Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Literatür Makalesi / Review Article

Avrupa Birliği Siber Güvenlik Kanunu

Sena NEZGITLI[a], Recep BENZER[b,*]

[a, b*] *Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Bölümü, ANKARA 06540, TÜRKİYE*

MAKALE BİLGİSİ

Alınma: 14.12.2019
Kabul: 29.06.2020

Anahtar Kelimeler:
Avrupa Siber Güvenlik Kanunu, Siber Güvenlik, Avrupa, Bilişim Sistemleri

[*]***Sorumlu Yazar:***
e-posta:
rbenzer@gazi.edu.tr

ÖZET

Günümüz dünyası her alanda büyük bir değişim ve dönüşüm içindedir. Bu değişim karşımıza teknoloji ve teknolojinin etkilediği alanlar olarak çıkmaktadır. Artık biliyoruz ki çağ teknoloji ve internet çağıdır. Her ne şekilde olursa olsun dünya çapında gelişmemiş ve köşede kaldığını sandığımız birçok noktaya bile internet hizmeti ulaşmaktadır. Bu olay beraberinde küreselleşmeyi getirerek insanların birbiriyle olan iletişim kavramını zaman ve mekândan bağımsız hale getirmiştir. Ülkeler nihayet bunun üstesinden tek başlarına gelemeyeceklerini anlamış ve siber dünya ile top yekûn bir mücadele anlayışına girerek ortaya "Avrupa Siber Suçlar Sözleşmesi'ni" çıkartmışlardır. 12 Mart 2019 tarihinde Avrupa Parlamentosu Üyeleri tarafından çıkarılan "Siber Güvenlik Kanunu" ile mücadelenin başlatılması sağlanmıştır. Ülkemizde de bu konuda yapılması gerekenler değerlendirilmiştir.

European Union Cyber Security Law

ARTICLE INFO

Received: 14.12.2019
Accepted: 29.06.2020

Keywords:
European Cybersecurity Act, CyberSecurity, European, Information System

[*]***Corresponding Authors***
e-mail:
rbenzer@gazi.edu.tr

ABSTRACT

Today's world is in a big change and transformation in every field. This change emerges as technology and areas affected by technology. Now it is known that the era is the age of technology and internet. In any case, internet service is available to many undeveloped places around the world. This event brought globalization and made people's communication concept independent from time and space. The countries finally realized that they would not be able to overcome it alone and issued the "European Cybersecurity Act" to fight the cyber world. The struggle against the "Cyber Security Law" issued by the European Parliament was initiated on 12 March 2019. In our country, what needs to be done about this subject has been evaluated.

1. GİRİŞ *(INTRODUCTION)*

Tarihten günümüze kadar uluslar için güvenlik, ekonomi ve askeri güce sahip olmak istedikleri en temel unsurların başında gelmektedir. Bu unsurlar teknolojinin gelişmesi ve aslında internetin keşfinden sonra ortaya koyduğu köklü reformlar ile beraber ülkeler için önemli olan bu temel unsurları da oldukça

değiştirmiş ve dünyayı tek bir çatı altında toplayarak küreselleştirmiştir. Bu küreselleşmeye birkaç örnek vermek gerekirse; Fransa'da yapılan bir terör saldırısı haberinin internet erişimi ile dünyanın neresinde olursa olsun dünyadaki herhangi birinin bu habere erişebilmesine imkân verir veya bir videosunun paylaşılmasıyla aslında kendi halinde ve internet ortamından uzak birinin bile bu büyülü dünyaya girmesini sağlayabilmiştir.

İnternetle zaman kavramından bağımsız olan bu erişilebilirlik, bireysel veya kitlesel bilgi paylaşımı ve elbette dünyadaki bütün insanların birbirine bağlamasıyla ortadan kalkan sınırlar beraberinde birçok tehlikeli durumu da maalesef açığa çıkartmıştır. Bunlardan en tehlikeli olabilecek örnekler: Siber zorbalık, internet bankacılık suçları, çocuk pornografisi, şiddet ve nefret söylemi gibi konular başlığı altında düşünüle bilir. Bu hususta dünyadan birkaç örnek vermek gerekirse; İlk örnek teknolojiyi hemen hemen her alanda kullanan Güney Kore'de seçimler internet üzerinden yapılmaktadır. Seçim sonucu mevcut merkezi yönetimin parti lideri tekrar başkanlığı kazanmış ancak oy sayımlarında muhalefetin oylarının yüksek olduğu şehirlerde oylamaya katılımın oldukça düşük olduğu ortaya çıkınca seçimlere şaibe karıştırdığı anlaşılmıştır. Hackerler yardımıyla siber saldırı yapılmış ve oy kullanımını yavaşlatıldığı tespit edilmiştir. Bu olay siber dünyanın tarihine siber saldırıyla gelip siber itirafla giden ilk devlet başkanı olarak kaydedilmiştir. Aynı şekilde, Hollanda bulunan vatandaşlara ve firmalara güvenli işlem yapabilmeleri için dijital imza sağlayan firma İran'lı genç bir hacker tarafından gerçekleştirilen siber saldırı sonrası iflas etmiştir [1-4].

Bu olaylar gösteriyor ki, insanlar iktidar, şöhret ve güç için siber dünyayı etik dışı kullanmaktan çekinmiyorlar. İşte bu süreçte Avrupa Birliği 1976 yılından itibaren konu hakkındaki uzmanlar ile oluşturulan birçok *öneri (recommendation)* 2001 yılına kadar devam etmiş ve 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesi tarafından onaylanarak "Avrupa Siber Suçlar Sözleşmesi" oluşturulmuştur. Bu sözleşme ABD'de dahil 38 devlet taraf olmuştur. Ancak 18 yıllık geçen süre içinde sözleşme sorumluluklarını fazlasıyla yerine getirmiştir ancak 2017 yılından itibaren siber suçlarla mücadele edebilmek için en temel husus bir kanun ve bu kanunun verdiği yetkili bir kuruluş olması gerekir ki bu yasa 12 Mart 2019 tarihinde 586 kabul, 44 red ve 36 çekimser oy ile çıkmıştır.

Bu çalışmada, Avrupa Birliği tarafından çıkarılan Siber Güvenlik Yasasına ilişkin bilgilendirme yapılarak ülkemizde de konuya ilişkin yapılması gerekenler ortaya konulmuştur.

2. SİBER GÜVENLİK YASASI TARİHSEL SÜREÇ *(CYBER SECURITY LAW HISTORICAL PROCESS)*

Yasa ilk olarak Siber Suçlar Sözleşmesi'nin altyapı operatörleri ve internet sağlayıcıları için iş birliğine gidilerek hareket etmesini önermiştir. Ancak bu iş birliği yapmak istemeyen altyapı operatörleri ve internet sağlayıcılar için bağlayıcı olmadığından yasa çıkarmanın gerekliliklerini ortaya koyar bu farkındalık 2017'de yasa için yapılacak olan çalışmaları başlatır. Yapılan çalışmalar neticesinde yasa kapsamında bu işletmeler için yaptırım kararlarını, hukukun üstünlüğü gözetilerek uygulanmış olur. Yasa güvenlik konusunu sadece altyapı operatörü ve internet sağlayıcılar için sınırlamamış elektrik, gaz, ulaşım, tren ve havayolu operatör ve şirketlerini de bu kapsama almıştır. Ayrıca sağlık kurumları ve bankalar hırsızlık girişimi gibi siber dünyada karşılaşılan durumları da anında rapor edeceklerdir etmeyenler yaptırıma tabi olacaktır. Sosyal ağlar kendine özgü yasal süreçlerden ötürü durumun dışında tutulmuştur [5-6].

Buradaki tarihsel sürece geçmeden önce etkili olup kabul gören durumlardan bahsedebiliriz ve bunları sıralayacak olursak [7].

1. Avrupa Parlamentosu, Avrupa Konseyi'nin teklifi (COM, 2017) 0477),
2. Komisyonun önerisini Meclise sunmasına müteakip, Avrupa Birliği'nin İşleyişine İlişkin Antlaşma Madde 294 (2) ve 114. Maddesi (C8-0310 / 2017),
3. Avrupa Birliği'nin İşleyişine İlişkin Antlaşma Madde 294 (3) 'ü,
4. 2 nolu sübvansiyon ve orantılılık ilkelerinin uygulanmasına ilişkin Protokol çerçevesinde, sübvansiyon ve orantılılık ilkelerinin uygulanması konusunda Fransız Senatosu tarafından sunulan gerekçeli görüşü dikkate alarak, yasa tasarısı taslağının sübvansiyon ilkesine uymadığını;
5. 14 Şubat 2018 tarihli Avrupa Ekonomik ve Sosyal Komite görüşünü dikkate alarak [8],
6. 31 Ocak 2018 Bölgeler Komitesi'nin görüşünü dikkate alarak [9],
7. 294 (4) Maddesine uygun olarak, bu Yasanın Kurallar 69f (4) 'e göre Sorumlu Komitesinin onayladığı geçici sözleşmeyi ve Konsey temsilcisi tarafından 19 Aralık 2018 tarihli mektubu ile Meclis temsilcisinin verdiği taahhüdü dikkate almak. Avrupa Birliği'nin İşleyişine İlişkin Antlaşma,
8. İçtüzüğünün 59. Kuralı,
9. Sanayi, Araştırma ve Enerji Komitesi raporunu ve İç Pazar ve Tüketiciyi Koruma Komitesi, Bütçe Komitesi ve Sivil Özgürlükler, Adalet ve İçişleri Komitesi hakkındaki görüşlerini (A8-0264 / 2018) dikkate alarak oluşturulmuştur.

Memorandumda yer alan ve bu yasanın tarihsel sürecini anlatan kronolojik bir akıştan bahsederek bu yasanın nasıl bir tarihsel süreçten geçtiğini düşünecek olursak [7]:

1. 2013 yılında siber suçları azaltmak, siber güvenlik politikası belirlemek ile beraber endüstri ve teknoloji kaynaklarını geliştirmek için AB Siber Güvenlik Stratejisi kabul edilmiştir. Bu bağlamda Avrupa Birliği Ağ ve Bilgi Güvenlik Ajansı (ENISA) için Ağ ve Bilgi Sistemi (NIS) direktifi bu yasa için temel oluşturmuştur.
2. 2016 yılında Avrupa Komisyonu, rekabetçi ve yenilikçi anlayışla Avrupa'nın siber güvenlik endüstrisi için siber esneklik sistemini açıkladı. Bu Avrupa Parlamentosu ve Konsey'in ENISA ile ilgili 526/2013 sayılı Tüzüğü ve AB'nin 460/2004 sayılı Tüzüğünün ("ENISA Tüzüğü") yürürlükten kaldırılmasından bahseder.
3. NIS direktifi temel ekonomik aktörler için güvenlik gerekliliklerini başta Temel Hizmet Operatörleri (OES) için zorunlu kılmıştır. Bu açıdan Dijital Servis Sağlayıcılar (DSP) ve 2016 yılında sağladığı Nesnelerin İnterneti (IoT) gibi internete bağlı birçok cihaz içinde gerekli güvenlik sertifikası alınması fikri öne sürülmüştür. Bu sertifikasyon sisteminde bağımsız AB kurumu olan ENISA'ya sertifikasyon alanındaki ulusal yetkili kuruluşların çalışmalarını bir araya getirmek ve koordine etmek için yetkilendirilmiştir.
4. 2017 Mayıs ayında aynı yılın eylül ayına kadar DSM Stratejisinde ENISA'nın görevini gözden geçireceğini belirterek, siber güvenliğin alanını tanımlama; siber güvenlik sertifikasyon ve standartları ayrıca Bilgi ve İletişim Teknolojileri (ICT) tabanlı sistemlerin daha güvenli hale getirilmesi için önlemler geliştirilmiştir.

Bu maddelere bakarak yasa öncesinde yasanın oluşmasına hizmet eden çalışmaları görebiliriz ve böylece bu yasanın neden gerekli olduğu konusunu anlayabiliriz. Yasanın sürecini ortaya koymakla beraber yasada ön plana çıkacak ENISA hakkında açıklayıcı memorandum da detaylı bilgilendirmeler mevcuttur. 2017 ile beraber işleyen süreç Şekil 1'de görülmektedir.

3. AB SİBER GÜVENLİK YASASI *(EU CYBER SECURITY LAW)*

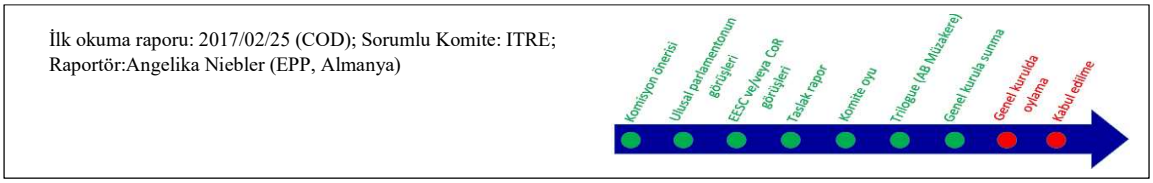
Yasa toplamda 58 madde ve 4 ana başlıktan oluşmaktadır. Bu ana başlıklar altında bölümler ve bu bölümler altında kısımlar yer almaktadır. Yasanın omurgasını oluşturan ve ENISA Ajansının görev ve sorumluluklarını ele alan yer 2. Başlıktır. Şimdi başlıklar ve ele aldıkları maddelere bakacak olursak:

Yasanın ilk başlığı konu, kapsam ve yasada geçen teknik terimlerin tanımlarını içerir. Bu tanımlardan: ASSS sözleşmesinde bahsedilen siber suç kavramından farklı olarak siber tehdit, siber güvenlik, ağ ve bilgi sistemi gibi kavramlar üzerinde durulmuştur.

Yasanın 2. Başlık altındaki bölümünde Avrupa Siber Güvenlik Ajansı (ENISA) hakkında onun görev ve sorumluluklarını verecek yetkiler tanımlanmıştır. Bu başlık için yasanın en detaylı bölümü ve yer teşkil etmesi bakımından en uzun kısmıdır. Ajansın görevi içinde beklenen üye devletlerin siber güvenliği hakkında ayrım gözetmeksizin ceza hukukunu dikkate alacaktır. Ajansa bu yasa ile yüklenen birçok amaç mevcuttur. Bunlardan bazıları:

1. Bağımsızlığı, sağladığı tavsiye ve yardım kararlarının bilimsel ve teknik kalitesi konusunda siber güvenlikle alakalı bir uzmanlık merkezi olacaktır.
2. Ajans, üye devletlerin siber güvenlik ile ilgili politikalarının geliştirilmesi ve uygulanmasında yardımcı olacaktır. Bu da ajansa kapsamlı bir yekti getirmektedir ve onu otoriter kılmaktadır.
3. Ajans, üye devletlerin özellikle sınır dışı olayları durumunda, siber tehditlerin önlenmesi ve bunlara cevap verilmesi konusundaki eylemlerini tamamlamak amacıyla bu birliğin içinde siber güvenlik kapasitesini arttırmak gibi birçok durumu vardır.

Burada iş birliği ve ajansın yetkilerini genişleterek Bilgisayar Acil Durum Müdahale Ekibi (CERT) ve Ulusal Bilgisayar Güvenliği Olay Müdahale Ekipleri (CSIRT's) geliştirilmesine etkin rol alması gerektiği yasa maddesi ile hukuksal bir dayanağa bağlanmıştır.



Şekil 1. Avrupa Siber Güvenlik Yasası'nın kabul edilme süreci [10]
(The adoption process of the European Cyber Security Act)

Ajansın siber saldırının karşısında durarak siber güvenlik ve alınacak tedbirler üzerindeki özellikle internete bağlanan IoT'lar için sertifikasyon ve standardizasyon konusunda yükümlülükler getirilmiştir ve bunun sonunda yasanın 44'üncü maddesindeki "Bilgi İletişim Teknolojileri (BİT) ürünleri ve hizmetleri Avrupa siber güvenlik şeması hazırlama" ve 53'üncü maddesi uyarınca "Avrupa Siber Güvenlik Sertifika Grubu'na sekretaryayı sağlamada yardım etmek" sorumluluğu getirilmiştir. Yasa hazırlayıcılar konunun özel uzmanlık alanı getirdiğini bildiği için ENISA'ya ortaya çıkan teknolojileri takip etme bu yeni teknolojilerde siber güvenlik üzerinde sosyal, yasal, ekonomik ve düzenleyici etkileri için konuya özel değerlendirme yapmasını zorunlu kılarak piyasa takibini birçok açıdan yapmasını ve ilerlemeleri zamanında keşfetme kolaylığı sağlanmıştır. ASSS'de olduğu gibi yasanın bu kısmında ulus boyutunda değil uluslararası alanda iş birliği organizasyonu esas kılınmıştır. Bu başlık altında ilk bölümde bunlar bahsedilmektedir.

Bu başlık altında 2. Bölüm 'de Ajansın nasıl organize edileceği yasa maddeleri ile belirlenmiştir. Ajans Yönetim Kurulu, İcra Kurulu, İcra Direktörü, Daimî Kurum Sahibi Grubundan oluşmaktadır. Bu birimlerin işlevlerini yerine getirmesi adına 14. Maddede Yönetim Kurulu, 18. Maddede İcra Kurulu, 19. Maddede İcra Direktörü, 20'nci Maddede Daimî Kurum Sahipleri Grubunun yetkileri tanımlanır. Kısaca bu birimler için Yönetim Kurulu "her üye devletin bir temsilcisi ve komisyon tarafından iki temsilciden oluşur ve tüm temsilcilerin oy hakkı vardır." Bu sistem alınacak kararlarda çok sesliliği ön plana çıkararak fikir birliğinde buluşmayı hedefler. Elbette bu kurulun önemli görevlerini saymak gerekirse 29. Maddesine göre Ajansa uygulanacak olan finansal kurallarını, Madde 17'ye göre 3'te 2 çoğunlukla Ajansın programlama belgesini kabul eder. Avrupa Yolsuzlukla Mücadele Ofisi (OLAF) ve çeşitli iç veya dış denetim raporları ve değerlendirmelerinden kaynaklanan bulgu ve önerilerin yeterli şekilde takip edilmesini sağlamak kurulun görevidir. Atanan makam için Yetkili Personel Görevlisi Atama Yetkileri ve Avrupa Birliğinin Diğer Görevlilerinin İstihdam Koşullarını ve Yetkilendirilen Kuruluşa İstihdam Koşullarını Verdiği İstihdam Sözleşmesini imzala görevi verilmiştir. Yönetim Kurulu ayrıca atanan makamın yetki vermesini durdurma konusuna da haizdir, İcra Direktörüne alt üyelerce yetkilendirilenlere karar verebilir ki bu hiyerarşik gücü arttırmaktadır. Yönetim Kurulu Başkanı, üyelerin 3'te 2'sinin ile başkan seçilir, başkan yardımcısını seçer görev süresi 4 yıldır. Yönetim Kurulu başkan tarafından yılda en az iki kez olağan toplantı yapar. Alınacak kararlar demokrasinin gereğinden ötürü oy çokluğu ile alınır. Bu kısımda başkan oylamaya katılabilir. Bu kısım usul ve esaslar konusundan kanunun çerçevesini düzgün şekillendirmektedir. Diğer kurul Yürütme Kuruludur ki bu Yönetim Kuruluna yardımcı olmak için vardır. Bu yönetim kurulunda alınacak kararları hazırlar, OLAF araştırmalarındaki, çeşitli iç ve dış denetim raporlarındaki bulguları takibini sağlar ve İcra Direktörüne madde 19'daki yönetim ve bütçe konularına dair Yönetim Kurulu kararlarının uygulanmasında yardımcı olur. Bu hazırlıkların güncel tutulabilmesi adına en az 3 ayda bir toplanılır. Ajans, görevlerini yaparken bağımsız olan İcra Direktörü tarafından yönetilir. İcra Direktörü Yönetim Kuruluna karşı sorumludur. Genel Müdür, davet edildiğinde görevlerinin yerine getirildiğini Avrupa Parlamentosu'na bildirir. Konsey, İcra Direktörünü faaliyetlerinin performansı hakkında rapor vermeye davet edebilir İcra Direktörü başlıca:

1. Ajansın günlük yönetimi
2. Yönetim Kurulu tarafından alınan kararları uygulamak
3. Taslak tek programlama belgesini hazırlamak ve Komisyona sunulmadan önce onay için Yönetim Kuruluna sunmak gibi madde 19'a 3'te belirtilen görevlerden sorumludur.

Kalıcı Paydaş Çalışma Grubuna bakacak olursak: İcra Direktörü tarafından yapılan bir teklifle hareket eden Yönetim Kurulu, BİT endüstrisi, kamuya açık elektronik iletişim ağları veya hizmet sağlayıcıları gibi ilgili paydaşları temsil eden tanınmış uzmanlardan oluşan bir Daimî Menfaat Sahipleri Grubu oluşturur. Tüketici grupları, siber güvenlikteki akademik uzmanlar ve [Avrupa Elektronik İletişim Kodunu Oluşturma Yönergesi] altında yasa uygulayıcı ve veri koruma denetleme makamları olarak bildirilen yetkili makamların temsilcilerinden oluşur. Kalıcı Paydaş Çalışma Grubu için, özellikle Yönetim Kurulunca, İcra Direktörünün önerisi ve Grubun işleyişi ve Yönetim Kurulunca üyelerin sayısı, bileşimi ve atanması ile ilgili prosedürler belirtilir.

Bölüm 3'de ise ENISA'nın kurulan bu 4 birimi için bütçe kurulumu ve bu bütçe yapısının nasıl olacağı madde 26 ile 30 arasında ele alınmıştır. Bu bölüm ileride çıkabilecek finansal problemlere tedbiren oluşturularak Ajansın işleyişinde sıkıntı çıkmaması için üzerinde yoğun çalışmalar yapılmıştır. İcra Direktörü her yıl, Ajansın bir sonraki mali yıla ilişkin gelir ve gider tahminlerini içeren bir taslak beyanı hazırlar ve taslak oluşturma planıyla birlikte Yönetim Kuruluna iletir. Bu işlem hem hiyerarşinin tam işlemesini hem de bütçe kontrolü için alınabilecek iyi bir tedbirdir. Bütçe kabul aşaması madde 26'ya göre uygulanır. Bütçeyi Yönetim Kurulu kabul eder. Ajans gelirleri madde 29'da belirtilmiştir ve ajanın personel, idari ve teknik destek, altyapı ve operasyonel giderleri bu gelirlerle karşılanır.

Bu başlık için son bölümdeki genel hükümlere geçmeden bu işleri yapacak olan bu konuda yeterli donanıma sahip Ajans personelini düşünürsek burada özel bir istihdamdan ziyade Personel Yönetmeliği ve Diğer Hizmetçilerin İstihdam Koşulları ve Birlik kurumları arasında bu Personel Yönetmeliğine etkide bulunma konusunda anlaşma ile kabul edilen kurallar Ajans çalışanlarına uygulanır. Bu durumlar madde 31 ile 34 arasında açıklanmaktadır.

Bu başlıktaki son bölüm genel hükümler kapsamında madde 35 ile 42 arasında Ajansın yasal statüsü, sorumluluğu, kişisel verilerin korunması, üçüncü ülkeler ve uluslararası kuruluşlar gibi durumları kapsar. Ajansın yasal statüyü elde edebilmesi için bu Ajans Birliğin bir organı olacak ve tüzel kişiliğe sahip olacaktır. Ajans, İcra Direktörü tarafından temsil edilir ve sorumluluğu söz konusu sözleşmeye uygulanan yasa ile yönetilir. Elbette ki ENISA Ajansı hakkında yasada her şey düzenlenmiştir ve ajans şeffaflık adına faaliyetlerinde idari olarak kontrol edilmesi gerekmektedir ve bu konuda Avrupa Birliği'nin İşleyişine İlişkin Anlaşma (TFEU)'nın 228. Maddesine göre "*Avrupa Parlamentosu tarafından seçilen bir Avrupa Ombudsmanı, Birliğin herhangi bir vatandaşından veya Bir Üye Devletinde tescilli birliğini, Birliğin faaliyetlerinde kötü idare vakalarına ilişkin olarak ikamet eden ya da bir Üye Devlette ikamet eden herhangi bir gerçek veya tüzel kişiden şikayet alma yetkisine sahip olacaktır. Avrupa Birliği Adalet Divanı haricindeki yargı rolü dışında kurumlar, organlar, makamlar veya ajanslar. Bu tür şikayetleri inceler ve rapor eder."* Ombudsman tarafından denetlenir.

Yasanın 3. Başlığında Siber Güvenlik Alanında Belgelendirme Çerçevesi oluşturulmuştur. Burada Avrupa Siber Güvenlik Sertifikasyon programı, programın hazırlanması, kabulü, güvenlik amaçları, güvence seviyeleri ve şema unsurlarının yanı sıra ulusal düzeyde de siber güvenlik program ve sertifikasyonunda denetleme makamlar, uygunluk değerlendirme kuruluşları unutulmamıştır. Bu yasanın 43 ile 54. Maddeleri arasında belirtilmiştir. Bunlara uymayanlar için ceza hukuku etkin kılınarak birlikteki tüm devletlere sertifikasyon ve uyum göstermeleri konusunda yardımlar ve yaptırımlar ön görülür. Öncelikle bu başlık dünya çapında gerçekleşen büyük saldırılardan IoT'ların kullanılmasıyla bu cihazlardaki zafiyetleri engellemek için ortaya çıkmıştır. Tarihte internet üzerinden yapılan en büyük saldırılardan biri de internet sitelerine haber olan "*Mirai: İnternetin düşüşü*" olmuştur. Bu saldırıda Nesnelerin İnternetinin ortaya çıkması ile Botnetlerde hiçbir antivirüs programı olmaması nedeniyle gerçekleşmiştir. Japonca'da "gelecek" anlamına gelen Mirai olarak adlandırılan kötü amaçlı bir yazılım üzerinden kurulan bu zombi donanma ile akıllı cihazlara yapılan büyük bir DDoS saldırısına dayanmaktadır. PayPal, Twitter, Netflix, Spotify, PlayStation çevrimiçi hizmetleri ve ABD'deki diğer pek çok kişi bu saldırıdan etkilenmiştir. Bu saldırı ile gerekli güvenlik önlemlerinin alınması gerektiği bir kez daha görülmüştür [11-13]. Şunu biliyoruz ki maalesef siber saldırılar olmadan siber güvenlik önlemi alınamaz, işte bu olayın olması bu başlığın omurgasını oluşturmuştur. Siber saldırı ve güvenlik arasında zaman içerisinde belirli şartların olgunlaşmasıyla deneyim kazanılır. İşte bu yüzden bu başlık güvenli sertifikasyon ve Avrupa standartlarını BİT ürünleri ve hizmetlerine uygulamak isteyerek bu denli büyük çaplı saldırılarda hasarın en aza indirilmesi sağlanmak amacıyla oluşturulmuştur. Avrupa Siber Suçlar Sözleşmesi için daha çok tamamlanan suç süreçlerine maddi ceza hukuku ve usul hukuku uygulanırken burada daha çok saldırı öncesi tedbir almak bunu yasal düzen içinde uygulamak ve güvenlik açıklarını her ne şekilde olursa olsun kapatmak için belirli bir standart geliştirmek bu başlığın en temel hedefidir. Avrupa Siber Güvenlik Sertifika Programının hazırlanması ve kabulü için [14]:

1. Komisyon'dan gelen bir talep üzerine, ENISA, bu Yönetmeliğin 45, 46 ve 47. maddelerinde belirtilen gereklilikleri karşılayan bir aday Avrupalı siber güvenlik sertifikasyon planı hazırlar. 53. Maddede kurulan Üye Devletler veya Avrupa Siber Güvenlik Sertifika Grubu (Grup), Aday Avrupa siber güvenlik sertifikasyon planının Komisyona hazırlanmasını önerebilir.
2. Bu maddenin 1. Paragrafında belirtilen aday programları hazırlarken, ENISA tüm ilgili paydaşlara danışacak ve Grup ile yakın işbirliği içinde olacaktır. Grup, ENISA'ya, gerektiğinde görüş bildirmek de dahil olmak üzere, aday programın hazırlanmasına ilişkin olarak ENISA'nın ihtiyaç duyduğu yardım ve uzman tavsiyesini sunmaktadır.
3. ENISA, bu maddenin 2. fıkrası uyarınca hazırlanan aday Avrupa siber güvenlik sertifikasyon planını Komisyona iletir.
4. ENISA tarafından önerilen aday programına dayanan Komisyon, Madde 55 (1) uyarınca, 45, 46 ve 47. Maddelerin gereksinimlerini karşılayan BİT ürünleri ve hizmetleri için Avrupa siber güvenlik sertifika şemaları öngören uygulama yasaları uygulayabilir.
5. ENISA, Avrupa siber güvenlik sertifikasyon programları hakkında bilgi ve tanıtım sağlayan özel bir web sitesi sağlaması gerekir.

Bu başlık için Avrupa siber güvenlik sertifikasyon programlarının güvence seviyeleri için yasanın 46. Maddesinde temel, önemli ve yüksek olarak 3

kategoriye ayrılmıştır. Temel güvence seviyesi, bir BİT ürün veya hizmetinin iddia edilen siber güvenlik niteliklerinde sınırlı bir güvencesi sağlar. Önemli güvence seviyesi, bir BİT ürünü veya hizmetinin iddia edilen güvenlik niteliklerine büyük ölçüde güvence sağlar. Güvence seviyesi yüksek olan ise BİT ürün veya hizmetlerinde güvence düzeyi en esaslı olan güvence sağlar. Madde 47 sertifika şeması ve özelliklerinden bahseder. Bu kısım sadece Avrupa Birliği için değil Madde 49 ve 50'de ise ulusal sertifikasyonun nasıl yapılacağından bahsedilir. Bu ürün ve hizmetler için de "*akreditasyon en fazla 5 yıl süreyle verilir..."* Madde 51'deki beyan ürün ve hizmetler konusunda sertifika sürecini etkin kılarak bu ürün ve hizmetleri yeni teknoloji ile daha güvenli hale getirmek istemektedir. Burada ürün ve hizmetler konusunda "*44. maddeye göre kabul edilen her Avrupa siber güvenlik sertifikasyon programı için, ulusal sertifika denetim otoriteleri yetkili makamlar, 46 ncı maddede belirtilen ve herhangi bir gecikmeden, sonradan yapılan değişiklikler belirli güvence seviyelerinde sertifika vermeleri için akredite edilmiş uygunluk değerlendirme kuruluşlarının Komisyonuna bildirirler*." Madde 52 ile interaktif bir süreç ve yapılan ürün ve hizmet değişikliklerinden haber olunması ve BİT konusunda güncel kalınmak amaçlanmıştır. Bu çalışmaların tamamı için esas alınan ve bu faaliyetleri yapacak olanda "*Avrupa Siber Güvenlik Sertifika Grubu*" dur. Madde 52'e göre yasa ile görevi belirtilmiştir. Tüm bu sertifikasyon çalışması için madde 54'de "*Üye Devletler, bu Başlığın ihlallerine ve Avrupa siber güvenlik sertifikasyon programlarına uygulanacak cezalara ilişkin kuralları belirleyecek ve bunların uygulanmasını sağlamak için gerekli tüm önlemleri alacaktır. Verilen cezalar etkili, orantılı ve caydırıcı olacaktır...*" birlikte uymayan devletler için yaptırımlar öngörülmüştür.

Yasanın son başlığında Nihai Hükümler kapsamında Komite ile alakalı prosedür, komisyon hakkındaki değerlendirme ve gözden geçirme 526/2013 (EC) sayılı Tüzüğün yürürlükten kaldırılması ve bu yasanın son maddesi olan 58. Maddesinde ise yasanın resmî gazetede yayınlandıktan sonraki yirminci gününde yürürlüğe gireceği bahsedilerek karışıklığın önüne geçilmiş ve yasa tamamlanmıştır.

Avrupa Birliği politikaların izlenmesini takip edecek bir birimin Cumhurbaşkanlığı bünyesinde tesis edilmesi Türkiye için bir şans alabileceği de bildirilmektedir [15]. AB örneği yanı sıra ABD, Rusya ve Çin gibi ülkeler iyi bir şekilde analiz edilip, gerekli mekanizma kurulabilirse siber güvenlik alanı bir sorunlu alan olmaktan çıkar, düzenlenen ve kontrol edilen bir boyuta taşınabilir [15].

3. SONUÇLAR *(CONCLUSIONS)*

Avrupa Siber Suçlar Yasası, yasanın önemi, yasanın tarihsel süreci, yasanın çıkmasında neden olan güncel olaylar ve tüm bu etkileri incelemiştik. Bu bölümde yapılan tüm araştırma konusunda hangi çıkarımlarda bulunduğumuz üzerine iyi bir analiz bölümü olacaktır. Bu ya en temel olarak teknoloji, bu teknolojinin yenilikleri, bu yeniliklerin avantaj ve dezavantajları gibi birçok konuya katkı sağlaması konusunda birçok kurum ve kuruluşa özellikle de Avrupa Birliğinde bulunan devletlere yeni bir ufuk sağlamaktadır. Bazı bölümlerdeki bazı kısımlarda ASSS ile bu yasayı kıyaslanmış olunabilir ki bunun asıl dayanağı işlenen bir siber karşısında alınacak siber güvenlik ilişkisinin birbirinin geri beslemesi şeklinde hareket etmesinden kaynaklanmaktadır. Unutulmamalıdır ki, teknoloji ve internetin ilk gelişim evresinde ne bu kadar siber saldırı ne de bu kadar siber güvenlik çabası mevcuttur. İnsanlar bireysel veya toplu olarak gelen bu sistemlerin açıklarını fark ettiler bunu etik dışı olarak başka insanlar üzerinde gerek şöhret gerek haksız kazanç gibi illegal yollarla kullandılar. Elbette devletler, uzmanlık sahibi etik düşünce yapısına sahip birçok kişi veya kişi toplulukları da bu güvenlik zafiyetlerini kapatmak için çalıştılar. Nitekim günümüz dünyası her konuda olduğu gibi siber alanda da iyi-kötü çalışmasında önemli bir rolünü aldı. Gerek ASSS gerek ASSY da bu uzun soluklu sürece dahil oldu. Yasanın incelenmesi ile beraber gerekli çıkarım ve incelemeleri hatta eksiklikleri düşünecek olursak:

1. Yasa tıpkı ASSS gibi ilk bölümünde tanımlar ile başlar burada sözleşmeden ayıran bir kısım mevcuttur. ASSS'de sözleşmenin esas konusu olan "siber suç" tanımı geniş yelpazeli olduğundan tanımı yapılmamış lakin yasaya esas oluşturulan "siber güvenlik" teriminin tanımı yapılmıştır.
2. Yasa oluşma süreci bakımından kendini her ne kadar eksiklikleri olsa bile hızlı toparlamış ve ortaya çıkmıştır.
3. ASSS ile kıyaslamak gerekirse yasa adından da anlaşılacağı gibi sözleşmeden farklı olarak yaptırım ve uygulanacak cezalar yerine üye ülkelere hem ülke içi hem de birlikle beraber hareket edip güvenlik alanındaki eksikliklerini gidererek suçu daha başta önlenmesi gerektiğini yasal güvence altına almış ve zorunluluklar getirmiştir.
4. Elbette bu yasa oluşurken bazı tüzüklerin iptali söz konusu olmuştur. Çünkü yasanın hem bu tüzüğü kapsaması ve Avrupa'nın özellikle güvenlik alanında çağı yakalamak ve yeterli tedbirleri alma kaygısı bu durumu tetiklemiştir. Teknoloji ve siber alanda güncellik her konudan önce gelmektedir.

5. Yasa özellikle siber güvenlik hakkında görev ve sorumluluğu alabilecek olan Avrupa Siber Güvenlik Ajansı (ENISA), birçok yetki vermiş ve bu yasanın Başlık 2 kısmında alt bölümler ve maddelerle açıkça ortaya koymuştur.
6. Yasa ayrıca ENISA ile sınırlı kalmayarak 4 temel başlıkta Ajansın işleyişi kurulları, İcra kurulu ve direktörlüğününde yetki sınırlarını belirtmiştir.
7. İleride çıkacak yasal tıkanıklıklara karşı ENISA'nın görev yetkileri ve birimleri maddelerle güvence altına alınmıştır. Ajansın yetkili olarak davranması için ajansa ait olacak gelir gider bütçesi oluşturulmuştur. Bu güvenlik alanı için Ajansı her konuda yetkin kılmak için yapılmıştır.
8. ASSS'de olduğu gibi yasanın bu kısmında ulus boyutunda değil uluslararası alanda iş birliği organizasyonu esas kılınmıştır. Bu başlık altında ilk bölümde bunlar bahsedilmektedir. Lakin BİT ürün ve hizmetlerin sertifikasyonu konusunda birliğe üye devletlere kendi ulusal düzenleri konusunda da sertifikasyon standardı belirlemeleri yasa maddeleri ile zorunlu kılınmıştır.
9. Üzerinde durulan en önemli konulardan birisi ise BİT ürün ve hizmetlerinin sertifikasyon seviyeleri ve buna göre güvenlik seviyeleri ile beraber aslında IoT başta olmak üzere IP adresi ile internete bağlanan her cihaz için güvenlik açıklarının kapatılarak bu cihazların zombileştirilmesinin önüne geçerek bu cihazlarla yapılan dünya çapında daha önce görülen Ddos veya başka siber ataklar için ihtimalleri azaltmaktır. Yani yasa geçmiş tecrübelerden büyük dersler çıkartıp siber saldırıların yıkıcı etkisini daha en başından önünü kesmek istemiştir.
10. Yasa kendini güncel tutmak için sertifika alan BİT ürün ve hizmetlerine 5 yıl şartı getirmiştir. Çünkü siber dünya 7/24 çalışan teknolojinin olabildiğine hızlı değiştiği ve her geçen gün yeni bir saldırı modelinin piyasaya çıktığı bir alandır. Bu açıdan BİT ürün ve hizmetleri buna ilişkin olarak kendini sadece ileri teknolojiye değil ileri güvenlik seviyesine de hazırlamalıdır.
11. Avrupa Birliği sözleşmeden ziyade son zamanlarda olan siber dünyadaki değişikliklere ayak uydurmak için bunu yasa ile güvence altına almış ve güvenlik açıkları ile ilgili ceza kararları ön görmüştür. BİT ürün ve hizmetlerinde güvenlik sertifikasyonu önemlidir uymayan birlikteki ülkeler için ceza maddesi etkili, orantılı ve caydırıcı olacağı söylenmiş ancak hangi kural ihlaline karşı nasıl bir cezalandırma yapılacağı detaylı açıklanmamıştır. Bu açıdan yasa çerçeve olarak kalmış kazuistik (detaylı anayasa) olmamıştır.
12. 58. Madde de yasanın resmî gazetenin yayınlanmasından itibaren ne zaman yürürlükte olacağının kesin olarak belirtilmesi Avrupa Birliği ülkeleri, BİT ürün ve hizmetleri ve buna bağlı birçok sektör için kafa karışlığını gidererek hükümler ve buna tabi olma durumlarını da aydınlatmış olur.

İşte bu sonuç ve çıkarımlar ile beraber bu yasa, bu yasanın başlıkları, içerik analizi ve hukuksal yorumu, eksiklikleri ve ASSS ile olan ortak ve farklı yönleri farklı bir bakış açısı ile çok boyutlu olarak ele alınmıştır.

Düzenleme ile, ürün ve hizmetlerin tasarımından geliştirilmesine, bunların son kullanıncaya teslimine değin tüm süreçleri etkileyecek ve üretim yönetimi ve planlamada "siber güvenliğin temel bileşen olarak dikkate alınmasına" neden olacak tüm piyasa koşullarını değiştirmeye aday bir yapı oluşturulmaktadır. Bu yapının ise çok büyük bir ekonomik etkisinin olacağı anlaşılmaktadır.

Dijital dönüşümün yaşandığı bu süreçte, kişisel verilerin korunmasında alınacak teknik ve idari tedbirlerden, internete bağlı cihazlar, sigorta hizmetleri ve ihale süreçlerine kadar akla gelebilecek her alanda "siber güvenlidir" onayı bulunan ürünler tercih sebebi olacağına göre ülkemizde de kendi çözümlerimiz için hem hukuki hem de teknik adımlar atılmalıdır.

TEŞEKKÜR *(Acknowledgment)*

Bu çalışma, 09-12 Ekim 2019 tarihlerinde İstanbul'da gerçekleştirilen 6. Uluslararası Yönetim Bilişim Sistemleri Konferansı'nda sözlü bildiri olarak sunulmuştur.

KAYNAKLAR *(References)*

[1] Life (Over) IP Siber Dünyada Suç Kavramı ve Sosyal Yaşama Etkileri. 2014 http://blog.lifeoverip.net/2014/12/27/siber-dunyada-suc-kavrami-ve-sosyal-yasama-etkileri/ (Alıntı tarihi: 16.05.2019)

[2] F. Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi." *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28, 2017.

[3] O. Değirmenci, "Bilişim Suçları" Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi. İstanbul. 2012.

[4] European Parliament The Cybersecurity Act strengthens Europe's cybersecurity. 2019. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity (Alıntı tarihi: 19.05.2019)

[5] CyberMag "Avrupa Çapında Siber Güvenlik Kanunu Kabul Edildi." 2015. https://www.cybermagonline.com/avrupa-capinda-siber-guvenlik-kanunu-kabul-edildi (Alıntı tarihi: 20.05.2019)

[6] B. Alaca, "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle)." Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi. Ankara. 2008.

[7] European Parliament EU Cybersecurity Act. 2019. http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.html?redirecttitle1 (Alıntı tarihi: 22.05.2019)

[8] Repart 1, "European Economic and Social Committee Report", OJC 227, 28.6, p. 86, 2018.

[9] Report 2, "European Economic and Social Committee Report" OJC 176, 23.5. p. 29, 2018

[10] Report 3, "European Parliament, ENISA and New EU Cybersecurity Act." 2019. http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/625160/EPRS_ATA(2019)625160_EN.pdf (Alıntı tarihi: 24.05.2019)

[11] Report 4, "Kasperky Gelmiş Geçmiş En Ünlü 5 Siber Saldırı." 2018. https://www.kaspersky.com.tr/blog/five-most-notorious-cyberattacks/5394/

[12] C. Kolias, G. Kambourakis, A. Stavrou ve J. Voas, "DDoS in the IoT: Mirai and other botnets." *Computer*, *50*(7), 80-84, 2017.

[13] D. Bekerman, D. "New Mirai Variant Launches 54 Hour DDoS Attack against US College," *blog, Imperva Incapsula*, 29 Mar. 2017. www.incapsula.com/blog/new-mirai -variant-ddos-us-college.html (Alıntı tarihi: 26.05.2019)

[14] Report 5, "European Commission Explanatory Memorandum." 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN (Alıntı tarihi: 22.05.2019)

[15] Kutlu, Ö., Kahraman, S., & Dinçer, S. 2019. Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Politikalarinin Analizi. ASSAM Uluslararası Hakemli Dergi, 13. Uluslararasi Kamu Yönetimi Sempozyumu Bildirileri Özel Sayisi, 1-14