış olmaktadır.

2.1.9. Devlet Güvenliği (Siber Savunma) Odaklı Birimler

Bilişim suçları konusunda faaliyet gösteren devlet kurumları düşünüldüğünde siber savunma ve suç tespit/önlemeye yönelik olarak birimleri ikiye ayırmak mümkündür. Siber savunmaya yönelik görev icra eden Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Başkanlığı, Milli İstihbarata Teşkilatı (MİT) Elektronik Teknik İstihbarat Başkanlığı, USOM- Ulusal Siber Olay Müdahale Merkezi, SOME- Sektörel Siber Olaylara Müdahale Ekibi ve Genelkurmay Başkanlığı Siber Savunma Komutanlığının görevleri aşağıda anlatılmıştır. Bu kısımdaki birimler ağırlıklı olarak internet trafiğinin denetim ve kontrolünden, bilgi güvenliği, kritik tesislerin bilgi sistem altyapılarının korunmasından sorumludur.

2.1.10. Ulaştırma ve Altyapı Bakanlığı

Bakanlar Kurulu kararı ve Ulusal Siber Güvenlik Stratejisi kararından da anlaşılacağı gibi, karar mekanizması olan siber güvenlik kurulu kararını izleyen en önemli birim,'Ulaştırma ve Altyapı Bakanlığıdır. Bakanlar Kurulu kararının bir sonucu olarak, Ulaştırma ve Altyapı Bakanlığı, ulusal siber güvenliğin sağlanması için politikalar, stratejiler ve eylem planları hazırlama görevini üstlenmiştir (Kurnaz ve Önen, 2019). Bakanlık, bilgi toplumuna geçiş sürecini hazırlamak, yeni teknolojilerin geliştirilmesi ve genişletilmesi politikalarının uygulanmasını hızlı bir şekilde gerçekleştirmektedir. İnternet okuryazarlığının artırılması, İnternet erişiminin yaygınlaştırılması, elektronik iletişim sektöründe rekabetin sağlanması, ucuz bilgi ve iletişim hizmetlerinin yapılması, dijital yayına geçişin sağlanması, uydu hizmetlerinin iyileştirilmesi, posta hizmetlerinin geliştirilmesi, e-devlet uygulamalarının kapsamının genişletilmesi ve sektörde Ar-Ge faaliyetlerinin yaygınlaştırılmasını bakanlığın başlıca görevlerini kapsamaktadır. (uab.gov.tr, 2018 faaliyet raporu, s.10)

2.1.11. Bilgi Teknolojileri ve İletişim Kurumu – BTK

Bilişim suçları konusunda BTK başta olmak üzere ilgili kamu kurum ve kuruluşları ile özel sektör aktörlerinin de etkin iş birliği ve koordinasyon içerisinde tedbirler almaktadır. E-devlet üzerinden "İnternet İhbar Başvurusu" ile birlikte internette karşılaşılan suç unsuru barındıran içeriklerle ilgili Bilgi Teknolojileri ve İletişim Kurumuna ihbar başvurusu yapılabilmektedir (türkiye.gov.tr, 2020).

2.1.12. Ulusal Siber Olay Müdahale Merkezi – USOM

Telekomünikasyon İletişim Başkanlığı bünyesinde "Ulusal Siber Olay Müdahale Merkezi" (USOM) ve "Sektörel ve Kurumsal Siber Olay Müdahale Merkezleri" (SOME) kurulmuştur. Bu birimler 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın 4. Maddesi uyarınca kurulmuştur. USOM, ülkemizdeki siber güvenlik olaylarına cevap olarak ulusal ve uluslararası koordinasyonu sağlamak amacıyla kurulmuştur. İnternet aktörleri, kolluk kuvvetleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM aracılığıyla gerçekleştirilmektedir. USOM, siber güvenlik olayları için alarmlar, uyarılar ve duyurular yapar ve kritik sektörlere karşı siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlar (usom.gov.tr, 2020).

2.1.13. Sektörel Siber Olaylara Müdahale Ekibi- SOME

SOME, sektörde doğrudan veya dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri almak amacıyla olaylara müdahale edebilecek mekanizma ve olay kayıt sistemlerini kurmak ve kurumlarının bilgi güvenliğini sağlamak için kurulmuştur. Kurumlarının bilgi sistemlerinin kurulmasında, işletilmesinde veya geliştirilmesinde siber kaynaklı olayları önlemek veya azaltmak için SOME teknik ve idari önlemler sağlamaktadır (SOME, 2014). USOM' lar ve SOME'ler, siber olayları ortadan kaldırmak, olası zararları önlemek, azaltmak ve ulusal düzeyde koordinasyon ve iş birliği içinde siber olay yönetimini yürütmek için hayati yapılardır.

2.1.14. MİT Elektronik Teknik İstihbarat Başkanlığı

Elektronik-Teknik İstihbarat Başkanlığı; karşı istihbarat yapmak ve terör faaliyetlerini önlemek, telekomünikasyon yoluyla iletişimi tespit etmek ve dinlemek, sinyal bilgilerini değerlendirmek ve kaydetmek amacıyla kurulmuştur. Başkanlık, ses ve video analizi yapar, görüntü zekâsı oluşturur, şifreli verilerin kodunu çözer

ve siber tehditlere karşı çalışmalar yürütür. Bu görevler MİT Bilim ve Teknoloji Uzmanları görevlerini siber alemde yürütürler. (Söylemez, 2019).

2.1.15. Genelkurmay Başkanlığı Siber Savunma Komutanlığı

Genelkurmay Başkanlığı bünyesinde çalışan kritik alt yapıyı ve komuta kontrol sistemlerini etkisiz hale getirmek için yapılan siber saldırılar, bazı tehdit ve risklerle siber savunmanın önemini artırır. Ulusal güvenlik açısından kara, deniz, hava ve uzay boyutlarına eklenen alan siber alanı, ulusal güvenliğin bir parçası haline gelmiştir. Günümüzün savaş ortamının beşinci boyutu olarak da tanımlanan bu yeni alanda tehditleri önlemek ve gelişmiş savunma alarm ve müdahale sistemleri ile güçlü bir siber savunma yeteneği kazanmak amacıyla 2012 yılında kurulan TSK Siber Savunma Merkezi Başkanlığı, 30 Ağustos 2013 tarihinde TSK Siber Savunma Komutanlığına dönüştürülmüştür (Siber Tehdit, 2016). Siber Saldırılara Karşı Önleyici Hizmet; 7 gün 24 saat hizmet veren Siber Savunma Operasyon Merkezi, TSK sistemlerine yönelik saldırı ve siber olaylar durumunda birçok önleyici faaliyet yürütmektedir. Dünyadaki siber olayların gerçek zamanlı izlenmesine ek olarak, Kara, Deniz ve Hava Kuvvetleri Komutanlığı, "hizmet dışı bırakma", "tespit", "teşhis", "önleme" gibi birçok web sitesi de dahil olmak üzere, Genelkurmay Başkanlığı resmî web sitesinin kontrolünü sağlamaktadır (Siber Savunma Merkezi, 2020)[1].

2.1.16. Kolluk odaklı (suç tespit/önleme) birimler

Kolluk olarak tabir ettiğimiz Emniyet Genel Müdürlüğü Siber Suçlar ile Mücadele Daire Başkanlığı, Jandarma Genel komutanlığı Bilişim ve Teknik istihbarat Başkanlığı ve Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü suçun önlenmesine, suçla mücadele ve suçun tespitine yönelik görev yapmaktadır.

2.1.17. Emniyet Genel Müdürlüğü Siber Suçlar ile Mücadele Daire Başkanlığı

Bilgi teknolojileri kullanılarak işlenen suçların ve dijital kanıtların araştırılmasını destekleyen Siber Suçlar ile Mücadele Dairesi, tekrarlanan yatırımları önlemek ve siber suçlarla etkin ve verimli bir şekilde mücadele etmek için kurulmuştur. İlk olarak, Bilişim Suçlarıyla Mücadele Dairesi olarak kurulmuş daha sonra adı Siber

[1] Türk Silahlı Kuvvetleri Siber Savunma Merkezi - SİSAMER

Suçlar ile Mücadele Dairesi olarak değiştirilmiştir. Gelişen teknolojinin ulusal ve uluslararası arenada kötüye kullanılmasının önlenmesi, bilgi sistemleri kullanılarak işlenen suçlarla etkin biçimde mücadele edilmesi, suçun devam etmesini ve ortaya çıkmasını önlemek başlıca görevlerindendir. Siber Suçlar ile Mücadele Daire Başkanlığı nüfus yoğunluğu bakımından bilişim suçlarının yoğun işlendiği ülke kesiminden sorumludur. Polis bölgesi nüfus yoğunluğunun yüksek olduğu yerleri kapsamaktadır.

2.1.18. Jandarma Genel Komutanlığı Bilişim ve Teknik İstihbarat Başkanlığı

Jandarma Genel Komutanlığı; sorumluluk alanındaki siber olaylarının önlenmesi veya tespiti için faaliyetler yürütmektedir. Jandarma siber birimlerinin görünürlüğü fazla olmamakla birlikte "Siber Suç", "Yüksek Teknoloji Suçu", suç işlenmesini önlemek ve uygulamak, olayları aydınlatmak görevini yerine getirmek için gerekli önlemleri almaktadır. Bu konuların yanı sıra, Siber Terörizm ve terörle ilgili bilgi suçları da bu görevi üstlenmektedir (jandarma.gov.tr,2020).

2.1.19. Sahil Güvenlik Komutanlığı İstihbarat Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü

Sahil Güvenlik, görevleri kapsamında kamu düzenini korumak, suçu önlemek için deniz alanlarına ilişkin egemen hakların korunması vardır. Sahil Güvenlik Komutanlığı'nın görev ve sorumluluk alanı olarak tanımlanan alanda siber suçlarla mücadele için bu birim kurulmuştur.

2.1.20. Siber Güvenlik Kurulu

Bakanlar Kurulunun 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Uygulanması, Yönetimi ve Koordinasyonuna İlişkin Kararı, 20/10/2012 tarihli ve 28847 sayılı Resmî Gazete'de yayımlandıktan sonra yürürlüğe girdi. Bakanlar Kurulunun kararına göre; Siber güvenlikle ilgili alınacak önlemlerin belirlenmesi, planların, programların, raporların, prosedürlerin, ilkelerin ve standartların onaylanması ve uygulanmasının sağlanması için bir Siber Güvenlik Kurulu oluşturulmasına karar verilmiştir. Kurul, ilk toplantısını 20/12/2012 tarihinde gerçekleştirmiştir ve "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" nı uygulamaya karar vermiştir. 16 Ocak 2013 tarihinde yürürlüğe

giren söz konusu Eylem Planında, Siber ortamda ortaya çıkan tehditlerin hızlı bir şekilde tespit edilmesi ve paylaşılması için ulusal düzeyde etkin bir şekilde çalışacak bir Siber Olay Müdahale Teşkilatı ülkemizi etkileyebilecek tehditlere karşı 7/24 müdahale temelinde kurulmaktadır.

2.1.21. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

2012 yılında Bilim Sanayi ve Teknoloji Bakanlığı Bilgi ve İletişim Teknolojileri Kurumu (BTK) koordinasyonunda Türkiye'de siber suçla mücadele sivil toplum kuruluşları ve kurumları ile birlikte yürütülmüştür (USGS 2013-2014). Aralık 2012'de "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" hazırlanmış ve yürürlüğe girmiştir. 20 Ekim 2012 tarihli ve 2012/3842 sayılı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetimi ve Koordinasyonu Hakkında Karar" 28447 sayılı Resmî Gazete'de yayımlanarak Ulaştırma, Denizcilik ve Haberleşme Bakanlığının sorumluluğuna verilmiştir.

2.1.22. Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı

2013- 2014 ulusal siber güvenlik stratejisinin güncellenmesi ve 2016-2019 dönemini kapsayan eylemlerin belirlenmesi ihtiyacı Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yapılan bir çalışmayla tamamlanmıştır. İlk olarak 10 Mart ve 7 Nisan 2015 tarihleri arasında eski eylem planında yer alan kurumlarla değerlendirme toplantıları yapılmıştır. Eski eylem planında yer alan faaliyetlerin gerçekleşme derecesi ve siber güvenlik kapsamında yürütülecek faaliyetler de tespit edilmiştir. Kamu kurumlarını, kritik altyapı operatörlerini, BT sektörünü, üniversiteleri ve sivil toplum kuruluşlarını temsil eden 73 kurum ve kuruluştan 126 uzmanın katıldığı Ortak Akıl Platformu gerçekleştirilmiştir.

2.1.23. Ulusal Siber Güvenlik Stratejisi ve 2020-2023 Eylem Planı Hazırlık Çalıştayı

BTK himayesinde 19 Şubat 2020 gerçekleştirilen çalıştayda ülkemizde ilk olan 2013-2014 Eylem Planı ve sonrasında 2016-2019 Eylem Planları değerlendirilmiştir. Özellikle bilişim suçları ile mücadele politikalarının belirlenmesinde önemli bir yer teşkil eden USOM ve SOME'ler ayrıntılarıyla değerlendirilmiştir. USOM koordinasyonunda çalışan 14'ü Sektörel olmak üzere 1291 SOME Türkiye'nin siber alanının korunmasında yer almaktadır. Çalıştay ile birlikte Türkiye'nin siber güvenliğinin sağlanmasına yönelik 4 yıllık bir perspektif çizilmiştir (BTK, 2020).

Siber güvenlik politikası geliştirmek ve bu politika çerçevesinde uyumlu stratejiler oluşturmak, diğer alanlarda kamu politikası yapmaktan daha zordur. Bu durumun önemli nedenlerinden biri, siber güvenliğin hem dikey hem de yatay eksendeki farklı alanlarla ilişkili olmasıdır. Türkiye de dahil olmak üzere birçok ülke tarafından siber alan; 5. muharebe alanı ya da kara, deniz, hava ve genel kolluktan sonra gelen yeni bir kuvvet olarak ilan edilmiştir. Siber suçlarla mücadele alanı kendi başına bir politikaya tabi olmakla birlikte, siber güvenlik politika tespitinde dijital tabanlı teknolojileri kullanan diğer sektörlerin ve alanların da göz önünde bulundurulması gerekir. USOM ve SOME'lerin kurulması siber güvenliğin çok yönlü yapısından kaynaklanmaktadır. Birçok sektöre ve onun çalışma alanına etkisi olan siber suçlar ile mücadelenin politika geliştirmekteki zorluğu, atılan adımların öngörülemez olmasından kaynaklanmaktadır.

3. 2010 ANAYASA DEĞİŞİKLİĞİ ÖNCESİ VE SONRASI BİLİŞİM SUÇLARIYLA MÜCADELE POLİTİKASININ KARŞILAŞTIRMASI

12 Eylül 2010 Anayasa referandumu ile Anayasa'nın 20. maddesinde kişisel verilerin korunma hakkı anayasal güvence altına alınmıştır. Her ne kadar bundan önce 1982 Anayasası'nın 17. Maddesi ile kişi dokunulmazlığı ve 20. ve 21. maddeleri ile özel hayatın gizliliği ve korunması öngörülmüş ise de uluslararası antlaşmalar ve gelişen teknolojiler anayasal değişikliği zorunlu kılmıştır. Anayasa değişikliği ile birlikte uygulama kanunu ve bu kanunda öngörülen kurum ve kurullar ihdas edilmiştir. Aslında bu Anayasa değişikliği etrafında hem bireysel hem de sistemsel tüm değişiklikler gerçekleşmiştir. Suç ile mücadele eden Almanya, ABD, İsviçre ve Norveç gibi gelişmiş ülkelerde suçlunun cezalandırılmasından önce masum vatandaşın korunması öngörülmektedir. Bu anlamda kişisel verilerin korunması Türkiye'de önemli bir eksiklikti (Küzeci, 2019). 2010 yılındaki Anayasa değişikliğinden önce kişisel veriler ilgili ilgisiz taraflarca tutulabiliyor ve bireylerin haberi olmadan üçüncü taraflara verilebiliyordu/satılabiliyordu, ayrıca kişilerin izni olmadan kullanılarak dolaşıma sokulabiliyordu. Kişisel verilerin başkalarının eline geçmesi/sahip olması mahremiyetin ciddi şekilde ihlali anlamına gelmektedir. Peki ama kişisel verileri kim elde etmek istiyor ve kim ifşa etmeye çalışıyor? Bankalar, sigorta şirketleri, emlakçılar kısaca bir ürün satan ve pazarlayan herkes kişisel veriler ile ilgilenmektedir. Veri pazarlama şirketleri verileri dağıtmakta ve verileri analiz edip uygun formatta paketledikten sonra diğer firmalara satabilecek değerli bilgilerdir. Kişisel Verilerin Korunması Kanunu çıkmasıyla birlikte bireylere ait verileri tutan

her kesim verileri hangi şartlarda tutacağını ve bu veriler ile hangi sınırlar içinde hareket edeceğini onaylatmak zorunda kalmıştır. Anayasa değişikliğine uygun olarak kanun ile kişisel mahremiyet alanı güvence altına alınmıştır. Örnek olarak Kişisel Verilerin Korunması Kanunu öncesi abone olunan bir GSM şirketinde tutulan kişisel veriler üçüncü taraflara satılarak, kişiler için mahrem olan bilgiler izinsiz paylaşabilirken, yasanın çıkmasından sonra veri sahipliği kavramı getirilmiş ve başkasının eline geçmemesi yasal olarak güvence altına alınmıştır (Kart ve Ketizmen, 2019).

Bilişim Suçları ile Mücadele birimleri yıllık raporlar hazırlamaktadır. Bu raporlar ile suç ile mücadele noktasında kamuoyu aydınlatılmakta ve tehdit değerlendirmesi açısından bilinçlendirme sağlanmaktadır. Bilişim suçlarıyla mücadele için EGM bünyesinde bir daire başkanlığı ihdas edilmesinden sonra da benzer bir faaliyet ile özellikle teknolojik suçlar konusunda suça maruz kalan vatandaşların bilinçlendirilmesine devam edilmiştir. Tüm kamuoyunun bilgi ve değerlendirilmesine sunulan bu istatistikler ile bilinçlendirme artırılarak, suç konusu ve olgusuna dikkat çekilebilir, farkındalık oluşturulmalıdır. 2010 yılı Anayasa referandumu ve içerdiği değişikliklerin de ruhuna uygun olarak genel zabıtanın, bilişim suçlarıyla mücadelede gösterdiği başarı artmış diğer aktörleri de etkilemiştir. Özellikle sivil aktörler mücadele konusunda elde edilen başarılardan dolayı bilişim sistemlerinin kullanımı konusuna daha fazla güven duymaktadır. Anayasa değişikliği suç işlemeye meyilli kişilere (Hackerlar) karşı caydırıcı bir etkisi de gözlenmektedir.

Birey düzeyinde karşılaştırma yapıldığında 2010 Anayasa değişikliği sonrası temel bazı değişiklikler olduğu görülmektedir. KVK Kurum ve Kurulu'nun fiilen oluşturulması ve göreve başlamasının hemen ardından kişisel veri tutan/saklayan tüm resmi ve özel kurum kuruluş ve işletmelerle ilgili yükümlülükler hayata geçirilmeye başlanmıştır. 10.03.2018 tarih ve 30356 sayılı Resmî Gazete'de yayınlanan "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkındaki Tebliğ" ile birlikte veri sorumluları tuttukları veriler ile ilgili bireyleri aydınlatma mecburiyeti getirilmiştir (Kişisel Verileri Koruma Kurumu, 2018). 2010 yılı Anayasa değişikliği ve içerdiği yeniliklerin de ruhuna uygun olarak Finans Sektöründe belirlenen ulusal ve uluslararası standartlar ile birlikte suçun önlenmesine yönelik birçok uygulama devreye alınmıştır. Kredi Kartlarında uygulanan PIN kodu, İnternet Bankacılığında çok kademeli güvenlik önlemleri, ATM cihazlarında kullanılan özel kart girişleri ve parmak izi cihazları gibi birçok uygulama bilişim suçlarının önlenmesi noktasında katkısı olmuştur. Yaygın olan kredi kartı dolandırıcılığı konusunda daha verimli mücadele etmek amacıyla tüm kredi kartlarının ortak şirketi olan Bankalar Arası Kart Merkezi- BKM bünyesinde suçla mücadele

birimlerinin irtibat noktaları oluşturulmuştur. Ayrıca BKM'nin kendi geliştirdiği ve internet üzerinden alışverişi daha güvenli hale getiren bir uygulama ile konuya destek olmaya başlanmıştır. Türkiye'de finans sektörü bilişim suçunun bir türü olan siber ataklar konusunda çok duyarlıdır. Kamu güvenlik politikaları açısından da örnek alınması gereken pek çok özelliğin paralel ve yöntem olarak benzer olduğu düşünülmektedir. Örneğin bankalar kendi güvenliklerini kırarak sistemlerine sızan hackerleri ödüllendirmek suretiyle ya da bünyesine katarak hem siyah alandan beyaz alana geçişlerini sağlamakta hem de yetişmiş insanları bünyesine güvenlik uzmanı olarak katmaktadır. Aynı şekilde Türkiye'de siber suçlardan dolayı yakalanan ve cezasını çeken / rehabilite olan hackerlar siber suçlar alanında kullanılmaktadır (Sandilaç, 2020).

3.1. Terör suçları ile mücadeleye yönelik karşılaştırma

Türk Ceza Kanunu'nda ve 5651 sayılı kanunla mücadele anlamında kolluk kuvvetlerine ciddi yetkiler tanımlanmıştır. MİT yasasında yapılan değişiklikler ile acil müdahale gerektiren konularda mahkeme kararı beklenmeden BTK vasıtasıyla web sitelerinin engellenmesi yetkisi verilmiştir. Kamuoyunda tartışılmadan yasalaşan bu ve benzeri kararlar bireysel haklara gölge düşmeden tekrar ele alınıp şekillendirilmesi faydalı olacağı değerlendirilmektedir. Özgürlük – güvenlik dengesi her alanda olduğu gibi Siber Suçlar ile Mücadele de her zaman gözetilmesi gereken bir kavramdır. Siber terör saldırılarına karşı kritik altyapı işletmecileri (Elektrik, Su, Doğalgaz, Ulaştırma, Bankacılık vb.) önlemlerini almak durumundadır. USOM bünyesinde Kurumsal SOME'ler, Sektörel SOME'ler ve onlara bağlı Kamu/ Özel Kritik Altyapı işletmecileri yer almaktadır. SOME' ler güvenlik olaylarının istatistiklerini toplar, araştırır, paylaşır. Olayın yayılmasını engeller ve gerekli olan faaliyetleri gerçekleştirir. Güvenlik ihlalleri ile ilgili gerekli duyuruları hazırlar ve koordine etmektedir (saglik.gov.tr, 2019).

2010 Anayasa değişikliği öncesi manuel çalışan kritik altyapılar içerdiği değişikliklerin de ruhuna uygun olarak bugün bilişim sistemleriyle kontrol edilmekte ve yönetilmektedir. Enerji üretimi ve dağıtımı, su ve kanalizasyon altyapısı, telekomünikasyon altyapısı, sağlık servisleri ulaşım sistemleri kritik altyapısını oluşturmaktadır. Bunlardan kritik üretim tesisleri, enerji ve su tesisleri SCADA/ICS ile kontrol edilmektedir. Bu manada bu sistemlere yapılacak hacker saldırıları hayati sonuçlara sebebiyet vermektedir. Siber terörizm istatistiğin gri alanında yer aldığından maalesef verilere ulaşılamadığı için ülkemizdeki durumu ile ilgili ancak genel bir değerlendirme yapılmıştır (Kara, Aydın ve Oğuz, 2013).

3.2. Çocuğa karşı işlenen suçlara yönelik karşılaştırma

2010 yılı Anayasa değişikliği de ruhuna uygun olarak çocuklara karşı işlenen suçların ailelere bakan yönü ise T.C. Aile, Çalışma ve Sosyal Hizmetler Bakanlığı ile birlikte çalışılmaya başlanmış böylelikle suçla mücadelenin sadece kolluk güçleriyle yürütülen bir mücadele olmaktan çıkarılmıştır. Öğrenciler önleyici kolluk adı altında kolluk kuvvetleri tarafından bilgilendirildiği gibi çocuklara da psikologlar vasıtasıyla mahremiyet eğitimi verilmeye başlanmıştır (Karataş, 2018). 2011 yılında bilişim suçlarıyla mücadele amaçlı olarak Emniyet Genel Müdürlüğü bünyesinde bağımsız bir daire başkanlığı ihdas edilmiştir. Siber suçlar ile mücadele alanında TÜBİTAK ve Emniyet Genel Müdürlüğü arasında 2015 yılında bir iş birliği protokolü imzalanmıştır (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, 2015). Bu protokol kapsamında TÜBİTAK BİLGEM ile EGM arasında farkındalık ve eğitim, adli analiz ve veri kurtarma, zararlı yazılımlar ile mücadele, büyük veri analizi ve paylaşımı eğitimlerinin verilmesi öngörülmüştür.

TSK Siber Savunma Komutanlığı, bilgi ve iletişim teknolojilerinin ve e-devlet uygulamalarının yayılmasına rağmen, kritik tehdit ve risklerin, altyapı ve komuta kontrol sistemlerinin etkisizliğine yol açtığı düşünülmektedir. Ulusal güvenlik açısından "kara", "deniz", "hava" ve "siber uzay" boyutlarına eklenen siber alanı, ulusal güvenliğin bir parçası haline gelmiştir. Günümüzün savaş ortamının 'beşinci boyutu' olarak da tanımlanan bu yeni alanda tehditleri önlemek için TSK Siber Savunma Merkezi Başkanlığı, gelişmiş savunma alarmı ve tepkisi ile güçlü bir siber savunma yeteneği kazanmak için kurulmuştur. 30 Ağustos 2013 tarihinde TSK Siber Savunma Komutanlığına dönüştürülmüştür.

Ulusal ve Uluslararası iş birliğini gerektiren bilişim suçları ile mücadele kurumsal ve yasal zeminin gelişmesiyle birlikte daha da artmıştır. Uluslararası antlaşmaların gerektirdiği zorunluluktan da kaynaklanan, farklı kurumlar arasındaki bilgi saklama, bilgi paylaşmama ortak operasyon birimlerinin kurulmasıyla azalmaya başlamıştır. Bilişim suçları, 2010 yılı öncesinde de geleneksel suçlarla kıyaslandığında artış hızı bakımından daha ilerideydi. Mücadele yöntemleri ve bu alandaki bilgilendirmelerle oldukça önemli sonuçlar ortaya koymuştur. Öte yandan 2010 yılı Anayasa değişikliği ve içerdiği konuların da ruhuna uygun olarak son yıllarda artış gösteren telefon üzerinden dolandırıcılık suçu kamu spotları ve değişik yöntemlerle yapılan bilgilendirmeler artmış ve sonuç vermektedir. Ayrıca bu süreçte dolandırıcı kişilerin kullandığı yöntemler de gelişmekte, çeşitlenmekte ve değişmektedir. Bu artış ve çeşitlilik karşısında ise genel kolluk acze düşme veya yılgınlıktan ziyade acil müdahale gibi özellikler ortaya çıkarmalıdır. Kolluk kuvvetleri mücadele için yeni

yöntemler geliştirmelidir. Ancak görünen odur ki, bu tür suçlar yeni ve değişik yöntemlerle karşımıza çıkmaya devam etmektedir. Anayasa Mahkemesi 26.11.2020 tarihinde Resmî Gazetede yayınlanarak yürürlüğe giren bir kararına gerekçe olarak mahremiyet vurgusu yapmış 657 sayılı Devlet Memurları Kanunu'nun memurluğa alınma şartlarını düzenleyen 48. maddesinin 8. bendini iptal etmiştir. İptal edilen kural, OHAL ilanı sonrasında getirilmişti ve bütün kamu görevlerine atanacaklar yönünden güvenlik soruşturması ve/veya arşiv araştırması yapılmasını öngörüyordu. (AYM 2019/65 sayılı Karar, 2019)

4. SONUÇ ve ÖNERİLER

Türkiye'de mahkeme kayıtlarına yansıyan haliyle ilk bilişim suçu 1990 yılında işlenmiştir. Yani o tarihten bu yana 30 yıl geçmiştir ve neresinden bakılırsa bakılsın bu suçlarla mücadele için kamu politikası geliştirmeye yarar durumda binlerce bilgi, belge, olay mevcuttur. Ancak bu kadar bilgi belge ve olayın incelenmesinde tarihsel dönüşümler ve karşılaştırmalar özel bir önem arz etmektedir. 2010 yılında meydana gelen Anayasa değişikliği bu açıdan önemli bir tarihsel dönüşüm olarak görülebilir ve yapılan çalışma, bu tarihin kıyas ve dönüşüm bakımından önemini ortaya koymuştur. Nitekim Bilişim Suçlarıyla Mücadele Kamu Politikalarının 2010 öncesindeki çalışmaların en önemli kilometre taşı olarak 2007 yılında çıkarılan 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" görülebilir. Öte yandan 2010 yılında yapılan Anayasa değişikliğinden sonra ise 2016 yılında yürürlüğe giren "Kişisel Verilerin Korunması Kanunu" bilişim suçlarıyla mücadelede düzenlemesi en önemli kilometre taşıdır.

2010 yılı Anayasa değişikliği sonrası değişimler Kişisel Verileri Koruma Kurumu mevzuatı ile sınırlı değildir ancak Kişisel Verilerin Korunması Kanunu (2016) 2010 yılı sonrasındaki en etkili ve köklü mevzuat dönüşümü olmuştur. Siber savaşlara evrilen dünyaya ayak uydurmanın bir gereği olarak Ulusal Siber Güvenlik Stratejisi ve Eylem Planları yayınlanmıştır. Bu planların yürürlüğe konması da 2010 sonrası döneme rastlamaktadır. 2010 yılındaki Anayasa Değişikliği ile Kişisel Verilerin Korunması Kanununun yürürlüğü arasında 6 yıllık bir zaman vardır. Bunun sebepleri ayrıca incelenmelidir ve başka çalışmaların konusu olabilir. Ancak aradan geçen 6 yıllık süre boyunca boş durulmamış ve pek çok hazırlık çalışması yapılmıştır. Yoğun ülke gündemi de düşünülürse Kişisel Verilerin Korunması konusunun önem sırası bakımından kendisine alan açmamıştır.

7 Nisan 2016 tarihinde hayatımıza giren 6698 sayılı Kişisel Verilerin Korunması Kanunu aynı anda başta bireyleri olmak üzere şirketleri ve kurumları bağlayan çok önemli yenilikler getirmiştir. En önemli değişikliğin ise hapis cezası da dahil olmak üzere artan ve caydırıcılığı konusunda hiç şüphe duyulmayan ceza düzenlemeleri olduğu ifade edilebilir. Daha önceki bir kısım düzenlemelerde de veri çalanlara karşı cezalar öngörülmekteyken bu kanun ile birlikte Kişisel Verileri 'çaldıran veya çalınmasına göz yumanlara' da ceza getirilmiştir. Çok önemli sayılabilecek bir diğer yenilik ise verileri çaldıran kurumlara da *kendi kendilerini ihbar etmeyi zorunlu hale* getirmektedir. Daha önceki benzer düzenlemelerde çerçeve çizilmiş ve ceza hükümleri konulmuş olmakla birlikte uygulamada bireylerin haklarını aramak için nasıl bir yol izleyeceği konusu oldukça karmaşıktı. Kişisel Verileri Koruma Kurumunun Kuruluşunun üzerinden kısa bir süre geçmiş olmasına rağmen Kurul'un teknik uzmanlarının ise oldukça yetkin oldukları da gözlenmektedir. Kullanımı hız kesmeden yaygınlaşan mobil cihazlar ve özellikle SMS mesajları konusundaki dağınıklık ve rahatsız edici SMS'lere maruz kalma olgusu da kişisel güvenlik ve mahremiyet alanının ihlali olarak değerlendirilmektedir. Ulusal basında da haber olan somut bir vakıada bir belediye bile bireyleri rahatsız edici mahiyetteki SMS gönderme uygulaması konusunda Kişisel Verileri Koruma Kurumundan ceza almıştır.

Bilişim suçları mevzuatında yapılan düzenlemeler, kolluk kuvvetlerinin düzenli çalışması ve bilgilendirici faaliyetlerin desteklenmesi ile kontrol altına alınabileceği görülmektedir. Ancak, siber suçlarla mücadelenin diğer suçlardan daha dinamik bir temelde gerçekleştiği göz ardı edilmemelidir. İnternet banka dolandırıcılığı suçlarıyla mücadele etmek amacıyla kullanıcıların farkındalık düzeyindeki artış gözlenmektedir. İnternet bankası müşterilerinin mobil imzalar, tek seferlik şifreler üreten cihazlar ve mobil yazılımlar kullanarak güvenliklerini arttırıldığı görülmektedir. Buna ek olarak, kablosuz internetin bir şifre ile kullanılması ve bu tür suçlara zemin hazırlamamak ve farkında olmadan katılmamak için internet aboneliğinin diğer kullanıcılarla paylaşılmaması büyük önem taşımaktadır. Bilişim suçlarıyla mücadele kamu politikalarının geliştirilmesi için eğitim ve bilinçlendirme çalışmaları ile farkındalık yaratılması çalışmaları az ya da çok olsun sürekli olarak yapılmalıdır. Bunun için temel anayasa metninde bir değişikliğe de ihtiyaç olmamıştır, ancak söz konusu eğitimin yeterli düzeyde yapıldığı da söylenemez. Toplumun her kesimine, hedef kitlenin eğitim-kültür düzeyine göre ayrıştırma yapılarak sürekllik arz edecek şekilde bu çalışmalar yapılmalıdır.

Çocuk ve gençlerin korunması özelinde; ebeveynler, eğitim kurumları, sivil toplum kuruluşlarının da dahil edildiği eğitimler düzenlenmelidir. Uygulayıcı kamu ve özel sektör personeli ile yargı mensuplarına ayrıntılı teknik ve hukuki eğitimler

verilmeli, uygulamalı pratik çalışmalar üzerinden somut olay örnekleri analiz edilmeye çalışılmalıdır. Üniversitelerin mühendislik ve hukuk fakülteleri basta olmak üzere, bilişim hukuku ve bilişim suçları alanında gerekli teknik ve hukuki kazanımları içeren dersleri müfredata eklemeleri ve ayrıca yüksek lisans-doktora programlarına da dahil etmeleri oldukça faydalı görünmektedir.

Ulusal bir politika ve strateji geliştirilmesi için her şeyden önce, alt düzeydeki planlar geliştirilmeli, sorumlulukları daha ayrıntılı olarak belirlenmeli, sektörel bazda belirli eylem planları ve eylemleri belirlenmeli ve kritik altyapılar hakkında rehberlik, standart ve çerçeve belgeler hazırlanmalıdır. Standart eylem tarzlarının ve çerçeve belgelerin hazırlanması, olası saldırılara karşı alınacak önlemlere karşı başarı olasılığını artırmaktadır. Yasal çerçevenin oluşturulması için siber saldırılar, uygulama ve kontrol kurallarının belirlenmesi ve saldırılara karşı caydırıcılığı yüksek yasal düzenlemelerin yapılması zorunludur.

Kurumsal yapılanmanın belirlenmesi için 2016-2019 Ulusal Siber Güvenlik Stratejisi planında başlatılan kurumsal sorumlulukların belirlenmesine ek olarak, ilgili tüm tarafların görev, sorumluluk ve yasal dayanaklarının en iyi şekilde belirlenmesi esas olmalıdır. Ulusal teknoloji kullanımı açısından siber saldırılarla mücadelede en önemli faktörlerden biri, tüm yönetimsel ve düzenleyici kurumlarımızla birlikte ulusal teknolojilerin kullanılmasıdır. Başarı sağlanması için öncelikle gelişmiş ülkelerin siber güvenlik uygulamalarının ülkemize aktarılması kapsamında uluslararası işbirliği yapılmalıdır. Ayrıca, siber saldırıların sadece ülke içinden değil, aynı zamanda internet üzerinden dünyanın herhangi bir yerinden yapılabileceği düşünüldüğünde, bu bağlamda diğer ülkelerle işbirliği ve uyum da önemlidir. 2010 yılındaki Anayasa değişikliğinden sonra bilişim suçlarıyla mücadele anlamında meydana gelen değişimlerin karşılaştırmalı olarak analiz edildiği bu makalenin alana ışık tutması ve ardıl çalışmaları teşvik etmesi ümit edilmektedir.

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Politikaları Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazarlarına aittir.

Yazar Katkıları: Hakan Yıldırım ve Volkan Kaplan çalışmanın tüm bölümlerinde ve aşamalarında katkı sağlamışlardır. Yazarlar esere eşit oranda katkı sunmuştur.

Çıkar Beyanı: Yazarlar ya da herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Ethics Statement: The authors declares that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the Journal of Public Administration and Policy has no responsibility and all responsibility belongs to the author of the study.

Author Contributions: Hakan Yıldırım and Volkan Kaplan have contributed to all parts and stages of the study. The authors contributed equally to the study

Conflict of Interest: There is no conflict of interest among the authors and/or any institution.

KAYNAKÇA

Alan, H. (2019). Disiplinler Arası Bir Bilim Dalı Olma Yolunda Yönetim Bilişim Sistemleri ve İşletme Enformatiğinin Temelleri. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi, 17* (2), 69-92.

Anderson, J. E. (1990). *Public Policy Making.* London: Thomas Nelson and Sons.

Bahar, A. (2018). Bilişim Suçları, İletişim ve Sosyal Medya. *İstanbul Aydın Üniversitesi Dergisi. 10*(3), 1-36.

Başlar, Y. (2020). Elektronik Delilin Toplanması ve Muhafazası. *Hacettepe Hukuk Fakültesi Dergisi, 10*(1), 77-107.

Bozkurt, H. (2019). *Kişisel Verilerin İşlenmesinin Hukuki Boyutu.* (Yayınlanmamış Yüksek Lisans Tezi.) Kadir Has Üniversitesi Lisansüstü Eğitim Enstitüsü Hukuk Anabilim Dalı. Kayseri.

Çavuş, F. (2008). Karar Verme, Karar Destek Sistemleri ve Yönetsel Etkinlik. *Akademik Bakış Dergisi, 15,* 1-18.

Dülger, M. V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3*(2), 101-168.

Dye, T. R. (2002). *Understanding Public Policy*. Upper Saddle River: Prentice Hall.

Hekim, H. ve Başıbüyük O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135-158.

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

Kara O., Aydın Ü. ve Oğuz A. (2013). *Ağ Ekonomisinin Karanlık Yüzü: Siber Terör.* Erişim adresi: http://kisi.deu.edu.tr/oguz.kara/Ag%20Ekonomisinin%20karanlik%20yuzu%20siber%20teror.pdf.

Kart, A. ve Ketizmen, M. (2019). Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme. *Kişisel Verileri Koruma Dergisi, 1*(2), 17-29.

Karataş, Z. (2018). Çocukların Cinsel İstismardan Korunmasında Çocuk Adalet Sisteminin Önleyici Fonksiyonu. *Türkiye Sosyal Hizmet Araştırmaları Dergisi. 2*(2), 136-147.

Kurnaz, S. ve Önen, S. (2019). Avrupa Birliğine Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security, 1*(2), 82-103.

Kutlu, Ö., Kahraman S. ve Dinçer S. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarının Analizi. *Assam Uluslararası Hakemli Dergi* (13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı, 1-14.

Küzeci, E. (2019). *Kişisel Verilerin Korunması.* Ankara: Turhan Kitabevi.

Kişisel Verilerin Korunması Kanunu (2018). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

Mutlu, M. S. (2019). *Kişisel Verilerin Soruşturma Evresinde İşlenmesi ve İnsan Hakları Kapsamında Korunması.* (Yayınlanmamış Yüksek Lisans Tezi). Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı. Kayseri.

Nacak, O. (2014). Kamu Politikalarının Belirlenmesinde Yeni İletişim Araçları ve Sosyal Ağların Rolü. *Akademik Bakış Dergisi, 46*, 100-116.

Oğuz, S. (2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi, 13*(2), 121-138.

Sandılaç, N. (2020). Ağ Toplumunda "Ağ" Dışı Kalan Hackerların Muhalefet Biçimi: Hacker Etiği ve Özgür Yazılım. *Sosyal ve Kültürel Araştırmalar Dergisi (SKAD)*, *6*(12), 47-74.

Sektörel SOME Kurulum ve Yönetim Rehberi (2014). Erişim adresi https://www.usom.gov.tr/dosya/1470335484-Sektorel%20SOME%20Rehberi.pdf

Siber Tehdit (2016). *TSK'nın Siber Savunma Komutanlığı.* Erişim adresi: https://sibertehdit.com/tsknin-siber-savunma-komutanligi/

SİSAMER TSK Siber Savunma Merkezi Projesi (2020). Erişim adresi: https://www.ssb.gov.tr/Website/contentList.aspx?PageID=1083&LangID=1

Söylemez, Z. (2019). Ulusal Güvenlik ve Türk İstihbarat Sistemi. (Yayınlanmamış Yüksek Lisans Tezi). Karabük Üniversitesi Lisansüstü Eğitim Enstitüsü Kamu Yönetimi Anabilim Dalı. Karabük.

Tulum, İ. (2006). *Bilişim Suçları ile Mücadele.* (Yayınlanmamış Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Isparta.